

範例：允許內外 Telnet 有 ack



✿ 雙向 Telnet 連線：允許 Telnet 連線，但採用 ACK 訊號

Telnet 封包訊息表

內部要求連線
及外部同意

外部要求連線
及內部同意

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

封包過濾規則表

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

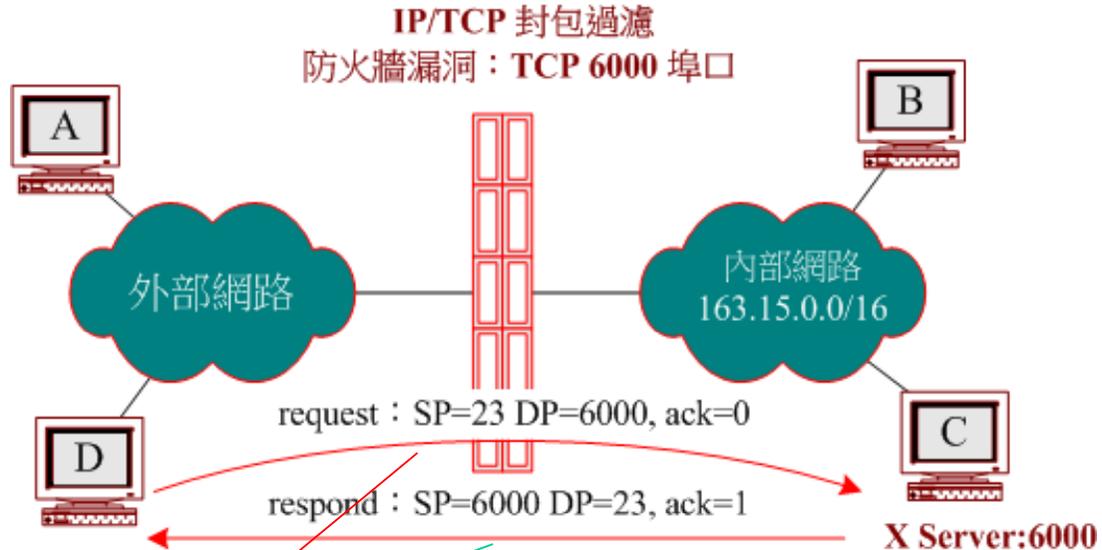


避免漏洞產生 - ack 參數



✿ TCP6000 漏洞

- ◆ 外部利用 23 埠口
連結內部 6000 埠口



封包過濾規則表

同意連線
不會發生

攔截要求連線

規則	封包方向	來源位址	目的位址	協定	來源埠口	目的埠口	ACK 設定	措施
A	出去	內部	任意	TCP	>1023	23	0	允許
B	進入	任意	內部	TCP	23	>1024	1	允許
C	進入	任意	內部	TCP	>1023	23	0	允許
D	出去	內部	任意	TCP	23	>1024	1	允許
E	皆可	任意	任意	TCP	任意	任意	皆可	拒絕

