

12000 ةلسلس لوصول مئوق ذي فنت تنترنإل تاهوم نم

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[نظرة عامة على دعم قائمة التحكم في الوصول \(ACL\) على موجه الإنترنت Cisco 12000 Series](#)
[قوائم التحكم في الوصول \(ACL\) المستندة إلى ASIC مقابل قوائم التحكم في الوصول \(ACL\) المستندة إلى وحدة المعالجة المركزية](#)

[تصفية مستوى التحكم والإدارة](#)

[تكوين قوائم التحكم في الوصول إلى مسار تلقي IP](#)

[دعم قائمة التحكم في الوصول \(ACL\) إلى IPv4 حسب نوع بطاقة الخط](#)

[المحرك 0 - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك 1 - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك 2 - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك ISE \(محرك خدمات 3 IP\) - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك 4 \(POS\) - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك +4 \(POS و DPT\) - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[المحرك +4 \(إشنت\) - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[تسجيل قائمة التحكم في الوصول \(ACL\)](#)

[قائمة التحكم في الوصول \(ACL\) الخاصة بإخراج IPv4 - مصفوفة عمليات تفاعل بطاقة الخط](#)

[دعم قائمة التحكم في الوصول إلى IPv6](#)

[مرجع أوامر قائمة التحكم في الوصول \(ACL\) ل Cisco 12000](#)

[مسرد المصطلحات](#)

[معلومات ذات صلة](#)

المقدمة

يصف هذا المستند دعم قوائم التحكم في الوصول (ACL) على موجهات الإنترنت من السلسلة 12000 من Cisco.

المتطلبات الأساسية

المتطلبات

Cisco يوصي أن يتلقى أنت معرفة من الأساسية من كيف ACL يعمل على Cisco مسحاج تخديد.

راجع هذه المستندات للحصول على معلومات عامة حول قوائم التحكم في الوصول (ACLs) وتطبيقاتها:

- [قوائم التحكم في الوصول: نظرة عامة وإرشادات](#)
- [تكوين خدمات IP: تصفية حزم IP](#)

[المكونات المستخدمة](#)

تستند المعلومات الواردة في هذا المستند إلى موجهات الإنترنت من السلسلة 12000 من Cisco.

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.

[الاصطلاحات](#)

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات](#).

[نظرة عامة على دعم قائمة التحكم في الوصول \(ACL\) على موجه الإنترنت Cisco 12000 Series](#)

على موجه الإنترنت من السلسلة Cisco 12000، يمكن معالجة قوائم التحكم في الوصول (ACL) في الأجهزة (الدائرة المتكاملة الخاصة بالتطبيق - ASIC)، أو البرنامج (وحدة المعالجة المركزية الخاصة ببطاقة الخط)، أو كميزة هجينة - تتم معالجتها في البرنامج باستخدام المساعدة في الأجهزة. تعتمد ما إذا كانت قائمة التحكم في الوصول (ACL) تتم معالجتها في الجهاز أو البرنامج على تطبيق قائمة التحكم في الوصول (ACL) ونوع محرك بطاقة الخط والتفاعل من قوائم التحكم في الوصول (ACL) في بطاقات الخط الأخرى.

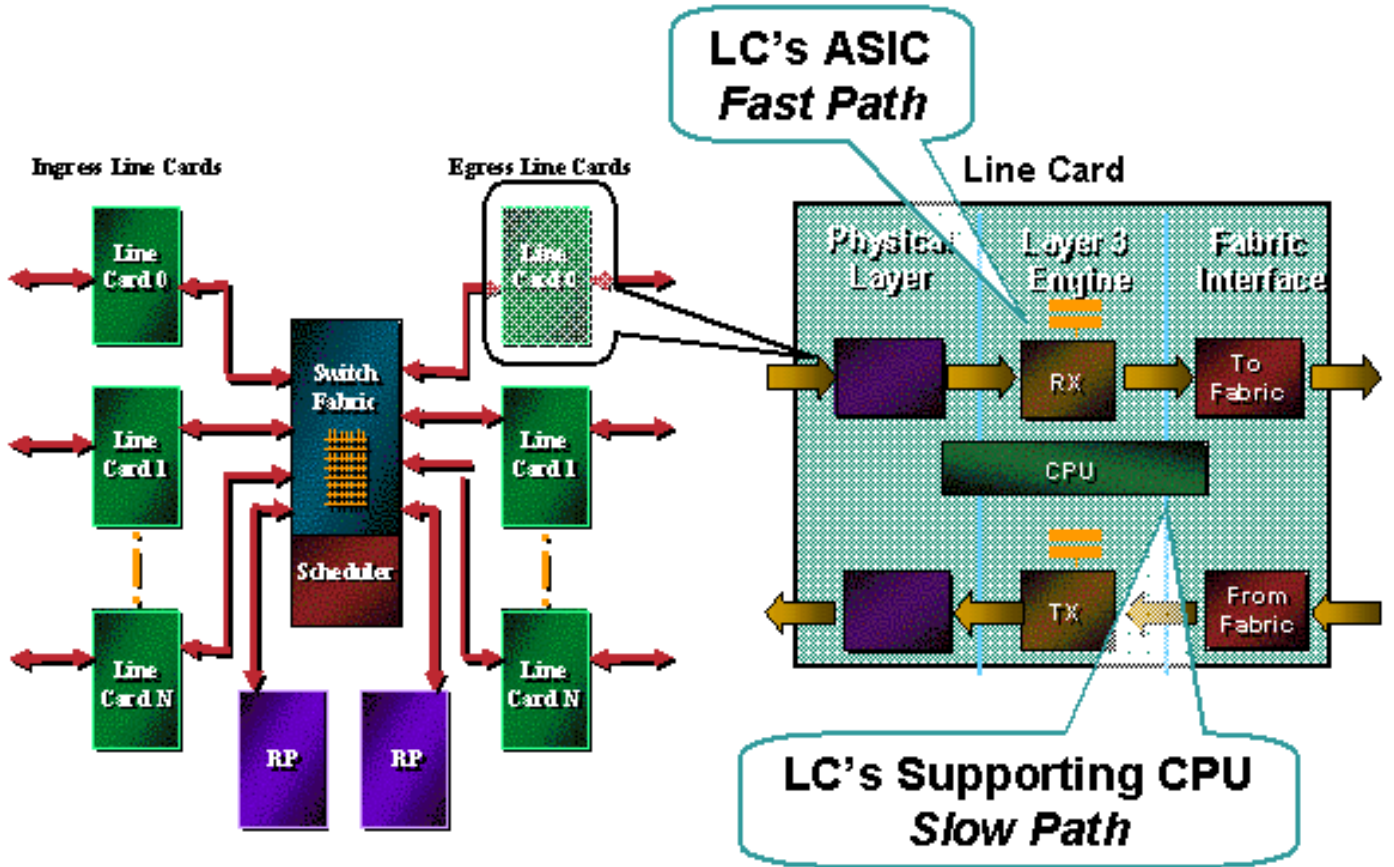
توفر محركات بطاقة الخط Cisco 12000 Series Line Card Engines إمكانات مختلفة لقائمة التحكم في الوصول (ACL). لمعلومات دعم قائمة التحكم في الوصول لمحرك بطاقة خط معين، انتقل إلى القسم المطابق في هذا المستند.

ملاحظة: قوائم التحكم في الوصول للثب المتعدد ل IP غير مدعومة في برنامج Cisco IOS @ الإصدار 12.0S. يمكن استخدام ميزة حد IP للثب المتعدد حيث تكون تصفية البث المتعدد مطلوبة. راجع [إعادة توجيه البث المتعدد للمسار السريع على بطاقات الخط Cisco 12000 Series Engine 2 و ISE Line Cards](#) للحصول على مزيد من المعلومات.

[قوائم التحكم في الوصول \(ACL\) المستندة إلى ASIC مقابل قوائم التحكم في الوصول \(ACL\) المستندة إلى وحدة المعالجة المركزية](#)

يدعم Cisco 12000 جميع أجيال معالجة قائمة التحكم في الوصول (ACL). يعد الفهم العملي لكيفية عمل كل من أوضاع المعالجة هذه والتفاعل ودعم بعضها البعض أمرا أساسيا للاستخدام الفعال لقائمة التحكم في الوصول (ACL) على Cisco 12000.

