网络安全 - 防火墙技术

曹越

国家网络安全学院

武汉大学

yue.cao@whu.edu.cn

防火墙技术的概述

防火墙的分类

防火墙的构建

示例

防火墙技术的概述

防火墙的分类

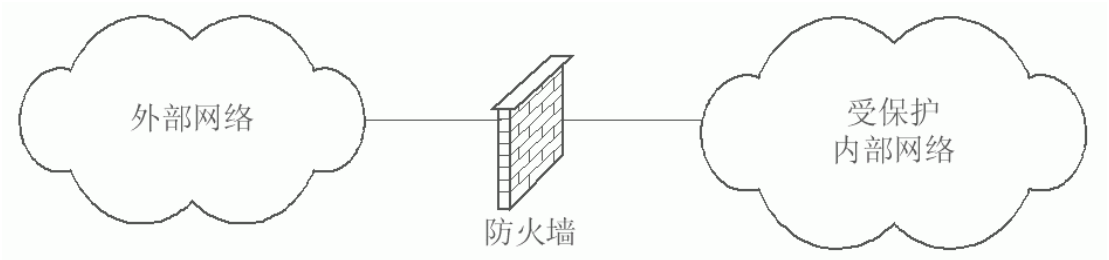
防火墙的构建

示例

防火墙技术概述 - 1

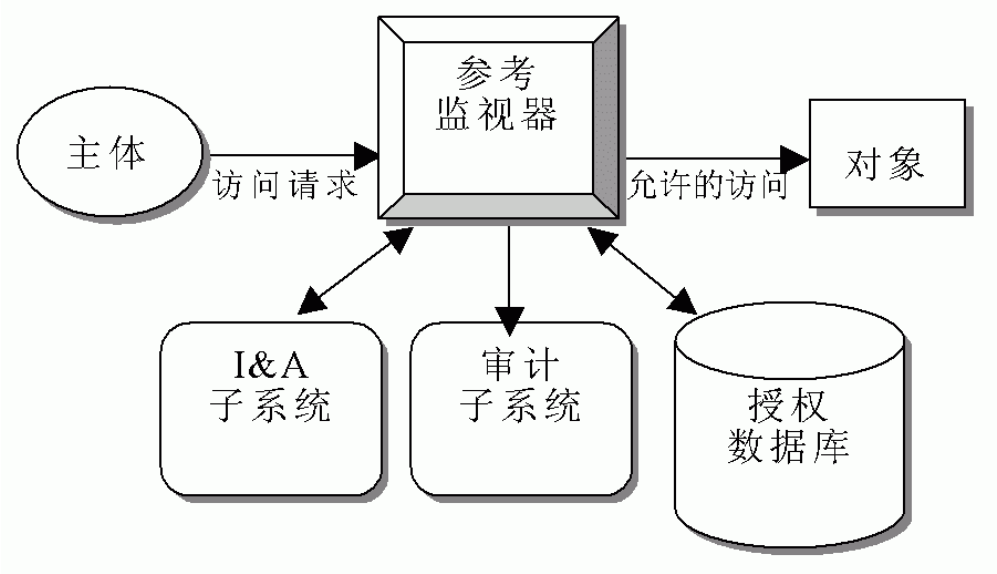
防火墙技术属于典型的静态安全技术，该类技术用于逻辑隔离内部网络与外部网络

通过数据包过滤与应用层代理等方法实现内外网络之间信息的受控传递，从而达到保护内部网络的目的

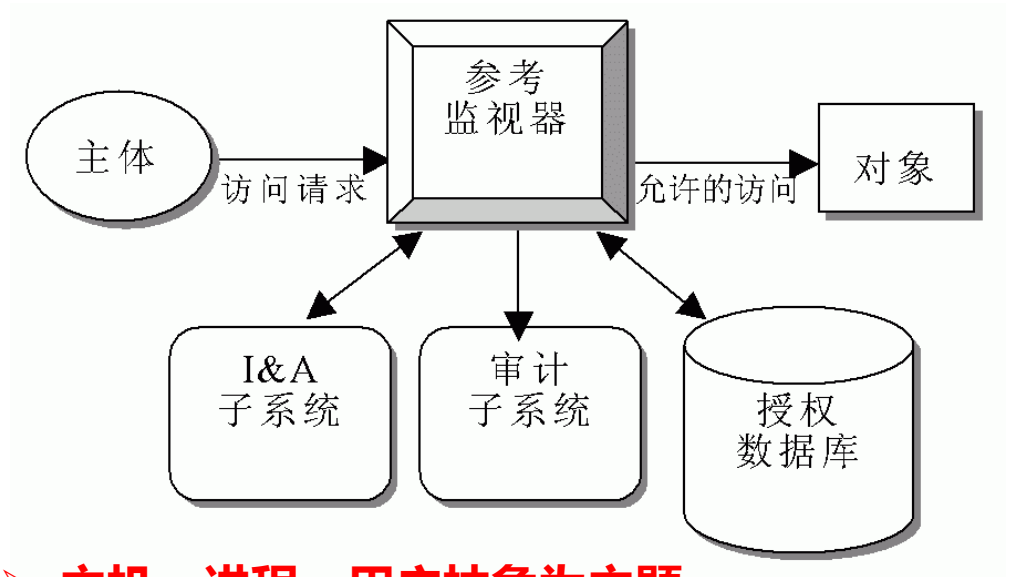


为了防止火灾蔓延，而在建筑物之间修筑的矮墙

经典安全模型



经典安全模型



- 主机、进程、用户抽象为主题
- 数据包传递抽象为访问
- 过滤规则抽象为?
- 防火墙抽象为?
- 用户认证抽象为?
- 过滤、日志抽象为?

