قوائم التحكم في الوصول وأجزاء IP

المحتويات

المقدمة

يشرح هذا التقرير الأنواع المختلفة لإدخالات قائمة التحكم في الوصول (ACL) وما يحدث عند مواجهة أنواع مختلفة من الحزم لهذه الإدخالات المختلفة. يتم إستخدام قوائم التحكم في الوصول (ACL) لحظر إعادة توجيه حزم IP بواسطة موجه.

يغطي RFC 1858 اعتبارات الأمان لتصفية أجزاء IP ويسلط الضوء على هجومين على مضيفين يتضمنان أجزاء IP من حزم TCP، وهجوم الأجزاء الصغيرة وهجوم الأجزاء المتداخلة. ومن المرغوب فيه منع هذه الهجمات لأنها قد تؤدي إلى تعريض مضيف ما للخطر، أو تقييد كل موارده الداخلية.

يصف RFC 1858 أيضا طريقتين للدفاع ضد هذه الهجمات، المباشرة وغير المباشرة. وفي الطريقة المباشرة، يتم تجاهل الأجزاء الأولية الأصغر من الحد الأدنى للطول. يتضمن الأسلوب غير المباشر تجاهل الجزء الثاني من مجموعة أجزاء، إذا كان يبدأ 8 بايت في مخطط بيانات IP الأصلي. يرجى الاطلاع على RFC 1858 للحصول على مزيد من التفاصيل.

وبشكل تقليدي، يتم تطبيق عوامل تصفية الحزم مثل قوائم التحكم في الوصول على الأجزاء غير الصغيرة والجزء الأولي من حزمة IP لأنها تحتوي على كل من معلومات الطبقة 3 و 4 التي يمكن لقوائم التحكم في الوصول (ACL) مضاهاتها للحصول على قرار السماح أو الرفض. يتم السماح بالأجزاء غير الأولية بشكل تقليدي من خلال قائمة التحكم في الوصول (ACL) لأنه يمكن حظرها استنادا إلى معلومات الطبقة 3 في الحزم؛ ومع ذلك، نظرا لأن هذه الحزم لا تحتوي على معلومات الطبقة الرابعة، فإنها لا تطابق معلومات الطبقة الرابعة في إدخال قائمة التحكم في الوصول، إذا كانت موجودة. يعد السماح بالأجزاء غير الأولية لمخطط بيانات IP من خلالها مقبولا لأن المضيف الذي يستقبل الأجزاء غير قادر على إعادة تجميع مخطط بيانات IP الأصلي دون الجزء الأولي.

كما يمكن إستخدام جدران الحماية لحظر الحزم من خلال الاحتفاظ بجدول لأجزاء الحزمة المفهرسة حسب عنوان IP للمصدر والوجهة والبروتوكول ومعرف IP. يمكن لكل من جدار حماية Cisco PIX وجدار حماية Cisco IOS® تصفية جميع الأجزاء الخاصة بتدفق معين من خلال الحفاظ على جدول المعلومات هذا، ولكن القيام بذلك على موجه للحصول على الوظائف الأساسية لقائمة التحكم في الوصول (ACL) يكلف كثيرا. تتمثل المهمة الأساسية لجدار الحماية في حظر الحزم، بينما يتمثل دوره الثانوي في توجيه الحزم؛ تتمثل المهمة الأساسية للموجه في توجيه الحزم، ويتلخص دوره الثانوي في حظرها.

تم إجراء تغييرين في برنامج CISCO IOS الإصدار 12.1(2) و 12.0(11) لمعالجة بعض مشاكل الأمان التي تحيط بأجزاء TCP. تم تنفيذ الطريقة غير المباشرة، كما هو موضح في RFC 1858 ، كجزء من التحقق القياسي من سلامة حزمة إدخال TCP/IP. كما تم إجراء تغييرات على وظائف قائمة التحكم في الوصول (ACL) فيما يتعلق بالأجزاء غير الأولية.

أنواع إدخالات قائمة التحكم في الوصول (ACL)

هناك ستة أنواع مختلفة من خطوط قائمة التحكم في الوصول، ولكل منها نتيجة إذا كانت الحزمة غير متطابقة أو غير متطابقة. في القائمة التالية، يشير FO = 0 إلى عدم وجود جزء أو جزء أولي في تدفق TCP، ويشير FO > 0 إلى أن الحزمة هي جزء غير أولي، و L3 تعني الطبقة 3، و L4 تعني الطبقة 4.