أستخدمت الأجيال الأولى من معالجة قائمة التحكم في الوصول (ACL) وحدة معالجة مركزية (CPU) قابلة للبرمجة لمعالجة قائمة التحكم في الوصول (ACL). ومع مرور الوقت، تجاوزت متطلبات معالجة الحزمة في الثانية (PPS) قدرة وحدات المعالجة المركزية الجديدة على المتابعة. تم تصميم بطاقات ASIC لتحقيق معدلات أعلى لمنافذ PPS لإعادة توجيه الموجهات وإمكانات الميزات. تم تحميل قوائم التحكم في الوصول (ACL) التي تم تحميلها على وحدة المعالجة المركزية (CPU) الخاصة ببطاقة الخط (LC) على ASIC LC. وظلت بطاقات ASIC مرتجلة للتعامل مع المعدلات الأعلى لمواصفات المنتج الشخصي. وقد تم بناء جيل ASICs الثاني هذا على العمل الرائد من الجيل السابق، وهو يوفر المزيد من قدرات ASIC. نظرا لأن Cisco 12000 عبارة عن منصة توجيه موزعة، فإن التفاعل بين الأجيال المختلفة من معالجة قائمة التحكم في الوصول (ACL) يمكن أن يحدث بعض الارتباك التشغيلي.



يتم استخدام مصطلحات مثل قائمة التحكم في الوصول (ACL) المستندة إلى ASIC، وقائمة التحكم في الوصول (ACL) المستندة إلى وحدة المعالجة المركزية (CPU)، و Fast Path، و Slow Path، ولكمات ASIC في هذا المستند للمساعدة في شرح ما يحدث مع معالجة قائمة التحكم في الوصول (ACL). فيما يلي توضيحات لهذه المصطلحات:

- قوائم التحكم في الوصول (ACL) المستندة إلى ASIC (المسار السريع) - يتم تحميل قوائم التحكم في الوصول (ACL) ومعالجتها في أجهزة ASIC. يحدد نطاق أداء ASIC عمق قائمة التحكم بالوصول (ACL) والأداء والإمكانات. تم استخدام المسار السريع لتوضيح الفرق بين المعالجة والمعالجة المستندة إلى ASIC التي تتم في وحدة المعالجة المركزية (CPU) التي تدعم LC. يتم استخدام المصطلح الأكثر عمومية، المستند إلى ASIC، في هذا المستند.
- قوائم التحكم في الوصول (ACL) المستندة إلى وحدة المعالجة المركزية (CPU) (المسار البطيء) - تتم معالجة قوائم التحكم في الوصول (ACL) في البرنامج على وحدة المعالجة المركزية (CPU) لبطاقة الخط. بالنسبة لبطاقات الجيل المبكر (المحرك 0 وفي بعض الحالات المحرك 1)، تتم جميع المعالجة على وحدة المعالجة المركزية (CPU) الخاصة بوحدة التحكم في الوصول (LC). تقوم قوائم التحكم في الوصول (LC) المستندة إلى ASIC بمعالجة قائمة التحكم في الوصول (ACL) على الحزم التي يتم ضربها من ASIC. تم استخدام Slow Path في الماضي لتوضيح كيف كانت عمليات الضرب على وحدة المعالجة المركزية LC أبطأ من ASIC. يتم استخدام المصطلح الأكثر عمومية، والقائم على وحدة المعالجة المركزية (CPU)، في هذا المستند.
- ASIC Punts - تحتوي ASICs على تصميم صارمة. عندما تتجاوز الحزمة الظروف المصمم، فإنها تتعرض لكم من ASIC لمعالجتها على إما ال LC الذي يدعم وحدة المعالجة المركزية أو يتم إرسالها إلى معالج التوجيه (RP). قوائم التحكم في الوصول (ACL) المستندة إلى ASIC الحزم النكمية التي تقع خارج تصميم ASIC. والمثال على ذلك هو قائمة التحكم في الوصول (ACL) التي تحتوي على ACE باستخدام الكلمة الأساسية log أو log-input. يجب معالجة المعلومات المطلوبة لتسجيل الحزمة خارج ASIC، لذلك يتم توقيع الحزمة تلقائياً من ASIC، داخل وحدة المعالجة المركزية LC، ويتم معالجتها مثل قائمة التحكم في الوصول (ACL) العادية المستندة إلى وحدة المعالجة المركزية.

ملاحظة: عند تكوين التوجيه المستند إلى السياسة (PBR) باستخدام عبارات مطابقة لقوائم التحكم في الوصول (ACL)، يجب ألا تطابق منفذ المصدر. لا يدعم موجه محول جيغابت (GSR) تحويل الأجهزة ل PBR باستخدام قوائم التحكم في الوصول (ACLs) التي تطابق منفذ المصدر. إنه يشغل تحويل العمليات ويتدهور أداء GSR.

تصفية مستوى التحكم والإدارة

يوفر معالج الموجه خدمات مستوى التحكم والإدارة في البنية الموزعة من السلسلة Cisco 12000 Series. توفر قوائم التحكم في الوصول الخاصة بمسار الاستقبال (rACLs) إمكانية تصفية موزعة بسيطة لحركة مرور التحكم والإدارة الموجهة ل RP. ويمكن منطقيا عرضه كطبقة إضافية من الأمان التي تستفيد من نقاط قوة بنية موزعة.

تكوين قوائم التحكم في الوصول إلى مسار تلقي IP

تم إدخال قائمة التحكم في الوصول للبنية الأساسية (rACL) من خلال تنازل خاص في تقييد الصيانة لإصدار البرنامج Cisco IOS® Software، الإصدار S2(21)12.0. ويتم دعمه رسميا في برنامج CISCOS IOS الإصدار S(22)12.0. راجع [قائمة التحكم في الوصول \(ACL\) الخاصة باستقبال IP](#) للحصول على مزيد من المعلومات.

يوفر معالج الموجه خدمات مستوى التحكم في البنية الموزعة لسلسلة Cisco 12000. توفر قوائم التحكم في الوصول للاستقبال إمكانات التصفية لحركة مرور البيانات الموجهة ل RP، مثل تحديثات التوجيه واستعلامات بروتوكول إدارة الشبكة البسيط (SNMP).

تعد قائمة التحكم في الوصول للبنية الأساسية (rACL) المرحلة 1 من جهد متعدد المراحل لإضافة أوجه حماية جديدة إلى التحكم في حركة مرور المستوى وإدارتها. تتم إضافة تحسينات جديدة تحدد المعدل من خلال تحديثات البرامج.

دعم قائمة التحكم في الوصول (ACL) إلى IPv4 حسب نوع بطاقة الخط

توفر بطاقات الخط Series 12000 إمكانات مختلفة لقائمة التحكم في الوصول (ACL) لكل نوع محرك. يصف هذا القسم إمكانات قائمة التحكم في الوصول (ACL) الخاصة بمحركات بطاقات الخط المختلفة. لمعلومات دعم قائمة التحكم في الوصول لمحرك بطاقة خط معين، راجع القسم المقابل في هذا المستند.

هناك بعض الخصائص العامة لجميع قوائم التحكم في الوصول (ACL) (المستندة إلى ASIC و CPU):

- يمكن تطبيق قائمة تحكم في الوصول (ACL) واحدة فقط على واجهة لكل إتجاه. على سبيل المثال، يمكن أن تحتوي الواجهة POS 0/0 على قائمة تحكم في الوصول (ACL) واحدة للإدخال وقائمة تحكم في الوصول (ACL) واحدة للإخراج.
- يتوقف اختبار الحزمة ضد قائمة التحكم في الوصول (ACL) بعد العثور على تطابق. إذا تطابقت قائمة التحكم في الوصول (ACL) التي تتألف من 300 إدخال لمدة طويلة مع الحزمة على إدخال قائمة الوصول (ACE) #45، حينئذ تتم معالجة الحزمة وتوقف معالجة قائمة التحكم في الوصول.
- هناك رفض ضمني لجميع الإدخال في نهاية كل قائمة تحكم في الوصول (ACL). نتيجة لذلك، إذا لم يكن هناك تطابق في قائمة التحكم في الوصول، يتم إسقاط الحزمة. يتم إنشاء قوائم التحكم في الوصول (ACL) من Cisco باستخدام بنية قائمة التحكم في الوصول (ACL) المسموح بها بشكل صريح. وهذا يعني أنه يجب أن يكون هناك ACE لمطابقة الحزمة حتى تتم معالجتها وإعادة توجيهها.
- يتم دائما إلحاق إدخال التحكم في الوصول (ACE) التي تمت إضافتها حديثا بنهاية قائمة التحكم في الوصول (ACL). كلما كانت قائمة التحكم في الوصول (ACL) تتطلب تحديثات، فمن الممارسات الجيدة إزالة قائمة التحكم في الوصول (ACL) (باستخدام الأمر no access-list) وإعادة إضافة قائمة التحكم في الوصول (ACL) الجديدة. نظرا لأن أجزاء IP غير الأولية لا تحتوي على معلومات بروتوكول الطبقة الرابعة في رأس IP، يتم دعم معايير المطابقة القياسية فقط للأجزاء غير الأولية. يمكن العثور على التفاصيل الكاملة حول كيفية توافق قوائم التحكم في الوصول من Cisco مع تصفية أجزاء IP في [قوائم التحكم في الوصول وأجزاء IP](#).
- تتم معالجة قوائم التحكم في الوصول (ACL) المرقمة وتطبيقها بمجرد إدخالها من خلال واجهة سطر الأوامر (CLI). باستخدام قوائم التحكم في الوصول (ACL) الكبيرة، ينتج عن ذلك في بعض الأحيان زيادة وحدة المعالجة المركزية (CPU) على وحدة المعالجة المركزية (RP) أو وحدة المعالجة المركزية (LC).

