Secure Firewall에서 전송하는 RST 패킷 이해

목차

소개

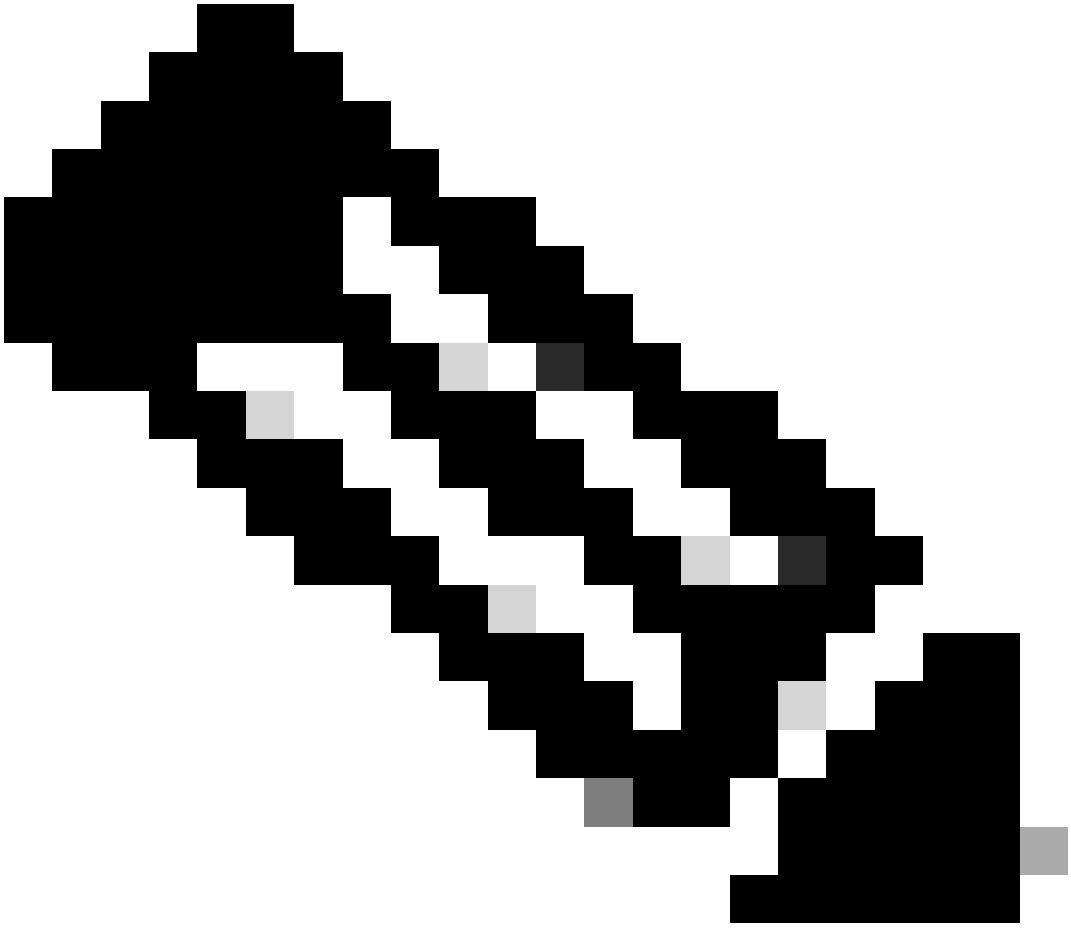
이 문서에서는 방화벽 전환을 시도하는 TCP 세션에 대해 TCP 재설정이 전송될 때의 Cisco 방화벽 동작을 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ASA 패킷 플로우
- FTD 패킷 플로우
- ASA/FTD 패킷 캡처



참고: 설명하는 동작은 ASA 및 Secure Firewall Threat Defense에 적용됩니다.

사용되는 구성 요소

이 문서의 정보는 이 소프트웨어를 기반으로 합니다.

