志存高远 责任为先

防火墙与入侵检测

地址：赣州市红旗大道86号 信息工程学院
网址：www.jxust.edu.cn
邮编：341000

目录/Contents

01
Part

防火墙

防火墙

- **将一个工作单位的内网和外面的因特网隔绝，对一些网络数据包进行屏蔽封锁**

防火墙作用

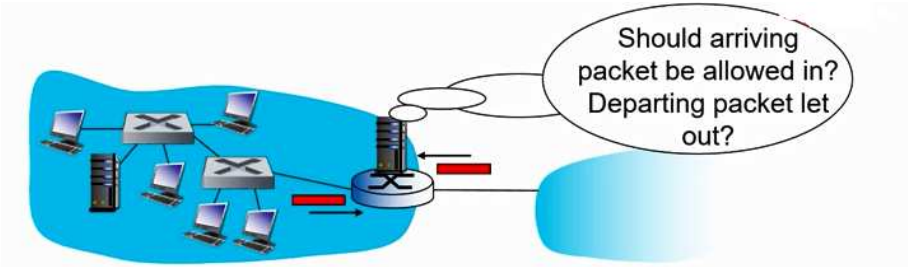
- **防止阻断服务攻击（denial of service attacks)**
  - **SYN flooding:攻击者同时建立很多TCP链接，以此耗尽服务器软、 硬件资源，使真正有需求的链接无法建立**
- **防止对内部数据的非法盗用和篡改**
  - **比如，攻击者可以攻入一个电商的网页服务器，并修改其网页内容**
- **只允许合法链接通过防火墙进入内网**
  - **内网应该只被有权限的设备和用户连接**

三种防火墙

- **无状态记录的数据包过滤**
- **有状态记录的数据包过滤**
- **基于应用的网关设置**

无状态记录的数据包过滤

- 内部通过路由器防火墙（router firewall)连接外网
- 路由器对数据包一个个进行筛选（filters packet-by-packet)，基于以下信息决定是否转发：
  - 发出方IP地址,接收方IP地址
  - TCP/UDP发出方和接收方的端口号（port number)
  - ICMP 信息类别（message type)
  - TCP SYN和ACK比特位的设置



无状态记录的数据包过滤例子

- 例 1: block incoming and outgoing datagrams with IP protocol field = 17 and with either source or dest port = 23
  - 结果：所有进出子网的UDP flows和telnet链接都被截断
- 例 2: block inbound TCP segments with ACK=0.
  - 结果：不允许子网外用户向子网内用户申请创建TCP链接，但允许子网内用户向子网外用户创建TCP链接

权限控制列表ACL

- **A CL： 一个权限控制条件表，以（action，condition)格式对进入内网数据包做筛查**

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

规则次序

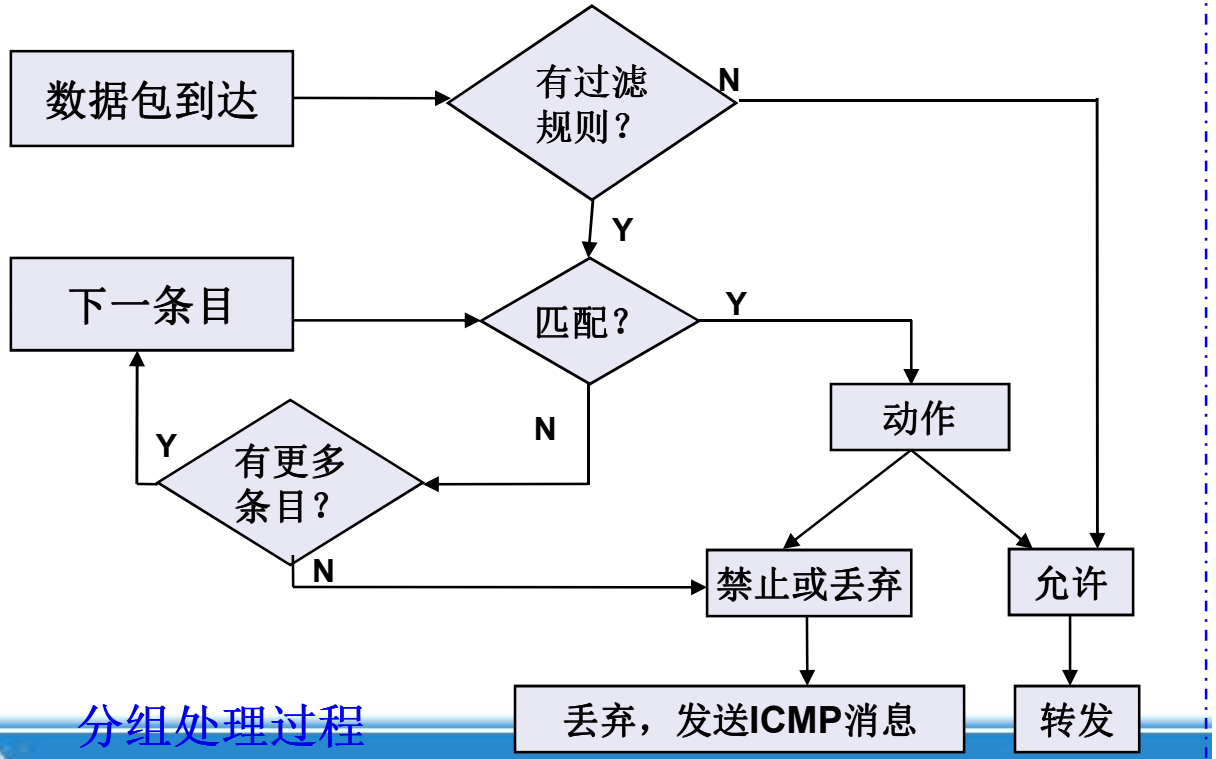
- 同样的规则，以不同的次序放置，可能会完全改变防火墙的运转情况
- 防火墙以顺序方式检查信息包，当防火墙接收到一个信息包时，它先与第一条规则相比较，然后是第二条、第三条……当它发现一条匹配规则时，就停止检查并应用那条规则。如果信息包经过每一条规则而没有发现匹配，这个信息包便会被拒绝。
- 通常的顺序是，较特殊的规则在前，较普通的规则在后，防止在找到一个特殊规则之前一个普通规则便被匹配，这可以使防火墙避免配置错误