المحرك 0 - معالجة قائمة التحكم في الوصول (ACL)

المحرك 0 هو بطاقة الخط الأولى التي يتم تسليمها ل Cisco 12000. فهي جميعا قائمة على وحدة المعالجة المركزية (CPU) وإعادة التوجيه. وبالتالي، تعمل بطاقات الخط 0 Engine على معالجة قوائم التحكم في الوصول (ACL) في وحدة المعالجة المركزية (CPU) الخاصة بوحدة التحكم في الوصول (LC).

تستند بطاقات الخط هذه إلى Engine 0:

نوع بطاقة الخط	نوع الواجهة	الاتصال
DS3 × 12	متمحور	الشركات الصغيرة والمتوسطة
DS3 × 12	متمحور	الشركات الصغيرة والمتوسطة
E3 × 12	متمحور	الشركات الصغيرة والمتوسطة
1xChoc12->DS3		الأشعة تحت الحمراء
1xCHOC12/STM4->OC3/STM1	POS	الأشعة تحت الحمراء
4xOC3c/STM1c	POS	SR
4xOC3c/STM1c	POS	ل.ر
4xOC3c/STM1c	POS	مم
1xOC12c/STM4c	POS	الأشعة تحت الحمراء
1xOC12c/STM4c	POS	مم
6xCT3->DS1		الشركات الصغيرة والمتوسطة
2xCHOC3/STM1->DS1/E1		الأشعة تحت الحمراء
4xOC3c/STM1c	ATM	الأشعة تحت الحمراء
4xOC3c/STM1c	ATM	مم
1xOC12c/STM4c	ATM	الأشعة تحت الحمراء
1xOC12c/STM4c	ATM	مم

معايير المطابقة المدعومة

يتم دعم جميع قوائم التحكم في الوصول (ACL) الموسعة وتقنية Turbo Software الإصدار 12.0S القياسية على المحرك 0 من Cisco IOS Software.

عدد إدخال التحكم في الوصول (ACE) المدعومة

لا يتم تحديد حجم قائمة التحكم في الوصول (ACL) إلا من خلال متطلبات الأداء وموارد الذاكرة المتوفرة.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

تتم معالجة قوائم التحكم في الوصول إلى الإخراج في مسار ميزة الدخول لبطاقات الخط الأخرى في النظام. يؤدي دفع قائمة التحكم في الوصول إلى الإخراج إلى جانب الدخول في قوائم التحكم في الوصول (LCs) الأخرى إلى حماية اللوحة الخلفية من حزم إعادة التوجيه التي سيتم إسقاطها. هذه وظيفة موروثه من البنية الموزعة على Cisco 7500. يتم توفير شرح تفصيلي وأسباب ومبادئ توجيهية تشغيلية في [قائمة التحكم في الوصول \(ACL\) لمخرجات IPv4 - مصفوفة عمليات التشغيل البيني لبطاقة الخط](#).

[إرشادات التشغيل والتفاعلات بين بطاقات الخط](#)

• إذا تم تكوين NetFlow على بطاقة خط للمحرك 0 وتم تكوين قائمة التحكم في الوصول إلى الإخراج على بطاقة خط 3 أو 4+ لمحرك الخروج، فإن قائمة التحكم في الوصول إلى الإخراج تتم معالجتها بواسطة كل من بطاقات خطوط الدخول والخروج للسماح ل NetFlow بالحساب للحزم التي تم رفضها بواسطة قوائم التحكم في الوصول بالإضافة إلى الحزم المعاد توجيهها.

[التوصيات](#)

توصي Cisco باستخدام قوائم التحكم في الوصول (ACL) من Turbo على المحرك 0 لقوائم التحكم في الوصول (ACL) الكبيرة. قوائم التحكم في الوصول (ACL) الخطية الصغيرة هي أكثر فعالية لقوائم التحكم في الوصول (ACL) الأصغر حجماً لأن قوائم التحكم في الوصول (ACL) من Turbo تتطلب ذاكرة إضافية.

[المحرك 1 - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[نظرة عامة](#)

بطاقة خط Engine 1 هي جسر بين المعالجة المستندة إلى وحدة المعالجة المركزية (CPU) على المحرك 0 والجيل الأول من إعادة التوجيه/الميزة ASIC على Engine 2. تعمل بطاقات الخط Engine 1 على معالجة قوائم التحكم في الوصول (ACL) في البرنامج بشكل افتراضي. باستخدام برنامج Cisco IOS الإصدار S(10)12.0 والإصدارات الأحدث، يوفر المحرك 1 قوائم التحكم في الوصول (ACL) الخاصة بالأجهزة للبطاقات المزودة بالإصدارات 4 أو 5 من Salsa ASIC (راجع مرجع أمر بطاقة الخط أدناه لتحديد إصدار Salsa المزود ببطاقة معينة).

تستند بطاقات الخط هذه إلى المحرك 1:

نوع بطاقة الخط	نوع الواجهة	الاتصال
8xFE	(منفذ RJ45)	100BaseT
8xFE	(مم)	100BaseF
8xFE	(منفذ RJ45)	100BaseT
8xFE	(مم)	100BaseF
1xGE	س س س،	:GBIC
1xGE	س س س،	:GBIC
2xOC12c/STM4c	DPT	الأشعة تحت الحمراء
2xOC12c/STM4c	DPT	ل.ر
2xOC12c/STM4 c	DPT	XLR
2xOC12c/STM4c	DPT	مم
2xOC12c/STM4c	DPT	الأشعة تحت الحمراء
2xOC12c/STM4c	DPT	ل.ر
2cOC12c/STM4c	DPT	XLR
2xOC12c/STM4c	DPT	مم

يتم دعم جميع قوائم التحكم في الوصول (ACL) من Cisco IOS Software الإصدار 12.0S التي تدعم قوائم التحكم في الوصول (ACL) القياسية والموسعة و Turbo في وحدة المعالجة المركزية (LC) (المسار البطني). بالإضافة إلى ذلك، يمكن أن يعالج المحرك 1 قوائم التحكم في الوصول (ACL) للإدخال في Salsa ASIC. يعالج ASIC Salsa معالجة قائمة التحكم في الوصول (ACL) للإدخال مع البحث عن المسار، مما يؤدي إلى زيادة الأداء عند مقارنته بالمعالجة الخطية التقليدية لقوائم التحكم في الوصول (ACL) من Turbo. يتعذر على ASIC ل Salsa معالجة قوائم التحكم في الوصول إلى الإخراج أو قوائم التحكم في الوصول (ACL) إلى الواجهة الفرعية.

عدد إدخلات التحكم في الوصول (ACE) المدعومة

لا يتم تحديد حجم قائمة التحكم في الوصول (ACL) إلا من خلال متطلبات الأداء وموارد الذاكرة المتوفرة.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

تتم معالجة قوائم التحكم في الوصول إلى الإخراج في مسار ميزة الدخول لبطاقات الخط الأخرى في النظام. راجع قسم قائمة التحكم في الوصول (ACL) الخاصة بمخرجات IPv4 - مصفوفة عمليات تفاعل بطاقة الخط للحصول على مزيد من المعلومات.

الأوامر الخاصة بطاقة الخط

- وصلة أجهزة قائمة الوصول (أ)
- show controller l3 | تضمين ASIC

إرشادات التشغيل والتفاعلات بين بطاقات الخط

- لا يمكن تشغيل ASIC Salsa و PSA ASIC في نفس الوقت. لا يقبل أمر `access-list hardware` إلا إما PSA (المحرك 2) أو Salsa (المحرك 1) ولكنه لا يقبل كلا.
- إذا تم تكوين NetFlow على بطاقة خط Engine 1 وتم تكوين قائمة التحكم في الوصول إلى الإخراج على بطاقة خط 3 أو 4+ لمحرك الخروج، فإن قائمة التحكم في الوصول إلى الإخراج تتم معالجتها بواسطة كل من بطاقات خطوط الدخول والخروج للسماح ل NetFlow بالحساب للحزم التي تم رفضها بواسطة قوائم التحكم في الوصول (ACL) بالإضافة إلى الحزم المعاد توجيهها.