- ASA
- Secure Firewall Threat Defense FTD

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

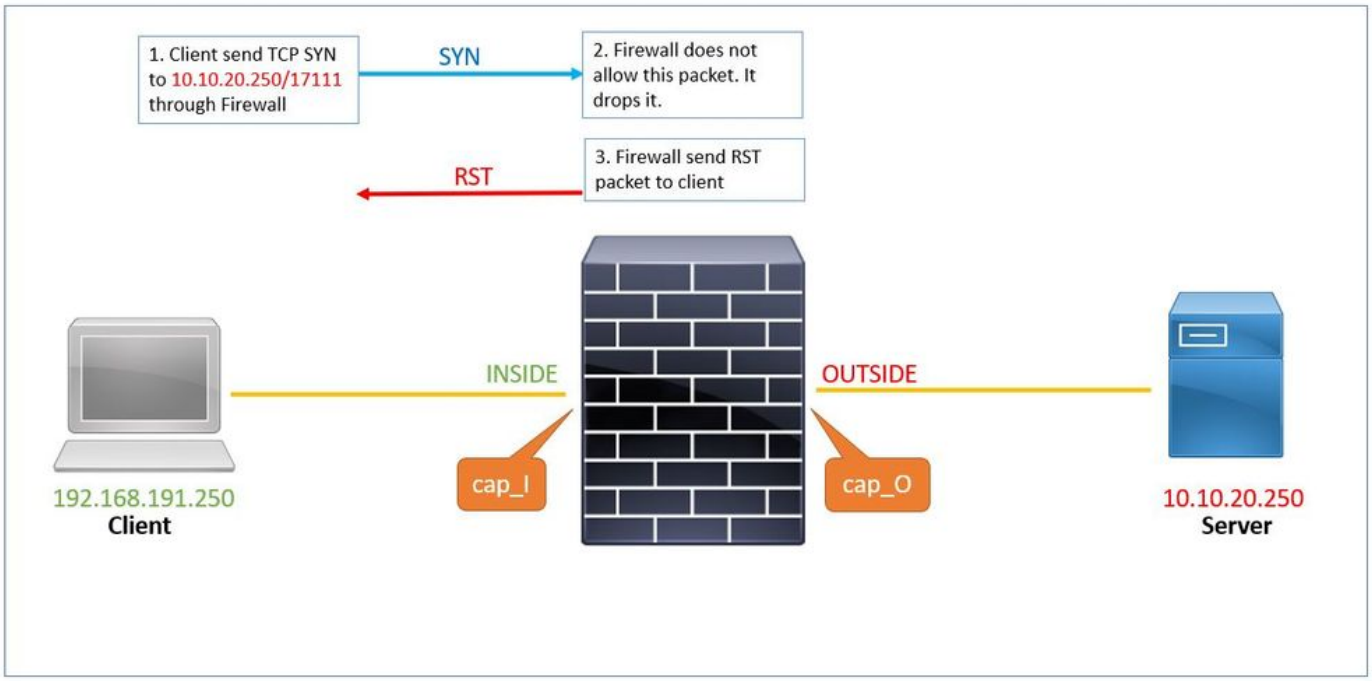
문제 해결

방화벽은 방화벽을 통과하려고 시도하고 액세스 목록을 기반으로 방화벽에 의해 거부된 TCP 세션에 대한 TCP 재설정을 전송합니다. 방화벽은 액세스 목록에서 허용하지만 방화벽에 있는 연결에

속하지 않아 스테이트풀 기능에 의해 거부된 패킷에 대한 재설정도 전송합니다.

사례 연구 1: 서비스 resetoutbound 가 활성화되고 클라이언트-서버 간 트래픽이 거부됩니다.

기본적으로 service **resetoutbound**는 모든 인터페이스에 대해 활성화됩니다. 이 고객 사례에는 클라이언트-서버 트래픽을 허용하는 규칙이 없습니다.



방화벽에 설정된 캡처:

```
# 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
```

service resetoutbound는 기본적으로 활성화됩니다. 따라서 명령의 출력에 show run service 아무 것도 표시되지 않으면 활성화되었음을 의미합니다.

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

1. 클라이언트가 방화벽을 통해 서버 10.10.20.250/17111에 TCP SYN을 전송합니다. 이 캡처의 패킷 번호 1:

```
# 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. 이 트래픽을 허용하는 ACL이 없으므로 보안 방화벽에서 이유 있는 이유로 이 패킷을 acl-drop 삭제합니다. 이 패킷은 asp-drop capture에서 캡처됩니다.

