فهم حزم RST المُرسلة بواسطة Secure Firewall

المحتويات

المقدمة

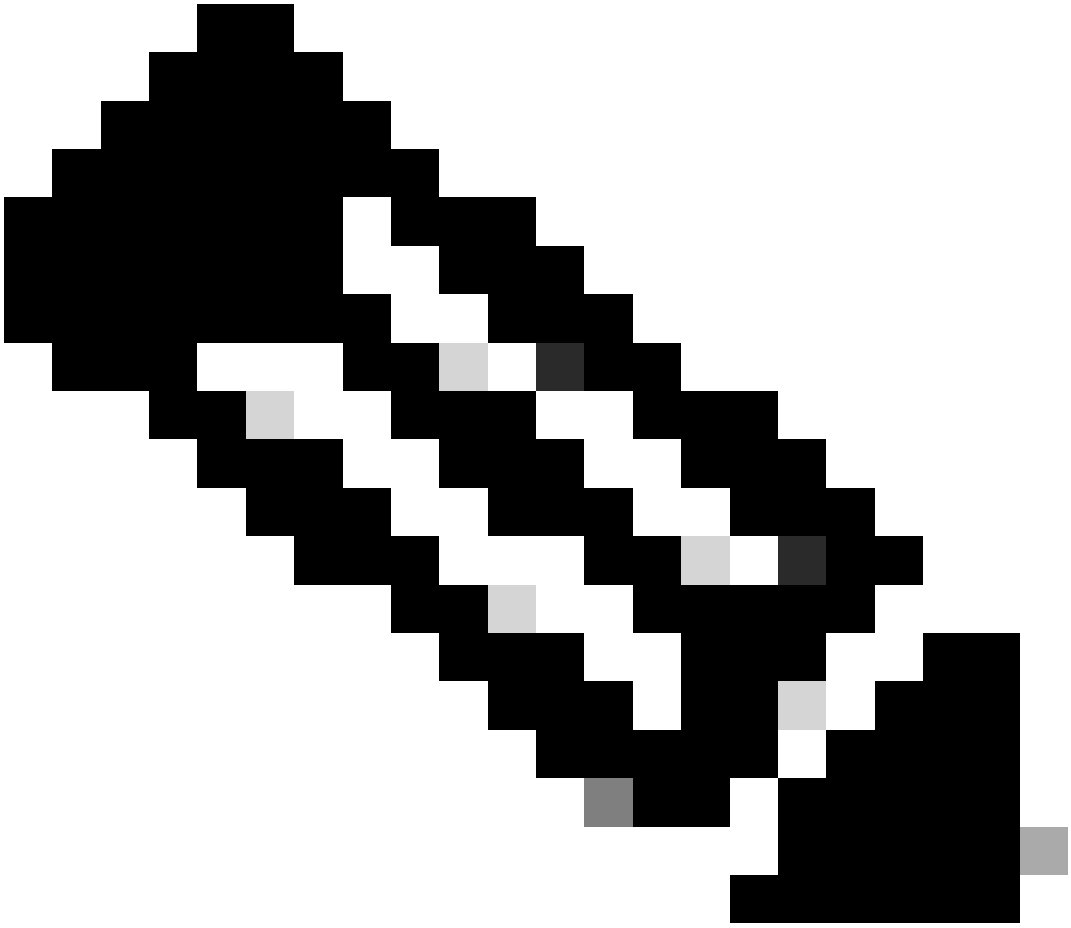
يصف هذا المستند سلوك Cisco Firewall عند إرسال عمليات إعادة تعيين TCP لجلسات عمل TCP التي تحاول عبور Firewall.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تدفق حزمة ASA
- تدفق حزم FTD
- التقاط حزمة ASA/FTD



ملاحظة: ينطبق هذا السلوك الموضح على الدفاع ضد تهديد جدار الحماية الآمن و ASA.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى هذا البرنامج:

- ASA
- برنامج الدفاع ضد تهديد جدار الحماية الآمن FTD

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 قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

