第7章　网络防御

罗文坚

主要内容

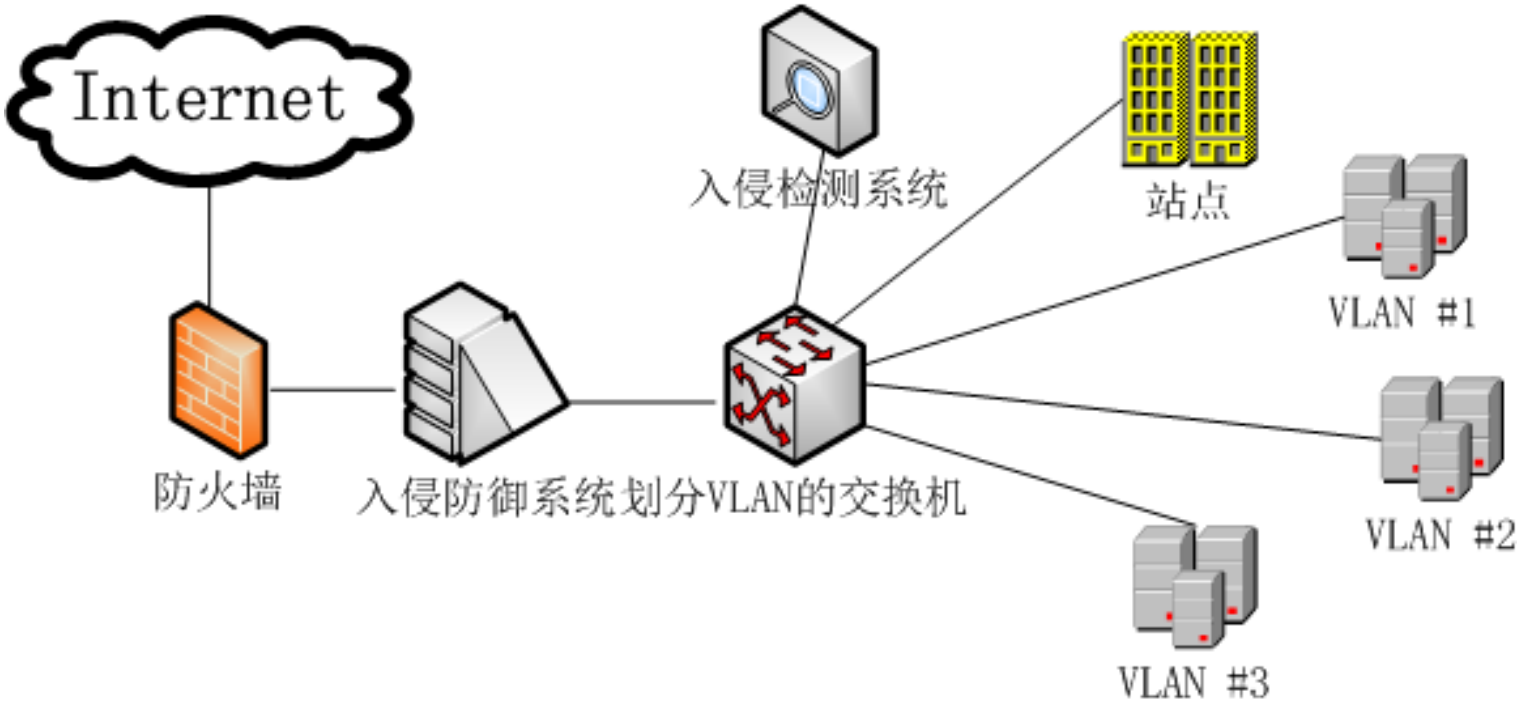
- 7.1 概述
- 7.2 防火墙
- 7.3 入侵检测系统
- 7.4 网络防御的新技术

概述

- 网络防御是一个综合性的安全工程，不是几个网络安全产品能够完成的任务。
  - 防御需要解决多层面的问题，除了安全技术之外，安全管理也十分重要。
  - 实际上，提高用户群的安全防范意识、加强安全管理所能起到效果远远高于应用几个网络安全产品。

- 从技术层面上看，网络安全防御体系应该是多层次、纵深型。
  - 这种防御体系可以有效地增加入侵攻击者被检测到的风险，同时降低攻击的成功几率，从而能够较好地防御各种网络入侵行为。
  - 目前，网络安全防御技术主要包括防火墙、入侵检测系统、VLAN、防病毒技术等。

网络安全防御体系



- **防火墙：**网络安全防御体系的**第一道防线**，是网络安全的网关设备。防火墙的工作机制是依据安全规则检查每一个通过防火墙的数据包，只有符合安全规则的数据包才能通过。

网络安全防御体系

- 入侵检测系统：一般部署在网络内部，对网络内部的数据进行检测。当发现具有攻击特征的数据报文时，发出报警信息。

- VLAN（Virtual Local Area Network，虚拟局域网）：将局域网中的各个节点，从逻辑上划分为多个网段（即VLAN），每一个VLAN都包含一组有着相同需求的工作站，与网络上形成的LAN有着相同的属性。
  - 任一个VLAN内部的广播和单播流量都不会转发到其他VLAN中，有助于控制流量、简化网络管理、提高网络的安全性。

- 防病毒系统主要包括两种形式：一种是基于网络的防病毒系统，另一种是目前广泛使用的主机防病毒软件。
  - 防病毒技术主要包括病毒检测引擎和病毒特征库两项核心技术，其中病毒检测引擎决定着系统的性能，而病毒特征库则与病毒检测的漏报率和误报率密切相关。

网络安全防御体系

- 网络入侵防御系统（IPS，Intrusion Prevention System）：可以看成是防火墙和入侵检测系统的融合。
  - 串接在网络关键路径上，保证受保护的网络的所有网络数据都经过IPS设备，类似于防火墙的部署。
  - 从工作机制上看，比较接近入侵检测系统，在抗躲避的处理、协议分析、攻击识别等过程中都包含了动态与静态检测的融合。
- 入侵管理系统（IMS，Intrusion Management System）：可以理解为过程管理，在入侵事件的各个阶段实施预测、检测、阻断、关联分析和系统维护等工作。
- 云安全：融合了并行处理、网格计算、未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中的特定数据和异常行为进行收集整理，并传送到云服务器端进行自动分析和处理，再把解决方案分发到每一个客户端。

主要内容

- 7.1 概述
- 7.2 防火墙
  - 7.2.1 防火墙概述
  - 7.2.2 防火墙的主要技术
  - 7.2.3 Netfilter/IPtables防火墙
- 7.3 入侵检测系统
- 7.4 网络防御的新技术

防火墙概述

- 防火墙指的是一个由软件和硬件设备组合而成、在内部网络和外部网络之间构造的安全保护屏障，从而保护内部网络免受外部非法用户的侵入。

- 简单地说，防火墙是位于两个或多个网络之间，执行访问控制策略的一个或一组系统，是一类防范措施的总称。

防火墙概述

- 防火墙设计目标是有效地控制内外网之间的网络数据流量，做到御敌于外。

- 防火墙的结构和部署考虑:
  ① 内网和外网之间的所有网络数据流必须经过防火墙。
    - 阻塞点可以理解为连通两个或多个网络的唯一路径上的点；当这个点被删除后，各网络之间不在连通。
  ② 只有符合安全政策的数据流才能通过防火墙。
    - 要求防火墙具有审计和管理的功能，具有可扩展性和健壮性。

