



# 防火墙TCP会话的几个过程

会话

孔梦龙

2022-01-17 发表

## 组网及说明

假设您已经了解和掌握了TCP的三次握手和四次挥手;

## 配置步骤

(1) 三次握手:

FW收到首包syn, 新建会话状态为 TCP\_SYN\_SENT;  
收到回包syn ack, 刷新状态成为TCP\_SYN\_RECV ;  
再收到ack, 就是Established , 状态为: TCP\_ESTABLISHED

(2) 四次挥手:

\*Jan 17 18:45:23:154 2022 RBM-P SESSION/7/TABLE:  
Tuple5 (FSM): 1.1.1.2/36742-->1.1.3.10/21(TCP(6))  
FSM:TCP\_ESTABLISHED-->TCP\_FIN\_WAIT, dir:REPLY, PacketType:FIN(17)

\*Jan 17 18:45:23:155 2022 RBM-P SESSION/7/TABLE:  
Tuple5 (FSM): 1.1.1.2/36742-->1.1.3.10/21(TCP(6))  
FSM:TCP\_FIN\_WAIT-->TCP\_CLOSE\_WAIT, dir:ORIGIN, PacketType:ACK(16)

\*Jan 17 18:45:23:449 2022 RBM-P SESSION/7/TABLE:  
Tuple5 (FSM): 1.1.1.2/36742-->1.1.3.10/21(TCP(6))  
FSM:TCP\_CLOSE\_WAIT-->TCP\_LAST\_ACK, dir:REPLY, PacketType:FIN(25)

\*Jan 17 18:45:23:491 2022 RBM-P SESSION/7/TABLE:  
Tuple5 (FSM): 1.1.1.2/36742-->1.1.3.10/21(TCP(6))  
FSM:TCP\_LAST\_ACK-->TCP\_TIME\_WAIT, dir:ORIGIN, PacketType:ACK(16)

配置关键点

无