防火墙规则 - 1

防火墙的安全规则由匹配条件与处理方式两个部分共同构成

其中匹配条件是一些逻辑表达式，根据信息中的特定值域可以计算出逻辑表达式的值为真（True）或假（False）

如果信息使匹配条件的逻辑表达式为真，则说明该信息与当前规则匹配

防火墙规则 - 2

信息一旦与规则匹配，就必须采用规则中的处理方式进行处理

处理方式主要包括

- Accept：允许数据包或信息通过
- Reject：拒绝数据包或信息通过，并且通知信息源该信息被禁止
- Drop：直接将数据包或信息丢弃，并且不通知信息源

防火墙规则 - 3

基本原则

- **“默认拒绝”原则**
- **“默认允许”原则**

现有的防火墙产品大多基于第一种规则

- **没有匹配，默认非安全流通过，因此拒绝，但是限制了用户服务种类、缺乏便利性**
- **默认允许，由于只考虑accept，未考虑reject、drop，缺乏安全性**

防火墙规则 - 4

匹配条件

- 网络层
  - IP源地址、IP目的地址、协议
- 传输层
  - 源端口 、目的端口
- 应用层
  - 根据各种具体应用而定
- 基于信息流向的匹配条件
  - 向内、向外

防火墙规则 - 5

防火墙的基本原理是对内部网络与外部网络之间的信息流传递进行控制

控制的功能是通过在防火墙中预先设定一定的安全规则（也称为安全策略）实现的

防火墙技术的概述

防火墙的分类

防火墙的构建

示例

防火墙分类 - 按防范领域分类

个人防火墙

- **禁止Internet文件共享 、隐藏端口 、过滤IP信息流 、控制Internet应用程序 、警告和日志 、漏洞检查**
- **保护主机**

网络防火墙

- **对网络数据流进行分析，并按照规则进行过滤**
- **保护内网、外网**

防火墙分类 - 按实现的方式分类

软件防火墙

- **一般基于某个操作系统平台开发，直接在计算机上进行软件的安装和配置。**

硬件防火墙

- **把“软件防火墙”嵌入在硬件中，把“防火墙程序”加入到芯片里面，由硬件执行这些功能，从而减少计算机或服务器的CPU负担。**

指标，内网控制，稳定性，工作原理

防火墙分类 - 按实现技术分类

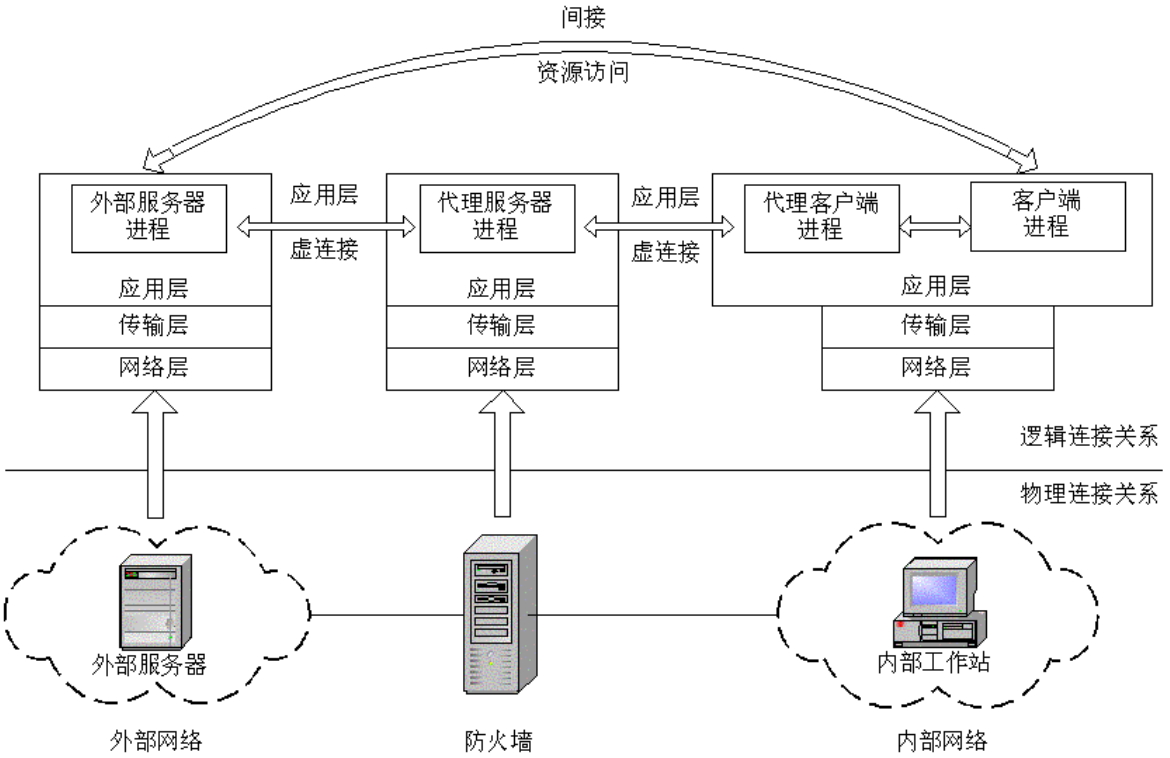
数据包过滤

- 在系统进行IP数据包转发时设置访问控制列表，访问控制列表主要由各种规则组成。
- 数据包过滤的规则主要采用网络层与传输层匹配条件

应用层代理

- 应用层代理是指运行在防火墙主机上的特殊应用程序或者服务器程序
- 这些程序根据安全策略接受用户对网络的请求，并在用户访问应用信息时依据预先设定的应用协议安全规则进行信息过滤

应用层代理示意图


间接
资源访问
外部服务器进程
应用层
虚连接
代理服务器进程
应用层
虚连接
代理客户端进程
客户端进程
应用层
应用层
传输层
网络层
应用层
传输层
网络层
应用层
传输层
网络层
逻辑连接关系
物理连接关系
外部服务器
内部工作站
外部网络
防火墙
内部网络

数据包过滤 vs 应用层代理

数据包过滤

- **优：服务无关、对用户透明**
- **劣：过滤规则复杂 、正确性难以检测、容易形成瓶颈**

应用层代理

- **优：传输层以下数据包无法通过防火墙主机在内外网传递**
- **优：内网安全性较高 、Cache机制可以提高信息访问效率、支持用户认证 、支持基于内容的信息过滤**
- **劣：必须对每种应用提供代理服务和代理客户端、实时性差**

防火墙常见术语

堡垒机

- 直接面向外部用户供给的主机系统，比如内网边缘
- 提供服务越少越好，降低被攻击可能性

双重宿主主机

- 实现多个网络互联的关键设备
- 多个网络接口?
- 链路层、网络层?