ملاحظة: عندما تكون هناك معلومات عن كل من الطبقة 3 والطبقة 4 في سطر قائمة التحكم في الوصول وتكون الكلمة الأساسية **الأجزاء** موجودة، يكون إجراء قائمة التحكم في الوصول (ACL) محافظا لكل من إجراءات السماح والرفض. تكون الإجراءات محافظة لأنك لا تريد رفض جزء مجزأ من التدفق بدون قصد لأن الأجزاء لا تحتوي على معلومات كافية لمطابقة كل سمات المرشح. في حالة الرفض، بدلا من رفض جزء غير أولي، تتم معالجة الإدخال التالي لقائمة التحكم في الوصول (ACL). في حالة السماح، يفترض أن معلومات الطبقة الرابعة في الحزمة، إن توفرت، تطابق معلومات الطبقة الرابعة في سطر قائمة التحكم في الوصول.

السماح لخط قائمة التحكم في الوصول (ACL) باستخدام معلومات L3 فقط

1. إذا تطابقت معلومات L3 الخاصة بالحزمة مع معلومات L3 في سطر قائمة التحكم في الوصول، فهذا مسموح به.
2. إذا لم تتطابق معلومات L3 للحزمة مع معلومات L3 في سطر قائمة التحكم في الوصول، فسيتم معالجة إدخال قائمة التحكم في الوصول التالي.

رفض خط قائمة التحكم بالوصول (ACL) باستخدام معلومات L3 فقط

1. إذا تطابقت معلومات الحزمة L3 مع معلومات L3 في سطر قائمة التحكم في الوصول، يتم رفضها.
2. إذا لم تتطابق معلومات L3 للحزمة مع معلومات L3 في سطر قائمة التحكم في الوصول، فسيتم معالجة إدخال قائمة التحكم في الوصول التالي.

السماح بسطر قائمة التحكم في الوصول (ACL) باستخدام معلومات L3 فقط، والكلمة الأساسية الأجزاء موجودة

إذا تطابقت معلومات الحزمة من المستوى الثالث مع معلومات L3 في سطر قائمة التحكم في الوصول، يتم التحقق من إزاحة جزء الحزمة.

1. إذا كانت الحزمة تساوي > 0، فإن الحزمة مسموح بها.
2. إذا كانت الحزمة = 0، تتم معالجة إدخال قائمة التحكم بالوصول (ACL) التالي.

رفض سطر قائمة التحكم في الوصول (ACL) بمعلومات L3 فقط، والكلمة الأساسية الأجزاء موجودة

إذا كانت معلومات الحزمة من المستوى الثالث لا تطابق معلومات L3 في سطر قائمة التحكم في الوصول، يتم التحقق من إزاحة جزء الحزمة.

1. إذا كانت الحزمة > 0، يتم رفض الحزمة.
2. إذا كانت الحزمة = 0، تتم معالجة سطر قائمة التحكم في الوصول (ACL) التالي.

السماح بخطوط قائمة التحكم في الوصول (ACL) مع معلومات L3 و L4

1. إذا تطابقت معلومات L3 و L4 الخاصة بالحزمة مع سطر قائمة التحكم في الوصول و FO = 0، يتم السماح للحزمة.
2. إذا تطابقت معلومات الحزمة من المستوى الثالث مع سطر قائمة التحكم بالوصول (ACL) وتعادل > 0، يتم السماح للحزمة.

