Grundlegendes zu RST-Paketen, die von Cisco Secure Firewall gesendet werden

Inhalt

Einleitung

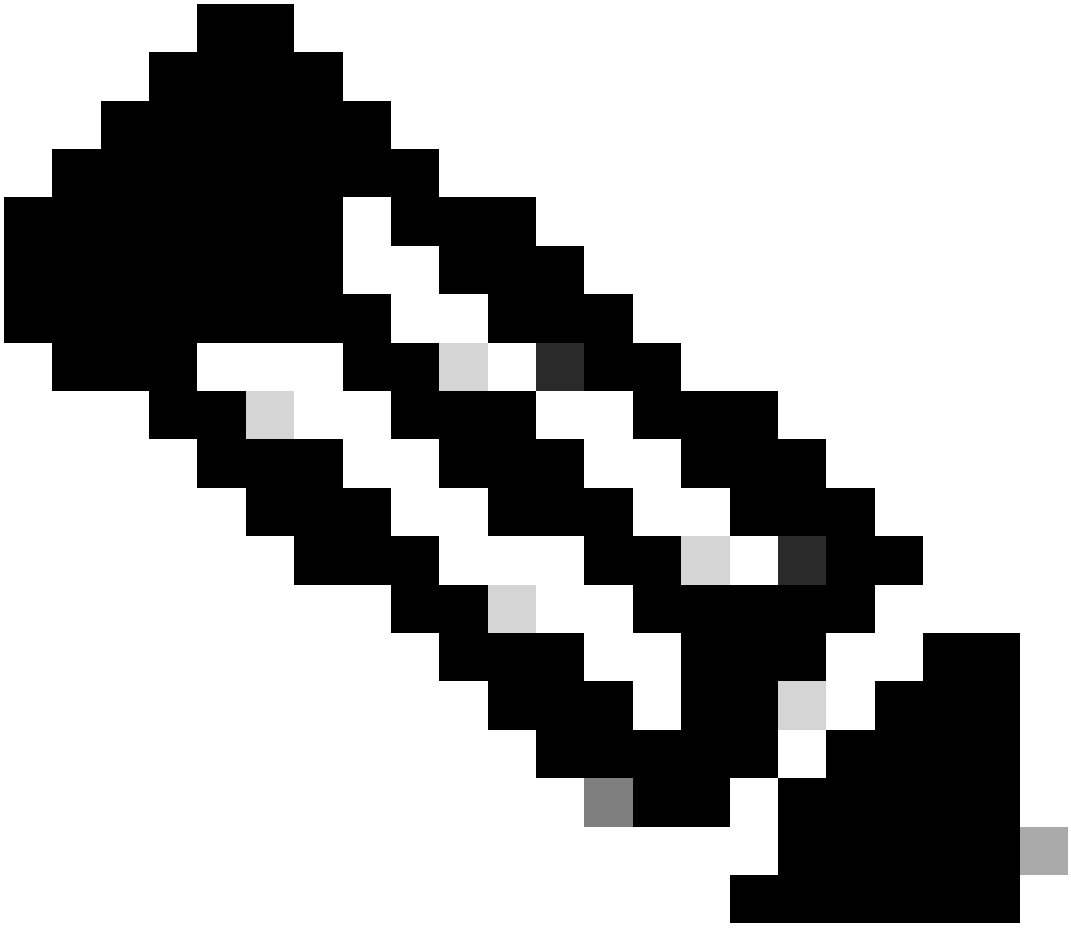
In diesem Dokument wird das Verhalten einer Cisco Firewall beschrieben, wenn TCP-Zurücksetzungen für TCP-Sitzungen gesendet werden, die versuchen, die Firewall zu passieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- ASA-Paketfluss
- FTD-Paketfluss
- ASA-/FTD-Paketerfassung



Hinweis: Dieses Verhalten gilt für die ASA und die sichere Abwehr von Bedrohungen durch Firewalls.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dieser Software:

- ASA
- Secure Firewall Threat Defense - FTD

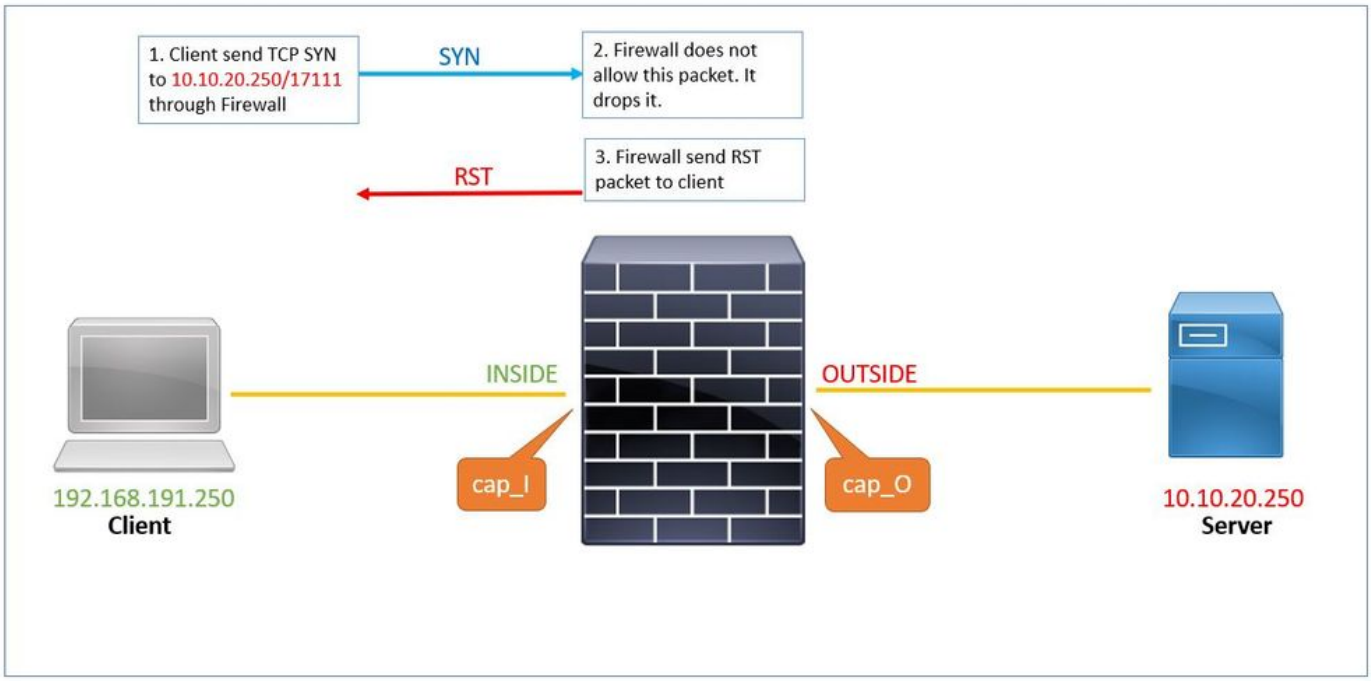
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Fehlerbehebung

Die Firewall sendet TCP-Resets für TCP-Sitzungen, die die Firewall passieren sollen und von der Firewall basierend auf Zugriffslisten abgelehnt werden. Die Firewall sendet auch Resets für Pakete, die von einer Zugriffsliste zugelassen werden, aber nicht zu einer Verbindung gehören, die in der Firewall vorhanden ist und daher von der Stateful-Funktion abgelehnt wird.

Anwenderbericht 1: Service resetoutbound ist aktiviert, und Datenverkehr zwischen Client und Server wird abgelehnt.

Service **ResetOutbound** ist standardmäßig für alle Schnittstellen aktiviert. In dieser Fallstudie gibt es keine Regel, die den Datenverkehr zwischen Client und Server zulässt.



Dies sind die in der Firewall konfigurierten Erfassungen:

```
# 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
```

Das Zurücksetzen des DienstsAusgehend ist standardmäßig aktiviert. Wenn die Ausgabe des show run service Befehls also nichts anzeigt, bedeutet dies, dass sie aktiviert ist:

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

1. Client sendet TCP SYN über Firewall an Server 10.10.20.250/17111. Paket Nr. 1 in dieser Erfassung:

```
# 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. Da keine ACL vorhanden ist, die diesen Datenverkehr zulässt, verwirft die sichere Firewall dieses Paket mit acl-drop einer Begründung. Dieses Paket wird bei der asp-drop-Erfassung erfasst.

