培训目标

- 学完本课程后，您应该能：
  - 了解防火墙的定义
  - 掌握防火墙的主要功能
  - 了解防火墙的分类

目录

引入

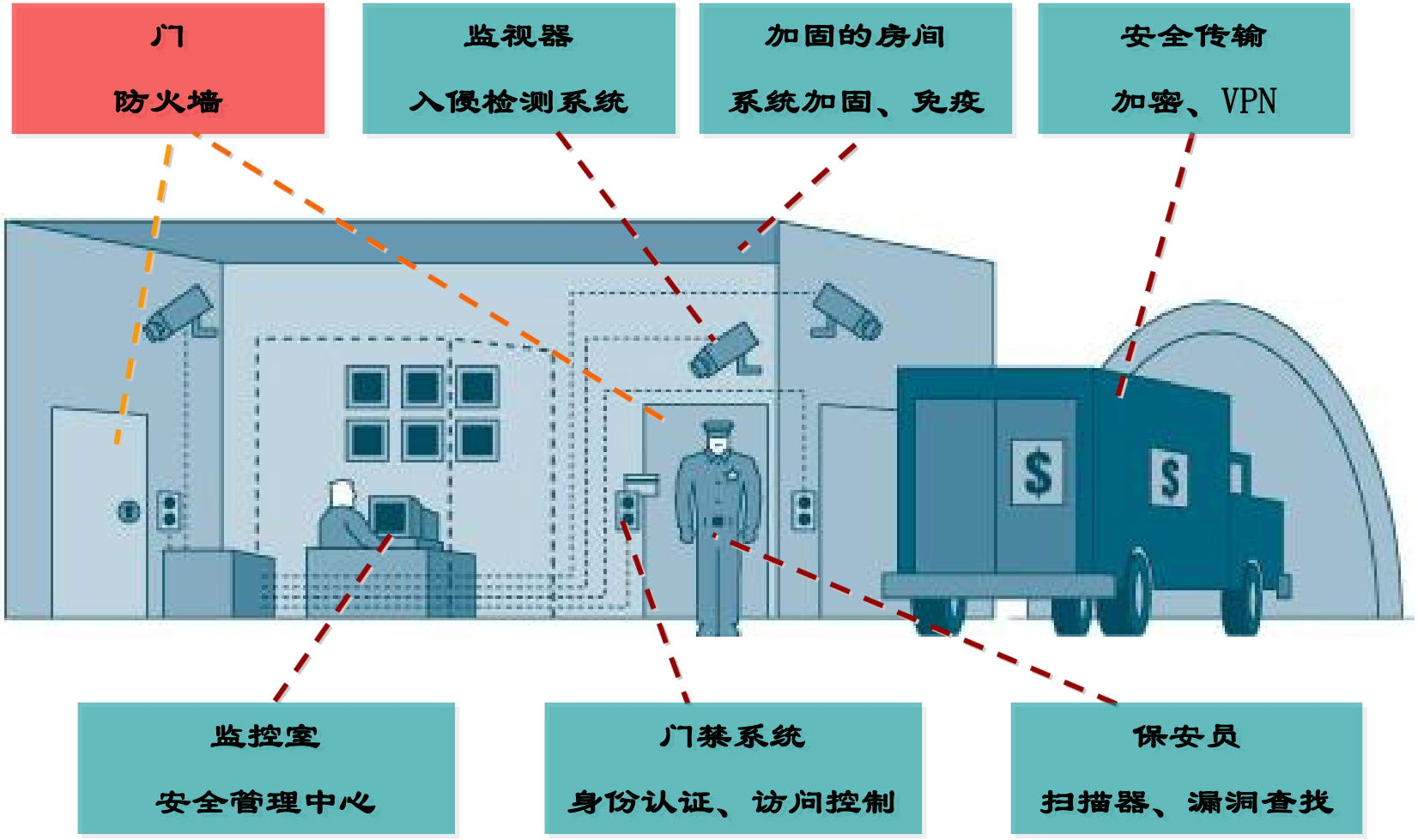
- 随着Internet的日益普及，开放式的网络带来了许多不安全的隐患。在开放网络式的网络上，我们的周围存在着许多不能信任的计算机（包括在一个LAN之间），这种这些计算机对我们私有的一些敏感信息造成了很大的威胁。
- 在大厦的构造中，防火墙被设计用来防止火灾从大厦的一部分传播到大厦的另一部分。我们所涉及的“防火墙”具有类似的目的：“防止Internet的危险传播到你的内部网络”。

什么是防火墙?

- 防火墙(Fire Wall)：网络安全的第一道防线，是位于两个信任程度不同的网络之间（如企业内部网络和Internet之间）的设备，它对两个网络之间的通信进行控制，通过强制实施统一的安全策略，防止对重要信息资源的非法存取和访问以达到保护系统安全的目的。

- 防火墙 = 硬件 + 软件 + 控制策略
  - 宽松控制策略：除非明确禁止，否则允许。
  - 限制控制策略：除非明确允许，否则禁止。

防火墙在安全体系中的位置

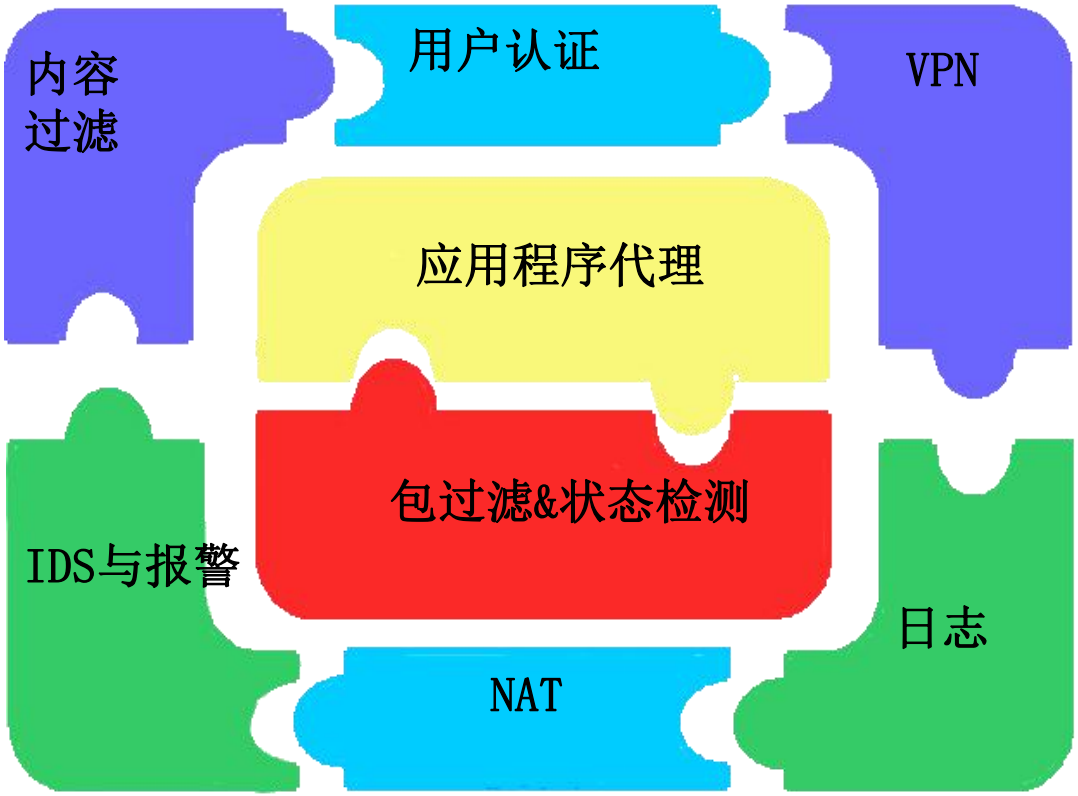


目录

防火墙的功能

- 防火墙能提供的功能：
  - 监控和审计网络的存取和访问，过滤进出网络的数据，管理进出网络的访问行为
  - 部署于网络边界，兼备提供网络地址翻译(NAT)、虚拟专用网(VPN)等功能
  - 防病毒、入侵检测、认证、加密、远程管理、代理 ……
  - 深度检测对某些协议进行相关控制
  - 攻击防范，扫描检测等