防火墙分类

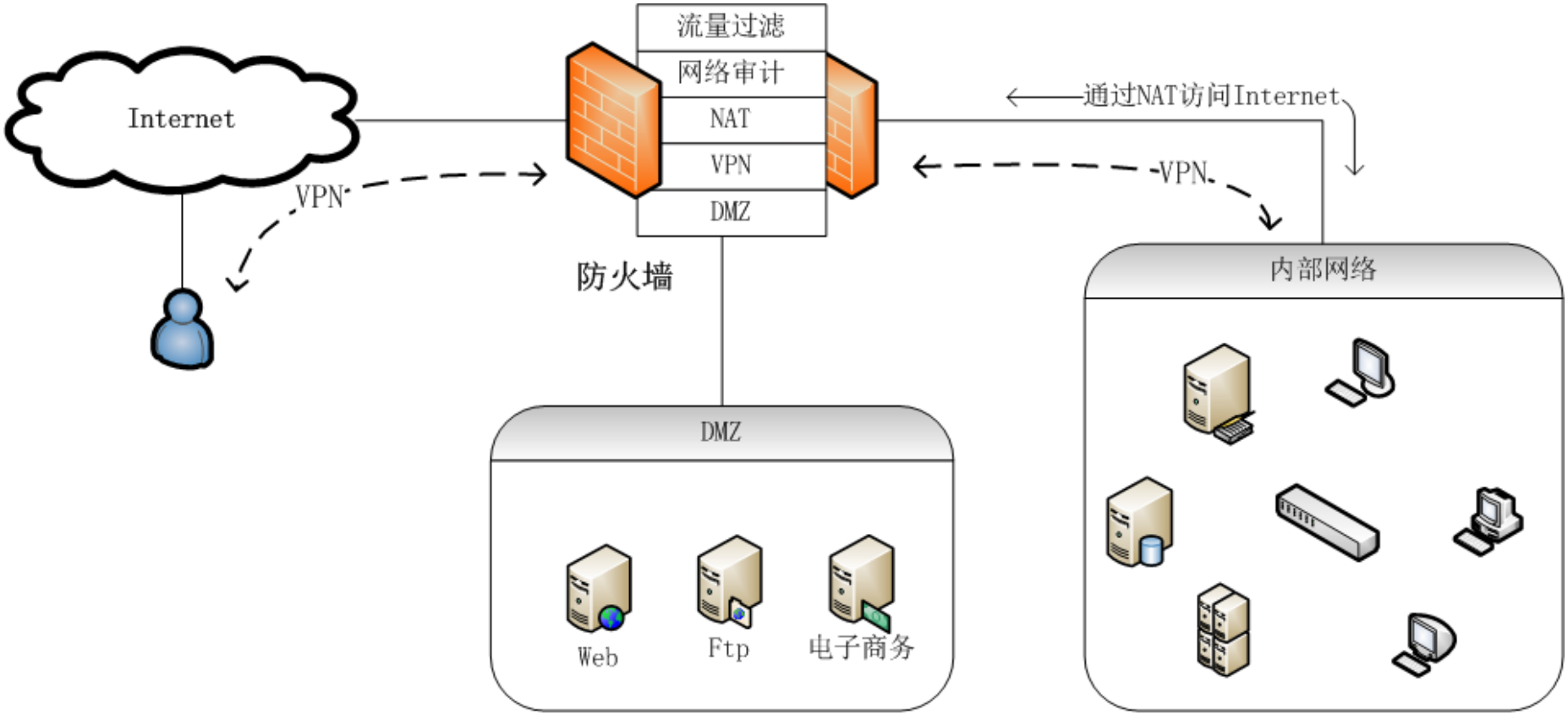
- 从应用对象上，分为企业防火墙和个人防火墙。
  - 企业防火墙的主要作用是保护整个企业网络免受外部网络的攻击。
  - 个人防火墙则是保护个人计算机系统的安全。

- 从存在形式上，可以分为硬件防火墙和软件防火墙。
  - 硬件防火墙采用特殊的硬件设备，有较高性能，可做为独立的设备部署；企业防火墙多数是硬件防火墙。
  - 软件防火墙是一套安装在某台计算机系统上，执行防护任务的安全软件；个人防火墙都是软件防火墙。

防火墙主要作用

- 网络流量过滤：通过在防火墙上进行安全规则配置，可以对流经防火墙的网络流量进行过滤。这是防火墙最主要的功能。
- 网络监控审计：防火墙记录访问并生成网络访问日志，提供网络使用情况的统计数据；发现可疑的网络访问时及时报警；将收集的信息提供给其他安全模块。
- 支持NAT部署：NAT（Network Address Translation，网络地址翻译）是用来缓解地址空间短缺的主要技术之一。
- 支持DMZ：DMZ（Demilitarized Zone，隔离区/非军事化区）是设立在非安全系统与安全系统之间的缓冲区，可以放置一些必须公开的服务器设施，如Web服务器。
- 支持VPN：通过VPN，企业可以将分布在各地的局域网有机地连成一个整体。

典型企业防火墙应用



该企业网络中，由于应用了防火墙，解决了网络流量过滤及审计、地址短缺、远程安全内网访问以及DMZ部署问题。

防火墙的局限性

1. 防火墙无法检测不经过防火墙的流量，如通过内部提供拨号服务接入公网的流量；

2. 防火墙不能防范来自内部人员的恶意攻击；

3. 防火墙不能阻止被病毒感染的和有害的程序或文件的传递，如木马；

4. 防火墙不能防止数据驱动式攻击，如一些缓冲区溢出攻击。

主要内容

- 7.1 概述
- 7.2 防火墙
  - 7.2.1 防火墙概述
  - 7.2.2 防火墙的主要技术
  - 7.2.3 Netfilter/IPtables防火墙
- 7.3 入侵检测系统
- 7.4 网络防御的新技术

