

Telnet 連線 - 無 Ack 規則表



✿ 允許內外部 Telnet 連線，無採用 ACK 訊號

Telnet
封包訊息表

	服務方	封包方	來源位	目的位	封包型態	來源	目的	ACK
要求連線	出去	出去	內部	任意	TCP	>1024	23	No
同意連線	出去	進入	任意	內部	TCP	23	>1024	Yes
要求連線	進入	進入	任意	內部	TCP	> 1024	23	No
同意連線	進入	出去	內部	任意	TCP	23	>1024	Yes

允許雙方連線
封包規則表

則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	措施
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許
E	皆可	任意	任意	TCP	任意	任意	拒絕



Telnet 連線 - 無 Ack 規則表



✿ 允許內外部 Telnet 連線，無採用 ACK 訊號

✿ 封包過濾規則表

則	封包方	來源位	目的位	協定	來源埠	目的埠	策略
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許
E	皆可	任意	任意	TCP	任意	任意	拒絕



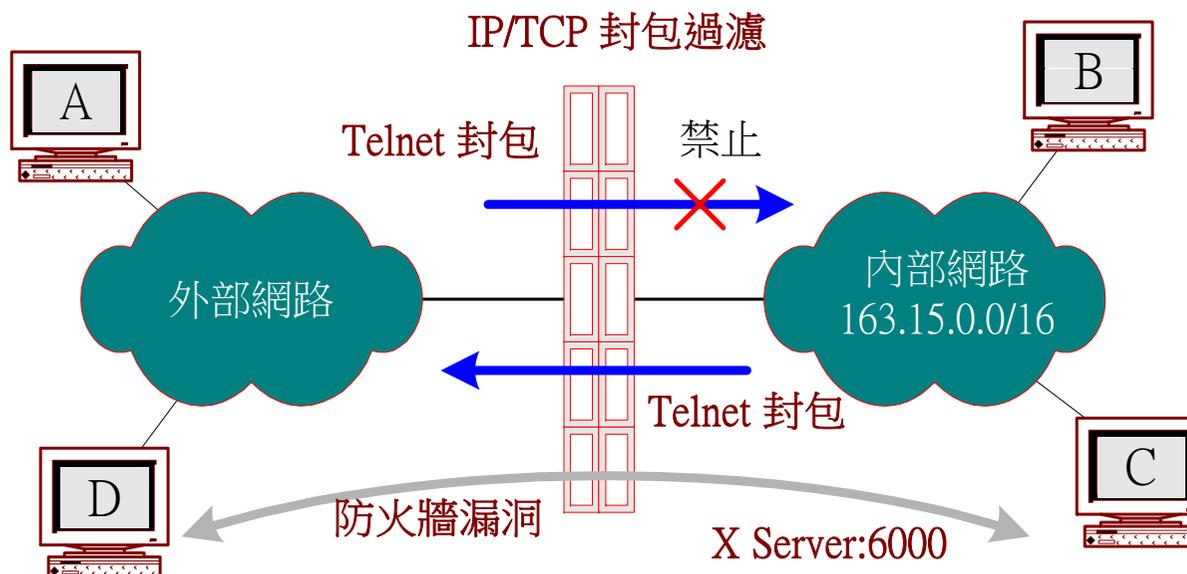
無 Ack 產生漏洞與補救



✦ TCP 6000 漏洞

◆ 無 ack 產生

服務方式	封包方向	來源位址	目的位址	封包型態	來源埠口	目的埠口	措施
要求連線	進入	外部	內部	TCP	23	6000	符合規則 B
同意連線	出去	內部	外部	TCP	6000	23	符合規則 D



無 Ack 產生漏洞與補救



原封包過濾規則表

則	封包方	來源位	目的位	協定	來源埠	目的埠	措施
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許
E	皆可	任意	任意	TCP	任意	任意	拒絕

新增封包過濾規則

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	措施
A	出去	內部	任意	TCP	>1023	23	允許
B	進入	任意	內部	TCP	23	>1024	允許
C	進入	任意	內部	TCP	>1023	23	允許
D	出去	內部	任意	TCP	23	>1024	允許
E	進入	任意	內部	TCP	>1023	6000	拒絕
F	出去	內部	任意	TCP	6000	>1023	拒絕
G	皆可	任意	任意	TCP	任意	任意	拒絕

