# WAF 阻擋封包分析

## 圖書館日治時期統計資料庫

# Test port 80 81

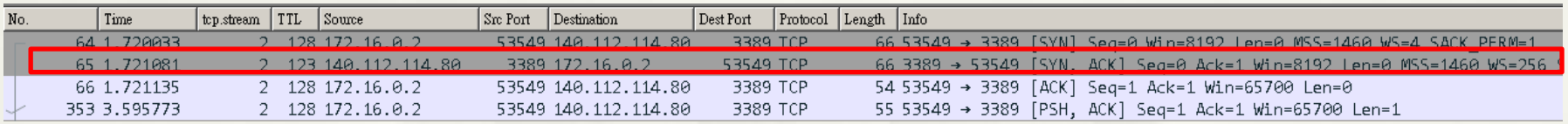
```
C:\Windows\System32>telnet  140.112.114.80 80
正連線到 140.112.114.80...無法開啟到主機的連線， 在連接埠 80: 連線失敗

C:\Windows\System32>telnet  140.112.114.80 81
正連線到 140.112.114.80...無法開啟到主機的連線， 在連接埠 81: 連線失敗
```

* Port 80 很快出現錯誤
* Port 81 Timeout 才出現錯誤

| No. | Time | tcp.stream | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| 127 | 2.594903 | 4 | 128 | 172.16.0.2 | 50815 | 140.112.114.80 | 80 | TCP | 66 | 50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 128 | 2.595441 | 4 | 250 | 140.112.114.80 | 80 | 172.16.0.2 | 50815 | TCP | 60 | 80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 163 | 3.089076 | 4 | 128 | 172.16.0.2 | 50815 | 140.112.114.80 | 80 | TCP | 66 | [TCP Retransmission] 50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_ |
| 164 | 3.090029 | 4 | 250 | 140.112.114.80 | 80 | 172.16.0.2 | 50815 | TCP | 60 | 80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 186 | 3.589163 | 4 | 128 | 172.16.0.2 | 50815 | 140.112.114.80 | 80 | TCP | 62 | [TCP Retransmission] 50815 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM= |
| 187 | 3.589807 | 4 | 250 | 140.112.114.80 | 80 | 172.16.0.2 | 50815 | TCP | 60 | 80 → 50815 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0 |
| 334 | 6.544895 | 11 | 128 | 172.16.0.2 | 50818 | 140.112.114.80 | 81 | TCP | 66 | 50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 825 | 9.546256 | 11 | 128 | 172.16.0.2 | 50818 | 140.112.114.80 | 81 | TCP | 66 | [TCP Retransmission] 50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_ |
| 1482 | 15.546509 | 11 | 128 | 172.16.0.2 | 50818 | 140.112.114.80 | 81 | TCP | 62 | [TCP Retransmission] 50818 → 81 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 SACK_PERM= |

* Port 80 被 reset. (TTL=250)
  * RST 封包間隔很短
* Port 81 Timeout
  * 間隔 3 秒、6 秒 重送 SYN