防火墙的基本功能模块



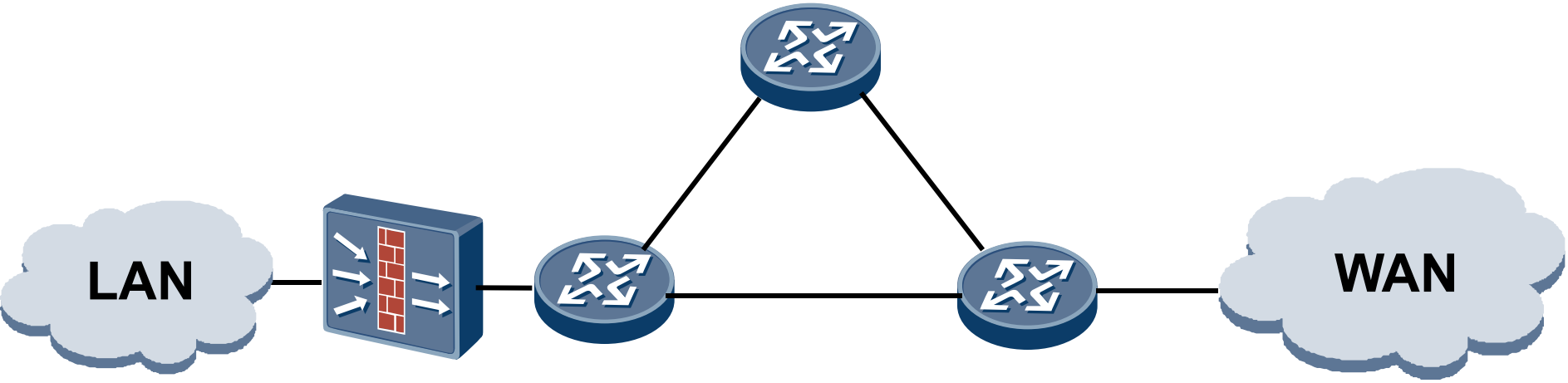
先进的 防火墙

- 先进的硬件体系结构。
- 强大的功能，丰富的业务支持。
- 电信级的高可靠性。
- 增强的日志统计功能。

防火墙的局限性

- 防火墙不是解决所有网络安全问题的万能药方，只是网络安全政策和策略中的一个组成部分，是保卫网络安全的第一道门户。

防火墙和路由器的差异



路由器的特点：

1、保证互联互通。

2、按照最长匹配算法逐包转发。

3、路由协议是核心特性。

防火墙的特点：

1、逻辑子网之间的访问控制，关注边界安全

2、基于连接的转发特性。

3、安全防范是防火墙的核心特性。

目录

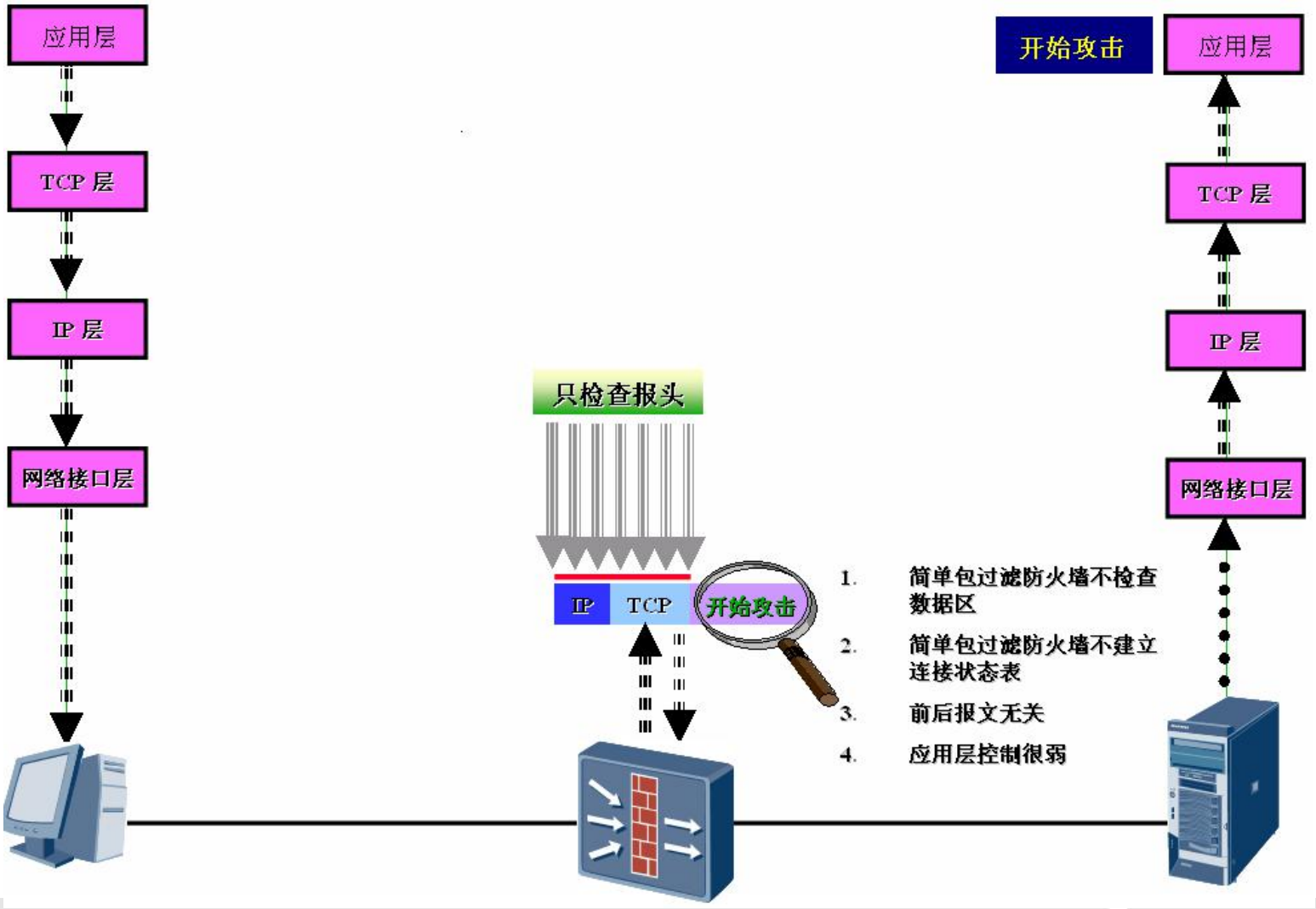
防火墙的分类

按照防火墙实现的方式，一般把防火墙分为如下几类:

- 包过滤防火墙(Packet Filtering)
- 代理型防火墙（Application Gateway）
- 状态检测防火墙 (State Detect)

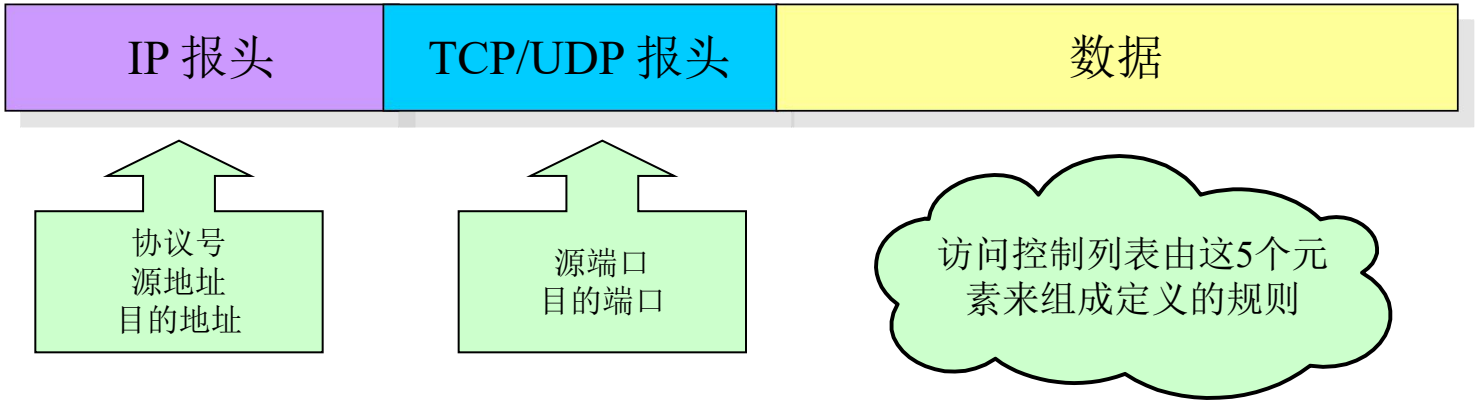
目前防火墙的主流产品为状态检测防火墙

包过滤防火墙(Packet Filtering)



