了解 Secure Firewall 发送的 RST 数据包

目录

简介

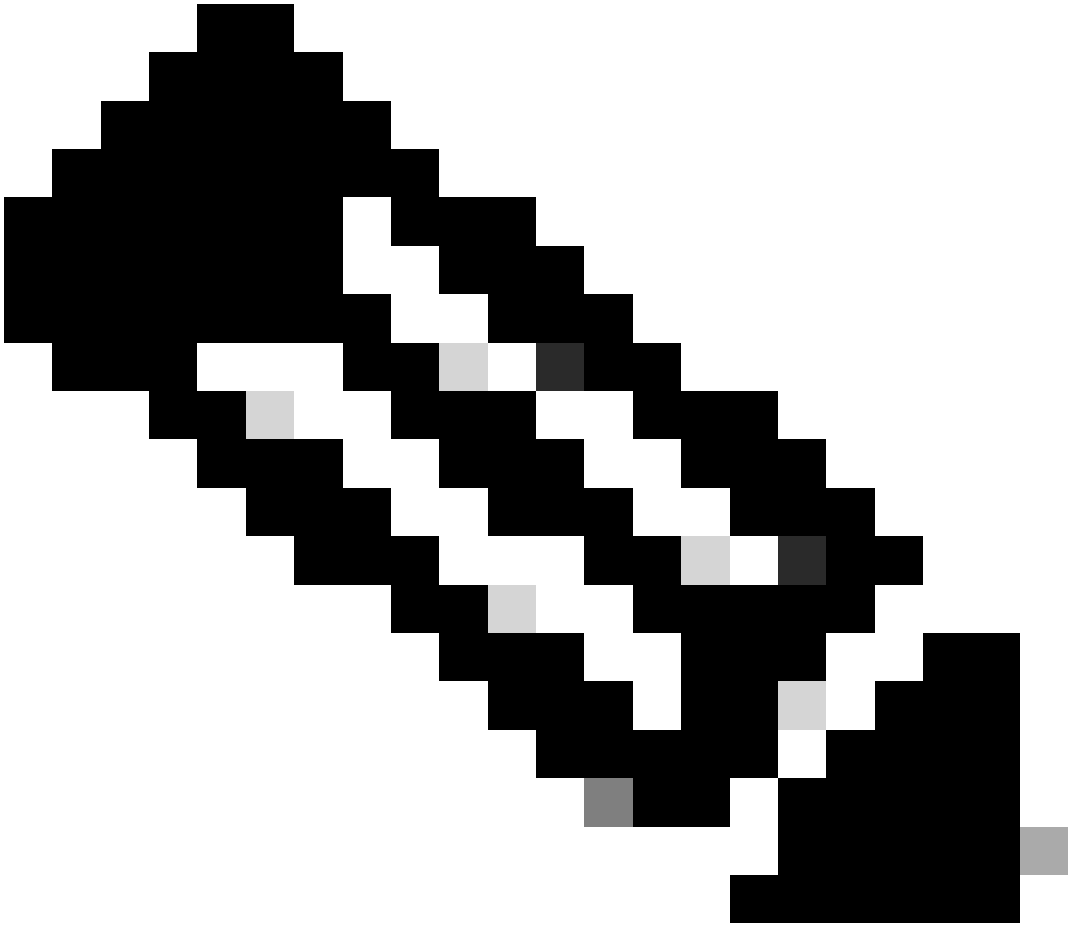
本文档介绍在针对尝试穿过防火墙的 TCP 会话发送 TCP 重置时思科防火墙的行为。

