

计算机网络安全

华中科技大学

第二部分 网络安全技术与应用

第4讲 防火墙技术



第4讲 防火墙技术

一

防火墙概述

二

包过滤防火墙

三

状态检测防火墙

四

应用代理防火墙

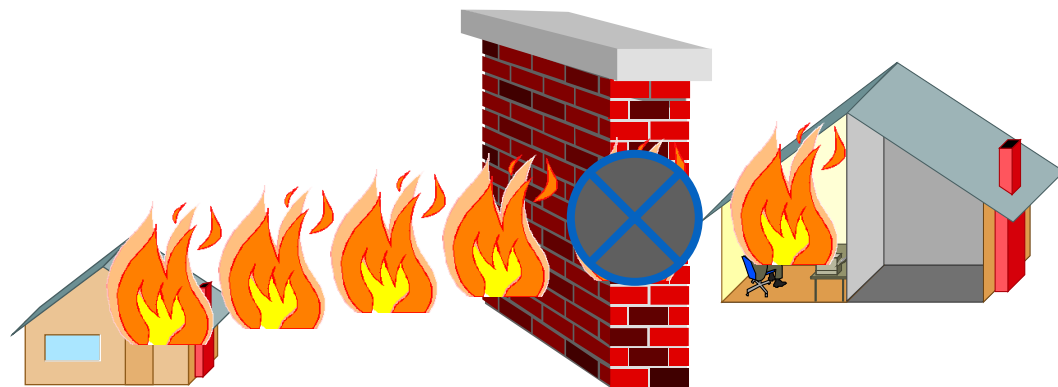
五

防火墙技术发展

1.1 防火墙的概念

➤ 原义

- ◆ 建筑设计领域
- ◆ 建筑中防止火灾蔓延至相邻区域的不燃性墙体
- ◆ 目的：隔离火灾风险



1.1 防火墙的概念

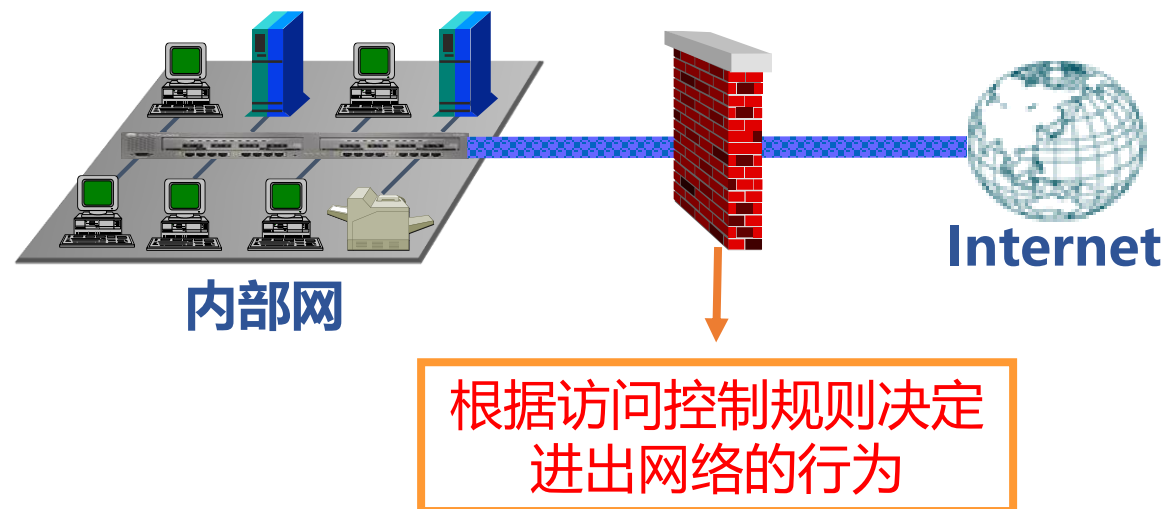


1.1 防火墙的概念

➤ 引申

- ◆ 网络安全领域，Firewall
- ◆ 内外网络边界上的过滤控制机制
 - ✓ 内部网络：安全、可信赖
 - ✓ 外部网络：安全性未知
- ◆ 功能：检查进出边界的数据流，防止未授权通信威胁内部网络安全

两个安全域之间通信流的唯一通道，
内外网之间的所有数据流都要流经防火墙



1.2 防火墙的基本要求

- 必经之路
- 授权放行
- 入侵免疫

1.3 防火墙的动作

- 允许 (ACCEPT)
- 拒绝 (REJECT) : 有反馈
- 丢弃 (DROP) : 无反馈 (发送者需等待超时)

1.4 防火墙的默认策略

- 默认允许
- 默认拒绝/丢弃：更安全

1.5 防火墙的分类

➤ 按形态分类

◆ 硬件防火墙



◆ 软件防火墙

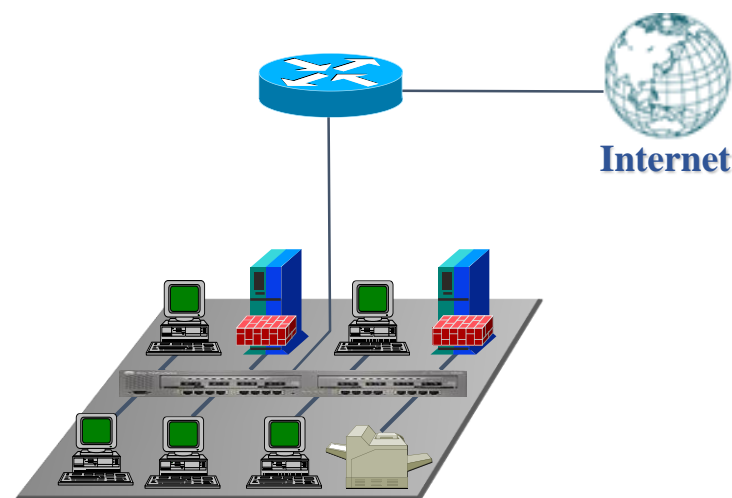
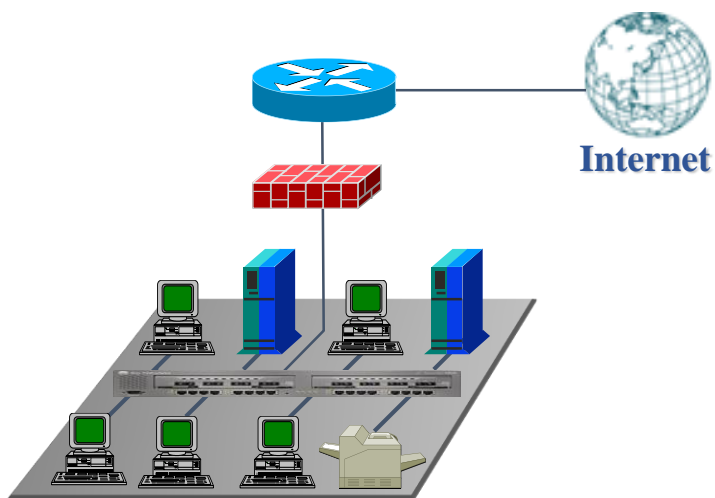


1.6 防火墙的分类

➤ 按保护对象分类

◆ 网络防火墙——保护整个网络

◆ 个人防火墙——保护单台主机



1.7 防火墙的性能指标

➤ 吞吐量——带宽

- ◆ 防火墙在不丢失数据包的情况下能达到的最大的转发数据包的速率

➤ 时延——快慢

- ◆ 从防火墙接收接口上输入帧的最后一个比特到达，到发送接口上输出帧的第一个比特发出所用的时间间隔

➤ 丢包率——稳定性

- ◆ 防火墙在不同负载情况下，由于资源不足应转发但丢弃的数据包比例

➤ 并发连接数——容量

- ◆ 防火墙能同时处理的，内外网主机通过防火墙通信的数据连接的最大数量

1.8 防火墙的作用

- 网络安全的中心 “扼制点”
- 集中强化安全策略
- 监视网络安全性
- 网络通信审计监控

1.9 防火墙的局限性

- 不能防范不经过它的攻击
- 不能防范来自内部网络的攻击
- 不能防范策略配置不当引起的威胁
- 不能防范物理接触破坏
- 不能防范对自身漏洞的攻击

1.10 防火墙安全区域

- 防火墙使用安全区域来区分一个网络是否安全
- 4个默认安全区域
 - ◆ Local——防火墙自身，凡是防火墙主动发出的报文，均可认为从Local区域发出
 - ◆ Trust——受信任的区域，位于防火墙之内的可信网络，是防火墙要保护的目标。主要用于连接局域网内部网络。比如企业网络中，通常员工网络设置为Trust区域
 - ◆ Dmz——非军事化区域，作为非信任区域与信任区域之间的缓冲区。一般用于防止企业内部服务器，如：OA服务器、邮件服务器等等

1.10 防火墙安全区域

- ◆ Untrust——不受信任的区域，处于防火墙之外的公开开放网络，由于Internet非常不安全，所以一般把连接Internet的接口划分到untrust区域，主要用于连接互联网。大部分情况下，非信任区域无法主动访问可信任区域
- 每个安全区域都会有一个安全级别，默认级别从高到低为
local>trust>dmz>untrust