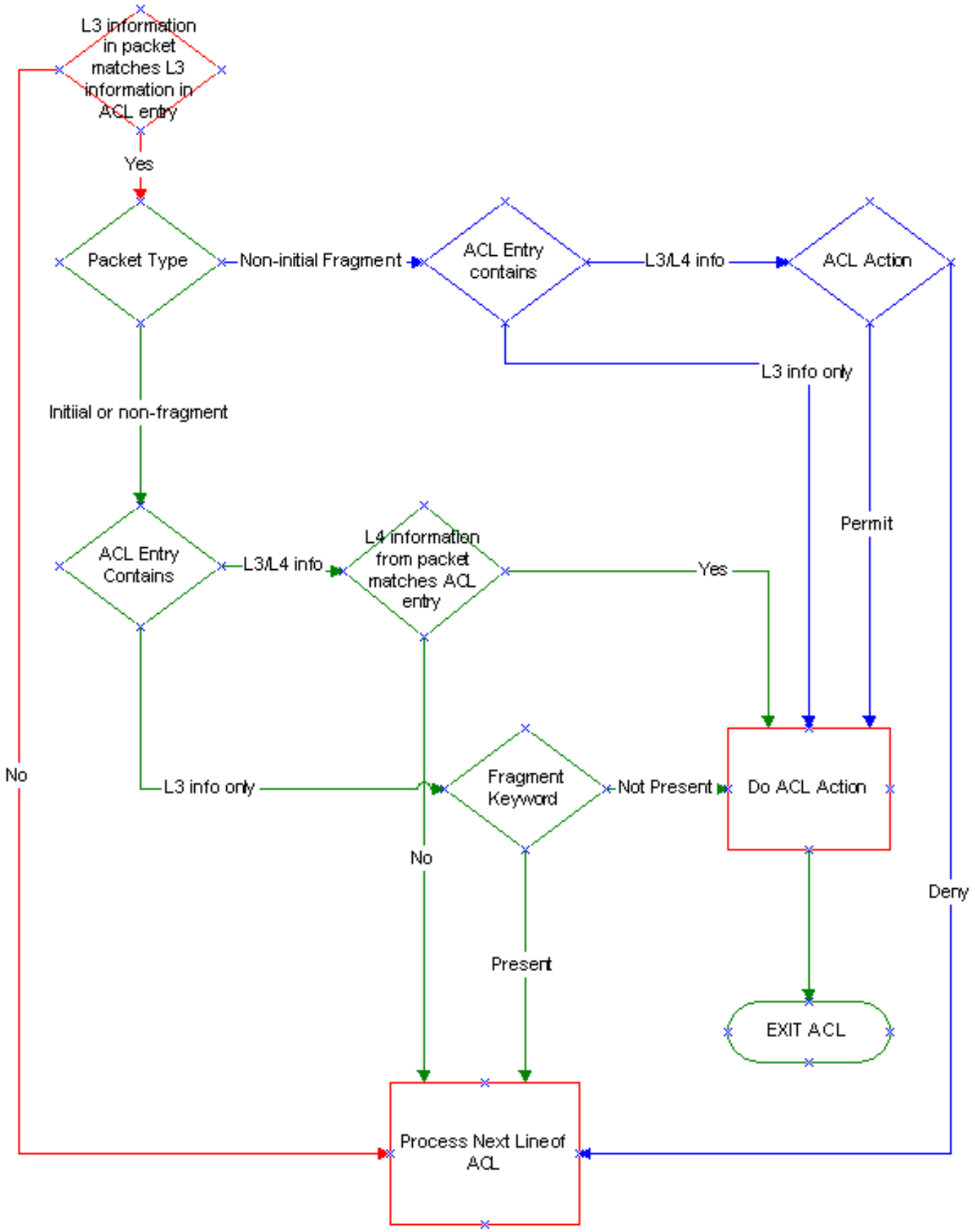
رفض خط قائمة التحكم بالوصول (ACL) باستخدام معلومات L3 و L4

1. إذا تطابقت معلومات L3 و L4 الخاصة بالحزمة مع إدخال قائمة التحكم بالوصول (ACL) و FO = 0، يتم رفض الحزمة.
2. إذا تطابقت معلومات L3 الخاصة بالحزمة مع سطر قائمة التحكم في الوصول (ACL) وتعادل > 0، فسيتم معالجة إدخال قائمة التحكم في الوصول التالي.

المخطط الانسيابي لقواعد قائمة التحكم في الوصول (ACL)

يوضح المخطط الانسيابي التالي قواعد قائمة التحكم في الوصول (ACL) عندما يتم التحقق من الأجزاء غير الأولية، والجزء الأولي، والجزء غير الأولية مقابل قائمة التحكم في الوصول (ACL).

ملاحظة: تحتوي الأجزاء غير الأولية نفسها على معلومات الطبقة 3 فقط، وليست أبدا من الطبقة 4، رغم أن قائمة التحكم في الوصول (ACL) قد تحتوي على معلومات من الطبقة 3 والطبقة 4.



كيف يمكن للحزم مطابقة قائمة التحكم في الوصول (ACL)

مثال 1

تتضمن السيناريوهات الخمسة المحتملة التالية أنواعا مختلفة من الحزم التي تواجه قائمة التحكم في الوصول ((ACL

100. يرجى الرجوع إلى الجدول ومخطط التدفق وأنت تتبع ما يحدث في كل حالة. عنوان IP الخاص بخادم الويب هو 171.16.23.1.

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

الحزمة هي جزء أولي أو ليست جزء موجه للخادم على المنفذ 80:

يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4 على السواء، والتي تطابق معلومات الطبقة 3 والطبقة 4 في الحزمة، لذلك يسمح بالحزمة.