先决条件

要求

Cisco 建议您了解以下主题：

- ASA数据包流
- FTD数据包流
- ASA/FTD数据包捕获



注意：上述行为适用于ASA和安全防火墙威胁防御。

使用的组件

本文档中的信息基于以下软件：

- ASA
- 安全防火墙威胁防御FTD

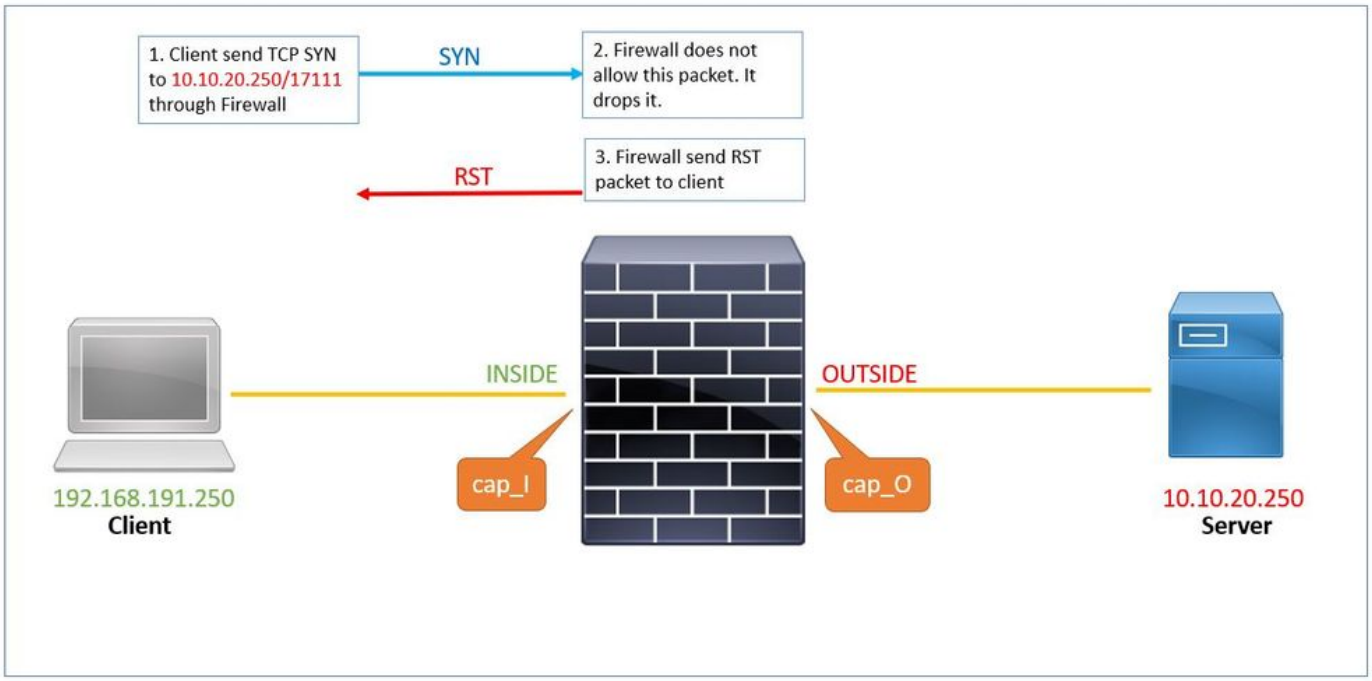
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

故障排除

对于尝试通过防火墙并被防火墙根据访问列表拒绝的TCP会话，防火墙会发送TCP重置。防火墙还会对访问列表允许但不属于防火墙中存在且因此被状态功能拒绝的连接的数据包发送重置。

案例研究1：服务 resetoutbound 已启用，客户端到服务器的流量被拒绝。

默认情况下，对所有接口启用服务**resetoutbound**。在此案例分析中，没有允许客户端到服务器流量的规则。



以下是在防火墙中配置的捕获：

```
# 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
```

默认情况下，Service resetoutbound处于启用状态。因此，如果show run service 命令的输出未显示任何内容，则意味着该命令处于启用状态：

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

1. 客户端通过防火墙将TCP SYN发送到服务器10.10.20.250/17111。此捕获中的1号数据包：

```
# 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. 由于没有允许此流量的ACL，安全防火墙基于acl-drop原因丢弃此数据包。此数据包在asp-drop捕获中捕获。