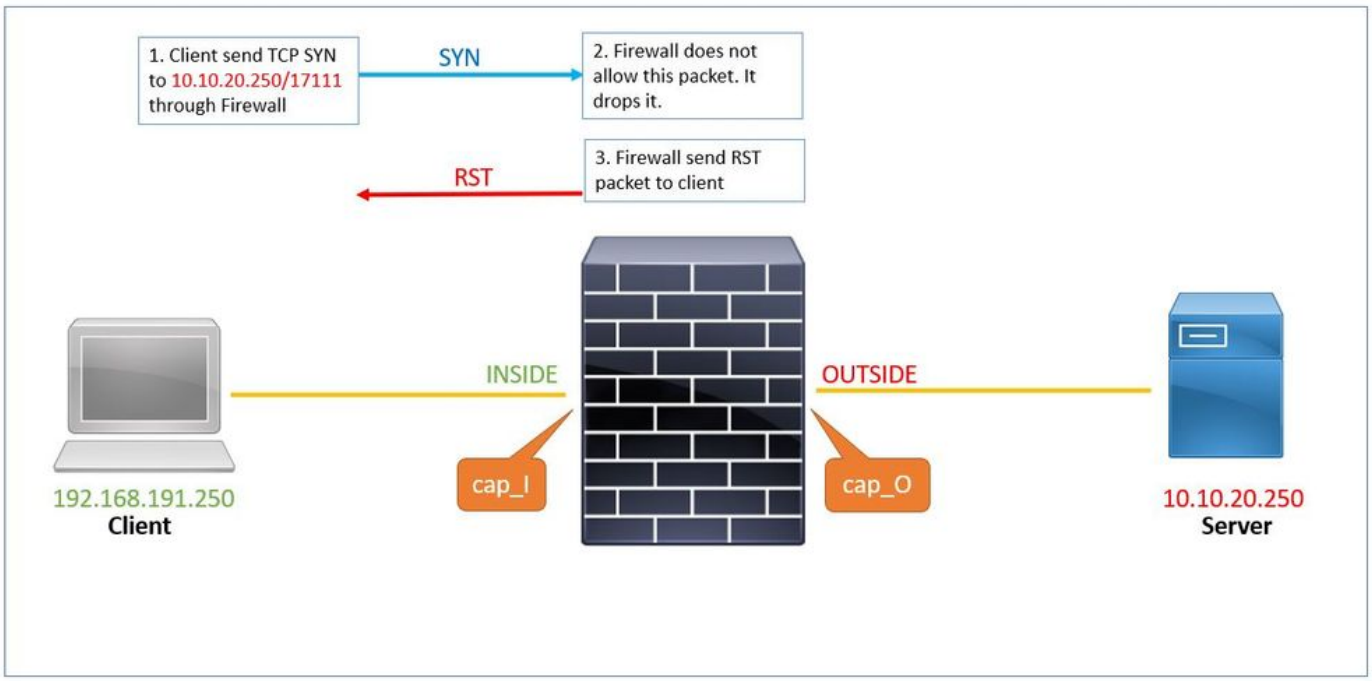
استكشاف الأخطاء وإصلاحها

يرسل جدار الحماية رسائل إعادة توجيه TCP لجلسات عمل TCP التي تحاول نقل جدار الحماية

ويتم رفضها بواسطة جدار الحماية استنادا إلى قوائم الوصول. يرسل جدار الحماية أيضا عمليات إعادة الضبط للحزم المسموح بها من قبل قائمة الوصول، ولكنها لا تنتمي إلى اتصال موجود في جدار الحماية وبالتالي يتم رفضها بواسطة ميزة بيان الحالة.

دراسة الحالة 1: resetoutbound يتم تمكين الخدمة ورفض حركة مرور العميل إلى الخادم.

بشكل افتراضي، يتم تمكين إعداد توزيع الخدمة لكافة الواجهات. في دراسة الحالة هذه، لا توجد قاعدة للسماح بحركة مرور البيانات من العميل إلى الخادم.