الحزمة هي جزء أولي أو ليست جزء موجه للخادم على المنفذ 21:

1. يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4 على السواء، ولكن معلومات الطبقة 4 في قائمة التحكم في الوصول (ACL) لا تطابق الحزمة، لذلك تتم معالجة سطر قائمة التحكم في الوصول التالي.
2. يرفض السطر الثاني من قائمة التحكم في الوصول (ACL) جميع الحزم، لذلك يتم رفض الحزمة.

الحزمة هي جزء غير أولي إلى الخادم في تدفق أيسر 80:

يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4، وتطابق معلومات الطبقة 3 في قائمة التحكم في الوصول (ACL) الحزمة، ويكون إجراء قائمة التحكم في الوصول هو المسموح به، لذلك يتم السماح للحزمة.

الحزمة هي جزء غير أولي إلى الخادم في تدفق منفذ 21:

يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على كل من معلومات الطبقة 3 والطبقة 4. تطابق معلومات الطبقة 3 في قائمة التحكم في الوصول الحزمة، ولا توجد معلومات الطبقة 4 في الحزمة، ويكون إجراء قائمة التحكم في الوصول هو المسموح به، لذلك تكون الحزمة مسموح بها.

الحزمة هي جزء أولي أو جزء غير أولي أو جزء غير أولي لمضيف آخر على الشبكة الفرعية للخادم:

1. يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 التي لا تطابق معلومات الطبقة 3 في الحزمة (عنوان الوجهة)، لذلك تتم معالجة سطر قائمة التحكم في الوصول (ACL) التالي.
2. يرفض السطر الثاني من قائمة التحكم في الوصول (ACL) جميع الحزم، لذلك يتم رفض الحزمة.

مثال 2

تتضمن السيناريوهات الخمسة التالية المحتملة أنواعا مختلفة من الحزم التي تواجه قائمة التحكم في الوصول ((ACL 101. مرة أخرى، يرجى الرجوع إلى الجدول ومخطط التدفق وأنت تتبع ما يحدث في كل حالة. عنوان IP الخاص بخادم الويب هو 171.16.23.1.

