瞭解安全防火牆傳送的 RST 封包

目錄

[簡介](#)

[必要條件](#)

- [需求](#)
- [採用元件](#)

[疑難排解](#)

- [案例分析1：啟用Service resetoutbound並拒絕trafficclient到server。](#)
- [案例分析2：未啟用Service resetoutbound，流量客戶端到伺服器被拒絕。](#)
- [案例分析3：服務重置出站停用（預設）服務重置入站停用（預設）](#)
- [案例分析4：Serviceresetoutbound disabled（預設）服務resetinbound disabled。](#)

[相關資訊](#)

簡介

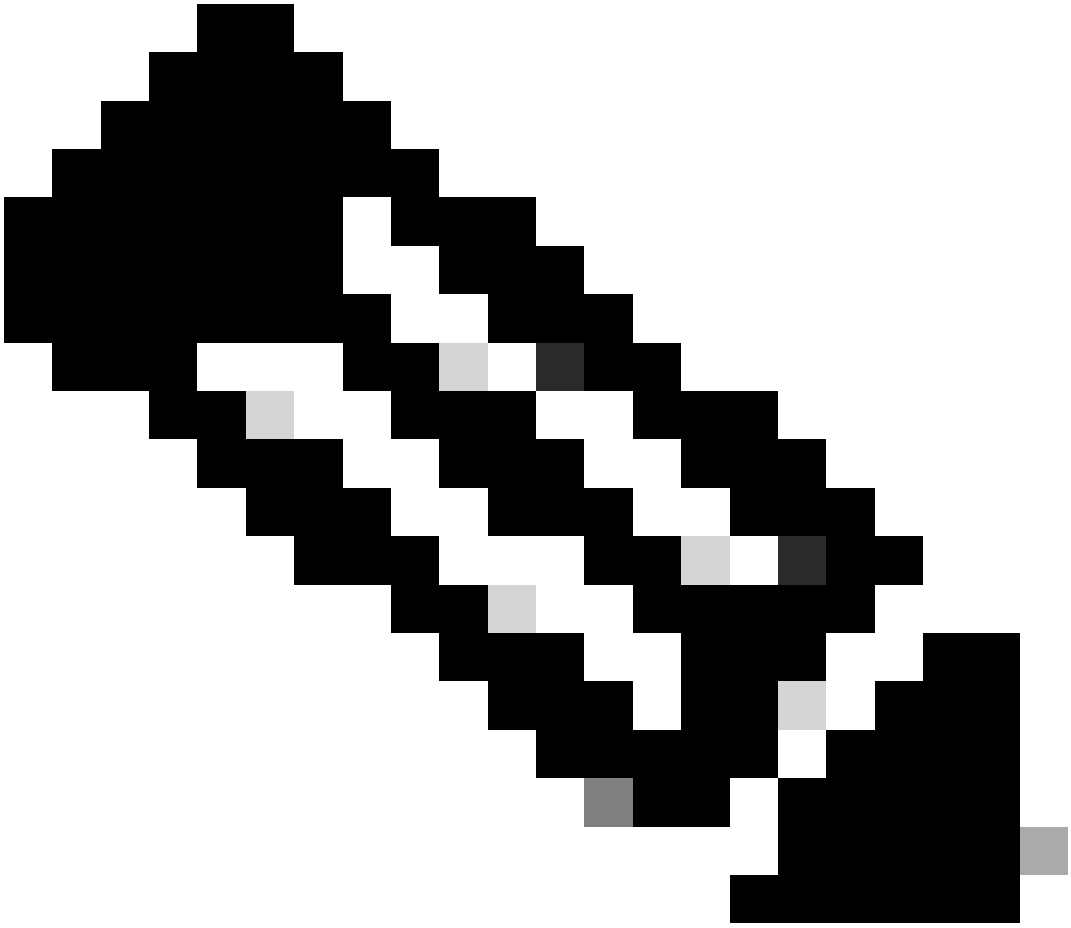
本文說明嘗試繞過防火牆的 TCP 工作階段傳送 TCP 重設時，思科防火牆會產生什麼行為。