规则不宜太多

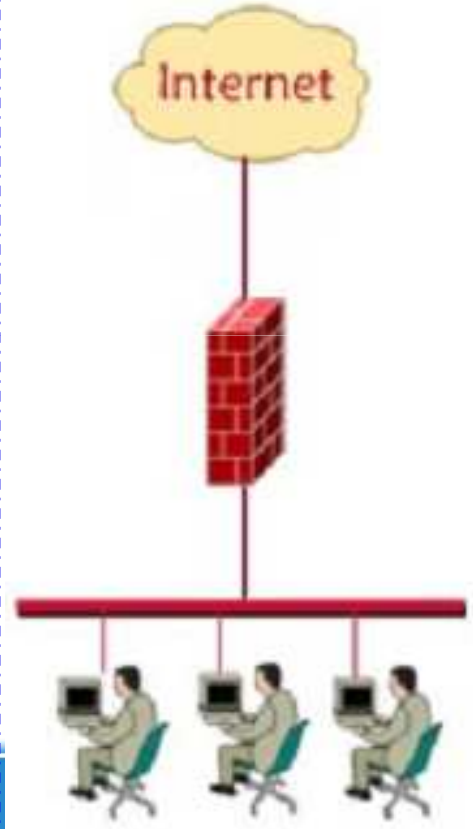
- 尽量保持规则集简洁和简短
- 规则越多，就越可能犯错误，规则越少，理解和维护就越容易。
- 一个好的准则是最好不要超过30条。一旦规则超过50条，就会以失败而告终
- 规则越少，规则集就越简洁，错误配置的可能性就越小，系统就越安全。 因为规则少意味着只分析少数的规则，防火墙的CPU周期就短，防火墙效率可提高

分组的处理

- 只在网络层和传输层检查数据，与应用层无关



分组处理过程



有状态记录包过滤

- **无状态记录过滤：**
  - **有可能满过一些没有意义的网包，如：dest port = 80，ACK bit set，even though no TCP connection established**

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

- **有状态记录过滤:对每一个TCP连接都跟踪其“状态”信息**
  - **实时监测建立（SYN),断开（FIN)信息：判断进入和离开内网的网报是否“合理”**
  - **对很久呆滞的连接进行切断处理**

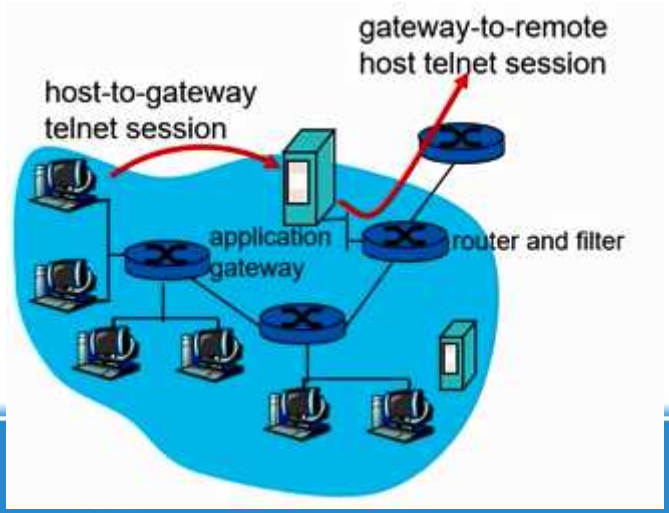
有状态记录包过滤

- **完善ACL，使其包含状态信息**

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	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

- 不光根据IP/TCP/UDP信息，而且根据应用层信息进行网包筛查
  - 例：允许有选择的一些内部用户通过 telnet连接外网
    - 1.要求所有用户通过网关建立telnet连接
    - 2.对有权限的用户，网关为其向目标终端建立telnet连接， 之后此连接的所有网络报文都通过网关转发
    - 3.路由器将拦截所有非网关转发的telnet连接