包过滤防火墙(Packet Filtering)-（续）

- 规则的定义就是按照IP数据包的特点定义的，可以充分利用上述条件定义通过防火墙数据包的条件。



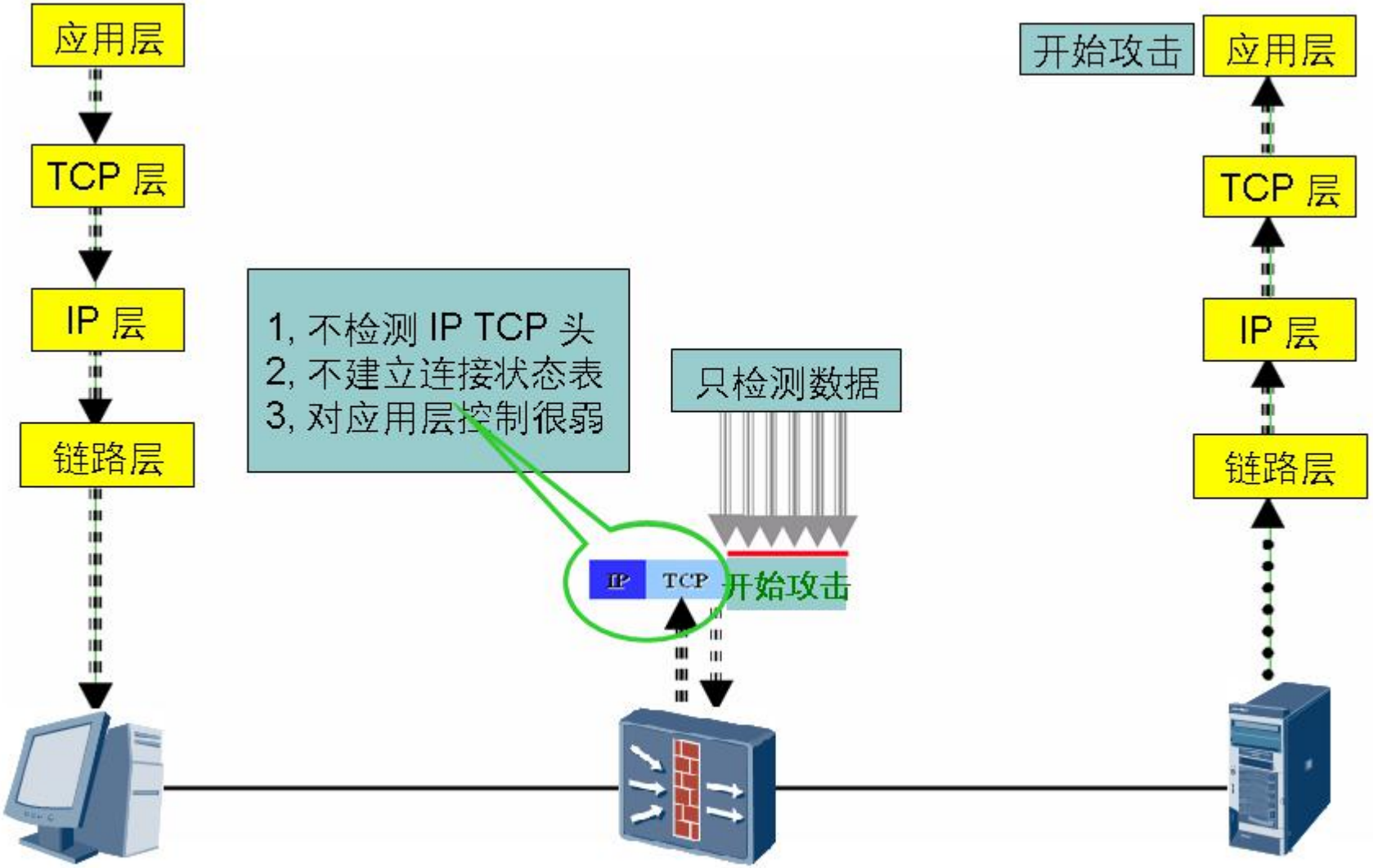
包过滤防火墙(Packet Filtering)-（续）

优点：设计简单，非常易于实现，而且价格便宜。其缺点也

缺点：

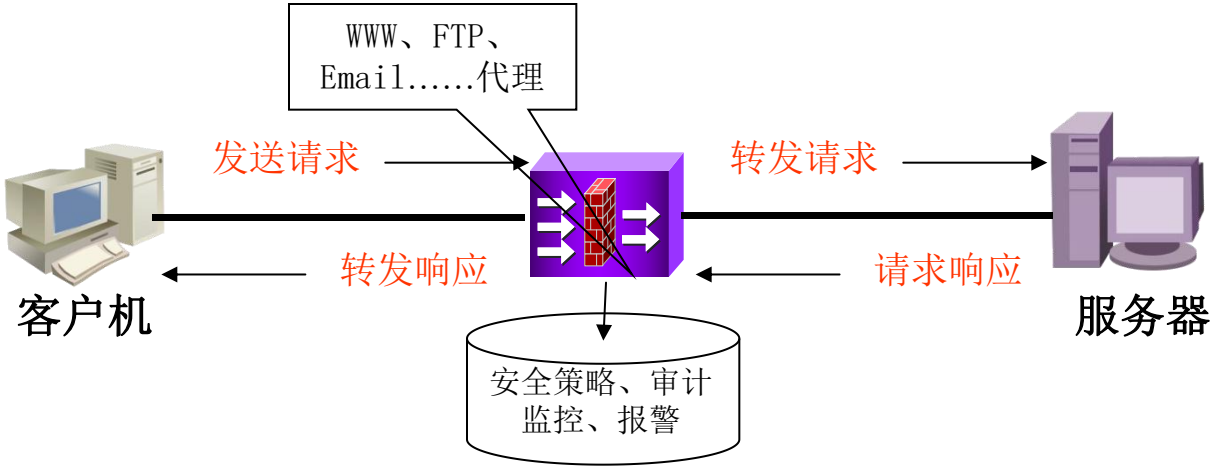
- 基于网络层的安全技术，对于应用层的黑客行为无能为力。
- 包过滤防火墙对于任何应用需要配置双方向的ACL规则，不能提供差异性保护。
- 随着ACL复杂度和长度的增加，其过滤性能成指数下降趋势。
- 静态的ACL规则难以适应动态的安全要求。

代理型防火墙(Application Gateway)



代理型防火墙(Application Gateway)-（续）

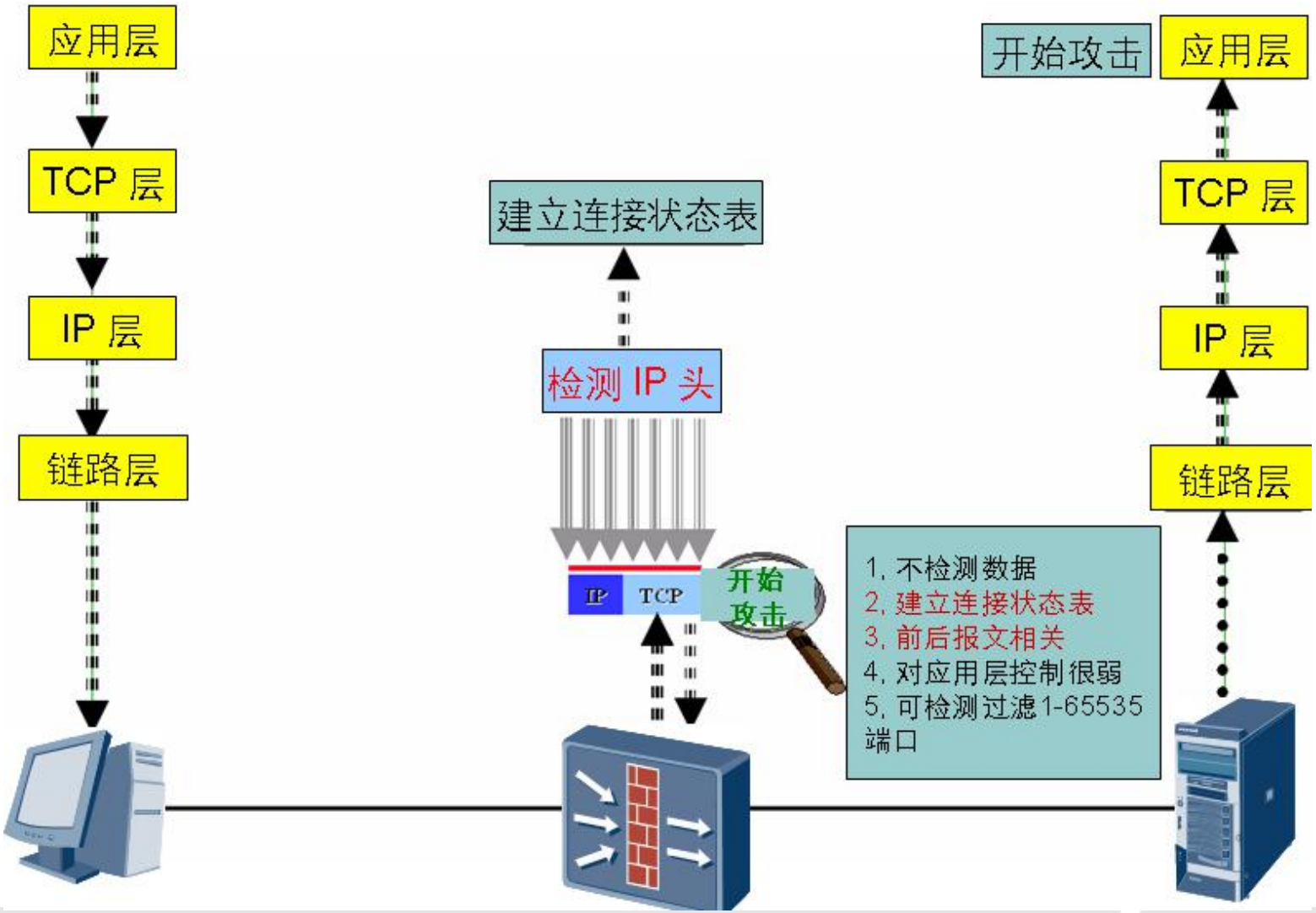
- 代理服务作用于网络的应用层，其实质是把内部网络和外部网络用户之间直接进行的业务由代理接管。代理检查来自用户的请求。认证通过后，该防火墙将代表客户与真正的服务器建立连接，转发客户请求，并将真正服务器返回的响应回送给客户。



代理型防火墙(Application Gateway)-（续）

- 优点：代理防火墙能够完全控制网络信息的交换，控制会话过程，具有较高的安全性。
- 缺点：
  - 软件实现限制了处理速度，易于遭受拒绝服务攻击；
  - 需要针对每一种协议开发应用层代理，升级很困难。因此代理型防火墙不能支持很丰富的业务，只能针对某些应用提供代理支持；
  - 代理型防火墙使得防火墙做为一个访问的中间节点，对Client来说防火墙是一个Server，对Server来说防火墙是一个Client，转发性能低；
  - 代理型防火墙很难组成双机热备的组网，因为状态无法保持同步；

状态检测防火墙（State Detect）



状态检测防火墙（State Detect）-（续）

- 状态检测是一种高级通信过滤。

- 状态分析技术是包过滤技术的扩展（非正式的也可称为“动态包过滤”）。

状态检测防火墙（State Detect）-（续）

- 状态防火墙具有以下优点：

速度快

安全性高

性能衡量指标

- 吞吐量
- 延时
- 最大并发连接数
- 最大新建并发连接数

吞吐量(Throughput)

