فهم قوائم التحكم في الوصول إلى نقطة الوصول إلى الخدمة

المحتويات

المقدمة

يشرح هذا المستند كيفية قراءة قوائم التحكم في الوصول إلى نقطة الوصول إلى الخدمة (ACLs) (SAP) وإنشائها في موجهات Cisco. على الرغم من وجود أنواع عديدة من قوائم التحكم في الوصول، يركز هذا المستند على الأنواع التي تقوم بالتصفية استنادا إلى قيم SAP. النطاق الرقمي لهذا النوع من قائمة التحكم في الوصول (ACL) هو من 200 إلى 299. يمكن تطبيق قوائم التحكم في الوصول (ACL) هذه على واجهات Token Ring لتصفية حركة مرور مسار المصدر (SRB)، أو إلى واجهات إيثرنت لتصفية حركة مرور الجسر الشفاف (TB)، أو إلى موجهات نظير تحويل إرتباط البيانات (DLSw).

يكمن التحدي الرئيسي مع قوائم التحكم في الوصول إلى SAP في معرفة ما هي SAP التي يتم السماح بها أو رفضها بواسطة إدخال خاص بقوائم التحكم في الوصول (ACL). سنقوم بتحليل أربعة سيناريوهات مختلفة حيث تتم تصفية بروتوكول معين.

قبل البدء

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، راجع اصطلاحات تلميحات Cisco التقنية.

المتطلبات الأساسية

لا توجد متطلبات أساسية خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

بنية شبكة أنظمة التصفية

تستخدم حركة مرور بنية شبكة الأنظمة (SNA) ل IBM خوادم SAP تتراوح من 0x00 إلى 0xFF. يدعم أسلوب الوصول الظاهري للاتصالات (V3R4 (VTAM وفيما بعد نطاق قيمة SAP من 4 إلى 252 (أو 0x04 إلى 0xFC في التمثيل السداسي العشري)، حيث يتم حجز 0xF0 لحركة مرور NetBIOS. يجب أن تكون SAPs مضاعفات 0x04، بدءا من 0x04. تسمح قائمة التحكم في الوصول (ACL) التالية بأكثر بروتوكولات SNA SAPs شيوعا، وترفض الباقي (مع مراعاة وجود **رفض** ضمني **الكل** في نهاية كل قائمة تحكم في الوصول (ACL):

```
access-list 200 permit 0x0000 0x0D0D
```

سداسي عشر	ثنائي
0x0000 0x0d0d	DSAP SSAP Wild card Mask for DSAP and SSAP resp ecti vely ---| ----| | ----|-- ---| ----| | ----|-- 0000 0000 0000 0000 0000 1101 0000 1101

أستخدم وحدات بت في قناع حرف البدل لتحديد وحدات SAP المسموح بها من قبل إدخال قائمة التحكم في الوصول (ACL) هذا الخاص. أستخدم القواعد التالية عند تفسير وحدات بت قناع حرف البدل:

- 0 = تطابق تام مطلوب. هذا يعني أنه يجب أن يكون ل SAP المسموح بها نفس قيمة SAP التي تم تكوينها في قائمة التحكم في الوصول (ACL). ارجع إلى الجدول أدناه للحصول على مزيد من التفاصيل.
- 1 = يمكن أن يكون ل SAP المسموح به 0 أو 1 في وضع البت هذا، موضع "لا تهتم".

SAPS المسموح بها بواسطة قائمة	قناع حرف البدل	تكوين SAP في ACL

التحكم في الوصول (ACL)، حيث X=0 أو X=1		
0	0	0
0	0	0
0	0	0
0	0	0
X	1	0
X	1	0
0	0	0
X	1	0

وباستخدام النتائج الواردة في الجدول السابق، ترد أدناه قائمة بخطط التكيف الهيكلي التي تفي بالنمط المذكور أعلاه.