必要條件

需求

思科建議您瞭解以下主題：

- ASA資料包流
- FTD封包流量
- ASA/FTD封包擷取



注意：描述的行為適用於ASA和安全防火牆威脅防禦。

採用元件

本檔案中的資訊是根據以下軟體：

- ASA
- 安全防火牆威脅防禦FTD

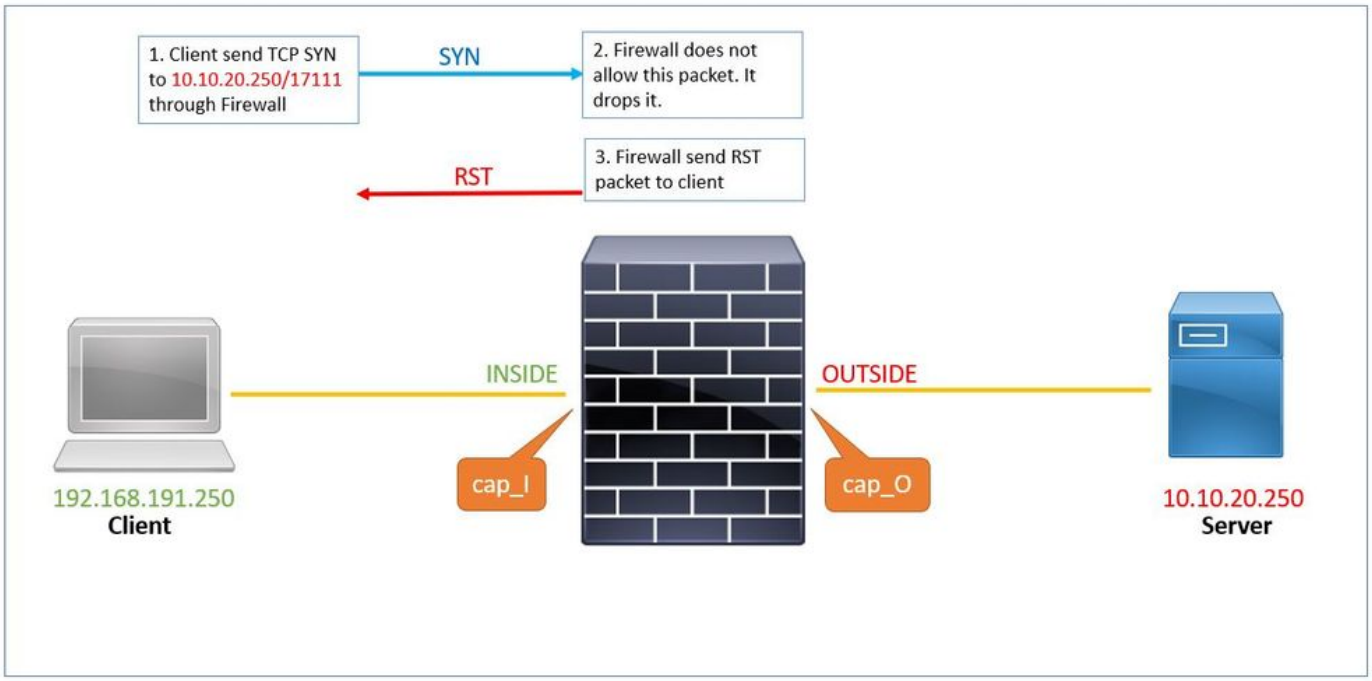
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

疑難排解

如果嘗試傳輸防火牆的TCP會話被防火牆根據訪問清單拒絕，防火牆將傳送TCP重置。防火牆還會對訪問清單允許的資料包傳送重置，這些資料包不屬於防火牆中存在的連線，因此被有狀態功能拒絕。