```
# 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
```

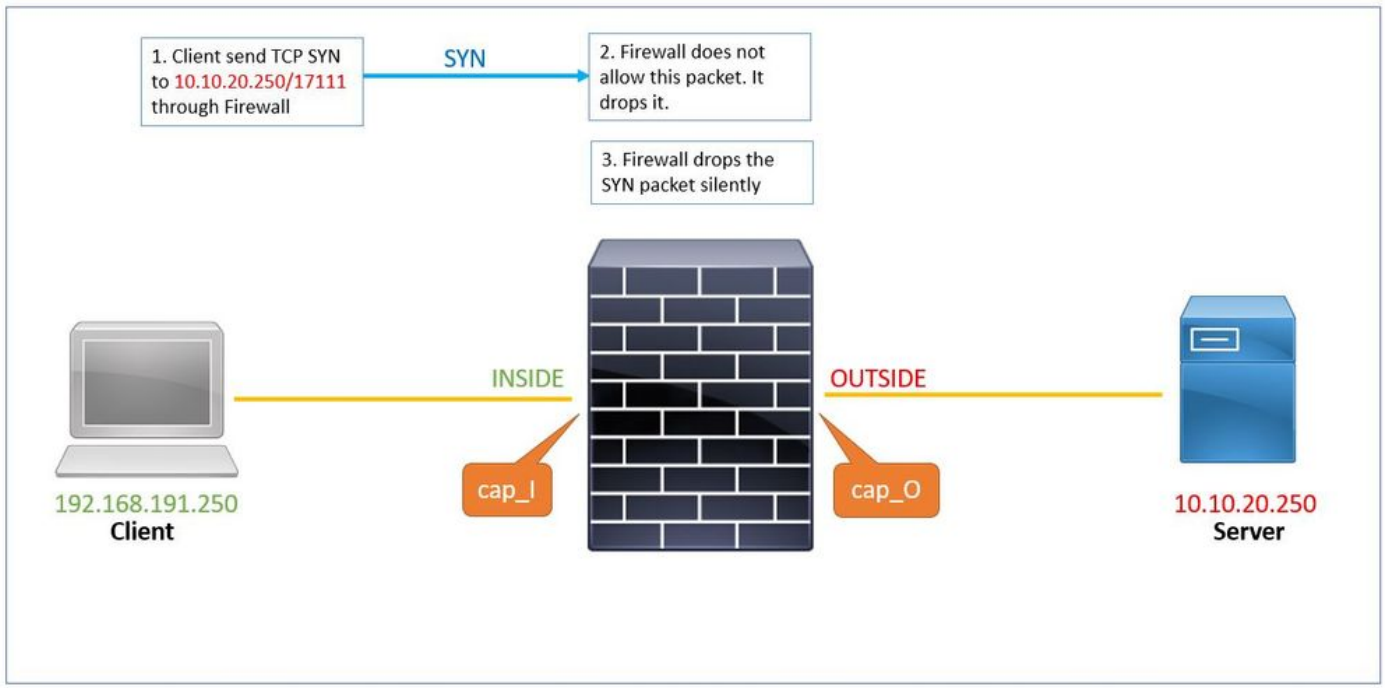
3. 防火墙发送RST数据包，其中服务器ip地址作为源ip地址。此捕获中的2号数据包：

```
# 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
```

案例分析2：服务resetoutbound未启用，客户端到服务器的流量被拒绝。

在案例分析2中，没有允许客户端到服务器流量的规则，并且服务**resetoutbound**处于禁用状态。

show run service



命令显示service **resetoutbound**已禁用。

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

1. 客户端通过防火墙将TCP TCP发送到服务器10.10.20.250/17111。此捕获中的1号数据包：