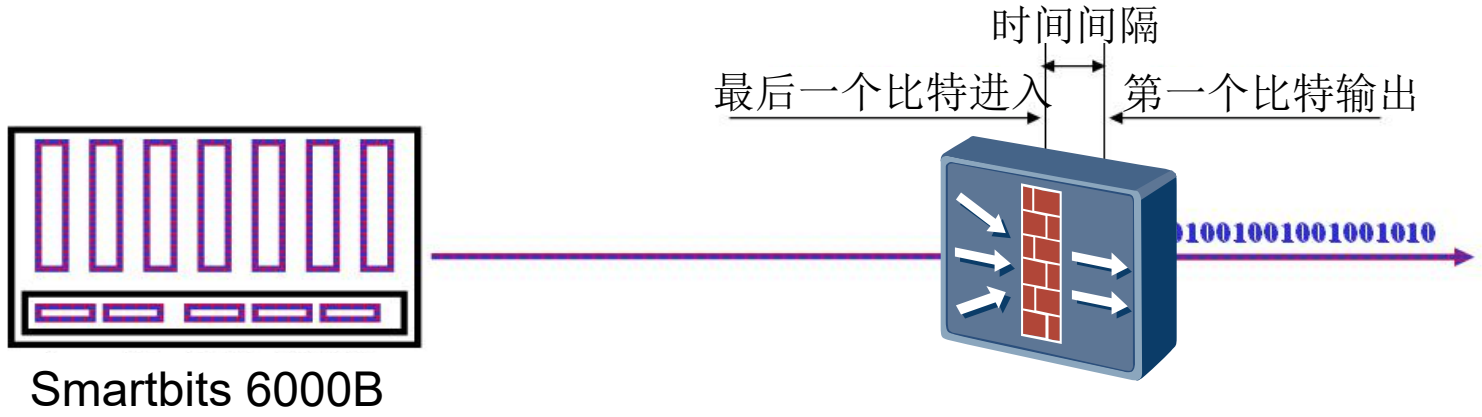
- 吞吐量：防火墙能同时处理的最大数据量。

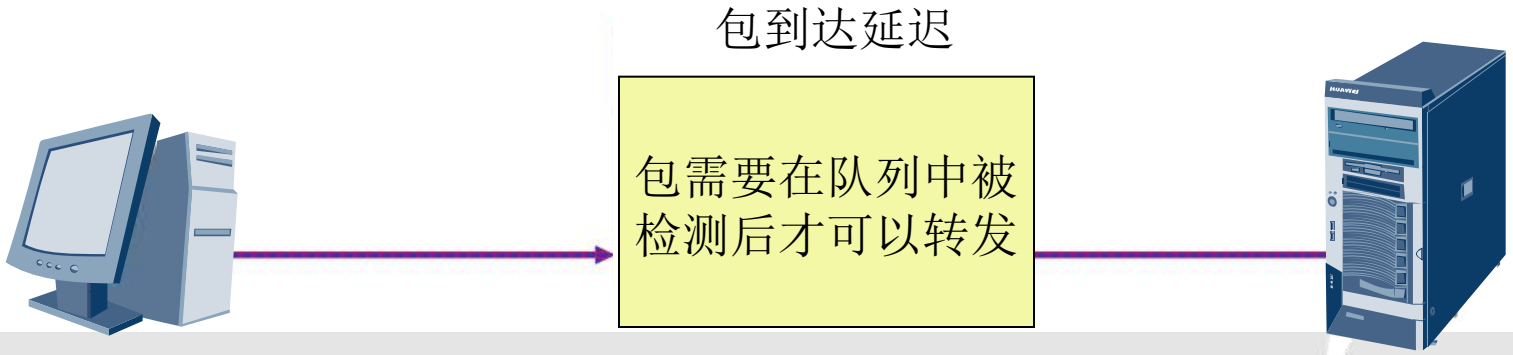
- 有效吞吐量：除掉TCP因为丢包和超时重发的数据，实际的每秒传输有效速率。

延时

定义：数据包的最后一个比特进入防火墙到第一个比特输出防火墙的时间间隔

指标：延时是用于测量防火墙处理数据的速度

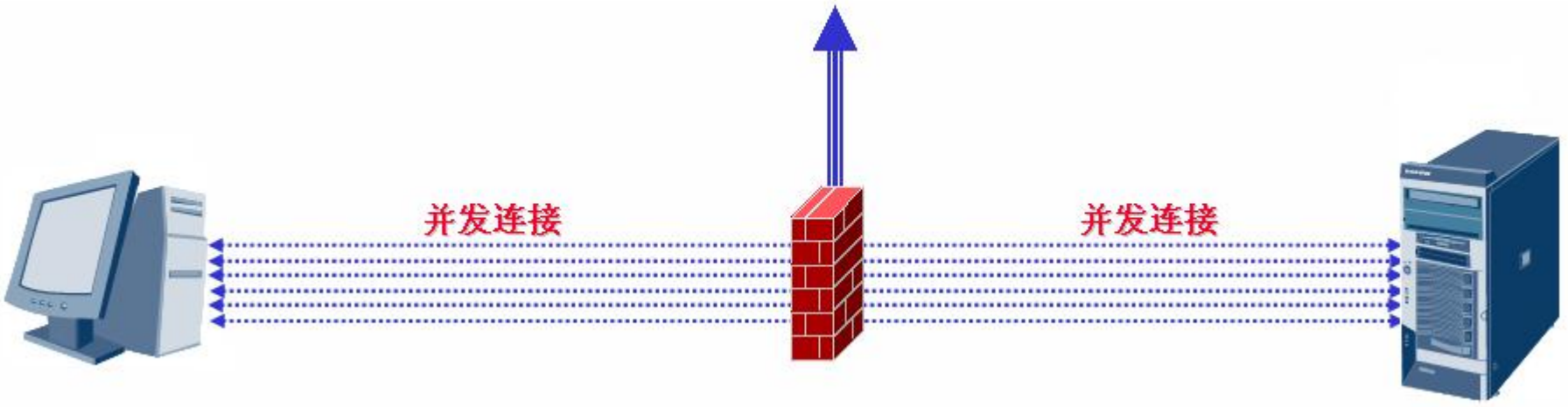




最大并发连接数

定义：由于防火墙是针对连接进行处理报文的，并发连接数目是指的防火墙可以同时容纳的最大的连接数目，一个连接就是一个TCP/UDP的访问。

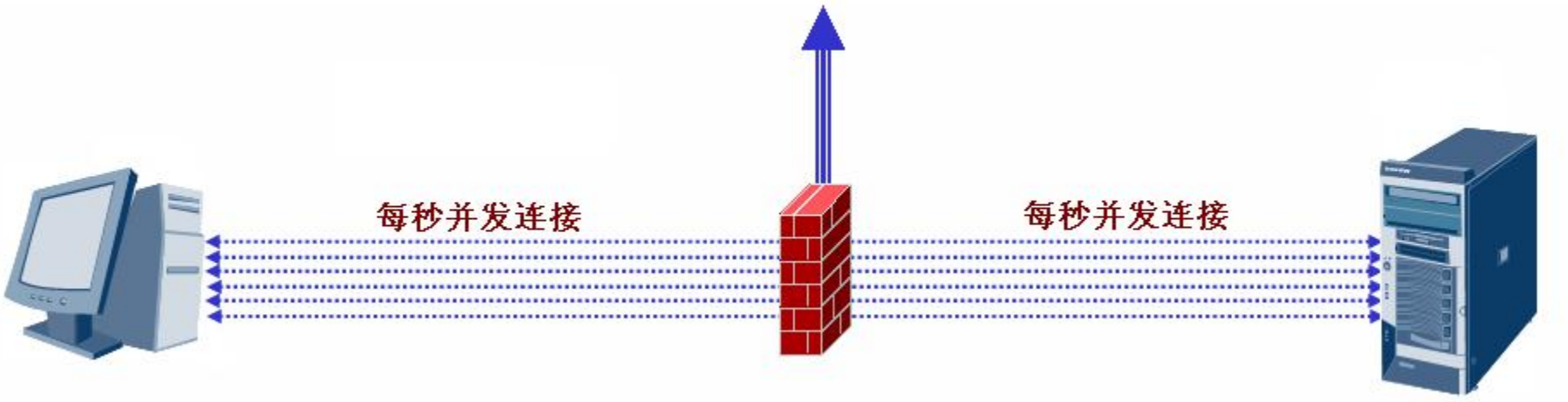
该参数是用来衡量主机和服务器间能同时建立的最大连接数