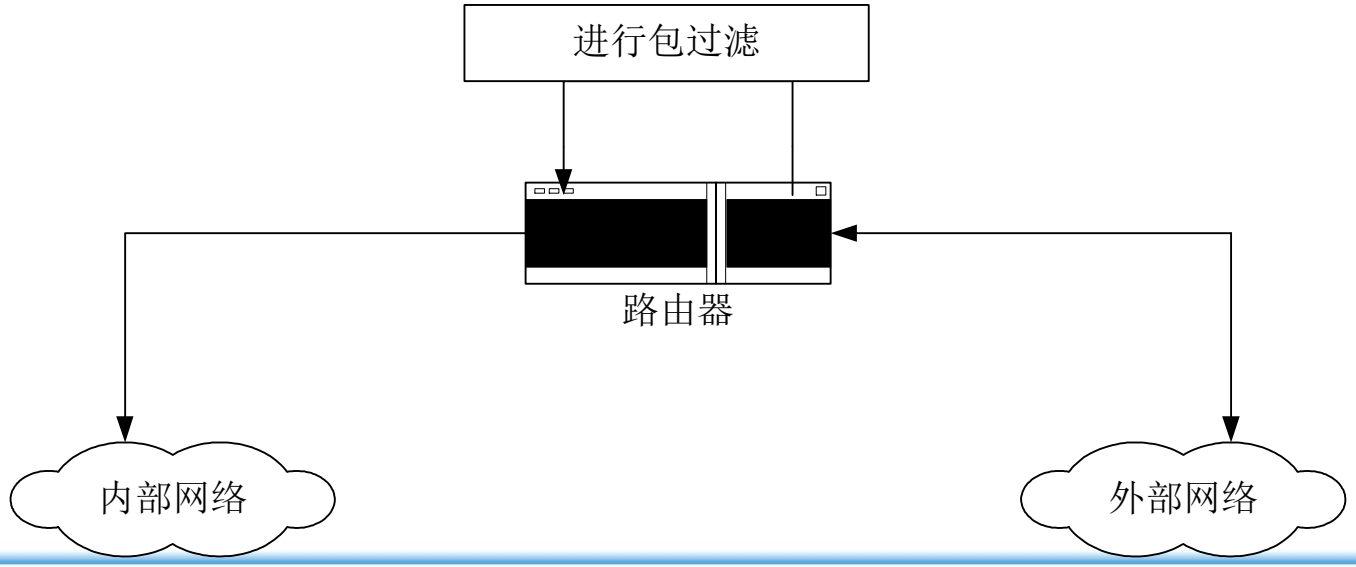


防火墙系统模型

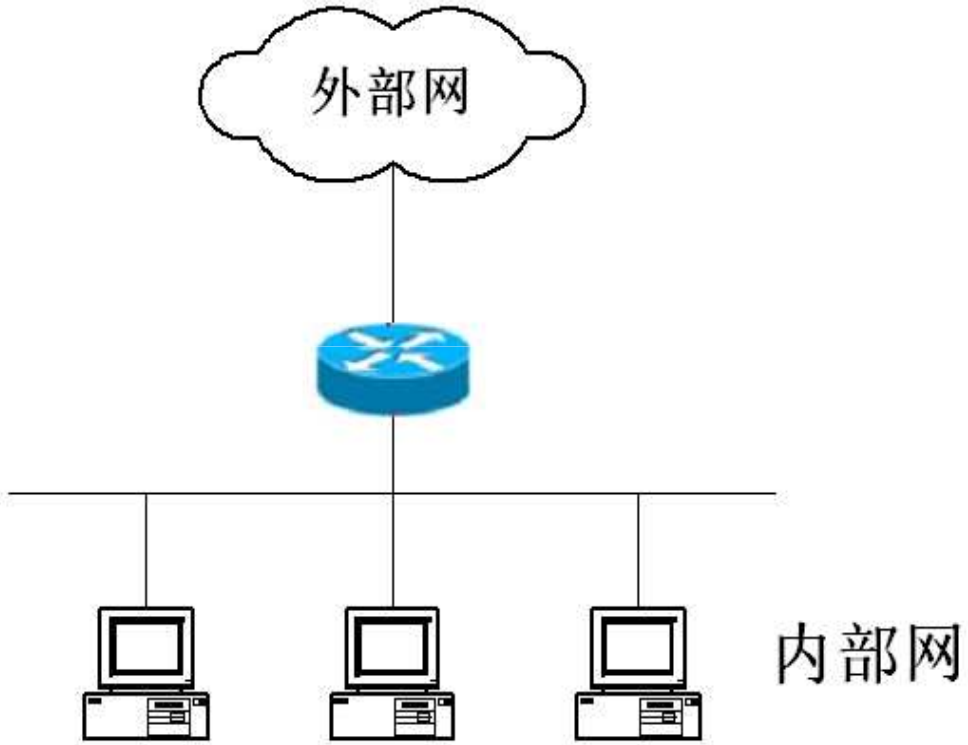
- **筛选路由器模型**
- **单宿主堡垒主机（屏蔽主机防火墙）模型**
- **双宿主堡垒主机模型（屏蔽防火墙系统模型）**
- **屏蔽子网模型**

