

常见病毒端口及处理方法

冲击波（变种）：

关闭TCP端口 135.193.445.593

关闭UDP端口 69(TFTP).135.137.138

关闭用于远程命令外壳程序TCP端口：4444

TCP: 135.139.445.4444

UDP: 69(TFTP).135.137.138

震荡波：

TCP: 5554.445.9996

SQL蠕虫病毒：

TCP:1433 UDP:1434

配置：

DCRS-5650-28(R4)(config)#access-list 110 deny tcp any any d-port 4444

DCRS-5650-28(R4)(config)#access-list 110 deny udp any any d-port 1434

DCRS-5650-28(R4)(config)#firewall enable 开启防火墙

DCRS-5650-28(R4)(config)#interface ethernet 1/0/1 应用到端口

DCRS-5650-28(R4)(config-if-ethernet1/0/1)#ip access-group 110 in

注：端口对网络应用是十分重要的，如udp 69端口是tftp的端口号，为了防范病毒关闭端口，TFTP的应用就无法使用。在关闭端口时注意端口其他用途。