1.11 防火墙工作模式

➤ 三种工作模式

◆ 路由模式（网关模式）

- ✓ 如果防火墙以第三层对外连接（接口具有IP 地址），则防火墙工作在路由模式下；

◆ 透明模式（桥模式）

- ✓ 若防火墙通过第二层对外连接（接口无IP 地址），则防火墙工作在透明模式下；

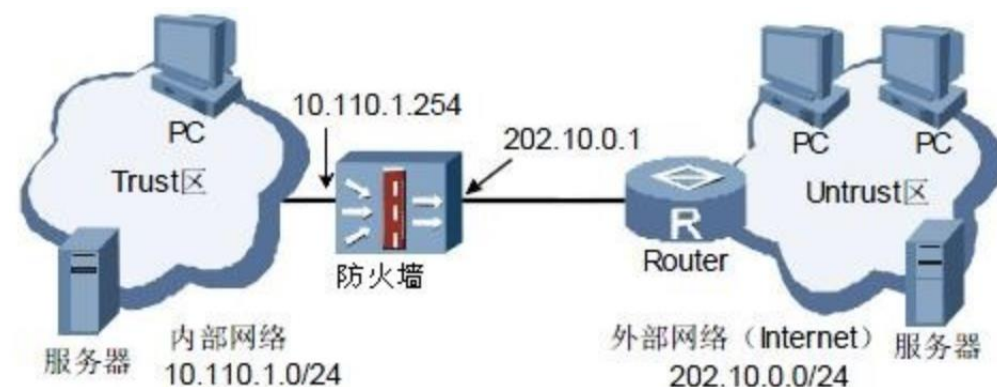
◆ 混合模式

- ✓ 若防火墙同时具有工作在路由模式和透明模式的接口（某些接口具有IP 地址，某些接口无IP 地址），则防火墙工作在混合模式下。

1.11 防火墙工作模式

➤ 路由模式

- ◆ 当防火墙位于内部网络和外部网络之间时，需要将防火墙与内部网络、外部网络以及DMZ三个区域相连的接口分别配置成不同网段的IP地址，重新规划原有的网络拓扑，此时相当于一台路由器
- ◆ 路由模式下可以完成ACL包过滤、ASPF动态过滤、NAT转换等
- ◆ 路由模式需要对网络拓扑进行修改（内部网络用户需要更改网关、路由器需要更改路由配置等），相当费事，使用需权衡利弊。



1.11 防火墙工作模式

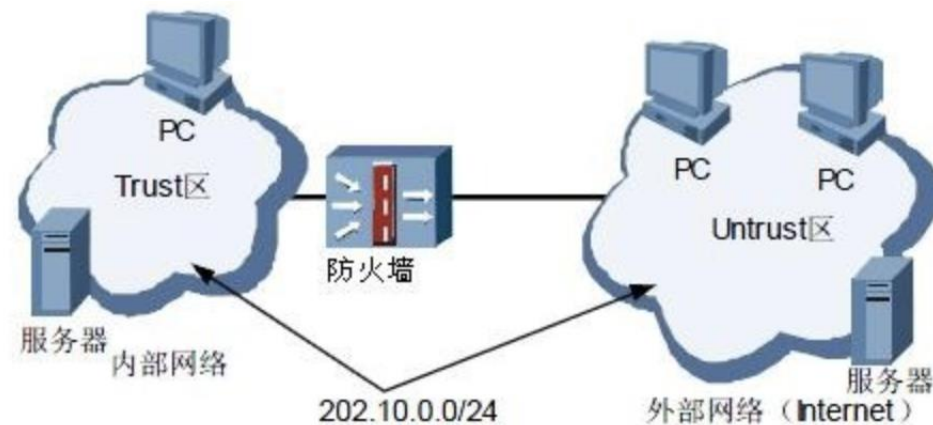
◆ 路由模式工作机制

- ✓ 所有接口都配置IP 地址，各接口所在的安全区域是三层区域，不同三层区域相关的接口连接的外部用户属于不同的子网。当报文在三层区域的接口间进行转发时，根据报文的IP 地址来查找路由表，此时防火墙表现为一个路由器。
- ✓ 防火墙与路由器存在不同，防火墙中IP报文还需要送到上层进行相关过滤等处理，通过检查会话表或访问控制列表(ACL)规则以确定是否允许该报文通过。此外，还要完成其它防攻击检查。路由模式的防火墙支持ACL规则检查、ASPF状态过滤、防攻击检查、流量监控等功能。

1.11 防火墙工作模式

➤ 透明模式

- ◆ 透明模式可以避免改变拓扑结构造成的麻烦，此时防火墙对于子网用户和路由器来说是完全透明的。也就是说，用户完全感觉不到防火墙的存在
- ◆ 采用透明模式时，只需在网络中像放置网桥（bridge）一样插入该防火墙设备即可，无需修改任何已有的配置。
- ◆ 与路由模式相同，IP报文同样经过相关的过滤检查（但是IP报文中的源或目的地址不会改变），内部网络用户依旧受到防火墙的保护



1.11 防火墙工作模式

◆ 透明模式工作机制

- ✓ 透明模式（也可以称为桥模式）下所有接口都不能配置IP 地址，接口所在的安全区域是二层区域，和二层区域相关接口连接的外部用户同属一个子网。当报文在二层区域的接口间进行转发时，需要根据报文的MAC 地址来寻找出接口，此时防火墙表现为一个透明网桥
- ✓ 防火墙与网桥存在不同，防火墙中IP报文还需要送到上层进行相关过滤等处理，通过检查会话表或访问控制列表(ACL) 规则以确定是否允许该报文通过
- ✓ 透明模式的防火墙支持ACL规则检查、ASPF状态过滤、防攻击检查、流量监控等功能。工作在透明模式下的 防火墙在数据链路层连接局域网（LAN），网络终端用户无需为连接网络而对设备进行特别配置，就像LAN Switch进行网络连接

1.11 防火墙工作模式

➤ 路由模式与透明模式对比

◆ 路由模式

- ✓ 优点：功能相对全面
- ✓ 缺点：需要对现有网络进行一定调整

◆ 透明模式

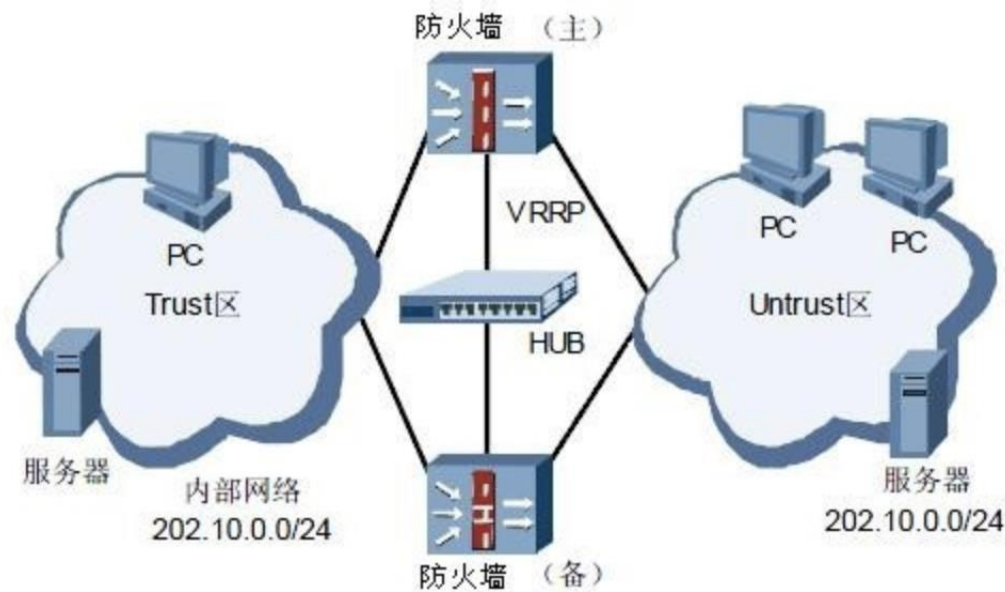
- ✓ 优点：不用重新进行IP划分
- ✓ 缺点：损失一些功能，如路由、VPN及nat等。

◆ 一般来说，如果是能用路由模式建议还是用路由模式

1.11 防火墙工作模式

➤ 混合模式

- ◆ 如果防火墙既存在工作在路由模式的接口（接口具有IP 地址），又存在工作在透明模式的接口（接口无IP 地址），则防火墙工作在混合模式下
- ◆ 例如：混合模式可用于透明模式作双机备份的情况，此时启动VRRP（Virtual Router Redundancy Protocol，虚拟路由冗余协议）功能的接口需要配置IP 地址，其它接口不配置IP地址



1.11 防火墙工作模式

◆ 混合模式工作机制

- ✓ 防火墙工作在混合透明模式下，此时部分接口配置IP 地址，部分接口不能配置IP 地址。
- ✓ 配置IP 地址的接口所在的安全区域是三层区域，接口上启动VRRP功能，用于双机热备份；
- ✓ 未配置IP地址的接口所在的安全区域是二层区域，和二层区域相关接口连接的外部用户同属一个子网
- ✓ 当报文在二层区域的接口间进行转发时，转发过程与透明模式的工作过程完全相同