```
# 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. 由于没有允许此流量的ACL，安全防火墙因为acl-drop丢弃此数据包。此数据包捕获在 **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
```

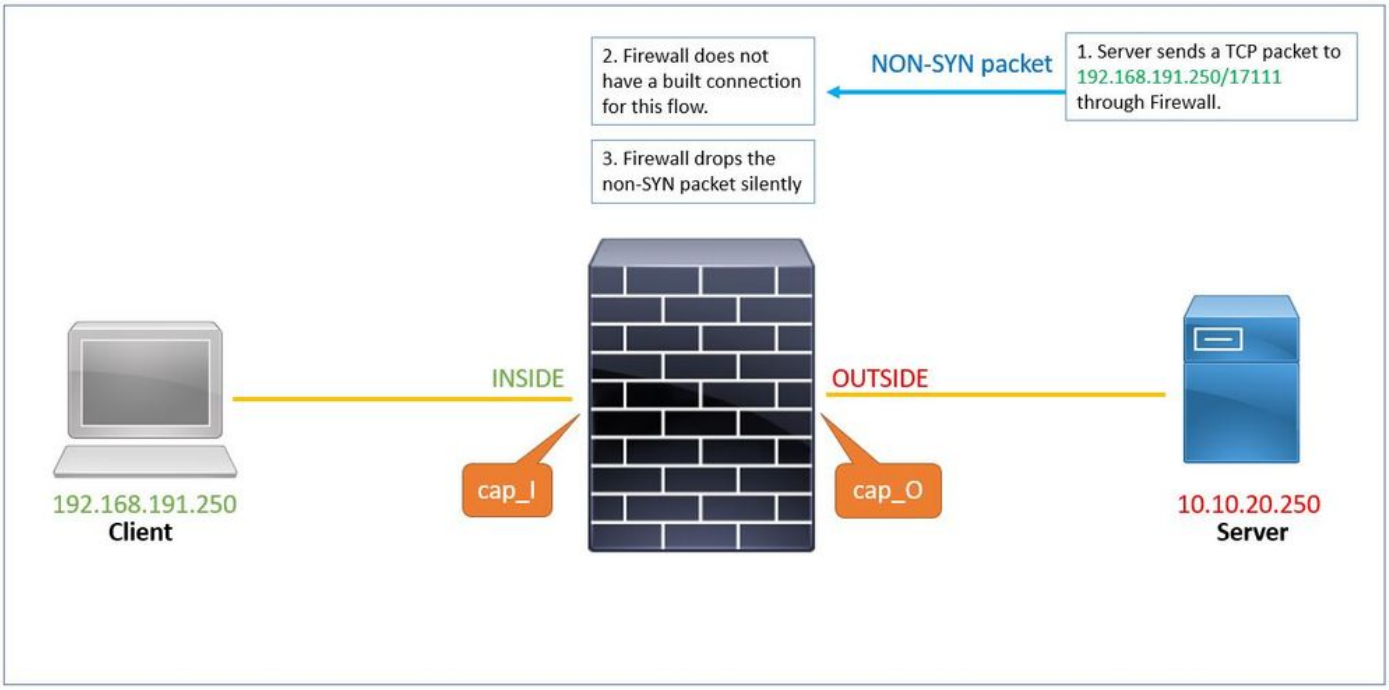
3.**asp-drop capture** 显示SYN数据包，但是没有通过内部接口在cap_I capture中发送回的RST数据包：

```
# 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
```

案例分析3：服务resetoutbound disabled（默认）服务resetinbound disabled（默认）

默认情况下，对所有接口启用**service resetoutbound**，并禁用服务**resetinbound**。



1. 服务器通过防火墙向客户端发送TCP数据包(SYN/ACK)。防火墙没有用于此流量的内置连接。

```
# 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. 重置不是从防火墙发送到服务器。此SYN/ACK数据包被无提示丢弃，原因为tcp-not-syn。 asp-drop capture也会捕获它。

```
# 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
```