筛选路由器（分组过滤防火墙）

- **实施包过滤**
- **不能隐藏内部网络信息、不具备监视和日志记录功能**

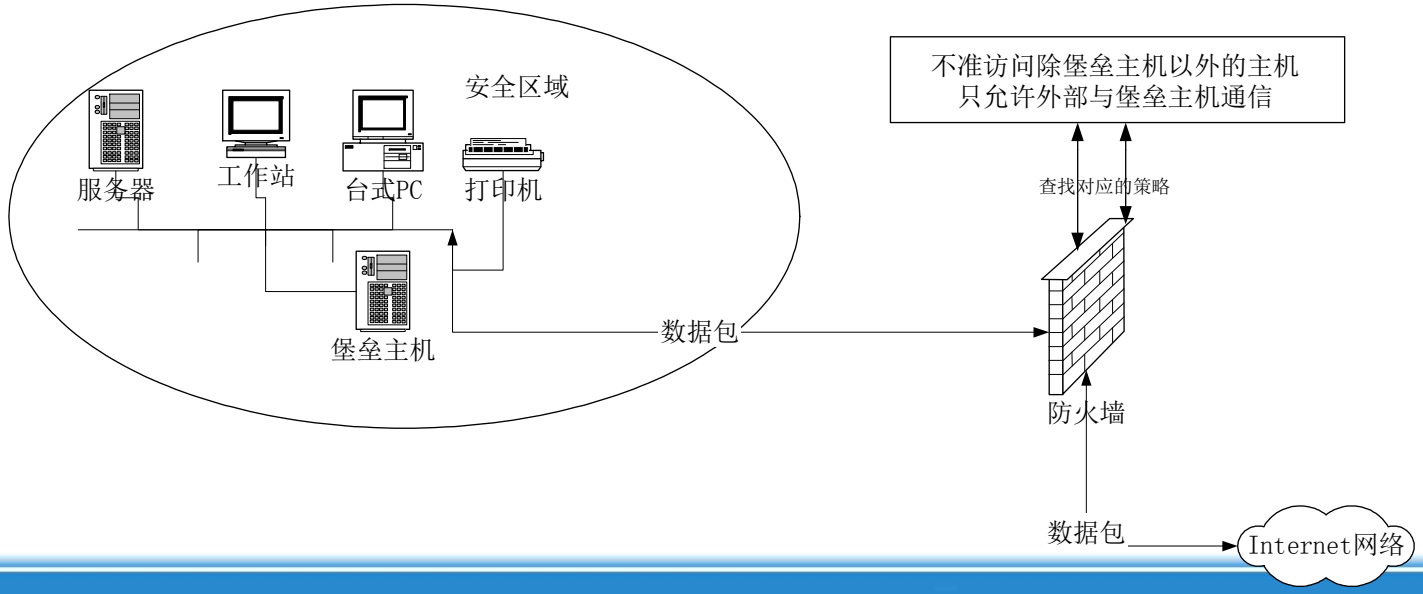


分组过滤防火墙的部署



单宿主堡垒主机（屏蔽主机防火墙）

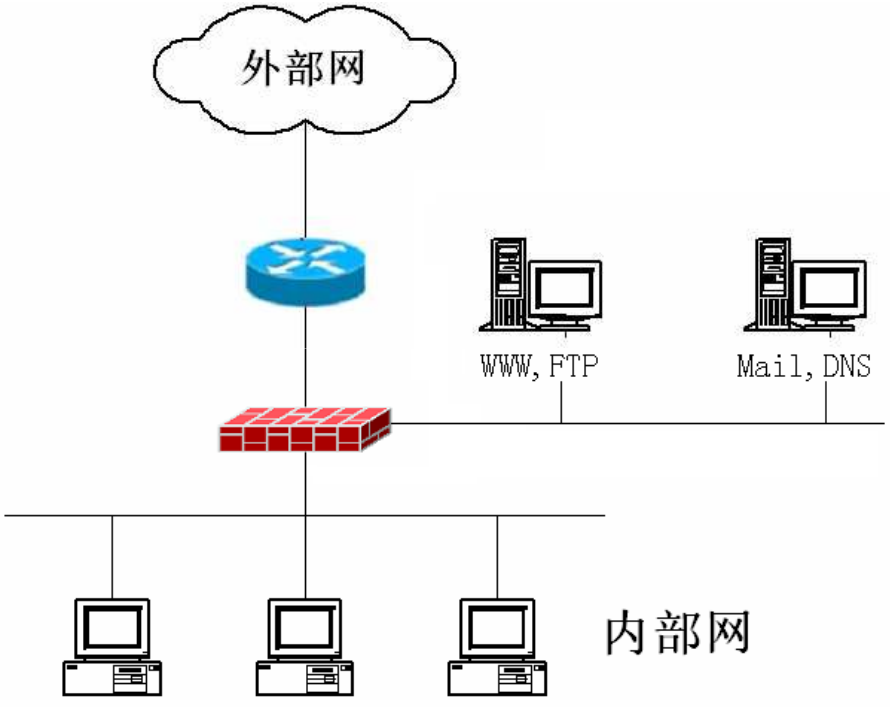
- **由分组过滤路由器和堡垒主机组成**
- **实现网络层安全和应用层安全**



堡垒主机

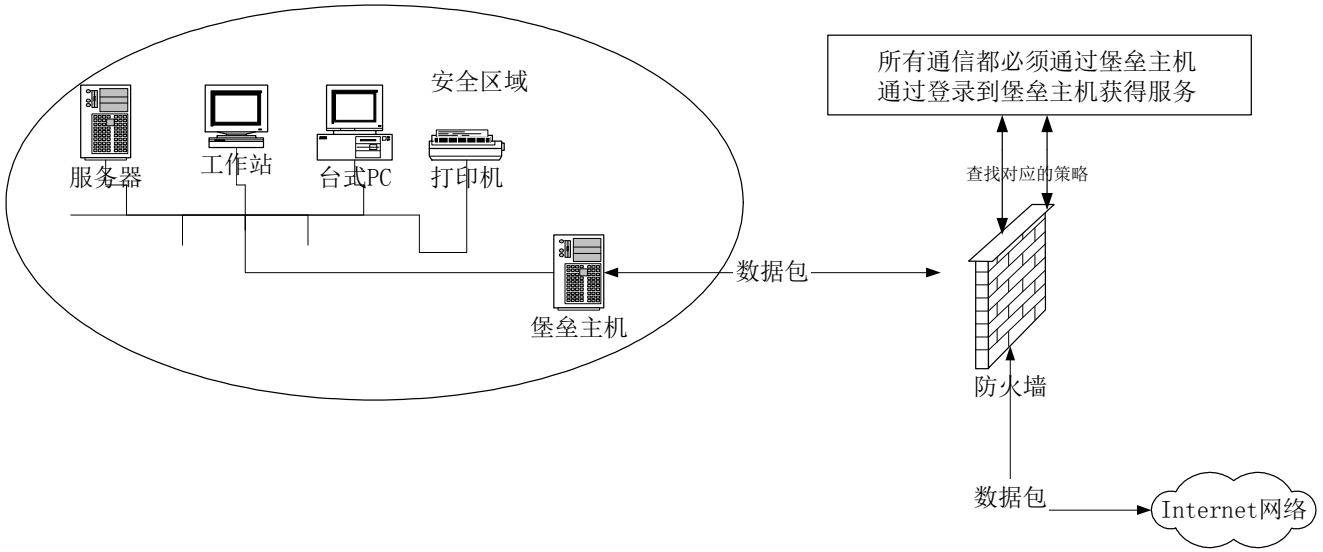
- 堡垒主机是一种被强化的可以防御进攻的计算机，被暴露于因特网之上，作为进入内部网络的一个检查点，以达到把整个网络的安全问题集中在某个主机上解决，从而省时省力，不用考虑其它主机的安全的目的。
- 堡垒主机是网络中最易受到侵害的主机，所以堡垒主机必须是自身保护最完善的主机。
- 防御的第一步就是把堡垒主机放在合适的位置上。
- 多数情况下，一个堡垒主机使用两块网卡，每个网卡连接不同的网络。一块网卡连接内部网络用来管理、控制和保护，而另一块连接另一个网络，也称为双宿主主机。

