哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY
立足航天，服务国防，面向国民经济主战场

计算机网络之危机四伏

主讲人：李全龙

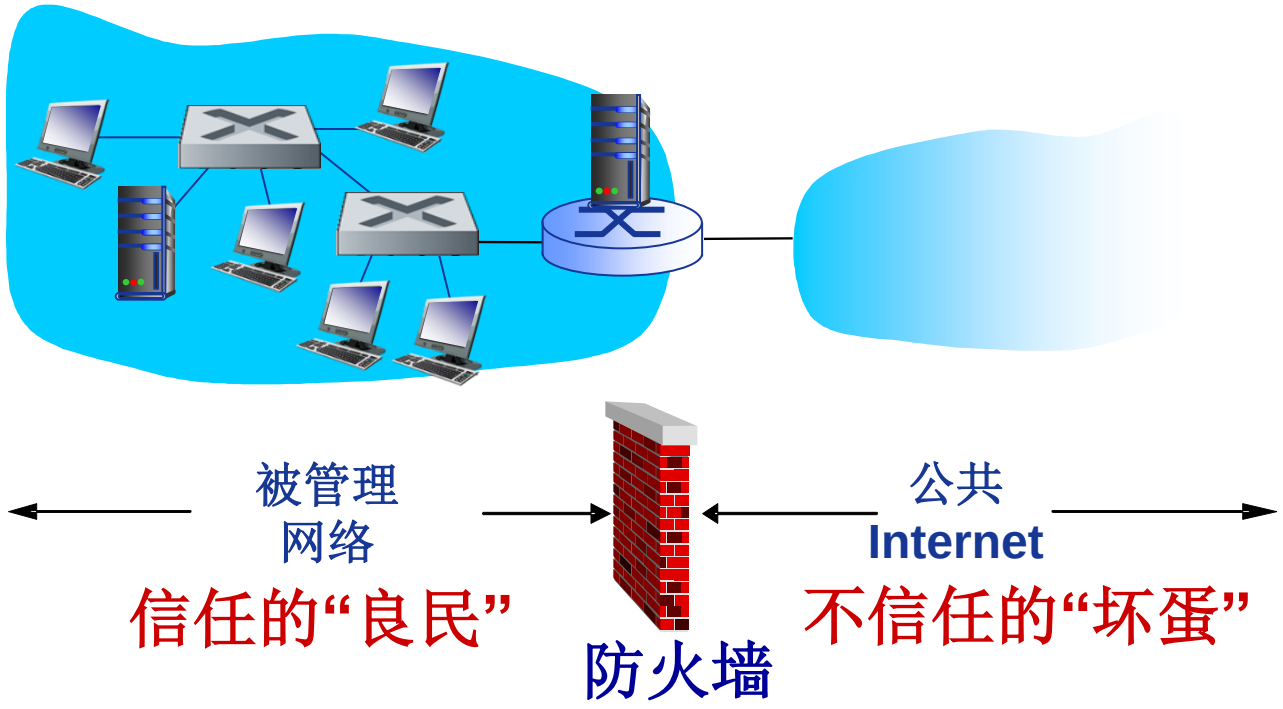
本讲主题

防火墙

防火墙

防火墙(firewall)

隔离组织内部网络与公共互联网，允许某些分组通过，而阻止其他分组进入/离开内部网络的软件/硬件设施。



为什么需要防火墙？

预防拒绝服务攻击（DoS）：

- SYN泛洪: 攻击者建立许多虚假TCP连接，耗尽资源，导致“真正”的连接无法建立

预防非法修改/内部数据访问:

- e.g., 攻击者替换CIA网站主页

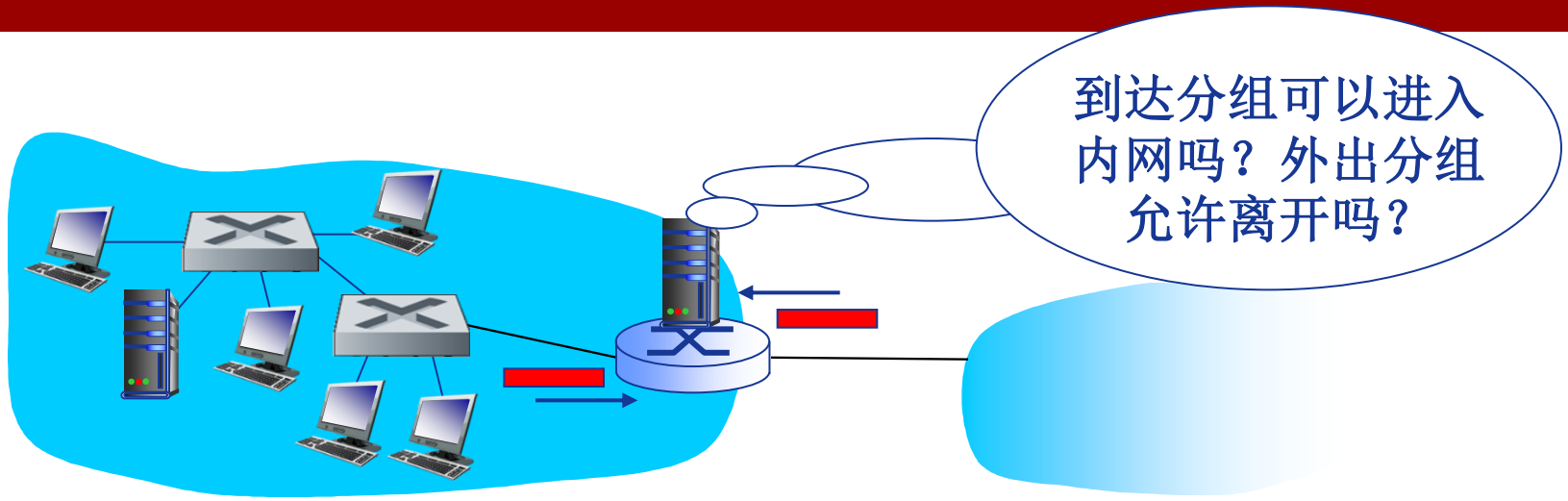
只允许对内部网络的授权访问：

- 认证的用户/主机

三种类型的防火墙:

- 无状态分组过滤器(stateless packet filters)
- 有状态分组过滤器(stateful packet filters)
- 应用网关(application gateways)

无状态分组过滤



- 内部网络通过路由器防火墙(router firewall)与Internet连接
- 路由器逐个分组过滤，决策是否转发/丢弃分组，依据：
  - 源IP地址、目的IP地址
  - TCP/UDP源、目的端口号
  - ICMP报文类型
  - TCP SYN和ACK标志位
  - ……

无状态分组过滤：举例

- 例1: 阻止协议字段=17，以及源或目的端口号=23的数据报进入与离开
  - 结果: 所有进入或离开的UDP流量，以及Telnet连接均被阻止
- 例2: 阻止进入的、 ACK=0的TCP段
  - 结果: 阻止外部客户与内部主机主动建立TCP连接，但是允许内部客户与外部主机主动建立连接

无状态分组过滤：更多例子

策略(Policy)	防火墙设置
不允许访问外部Web站点	丢弃所有目的端口号=80的外出分组
禁止进入的TCP连接，连接组织公共Web服务器除外	丢弃所有TCP SYN段，目的IP地址为130.207.244.203, 端口号为80的IP数据报除外
阻止Web电台应用，以防消耗可用带宽	丢弃所有进入的UDP分组，DNS分组和路由器广播分组除外
阻止你的网络被用于蓝精灵DoS攻击	丢弃所有发往广播地址(e.g. 130.207.255.255)的ICMP分组
阻止你的网络被路由跟踪	丢弃所有外出的TTL失效ICMP流量

访问控制列表

- **ACL(Access Control Lists):** 规则表，自顶向下应用于到达的分组：(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

有状态分组过滤

- 无状态分组过滤器: 笨拙
  - 不加以区分放行满足条件的所有分组
  - 例如：放行dest port = 80、ACK=1的分组，即使没有建立的TCP连接:

action	source address	dest address	protocol	source port	dest port	flag bit
allow	outside of 222.22/16	222.22/16	TCP	80	> 1023	ACK

- 有状态分组过滤器: 跟踪每个TCP连接
  - 跟踪连接建立(SYN)、拆除(FIN): 根据状态确定是否放行进入或外出的分组
  - 超时的非活动连接: 不再允许分组通过

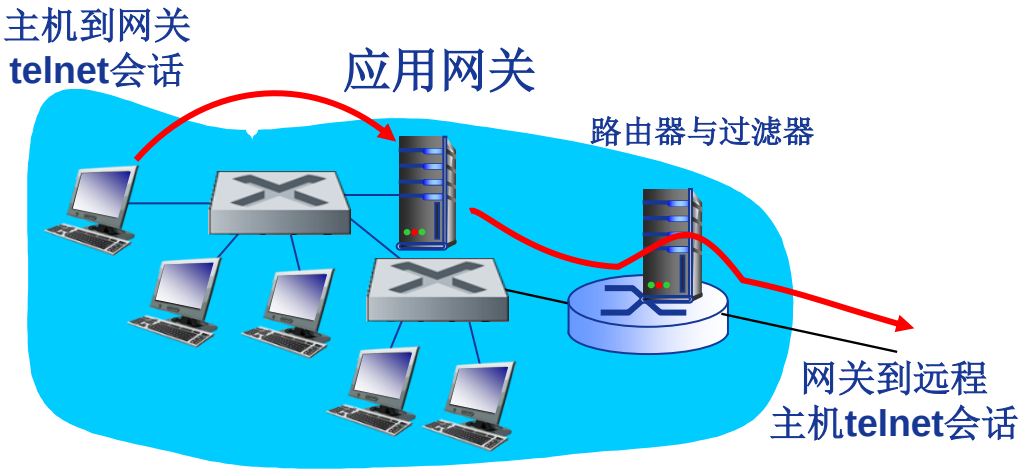
有状态分组过滤

- 扩展ACL，以便在放行分组前，检测连接状态表

action	source address	dest address	proto	source port	dest port	flag bit	check connection
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	X
allow	222.22/16	outside of 222.22/16	UDP	> 1023	53	---	
allow	outside of 222.22/16	222.22/16	UDP	53	> 1023	----	X
deny	all	all	all	all	all	all	

应用网关

- 基于应用数据以及IP/TCP/UDP头部字段过滤分组
- 例如：允许特定用户telnet外部网络



1. 要求所有Telnet用户通过网关Telnet外部网络；
2. 对于授权的用户，网关代理用户与目的主机建立Telnet连接，并且在两个连接之间进行数据中继；
3. 路由器阻止所有不是由网关发起的Telnet连接。

防火墙、应用网关的局限性

- IP欺骗(spoofing): 路由器不知道数据是否来自于声称的源
- 如果多个应用需要特殊处理，则每个应用需要一个应用网关
- 客户软件必须知道如何连接网关
  - e.g., 必须配置Web浏览器的代理服务器的IP地址
- 过滤器经常对UDP流量使用“全部通过”或者“全部不通过”策略
- 折衷(tradeoff): 确定安全级别
  - 与外部网络的通信度
- 很多安全防护级别很高的网站仍然遭受攻击

哈爾濱工業大學
HARBIN INSTITUTE OF TECHNOLOGY

立足航天，服务国防，面向国民经济主战场

谢 谢！