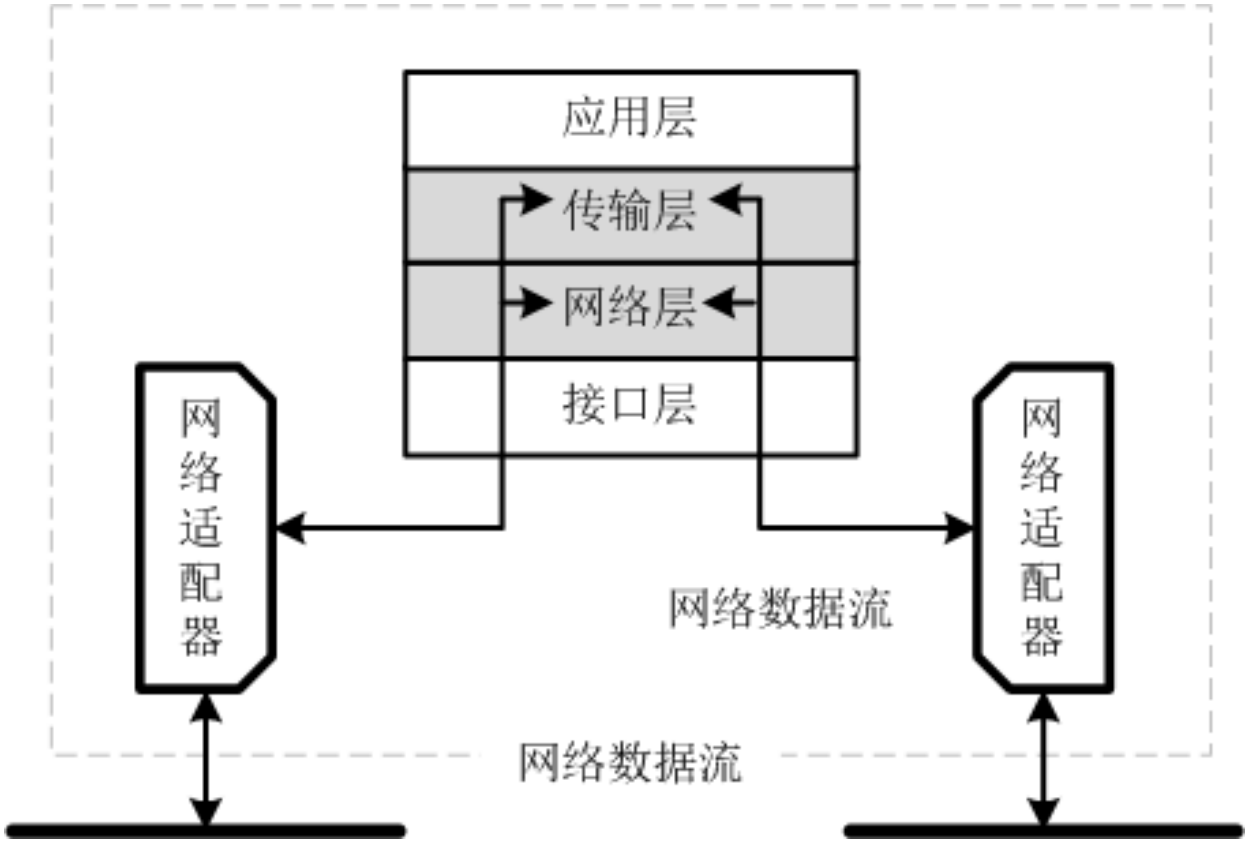
依据技术特征的防火墙分类

- 依据防火墙的技术特征，常见的防火墙可以分为：
  - 包过滤防火墙
  - 代理防火墙
  - 个人防火墙

- 这三类防火墙的侧重点不同，因而采用的技术路线也有较大的区别。

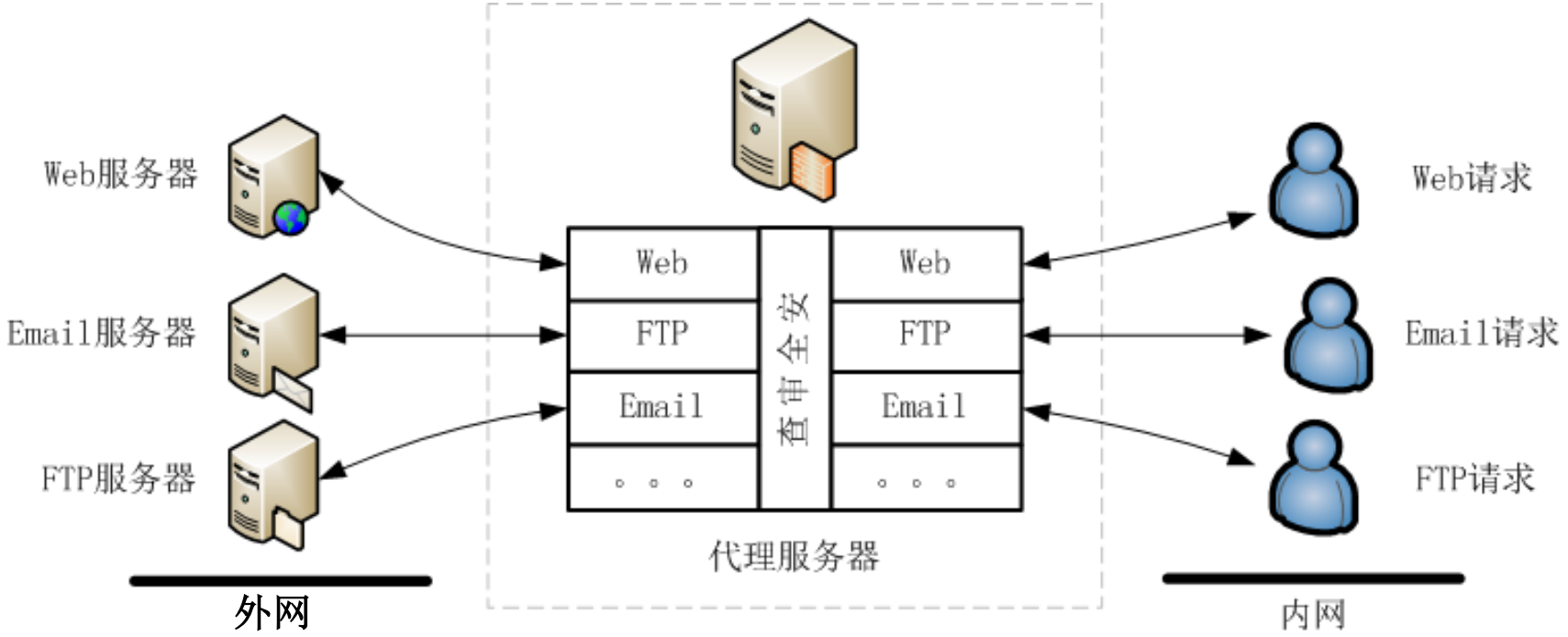
包过滤防火墙

- 包过滤防火墙主要是面向网络底层数据流进行审计和控管。
  - 其安全策略主要根据数据包头的源地址、目的地址、端口号和协议类型等标志来制定，可见其主要工作在网络层和传输层。



代理防火墙

- 代理防火墙基于代理（Proxy）技术，使防火墙参与到每一个内外网络之间的连接过程。
  - 防火墙需要理解用户使用的协议，对内部节点向外部节点的请求进行还原审查后，转发给外部服务器；外部节点发送来的数据也要进行还原审查，然后封装转发给内部节点。
  - 主要工作在应用层，有时也称为应用级网关。



个人防火墙

- 目前普通用户最常使用的一种，常见如天网个人防火墙。

- 个人防火墙是一种能够保护个人计算机系统安全的软件。
  - 直接在用户的计算机上运行，帮助普通用户对系统进行监控及管理，使个人计算机免受各种攻击。

防火墙涉及的技术

- **ACL（Access Control List，访问控制列表）**
- 静态包过滤
- 动态包过滤
- 应用网关代理
- 电路级网关（**Circuit Gateway**）
- **NAT（Network Address Translation，网络地址翻译）**
- **VPN（Virtual Private Network，虚拟专用网）**