# Test port 3389

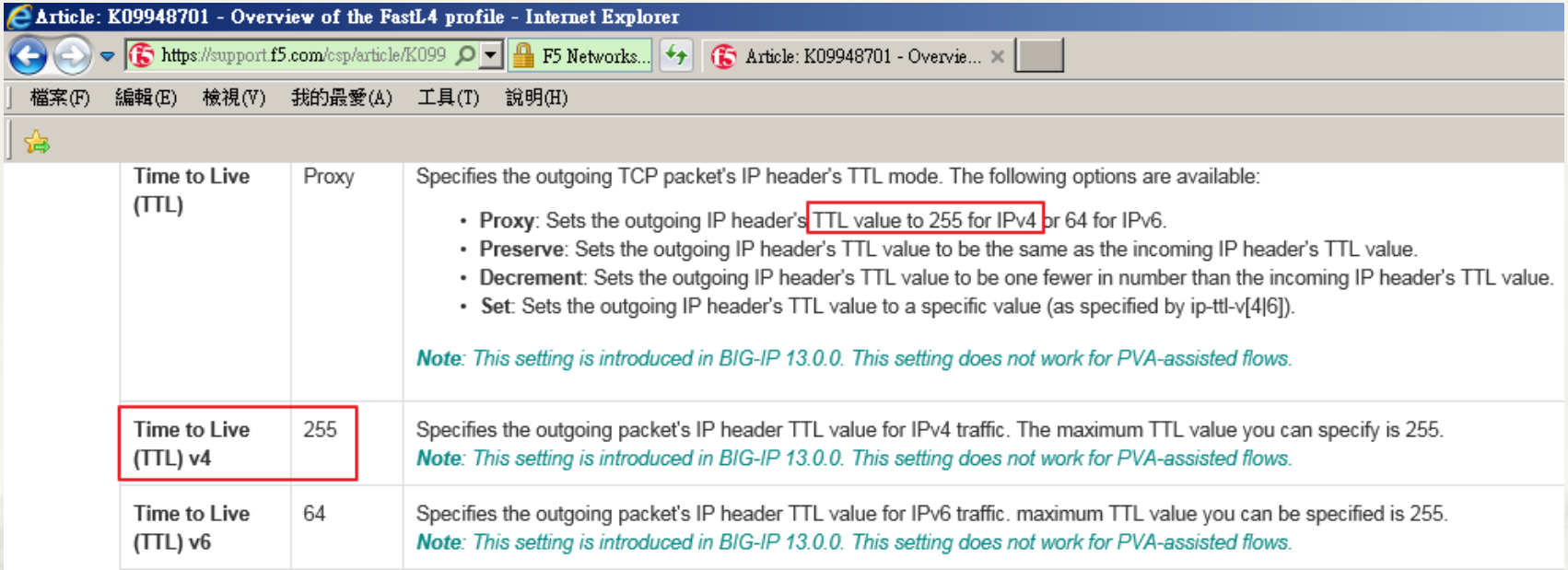


| No. | Time | tcp.stream | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| 64 | 1.720033 | 2 | 128 | 172.16.0.2 | 53549 | 140.112.114.80 | 3389 | TCP | 66 | 53549 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 65 | 1.721081 | 2 | 123 | 140.112.114.80 | 3389 | 172.16.0.2 | 53549 | TCP | 66 | 3389 → 53549 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 |
| 66 | 1.721135 | 2 | 128 | 172.16.0.2 | 53549 | 140.112.114.80 | 3389 | TCP | 54 | 53549 → 3389 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |
| 353 | 3.595773 | 2 | 128 | 172.16.0.2 | 53549 | 140.112.114.80 | 3389 | TCP | 55 | 53549 → 3389 [PSH, ACK] Seq=1 Ack=1 Win=65700 Len=1 |

* Port 3389 正常(TTL=123)

* 140.112.114.80 為 Windows Server，TTL 初始值 128，但發出 Reset 封包 TTL=250，推測該設備 TTL 初始值為 255
  * 128-123=5 hops -> Windows Server
  * 255-250=5 hops -> 發出 Reset 設備

# F5 Default TTL




| | | |
|---|---|---|
| **Time to Live (TTL)** | Proxy | Specifies the outgoing TCP packet's IP header's TTL mode. The following options are available:<br>• **Proxy**: Sets the outgoing IP header's TTL value to 255 for IPv4 or 64 for IPv6.<br>• **Preserve**: Sets the outgoing IP header's TTL value to be the same as the incoming IP header's TTL value.<br>• **Decrement**: Sets the outgoing IP header's TTL value to be one fewer in number than the incoming IP header's TTL value.<br>• **Set**: Sets the outgoing IP header's TTL value to a specific value (as specified by ip-ttl-v[4\|6]).<br>***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.* |
| **Time to Live (TTL) v4** | 255 | Specifies the outgoing packet's IP header TTL value for IPv4 traffic. The maximum TTL value you can specify is 255.<br>***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.* |
| **Time to Live (TTL) v6** | 64 | Specifies the outgoing packet's IP header TTL value for IPv6 traffic. maximum TTL value you can be specified is 255.<br>***Note***: *This setting is introduced in BIG-IP 13.0.0. This setting does not work for PVA-assisted flows.* |