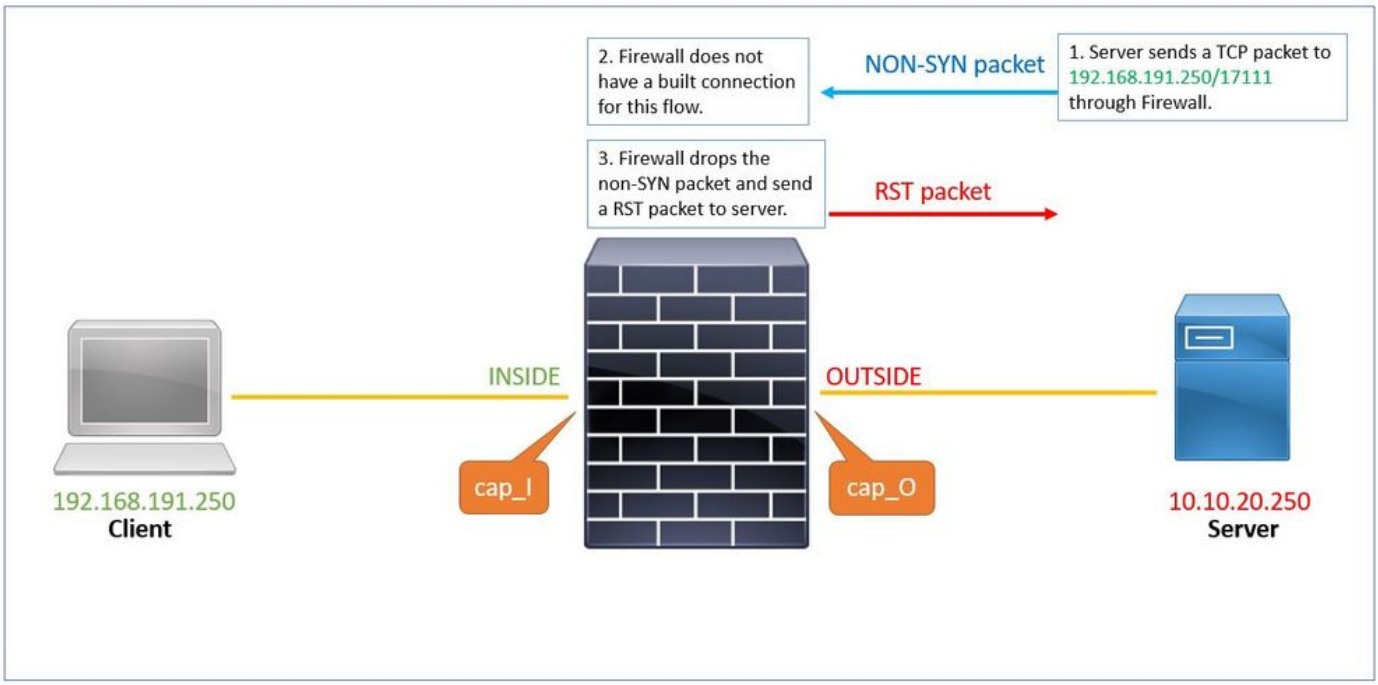
```
# show capture asp
```

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

案例研究4：服务resetoutbound disabled（默认）服务resetinbound disabled。

默认情况下，所有接口的服务**resetoutbound**都处于禁用状态，同时使用配置命令也禁用了服务**resetinbound**。

show run service



命令输出显示，配置命令已禁用service **resetoutbound**（默认）和service **resetinbound**。

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

1. 服务器通过防火墙向客户端发送TCP数据包(SYN/ACK)。

```
# 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. 防火墙没有用于此流的已建立连接，因此会将其丢弃。asp-drop captures显示数据包：

```
# show capture cap_O packet-number 1 trace detail
1: OO:32:26.434395 a2c7.1eOO.OO3e OO5O.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 0xOOOO561961c89aaa flow (NA)/
```

3. 自服务**resetinbound**之后，防火墙将向服务器发送一个RST数据包，其中含有客户端的源IP地址。

```
# 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
```

相关信息

- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。