最大新建并发连接数

指每秒钟可以通过防火墙建立起来的完整TCP连接。

该指标是用来衡量防火墙随数据流的实时处理能力

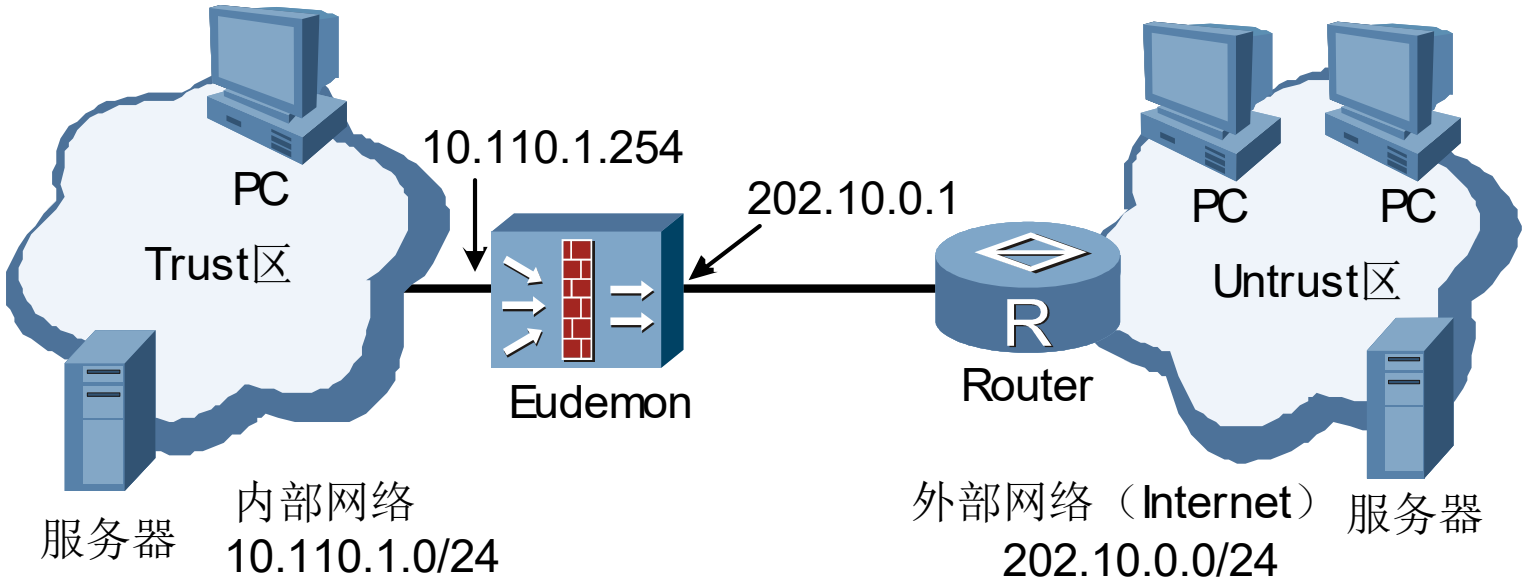


目录

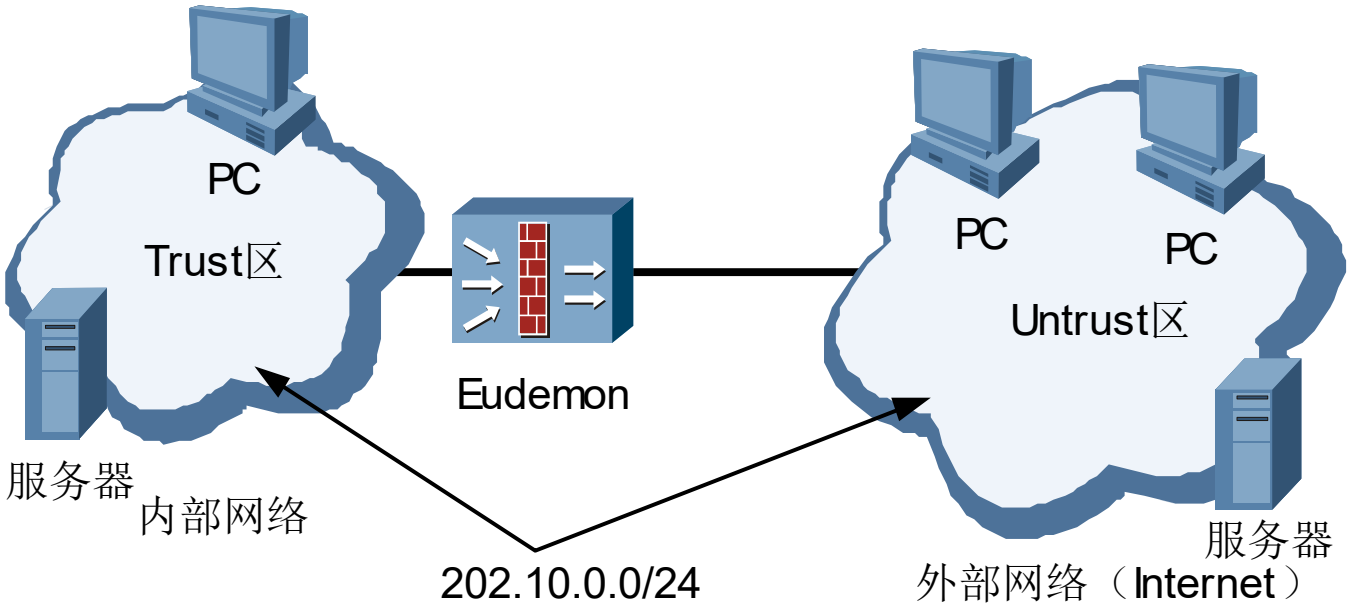
防火墙的工作模式（Mode）

- 防火墙能够工作在三种模式下：
  - 路由模式
  - 透明模式
  - 混合模式

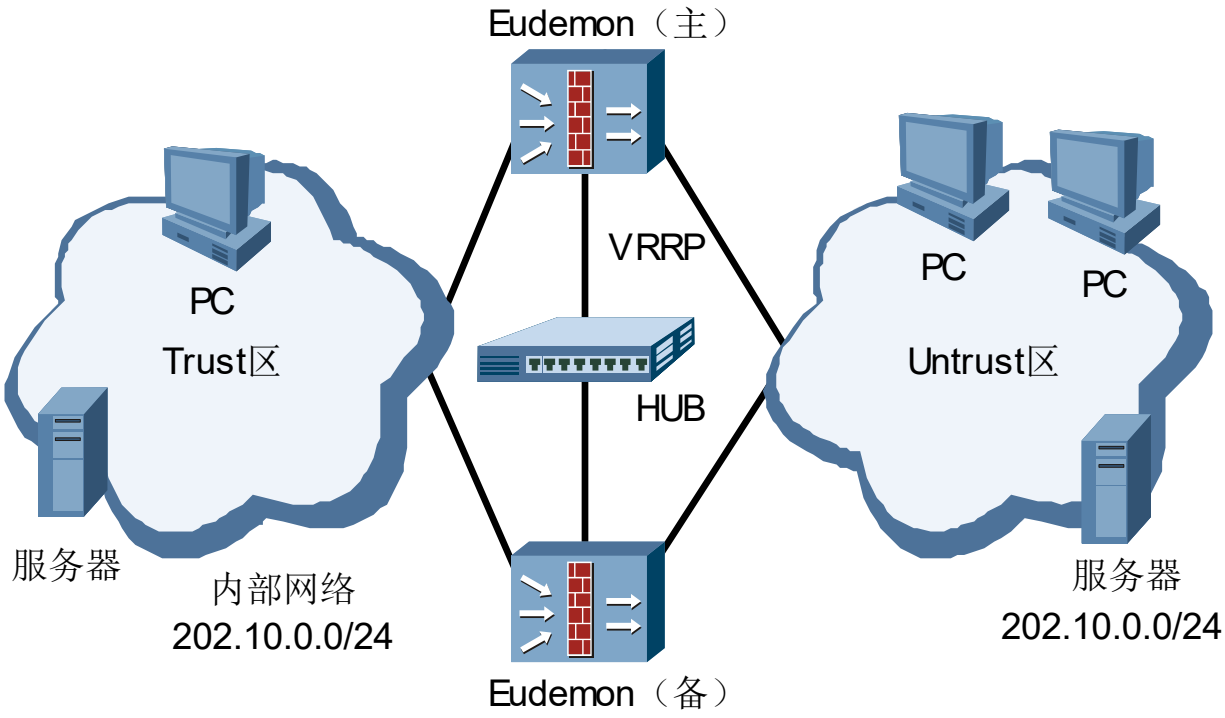
路由模式（Mode）


PC
Trust区
10.110.1.254
202.10.0.1
Eudemon
R
Router
PC
PC
Untrust区
服务器
内部网络
10.110.1.0/24
外部网络（Internet）
202.10.0.0/24
服务器

