7. 防火墙

防火墙：firewall
    将组织内部网络和互联网络隔离开来，按照规则允许某些分组通过（进出），或者阻塞掉某些分组

    为什么？
        阻止拒绝服务攻击： DOS攻击
            SYN flooding：攻击者建立很多伪造TCP链接，对于真正用户而言已经没有资源留下了
        阻止非法的修改/对非授权内容的访问
            e.g.，攻击者替换掉CIA的主页
        只允许认证的用户能否访问内部网络资源 (经过认证的用户/主机集合)
        2种类型的防火墙：
            网络级别：分组过滤器
                有状态，无状态
            应用级别：应用程序网关

    分组过滤
        内部网络通过配置防火墙的路由器连接到互联网上
        路由器对分组逐个过滤，根据以下规则来决定转发还是丢弃
            源IP地址，目标IP地址
            TCP/UDP源和目标端口
            ICMP报文类别
            TCP SYN 和 ACK bits

        分组过滤-无状态   防火墙不维护连接状态
            例1:阻塞进出的数据报：只要拥有IP协议字段 = 17，而且 源/目标端口号 = 23.
                所有的进出UDP流 以及telnet 连接的数据报都被阻塞掉
            例2：阻塞进入内网的TCP段：它的ACK=0.
                阻止外部客户端和内部网络的主机建立TCP连接
                但允许内部网络的客户端和外部服务器建立TCP连接

        分组锅炉-有状态
            无状态分组过滤根据每个分组独立地检查和行动
            有状态的分组过滤联合分组状态表检查和行动
            ACL增强：在允许分组之前需要检查连接状态表
            图3

    应用程序网关 在应用层
        根据应用数据的内容来过滤进出的数据报，就像根据IP/TCP/UDP字段来过滤一样
            检查的级别：应用层数据
        Example：允许内部用户登录到外部服务器，但不是直接登录

        1. 需要所有的telnet用户通过网关来telnet
        2. 对于认证的用户而言，网关建立和目标主机的telnet connection ，网关在2个连接上进行中继
        3. 路由器过滤器对所有不是来自网关的telnet的分组全部过滤掉

无状态分组过滤器: 例子

策略	防火墙设置
不允许外部的web进行访问	阻塞掉所有外出具有目标端口80的IP分组
不允许来自外面的TCP连接，除非是机构公共WEB服务器的连接	阻塞掉所有进来的TCP SYN分组，除非130.207.244.203, port 80
阻止Web无线电占用可用带宽.	阻塞所有进来的UDP分组 - 除非 DNS 和路由器广播
阻止你的网络被smurf DoS所利用	阻塞掉所有具有广播地址的ICMP分组 (eg 130.207.255.255).
阻止内部网络被tracerout，从而得到你的网络拓扑	阻塞掉所有外出的 ICMP TTL过期的流量

- *ACL:* 规则的表格，top - bottom应用到输入的分组: (action, condition) 对

action	source address	dest address	protocol	source port	dest port	flag bit
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----
deny	all	all	all	all	all	all

action	source address	dest address	proto	source port	dest port	flag bit	check conxion
allow	222.22/16	outside of 222.22/16	TCP	> 1023	80	any	
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK	✗
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	✗
deny	all	all	all	all	all	all	

局限性：

IP spoofing: 路由器不知道数据报是否真的来自于声称的源地址

如果有多个应用需要控制，就需要有多个应用程序网关

客户端软件需要知道如何连接到这个应用程序

e.g., 必须在Web browser中配置网络代理的Ip地址

过滤器对UDP段所在的报文，或者全过或者全都不过

折中：与外部通信的自由度，安全的级别

很多高度保护的站点仍然受到攻击的困扰