# F5 Rule 刪除
# 恢復正常

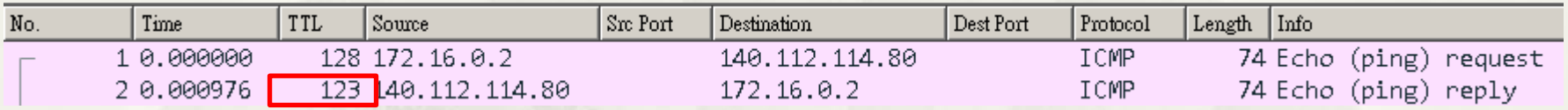
* 將 F5 Rule 刪除，Port 80 正常連線，TTL=123

ip.addr==140.112.114.80 Expression…

| No. | Time | tcp.stream | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|---|
| 316 | 1.942571 | 4 | 128 | 172.16.0.2 | 53512 | 140.112.114.80 | 80 | TCP | 66 | 53512 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1 |
| 317 | 1.943527 | 4 | 123 | 140.112.114.80 | 80 | 172.16.0.2 | 53512 | TCP | 66 | 80 → 53512 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1 |
| 318 | 1.943584 | 4 | 128 | 172.16.0.2 | 53512 | 140.112.114.80 | 80 | TCP | 54 | 53512 → 80 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |

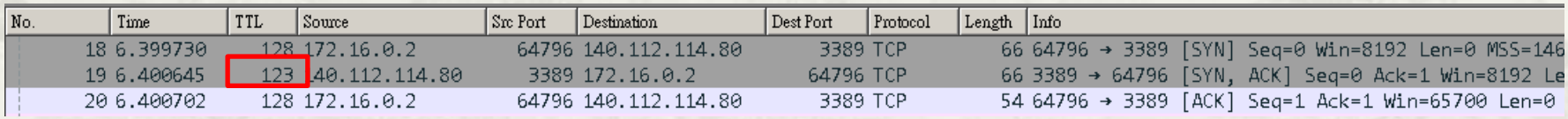
# F5 Rule 設定正確後

- ping 140.112.114.80
  - TTL=123 Windows



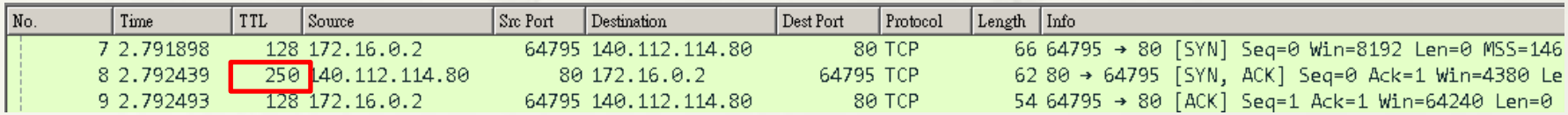
| No. | Time | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|
| 1 | 0.000000 | 128 | 172.16.0.2 | | 140.112.114.80 | | ICMP | 74 | Echo (ping) request |
| 2 | 0.000976 | 123 | 140.112.114.80 | | 172.16.0.2 | | ICMP | 74 | Echo (ping) reply |

- telnet 140.112.114.80 3389
  - TTL=123 Windows



| No. | Time | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|
| 18 | 6.399730 | 128 | 172.16.0.2 | 64796 | 140.112.114.80 | 3389 | TCP | 66 | 64796 → 3389 [SYN] Seq=0 Win=8192 Len=0 MSS=146 |
| 19 | 6.400645 | 123 | 140.112.114.80 | 3389 | 172.16.0.2 | 64796 | TCP | 66 | 3389 → 64796 [SYN, ACK] Seq=0 Ack=1 Win=8192 Le |
| 20 | 6.400702 | 128 | 172.16.0.2 | 64796 | 140.112.114.80 | 3389 | TCP | 54 | 64796 → 3389 [ACK] Seq=1 Ack=1 Win=65700 Len=0 |

- telnet 140.112.114.80 80
  - TTL=250 F5



| No. | Time | TTL | Source | Src Port | Destination | Dest Port | Protocol | Length | Info |
|---|---|---|---|---|---|---|---|---|---|
| 7 | 2.791898 | 128 | 172.16.0.2 | 64795 | 140.112.114.80 | 80 | TCP | 66 | 64795 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=146 |
| 8 | 2.792439 | 250 | 140.112.114.80 | 80 | 172.16.0.2 | 64795 | TCP | 62 | 80 → 64795 [SYN, ACK] Seq=0 Ack=1 Win=4380 Le |
| 9 | 2.792493 | 128 | 172.16.0.2 | 64795 | 140.112.114.80 | 80 | TCP | 54 | 64795 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0 |