التوصيات

بالنسبة لإصدارات بطاقات الخط Engine 1 التي لا تدعم قوائم التحكم في الوصول (ACL) إلى الأجهزة، توصي Cisco باستخدام قوائم التحكم في الوصول (ACL) من Turbo لقوائم التحكم في الوصول (ACL) الكبيرة. يمكن تنفيذ قوائم التحكم في الوصول (ACL) الصغيرة (أقل من 20 خطا) كقوائم تحكم في الوصول (ACL) خطية للحفاظ على الذاكرة.

المحرك 2 - معالجة قائمة التحكم في الوصول (ACL)

نظرة عامة

كان المحرك 2 هو بطاقة الخط الأولى مع ASIC لإعادة التوجيه/الميزة. باستخدام برنامج Cisco IOS الإصدار S(10)12.0 والإصدارات الأحدث، توفر بطاقات الخط Engine 2 إمكانات قائمة التحكم في الوصول للأجهزة في بطاقة ASIC عالية الأداء لتحويل الحزم (PSA). كما هو الحال مع جميع بطاقات ASIC لإعادة التوجيه/الميزات، تضع مظاريف الأداء الصارمة حدود على قدرة ASIC. يرجع طرف الأداء الرئيسي على قوائم التحكم في الوصول (ACL) الخاصة بالمحرك 2 إلى قيود الذاكرة في PSA ASIC.

يتم إعادة توجيه الحزمة في المحرك 2 بواسطة PSA ASIC. ويملك جهاز الأمن الوقائي ثلاث ذكريات خارجية رئيسية:

- PLU (بحث عن المسار)- يستخدم لتخزين عقد العمل
- TLU (بحث الجدول)- يستخدم لتخزين أوراق FIB وربما بنيات موازنة التحميل. يستخدم أيضا لاحتجاز العديد من بنى بيانات قائمة التحكم في الوصول (ACL) الخاصة ببروتوكول PSA SRAM - الموقع الرئيسي لتراكيبات LoadShare

تعد ميزة قائمة التحكم في الوصول (ACL) ل PSA تنفيذ قائمة تحكم في الوصول (ACL) يستند إلى ميكروكود. يتم تحميل مجموعة خاصة من الإرشادات في رقاقة PSA التي تسمح بالتحقق الأساسي من قائمة التحكم في الوصول (ACL). هناك عدد من القيود على هذه الميزة التي يجب فهمها بعناية قبل النشر. يتمثل أحد العيوب الرئيسية لقوائم التحكم في الوصول (ACL) إلى PSA في الكمية الكبيرة من ذاكرة إعادة توجيه الأجهزة المطلوبة.

تتطلب ميزة قائمة التحكم في الوصول (ACL) الخاصة بمنفذ PSA تخصيص كتلة كبيرة من ذاكرة PLU/TLU مسبقا بغض النظر عن عدد البادئات، وما إلى ذلك. نظرا لأن هذا التخصيص يأتي في المقام الأول من منطقة TLU، فإنه يؤثر بشكل كبير على عدد المسارات التي يمكن صيانتها على هذه البطاقات عند تكوين قوائم التحكم في الوصول (ACLs) إلى PSA.

بالإضافة إلى التكلفة الأولية لذاكرة PLU/TLU، تتطلب كل بادئة يتم تخزينها في ذاكرة TLU مساحة ذاكرة أكبر بكثير. يختلف مقدار الذاكرة المطلوب لكل بادئة، بناء على اتجاه قائمة التحكم بالوصول (ACL) المطبقة (مدخل مقابل مخرج) ونوع بطاقة الخط. بشكل عام، تتطلب قوائم التحكم بالوصول (ACL) إلى المخرج ذاكرة أكثر من الدخول، والسطور ذات المنافذ المادية الكثيرة تتطلب ذاكرة أكثر من تلك التي تحتوي على منافذ أقل.

في الحالة التي لا تستخدم فيها قائمة التحكم في الوصول (ACL) الخاصة بالمحرك 2، يتم إنشاء بنى البيانات لقائمة التحكم في الوصول (ACL) بغض النظر عن قوائم التحكم في الوصول الفعلية التي تم تكوينها. للتغيير إلى البنيات الأصغر غير قائمة التحكم في الوصول، يجب تكوين الأمر no access-list hardware psa على الموجه. يقوم هذا الأمر بتعطيل جميع معالجة قائمة التحكم في الوصول (ACL) على جميع سلاسل المحرك 2 في جميع الاتجاهات. تطلب Cisco استخدامها بحذر شديد.

نظرة عامة

لتوفير أداء معالجة قائمة التحكم في الوصول (ACL) بشكل مستقل عن عمق المطابقة، يتم دمج قوائم التحكم في الوصول (ACL) الخاصة بالمحرك 2 في جدول إعادة توجيه الأجهزة. انظر أدناه للحصول على توضيحات حول كيفية تأثير ذلك على إمكانية توسع البادئة.

تستند بطاقات الخط هذه إلى المحرك 2:

نوع بطاقة الخط	نوع الواجهة	الاتصال
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	ل.ر
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	ل.ر
1xOC192c/STM64c	أداة تمكين	SR
16xOC3c/STM1c	POS	الأشعة تحت الحمراء
16xOC3c/STM1c	POS	مم
4xOC12c/STM4c	POS	الأشعة تحت الحمراء
4xOC12c/STM4c	POS	مم
4xOC12c/STM4c	POS	الأشعة تحت الحمراء
4xOC12c/STM4c	POS	مم
4xOC12c/STM4c	ATM	الأشعة تحت الحمراء

مم	ATM	4xOC12c/STM4c
الأشعة تحت الحمراء	ATM/TS	8xOC3cSTM1c
مم	ATM/TS	8xOC3c/STM1c
:GBIC	Sx	3xGE
:GBIC	CWDM	3xGE
SR	DPT	1xOC48c/STM16c
ل.ر	DPT	1xOC48c/STM16c
SR	DPT	1xOC48c/STM16c
ل.ر	DPT	1xOC48c/STM16c

معايير المطابقة المدعومة

جميع برامج Cisco IOS الإصدار 12.0S المدعومة معايير مطابقة قائمة التحكم في الوصول (ACL) الموسعة القياسية، باستثناء منافذ مصدر الطبقة 4. يتم اختبار الأقنعة غير المتصلة وحقول أسبقية IP ومنافذ مصدر الطبقة 4 من PSA ASIC ويتم معالجتها على وحدة المعالجة المركزية (CPU) الخاصة بوحدة التحكم في الوصول إلى LC.

عدد إدخلات التحكم في الوصول (ACE) المدعومة

ما يصل إلى خمس قوائم تحكم في الوصول (ACL) لإدخال 448 سطرا في PSA. يمكن تكوين قائمة تحكم في الوصول (ACL) وإحدة لكل منفذ. تتم إدارة قوائم التحكم في الوصول (ACL) الإضافية بواسطة وحدة المعالجة المركزية (CPU) لبطاقة الخط. راجع قسم "القيود" أدناه لمعرفة القيود على قوائم التحكم في الوصول إلى الإخراج.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

سيتم تنفيذ قائمة التحكم في الوصول للإخراج التي تم تكوينها على بطاقة الخط هذه في مسار ميزة الدخول لبطاقات الخط الأخرى في النظام. راجع قائمة التحكم في الوصول (ACL) الخاصة بإخراج IPv4 - مصفوفة عمليات تفاعل بطاقة الخط للحصول على تفاصيل.

الأوامر الخاصة بطاقة الخط

- حد PSA الخاص بالأجهزة لقائمة الوصول 128
- PSA لجهاز قائمة الوصول
- مجرى جانبي ل PSA
- تفاصيل PSA show access-list
- show access-list psa summary
- show controller psa سمة

إرشادات التشغيل والتفاعلات بين بطاقات الخط

- تتطلب معالجة قائمة التحكم في الوصول (ACL) للمسار السريع استيفاء الشروط التالية: قائمة التحكم في الوصول (ACL) المطبقة تقع ضمن حد ACE البالغ 128 أو 448. يجب أن يكون الطول أقل من 128 إدخال تحكم في الوصول (ACE) في حالة تكوين الأمر 128 access-list hardware psa limit. يجب أن يكون الطول أقل من 448 قائمة تحكم في الوصول (ACE) عندما تكون حزمة الرمز المجهرى لقائمة التحكم في الوصول (ACL) المكونة من 448 سطرا مطلوبة. لم يتم تكوين قوائم التحكم في الوصول الخاصة بالإدخال والإخراج معا لكل بطاقة. قد يتم تكوين ما يصل إلى خمسة قوائم تحكم في الوصول (ACL) إلى الإخراج على الموجه.
- يتم دعم قوائم التحكم في الوصول (ACL) ذات 128 سطرا فقط على بطاقات الخط ذات 8 و 16 منفذا OC-