第4讲 防火墙技术

一

防火墙概述

二

包过滤防火墙

三

状态检测防火墙

四

应用代理防火墙

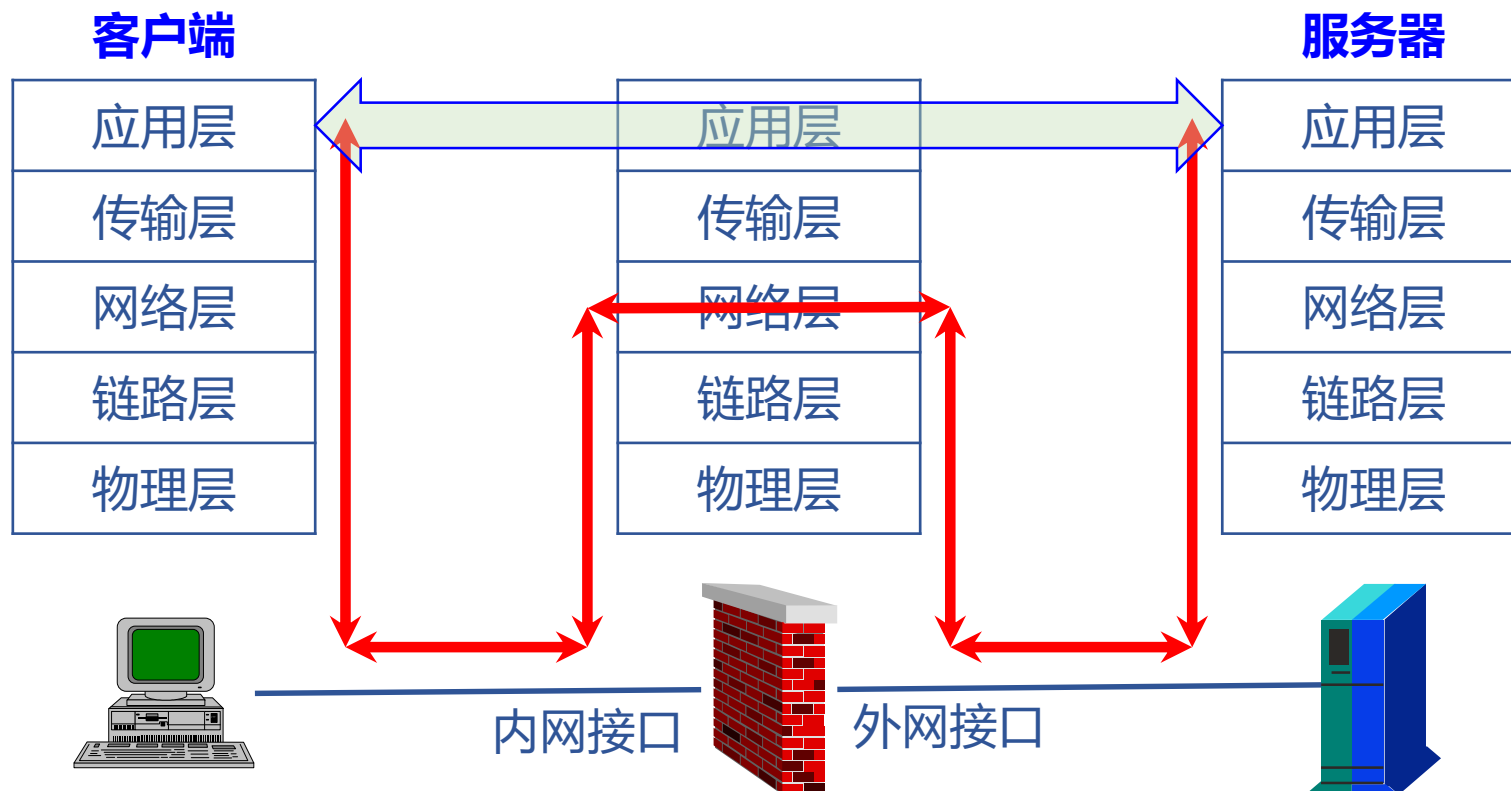
五

防火墙技术发展

2.1 基本概念

- 包过滤——Packet Filtering
- 处理对象——数据包
- 最基础的防火墙技术

2.2 包过滤工作机制



2.3 包过滤规则

➤ 组成

- ◆ 条件
- ◆ 动作

➤ 检查原则

- ◆ 顺序逐条检查
- ◆ 首条命中
- ◆ 每个数据包单独检查

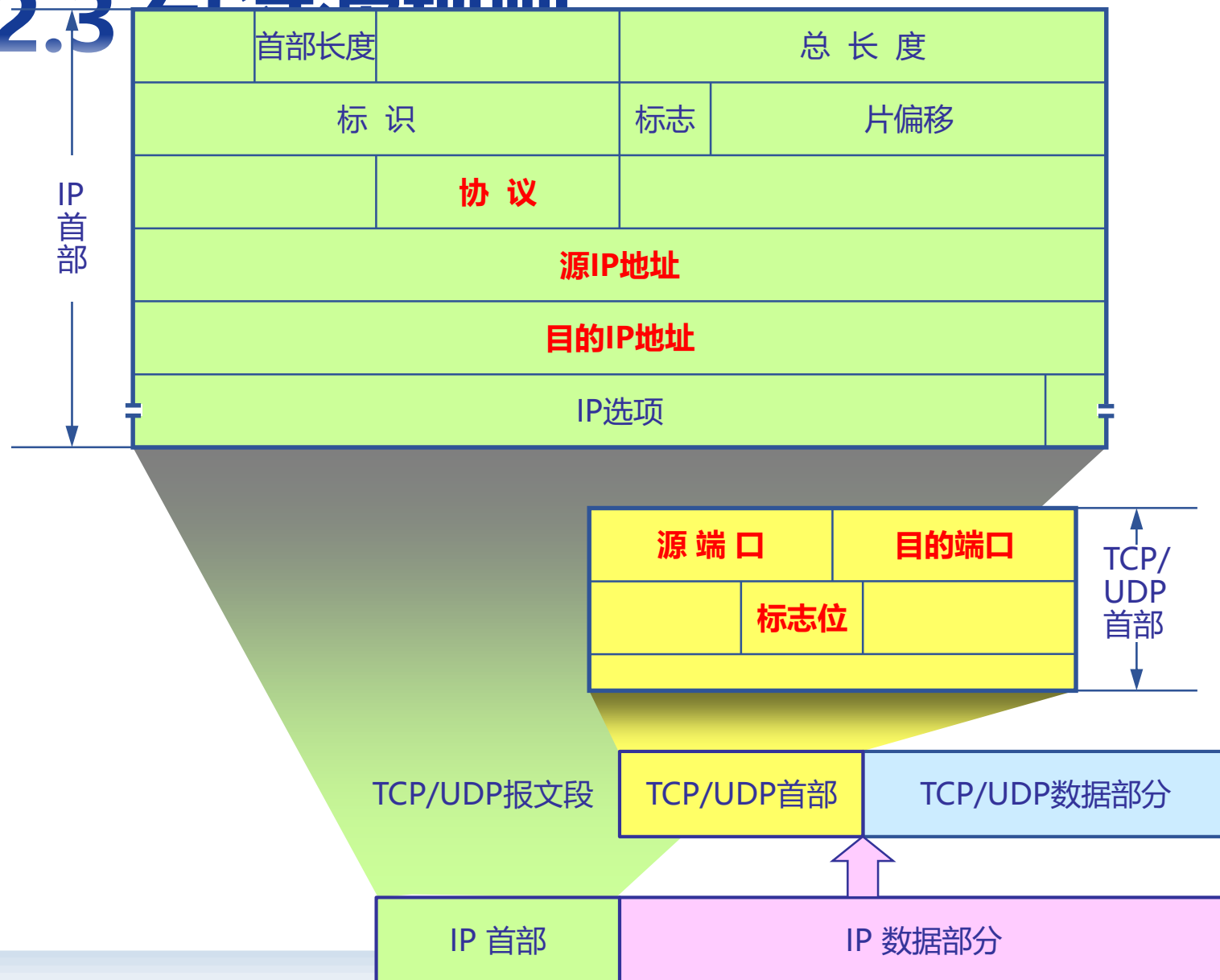
动 作	源	端 口	目 的	端 口	标 志	解 释
allow	secondary	*	our-dns	53	TCP	allow secondary nameserver access
block	*	*	*	53	TCP	no other DNS zone transfers
allow	*	*	*	53	UDP	permit UDP DNS queries
allow	ntp.outside	123	ntp.inside	123	UDP	ntp time access
block	*	*	*	69	UDP	no access to our tftpd
block	*	*	*	87	TCP	the link service is often misused
block	*	*	*	111	TCP	no TCP RPC and ...
block	*	*	*	111	UDP	no UDP RPC and no ...
block	*	*	*	2049	UDP	NFS. This is hardly a guarantee
block	*	*	*	2049	TCP	TCP NFS is coming: exclude it
block	*	*	*	512	TCP	no incoming "r" commands...
block	*	*	*	513	TCP	...
block	*	*	*	514	TCP	...
block	*	*	*	515	TCP	no external lpr
block	*	*	*	540	TCP	uucpd
block	*	*	*	6000-6100	TCP	no incoming X
allow	*	*	adminnet	443	TCP	encrypted access to transcript mgr
block	pclab-net	*	adminnet	*	TCP	nothing else
block	pclab-net	*	*	*	TCP	anon. students in pclab can't go outside
block	*	*	*	*	UDP	... not even with TFTP and the like!
allow	*	*	*	*	TCP	all other TCP is OK
block	*	*	*	*	UDP	suppress other UDP for now