案例分析1：服務 resetoutbound 已啟用，客戶端到伺服器的流量被拒絕。

預設情況下，所有介面都啟用服務**resetoutbound**。在此案例分析中，沒有允許客戶端到伺服器流量的規則。



以下是防火牆中設定的擷取：

```
# 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
```

預設情況下，服務重置出站處於啟用狀態。因此，如果show run service 命令的輸出未顯示任何內容，則意味著該命令已啟用：

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

1. 客戶端透過防火牆將TCP SYN傳送到伺服器10.10.20.250/17111。此擷取中的封包編號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. 由於沒有允許此流量的ACL，安全防火牆基於acl-drop原因丟棄此資料包。此封包在asp-drop擷取中擷取。

```
# 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
```

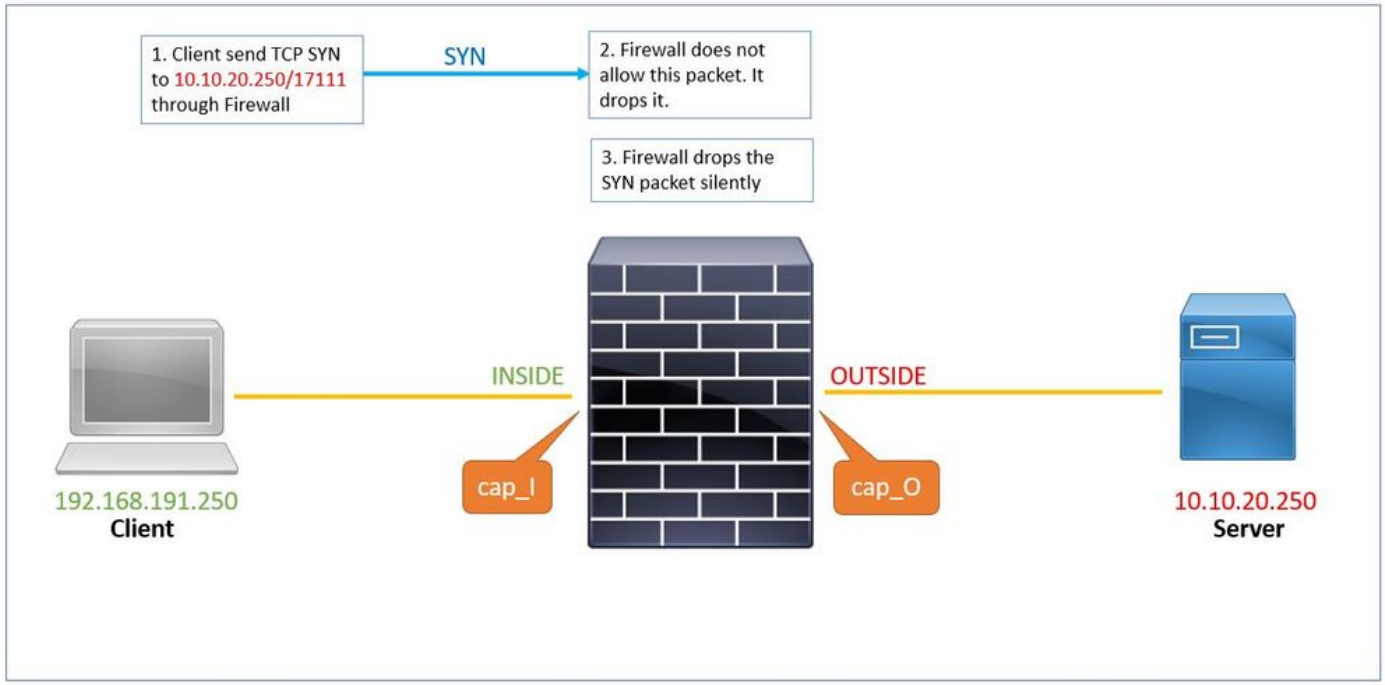
3. 防火牆會傳送一個RST封包，其中包含作為來源IP位址的伺服器IP位址。此擷取中的封包編號2：

```
# 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
```