```
# 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
```

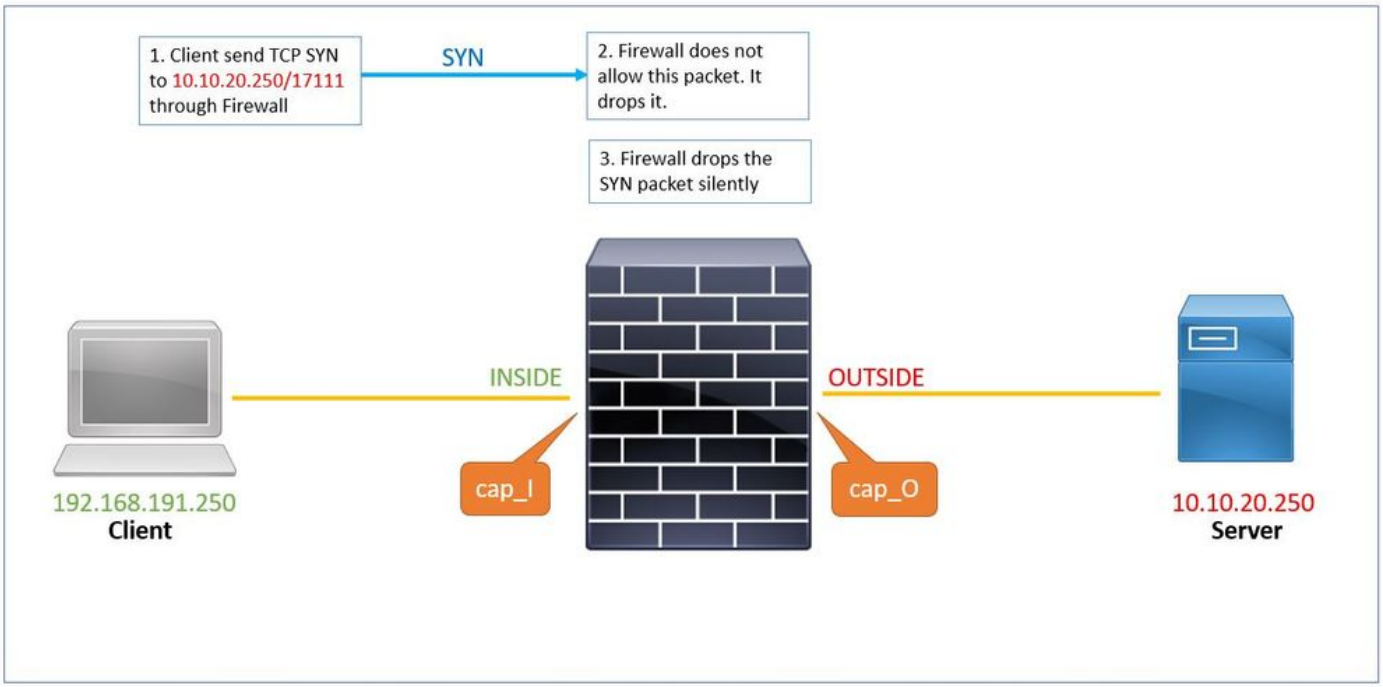
```
Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000561961c8333f flow
```

3. 방화벽은 소스 IP 주소로 서버 IP 주소를 사용하여 RST 패킷을 전송합니다. 이 캡처의 패킷 번호 2:

```
# 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
```

고객 사례 2: service resetoutbound가 활성화되지 않고 클라이언트-서버 트래픽이 거부됨

고객 사례 2에는 클라이언트-서버 트래픽을 허용하는 규칙이 없으며 service **resetoutbound**가 비활성화되어 있습니다.



이 show run service 명령은 서비스 resetoutbound가 **비활성화되었음을** 표시합니다.

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

1. 클라이언트는 방화벽을 통해 TCP TCP를 서버 10.10.20.250/17111에 전송합니다. 이 캡처의 패킷 번호 1:

```
# 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. 이 트래픽을 허용하는 ACL이 없으므로 보안 방화벽에서 이유를 붙여 이 패킷을 acl-drop 삭제합니다. 이 패킷은 **asp-drop capture**.