- يتم دعم قوائم التحكم في الوصول (ACL) الخاصة بالخط 448 على بطاقات الخط Port-4 POS 3/STM-1 و OC-12/STM-4 POS و OC-48/STM-16 POS و Port Gigabit Ethernet Line Cards-3 .
- تأخذ قوائم التحكم في الوصول (ACL) للإدخال الأولية في المسار السريع عبر قوائم التحكم في الوصول إلى الإخراج عندما يتم تكوين كل منهما بشكل متزامن على البطاقة نفسها (تتم معالجة قائمة التحكم في الوصول إلى الإخراج في المسار البطيء).
- إذا تم تكوين قائمة التحكم في الوصول للإخراج على بطاقة Engine 2، وكانت بطاقة الخط المدخل هي Engine 0/1/2/4، فسيتم معالجة قائمة التحكم في الوصول للإخراج في بطاقة الدخول. بالنسبة لأنواع المحرك الأخرى، سيتم معالجة قائمة التحكم في الوصول (ACL) إلى الإخراج في المسار البطيء ل Engine 2 egress.
- قوائم التحكم في الوصول إلى الإخراج غير مدعومة لحركة مرور IP إلى MPLS (يتم "دفع" التسمية الأولى MPLS على حزمة IP).
- يتم دمج معلومات معالجة قائمة التحكم في الوصول (ACL) في FIB الخاص بالأجهزة ويمكن أن تؤثر على قابلية توسع البادئة. يتم الإبلاغ عن إستهلاك الذاكرة للبادئة بواسطة حالات فشل تخصيص الذاكرة مع توقيع "exmem=1" في رسالة السجل المرفقة.

التوصيات

- يتم دمج معلومات معالجة قائمة التحكم في الوصول (ACL) في جدول إعادة توجيه CEF، مما يقلل من إمكانية توسع البادئة. يمكن للتطبيقات التي لا تستخدم قوائم التحكم في الوصول تعطيل دعم قائمة التحكم في الوصول في جدول CEF، وبالتالي زيادة ذاكرة البادئات المتاحة من خلال إصدار الأمر **no access-list hardware psa**.
- يعمل تكوين الأمر **no access-list hardware psa** على تعطيل جميع معالجة قائمة التحكم في الوصول (ACL) بواسطة بطاقات المحرك 2 بالإضافة إلى تعطيل دعم PSA لقوائم التحكم في الوصول (ACL). لا يفرض تنفيذ البرامج لقوائم التحكم في الوصول (ACL). يطبق هذا شرط أيضا إن المخرج خط بطاقة يتلقى إنتاج ACL بشكل.
- يعمل تكوين الأمر **access-list compiled** بعد الأمر **access-list hardware psa** على تحويل وحدات ACE التي تتجاوز سعة وحدات PSA إلى قائمة التحكم في الوصول (ACL) من Turbo وهذا يوفر الأداء الأمثل لقوائم التحكم في الوصول (ACL) لقوائم التحكم في الوصول (ACL) لأكثر من 448 ACE بطول الرمز المجهري الافتراضي لقائمة ACL هو 128 (بدءا من البرنامج Cisco IOS Software، الإصدار S/ST(14)12.0). إذا كانت قوائم التحكم في الوصول (ACL) الأصغر حجما قيد الاستخدام ولم تكن إمكانية الخط 448 مطلوبة، فإن تكوين الأمر **access-list hardware psa limit 128** يحفظ ذاكرة إعادة توجيه (TLU)، والتي تعمل على تحسين إمكانية توسع البادئة). يجب تمكين معالجة قائمة التحكم في الوصول (ACL) من Turbo مع الأمر **access-list compiled** لقوائم التحكم في الوصول (ACL) الأطول من 129 خطأ مع الأمر **access-list hardware psa limit 128**. تعمل هذه المجموعة على معالجة الخطوط الأولى 128 في PSA ASIC والأسطر المتبقية مع قوائم التحكم في الوصول (ACL) من Turbo، والتي تعمل على تحسين الأداء مع الحفاظ على ذاكرة إعادة توجيه في نفس الوقت.
- لا تدعم بطاقة الخط OC12 ATM التي تحتوي على 4 منافذ قوائم التحكم في الوصول (ACL) للإدخال، ولكنها توفر اكتشاف قائمة التحكم في الوصول (ACL) للإخراج في الميكروكود، مما يسمح بعملية قوائم التحكم في الوصول إلى الإخراج في المسار البطيء.
- تدعم بطاقة الخط 8xOC3 ATM قوائم التحكم في الوصول (ACL) الخطية لكل VC 128 مع برنامج Cisco IOS الإصدار S(23)12.0 والإصدارات الأحدث. يمكن تكوين 16 قائمة تحكم في الوصول (ACL) خاصة بالإدخال كحد أقصى في المسار السريع. يتم دعم قائمة التحكم في الوصول (ACL) الخاصة بالإدخال 448 على أساس كل مركز افتراضي (VC) في مسار بطيء فقط. قوائم التحكم في الوصول للإخراج غير مدعومة.

المحرك ISE (محرك خدمات 3 IP - معالجة قائمة التحكم في الوصول (ACL))

نظرة عامة

يعد Engine 3 هو أول بطاقة خط إعادة توجيه ثنائية المرحلة. يحتوي المحرك 3 على نقاط وصول (ASIC) خاصة

إعادة التوجيه/الميزات على مسار الدخول والخروج. وهذا يسمح بوضع قوائم التحكم في الوصول في ASIC على كل من مسارات الدخول والخروج. بالإضافة إلى ذلك، فإن بنية ASIC الخاصة بالمحرك 3 هي عبارة عن صفيح متواز/خط أنابيب هجين. يقوم بنية ASIC بتنفيذ معالجة قائمة التحكم في الوصول (ACL) في ذاكرة TCAM المتوازية عالية السرعة والقابلة للتوجيه (TCAM)، والتي توفر معالجة بسرعة خط تصل إلى 20 ألف إدخال وإخراج لكل مدخل، و 20 ألف إدخال وإخراج لكل مخرج.

تستند بطاقات الخط هذه إلى Engine 3:

نوع بطاقة الخط	نوع الواجهة	الاتصال
4xOC12c/STM4c	POS	الأشعة تحت الحمراء
4xOC12c/STM4c	POS	مم
4xCHOC12/STM4 ->OC3/STM1- >DS3/E3	POS	الأشعة تحت الحمراء
16xOC3c/STM1c	POS	الأشعة تحت الحمراء
16xOC3c/STM1c	POS	مم
8xOC3/STM1c	POS	الأشعة تحت الحمراء
8xOC3c/STM1c	POS	مم
4xOC3c/STM1c	POS	الأشعة تحت الحمراء
4xOC3c/STM1c	POS	مم
4xOC3c/STM1c	POS	ل.ر
1xOC48c/STM16c	POS	SR
1xOC48c/STM16c	POS	ل.ر
1xCHOC48/STM1 6->STM4- >OC3/STM1- >DS3/E3	POS	SR
4xOC12c/STM4c	ATM/IP	الأشعة تحت الحمراء
4xOC12c/STM4c	ATM/IP	مم
4xGE	ge	
4xOC12c/STM4c	DPT	الأشعة تحت الحمراء
4xOC12c/STM4c	DPT	XLR

معايير المطابقة المدعومة

يتم دعم جميع معايير التطابق القياسية والموسعة لبرنامج Cisco IOS Software في المسار السريع باستثناء إدخالات التحكم في الوصول (ACE) إلى السجل التي تتم معالجتها بواسطة وحدة المعالجة المركزية (CPU) لبطاقة الخط.

عدد إدخالات التحكم في الوصول (ACE) المدعومة

- معالجة معدل الخط في كل من اتجاه المدخل والمخرج لكل منفذ، لكل شبكة VLAN، لكل واجهة فرعية لترحيل الإطارات، ولكل واجهة فرعية ATM. يتم دعم ما يصل إلى 20000 إدخال تحكم في الوصول (ACE) موسع لكل اتجاه وكل بطاقة.
- معايير المطابقة الخاصة بمصدر TCP/UDP/منفذ الوجهة "range" و"lt" و"gt" يتم التعامل معها في الأجهزة باستخدام موارد "مشغل L4".

- يقتصر عدد عمليات L4 المميزة على 32 لبطاقة الخط بالكامل. يقتصر عدد مشغلي منفذ المصدر على ستة مشغلات كحد أقصى.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

دعم المسار السريع الأصلي لمعالجة قائمة التحكم في الوصول (ACL) ذات معدل الخط في واجهة ASIC لمعالجة حزمة مسار الإرسال. راجع [قائمة التحكم في الوصول \(ACL\) الخاصة بإخراج IPv4 - مصفوفة عمليات تفاعل بطاقة الخط](#) للحصول على تفاصيل.