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80
```

```
access-list 101 deny ip any any
```

الحزمة هي جزء أولي أو غير جزء موجه للخادم على المنفذ 80:

1. يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 التي تطابق معلومات الطبقة 3 في الحزمة. الإجراء قائمة التحكم في الوصول (ACL) هو الرفض، ولكن نظرا لأن الكلمة الأساسية **الأجزاء** موجودة، تتم معالجة إدخال قائمة التحكم في الوصول (ACL) التالي.
2. يحتوي السطر الثاني من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4، والتي تطابق الحزمة، لذلك يسمح بالحزمة.

الحزمة هي جزء أولي أو غير جزء موجه للخادم على المنفذ 21:

1. يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3، والتي تطابق الحزمة، ولكن إدخال قائمة التحكم في الوصول (ACL) يحتوي أيضا على الكلمة الأساسية **أجزاء**، والتي لا تطابق الحزمة بسبب FO = 0، لذلك تتم معالجة إدخال قائمة التحكم في الوصول التالي.
2. يحتوي السطر الثاني من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4. في هذه الحالة، لا تتطابق معلومات الطبقة الرابعة، لذلك تتم معالجة إدخال قائمة التحكم في الوصول (ACL) التالي.
3. يرفض السطر الثالث من قائمة التحكم في الوصول جميع الحزم، لذلك يتم رفض الحزمة

الحزمة هي جزء غير أولي إلى الخادم في تدفق أيسر 80:

يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 التي تطابق معلومات الطبقة 3 في الحزمة. تذكر أنه على الرغم من أن هذا جزء من تدفق منفذ 80، إلا أنه لا توجد معلومات للطبقة 4 في الجزء غير الأولي. يتم رفض الحزمة لأن معلومات الطبقة 3 تتطابق.

الحزمة هي جزء غير أولي إلى الخادم في تدفق منفذ 21:

يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 فقط، وهو يطابق الحزمة، لذلك يتم رفض الحزمة.

الحزمة هي جزء أولي أو جزء غير أولي لمضيف آخر على الشبكة الفرعية للخادم:

1. يحتوي السطر الأول من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 فقط، ولا يطابق الحزمة، لذلك تتم معالجة سطر قائمة التحكم في الوصول (ACL) التالي.
2. يحتوي السطر الثاني من قائمة التحكم في الوصول (ACL) على معلومات الطبقة 3 والطبقة 4. لا تتطابق معلومات الطبقة 4 والطبقة 3 في الحزمة مع معلومات قائمة التحكم في الوصول (ACL)، لذلك تتم معالجة سطر قائمة التحكم في الوصول التالي.
3. يرفض السطر الثالث من قائمة التحكم في الوصول (ACL) هذه الحزمة

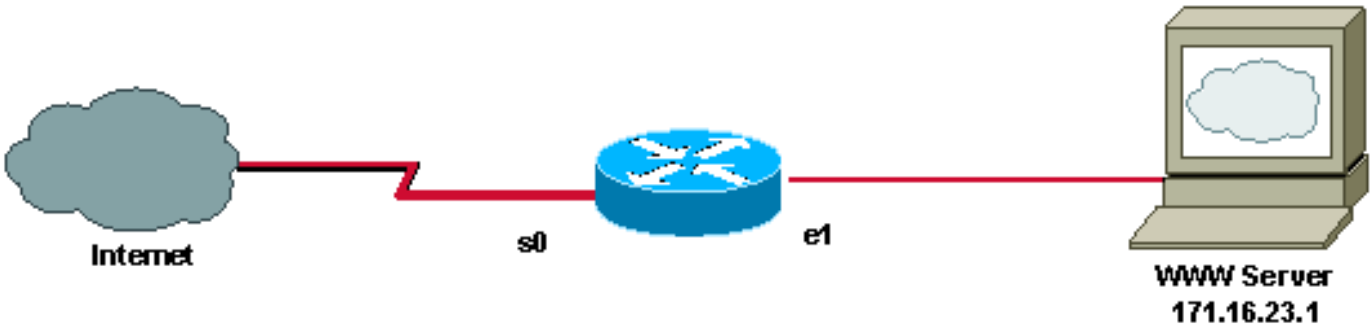
أجزاء سيناريوهات الكلمة الأساسية

السيناريو 1

يتصل الموجه B بخادم ويب، ولا يرغب مسؤول الشبكة في السماح لأي أجزاء بالوصول إلى الخادم. يوضح هذا السيناريو ما يحدث إذا قام مسؤول الشبكة بتنفيذ قائمة التحكم في الوصول (100 (ACL مقابل قائمة التحكم في الوصول (101 (ACL. يتم تطبيق قائمة التحكم في الوصول (ACL) الواردة على واجهة الموجهات S0) Serial0)

ويجب أن تسمح للحزم غير المجزأة فقط بالوصول إلى خادم الويب. راجع المخطط الانسيابي لقواعد قائمة التحكم في الوصول وكيف يمكن للحزم تطابق أقسام قائمة التحكم في الوصول وأنت تتبع السيناريو.

عواقب إستخدام الكلمة الأساسية للأجزاء



فيما يلي قائمة التحكم في الوصول (ACL) رقم 100:

```
access-list 100 permit tcp any host 171.16.23.1 eq 80

access-list 100 deny ip any any
```

يتيح السطر الأول من قائمة التحكم في الوصول (ACL) رقم 100 ل HTTP فقط إلى الخادم، ولكنه يسمح أيضا بالأجزاء غير الأولية إلى أي منفذ TCP على الخادم. وهو يسمح بهذه الحزم لأن الأجزاء غير الأولية لا تحتوي على معلومات الطبقة الرابعة، ويفترض منطق قائمة التحكم في الوصول (ACL) أنه إذا تطابقت معلومات الطبقة الثالثة، فستتطابق أيضا معلومات الطبقة الرابعة، إذا كانت متوفرة. الخط الثاني ضمني ويرفض كل آخر حركة مرور.

من المهم ملاحظة أنه، بدءا من الإصدار 12.1(2) من البرنامج Cisco IOS Software و 12.0(11)، تسقط التعليمات البرمجية لقائمة التحكم في الوصول (ACL) الجديدة الأجزاء التي لا تطابق أي سطر آخر في قائمة التحكم في الوصول (ACL). تتيح الإصدارات السابقة إمكانية مرور الأجزاء غير الأولية إذا لم تتطابق مع أي سطر آخر من قائمة التحكم في الوصول (ACL).

فيما يلي قائمة التحكم في الوصول (ACL) رقم 101:

```
access-list 101 deny ip any host 171.16.23.1 fragments

access-list 101 permit tcp any host 171.16.23.1 eq 80

access-list 101 deny ip any any
```

لا تسمح قائمة التحكم في الوصول (ACL) رقم 101 بالأجزاء غير الأولية التي تصل إلى الخادم بسبب السطر الأول. يتم رفض الجزء غير الأولي إلى الخادم عندما يواجه خط قائمة التحكم في الوصول (ACL) الأول لأن معلومات الطبقة 3 في الحزمة تطابق معلومات الطبقة 3 في سطر قائمة التحكم في الوصول (ACL).

كما تطابق الأجزاء الأولية أو غير الجزئية لمنفذ 80 على الخادم السطر الأول من قائمة التحكم في الوصول (ACL) لمعلومات الطبقة 3، ولكن نظرا لوجود الكلمة الأساسية الأجزاء، تتم معالجة إدخال قائمة التحكم في الوصول (ACL) التالي (السطر الثاني). يتيح السطر الثاني من قائمة التحكم في الوصول (ACL) المجال للأجزاء الأولية أو غير الأجزاء لأنها تطابق سطر قائمة التحكم في الوصول (ACL) لمعلومات الطبقة الثالثة والطبقة الرابعة.

يتم حظر الأجزاء غير الأولية الموجهة إلى منافذ TCP للأجهزة المضيفة الأخرى على الشبكة 171.16.23.0 بواسطة قائمة التحكم في الوصول (ACL) هذه. لا تتطابق معلومات الطبقة 3 في هذه الحزم مع معلومات الطبقة 3 في

سطر قائمة التحكم في الوصول (ACL) الأول، لذلك تتم معالجة سطر قائمة التحكم في الوصول (ACL) التالي. لا تطابق معلومات الطبقة 3 في هذه الحزم معلومات الطبقة 3 في سطر قائمة التحكم في الوصول (ACL) الثاني أيضا، لذلك تتم معالجة سطر قائمة التحكم في الوصول (ACL) الثالث. السطر الثالث ضمني ويرفض كل حركة مرور.

يقرر مسؤول الشبكة في هذا السيناريو تنفيذ قائمة التحكم في الوصول (ACL 101) لأنه يسمح فقط بتدفقات HTTP غير المجزأة إلى الخادم.

السيناريو 2

يتوفر لدى أحد العملاء اتصال بالإنترنت في موقعين مختلفين، كما يوجد اتصال خلفي بين الموقعين. نهج مسؤول الشبكة هو السماح للمجموعة A في الموقع 1 بالوصول إلى خادم HTTP في الموقع 2. تستخدم الموجهات في كلا الموقعين العناوين الخاصة (RFC 1918) وترجمة عنوان الشبكة (NAT) لترجمة الحزم التي يتم توجيهها عبر الإنترنت.

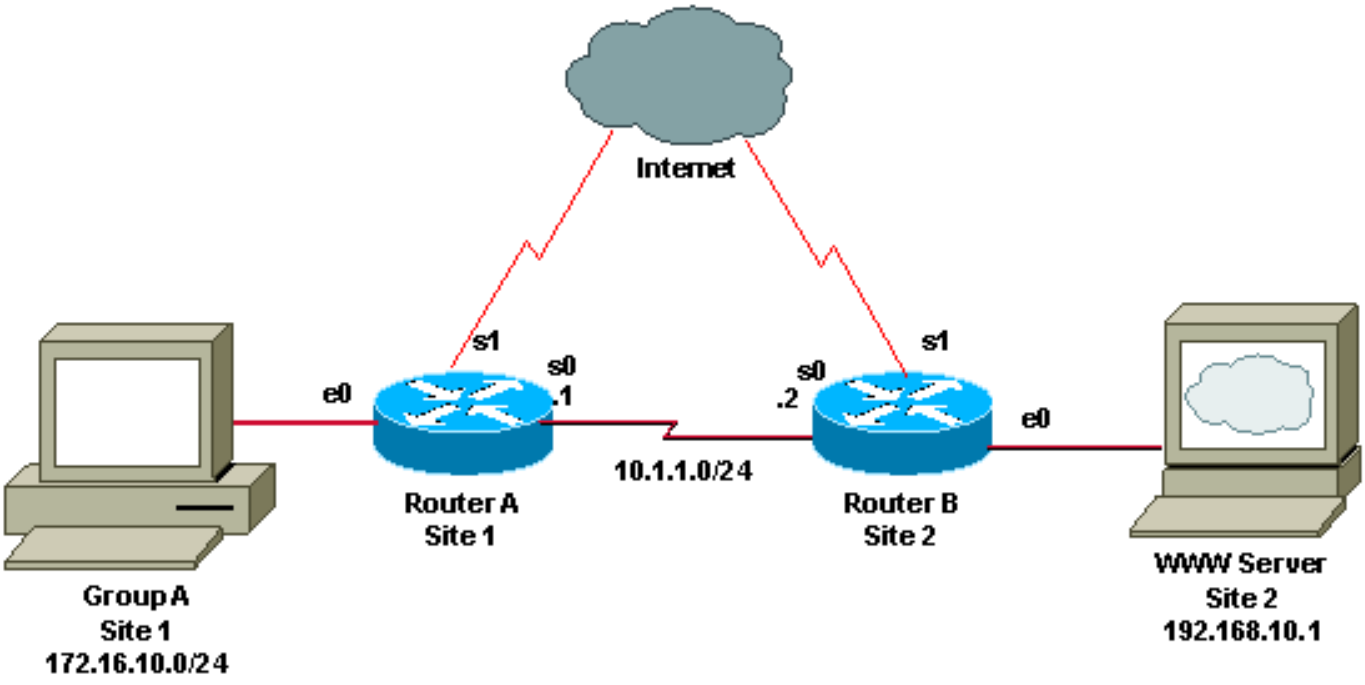
يقوم مسؤول الشبكة في الموقع 1 بتوجيه السياسات للعناوين الخاصة المعينة إلى المجموعة A، بحيث يستخدمون الباب الخلفي من خلال السلسلة التسلسلية0 للموجه A (S0) عند الوصول إلى خادم HTTP في الموقع 2. الموجه في الموقع 2 لديه مسار ثابت إلى 172.16.10.0، بحيث يتم توجيه حركة مرور البيانات العائدة إلى المجموعة A أيضا من خلال الباب الخلفي. كل آخر حركة مرور عولجت ب nat وموجهة عبر الإنترنت. يجب على مسؤول الشبكة في هذا السيناريو تحديد التطبيق أو التدفق الذي سيعمل إذا كانت الحزم مجزأة. لا يمكن جعل كلا من تدفقات بروتوكول نقل الملفات (HTTP) وبروتوكول نقل الملفات (FTP) تعمل في نفس الوقت بسبب حدوث فواصل أو أخرى.

راجع المخطط الانسيابي لقواعد قائمة التحكم في الوصول وكيف يمكن للحزم تطابق أقسام قائمة التحكم في الوصول وأنت تتبع السيناريو.

شرح خيارات مسؤول الشبكة

في المثال التالي، ترسل خريطة المسار المسماة FOO على الموجه A الحزم التي تطابق قائمة التحكم في الوصول (ACL 100) عبر الموجه B عبر S0. تتم معالجة جميع الحزم التي لا تطابق بواسطة NAT وتأخذ المسار الافتراضي من خلال الإنترنت.

ملاحظة: إذا سقطت حزمة من أسفل قائمة التحكم في الوصول (ACL)، أو تم رفضها بواسطتها، فلا يتم توجيهها وفقا للسياسة.



فيما يلي تكوين جزئي للموجه A، يوضح أن خريطة مسار السياسة المسماة FOO يتم تطبيقها على الواجهة E0، حيث

تدخل حركة المرور من المجموعة A إلى الموجه:

```
hostname Router_A
int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

تسمح قائمة التحكم في الوصول (100 (ACL بتوجيه السياسة على كل من الأجزاء الأولية وغير الأولية من HTTP المتدفقة إلى الخادم. يتم السماح بالأجزاء الأولية وغير الأولية من تدفقات HTTP إلى الخادم من قبل قائمة التحكم في الوصول (ACL) وتوجيه السياسة لأنها تطابق معلومات الطبقة الثالثة والطبقة الرابعة في سطر قائمة التحكم في الوصول (ACL) الأول. يتم السماح بالأجزاء غير الأولية بواسطة قائمة التحكم في الوصول (ACL) ويتم توجيه السياسة لأن معلومات الطبقة الثالثة في الحزمة تطابق أيضا سطر قائمة التحكم في الوصول (ACL) الأول؛ ويفترض منطق قائمة التحكم في الوصول أن معلومات الطبقة الرابعة في الحزمة ستتطابق أيضا إذا كانت متوفرة.

ملاحظة: ACL 100 تعطل الأنواع الأخرى من تدفقات TCP المجزأة بين المجموعة A والخادم لأن الأجزاء الأولية وغير الأولية تصل إلى الخادم من خلال مسارات مختلفة؛ وتتم معالجة الأجزاء الأولية بواسطة NAT ويتم توجيهها عبر الإنترنت، ولكن يتم توجيه الأجزاء غير الأولية من نفس التدفق عبر النهج.

يساعد تدفق FTP المجزأ على توضيح المشكلة في هذا السيناريو. تطابق الأجزاء الأولية لتدفق FTP معلومات الطبقة الثالثة، وليس معلومات الطبقة الرابعة، من سطر قائمة التحكم في الوصول (ACL) الأول، ويتم رفضها بعد ذلك بواسطة السطر الثاني. تتم معالجة هذه الحزم بواسطة NAT ويتم توجيهها عبر الإنترنت.