周边网络

- 内网、外网之间的网络
- 对外提供服务，防止周边网络，不需进入内网

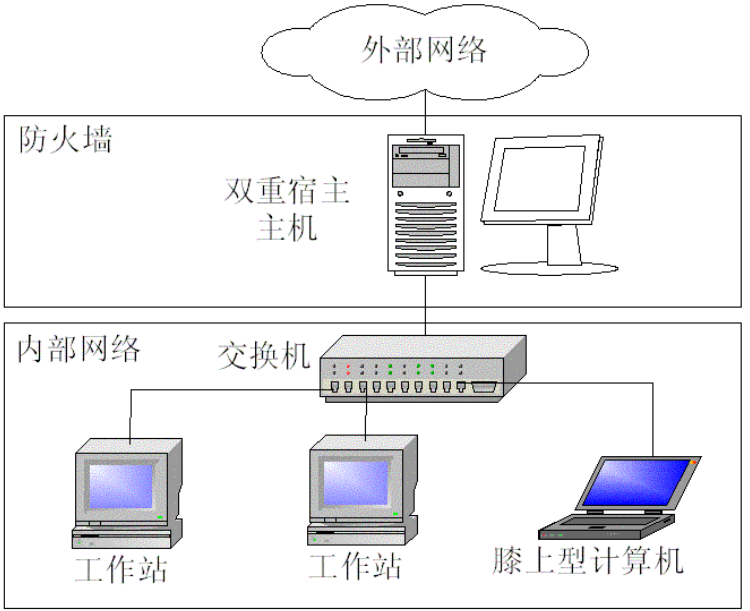
经典防火墙体系结构 - 双重宿主主机体系结构

内外网数据转发被禁止

通过代理方式访问外网

缺点?

- **主机开销**
- **抗攻击能力弱**



经典防火墙体系结构 - 被屏蔽主机体系结构

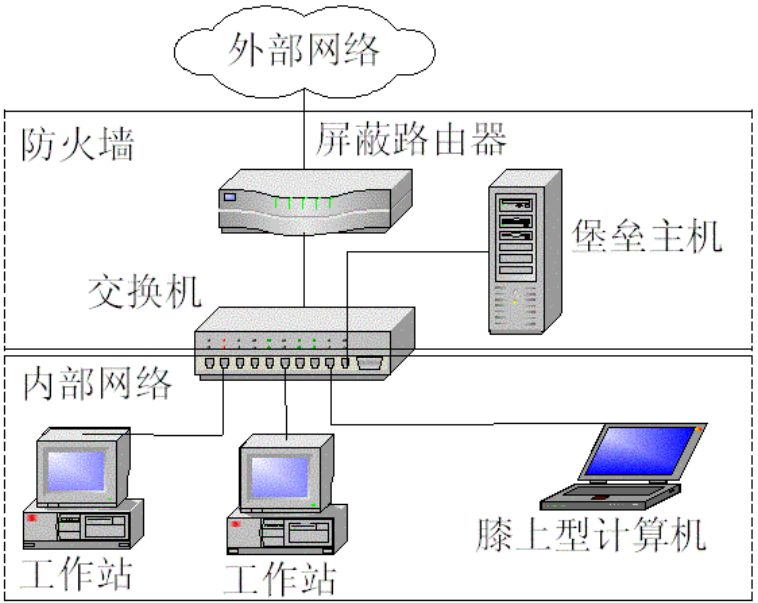
仅堡垒主机可连外网

比双重体系更安全

内网访问外网更方便

减轻堡垒主机压力

缺点?