案例分析2：服務resetoutbound未啟用，客戶端到伺服器的流量被拒絕。

在案例分析2中，沒有允許客戶端到伺服器資料流的規則，並且已停用服務**resetoutbound**。

show run service



命令顯示服務**resetoutbound**已停用。

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

1. 客戶端透過防火牆將TCP TCP傳送到伺服器10.10.20.250/17111。此擷取中的封包編號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. 由於沒有允許此流量的ACL，安全防火牆基於理由丟棄此資料包acl-drop。此封包擷取自 **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
```

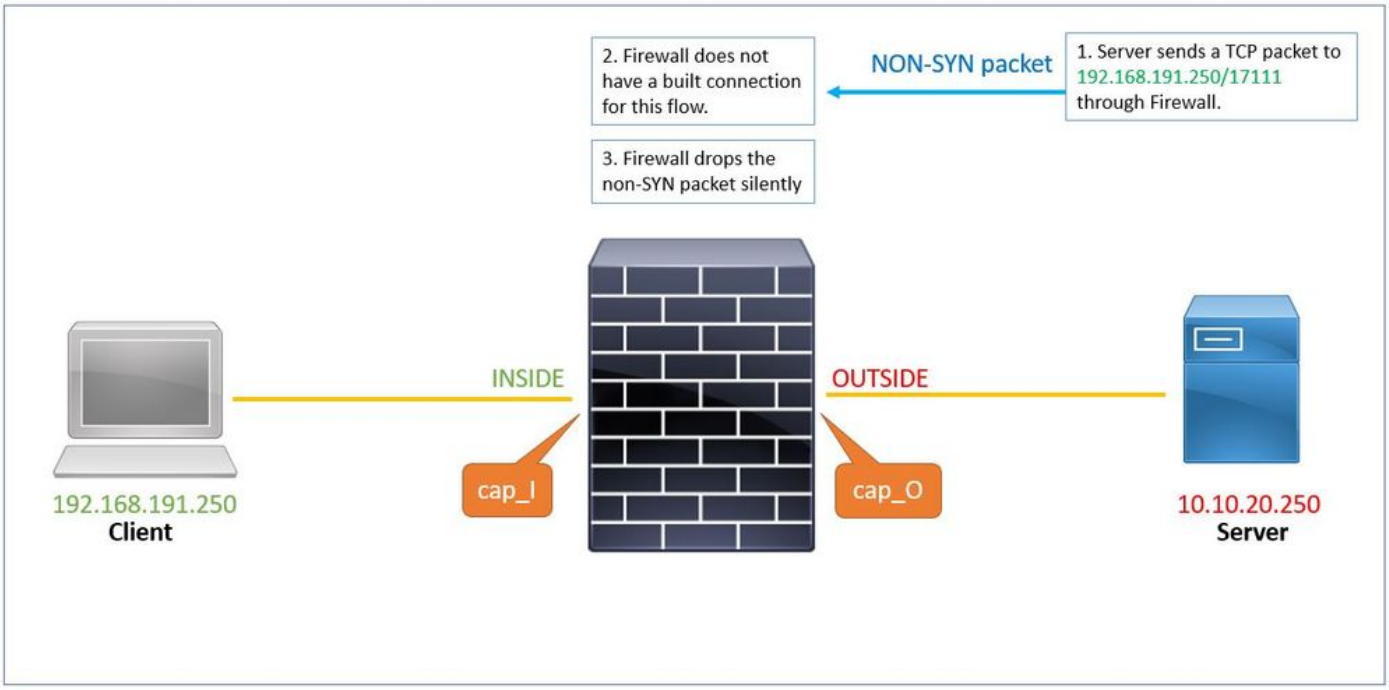
3. **asp-drop capture** 顯示SYN資料包，但沒有透過內部介面在cap_I capture中傳送回RST資料包：

```
# 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：服務重置出站停用（預設）服務resetinbound disabled（預設）

預設情況下，所有介面都啟用服務**resetoutbound**，並停用服務**resetinbound**。



1. 伺服器透過防火牆向客戶端傳送TCP資料包(SYN/ACK)。防火牆沒有為此流建立的連線。

```
# 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. 重設不會從防火牆傳送到伺服器。由於tcp-not-syn原因，此SYN/ACK資料包被靜默丟棄。它也在 asp-drop capture中捕獲。