```
# 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
```

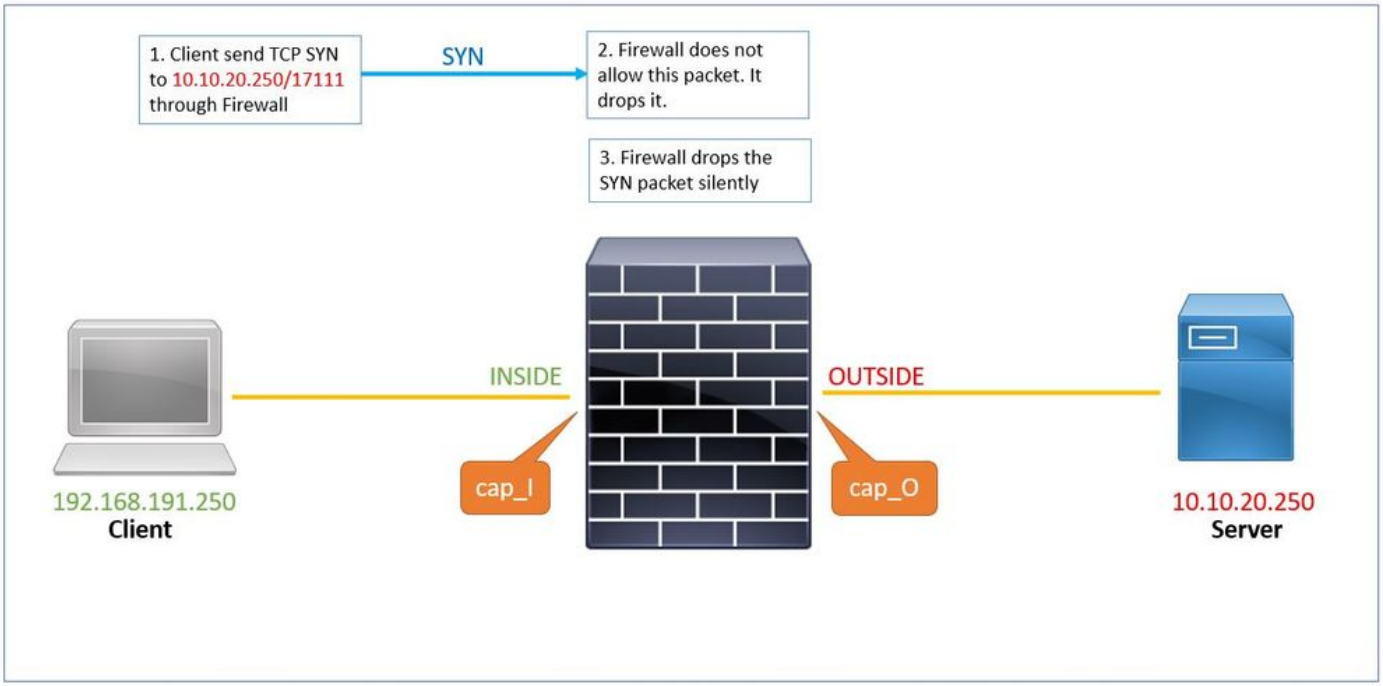
```
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. Die Firewall sendet ein RST-Paket mit der IP-Adresse des Servers als IP-Quelladresse. Paket Nr. 2 in dieser Erfassung:

```
# 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
```

Anwenderbericht 2: Service-Resetoutbound ist nicht aktiviert, Datenverkehr zwischen Client und Server wird abgelehnt.

In Fallstudie 2 gibt es keine Regel, die Datenverkehr zwischen Client und Server zulässt, und die **Rücksetzung** des ausgehenden Diensts ist deaktiviert.



Der show run service Befehl zeigt an, dass die **Rücksetzung des ausgehenden** Diensts deaktiviert ist.