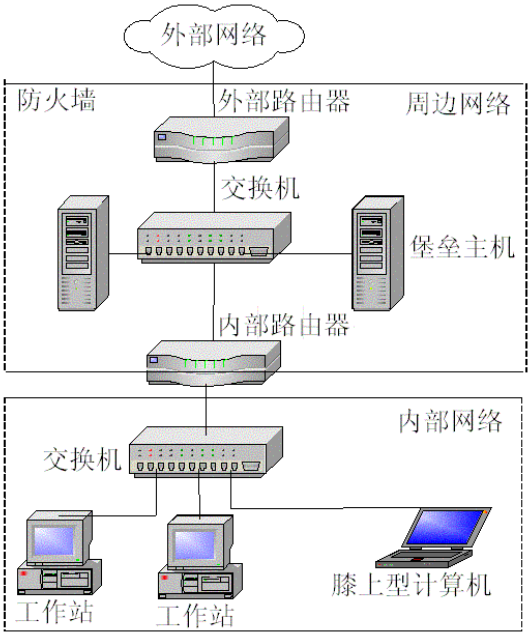


经典防火墙体系结构 - 被屏蔽子网体系结构

通过两台路由器包围防护堡垒主机

外部用户访问服务器无需进入内网

即使攻陷了主机，无法窃听周边网络



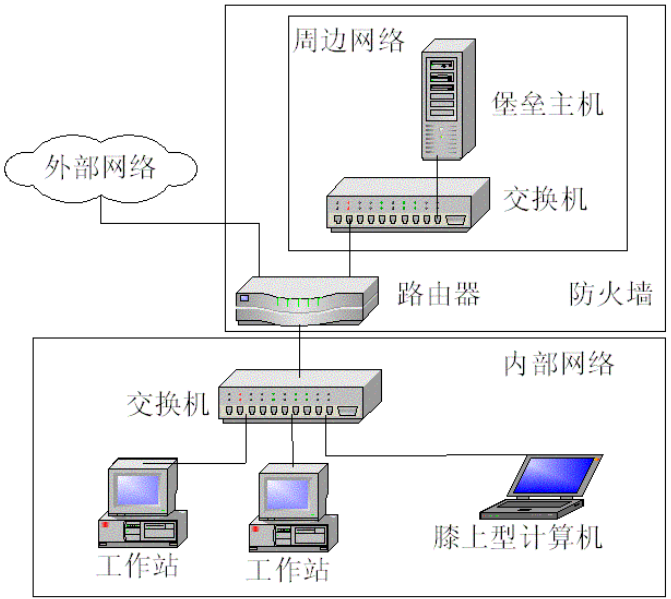
外部路由器不对周边网络数据过滤
内部路由器复制外部路由器规则

扩展防火墙体系结构 - 合并内部和外部路由器

内部路由器，外部路由合并为一个

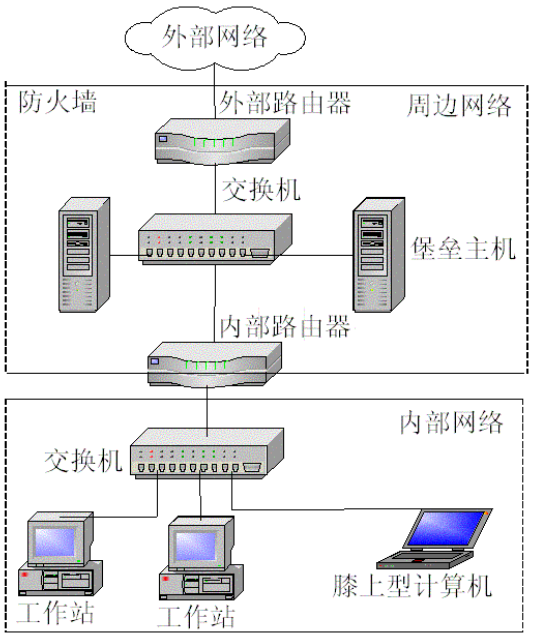
合并路由器的过滤规则变化

单点失效隐患大

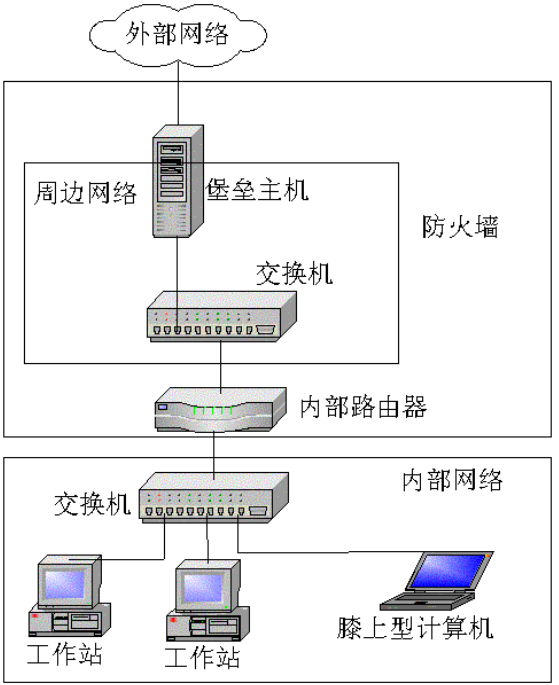


扩展防火墙体系结构 – 合并堡垒主机和外部路由器

屏蔽子网结构

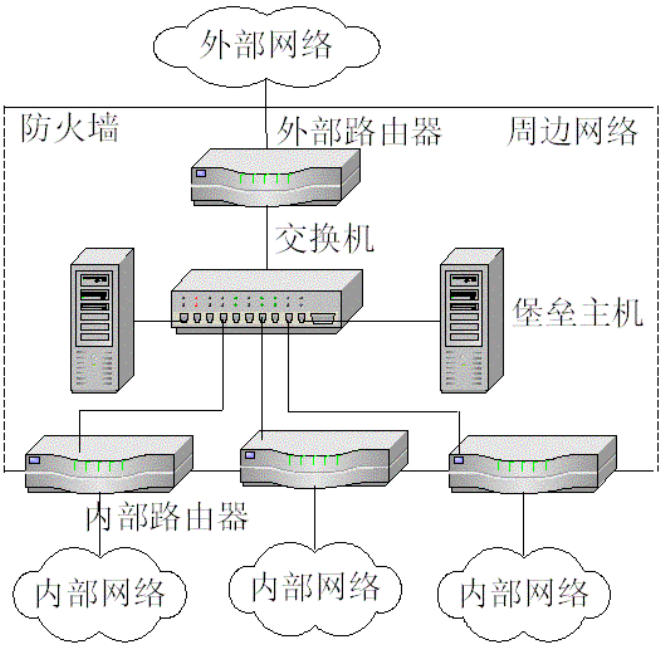


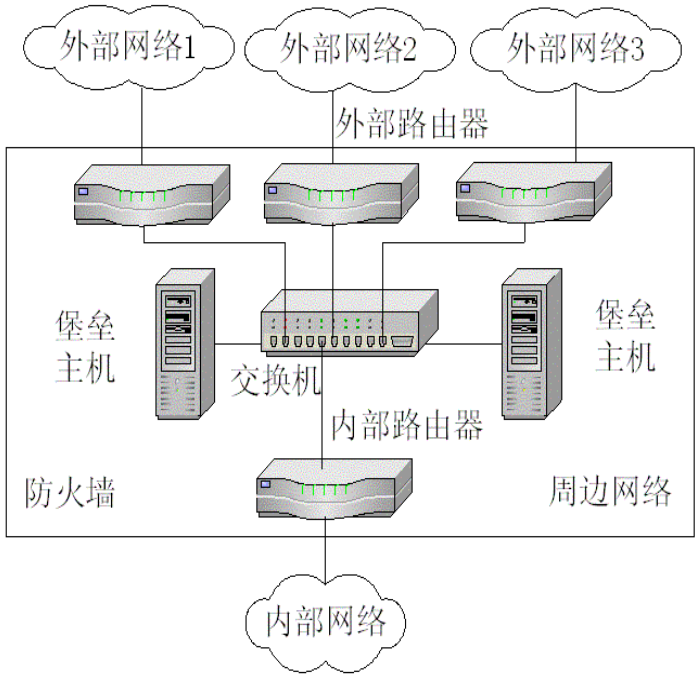
合并堡垒主机和外部路由器



堡垒机被攻破，可监听周边网络

扩展防火墙体系结构 - 多台内/外部路由器

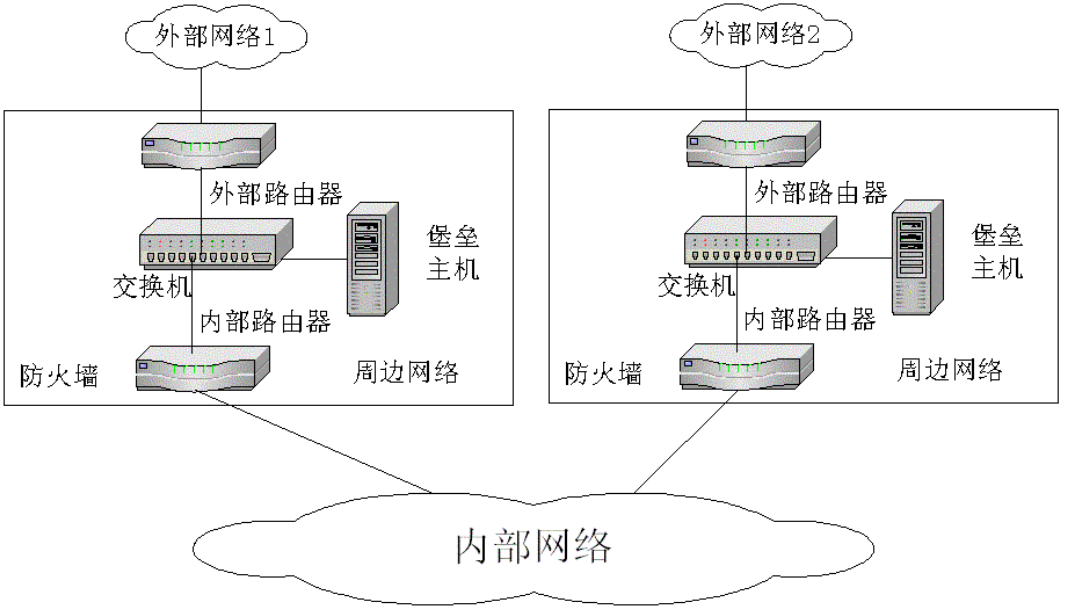




坏处？周边网络被监听

好处？内外网不需要交流，采用合并方式节约开销