访问控制列表ACL

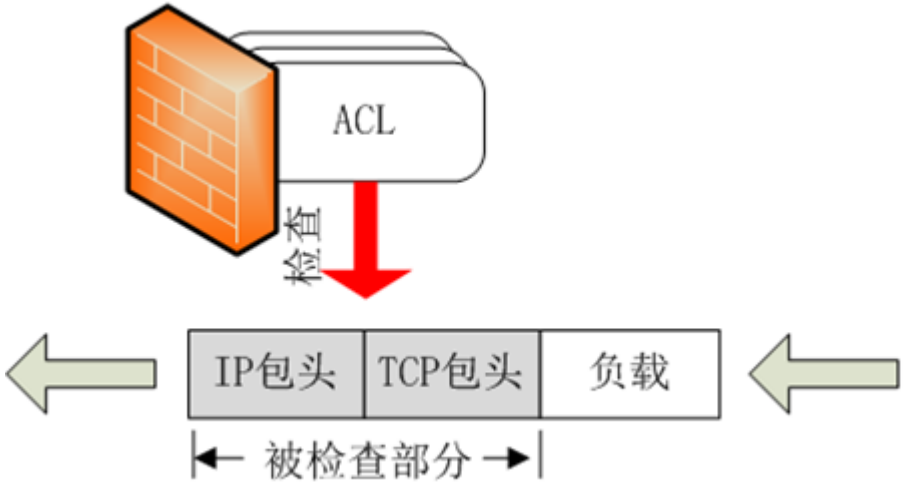
- **Access Control List是允许和拒绝匹配规则的集合。**
  - **规则告诉防火墙哪些数据包允许通过、哪些被拒绝。**

顺序	方向	源地址	目的地址	协议	源端口	目的端口	是否通过
Rule 1	out	192.168.10.11	*.*.*.*	TCP	any	80	deny
Rule 2	out	*.*.*.*	202.106.85.36	TCP	any	80	accept

- **ACL可以清晰体现防火墙的访问控制策略。**
- **规则的顺序非常重要。**

静态包过滤

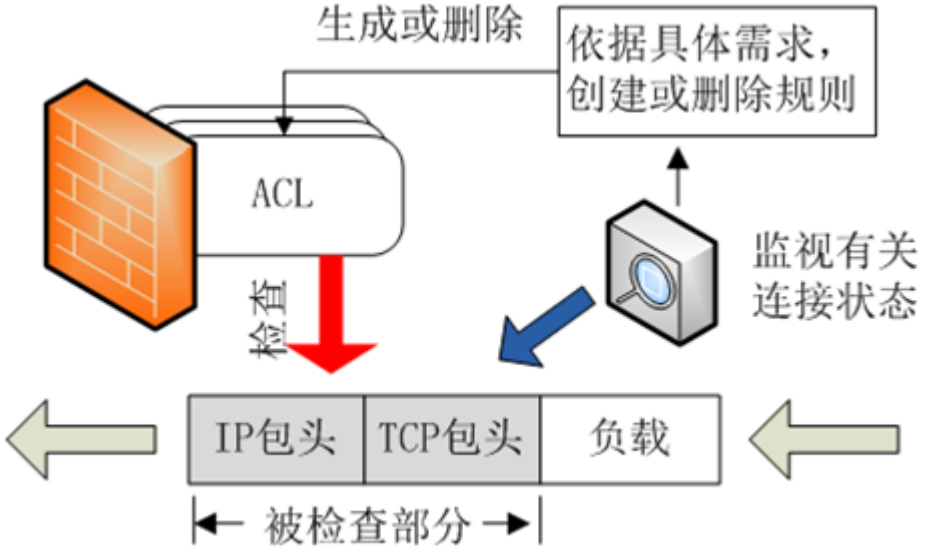
- 静态包过滤是指防火墙根据定义好的包过滤规则审查每个数据包，确定其是否与某一条包过滤规则匹配。



- 过滤规则基于数据包的包头信息进行制定，并存储在ACL中。
  - 包头信息中包括IP源地址、IP目标地址、传输协议（如TCP、UDP、ICMP等）、TCP/UDP目标端口、ICMP消息类型等。

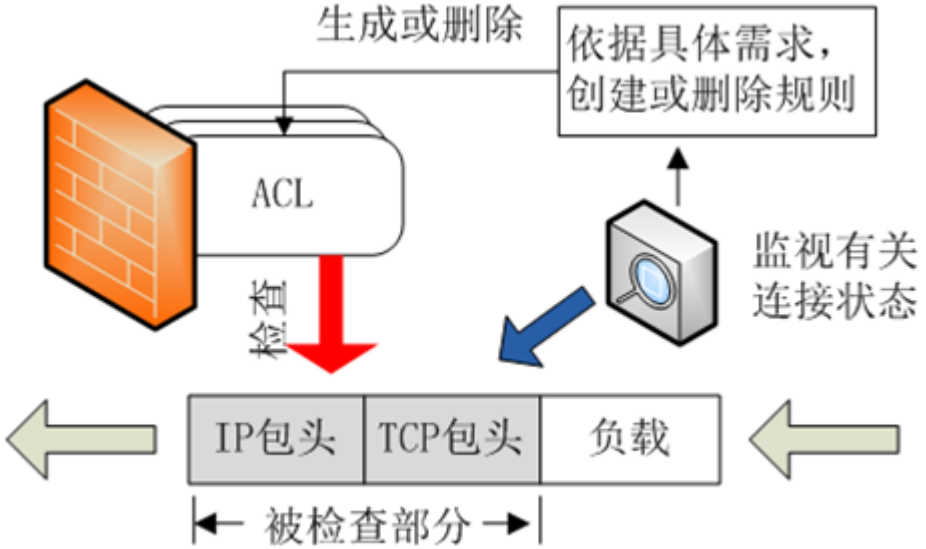
动态包过滤

- 动态包过滤是指防火墙采用动态配置包过滤规则的方法。



- 根据需求动态地添加或删除ACL中的过滤规则，并通过对其批准建立的每一个连接进行跟踪，更加灵活地实现对网络连接访问的控制。

动态包过滤



- 当一个合法用户请求访问外网时，向防火墙发出连接请求，防火墙审核通过后，向ACL中添加放行该用户访问的规则，该用户可以建立访问外网的会话。当防火墙接收到该用户结束访问的通知或检测到会话结束或超时的时候，将自行删除为该用户创建的规则。
- 实际上，静态包过滤是依据数据包的包头信息进行控管，而动态包过滤是基于会话，动态建立和删除规则。

应用代理网关

- 应用代理网关被认为是最安全的防火墙技术。
  - 应用代理网关防火墙彻底隔断内网与外网的直接通信，内网用户对外网的访问变成防火墙对外网的访问，外网返回的消息再由防火墙转发给内网用户。
  - 应用层的协议会话过程必须符合代理的安全策略要求。

- 缺陷：
  - 首先，必须能够理解繁杂的应用层协议和不断产生的新协议，才能较好地为用户服务。
  - 其次，为了应付大量的网络连接并还原到应用层，防火墙的工作量势必大幅度提升，甚至成了网络瓶颈。
- 应用代理网关只适合那些用户较少，同时应用服务较少的网络。