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

1. Client sendet TCP über Firewall an Server 10.10.20.250/17111. Paket Nr. 1 in dieser Erfassung:

```
# 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. Da es keine ACL gibt, die diesen Datenverkehr zulässt, verwirft die sichere Firewall dieses Paket mit acl-drop gutem Grund. Dieses Paket wird im **asp-drop capture**.

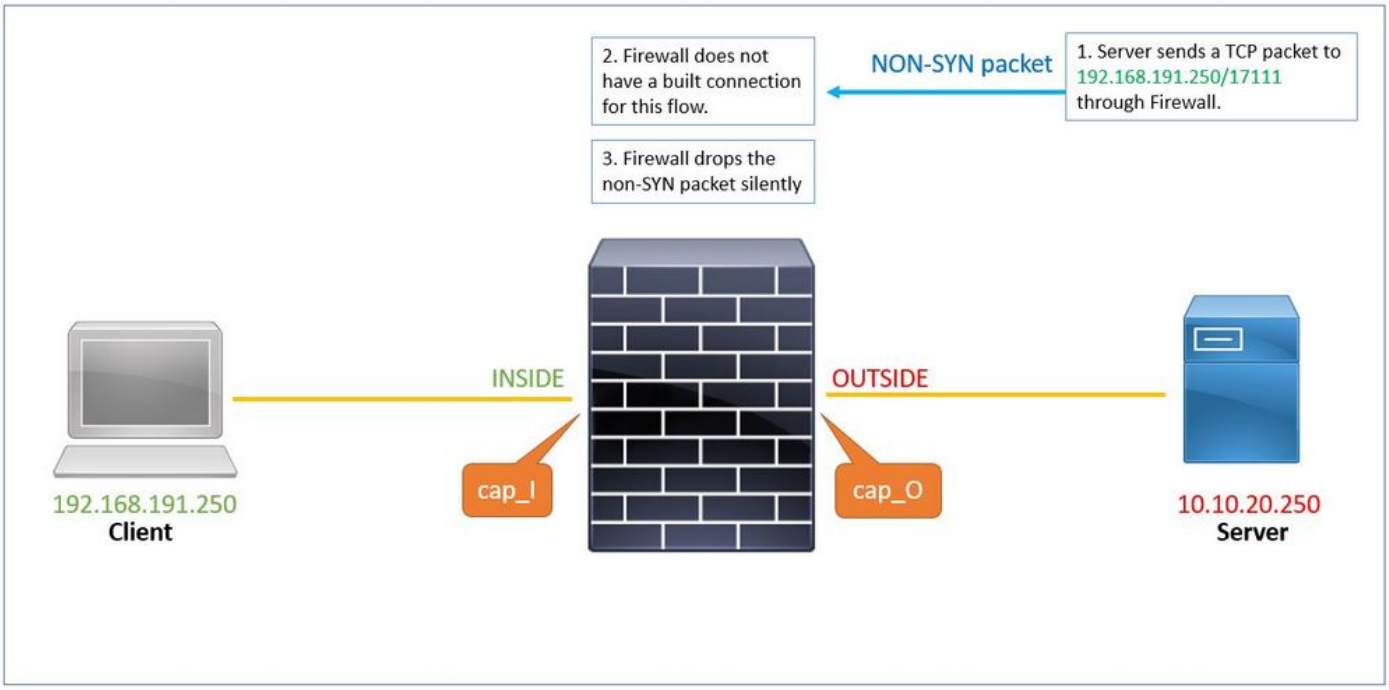
```
# show capture cap_I packet-number 1 trace det

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

3. Das **asp-drop capture** zeigt das SYN-Paket, aber es wird kein RST-Paket über die interne Schnittstelle zurückgesendetcap_I capture:

```
# 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
```

Anwenderbericht 3: Service-Resetoutbound deaktiviert (standardmäßig) Service-Resetinbound deaktiviert (standardmäßig)

Standardmäßig ist das Zurücksetzen des **ausgehenden** Diensts für alle Schnittstellen aktiviert, und das **Zurücksetzen des eingehenden Diensts** ist deaktiviert.