透明模式（Mode）

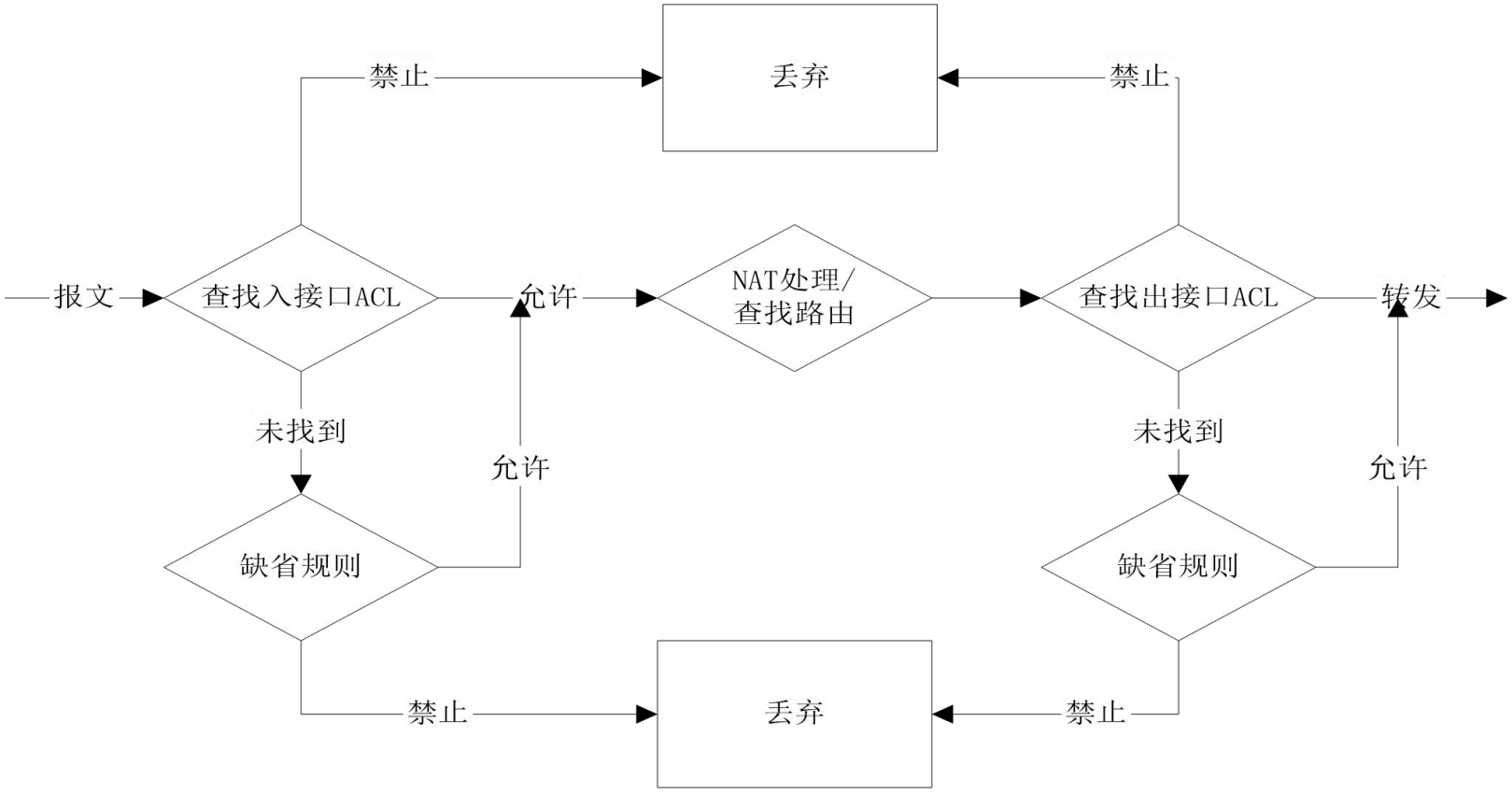

PC
Trust区
Eudemon
PC
PC
Untrust区
服务器
内部网络
202.10.0.0/24
服务器
外部网络（Internet）

混合模式（Mode）

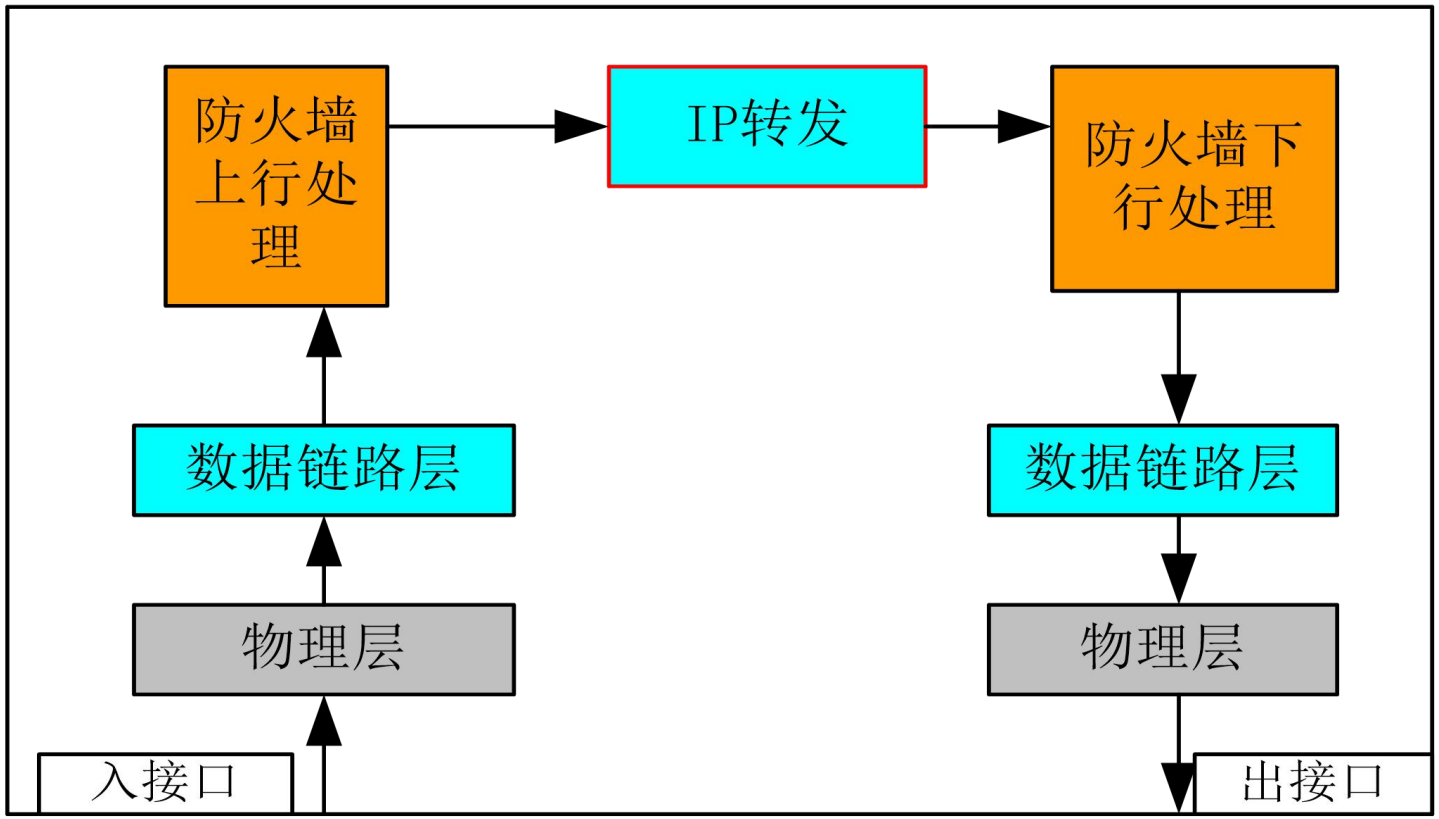

Eudemon（主）
VRRP
PC
Trust区
HUB
PC
PC
Untrust区
服务器
内部网络
202.10.0.0/24
Eudemon（备）
服务器
202.10.0.0/24