扩展防火墙体系结构 - 多个周边网络



保证内外网络不存在单点失效

防火墙技术的概述

防火墙的分类

防火墙的构建

示例

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

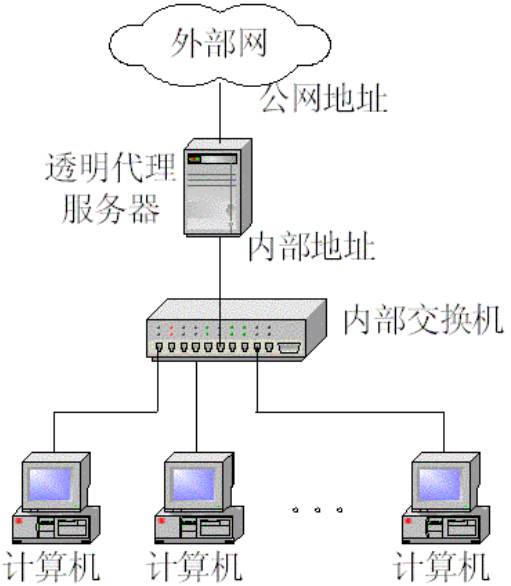
构建防火墙

选择防火墙体系结构

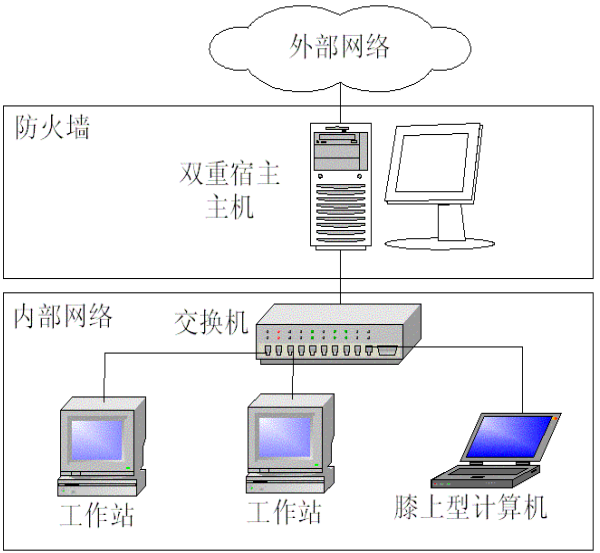
- **小型网络**
- **中型网络**
- **大型网络**

选择防火墙体系结构 – 小型网络 1

透明代理



双重宿主主机

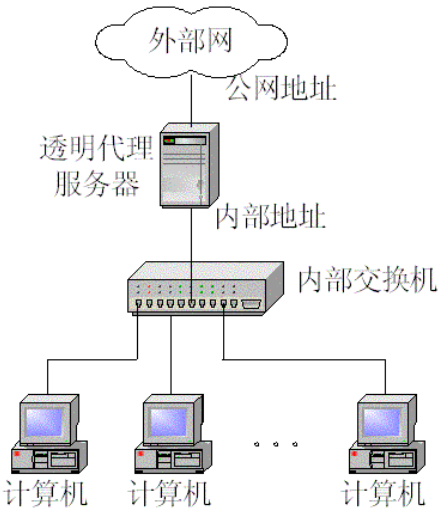


由于网络规模较小，添加专门的路由器、堡垒主机无法实施

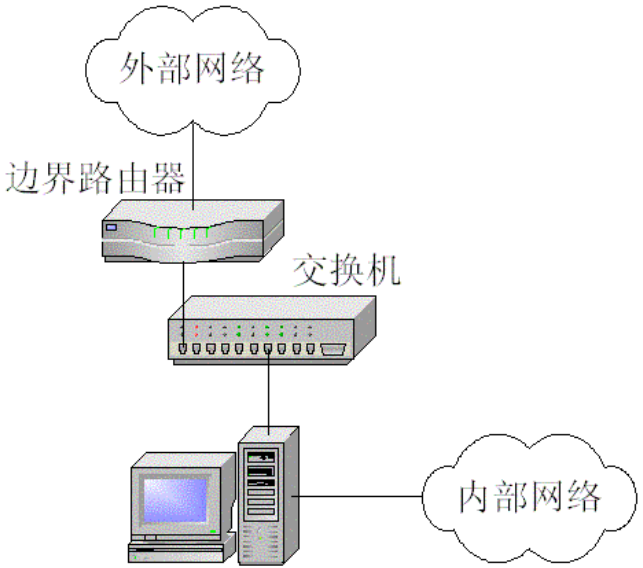
选择防火墙体系结构 – 小型网络 2

透明代理的特点

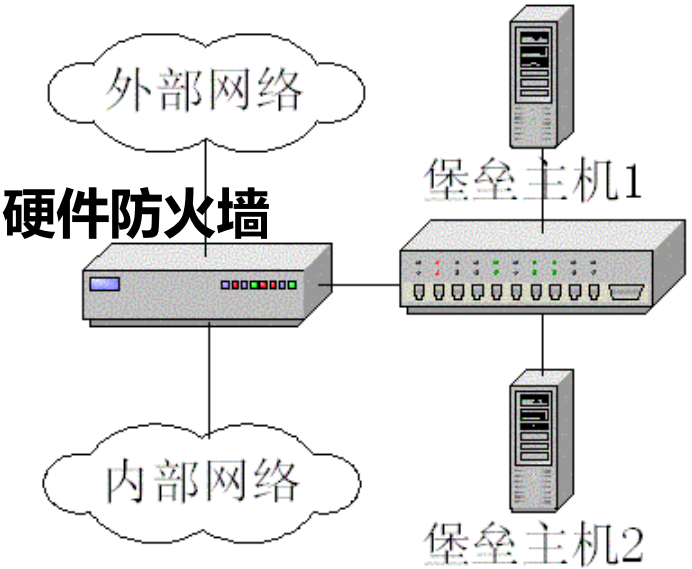
- **两个网络接口，外部接口直接与外部网络连接、内部接口直接与内部网络连接**
- **透明代理不向外提供服务，仅地址转换**
- **WWW缓存功能**
- **NAT网络过滤原则**
- **代理账号、应用层过滤**