主机屏蔽防火墙的部署

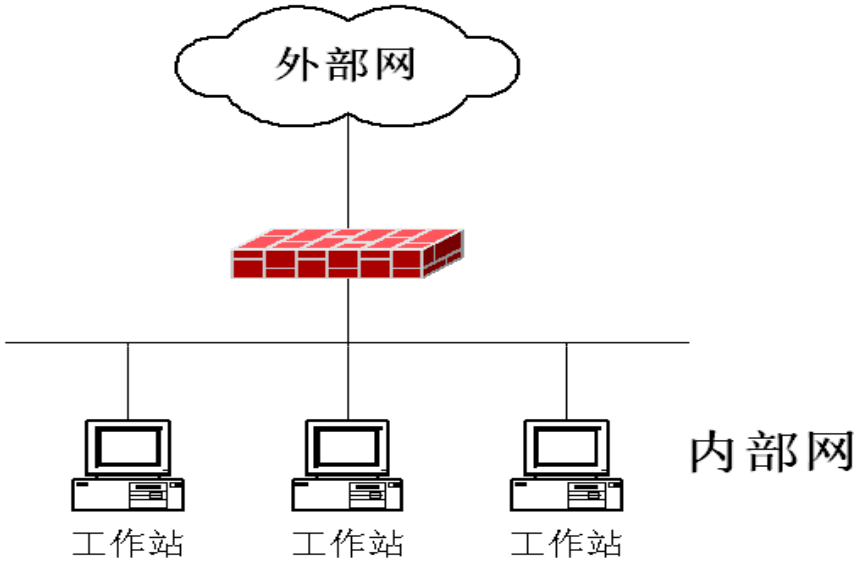


双宿主堡垒主机模型（屏蔽防火墙系统）

- **双宿主堡垒主机有两个网络接口，但是在两个端口之间直接转发信息的功能被关闭**
- **在物理结构上强行将所有去往内部网络的信息经过堡垒主机**

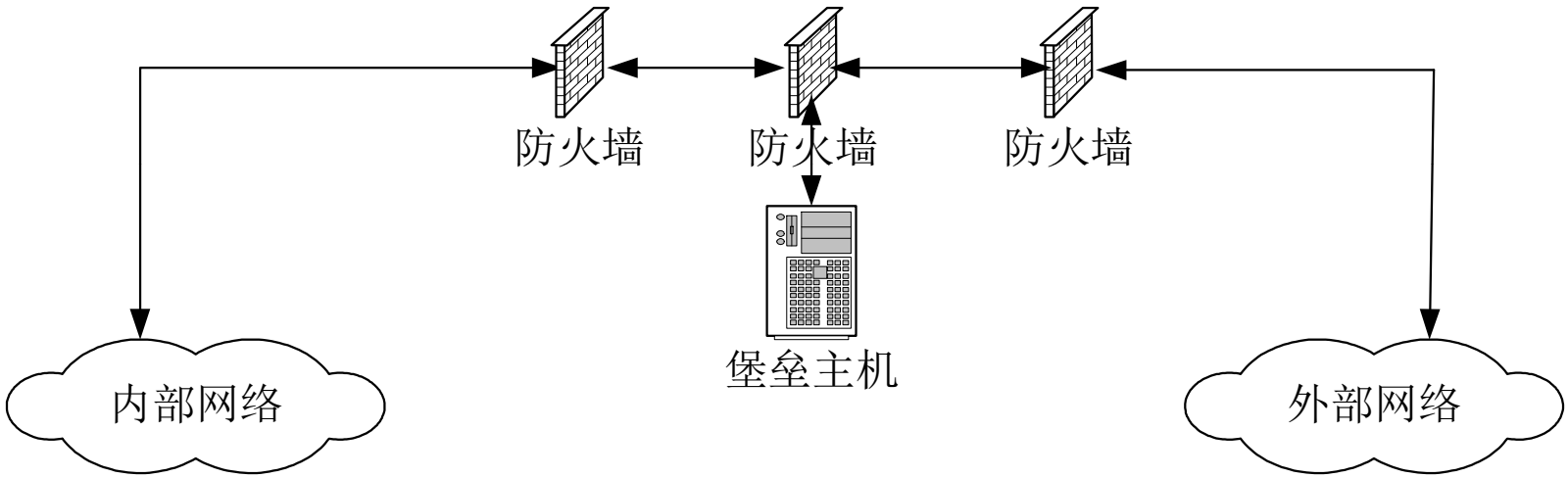


代理网关（双宿主主机）防火墙的部署

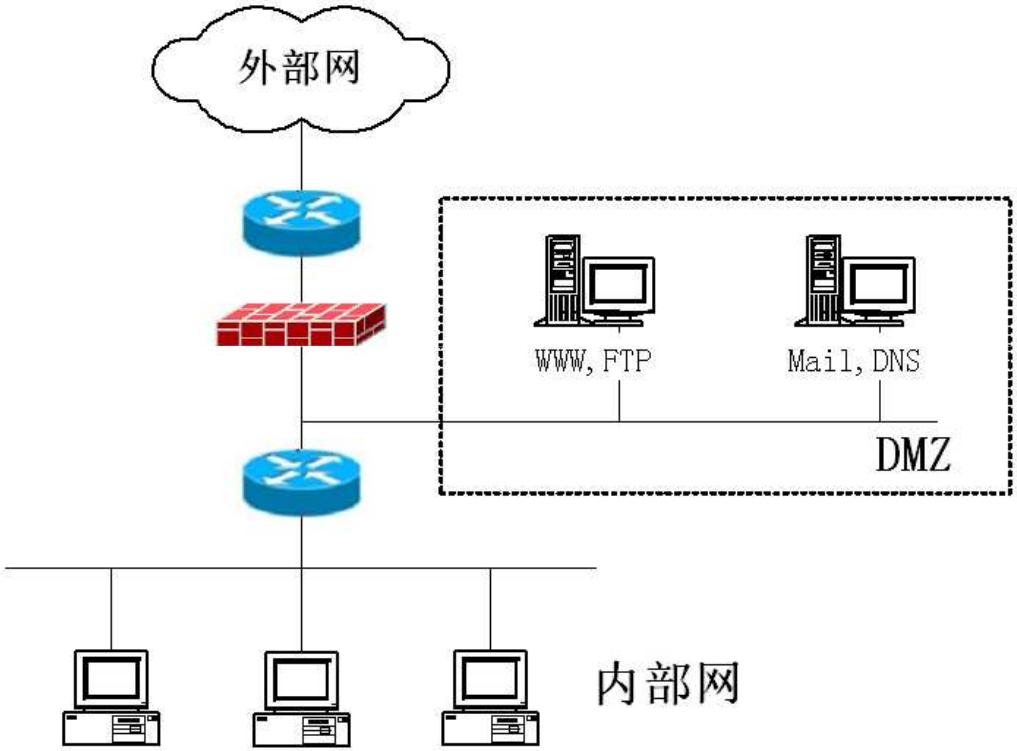


屏蔽子网模型

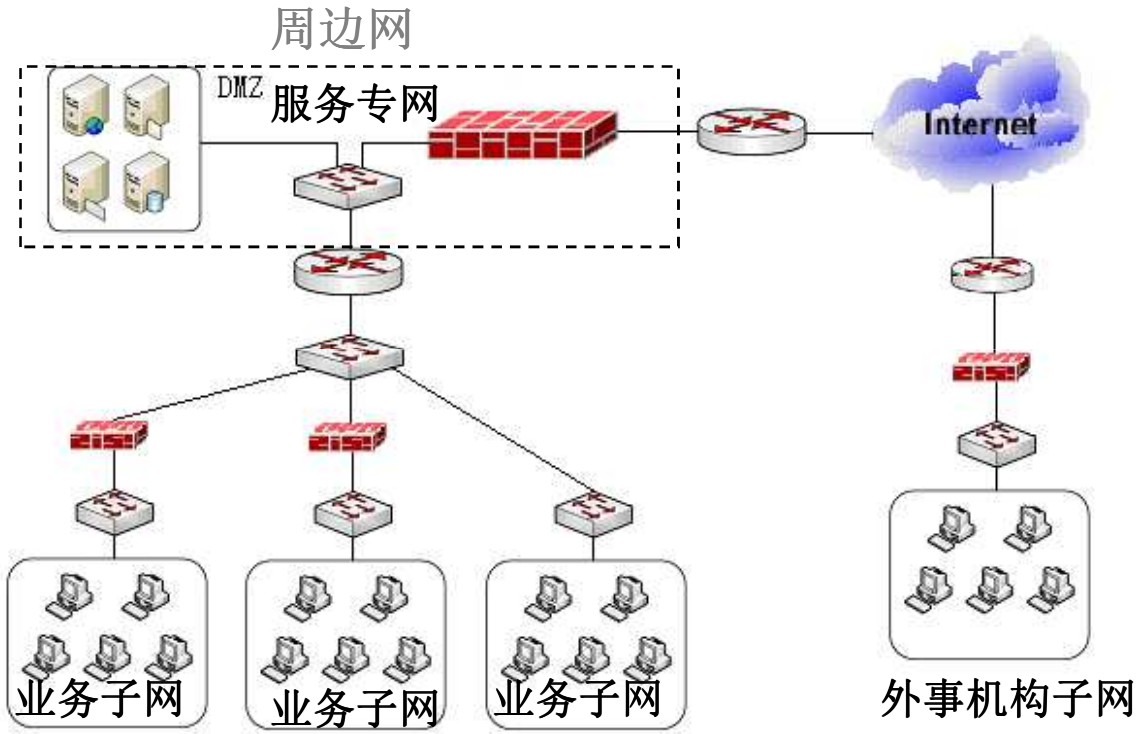
- **两个包过滤路由器和一个堡垒主机**



子网屏蔽防火墙的部署



企业常见分布式防火墙的部署



防火墙及网关的局性

- IP spoofing:路由器无法判断一组数据包是否真来自于自称的发出方
- 如果有多个应用需要过滤处理，那么每一个应用都要有一个应用网关
- 用户端应用软件需要知道如何连接网关
  - 如，必须要在网页浏览器应用里设置网关IP地址
- 过滤器一般对UDP网包要么使用所有过滤规则，要么完全不设置规则
- 取舍决策：跟外之间通讯的方便性，及系统安全性之间的矛盾
- 很多防火墙设置很全面的网络服务器还是会受到攻击