目录

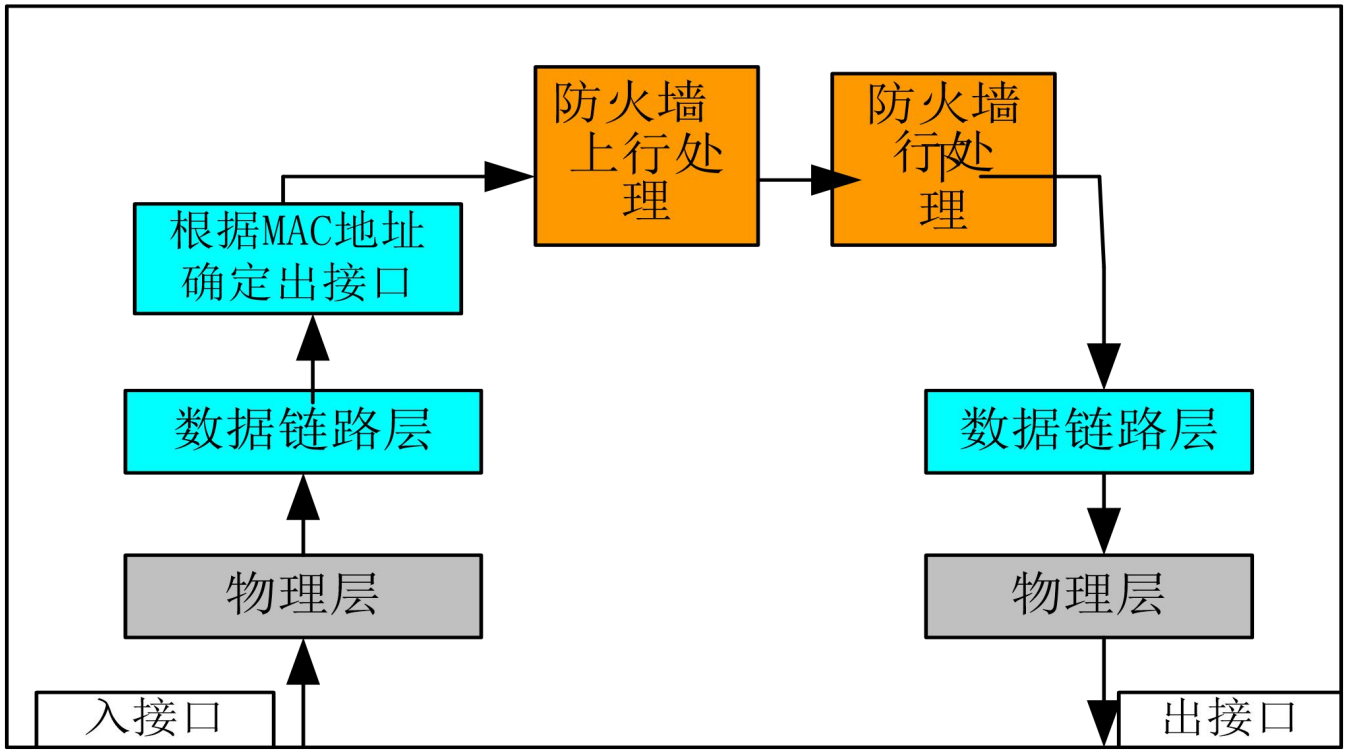
路由器的基本工作流程


丢弃
禁止
禁止
报文
查找入接口ACL
允许
NAT处理/
查找路由
查找出接口ACL
转发
未找到
允许
未找到
允许
缺省规则
缺省规则
禁止
丢弃
禁止

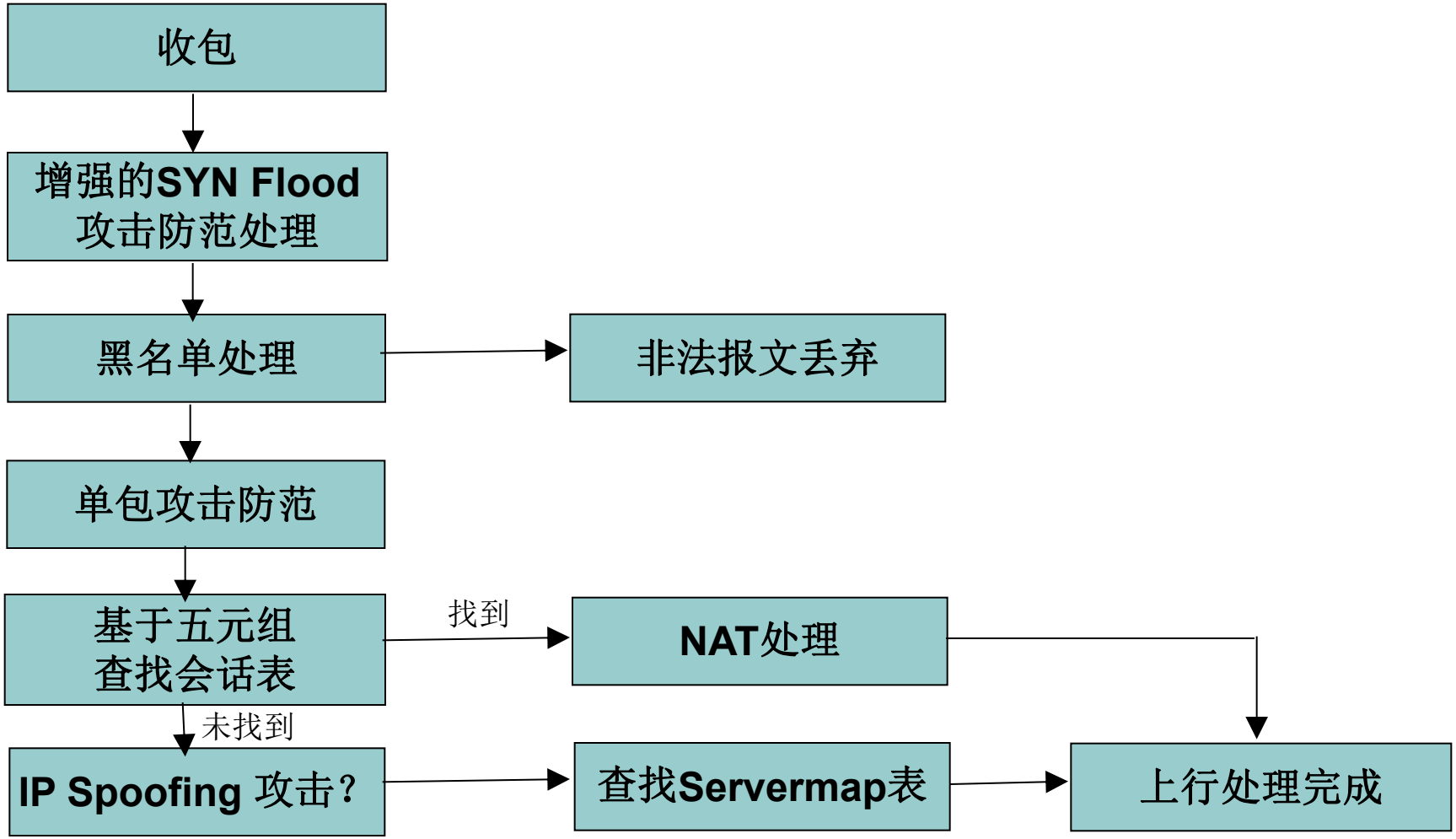
防火墙概要处理流程图—路由模式



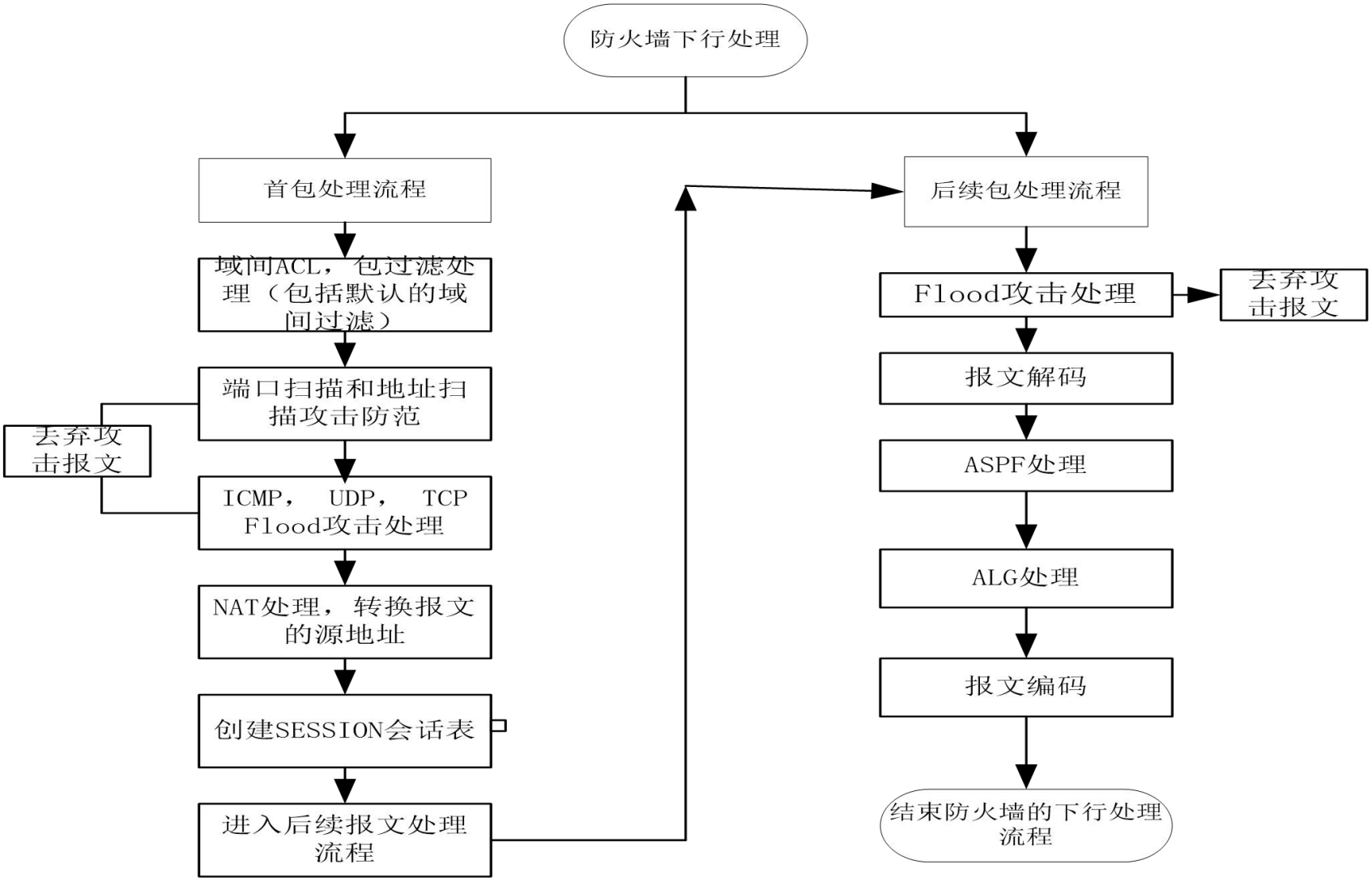
透明模式：概要处理流程图



防火墙上行处理—流程图


收包
增强的SYN Flood
攻击防范处理
黑名单处理
非法报文丢弃
单包攻击防范
基于五元组
查找会话表
找到
NAT处理
未找到
IP Spoofing 攻击?
查找Servermap表
上行处理完成

防火墙下行处理—流程图


防火墙下行处理
首包处理流程
域间ACL，包过滤处理（包括默认的域间过滤）
端口扫描和地址扫描攻击防范
丢弃攻击报文
ICMP， UDP， TCP Flood攻击处理
NAT处理，转换报文的源地址
创建SESSION会话表
进入后续报文处理流程
后续包处理流程
Flood攻击处理
丢弃攻击报文
报文解码
ASPF处理
ALG处理
报文编码
结束防火墙的下行处理流程

防火墙转发处理—快速转发

防火墙快转流程只适用于200， 处理过程和上面类似。

（1）为了提高转发效率

（2）为了进一步提高防火墙的转发效率，采用了cache机制

（3）实现了会话表的触发更新

目录

防火墙基本概念—安全区域（Zone）

- 域（Zone）：

域是防火墙上引入的一个重要的逻辑概念；通过将接口加入域并在安全区域之间启动安全检查（称为安全策略），从而对流经不同安全区域的信息流进行安全过滤。

防火墙的内部划分为多个区域，所有的转发接口都唯一的属于某个区域

防火墙基本概念—安全区域（Zone）续

防火墙上预定义了4个安全区域：

本地区域Local（指防火墙本身）、受信区域Trust、非军事化区域DMZ（Demilitarized Zone）、非受信区域Untrust，用户可以根据需要自行添加新的安全区域。

根据防火墙的内部划分的安全区域关系，确定其所连接网络的安全区域

会话

- 会话（Session）

  防火墙是状态防火墙，采用会话表维持通信状态。会话表包括五个元素：源IP地址、源端口、目的IP地址、目的端口和协议号。当防火墙收到报文后，根据上述五个元素查询会话表，并根据具体情况进行如下操作：