电路级网关

- 工作原理与应用代理网关基本相同，代理的协议以传输层为主，在传输层上实施访问控制策略，是在内外网络之间建立一个虚拟电路，进行通信。

- 由于代理传输层协议，应用电路级网关不需要审计应用层数据，只是检查内网主机与外网主机之间的传输数据来决定该会话是否合法。

- 因此，其所要处理的工作量远小于应用代理网关，但安全性低于应用代理网关。

NAT

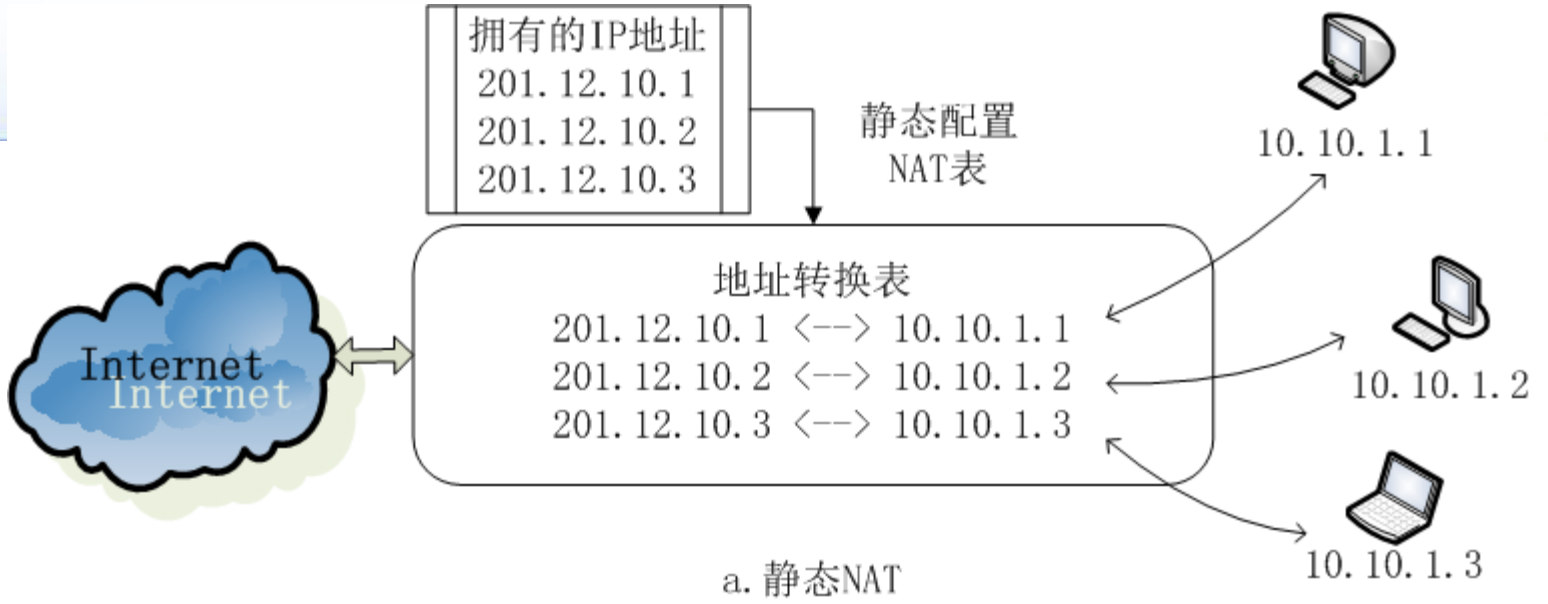
- NAT是一种将私有地址转换为合法IP地址的转换技术，广泛应用于各种类型网络连接Internet的工程中。

- NAT不仅完美解决了IP地址不足的问题，而且还能够有效地避免来自网络外部的攻击，隐藏并保护网络内部的计算机。
- 同时，对于内网用户来说，整个地址翻译过程是透明的。

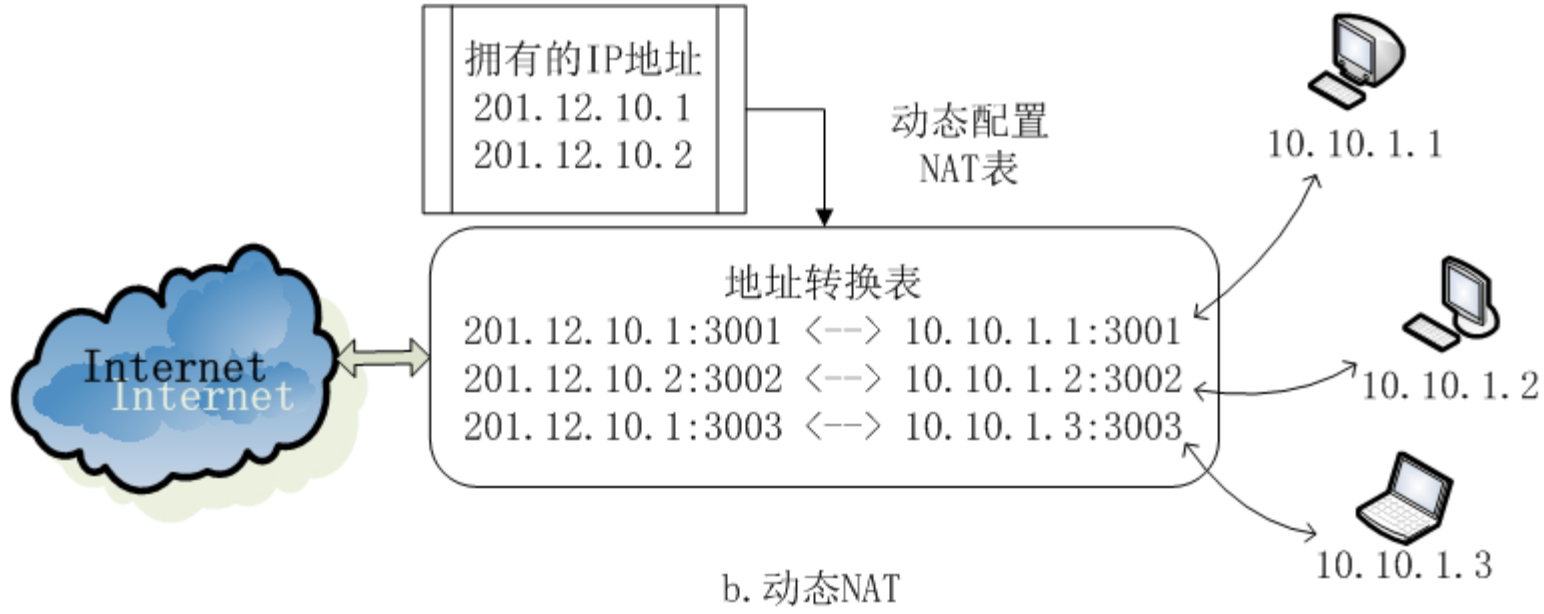
- 实际上NAT就是把内部网络中的IP包头内内部IP地址信息用可以访问外部网络的真实IP地址信息来替换。