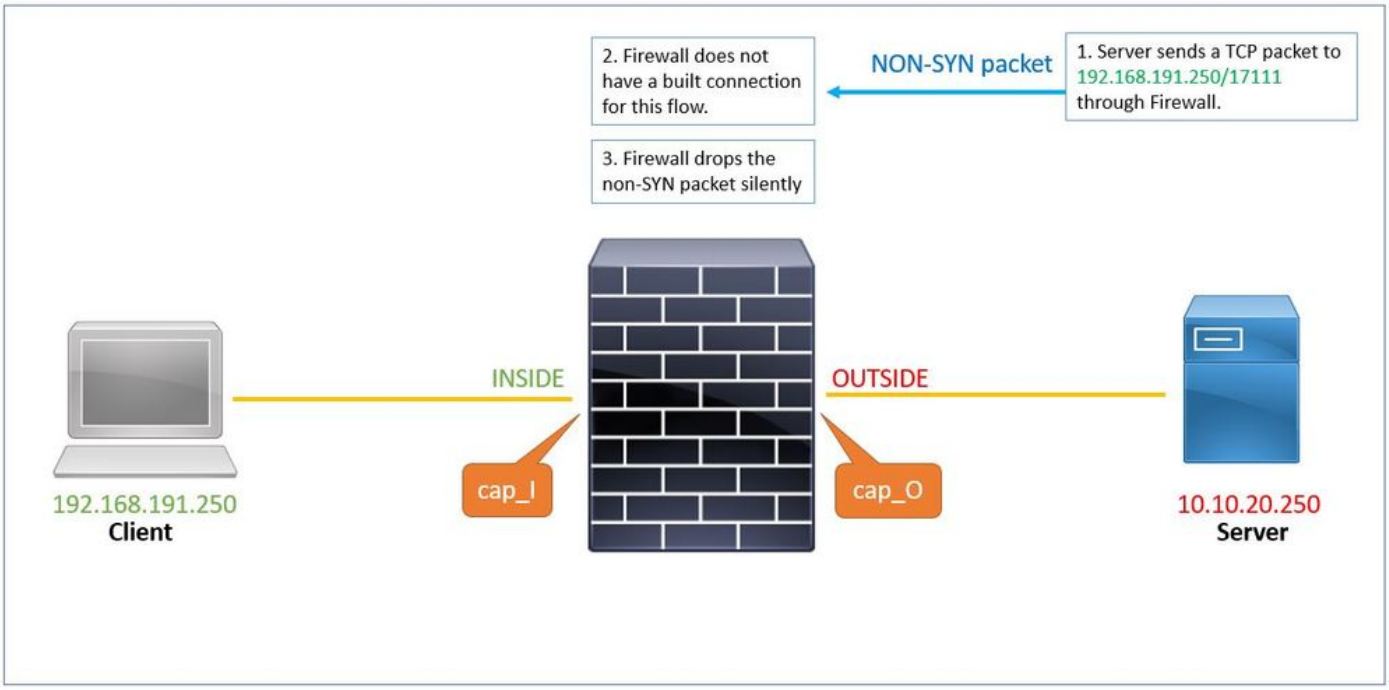
```
# show capture cap_I packet-number 1 trace det

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

3. 는 SYN 패킷을 **asp-drop capture** 표시하지만 내부 인터페이스를 통해 다시 전송된 RST 패킷이cap_I capture 없습니다.

```
# 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
```

고객 사례 3: service resetoutbound가 비활성화되고(기본적으로) service resetinbound가 비활성화됨(기본적으로)

기본적으로 service **resetoutbound**는 모든 인터페이스에 대해 활성화되고 service **resetinbound**는 비활성화됩니다.



1. 서버에서 방화벽을 통해 클라이언트에 TCP 패킷(SYN/ACK)을 전송합니다. 방화벽에는 이 플로우에 대해 구축된 연결이 없습니다
.

