Understand RST Packets Sent by Secure Firewall

Contents

Introduction

This document describes the behavior of a Cisco Firewall when TCP resets are sent for TCP sessions that attempt to transit the Firewall.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- ASA packet flow
- FTD packet flow
- ASA/FTD packet captures

Note: This described behavior applies for ASA and Secure Firewall Threat Defense.

Components Used

The information in this document is based on this software:

- ASA
- Secure Firewall Threat Defense FTD

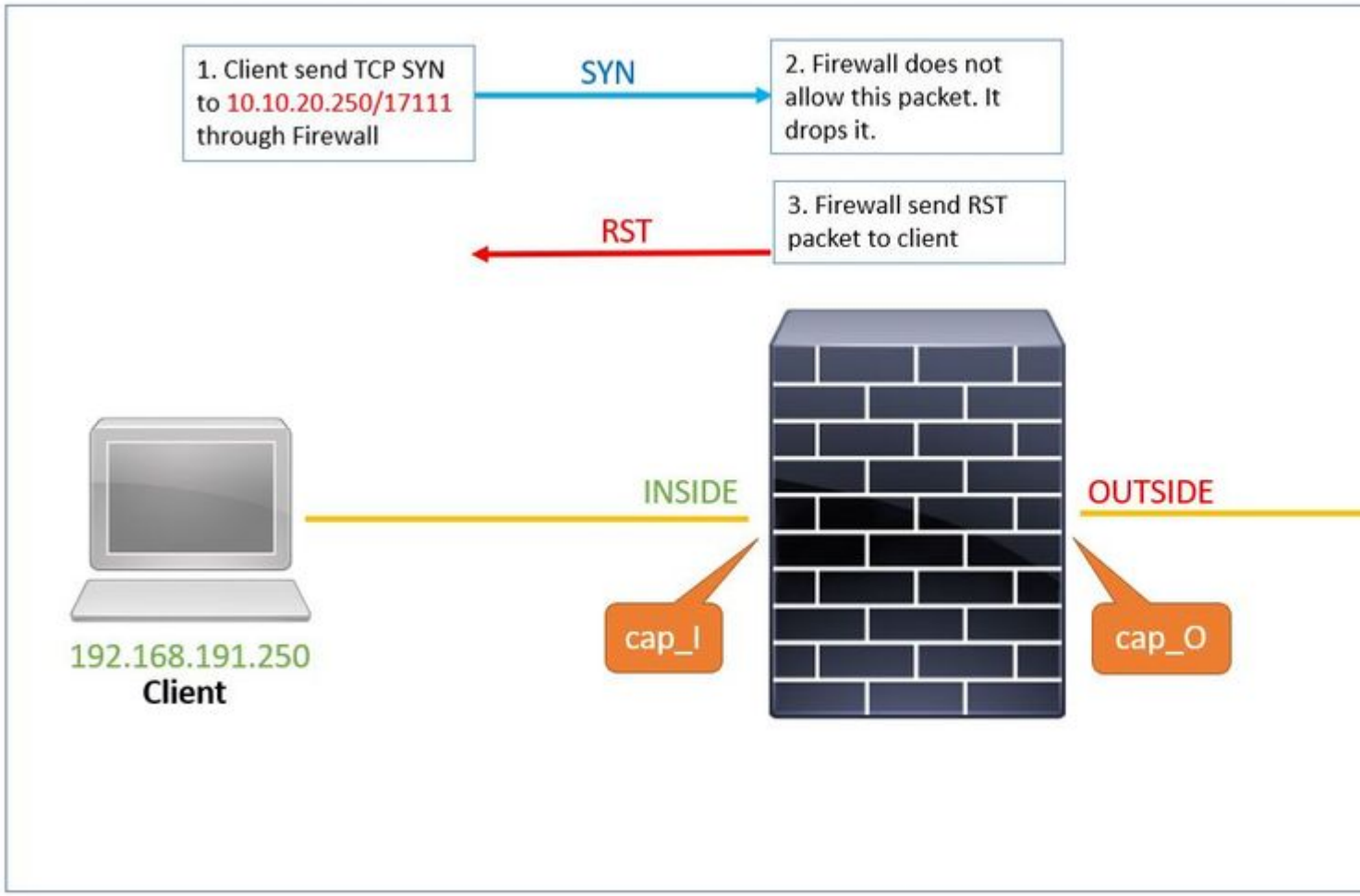
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Troubleshoot