الأوامر الخاصة بطاقة الخط

- HW-Module <slot#> tcam no-merge!—12.0(21)S3
- <اسم الواجهة> الخاص بواجهة جهاز <show-access-list show cef int pos[x/y] | inc if_number

إرشادات التشغيل والتفاعلات بين بطاقات الخط

- تتم معالجة الحزم التي تطابق إدخلات التحكم في الوصول (ACEs) إلى المسار البطيء.
- تتم معالجة الحزم التي تطابق إدخلات التحكم في الوصول (ACE) المرفوضة للتأكد ضد مقاطعة النظام) في المسار البطيء.
- عندما تتضمن قائمة التحكم في الوصول مجموعة من العناوين، يستخدم الجهاز وحدات ACE خاصة تسمى "وحدات ACE النطاق" والتي تتطلب ما يصل إلى ثلاثة وحدات ACE.
- يمكن أن يحافظ دمج قائمة التحكم في الوصول (ACL) على موارد TCAM من خلال مشاركة إدخلات التحكم في الوصول (ACEs) الشائعة عبر قوائم التحكم في الوصول (ACL) الفردية. لتحديد ما إذا تم دمج قائمة التحكم في الوصول (ACL)، أستخدم أمر `show-access-list hardware interface`.
- عدادات قائمة التحكم في الوصول (ACL) غير مدعومة لقوائم التحكم في الوصول (ACL) المدمجة. باستخدام برنامج Cisco IOS الإصدار S3(21)12.0 والإصدارات الأحدث، يمكن تعطيل دمج قائمة التحكم في الوصول (ACL) باستخدام الأمر `hw-module <slot #> tcam no-merge`. لتحديد ما إذا تم دمج قائمة التحكم في الوصول (ACL)، أستخدم أمر `show-access-list hardware interface`.
- إذا تم تكوين NetFlow على بطاقة خط لمحرك 1/0 وتم تكوين قائمة التحكم في الوصول إلى الإخراج على بطاقة خط من نوع محرك الخروج 3 أو 4+، فسيتم معالجة قائمة التحكم في الوصول إلى الإخراج بواسطة بطاقات خطوط الدخول والخروج للسماح ل NetFlow بالحساب للحزم التي تم رفضها بواسطة قوائم التحكم في الوصول بالإضافة إلى الحزم المعاد توجيهها.

دعم عداد ACL

Per-ACE	Per-ACE (hardware counters)	Aggregate	
		21S3/ST3	X
22S		X	X
23S	X	X	X

التعاريف:

- Per-ACE — دعم برنامج Cisco IOS العادي، يعرض الأمر `show access-list <number>` على RP/LC قائمة التحكم في الوصول والعداد المقترنين بكل ACE. يتوفر فقط عندما يتم تعطيل الدمج قبل تكوين أي قوائم التحكم في الوصول (ACL). ويمكن القيام بذلك باستخدام أمر التكوين هذا:
Router(config)#hw-module slot <number> tcam compile acl no-merge

يقوم هذا الخيار عند تمكينه بإيقاف تشغيل بعض عمليات تحسين دمج TCAM ويؤثر على إمكانية التوسع. يعتمد التأثير المحدد على قوائم التحكم في الوصول (ACL) الفردية. لاحظ أيضا أن العدادات لن تكون صحيحة إذا تم تطبيق التوجيه المستند إلى السياسة على تلك الواجهة. وفي هذه الحالة، يجب استخدام عداد التجميع.

- (PER-ACE (TCAM) —عدادات الأجهزة المرتبطة بكل إدخال TCAM. لا يلزم إجراء أي تهيئة، كما لا يوجد أي تأثير على الأداء/قابلية التطوير. متوفر فقط على بطاقة الخط باستخدام واجهة سطر الأوامر هذه. لا يمكن مسح هذه العدادات بواسطة البرنامج.

```
LC-Slot4#show contr tofab alpha ac1 <if-number> vnr2ace
```

ستوفر واجهة سطر أوامر (CLI) عامة جديدة لهذا الأمر في برنامج Cisco IOS الإصدار 22S:

```
LC-Slot4#show access-list hardware interface p0:1 in
```

كما هو الحال مع عداد كل إدخال تحكم في الوصول إلى الوصول (ACE)، تكون عدادات TCAM صالحة فقط عندما لا يتم استخدام PBR على تلك الواجهة باستخدام قائمة التحكم في الوصول (ACL). التجميع - تظهر كل قائمة تحكم في الوصول (ACL) عداد تصريح/رفض ملخص. هذا هو مجموع جميع عدادات ACE الفردية. ليست هناك حاجة للتكوين، كما أنه ليس هناك أي تأثير على الأداء أو قابلية التطوير.

التوصيات

لا شيء في هذا الوقت.

المحرك 4 (POS) - معالجة قائمة التحكم في الوصول (ACL)

نظرة عامة

يوفر المحرك 4 دعم قائمة التحكم في الوصول (ACL) هذا مع البرنامج Cisco IOS Software الإصدار S(18)12.0 والإصدارات الأحدث:

- يتم دعم قوائم التحكم في الوصول للإخراج على بطاقات خط E0/1/2 إذا كانت بطاقة الخط 4 Engine هي بطاقة الدخول. في هذا التكوين، تتم معالجة قائمة التحكم في الوصول إلى الإخراج بواسطة وحدة المعالجة المركزية (CPU) لبطاقة خط الخروج. تستند بطاقات الخط هذه إلى المحرك 4:

نوع بطاقة الخط	نوع الواجهة	نوع المحرك	الاتصال
4xOC48c/STM16c	POS	الفئة E4	
4xOC48c/STM16c	POS	الفئة E4	ل.ر
1xOC192c/STM64c	POS	الفئة E4	الأشعة تحت الحمراء
1xOC192c/STM64c	POS	الفئة E4	SR
1xOC192c/STM64c	POS	الفئة E4	VSR-1
10xGE	SFP	الفئة E4	

المحرك +4 (POS و DPT) - معالجة قائمة التحكم في الوصول (ACL)

نظرة عامة

يقدم Engine 4+ وظيفة قائمة التحكم في الوصول (ACL) إلى مجموعة 10 جيجابت من Cisco 12000 Series.

يتم دعم حتى 1024 ACEs في كل مسار من مسارات الدخول والخروج. تتم معالجة كل من قوائم التحكم في الوصول الإدخال والإخراج بمعدل الخط لما يصل إلى 96 إدخال وإخراج. يختلف الأداء للمطابقات الأطول باختلاف عمق المطابقة.

تستند بطاقات خطوط نقطة البيع هذه إلى Engine 4+:

نوع بطاقة الخط	نوع الواجهة	الاتصال
4xOC48c/STM16c	POS	SR
4xOC48c/STM16c	POS	ل.ر
1xOC192c/STM64c	POS	الأشعة تحت الحمراء
1xOC192c/STM64c	POS	SR
1xOC192c/STM64c	POS	VSR-1
1xOC192/STM64c	POS	ل.ر
4xOC48c/STM16c	DPT	:SFP
1xOC192c/STM64c	DPT	الأشعة تحت الحمراء
1xOC192c/STM64c	DPT	SR
1xOC192c/STM64c	DPT	VSR-1
1xOC192c/STM64c	DPT	ل.ر

معايير المطابقة المدعومة

يتم دعم جميع معايير قائمة التحكم في الوصول (ACL) القياسية والموسعة من برنامج Cisco IOS Software في المسار السريع باستثناء إدخالات التحكم في الوصول (ACEs) إلى السجل أو الأجزاء.

عدد إدخالات التحكم في الوصول (ACE) المدعومة

يتم دعم ما يصل إلى 1024 وحدات ACE لكل اتجاه في المسار السريع.

ملاحظة: 1021 من إدخالات التحكم في الوصول (ACEs) قابلة للتكوين. يتم حفظ ثلاثة إدخالات لأوامر ACE الضمنية IP any، ورفض ip any، والإرسال إلى وحدة المعالجة المركزية.

لا يوجد حد أعلى لعدد إدخالات التحكم في الوصول (ACEs) المدعومة. يتم تنفيذ أي وحدات ACE تتجاوز حد 1021 في المسار البطيء لبطاقة الخط.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

تتم معالجة قوائم التحكم في الوصول (ACL) إلى الإخراج في المسار السريع لجانب الإرسال. راجع [قائمة التحكم في الوصول \(ACL\) الخاصة بإخراج IPv4 - مصفوفة عمليات تفاعل بطاقة الخط](#) للحصول على تفاصيل.