تتطابق الأجزاء غير الأولية لتدفق FTP مع معلومات الطبقة الثالثة في خط قائمة التحكم في الوصول (ACL) الأول، ويفترض منطق قائمة التحكم في الوصول (ACL) تطابق موجب على معلومات الطبقة الرابعة. ويتم توجيه هذه الحزم وفقا للسياسة، ولا يتعرف المضيف الذي يعيد تجميع هذه الحزم على الأجزاء الأولية كجزء من نفس التدفق كأجزاء غير أولية موجهة وفقا للسياسة نظرا لأن NAT قام بتغيير عنوان المصدر الخاص بالأجزاء الأولية.

تقوم قائمة التحكم في الوصول (100 (ACL في التكوين أدناه بإصلاح مشكلة FTP. ينكر السطر الأول من قائمة التحكم في الوصول (100 (ACL كلا من الأجزاء الأولية وغير الأولية لبروتوكول FTP من المجموعة A إلى الخادم.

```
hostname Router_A

int e0
ip policy route-map FOO
route-map FOO permit 10
match ip address 100
set ip next-hop 10.1.1.2

access-list 100 deny tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 fragments
access-list 100 permit tcp 172.16.10.0 0.0.0.255 host 192.168.10.1 eq 80
access-list 100 deny ip any any
```

تتطابق الأجزاء الأولية على معلومات الطبقة الثالثة في سطر قائمة التحكم في الوصول (ACL) الأول، ولكن يتسبب وجود الكلمة الأساسية **الأجزاء** في معالجة سطر قائمة التحكم في الوصول (ACL) التالي. لا يطابق الجزء الأولي سطر قائمة التحكم في الوصول (ACL) الثاني لمعلومات الطبقة 4، وبالتالي تتم معالجة السطر الضمني التالي من قائمة التحكم في الوصول (ACL)، مما يرفض الحزمة. تطابق الأجزاء غير الأولية معلومات الطبقة الثالثة في السطر الأول من قائمة التحكم في الوصول (ACL)، لذلك يتم رفضها. تتم معالجة كل من الأجزاء الأولية وغير الأولية بواسطة

NAT ويتم توجيهها عبر الإنترنت، لذلك لا توجد مشكلة لدى الخادم في إعادة التجميع.

يفكك إصلاح تدفقات FTP تدفقات HTTP المجزأة لأن أجزاء HTTP الأولية يتم توجيهها الآن وفقا للسياسة، ولكن تتم معالجة الأجزاء غير الأولية بواسطة NAT ويتم توجيهها عبر الإنترنت.

عندما يصادف جزء أولي من تدفق HTTP من المجموعة A إلى الخادم السطر الأول من قائمة التحكم في الوصول (ACL)، فإنه يتطابق مع معلومات الطبقة 3 في قائمة التحكم في الوصول (ACL)، ولكن بسبب الكلمة الأساسية **أجزاء**، تتم معالجة السطر التالي من قائمة التحكم في الوصول (ACL). يسمح السطر الثاني من قائمة التحكم في الوصول (ACL) ويوجه السياسة الحزمة إلى الخادم.

عندما تواجه أجزاء HTTP غير الأولية الموجهة من المجموعة A إلى الخادم السطر الأول من قائمة التحكم في الوصول (ACL)، فإن معلومات الطبقة 3 في الحزمة تطابق سطر قائمة التحكم في الوصول (ACL) ويتم رفض الحزمة. تتم معالجة هذه الحزم بواسطة NAT واجتياز الإنترنت للوصول إلى الخادم.

تسمح قائمة التحكم في الوصول (ACL) الأولى في هذا السيناريو بتدفقات HTTP المجزأة وتكسر تدفقات FTP المجزأة. تسمح قائمة التحكم في الوصول (ACL) الثانية بتدفقات FTP المجزأة وتكسر تدفقات HTTP المجزأة. يتدفق بروتوكول TCP في كل حالة لأن الأجزاء الأولية وغير الأولية تأخذ مسارات مختلفة إلى الخادم. لا يمكن إعادة التجميع لأن NAT قام بتغيير عنوان المصدر للأجزاء غير الأولية.

لا يمكن إنشاء قائمة تحكم في الوصول (ACL) تتيح كلا النوعين من التدفقات المجزأة إلى الخادم، لذلك يجب على مسؤول الشبكة إختيار التدفق الذي يريد عمله.

معلومات ذات صلة

- صفحة دعم توجيه IP
- 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).