- 根据NAT的工作方式，可以分为静态NAT和动态NAT两种。

NAT



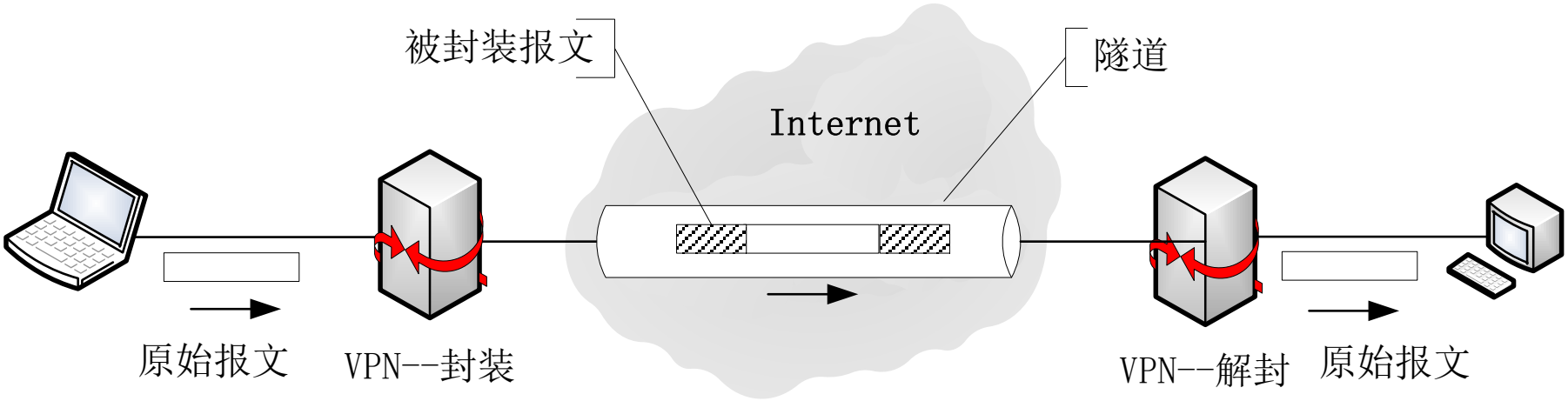
a. 静态NAT



b. 动态NAT

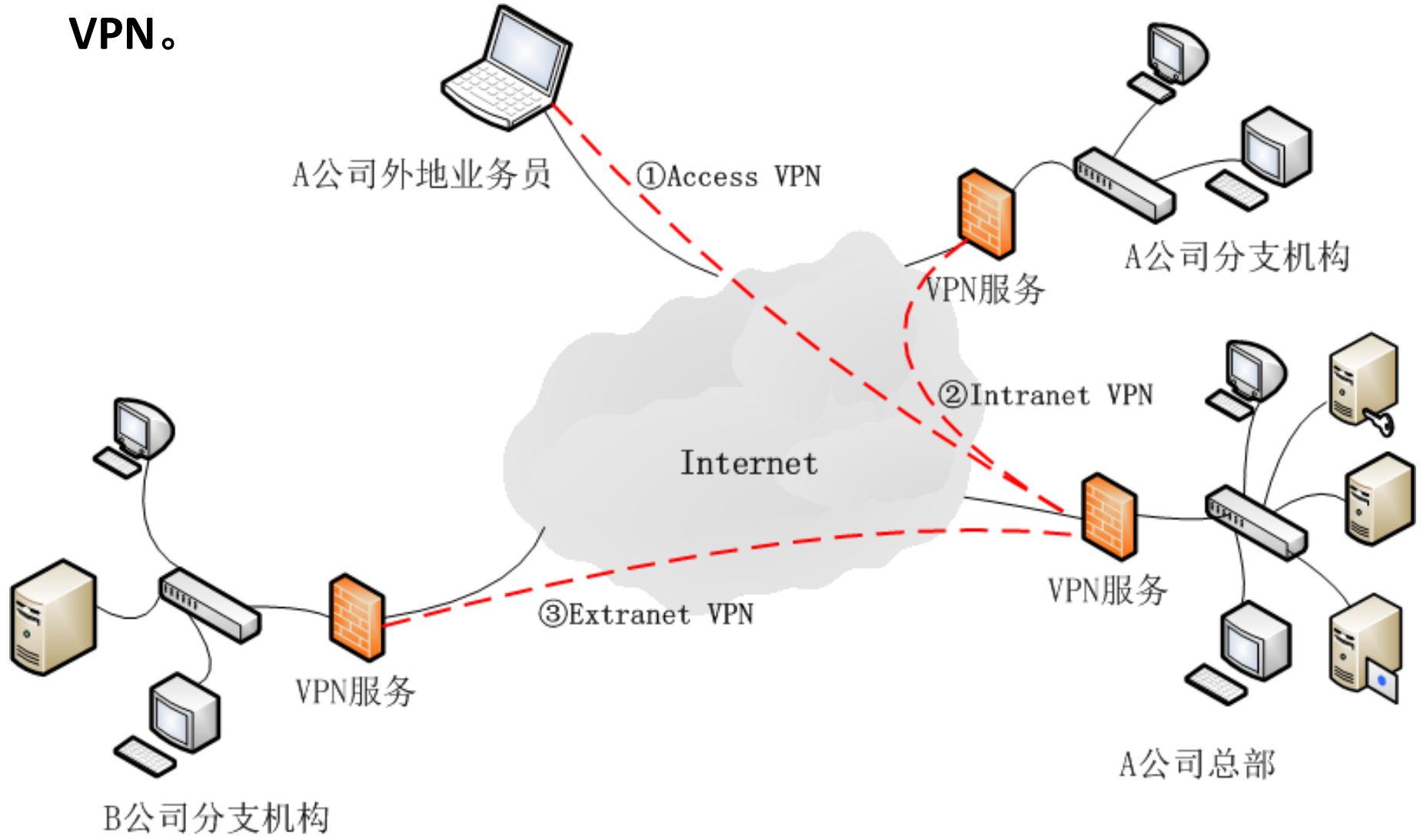
VPN

- VPN是通过一个公用网络（通常是Internet）建立一个临时的、安全的连接。
  - 可以理解为一条穿过公用网络的安全、稳定的隧道。
  - 两台分别处于不同网络的机器可以通过这条隧道进行连接访问，就像在一个内部局域网一样。



VPN典型应用

- VPN服务大致分为三类：Access VPN、Intranet VPN和Extranet VPN。



VPN典型应用

- **Access VPN**，又称为虚拟专用拨号网（Virtual Private Dial-up Network，VPDN），是指企业员工或企业的小分支机构通过公网远程拨号的方式构筑的虚拟网。

- **Intranet VPN**，及企业的内部与分支机构间通过VPN虚拟网进行网络连接，其最大特点是可以为总部及各分支机构提供整个企业网络的访问权限。

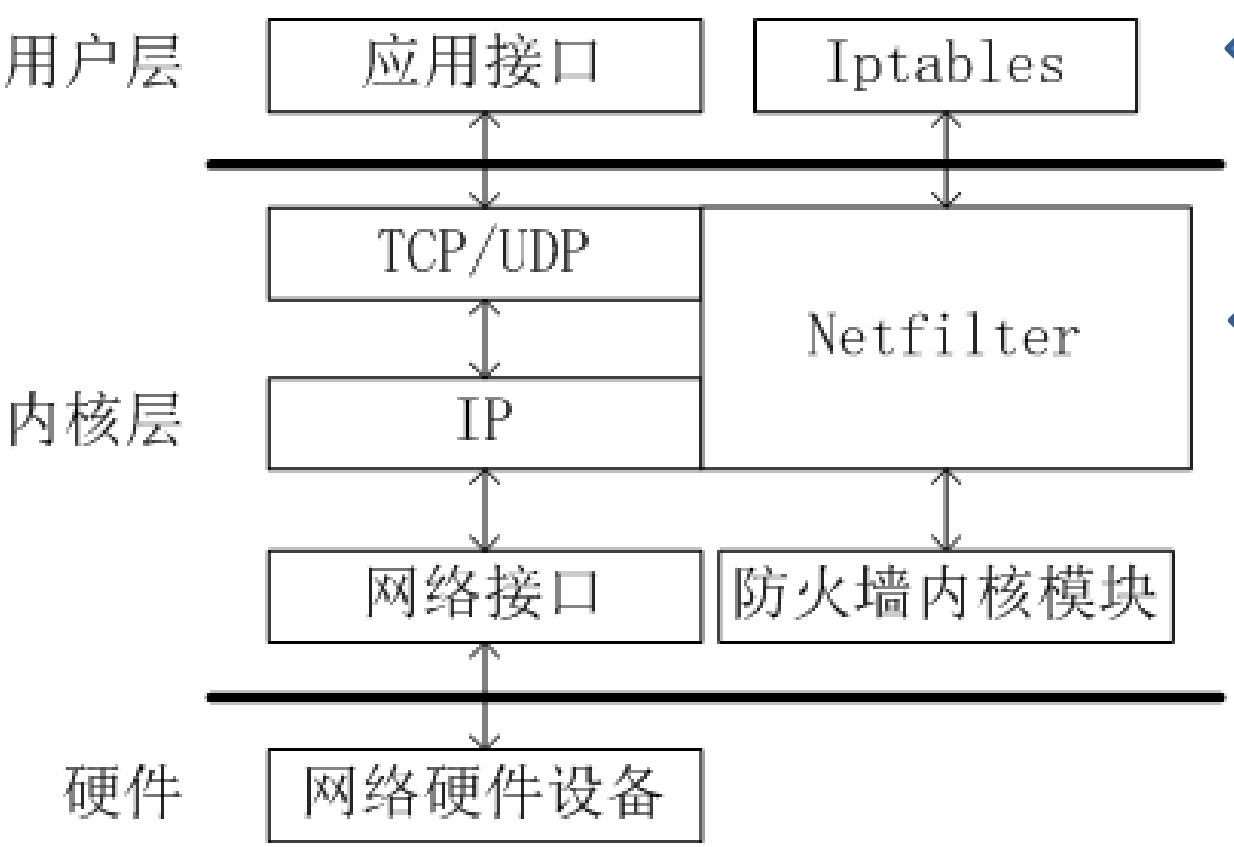
- **Extranet VPN**，目的是通过一个使用专用连接的共享基础设施，将客户、供应商、合作伙伴或兴趣群体连接到企业内部网，其特点是支持对外部用户进行相应访问权限的设定。