选择防火墙体系结构 – 中型网络 3



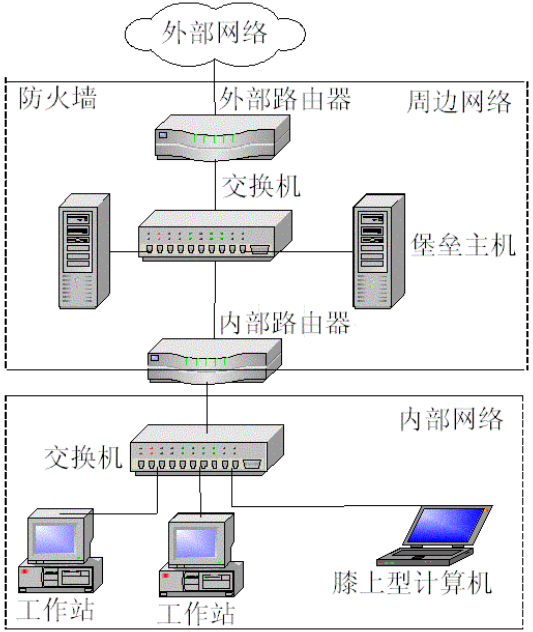
软件防火墙



选择防火墙体系结构 – 中型网络 4

软件防火墙的特点

- 边界路由器只运行路由算法，对外声明内部网络不存在
- 边界路由的简单访问控制方法
- 数据包过滤在软件防火墙实现
- 软件防火墙实现内外访问

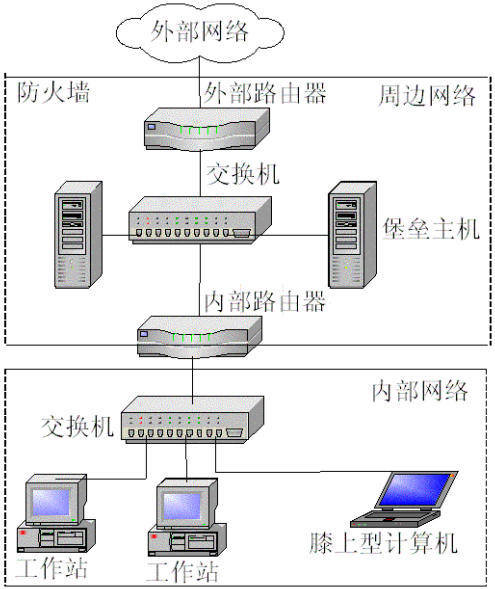


被屏蔽子网中合并内部路由器+堡垒主机

选择防火墙体系结构 – 中型网络 5

硬件防火墙的特点

- **被屏蔽子网体系结构的扩展**
- **过滤功能和应用层代理在硬件防火墙实现**
- **对外提供服务的主机在周边网络**

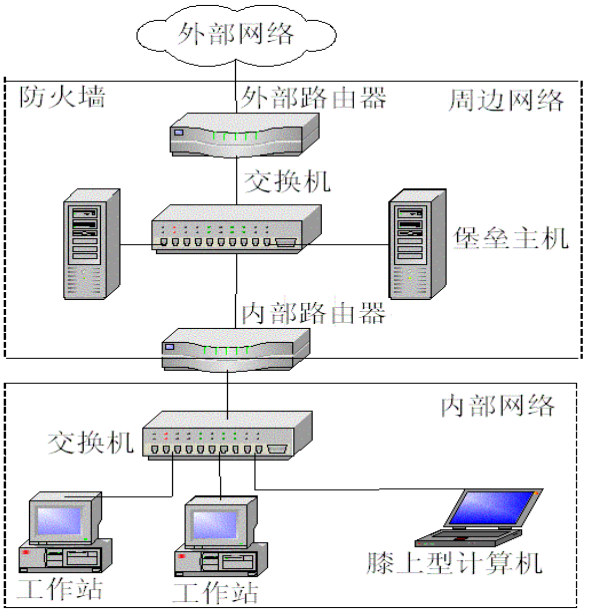


被屏蔽子网中合并内外路由器

选择防火墙体系结构 – 大型网络

大型网络

- 被屏蔽子网



构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙 - 安装外部路由器 1

1. 连接线路
2. 配置网络接口
3. 测试网络连通性
4. 配置路由算法
5. 路由器的访问控制

构建防火墙 - 安装外部路由器 2

连接线路

- **保证设备与外部网络、周边网络（或内部网络）的线路连接正常**
- **由于外部路由器的外部网络接口一般较为复杂，可能会使用XDSL、ISDN、ATM等广域网、城域网协议与接口，必须首先完成线路申请、线路连接等前期工作**

构建防火墙 - 安装外部路由器 3

配置网络接口

- **配置网络接口的工作主要包括IP地址、子网掩码、开启网络接口等**
- **在配置完毕后需要进行网络接口连通性测试**
- **必需保证路由器上的测试程序可以通过外部网络接口访问外部网络，通过内部网络接口可以访问周边网络（或内部网络）**

构建防火墙 - 安装外部路由器 4

测试网络连通性

- **在不添加访问控制规则的情况下，用户应该能够通过路由器从周边网络访问外部网络，同样从外部网络访问周边网络**

构建防火墙 - 安装外部路由器 5

配置路由算法

- **为让外部路由器能够参与外部网络的路由运算，必需在外部路由器上配置相应的动态路由算法或静态路由，同时将外部网络访问内部网络的下一跳地址指向内部路由器或双重宿主主机**
- **OSPF、BGP…**

构建防火墙 - 安装外部路由器 6

路由器的访问控制

- **在路由算法配置完毕后，需要配置针对路由器自身的访问控制，限制路由器对外部提供Telnet等服务，将这些服务的服务范围限制在内部网络中的管理员使用的计算机**