```
# 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
```

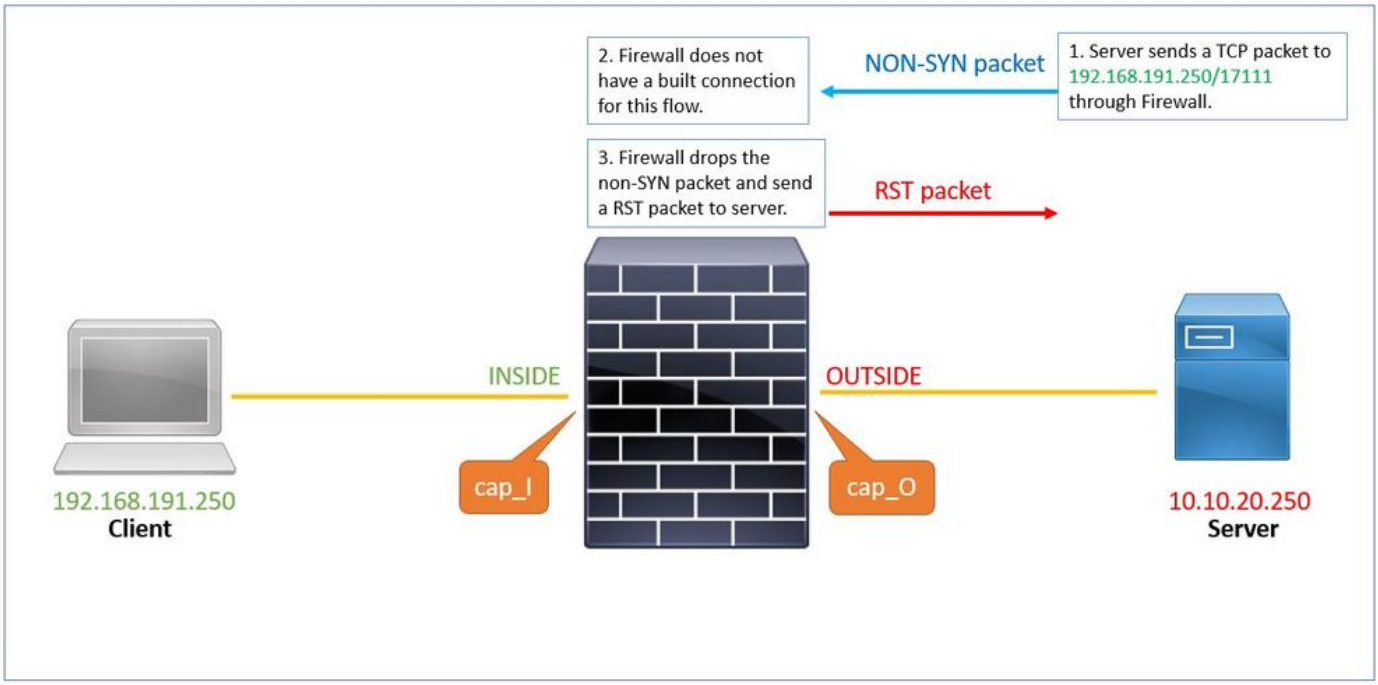
2. 재설정은 방화벽에서 서버로 전송되지 않습니다. 이 SYN/ACK 패킷은 이유 때문에 자동으로 tcp-not-syn 삭제됩니다. 또한 asp-drop capture 캡처됩니다.

```
# 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
```

고객 사례 4: service resetoutbound가 비활성화되고(기본적으로) service resetinbound가 비활성화됨

기본적으로 service **resetoutbound**는 모든 인터페이스에 대해 비활성화되고 service **resetinbound**는 다음 설정 명령으로 비활성화됩니다.



이 명령의 show run service 출력에는 service resetoutbound가 **기본적**으로 비활성화되어 있고 service resetinbound가 컨피그레이션 **명령**에 의해 비활성화되어 있음을 표시합니다.

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

1. 서버에서 방화벽을 통해 클라이언트에 TCP 패킷(SYN/ACK)을 전송합니다.

```
# 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.방화벽에는 이 플로우에 대해 구축된 연결이 없으며 이를 삭제합니다. 는 asp-drop captures 패킷을 표시합니다.

```
# show capture cap_O packet-number 1 trace detail
1: OO:32:26.434395 a2c7.1eOO.003e OO50.56b3.1ef5 OxO8OO 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. service **resetinbound** 이후 방화벽은 클라이언트의 소스 IP 주소와 함께 서버로 RST 패킷을 전송합니다.

```
# 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
```

관련 정보

- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.