主要内容

- 7.1 概述
- 7.2 防火墙
  - 7.2.1 防火墙概述
  - 7.2.2 防火墙的主要技术
  - 7.2.3 Netfilter/IPtables防火墙
- 7.3 入侵检测系统
- 7.4 网络防御的新技术

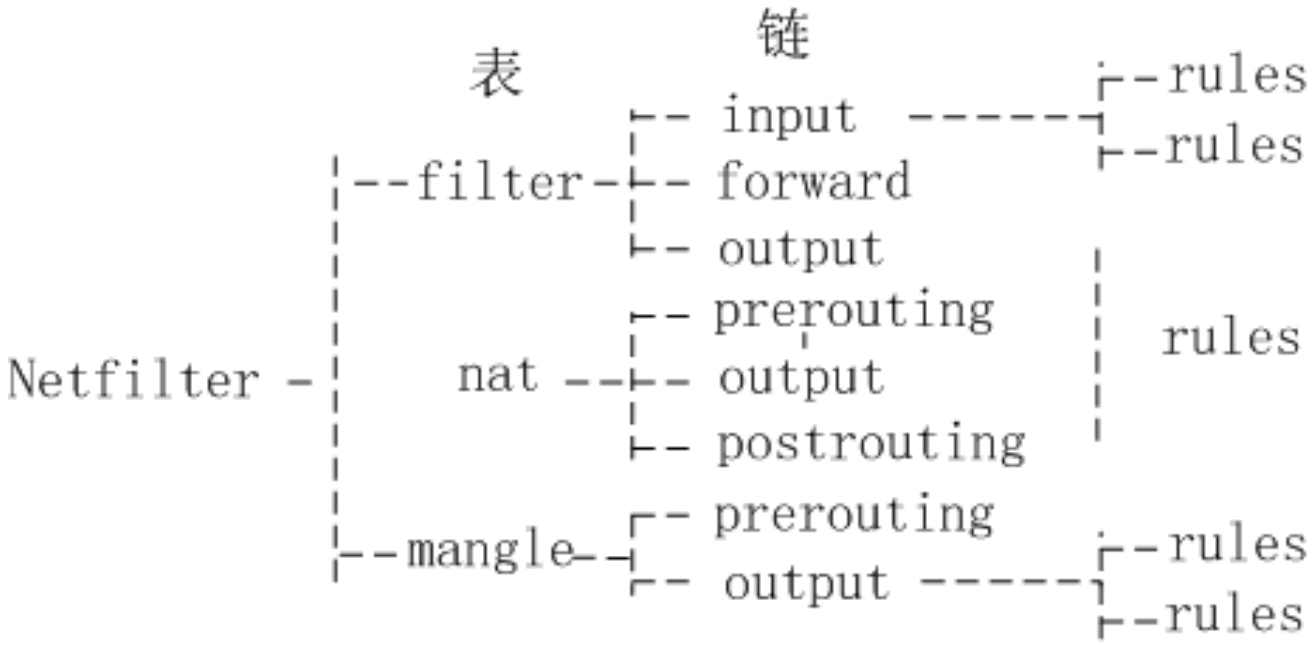
Netfilter/IPtables防火墙

- 2001年，Linux 2.4版内核，Netfilter/IPtables包过滤机制，被业内称为第三代Linux防火墙。



Netfilter通用架构

- Netfilter是嵌入在Linux内核IP协议栈中的一个通用架构。
  - 它提供了一系列的“表”（tables）。
    - 每个表由若干“链”（chains）组成。
    - 每条链中可以有一条或数条规则（rule）。