```
# 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
```

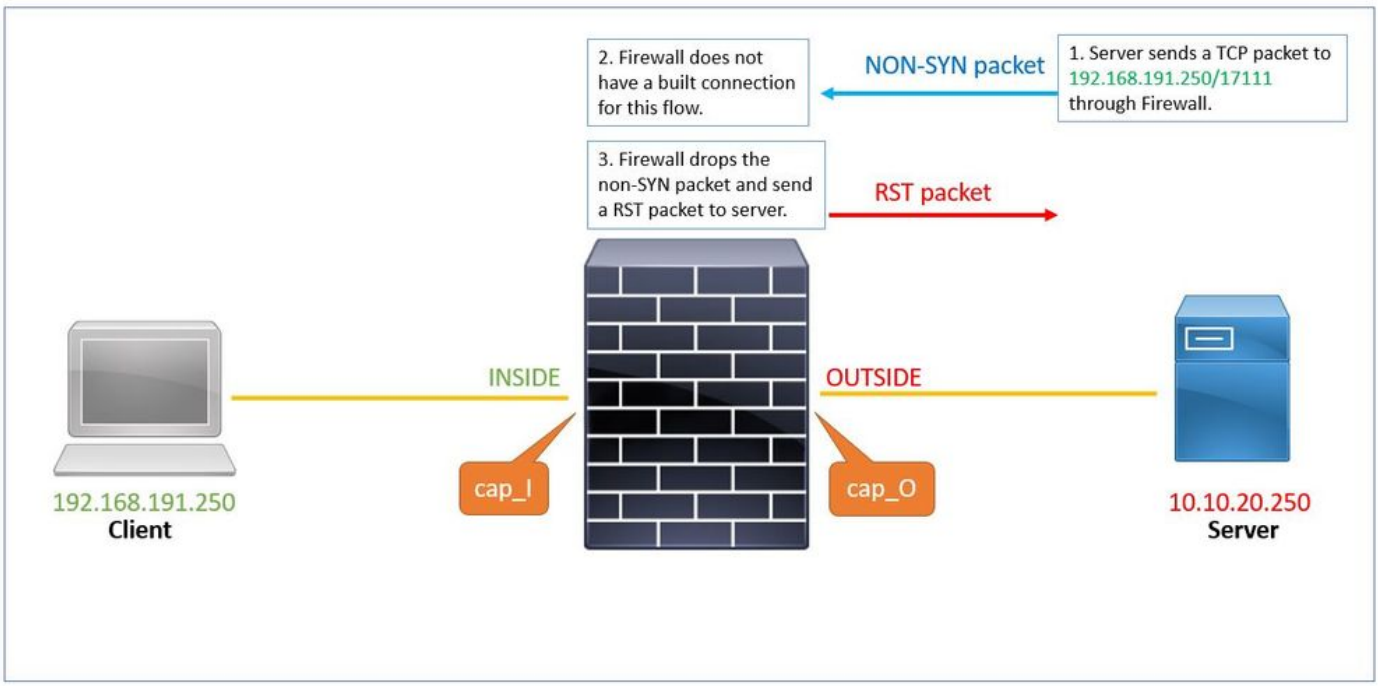
```
# show capture asp
```

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

案例分析4：服務重置出站停用（預設）服務resetinbound停用。

預設情況下，所有介面都會停用服務**resetoutbound**，並且還會透過配置命令停用服務**resetinbound**。

show run service



命令的輸出顯示service **resetoutbound**已停用（預設），service **resetinbound**則由配置命令停用。

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

1. 伺服器透過防火牆向客戶端傳送TCP資料包(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. 防火牆沒有為此流建立的連線並丟棄它。asp-drop captures顯示資料包：

```
# 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. 由於服務**resetinbound**，因此防火牆使用客戶端的源IP地址向伺服器傳送RST資料包。

```
# 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
```

相關資訊

- **思科技術支援與下載**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。