02
Part

入侵检测系统

防火墙的不足

- **入侵很容易**
  - **入侵教程随处可见**
  - **各种工具唾手可得**
- **防火墙对网络包进行过滤**
  - **第一道安全闸门、边界**
  - **但不完善，80%的攻击来自内部**
  - **只对TCP/IP协议数据“头区间”进行分析**
  - **对连接与连接之间的相关性不做检查**
- **有效补充---入侵检测，防火墙是锁，入侵检测系统是监视器**

IDS（入侵检测系统）

- **IDS: intrusion detection system**
  - **更深入的数据包检查：同时检测协议包的“数据段”（data contents)内容（如，对一 个数据包的字符串做比较检查，检查其与已知病毒数据库中电脑病毒的相似性）**
- **检查属于不同网络连接的数据包的相关性**
  - **port scanning**
  - **DoS attack**

IDS作用

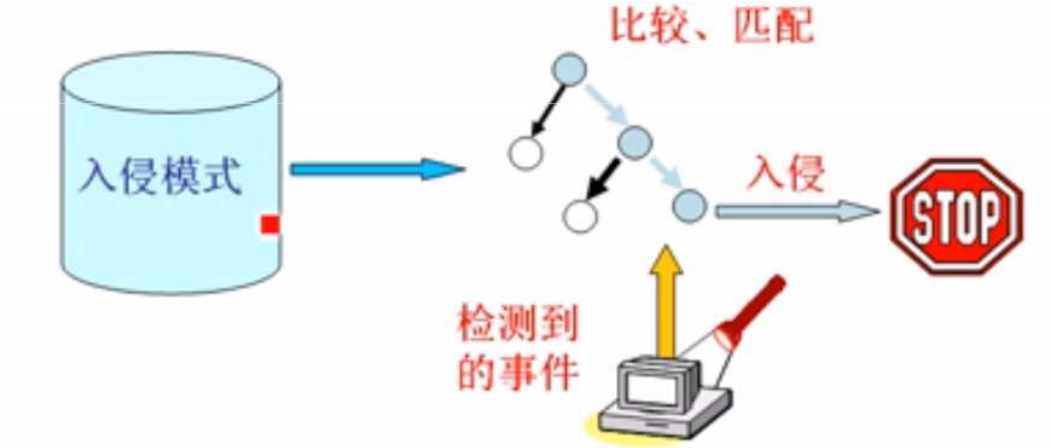
- **实时监测**
  - **实时监视、分析网络中所有的数据报文**
  - **发现并实时处理所捕获的数据包**
- **安全审计**
  - **对系统记录的网络事件进行分析**
  - **发现异常现象**
  - **寻找入侵证据**
- **主动响应**
  - **切断连接或与防火墙联动生成新规则或调用其他措施**

IDS的分类

- **基于主机的入侵检测系统HIDS**
  - **主要用于保护运行关键应用的服务器**
  - **监视与分析主机的审计记录和日志文件来检测入侵**
- **基于网络的入侵检测系统NIDS**
  - **主要用于实时监控网络关键路径的信息，它监听网络上的所有数据包和流量，分析可疑现象**

IDS的工作原理

- **第一步：信息收集**
  - **系统、网络、数据、以及用户的状态和行为**
  - **日志文件**
  - **目录和文件的异常改变**
  - **程序执行的异常改变**
  - **物理形式入侵**
- **第二步：数据分析**
  - **模式匹配：实时入侵检测**
  - **统计分析：实时入侵检测**
  - **完整性分析：事后分析**