هذه هي عمليات الالتقاط التي تم تكوينها في جدار الحماية:

```
# show capture
capture cap_I type raw-data trace trace-count 50 interface INSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture cap_O type raw-data trace trace-count 50 interface OUTSIDE [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
capture asp type asp-drop all [Capturing - 0 bytes]
match tcp host 192.168.191.250 host 10.10.20.250
```

تم تمكين إعادة تعيين الخدمة بشكل افتراضي. لذلك، إذا عرض مخرجات show run service الأمر ال شيء، فهذا يعني أنه ممكن:

```
# show run service ...
```

1. يرسل العميل TCP SYN إلى الخادم 10.10.20.250/17111 من خالل جدار الحماية. الحزمة رقم 1 في هذا التقاط:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

2. وظهر عدم وجود قائمة التحكم في الوصول (ACL) للسماح بحركة المرور هذه، يقوم جدار الحماية الآمن بإسقاط هذه الحزمة acl-dropبسبب. يتم التقاط هذه الحزمة في التقاط ASP-drop.

```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74
192.168.191.250.46118 > 10.10.20.250.17111: S [tcp sum ok] 3490277958:3490277958(0) win 29200 <mss 1380
    (DF) (ttl 49, id 60335)

<output removed>

Subtype: log
Result: DROP
Config:
access-group allow_all global
access-list allow_all extended deny ip any any
Additional Information:

<output removed>

Result:
input-interface: INSIDE
input-status: up
input-line-status: up
output-interface: OUTSIDE
output-status: up
output-line-status: up
Action: drop
```

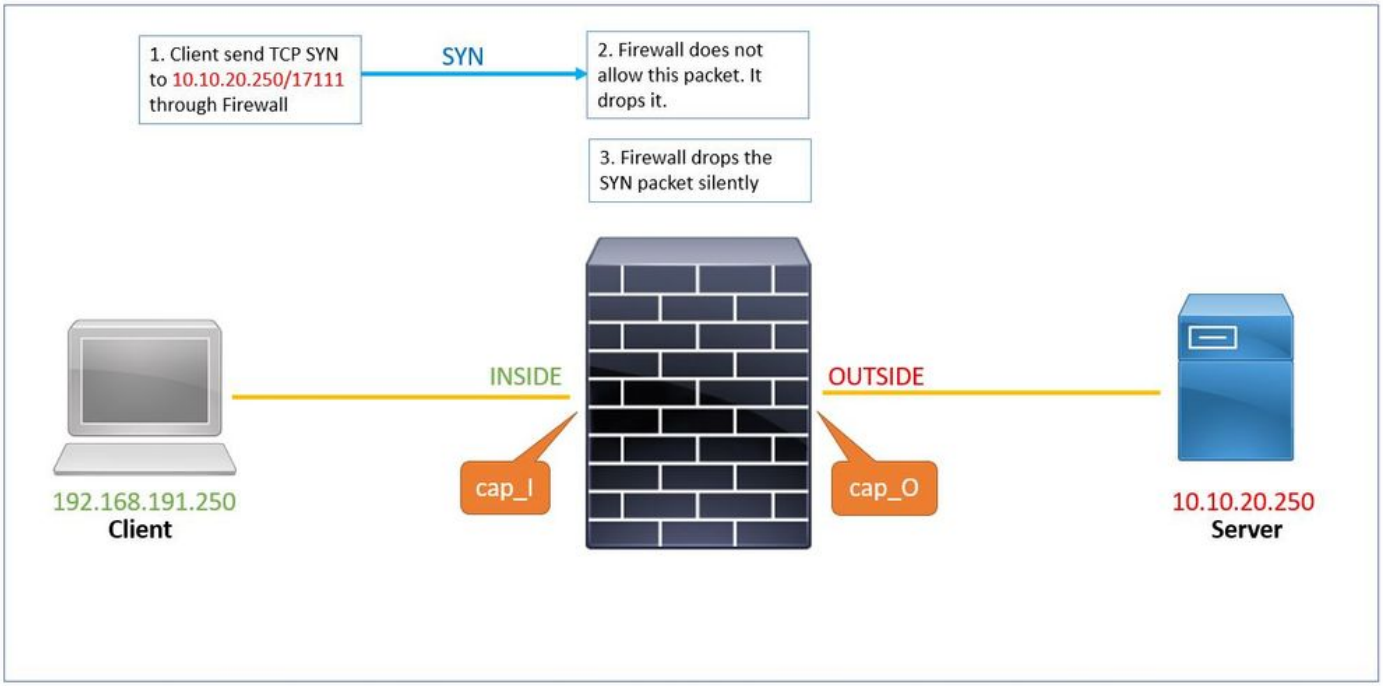
```
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. يرسل جدار الحماية حزمة RST مع الخادم عنوان كمصدر عنوان. الحزمة رقم 2 في هذا التقاط:

```
# show capture cap_I
1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
        timestamp 2096884214 0,nop,wscale 7>
2: 19:48:55.512806 10.10.20.250.17111 > 192.168.191.250.46118: R 0:0(0) ack 3490277959 win 29200
```

دراسة الحالة 2: لم يتم تمكين إعادة توزيع الخدمة ورفض نقل البيانات من عميل إلى خادم.

في دراسة الحالة 2، لا توجد قاعدة للسماح بحركة مرور البيانات من العميل إلى الخادم وتعطيل إعادة توزيع الخدمة.



يعرض show run service الأمر أن إعادة تعيين الخدمة معطلة.

```
# show run service
no service resetoutbound
```

1. يرسل العميل TCP إلى الخادم 10.10.20.250/17111 من خالل جدار الحماية. الحزمة رقم 1 في هذا التقاط:

```
# show capture cap_I

1: 19:48:55.512500 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200
<mss 1380,sackOK,timestamp 2096884214 0,nop,wscale 7>
```

2. انظر لعدم وجود قائمة التحكم في الوصول (ACL) للسماح بحركة المرور هذه، يقوم جدار الحماية الآمن بإسقاط هذه الحزمة بسبب acl-drop. تم التقاط هذه الحزمة في **asp-drop capture**.

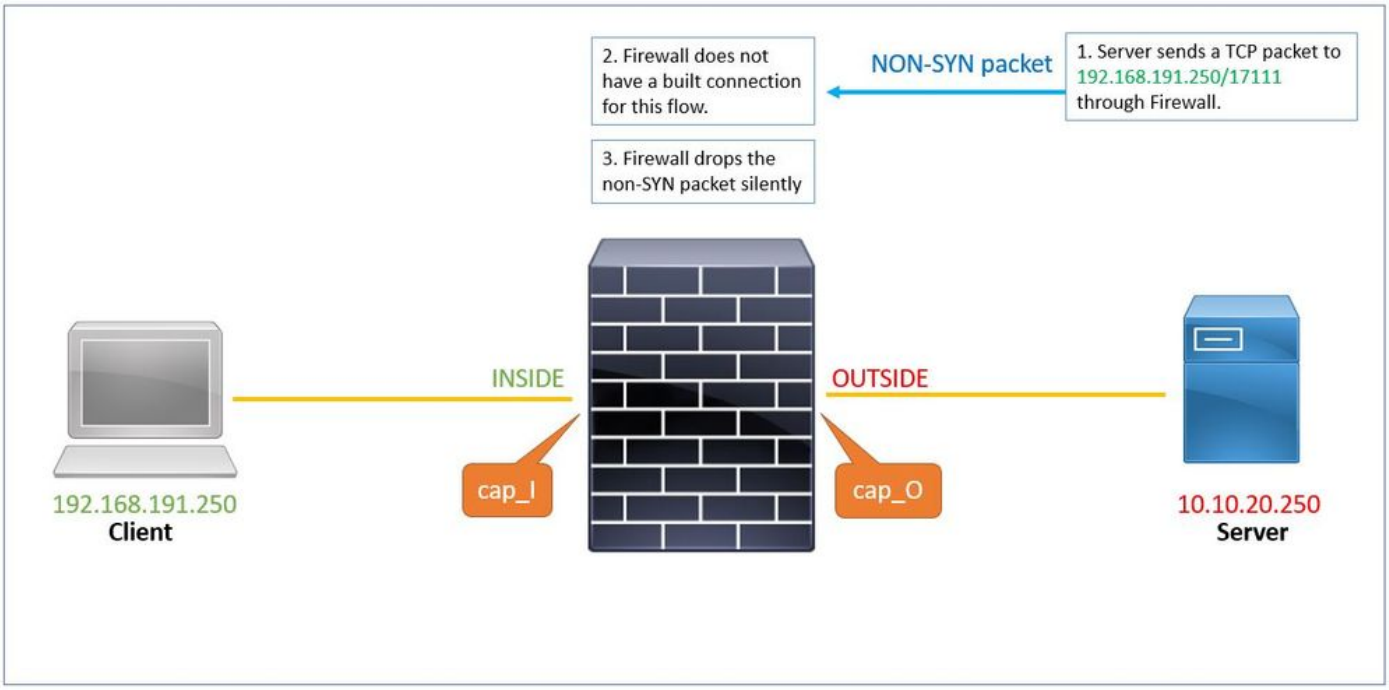
```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74 192.168.191.250.46118 > 10.10.20.250
```

3. **asp-drop capture** يعرض الحزمة syn ولكن ال يوجد حزمة RST مرسلة مرة أخرى cap_I capture عبر الواجهة الداخلية:

```
# show cap cap_I
1: 23:58:32.850755 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms

# show cap asp
1: 23:58:32.850999 192.168.191.250.46118 > 10.10.20.250.17111: S 3490277958:3490277958(0) win 29200 <ms
```

دراسة الحالة 3: تم تعطيل إعادة تعيين الخدمة (بشكل افتراضي) تم تعطيل إعادة تعيين الخدمة (بشكل افتراضي)

بشكل افتراضي، يتم تمكين إعادة توجيه الخدمة لجميع الواجهات وتعطيل إعادة تعيين الخدمة.



1. يرسل الخادم حزمة TCP (SYN/ACK) إلى العميل من خلال جدار الحماية. لا يحتوي جدار الحماية على اتصال تم إنشاؤه لهذا التدفق.

```
# show capture cap_O

1: 00:22:35.111993 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

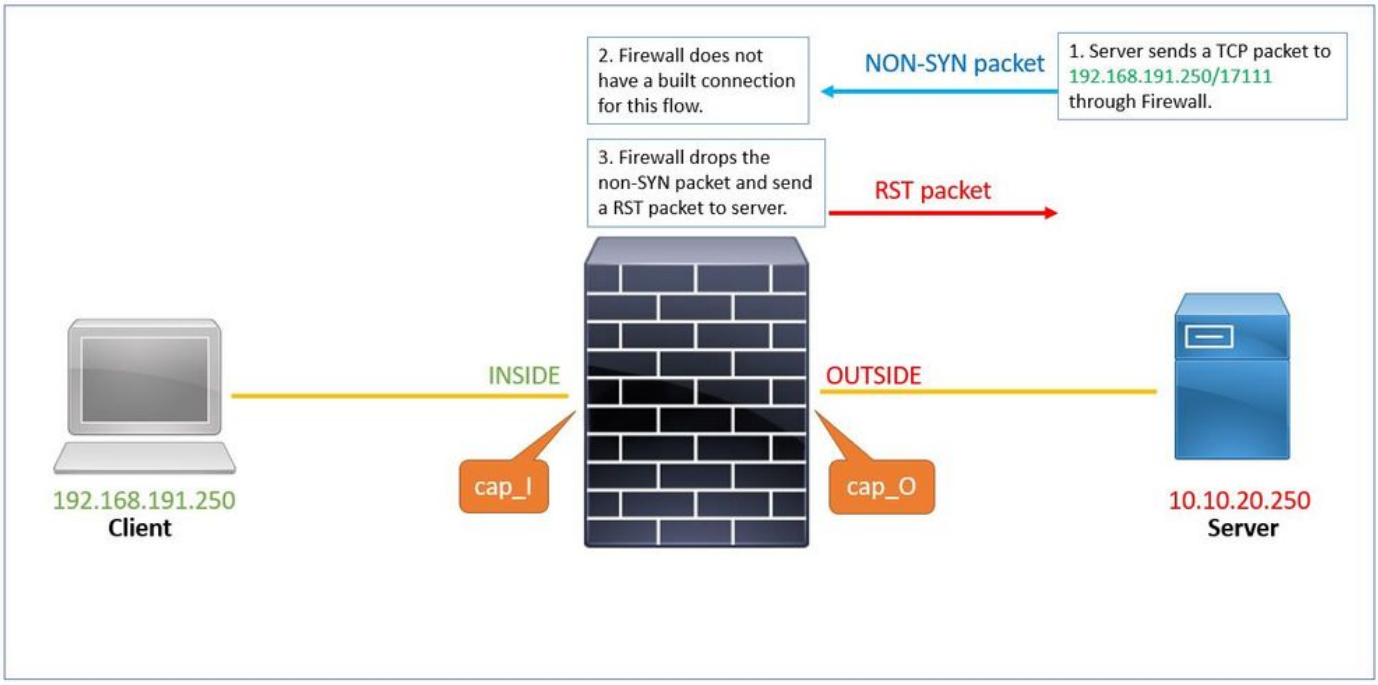
2. لم يتم إرسال إعادة التعيين من "جدار الحماية" إلى الخادم. يتم إسقاط حزمة SYN/ACK هذه بصمت لسببtcp-not-syn. و يتم القبض عليها asp-drop capture أيضا.

```
# show capture cap_O packet-number 1 trace detail
1: 00:22:35.111993 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
</pre
```

```
# show capture asp

1: 00:22:35.112176 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

دراسة الحالة 4: تم تعطيل إعادة تعيين الخدمة (بشكل افتراضي) تم تعطيل إعادة تعيين الخدمة.

بشكل افتراضي، يتم تعطيل إعادة توجيه الخدمة لجميع الواجهات ويتم تعطيل إعادة تعيين الخدمة أيضا باستخدام أمر التكوين.



يعرض إخراج show run service الأمر أن إعادة تعيين الخدمة معطلة (بشكل افتراضي) وأن إعادة تعيين الخدمة معطلة بواسطة أمر التكوين.