1. Der Server sendet ein TCP-Paket (SYN/ACK) über die Firewall an den Client. Die Firewall verfügt über keine für diesen Fluss entwickelte Verbindung.

```
# 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
```

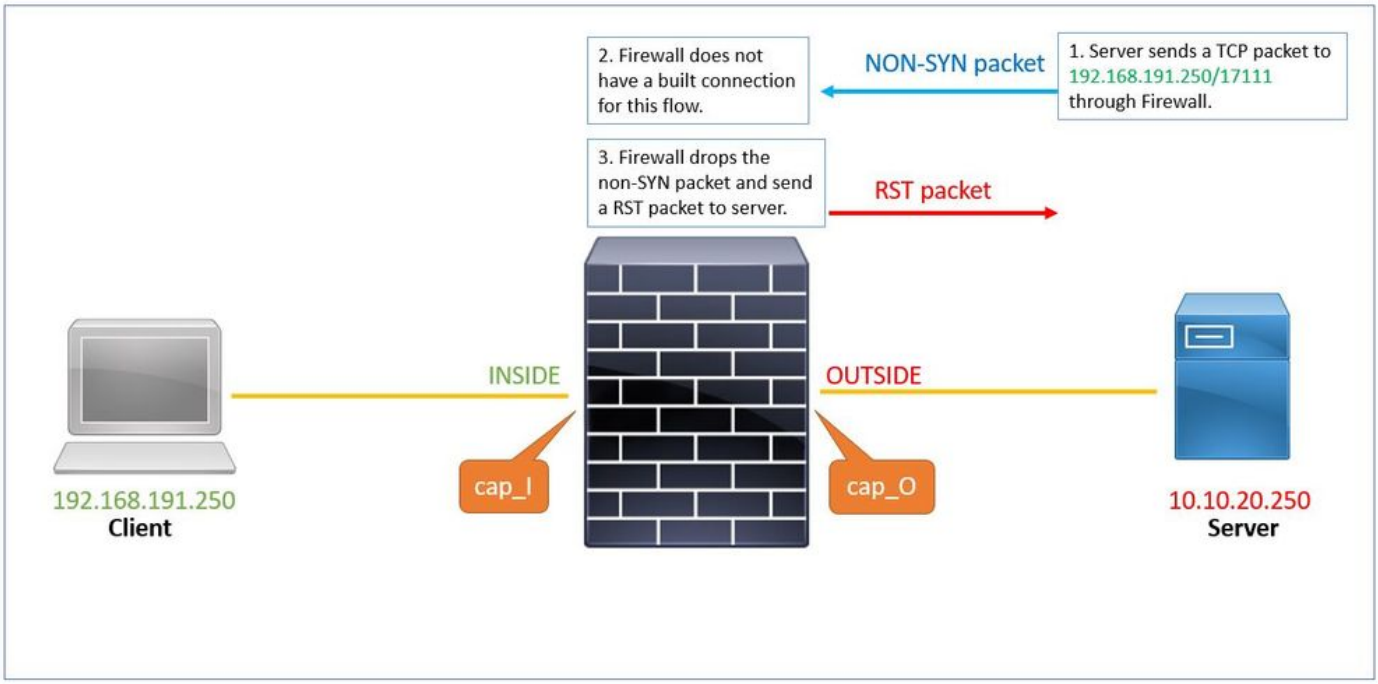
2. Das Zurücksetzen wird nicht von der Firewall an den Server gesendet. Dieses SYN/ACK-Paket wird ohne Angabe von Gründen verworfentcp-not-syn. Es wird auch in erfasst asp-drop capture.

```
# 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
```

Anwenderbericht 4: Service-Resetoutbound deaktiviert (standardmäßig) Service-Resetinbound deaktiviert

Standardmäßig ist service **resetoutbound** für alle Schnittstellen deaktiviert, service **resetinbound** wird ebenfalls mit dem Konfigurationsbefehl deaktiviert.



Die Ausgabe des show run service Befehls zeigt an, dass Service **Resetoutbound** standardmäßig deaktiviert ist und Service **Resetinbound** durch Konfigurationsbefehl deaktiviert ist.

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

1. Der Server sendet ein TCP-Paket (SYN/ACK) über die Firewall an den Client.

```
# 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. Die Firewall hat keine Verbindung für diesen Fluss und lässt ihn fallen. Das asp-drop captures Paket wird angezeigt:

```
# show capture cap_O packet-number 1 trace detail
1: OO:32:26.434395 a2c7.1eOO.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. Da der Dienst **wieder eingehend** ist, sendet die Firewall ein RST-Paket mit der Quell-IP-Adresse des Clients an den Server.

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

Zugehörige Informationen

- **Technischer Support und Downloads von Cisco**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.