The Firewall sends TCP resets for TCP sessions that attempt to transit the Firewall and are denied by the Firewall based on access lists. The Firewall also sends resets for packets that are allowed by an access list, but do not belong to a connection that exists in the firewall and therefore is denied by the stateful feature.

Case Study 1: Service resetoutbound is enabled and traffic client-to-server is denied.

By default, service **resetoutbound** is enabled for all interfaces. In this case study, there is no rule to allow client-to-server traffic.



These are the captures configured in the Firewall:

```
# 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 resetoutbound is enabled by default. Therefore, if the output of the show run service command displays nothing, that means it is enabled:

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

1. Client sends TCP SYN to server 10.10.20.250/17111 through Firewall. Packet number 1 in this capture:

```
# 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
```

2. Since there is no ACL to allow this traffic, the Secure Firewall drops this packet with acl-drop reason. This packet is captured in the asp-drop capture.

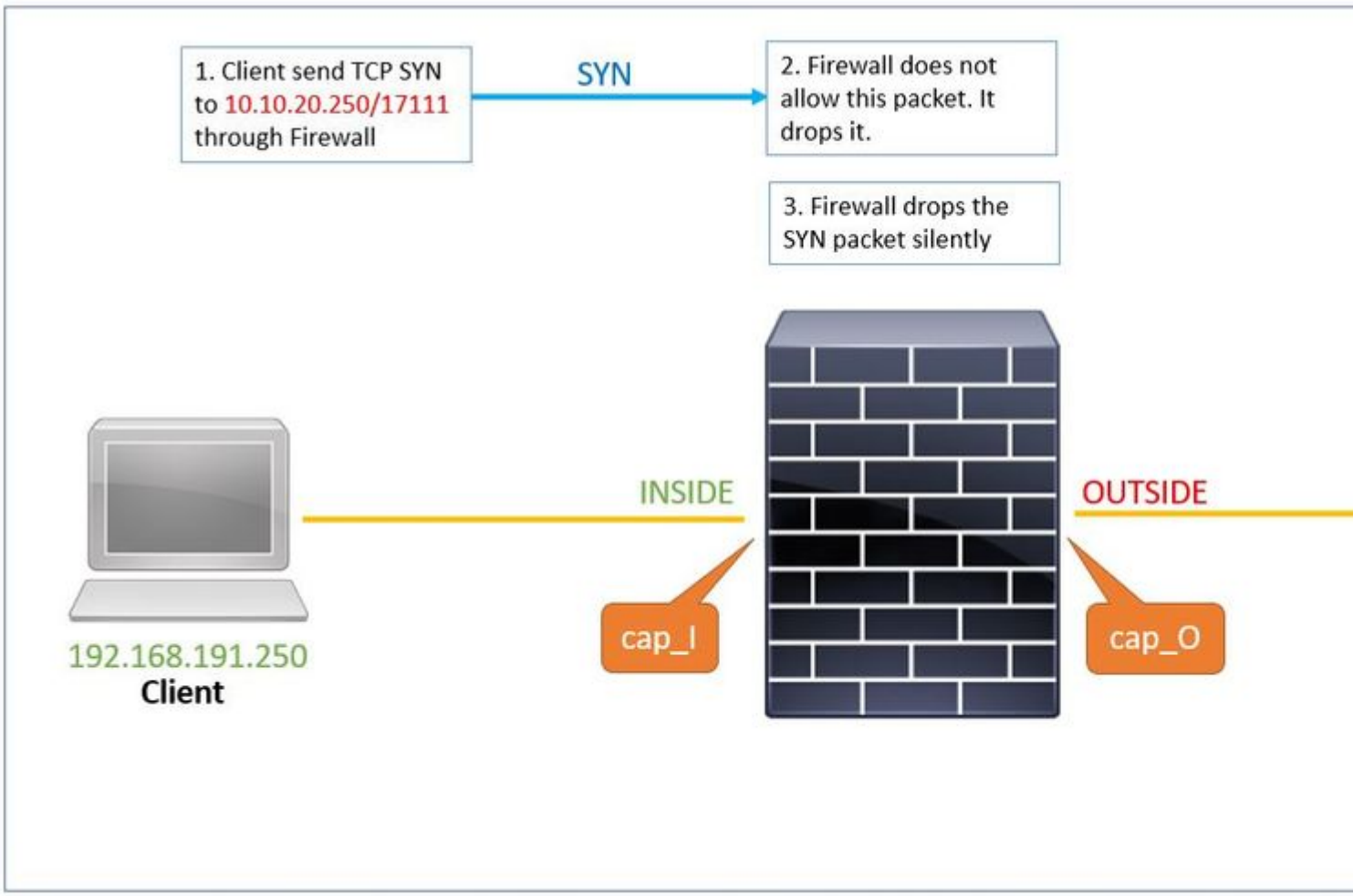
```
# show capture cap_I packet-number 1 trace det