2.3 检查规则

➤ 检查对象

- ◆ 源IP地址
- ◆ 目的IP地址
- ◆ 传输层协议
- ◆ 源端口
- ◆ 目的端口
- ◆ TCP ACK标志

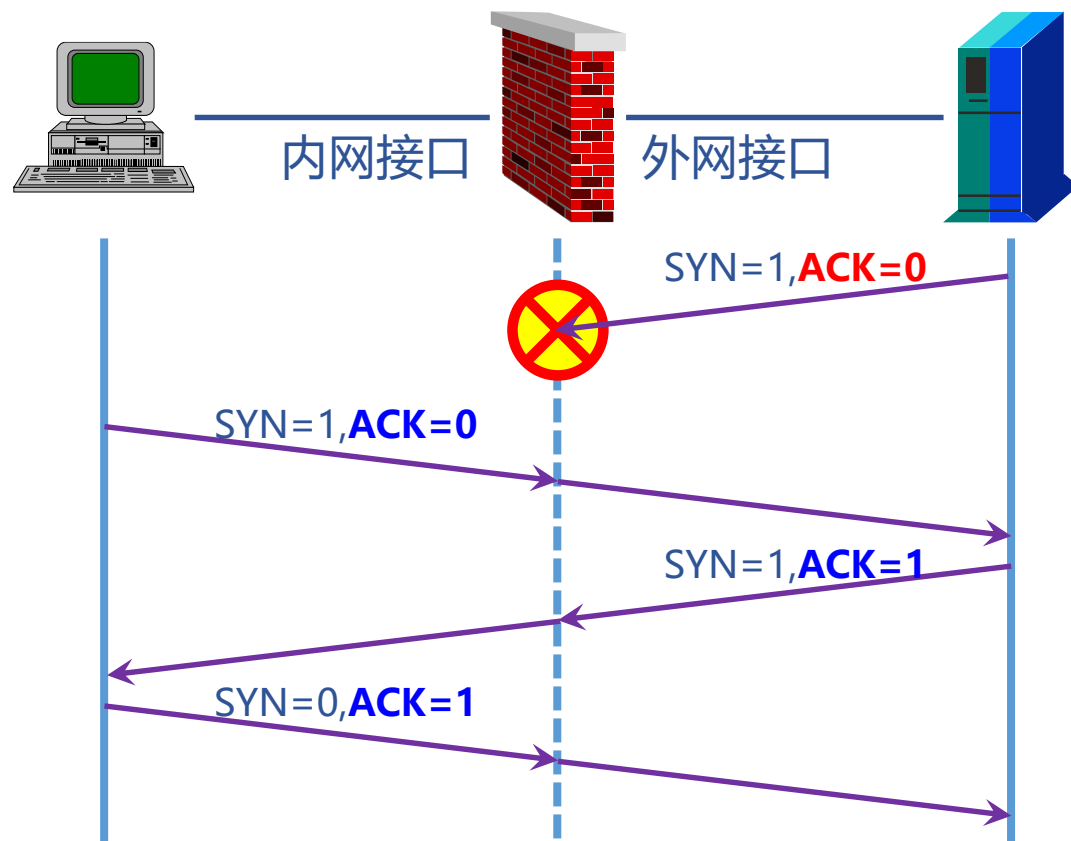
➤ 关于IP分片的检查



2.3 包过滤规则

➤ TCP ACK控制连接方向

- ◆ 外网→内网
 - ✓ ACK=0, 禁止
 - ✓ ACK=1, 允许
- ◆ 内网→外网
 - ✓ ACK=0或1, 允许
- ◆ 效果：外网向内网的连接企图被阻止



2.3 包过滤规则

➤ 规则制定的策略

- ◆ 按地址过滤：源IP、目的IP
- ◆ 按服务过滤：协议、源端口、目的端口
- ◆ 按连接方向过滤：ACK位
- ◆ 按时间、用户等过滤
- ◆ 对数据包做日志记录

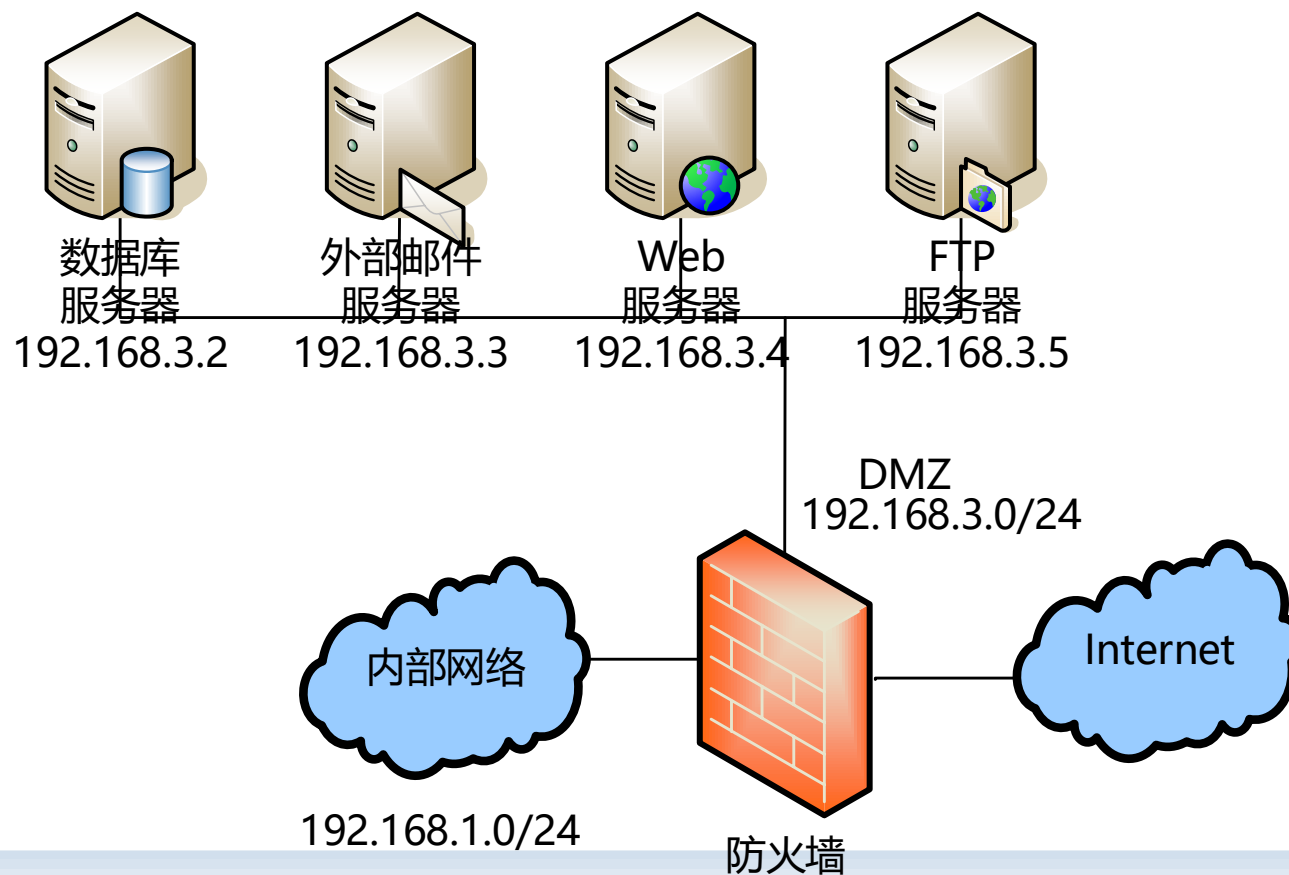
2.3 包过滤规则

➤ 设置规则的步骤

- ◆ 建立安全策略（分析并列列出所有允许的和禁止的任务）。
- ◆ 将安全策略转化为分组字段的逻辑表达式。
- ◆ 用防火墙提供的过滤规则句法重写逻辑表达式并设置。

2.4 包过滤配置实例

➤ 网络拓扑



2.4 包过滤配置实例

➤ 安全策略

- ◆ 任何时间，内网 → 邮件服务器：允许
- ◆ 任何时间，内网 → web服务器：允许
- ◆ 上班时间，内网 → Internet：允许
- ◆ 任何时间，Internet → 内网：禁止
- ◆ 任何时间，Internet → 邮件服务器：允许
- ◆ 任何时间，Internet → web服务器：允许
- ◆ 任何时间，Internet → 数据库服务器：禁止
- ◆ 其它：禁止

2.4 包过滤配置实例

➤ 逻辑表达式

- ◆ Sip=192.168.1.0/24 and dip=192.168.3.3 and (dport=25 or dport=110) , action=permit
- ◆ Sip=any and dip=192.168.1.0/24, action=reject
- ◆ Sip=any and dip=192.168.3.4 and dport=80, action=permit
- ◆ Sip=any and dip=192.168.3.2 and dport=1358, action=reject
- ◆
- ◆ Default=reject

2.4 包过滤配置实例

规则列表

源地址	源端口	协议	目的地址	目的端口	时间	动作
ANY	ANY	TCP	192.168.3.3	25,110	ANY	Permit
ANY	ANY	ANY	192.168.1.0/24	ANY	ANY	Reject
ANY	ANY	TCP	192.168.3.2	1358	ANY	Reject
ANY	ANY	TCP	192.168.3.4	80	ANY	Permit
192.168.1.0/24	ANY	ANY	ANY	ANY	WORK	Permit
ANY	ANY	ANY	ANY	ANY	ANY	Reject

2.4 包过滤配置实例

➤ 新的需求

- ◆ 上班时间，内网 → 数据库服务器：允许

源地址	源端口	协议	目的地址	目的端口	时间	动作
ANY	ANY	TCP	192.168.3.3	25,110	ANY	Permit
ANY	ANY	ANY	192.168.1.0/24	ANY	ANY	Reject
ANY	ANY	TCP	192.168.3.2	1358	ANY	Reject
ANY	ANY	TCP	192.168.3.4	80	ANY	Permit
192.168.1.0/24	ANY	ANY	ANY	ANY	WORK	Permit
ANY	ANY	ANY	ANY	ANY	ANY	Reject
192.168.1.0/24	ANY	TCP	192.168.3.2	1358	WORK	Permit