[الأوامر الخاصة بطاقة الخط](#)

```
<show tcam appl [acl-in / ACL-Out] tcam <label-no >
<show tcam appl [acl-in / ACL-Out] <port><عدد الإدخالات>
```

[إرشادات التشغيل والتفاعلات بين بطاقات الخط](#)

- قوائم التحكم في الوصول (ACL) للواجهة الفرعية غير مدعومة.
- يختلف الأداء حسب عمق المطابقة.
- تستخدم إدخالات النطاق قاعدتي قائمة تحكم بالوصول (ACL) (ثلاثة إذا كان إدخالان يتقاطعان مع حد).
- يتم دعم قائمة تحكم في الوصول (ACL) واحدة لكل واجهة مادية.
- يتم دعم ما يصل إلى 1024 وحدات ACE (لكل اتجاه) في المسار السريع.
- يمكن مشاركة أي من وحدات ACE للمسار السريع 1024 عبر المنافذ.
- تتم تصفية إدخالات التحكم في الوصول (ACEs) التي تستخدم الكلمة الأساسية الجزء في المسار البطيء.
- لا يتم حساب الحزم المرفوضة ل ACEs التي تتم معالجتها في المسار البطيء.
- إذا تم تكوين NetFlow على بطاقة خط للمحرك 0 وتم تكوين قائمة التحكم في الوصول إلى الإخراج على بطاقة خط 3 أو 4+ لمحرك الخروج، فسيتم معالجة قائمة التحكم في الوصول إلى الإخراج بواسطة كل من بطاقات خطوط الدخول والخروج للسماح ل NetFlow بالحساب للحزم التي تم رفضها بواسطة قوائم التحكم في الوصول بالإضافة إلى الحزم المعاد توجيهها.

[التوصيات](#)

لا شيء في هذا الوقت.

[المحرك 4+ \(إيثرنت\) - معالجة قائمة التحكم في الوصول \(ACL\)](#)

[نظرة عامة](#)

تعمل بطاقات خط إيثرنت طراز 4+ Engine على توفير وظائف قوائم التحكم في الوصول (ACL) للإدخال لكل شبكة محلية ظاهرية (VLAN) في الأجهزة لمجموعة إيثرنت بسرعة 10 جيجابت طراز Cisco 12000. هذه بعض الخصائص:

- يمكن تطبيق قوائم التحكم في الوصول (ACL) الخاصة بالإدخال والإخراج في الوقت نفسه على منفذ واحد دون تأثير على الأداء.
 - يمكن تطبيق قوائم التحكم في الوصول (ACL) لكل شبكة محلية ظاهرية (VLAN) أو لكل منفذ.
 - لا ينخفض أداء قائمة التحكم في الوصول (ACL) للإدخال حتى 15 ألف إدخال مع عمق المطابقة.
 - تتم معالجة قوائم التحكم في الوصول (ACL) إلى الإخراج بمعدل الخط لما يصل إلى 96 إدخال/إخراج. يختلف الأداء للمطابقات الأطول باختلاف عمق المطابقة.
- تستند بطاقات خط إيثرنت هذه إلى Engine 4+:

نوع بطاقة الخط	نوع الواجهة	نوع المحرك
بطاقة 10xGE Rev ("X-B")	:SFP	الفئة E4+
نمطي	:SFP	الفئة E4+

شبكة إيثرنت بسرعة 10 جيجابت	10G	الفئة E4+
شبكة إيثرنت بسرعة 10 جيجابت	10G	الفئة E4+

معايير المطابقة المدعومة

يتم دعم جميع معايير قائمة التحكم في الوصول (ACL) القياسية والموسعة من برنامج Cisco IOS Software في المسار السريع باستثناء إدخلات التحكم في الوصول (ACEs) إلى السجل أو الأجزاء.

عدد إدخلات التحكم في الوصول (ACE) المدعومة

- ما يصل إلى 15000 قائمة تحكم في الوصول (ACL) للإدخال يمكن تكوينها لكل منفذ أو لكل شبكة VLAN.
- وحدات ACE للإخراج لكل بطاقة طراز 1024 يمكن تطبيقها على كل منفذ. ملاحظة: 1021 من إدخلات التحكم في الوصول (ACEs) قابلة للتكوين. يتم حفظ ثلاثة إدخلات لأوامر ACE الضمنية IP any، ورفض ip any، والإرسال إلى وحدة المعالجة المركزية.

معالجة قائمة التحكم في الوصول (ACL) للإخراج

تتم معالجة قوائم التحكم في الوصول (ACL) إلى الإخراج بشكل طبيعي في المسار السريع لجانب الإرسال. راجع قائمة التحكم في الوصول (ACL) الخاصة بمخرجات IPv4 - مصفوفة عمليات تفاعل بطاقة الخط للحصول على مزيد من المعلومات.

الأوامر الخاصة بطاقة الخط

- دمج قائمة التحكم بالوصول (ACL) إلى IP الخاص بفتحة الوحدة <number> hw-module <

إرشادات التشغيل والتفاعلات بين بطاقات الخط

- تتم معالجة إدخلات التحكم في الوصول (ACEs) التي تحتوي على الكلمة الأساسية 'الجزء' في المسار البطيء.
- عدادات قائمة التحكم في الوصول غير مدعومة لقوائم التحكم في الوصول المقترنة بميزات أخرى.
- عدادات قائمة التحكم في الوصول (ACL) غير مدعومة لقوائم التحكم في الوصول (ACL) المدمجة. قوائم التحكم في الوصول (ACL) المدمجة قابلة للتكوين باستخدام الأمر `hw-module slot <slot number> ip acl merge`.
- يتم دعم ما يصل إلى 168 عملية من المستوى الرابع لكل بطاقة خط. وبمجرد تجاوز هذا الإجراء، يتم تشغيل قائمة التحكم في الوصول (ACL) في المسار البطيء.
- إذا تم تمكين بطاقة خط Engine 1 وتم تمكين قائمة التحكم في الوصول إلى الإخراج على بطاقة خط Egress Engine 3 أو +4، فإن قائمة التحكم في الوصول إلى الإخراج تتم معالجتها بواسطة كل من بطاقات خطوط الدخول والخروج للسماح لـ NetFlow بالحساب للحزم التي تم رفضها بواسطة قوائم التحكم في الوصول بالإضافة إلى الحزم المعاد توجيهها.

التوصيات

لا شيء في هذا الوقت.

تسجيل قائمة التحكم في الوصول (ACL)

قبل برنامج Cisco IOS الإصدار S(21)12.0، تم إرسال معلومات تسجيل قائمة التحكم في الوصول إلى RP بشكل حصري عبر حافلة الصيانة (MBUS). أثناء المستويات العالية لنشاط تسجيل قائمة التحكم في الوصول، كان من الممكن تجاوز قدرة MBUS. يقدم برنامج IOS الإصدار S(21)12.0 من Cisco العديد من التحسينات التي تمنع هذا السيناريو.

يتم الإبلاغ عن حالات الحمل الزائد ل MBUS بواسطة برنامج Cisco IOS مع رسائل الخطأ التالية:

LCLOG-3 - INVSTATE

MBUS_SYS-3 - SEQUENCE

باستخدام برنامج Cisco IOS الإصدار S(21)12.0 والإصدارات الأحدث، يتم تسليم رسائل التسجيل عالية الخطورة (من 0 إلى 4) إلى RP من خلال MBUS بينما يتم تسليم رسائل السجل الأقل خطورة (من 5 إلى 7) إلى RP من خلال بنية التحويل عالية السعة. رسائل سجل قائمة التحكم في الوصول (ACL) عالية الخطورة، وبالتالي يتم تسليمها الآن إلى RP من خلال بنية التحويل.

يمكن تكوين وظيفة التسجيل المضافة هذه باستخدام الأوامر التالية:

- **مكبر طريقة التسجيل [الخطورة]**—يحدد أي الرسائل سيتم إرسالها، حسب الخطورة، إلى RP باستخدام MBUS. سيتم إرسال رسائل ذات خطورة أكبر من خلال بنية المحول.
- **show logging method** — يعرض طريقة التسجيل الحالية لجميع مستويات خطورة الرسالة.
- **logging sequence-number** — يتيح هذا الأمر إرسال بطاقة الخط إلى رسائل سجل الرقم التسلسلي بحيث يمكن إعادة ترتيب الرسائل بشكل صحيح بواسطة RP. بدون هذا الأمر، يمكن تسليم رسائل السجل إلى RP بترتيب غير تسلسلي.

قائمة التحكم في الوصول (ACL) الخاصة بإخراج IPv4 - مصفوفة عمليات تفاعل بطاقة الخط

قبل إدخال معالجة قائمة التحكم في الوصول (ACL) إلى المخرج باستخدام إصدار المحرك 3 والمحرك 4+، تمت معالجة قوائم التحكم في الوصول إلى الإخراج بواسطة بطاقة خط الدخول. تم تحديث قوائم التحكم في الوصول (ACL) للإخراج للاستفادة من إمكانيات معالجة قوائم التحكم في الوصول (ACL) للإخراج ذات المحرك 3 فائق الأداء وقوائم التحكم في الوصول (ACL) للإخراج Engine 4+.