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙 - 安装内部路由器 1

连接线路

- 内部网络一般比较单纯，多局限于以太系列网络，线路连接较为简单

配置路由算法

- 内部路由器不参与外部路由算法，也不参与内部网络中各子网间的路由转发，因此只需要通过**静态路由**配置外部网络、内部网络、周边网络之间的数据包转发

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙 - 安装堡垒机 1

选择合适的物理位置

- 要求堡垒主机必须存放在安全措施完善的机房内部，同时要保证机房的供电、通风、恒温、监控条件良好

选择合适的硬件设备

- 选择堡垒主机一定要以满足服务性能需求作为最终依据，过高、过低的配置都是不合时宜的
- WWW内存需求、FTP存储空间需求

构建防火墙 - 安装堡垒机 2

选择合适的操作系统

- 堡垒主机操作系统的选择必须考虑到安全性、高效性等方面的因素
- Unix、Windows

注意堡垒主机的网络接入位置

- 堡垒主机应该放置于不涉及敏感信息的位置（周边网络）
- 不应该采用集线器这样的共享设备（防止监听）

构建防火墙 - 安装堡垒机 3

设置堡垒主机提供的服务

- **关闭不需要的服务**
- **对提供的服务需要添加一定的安全措施，包括用户IP限制、DOS攻击屏蔽等**
- **在堡垒主机上禁止使用用户账号**

核查堡垒主机的安全保障体制

- **核查的手段主要是在主机上运行相应的安全分析软件或者漏洞扫描程序，在发现堡垒主机的安全漏洞后应该及时排除**

维护与备份

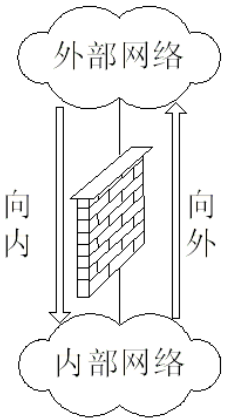
构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

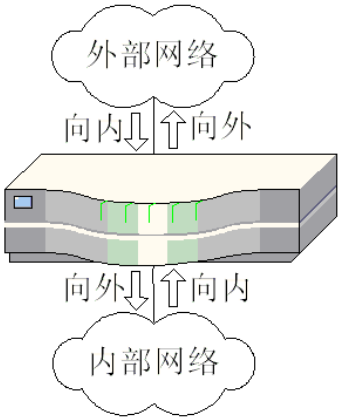
构建防火墙 - 设置数据包过滤规则 1

首先需要确定设置数据包过滤规则设备对“向内”与“向外”的具体概念

- 要尽可能地对双向的数据包都进行限制
- 采用“默认拒绝”
- 脱机编辑过滤规则



（a）采用软件、硬件防火墙或堡垒主机



（b）采用路由器
向内=接收、向外=发送

构建防火墙 - 设置数据包过滤规则 2

数据包过滤的方式

- 堡垒主机

序号	流向	源地址	目的地址	动作
1	向内	202.102.0.0/255.255.0.0	203.104.64.0/255.255.240.0	Accept
2	向外	203.104.64.0/255.255.240.0	202.102.0.0/255.255.0.0	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.0/255.255.255.0	Accept
4	向外	203.104.64.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
5	向内	0.0.0.0/0.0.0.0	203.104.65.0/255.255.255.0	Accept
6	向外	203.104.65.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
7	--	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject

构建防火墙 - 设置数据包过滤规则 3

数据包过滤的方式

- 服务过滤规则

FTP 20，21
WWW 80
DNS 53
1024以下为系统专用端口

序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	0.0.0.0/0.0.0.0	203.104.64.32	TCP	>1023	21	Accept
2	向外	203.104.64.32	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	20	Accept
4	向外	203.104.64.32	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
5	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	80	Accept
6	向外	203.104.64.100	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
7	向内	202.102.22.66	203.104.64.2	UDP	53	53	Accept
8	向外	203.104.64.2	202.102.22.66	UDP	53	53	Accept
9	--	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

构建防火墙 - 设置数据包过滤规则 4

数据包过滤的方式

- **路由器地址过滤规则**

路由器外部接口				
序号	流向	源地址	目的地址	动作
1	向内	202.102.0.0/255.255.0.0	203.104.64.0/255.255.240.0	Accept
2	向内	0.0.0.0/0.0.0.0	203.104.64.0/255.255.255.0	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.65.0/255.255.255.0	Accept
4	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject
路由器**内部**接口				
1	向内	203.104.64.0/255.255.240.0	202.102.0.0/255.255.0.0	Accept
2	向内	203.104.64.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
3	向内	203.104.65.0/255.255.255.0	0.0.0.0/0.0.0.0	Accept
4	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	Reject

构建防火墙 - 设置数据包过滤规则 5

数据包过

- **路由**

路由器外部接口							
序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	0.0.0.0/0.0.0.0	203.104.64.32	TCP	>1023	21	Accept
2	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	20	Accept
3	向内	0.0.0.0/0.0.0.0	203.104.64.100	TCP	>1023	80	Accept
4	向内	202.102.22.66	203.104.64.2	UDP	53	53	Accept
5	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
路由器内部接口							
序号	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	向内	203.104.64.32	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
2	向内	203.104.64.32	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
3	向内	203.104.64.100	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
4	向内	203.104.64.2	202.102.22.66	UDP	53	53	Accept
5	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

构建防火墙 - 设置数据包过滤规则 5

注意包过滤规则的顺序

- **获得更高的过滤效率**
- **避免出现漏洞**

设置网络服务

- **对外提供正常的服务**

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙 - 设置代理系统 1

可以直接访问外部网络，又可以通过代理访问

设置代理服务器

- 尽量选择较为成熟、稳定的产品或版本
- 尽量避免根据用户账号提供代理服务的方式
- 应该只对一定IP地址范围内的主机提供服务
- 禁用远程配置，只允许在本机实施配置
- 定期升级，并通过相应的扫描软件及早发现代理服务配置的漏洞

构建防火墙 - 设置代理系统 2

设置代理客户端

- **使用定制客户端软件**
- **使用定制的用户过程**

构建防火墙的步骤

1. 选择防火墙体系结构
2. 安装外部路由器
3. 安装内部路由器
4. 安装堡垒主机
5. 设置数据包过滤规则
6. 设置代理系统
7. 检查防火墙运行效果

构建防火墙 - 检查防火墙运行效果

检查的内容包括

- 对外提供的服务
  - WWW、FTP、BBS、EMAIL
- 对内提供的服务
  - DNS等
- 网络访问
  - 检查过滤规则是否生效，并及早发现规则中存在的漏洞