2.5 包过滤的优缺点

➤ 优点

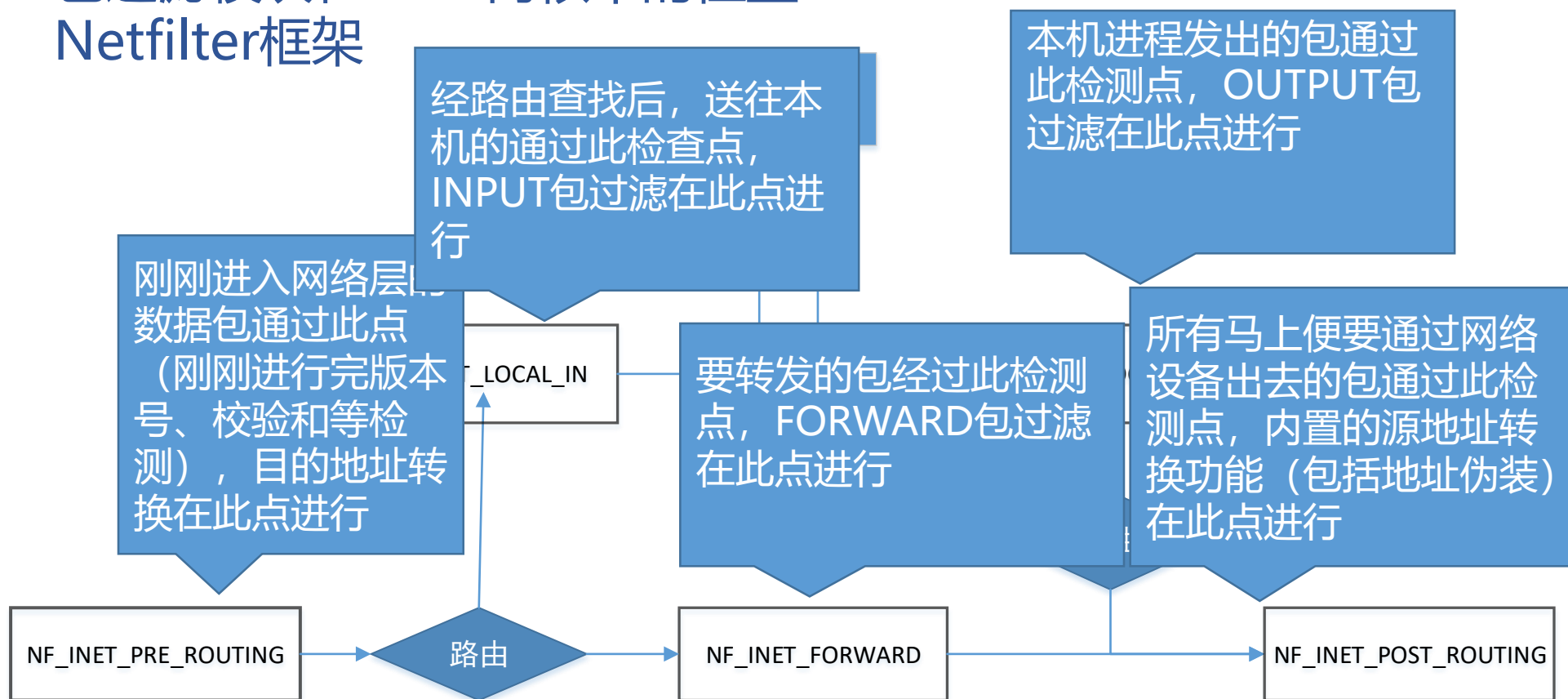
- ◆ 对网络性能影响较小
- ◆ 成本较低
- ◆ 对用户透明

➤ 缺点

- ◆ 访问控制规则配置较复杂
- ◆ 易受IP欺骗攻击
- ◆ 缺乏状态感知能力

2.6 Linux Netfilter架构

包过滤模块在linux内核中的位置
Netfilter框架



2.6 Linux Netfilter架构

➤ Netfilter hook 点

Hook点	调用的时机
NF_INET_PRE_ROUTING	刚刚进入网络层的数据包通过此点（刚刚进行完版本号、校验和等检测），目的地址转换在此点进行。
NF_INET_LOCAL_IN	经路由查找后，送往本机的通过此检查点，INPUT包过滤在此点进行
NF_INET_FORWARD	要转发的包经过此检测点，FORWARD包过滤在此点进行
NF_INET_LOCAL_OUT	本机进程发出的包通过此检测点，OUTPUT包过滤在此点进行
NF_INET_POST_ROUTING	所有马上便要通过网络设备出去的包通过此检测点，内置的源地址转换功能（包括地址伪装）在此点进行

2.6 Linux Netfilter架构

- Hook函数返回值：在hook函数完成了对数据包的操作之后，必须返回一个预定义的Netfilter返回值

返回值	含义
NF_DROP	丢弃该数据包
NF_ACCEPT	保留该数据包
NF_STOLEN	告知netfilter忽略该数据包
NF_QUEUE	将该数据包插入到用户空间
NF_REPEAT	请求netfilter再次调用该HOOK函数

第4讲 防火墙技术

一

防火墙概述

二

包过滤防火墙

三

状态检测防火墙

四

应用代理防火墙

五

防火墙技术发展

3.1 包过滤的问题

➤ 效率低

- ◆ 规则列表顺序匹配
- ◆ 一个数据流的每个数据包特征相同重复检查

➤ 易用性

- ◆ 一个数据流的正反方向要配一对规则
- ◆ 协商端口的动态数据流没法预先配规则，若放开所有端口安全性下降
 - ✓ FTP数据连接
 - ✓ 流媒体协议H.323、SIP
 - ✓ 数据库协议SQLNET

➤ 安全性低

- ◆ 只检查数据包首部，不检查数据

3.2 解决思路——状态检测

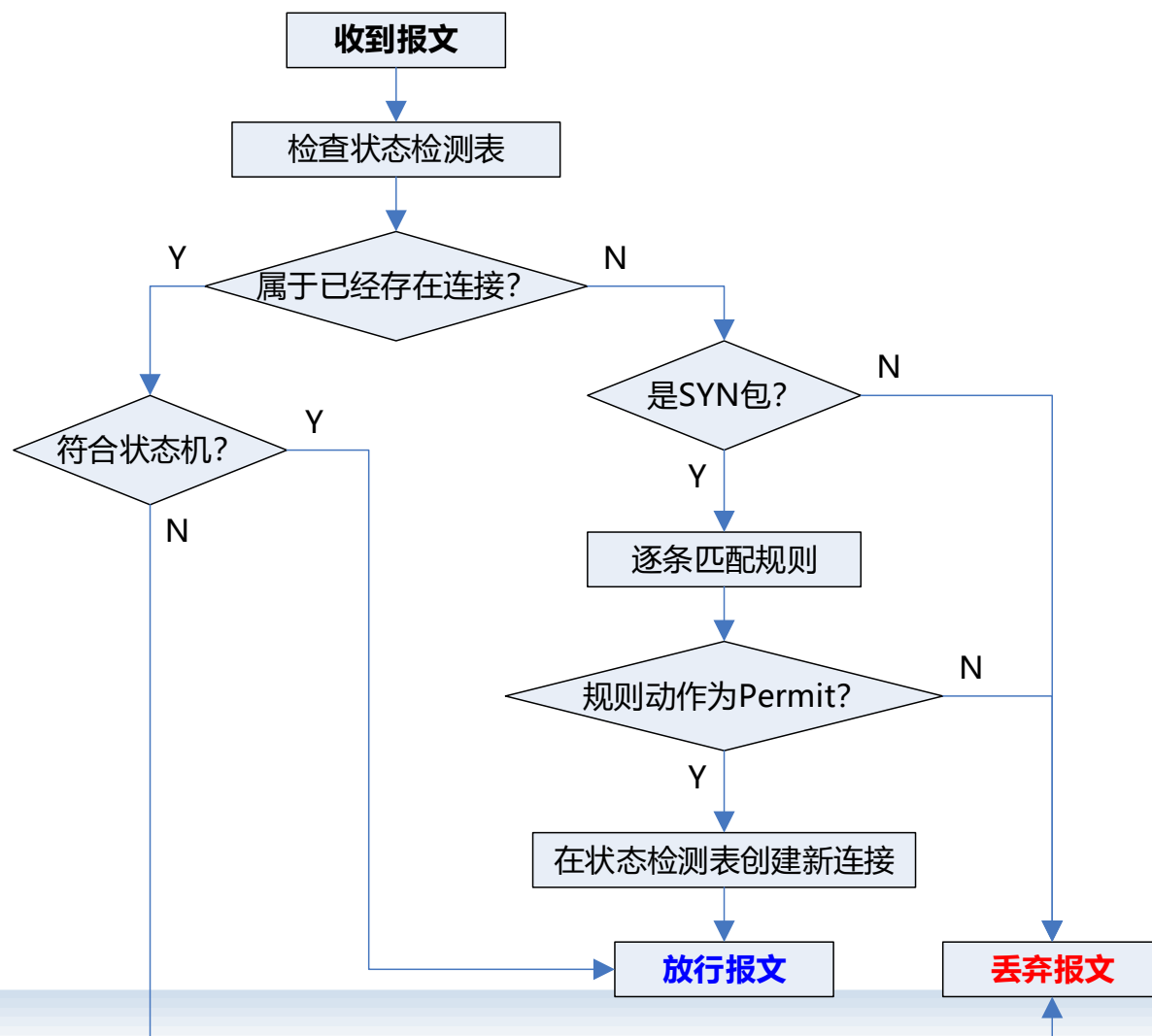
- 一个数据流的所有数据包有内在联系→连接→状态表
- 效率
 - ◆ 数据流的第一个数据包，检查规则表，新建连接
 - ◆ 后续数据包，检查状态表
- 易用性
 - ◆ 单向配置规则，双向检查状态表
 - ◆ 配置主连接规则，追踪分析数据流，为动态端口自动创建连接
- 安全性
 - ◆ 追踪连接数据流，可对数据检查

3.3 状态检测表（连接表）

- 状态检测表包括所有通过防火墙的连接
- 连接的信息（状态）
 - ◆ 源、目的IP地址
 - ◆ 协议类型
 - ◆ 传输层信息：TCP/UDP端口、ICMP ID号
 - ◆ 连接状态：TCP连接状态
 - ◆ 超时时间