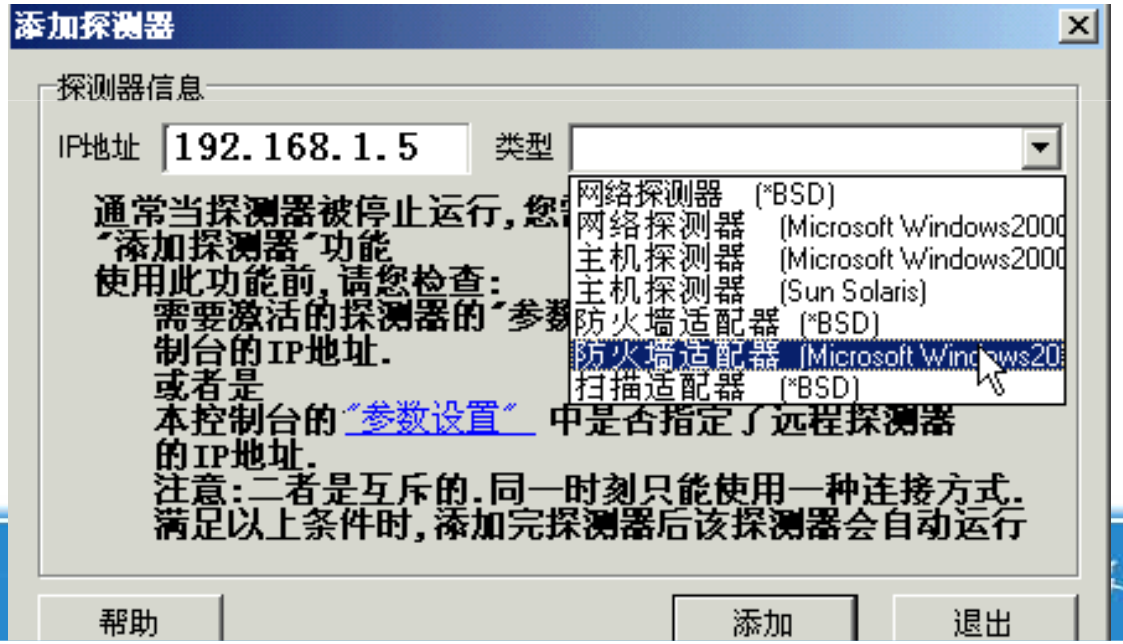


IDS的工作原理

- **第三步：响应，包括切断网络连接、记录事件和报警等**
  - **被动响应**
    - **将分析结果记录在日志文件中，并产生相应的报告**
  - **主动响应**
    - **触发警报：如在系统管理员的桌面上产生一个告警标志位，向系统管理员发送传呼或电子邮件等等**
    - **修改入侵检测系统或目标系统，如终止进程、切断攻击者的网络连接，或更改防火墙配置等**

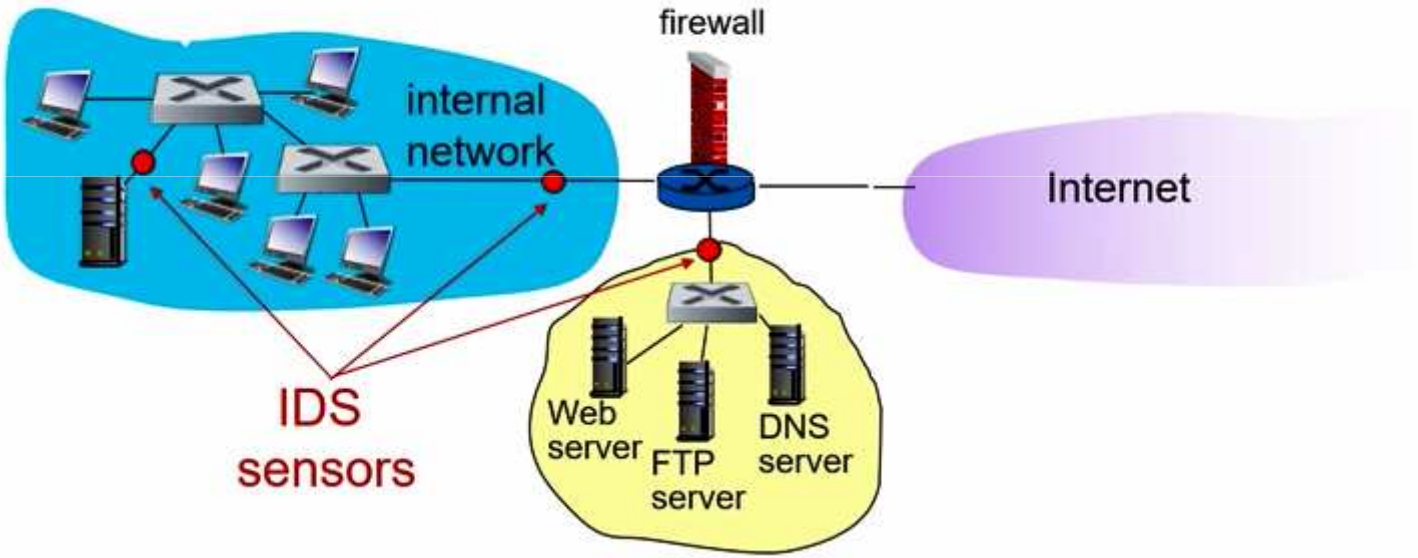
入侵检测系统BlackICE

- 以后台服务的方式运行
- 前端有一个控制台可以进行各种报警和修改程序的配置，界面很简洁
- 内置了**应用层的入侵检测功能**，并且能够与自身的防火墙进行联动，可以自动阻断各种已知的网络攻击行为



IDS

- **多个IDSs:在不同网络位置同时安放不同类别的IDS检测系统**



IDS面临的挑战

- **误报**
  - **正常数据 到 非法数据**
  - **误报是入侵检测系统最头疼的问题，攻击者利用包的结构伪造无威胁的“正常”假警报，而诱导没有警觉性的管理员人把入侵检测系统关掉**
  - **一个有效的入侵检测系统应限制误报出现的次数，但同时又能有效截击**

IDS面临的挑战

- **漏报**
  - **非法数据 到 正常数据**
  - **漏报也是入侵检测系统困难问题，过于严厉的检测规则可以减少漏报却不能杜绝。**
  - **漏报和误报可同时存在**
  - **关键在于未能把握入侵的特征**
  - **一个有效的入侵检测系统应限制漏报出现的次数**

基于异常的检测

- 建立正常活动特征模式
- 制定偏离正常特征许可阈值
- 模式匹配
- 难点在于匹配方式和阈值的确定
- 特征库需要不断更新
- 难点在于如何降低误报

基于误用的检测

- 建立异常活动特征模式
- 制定匹配异常特征的许可阈值
- 模式匹配
- 难点在于匹配方式和阈值的确定
- 特征库需要不断更新
- 难点在于如何降低漏报

志存高远 责任为先

感谢聆听

网址：www.jxust. edu.cn
邮编：341000