SAPs المسموح بها (سداسي عشري)	SAPS المسموح بها (بالقيم الثنائية)							
0x00	0	0	0	0	0	0	0	0
0x01	1	0	0	0	0	0	0	0
0x04	0	0	1	0	0	0	0	0
0x05	1	0	1	0	0	0	0	0
0x08	0	0	0	1	0	0	0	0
0x09	1	0	0	1	0	0	0	0
0x0C	0	0	1	1	0	0	0	0
0x0d	1	0	1	1	0	0	0	0

كما يمكنك أن ترى من الجدول أعلاه، لا يتم تضمين جميع بروتوكولات SNA المحتملة في قائمة التحكم في الوصول (ACL) هذه. غير أن هذه البرامج تغطي الحالات الأكثر شيوعا.

نقطة أخرى يجب مراعاتها عند تصميم قائمة التحكم في الوصول (ACL) هي أن قيم SAP تتغير اعتمادا على ما إذا كانت أوامر أو استجابات. تتضمن نقطة الوصول إلى الخدمة المصدر (SSAP) بت الأمر/الاستجابة (C/R) للتمييز بينهم. يتم تعيين C/R على 0 للأوامر وعلى 1 للاستجابات. لذلك، يجب أن تسمح قائمة التحكم في الوصول (ACL) بإصدار الأوامر وكذلك الاستجابات أو حظرها. على سبيل المثال، 0x05 SAP (المستخدم للاستجابات) هو 0x04 SAP مع تعيين C/R على 1. وينطبق الأمر نفسه على 0x08 SAP) 0x09 SAP مع تعيين C/R على 1) و 0x0D و 0x01.

NetBIOS للتصفية

تستخدم حركة مرور NetBIOS قيم 0xF0 SAP (للأوامر) و 0xF1 (للاستجابات). يستخدم مسؤولو الشبكة قيم SAP هذه بشكل نموذجي لتصفية هذا البروتوكول. يسمح إدخال قائمة الوصول الموضحة أدناه بحركة مرور NetBIOS ويرفض كل شيء آخر (تذكر **الرفض** الضمني **all** في نهاية كل قائمة تحكم في الوصول):

```
access-list 200 permit 0xF0F0 0x0101
```

باستخدام نفس الإجراء الموضح في القسم السابق، يمكنك تحديد أن قائمة التحكم في الوصول (ACL) أعلاه تسمح ل 0xF0 SAPs و 0xF1.

على العكس، إذا كان المتطلب هو حظر NetBIOS والسماح بباقي حركة المرور، فاستخدم قائمة التحكم في الوصول (ACL) التالية:

```
access-list 200 deny 0xF0F0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

تصفية IPX

بشكل افتراضي، تعمل موجهات Cisco على جسر حركة مرور IPX. لتغيير هذا السلوك، يجب عليك إصدار الأمر **ipx routing** على الموجه. يستخدم IPX، باستخدام عملية كبسلة 802.2، 0xE0 SAP كنقطة الوصول إلى الخدمة الوجهة (DSAP) و SSAP. لذلك، إذا كان موجه Cisco يجسر IPX والمطلب هو السماح بهذا النوع من حركة المرور فقط، فاستخدم قائمة التحكم في الوصول (ACL) التالية:

```
access-list 200 permit 0xE0E0 0x0101
```

على العكس، تقوم قائمة التحكم في الوصول التالية بحظر IPX والسماح بباقي حركة المرور:

```
access-list 200 deny 0xE0E0 0x0101
access-list 200 permit 0x0000 0xFFFF
```

السماح لجميع حركات المرور أو رفضها

تتضمن كل قائمة تحكم في الوصول (ACL) **رفض** ضمني **للكل**. يجب أن تكون على دراية بهذا الإدخال عند تحليل

سلوك قائمة التحكم في الوصول (ACL) التي تم تكوينها. يرفض آخر إدخال لقائمة التحكم في الوصول (ACL) الموضح أدناه جميع حركة المرور.

```
.... access-list 200 permit
.... access-list 200 permit
access-list 200 deny 0x0000 0xFFFF
```

تذكر عند قراءة قناع حرف البدل (بالقيم الثنائية)، أن 1 يعتبر موضع بت "لا تهتم". يترجم قناع حرف بدل كل 1s في التمثيل الثنائي إلى 0xFFFF في التمثيل سداسي عشر.

معلومات ذات صلة

- صفحة دعم DLSw
- قوائم التحكم في الوصول: نظرة عامة وإرشادات
- تقنيات تصفية DLSw+ SAP/MAC
- الدعم الفني - 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).