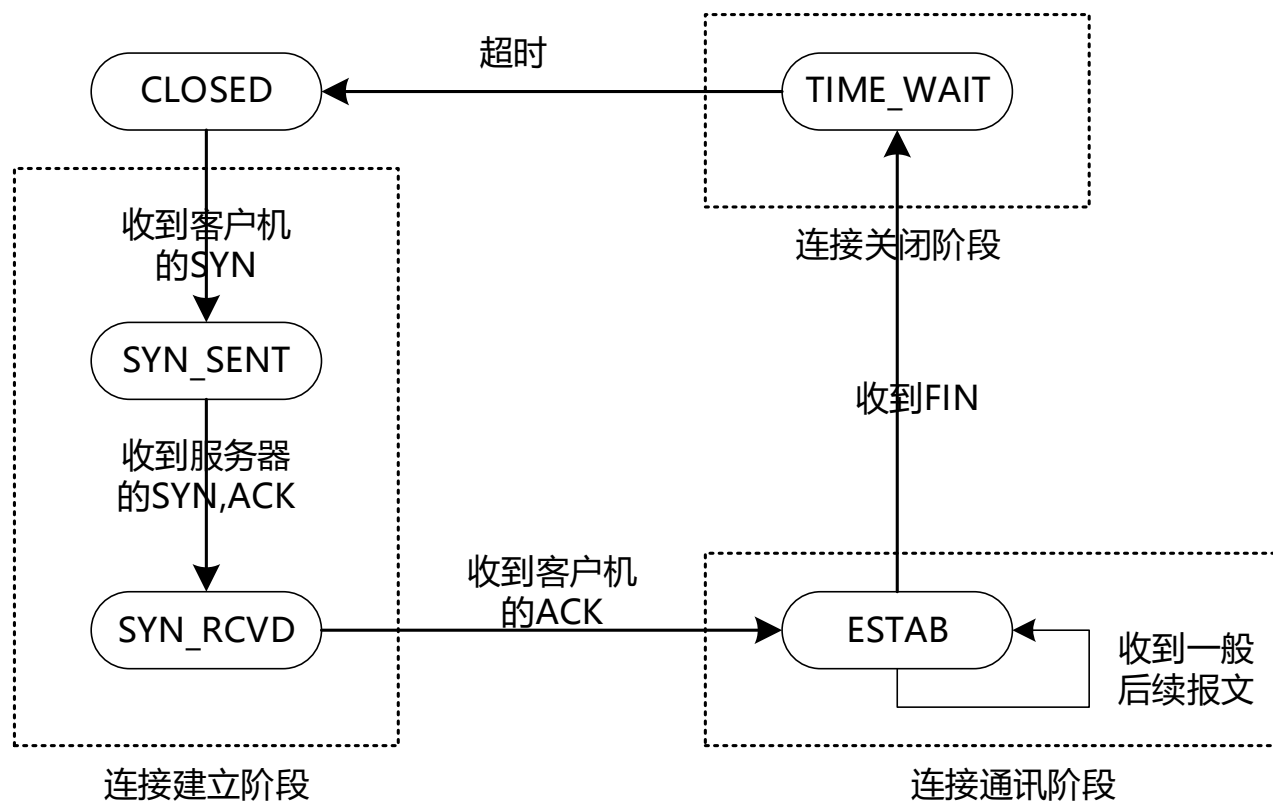
3.4 TCP状态检测

➤ 基本流程



3.4 TCP状态检测

➤ 简化的TCP状态机



3.5 非TCP状态检测

➤ 防火墙建立虚拟连接

◆ UDP

- ✓ 一方发出UDP包，如DNS请求，建立连接
- ✓ UDP应答的源和目的反向匹配连接，允许通过

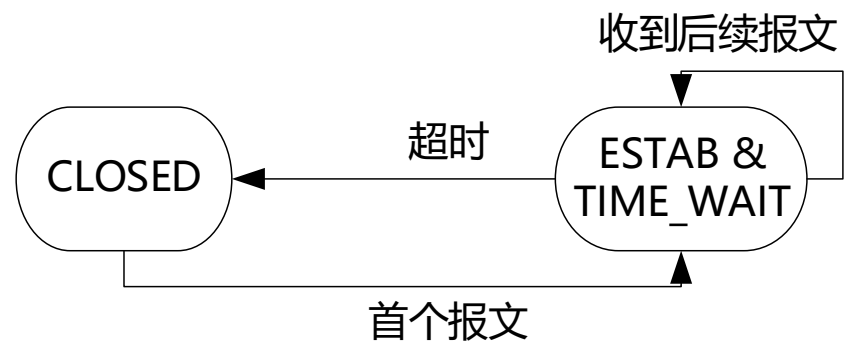
◆ ICMP

- ✓ 信息查询报文，如ping (echo request) 包，建立连接
- ✓ 源和目的IP反向匹配的echo reply包，允许通过

➤ 这些状态的超时时间比较短

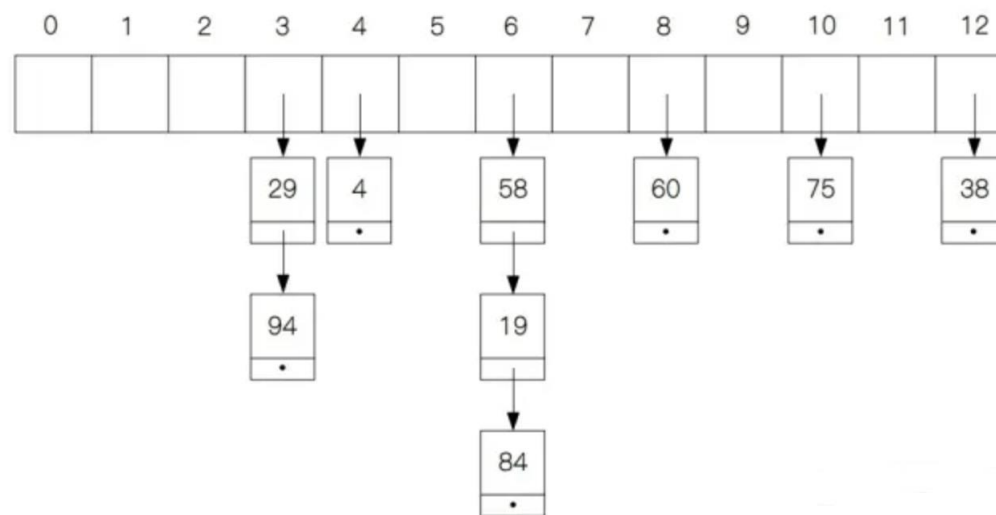
3.5 非TCP状态检测

➤ 虚拟UDP状态机



3.6 连接表的组织

- 非线性数据结构——hash表
- 快速匹配
- 可用硬件加速进一步加快



3.7 状态检测防火墙优缺点

➤ 优点

- ◆ 速度更快，性能更强
- ◆ 安全性提升
- ◆ 配置更简单
- ◆ 对用户透明

➤ 缺点

- ◆ 主要在协议栈中工作，对病毒等威胁防护不足
- ◆ 用户的C/S连接得到保持，存在内网信息泄露风险

第4讲 防火墙技术

一

防火墙概述

二

包过滤防火墙

三

状态检测防火墙

四

应用代理防火墙

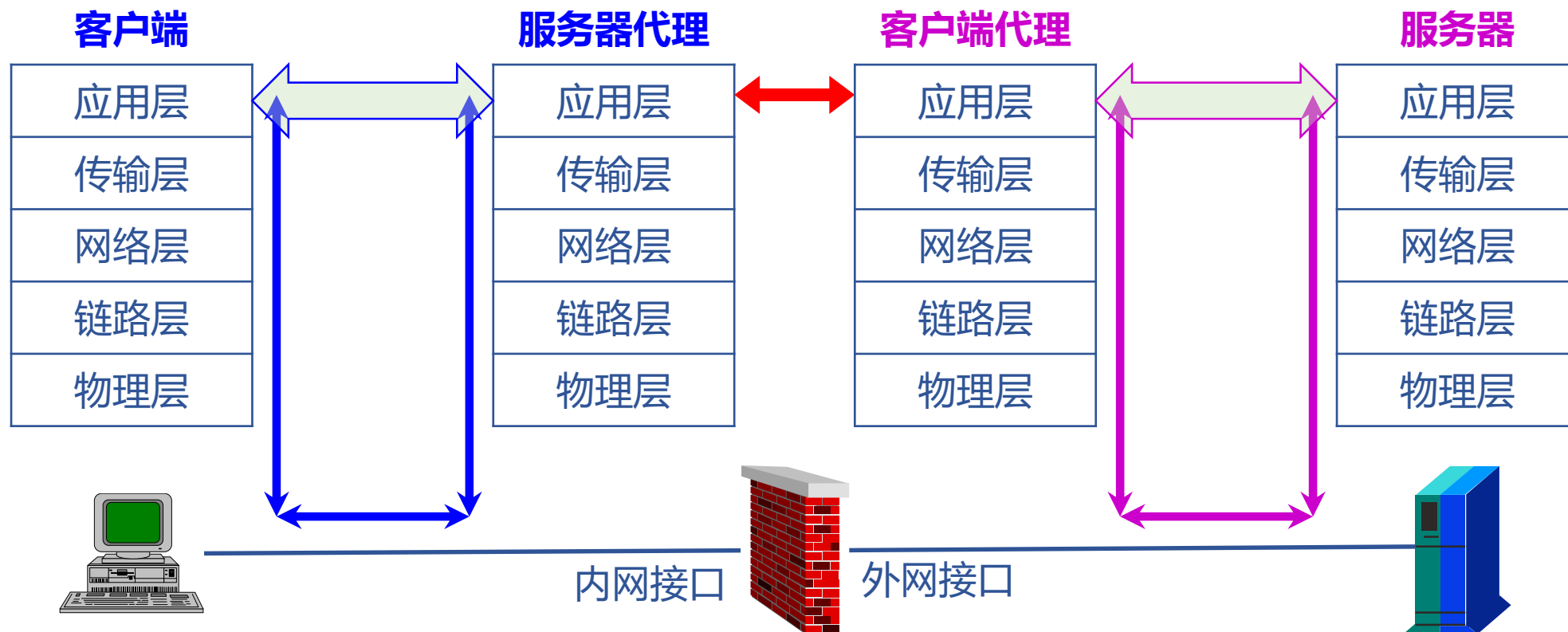
五

防火墙技术发展

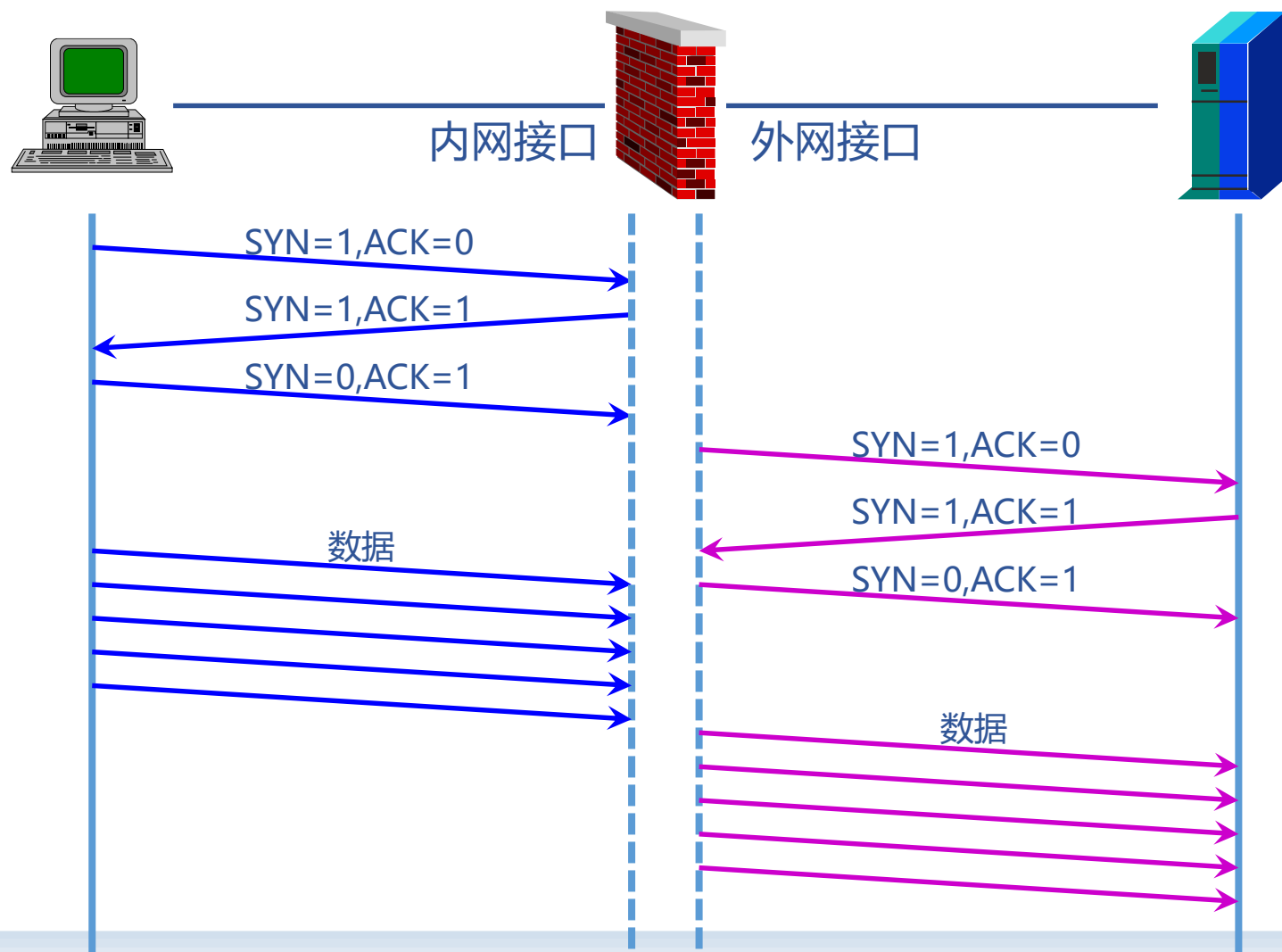
4.1 应用代理的提出