```
# show run service
service resetinbound
```

1. يرسل الخادم حزمة TCP (SYN/ACK) إلى العميل من خلال جدار الحماية.

```
# show cap cap_O

1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
```

2. لا يحتوي جدار الحماية على اتصال تم إنشاؤه لهذا التدفق ويقوم بإسقاطه. يعرض asp-drop captures الحزمة:

```
# show capture cap_O packet-number 1 trace detail
1: 00:32:26.434395 a2c7.1e00.003e 0050.56b3.1ef5 0x0800 Length: 70
10.10.20.250.17111 > 192.168.191.250.46118: S [tcp sum ok] 3475024584:3475024584(0) ack 3490277959 win
   (DF) (ttl 255, id 62104)

<output removed>

Result:
input-interface: OUTSIDE
input-status: up
input-line-status: up
output-interface: INSIDE
output-status: up
output-line-status: up
Action: drop
Drop-reason: (tcp-not-syn) First TCP packet not SYN, Drop-location: frame 0x0000561961c89aaa flow (NA)/
```

3. منذ إعادة تعيين الحزمة، يرسل جدار الحماية حزمة RST إلى الخادم باستخدام عنوان IP المصدر الخاص بالعميل.

```
# show capture cap_O
1: 00:32:26.434395 10.10.20.250.17111 > 192.168.191.250.46118: S 3475024584:3475024584(0) ack 349027795
2: 00:32:26.434608 192.168.191.250.46118 > 10.10.20.250.17111: R 3490277959:3490277959(0) ack 347502458
```

معلومات ذات صلة

- [الدعم الفني والتنزيلات من Cisco]

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).