条件		操作
报文的五元组匹配会话表		转发该报文
报文的五元组不匹配会话表	域间规则允许通过	转发该报文，并创建会话表表项
	域间规则不允许通过	丢弃该报文

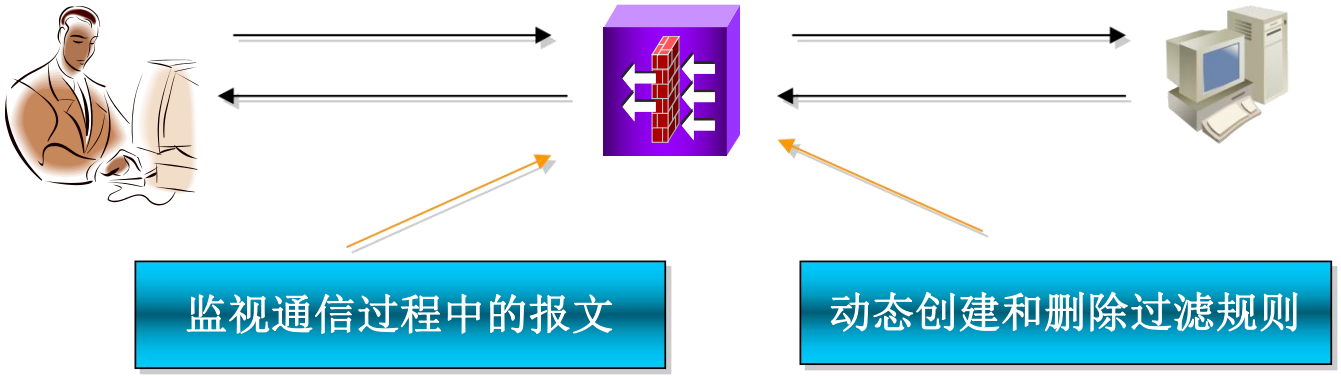
防火墙基本概念—多通道协议&服务表项

- 多通道协议：应用在进行通讯或提供服务时需要建立两个以上的会话（通道），其中有一个控制通道，其他的通道是根据控制通道中双方协商的信息动态创建的，一般我们称之为数据通道或子通道，这样的协议我们称为多通道协议。

- ServerMap：对于多通道协议（比如FTP），五元组过于严厉，导致多通道协议无法通过会话检查，所以为了达到对多通道协议的支持，开发除了ServerMap这样的数据结构。

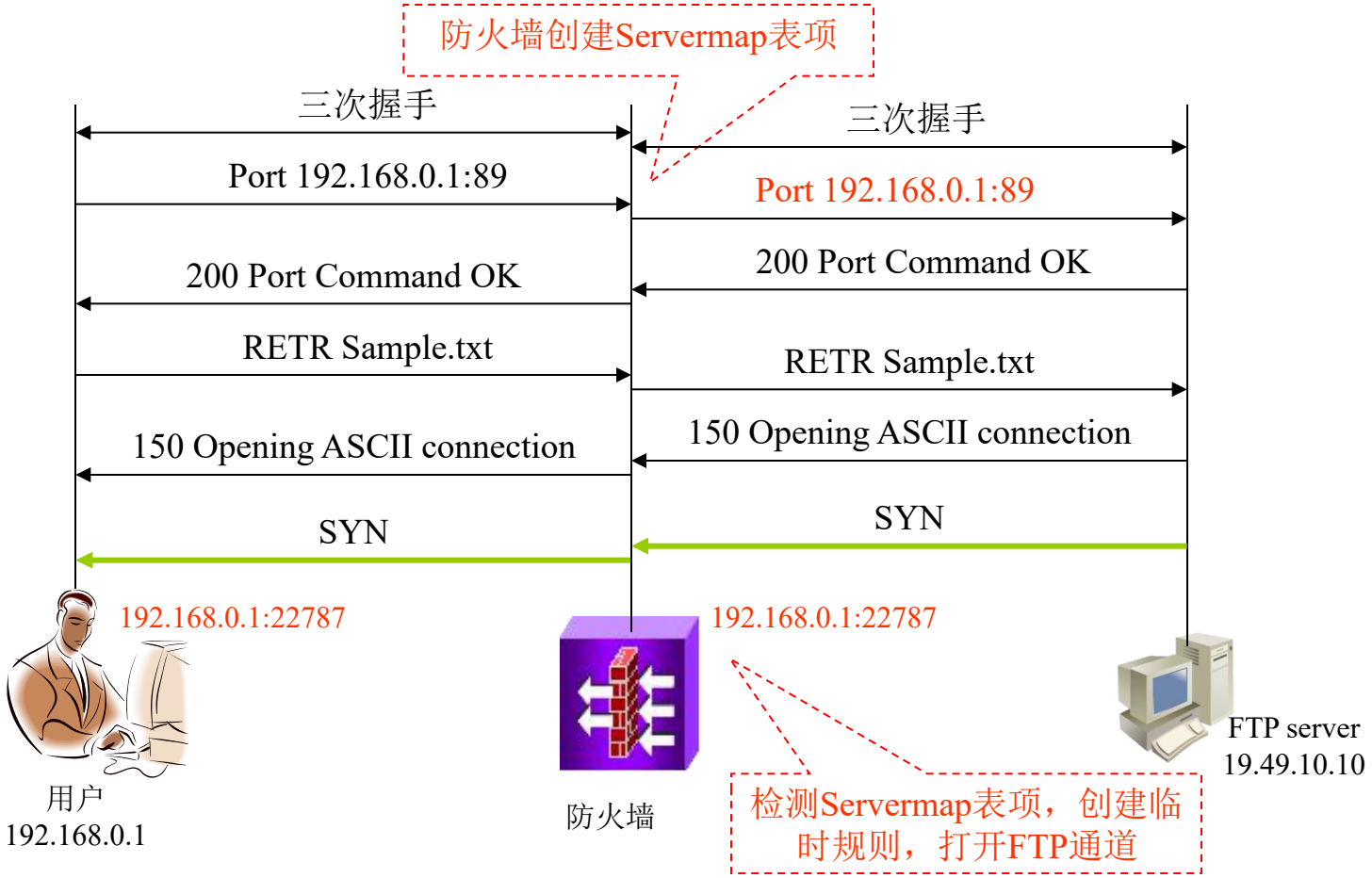
防火墙基本概念—— ASPF

- ASPF(Application Specific Packet Filter)：
  - 是一种改进的高级通信过滤技术，ASPF不但对报文的网络层的信息进行检测，还能对丰富的应用层协议进行深度检测，支持多媒体业务的NAT以及安全防范功能。



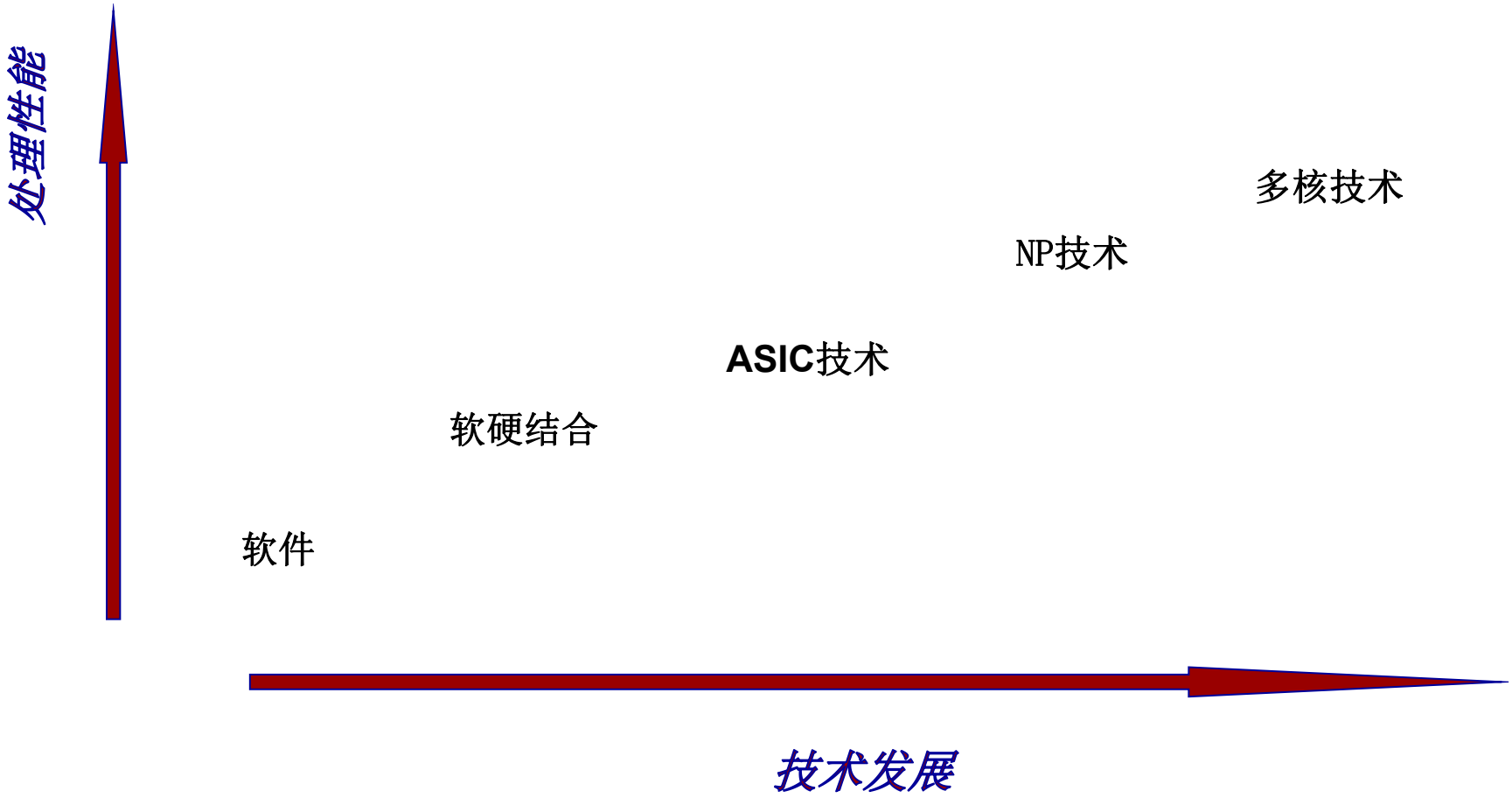
丰富的ASPF功能保证开展业务时安全性得到保证

ASPF 对多通道协议的支持



可以针对某些多通道协议（例如FTP）报文中的内容动态决定是否允许其通过防火墙。

防火墙产品技术发展趋势



谢谢