1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74
192.168.191.250.46118 > 10.10.20.250.17111: 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. The firewall sends a RST packet with the server ip address as the source ip address. Packet number 2 in this capture:

```
# 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
        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
```

Case Study 2: Service resetoutbound not enabled and traffic client-to-server is denied.

In Case Study 2, there is no rule to allow client-to-server traffic and the service **resetoutbound** is disabled.



The show run service command displays that service **resetoutbound** is disabled.

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

1. Client sends TCP TCP to server 10.10.20.250/17111 through Firewall. Packet number 1 in this capture:

```
# 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. Since there is no ACL to allow this traffic, the Secure Firewall drops this packet with acl-drop reason. This packet is captured in the **asp-drop capture**.

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

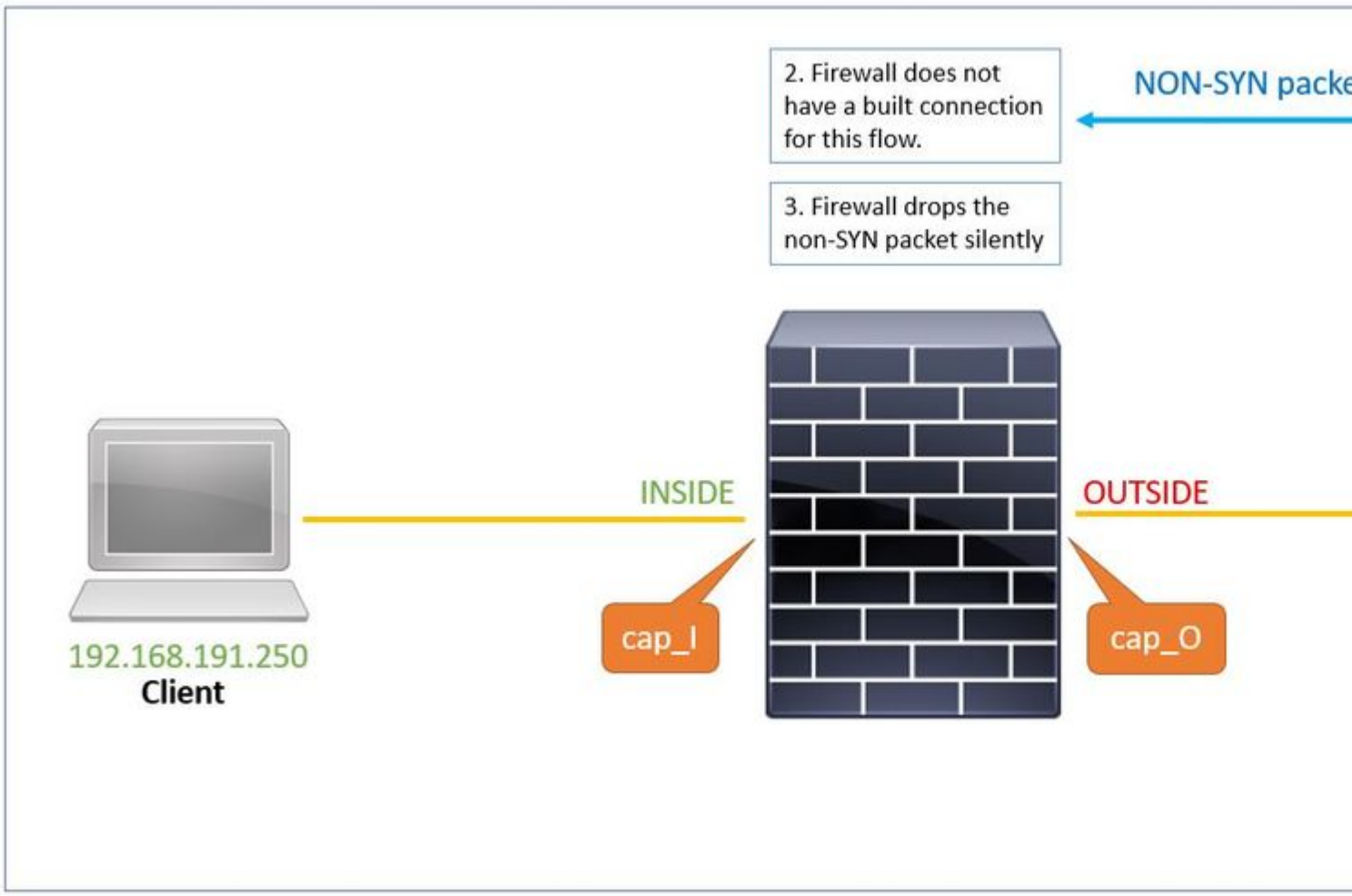
```
1: 19:48:55.512500 a2c7.1e00.0004 0050.56b3.05b1 0x0800 Length: 74 192.168.191.250.46118 > 10.10.20.250.
```

3. The **asp-drop capture** shows the SYN packet but there is no RST packet sent back in cap_I capture via inside interface:

```
# 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 <mss

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

Case Study 3: Service resetoutbound disabled (by default) service resetinbound disabled (by default)

By default, service **resetoutbound** is enabled for all interfaces and service **resetinbound** is disabled.



1. The server sends a TCP packet (SYN/ACK) to the client through the firewall. The firewall does not have a built connection for this flow.

```
# 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
```

