调整 TCP_IP 防范攻击 PDF转换可能丢失图片或格式，建议阅读原文
https://www.100test.com/kao_ti2020/224/2021_2022__E8_B0_83_E6_95_B4_TCP_c101_224826.htm TCP/IP安全设置除了上述所列出的设置之外，可以修改下列项以辅助系统更有效地抵御攻击。请注意，这些推荐值决不是使系统不受攻击，而只在于调整TCP/IP栈防范攻击。这些项的设置并不涉及系统上的许多其它组件（可能被用于攻击系统）。对于注册表的任何更改，管理员必须充分了解这些更改对系统默认功能的影响以及在他们的环境中是否适当。 SynAttackProtect 项：TcpipParameters 数值类型：REG_DWORD 有效范围：0、1、2 0（没有SYN攻击保护） 1（如果满足TcpMaxHalfOpen和TcpMaxHalfOpenRetried设置，减少重传重试次数与延迟的RCE（路由缓存项）创建。） 2（除1之外的另一个Winsock延迟指示。） 备注当系统发现自己受到攻击时，任何套接字上的下列选项不再启用：可缩放窗口(RFC 1323)与每个适配器上已配置TCP参数（初始RTT、窗口大小）。这是因为当保护生效时，在发送SYN-ACK之前不再查询路由缓存项，并且连接过程中Winsock选项不可用。 默认值：0 (false) 推荐值：2 说明：SYN攻击保护包括减少SYN-ACK重传次数，以减少分配资源所保留的时间。路由缓存项资源分配延迟，直到建立连接为止。如果synattackprotect = 2，则AFD的连接指示一直延迟到三路握手完成为止。注意，仅在TcpMaxHalfOpen和TcpMaxHalfOpenRetried设置超出范围时，保护机制才会采取措施。 TcpMaxHalfOpen 项：TcpipParameters 数值类型：REG_DWORD -数字 有效范围：100-0xFFFF 默认值：100

(Professional、Server)、500 (Advanced Server) 说明：该参数控制SYN攻击保护启动前允许处于SYN-RCVD状态的连接数量。如果将SynAttackProtect设为1，确保该数值低于要保护的端口上AFD侦听预备的值（有关详细信息，参见附录C中的预备参数）。有关详细信息，请参见 SynAttackProtect参数。[1] [2] [3] 