- 面向数据包的技术不足
 - ◆ 内核协议栈实现，功能受限
 - ◆ 数据在客户端和服务端之间直传，存在风险
- 解决思路
 - ◆ 数据过滤提升到应用层实现
 - ◆ 断开客户端和服务器的直接连接
- 应用代理防火墙（应用级网关）

4.2 应用代理工作机制



4.2 应用代理工作机制



4.3 应用代理的功能

➤ 基本访问控制

- ◆ 源是否允许访问
- ◆ 目的是否允许被访问
- ◆ ...

➤ 应用数据检查

- ◆ 检查通信是否符合协议
- ◆ 检查应用级的用户合法性
- ◆ 深度检查和审计传输的数据内容
- ◆ 数据对象缓存传输

代理对象

对象名称:

HTTP方法:
☐ Get ☐ Head ☐ Option ☐ Post ☐ Put ☐ Delete ☐ Trace

网站域名:
添加 删除

URL路径名:
添加 删除

动作: ☒ 允许 ☐ 禁止 日志: ☒ 是 ☐ 否

病毒检查: ☒ 启用 ☐ 不启用

过滤: ☐ JavaApplet ☐ JavaScript ☐ VBScript ☐ ActiveX

优化: ☐ 缩小图片尺寸 ☐ 降低图片质量 ☐ web压缩

注释:

添加 关闭

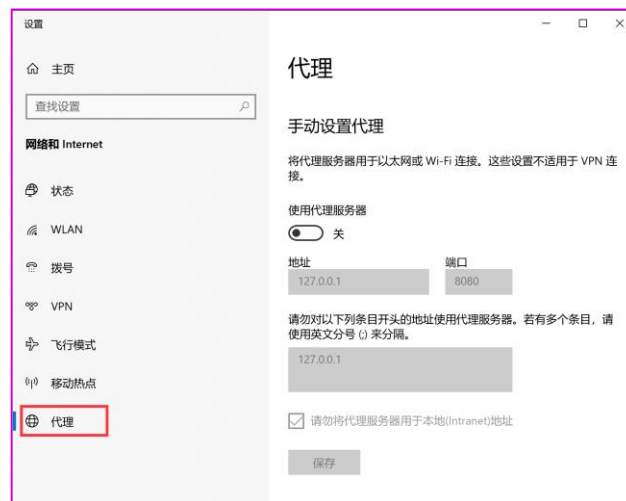
4.4 透明代理

➤ 普通代理

- ◆ 客户端专门设置
- ◆ 客户端专门功能

➤ 透明代理

- ◆ 客户端无感知
- ◆ 协议栈包过滤配合实现
 - ✓ 记录客户端消息的真实服务器地址，通知代理程序
 - ✓ 修改消息的目的地址为代理程序的监听地址
 - ✓ 服务器代理的应答消息，源地址改回真实服务器地址