Netfilter的三个主要功能表

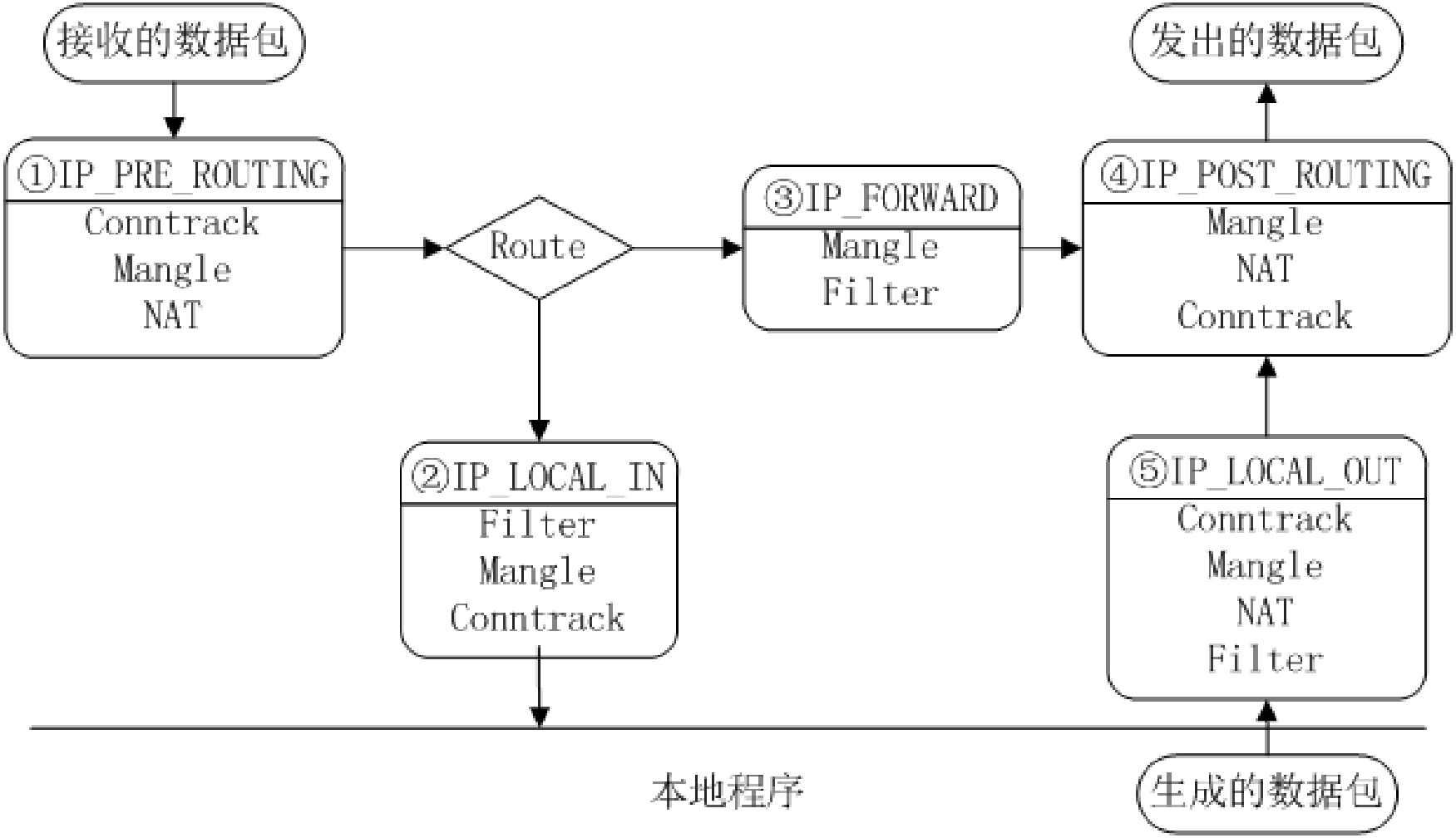
- **Filter**，数据包过滤表，用于检查数据包的内容信息，决定放行还是丢弃该数据包。
  - Filter包含**Input**、**Forward**和**Output**三个链，分别用于处理目的地址是本地的数据包、目的地址不是本地的数据包和由本地产生的数据包。

- **Nat**，网络地址转换表，用于数据包的地址翻译。

- **Mangle**，数据包处理表，提供了修改数据包某些字段值的方法，用于IP网络中的流量控制和服务质量的实现。

Netfilter程序流程架构

- Netfilter的具体实现，是通过在网络处理流程的若干位置放置一些钩子(hook)来实现的。



Netfilter程序流程架构

- **IP_PRE_ROUTING：** 处于数据包从数据链路层进入网络层的钩子点。
- **IP_LOCAL_IN：** 处于数据包从网络层进入传输层的钩子点。
- **IP_FORWARD：** 处于数据包在网络层转发的钩子点。
- **IP_POST_ROUTING：** 处于数据包从网络层进入数据链路层的钩子点。
- **IP_LOCAL_OUT：** 处于数据包从传输层进入网络层的钩子点。

规则组成

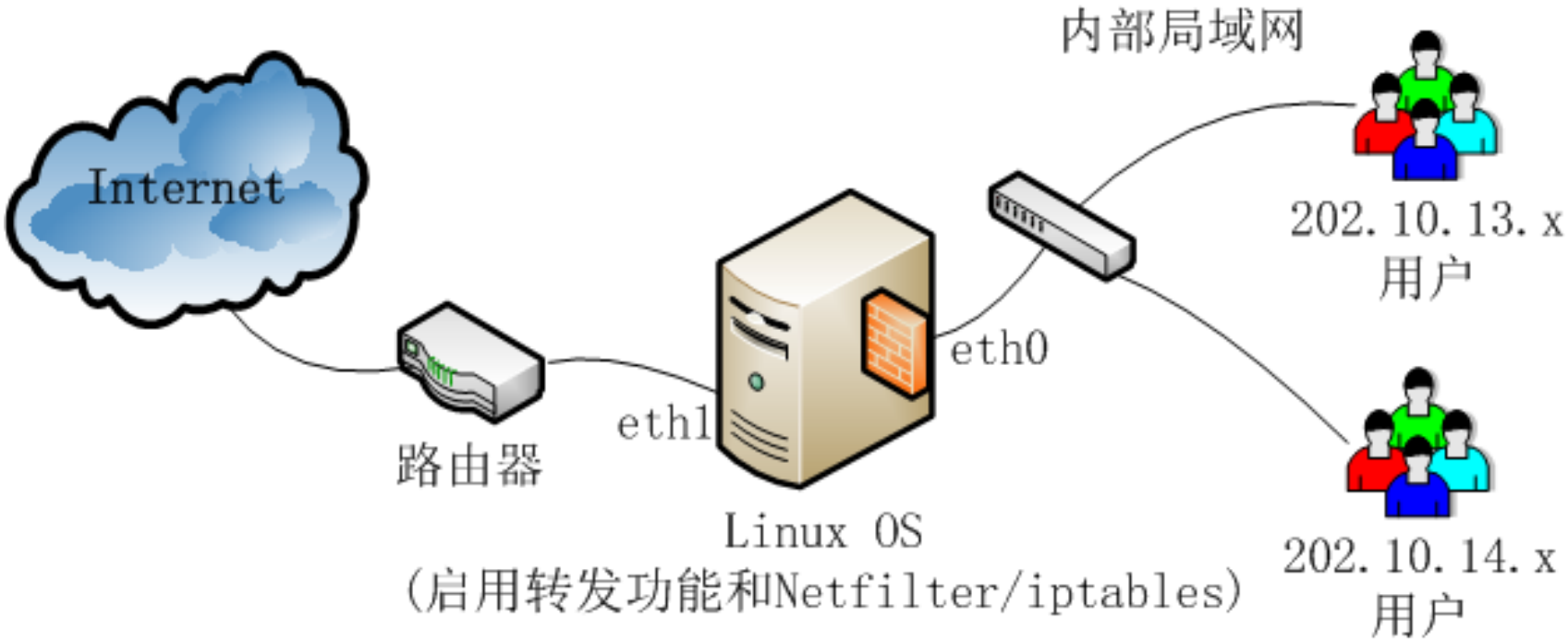
- 包过滤表中的规则是通过IPtables的命令来进行管理的。

IPtables命令 = 工作表 + 使用链 + 规则操作 + 目标动作 + 匹配条件

- 工作表：指定该命令针对的表，缺省表为filter；
- 使用链：指定表下面的某个链，实际上就是确定哪个钩子点；
- 规则操作：包括添加规则、插入规则、删除规则、替代规则、列出规则；
- 目标动作：有两个，ACCEPT（继续传递数据包），DROP（丢弃数据包）；
- 匹配条件：指过滤检查时，用于匹配数据包头信息的特征信息串，如地址、端口等。

Netfilter/IPtables 例子

- 配置目的：内网中只有202.10.13.0/24网段的用户可以访问外网，同时又只能使用TCP。
  - iptables -P FORWARD DROP
  - iptables -A FORWARD -p tcp -s 202.10.13.0/24 -j ACCEPT
  - iptables -A FORWARD -p tcp -d 202.10.13.0/24 -j ACCEPT



作业

- 习题2（1）：静态包过滤和动态包过滤有什么区别？
- 习题2（2）：DMZ的主要功能是什么？
- 习题2（4）：代理网关与电路级网关有什么区别？