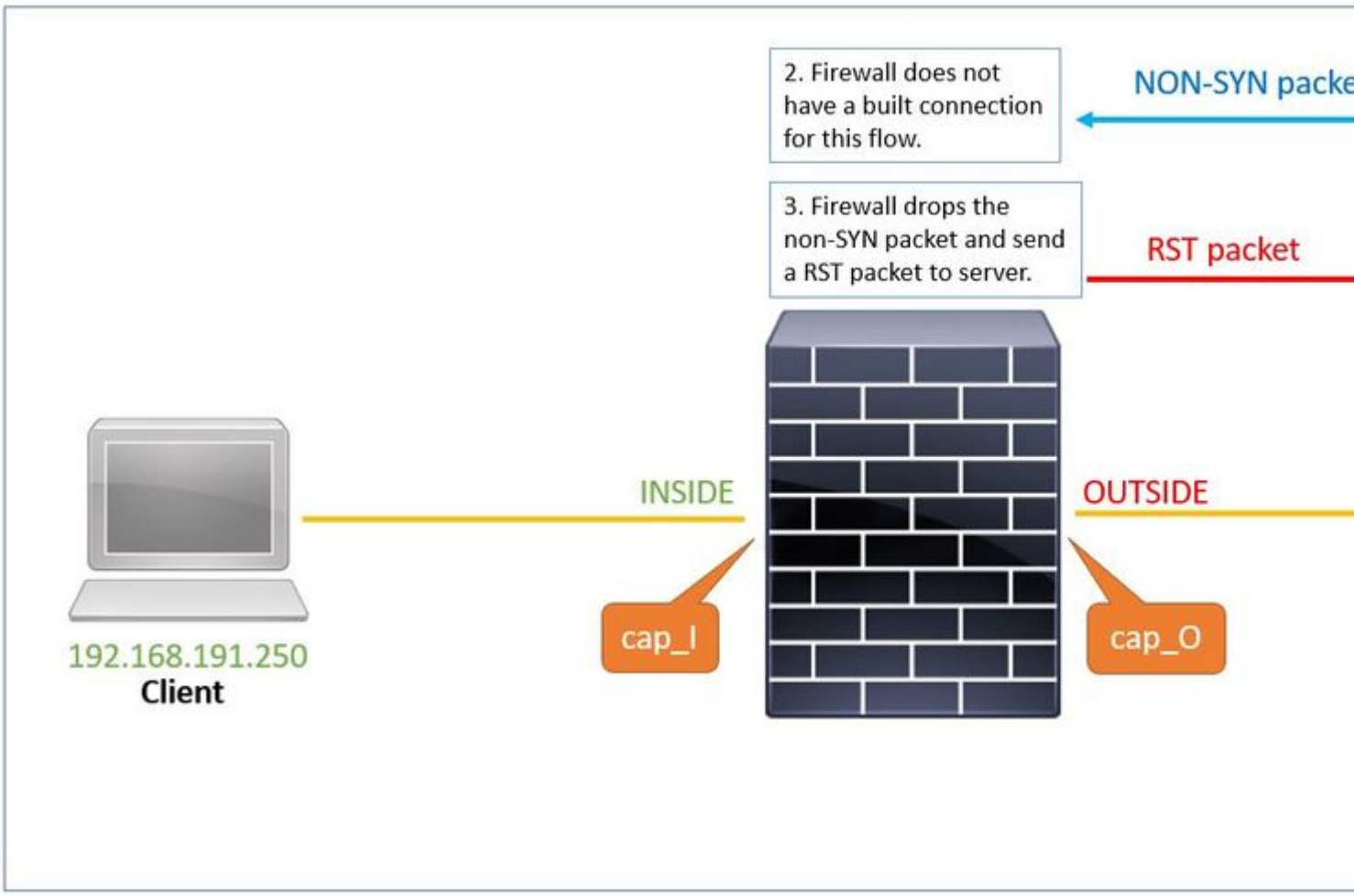
2. Reset is not sent from Firewall to server. This SYN/ACK packet is dropped silently with reason tcp-not-syn. It is captured in asp-drop capture as well.

```
# 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 4
   (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)/N
</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
```

Case Study 4: Service resetoutbound disabled (by default) service resetinbound disabled.

By default, service **resetoutbound** is disabled for all interfaces and service **resetinbound** is disabled also with configuration command.



The output of the show run service command displays that service **resetoutbound** is disabled (by default) and service **resetinbound** is disabled by configuration command.

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

1. The server sends a TCP packet (SYN/ACK) to the client through the firewall.

```
# 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. The firewall does not have a built connection for this flow and drops it. The asp-drop captures shows the packet:

```
# 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 4
   (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)/N
```

3. Since service **resetinbound**, the firewall sends a RST packet to the Server with the source ip address of the client.

```
# 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
```

Related Information

- **Cisco Technical Support & Downloads**