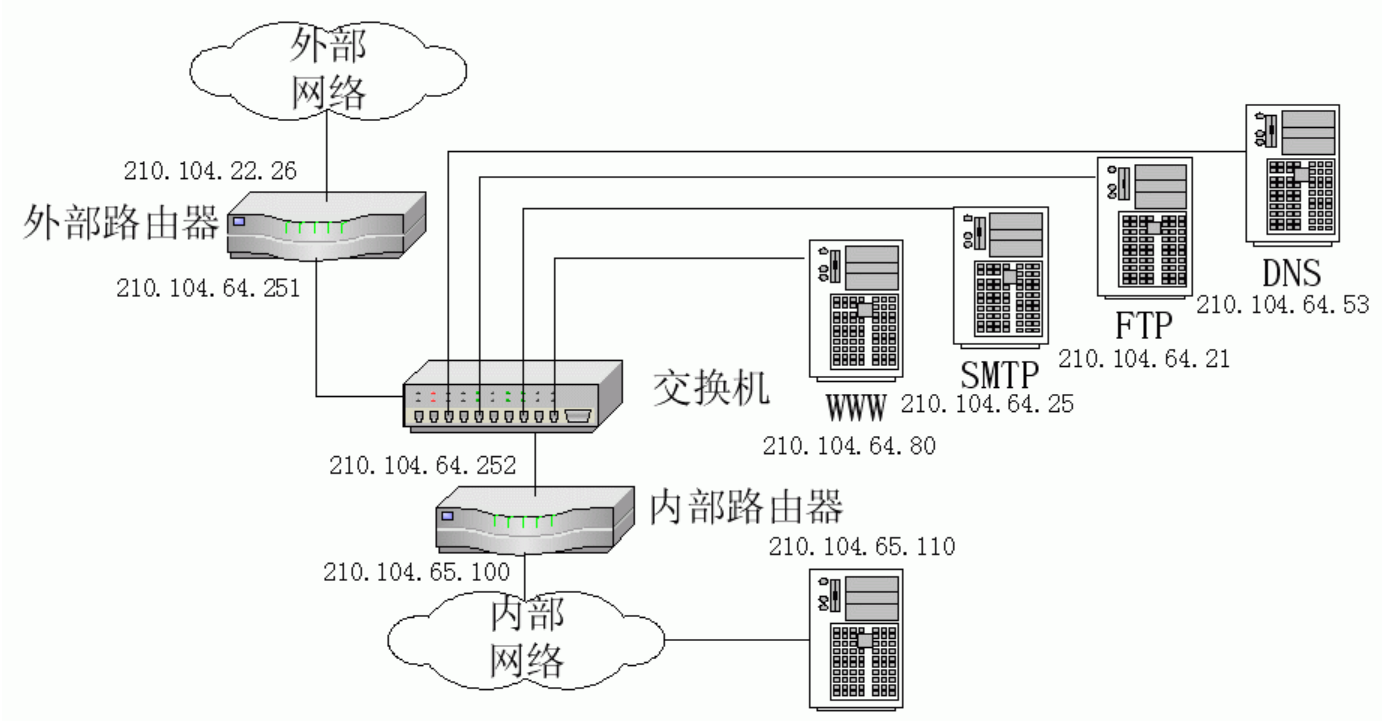
防火墙技术的概述

防火墙的分类

防火墙的构建

示例

示例 – 网络结构


外部
网络
210. 104. 22. 26
外部路由器
210. 104. 64. 251
交换机
210. 104. 64. 252
内部路由器
210. 104. 65. 100
内部
网络
210. 104. 65. 110
WWW
210. 104. 64. 80
SMTP
210. 104. 64. 25
FTP
210. 104. 64. 21
DNS
210. 104. 64. 53

示例 - Web服务过滤规则

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.80	TCP	>1023	80	Accept
2	外部	内网	向内	210.104.64.80	0.0.0.0/0.0.0.0	TCP	80	>1023	Accept
3	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.80	TCP	>1023	80	Accept
4	内部	外网	向内	210.104.64.80	210.104.65.0/ 255.255.255.0	TCP	80	>1023	Accept

示例 - FTP服务过滤规则

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.21	TCP	>1023	21	Accept
2	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.21	TCP	>1023	20	Accept
3	外部	内网	向内	210.104.64.21	0.0.0.0/0.0.0.0	TCP	21	>1023	Accept
4	外部	内网	向内	210.104.64.21	0.0.0.0/0.0.0.0	TCP	20	>1023	Accept
5	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.21	TCP	>1023	21	Accept
6	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.21	TCP	>1023	20	Accept
7	内部	外网	向内	210.104.64.21	210.104.65.0/ 255.255.255.0	TCP	21	>1023	Accept
8	内部	外网	向内	210.104.64.21	210.104.65.0/ 255.255.255.0	TCP	20	>1023	Accept

示例 - SMTP服务过滤规则

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.25	TCP	25	25	Accept
2	外部	内网	向内	210.104.64.25	0.0.0.0/0.0.0.0	TCP	25	25	Accept
3	内部	外网	向内	210.104.64.25	210.104.65.110	TCP	25	25	Accept
4	内部	内网	向内	210.104.65.110	210.104.64.25	TCP	25	25	Accept
5	内部	内网	向内	210.104.65.0/ 255.255.255.0	210.104.64.25	TCP	>1023	25	Accept
6	内部	外网	向内	210.104.64.25	210.104.65.0/ 255.255.255.0	TCP	25	>1023	Accept

构建防火墙 - DNS服务过滤规则

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.53	UDP	53	53	Accept
2	外部	内网	向内	210.104.64.53	0.0.0.0/0.0.0.0	UDP	53	53	Accept
3	外部	外网	向内	0.0.0.0/0.0.0.0	210.104.64.53	UDP	>1023	53	Drop
4	外部	内网	向内	210.104.64.53	0.0.0.0/0.0.0.0	UDP	53	>1023	Drop
5	内部	内网	向内	210.104.65.0/255.255.255.0	210.104.64.53	UDP	>1023	53	Accept
6	内部	外网	向内	210.104.64.53	210.104.65.0/255.255.255.0	UDP	53	>1023	Accept

示例 - 默认拒绝过滤规则

序号	路由器	接口	方向	源地址	目标地址	协议	源端口	目标端口	动作
1	外部	外网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
2	外部	内网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
3	内部	外网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject
4	内部	内网	向内	0.0.0.0/0.0.0.0	0.0.0.0/0.0.0.0	ANY	ANY	ANY	Reject

思考题

1. 防火墙规则的处理方式中，“Reject”与“Drop”的区别是什么?

2. 防火墙体系结构

3. 构建防火墙步骤

4. 如果防火墙允许周边网络上的主机访问内部网络上的任何基于TCP协议的服务，而禁止外部网络访问周边网络上的任何基于TCP协议的服务，给出实现的思路?