4.5 应用代理的优缺点

➤ 优点

- ◆ 按协议进行内容过滤
- ◆ 可以调用其他安全功能
- ◆ 屏蔽保护内网信息

➤ 缺点

- ◆ 只支持特定服务，可扩展性不高
- ◆ 性能较低

第4讲 防火墙技术

一

防火墙概述

二

包过滤防火墙

三

状态检测防火墙

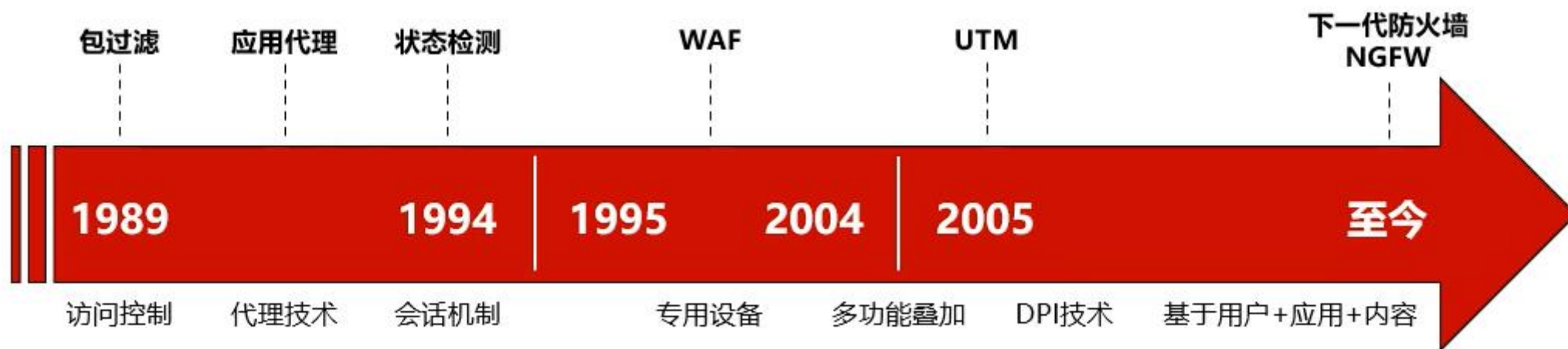
四

应用代理防火墙

五

防火墙技术发展

5.1 防火墙技术发展历程



5.2 统一威胁管理UTM

➤ 定义

- ◆ 由IDC提出的UTM是指由硬件、软件和网络技术组成的具有专门用途的设备，将多种安全功能和特性集成于一个硬设备里，构成一个标准的统一管理平台

➤ 功能

- ◆ FW、IDS、IPS、AV等**串行连接**

➤ 特点

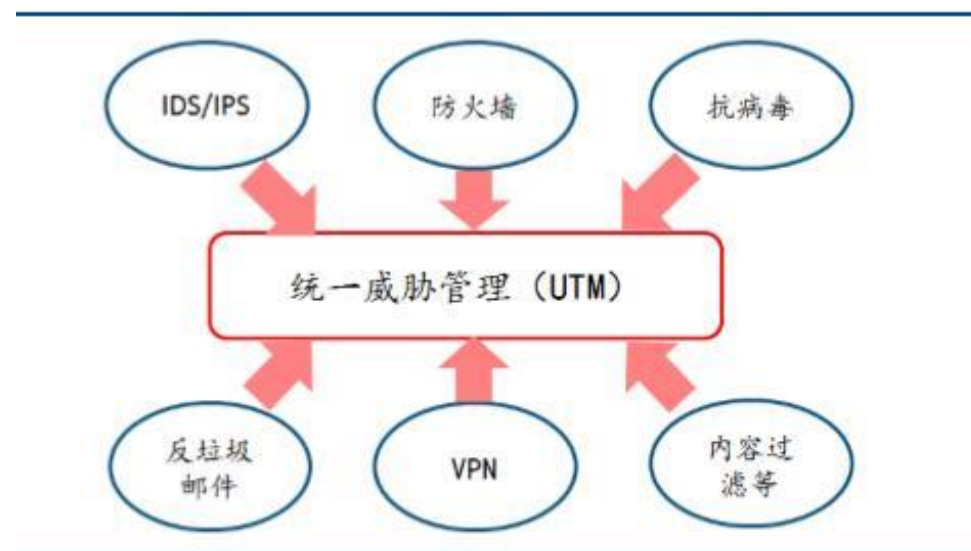
- ◆ 把应用网关和IPS等设备在状态检测防火墙的基础上进行整合和统一

➤ 优点

- ◆ 整合所带来的成本降低、降低信息安全工作强度、降低技术复杂度

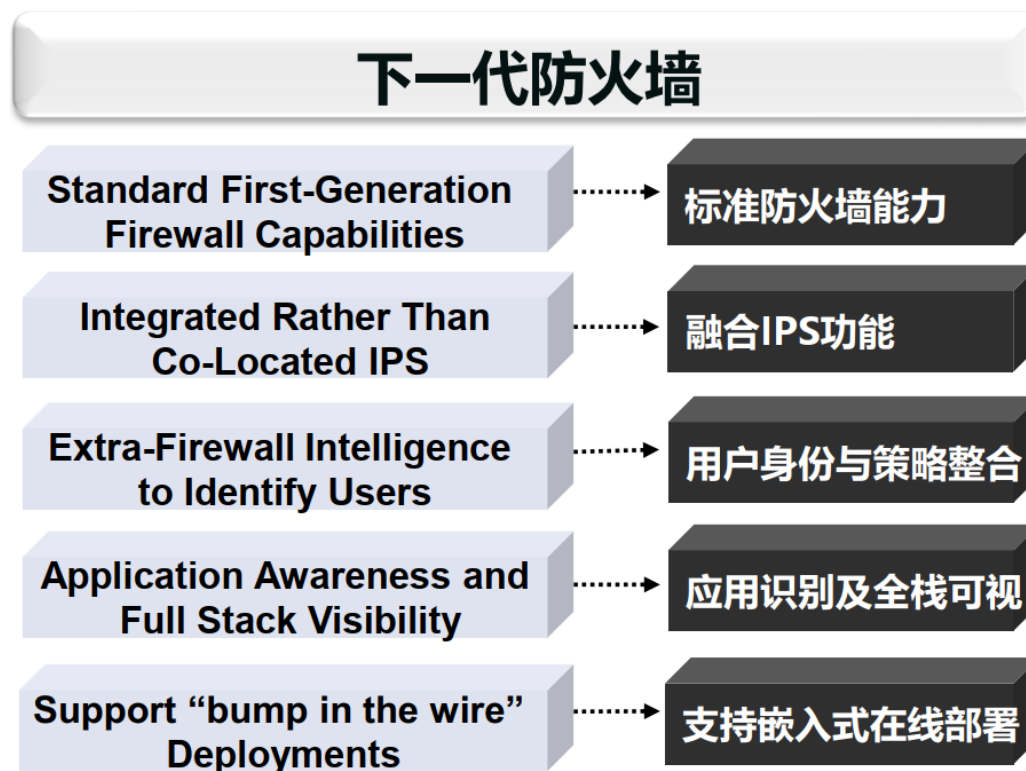
➤ 缺点

- ◆ 模块串联检测效率低，性能消耗大



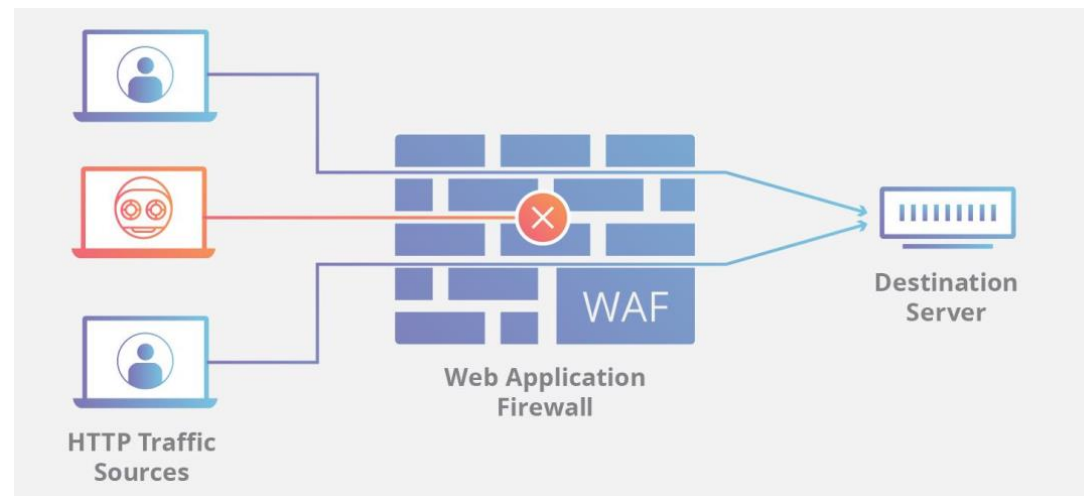
5.3 下一代防火墙 NG Firewall

- Next Generation Firewall, 简称NG Firewall, 全面应对**应用层威胁**的高性能防火墙
- 工作范围: 2-7层
- 核心处理
 - ◆ 会话管理、**应用识别**、内容检测
- 功能
 - ◆ FW、IDS、IPS、AV、WAF
- 优点
 - ◆ 与UTM相比增加的web应用防护功能, 功能更全
 - ◆ UTM是串行处理机制, NGFW是**并行处理**机制, 效率更高
 - ◆ NGFW的性能更强, 管理更高效



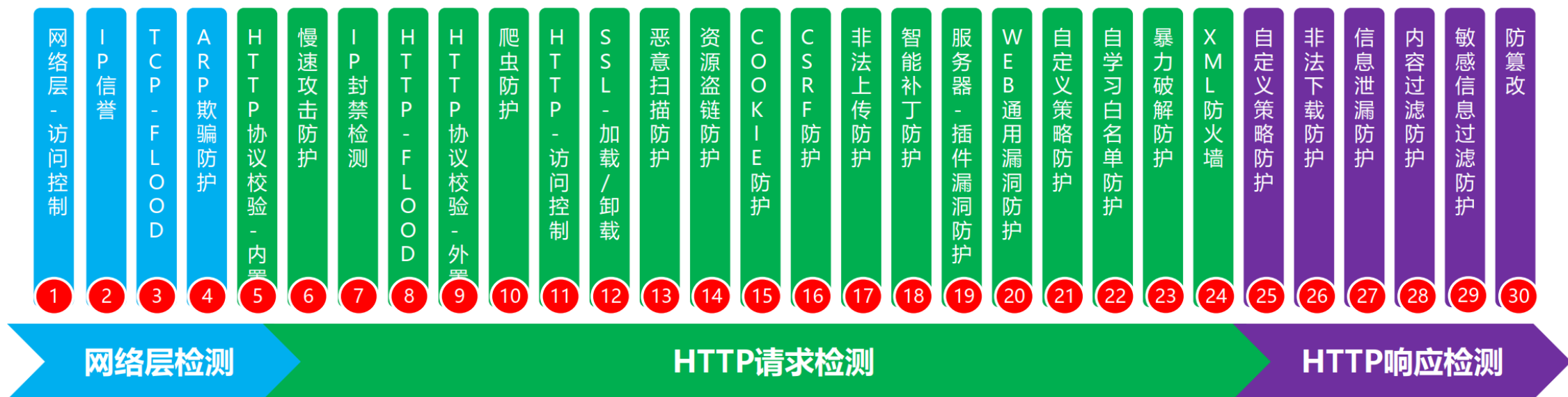
5.4 WEB应用防火墙WAF

- 工作范围：应用层（7层）
- 目的：防止基于应用层的攻击影响**Web应用**系统
- 主要技术原理：
 - ◆ 判断信息：HTTP协议数据的request和response
 - ◆ 代理服务：会话双向代理，用户与服务器不产生直接链接，对于DDOS攻击可以抑制
 - ◆ 特征识别：通过正则表达式的特征库进行特征识别
 - ◆ 算法识别：针对攻击方式进行模式化识别，如SQL注入、DDOS、XSS等



5.4 WEB应用防火墙WAF

➤ WAF常见功能



谢谢观看

