أستكشاف أخطاء تكوينات جدار حماية Cisco وإصلاحها IOS

المحتويات

المقدمة

يوفر هذا المستند معلومات يمكنك إستخدامها لاستكشاف أخطاء تكوينات جدار حماية Cisco IOS® وإصلاحها.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

لا يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

الاصطلاحات

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

استكشاف الأخطاء وإصلاحها

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إصدار أوامر **debug**.

- لعكس (إزالة) قائمة الوصول، ضع "لا" أمام الأمر **access-group** في وضع تكوين الواجهة:

```
int
```

- إذا تم رفض عدد كبير للغاية من الزيارات، فقم بدراسة منطق القائمة أو حاول تحديد قائمة إضافية أوسع، ثم تطبيقها بدلا من ذلك. على سبيل المثال:

```
access-list # permit tcp any any
access-list # permit udp any any
access-list # permit icmp any any
int
```

- يوضح الأمر **show ip access-lists** قوائم الوصول التي يتم تطبيقها وحركة المرور التي يتم رفضها بواسطة هذه القوائم. إذا نظرت إلى عدد الحزم المرفوض قبل وبعد العملية الفاشلة مع عنوان IP للمصدر والوجهة، فإن هذا الرقم يزيد إذا كانت قائمة الوصول تمنع حركة المرور.
- إذا لم يتم تحميل الموجه بشدة، يمكن إجراء تصحيح الأخطاء على مستوى الحزمة في قائمة الوصول الموسعة أو ip inspection. إذا تم تحميل الموجه بشدة، يتم إبطاء حركة المرور من خلال الموجه. أستخدم التمييز مع أوامر تصحيح الأخطاء.قم بإضافة الأمر **no ip route-cache** بشكل مؤقت إلى الواجهة:

```
int
```

بعد ذلك، في وضع التمكين (ولكن ليس التكوين):

```
term mon
debug ip packet # det
```

ينتج مخرجات مماثلة لهذا:

```
,(Mar 1 04:38:28.078: IP: s=10.31.1.161 (Serial0), d=171.68.118.100 (Ethernet0*
                                                    g=10.31.1.21, len 100, forward
,Mar 1 04:38:28.086: IP: s=171.68.118.100 (Ethernet0), d=9.9.9.9 (Serial0), g=9.9.9.9*
                                                      len 100, forward
```

- كما يمكن إستخدام قوائم الوصول الموسعة مع خيار "log" في نهاية العبارات المختلفة:

```
access-list 101 deny ip host 171.68.118.100 host 10.31.1.161 log
access-list 101 permit ip any any
```

لذلك يمكنك الاطلاع على الرسائل على الشاشة لحركة المرور المسموح بها والمرفوضة:

```
Mar 1 04:44:19.446: %SEC-6-IPACCESSLOGDP: list 111 permitted icmp 171.68.118.100*
                                                  packets 15 ,(0/0) 10.31.1.161 <-
(Mar  1 03:27:13.295: %SEC-6-IPACCESSLOGP: list 118 denied tcp 171.68.118.100(0*
                                                    packet 1 ,(0)10.31.1.161 <-
```

- إذا كانت قائمة فحص ip مشتبه فيها، فإن الأمر **debug ip inspection <type_of_traffic>**ينتج مخرجات مثل هذا الإخراج:

```
Feb 14 12:41:17 10.31.1.52 56: 3d05h: CBAC* sis 258488 pak 16D0DC TCP P ack 3195751223
                                (seq 3659219376(2) (10.31.1.5:11109) => (12.34.56.79:23
Feb 14 12:41:17 10.31.1.52 57: 3d05h: CBAC* sis 258488 pak 17CE30 TCP P ack 3659219378
                                (seq 3195751223(12) (10.31.1.5:11109) <= (12.34.56.79:23
```

بالنسبة لهذه الأوامر، ارجع إلى وكيل مصادقة أستكشاف الأخطاء وإصلاحها، إلى جانب معلومات أستكشاف الأخطاء وإصلاحها الأخرى.

معلومات ذات صلة

- دعم منتج جدار حماية Cisco IOS
- 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).