يقدم هذا المخطط ملخصاً للمكان الذي تتم فيه معالجة قوائم التحكم في الوصول إلى الإخراج لمجموعات بطاقات الخط المختلفة:

بطاقة خط الخروج						
بطاقة خط الدخول (يتم تطبيق قائمة التحكم في الوصول على واجهة العضو)	E0	E1	E2	E3	الفئة E4	E4+

E0	مدخل	مدخل	مدخل	مخرج	غير متوفر	مخرج
E1	مدخل	مدخل	مدخل	مخرج	غير متوفر	مخرج
E2	مدخل	مدخل	مدخل	مخرج	غير متوفر	مخرج
E3	مخرج	مخرج	مخرج	مخرج	غير متوفر	مخرج
الفئة E4	مخرج	مخرج	مخرج	مخرج	غير متوفر	مخرج
الفئة E4+	مخرج	مخرج	مخرج	مخرج	غير متوفر	مخرج

دعم قائمة التحكم في الوصول إلى IPv6

يتم دعم قوائم التحكم في الوصول (ACL) الموسعة ل IPv6 في المسار البطيء (الدخول والخروج) على E0، E1، E2، E3 و E4+ في برنامج Cisco IOS الإصدار S(23)12.0.

في المحرك 3، يتم دعم وظائف قائمة التحكم في الوصول (ACL) إلى IPv6 في الأجهزة في برنامج Cisco IOS الإصدار S(25)12.0. يتم تطبيق قوائم التحكم في الوصول (ACL) على واجهة معينة، مع بيان رفض ضمني في نهاية كل قائمة وصول. يتم تكوين قوائم التحكم في الوصول إلى IPv6 باستخدام الأمر `ipV6 access-list` مع كلمات المرور والسماح في وضع التكوين العام. تدعم البطاقات القائمة على المحرك 3 تصفية رؤوس خيار IPv6 القائمة على حركة المرور، وعناوين التدفق، ومعلومات إختيارية عن نوع بروتوكول الطبقة العليا.

مرجع أوامر قائمة التحكم في الوصول (ACL) ل Cisco 12000

أوامر المحرك 1

- وصلة أجهزة قائمة الوصول (أ)
- `show controller l3` | تضمين ASIC

أوامر المحرك 2

- حد PSA الخاص بالأجهزة لقائمة الوصول 128
- PSA لجهاز قائمة الوصول
- مجرى جانبي ل PSA
- تفاصيل `show access-list PSA`
- `show access-list psa summary`
- `show controller psa` سمة

أوامر المحرك 3

- `tcam no-merge <slot#> HW-Module` — بدءا من الإصدار S3(21)12.0 من برنامج Cisco IOS Software

- `<اسم الواجهة> <الخاص بواجهة جهاز show-access-list>`
- `show contr [tofab]frfab` قائمة التحكم في الوصول (int) ل vmr2ace

أوامر Engine 4+

- `show access-list gen7 label`

<show tcam appl [acl-in / ACL-Out] tcam <label-no >
<port> [show tcam appl [acl-in / ACL-Out] ذاكرة <عدد الإدخالات>
Engine 4+ Ethernet أوامر

• دمج قائمة التحكم بالوصول (ACL) إلى IP الخاص بفتحة الوحدة <number >hw-module

مسرد المصطلحات

يقدم هذا القسم تعريفات قياسية للمصطلحات ذات الصلة:

- **مستويات المعالجة**—يمكن تقسيم جهاز الشبكة بشكل منطقي إلى ثلاثة مستويات للمعالجة: مستوى البيانات—معالجة على الحزم المتدفقة عبر جهاز الشبكة. مستوى التحكم—المعالجة على الحزم المستخدمة لتلصيق أجهزة الشبكة معا. ويتضمن ذلك بروتوكولات الخط (مثل بروتوكول الاتصال من نقطة إلى نقطة - PPP والتحكم في إرتباط البيانات عالي المستوى - HDLC)، وبروتوكولات التوجيه (بروتوكول العبارة الحدودية - BGP، وبروتوكول معلومات التوجيه الإصدار 2 - RIPV2، وفتح أقصر مسار أولا - OSPF، وما إلى ذلك)، وبروتوكولات التوقيت (مثل بروتوكول وقت الشبكة - NTP). مستوى الإدارة—معالجة على الحزم التي يتم إستخدامها لإدارة أجهزة الشبكة. ويتضمن ذلك بروتوكول Telnet وبروتوكول SSH (Secure Shell) وبروتوكول نقل الملفات (FTP) وبروتوكول نقل الملفات المبسط (TFTP) وبروتوكول SNMP وبروتوكولات الإدارة الأخرى.
- **قوائم التحكم في الوصول (ACL) القياسية** - مرشح قوائم التحكم في الوصول (ACL) القياسية بشكل خاص في الطبقة 3.
- **تستخدم قوائم التحكم في الوصول (ACL) الموسعة** — قوائم الوصول إلى IP الموسعة عناوين المصدر والوجهة لعمليات المطابقة بالإضافة إلى معلومات نوع البروتوكول الاختياري للحصول على مستويات تحكم أكثر دقة.
- **قوائم التحكم في الوصول (ACL) الخطية المعالجة** — تتم معالجتها خطيا في البرنامج. يختلف الأداء حسب عمق المطابقة (عدد الإدخالات التي يجب فحصها قبل تحديد المطابقة).
- **قوائم التحكم في الوصول (ACL) من Turbo (محولة)** - تعمل قوائم التحكم في الوصول (ACL) من Turbo على تحسين معالجة قائمة التحكم في الوصول (ACL) للبرامج من خلال تجميع قائمة التحكم في الوصول (ACL) في سلسلة محسنة للغاية من جداول البحث التي تعمل على سرعة معالجة البرامج. لا يختلف أداء قوائم التحكم في الوصول (ACL) من Turbo مع عمق المطابقة.
- **قوائم التحكم في الوصول (ACL) للإدخال** — قائمة تحكم في الوصول (ACL) يتم تطبيقها على حركة المرور التي تدخل المنفذ الذي يتم تطبيقها عليه.
- **قوائم التحكم في الوصول إلى الإخراج** — قائمة تحكم في الوصول (ACL) يتم تطبيقها على حركة المرور التي تخرج المنفذ الذي يتم تطبيقها عليه. مع بعض الاستثناءات، تتم معالجة قوائم التحكم في الوصول للإخراج بواسطة بطاقة خط الإدخال.
- **قوائم التحكم في الوصول الخاصة بمسار الاستقبال**—توفر قوائم التحكم في الوصول الخاصة بمسار الاستقبال التصفية لحركة مرور التحكم الموجهة للموجه نفسه، مثل تحديثات التوجيه واستعلامات SNMP.
- **بطاقة خط إعادة توجيه المرحلة المزدوجة**—بطاقات خط تحتوي على ASICs لإعادة التوجيه/سمة على كل من مسار الدخول والخروج. وهذا يسمح لبطاقة الخط أن ينجز سمة على على حد سواء المدخل ربط تدفق ومخرج ربط تدفق دون ضرب ربط إلى ال CPU LC. كما تتيح إستخدام موجات جديدة من خوارزميات إعادة التوجيه ثنائية المراحل داخل Cisco 12000. بطاقة الخط Engine 3 Line Card هي مثال لبطاقة خط إعادة توجيه ثنائية المرحلة.
- **بطاقة خط إعادة توجيه مرحلة واحدة**—بطاقات خط تحتوي على بطاقات ASIC لإعادة التوجيه/الميزات على مسار الدخول فقط. تؤدي بطاقات الخط هذه معالجة تستند إلى ASIC فقط على الحزم التي تتدفق على مسار الدخول. لم تتم معالجة حركة مرور الخروج (فقط تمت إعادة توجيهها)، أو تمت معالجتها بواسطة مدخل ASICs من قوائم التحكم في الوصول (LC) الأخرى، أو تتم إدارتها بواسطة وحدة المعالجة المركزية (CPU) الخاصة بوحدة التحكم في الوصول (Engine 2) و Engine 4 و Engine 4+ هي أمثلة لبطاقات خط إعادة توجيه المرحلة الواحدة.

معلومات ذات صلة

- سلسلة موجهات الإنترنت طراز 12000 من Cisco
- الدعم التقني والمستندات - Cisco Systems

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س مل ا ذه Cisco ت مچرت
م ل اع ل اء ان ا ع مچ م ف ن م دخت س مل ل م عد و ت م م م دقت ل ة م ش ب ل و
م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م م چ ر ي . ة ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ل ا ا م ا د ع و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل چ ن ا ل ا دن ت س مل ا