2014’中国教育和科研计算机网
华东北地区教育信息化技术研讨会

嵌入式防火墙及其关键技术研究

南京航空航天大学计算机科学与技术学院
陈 兵

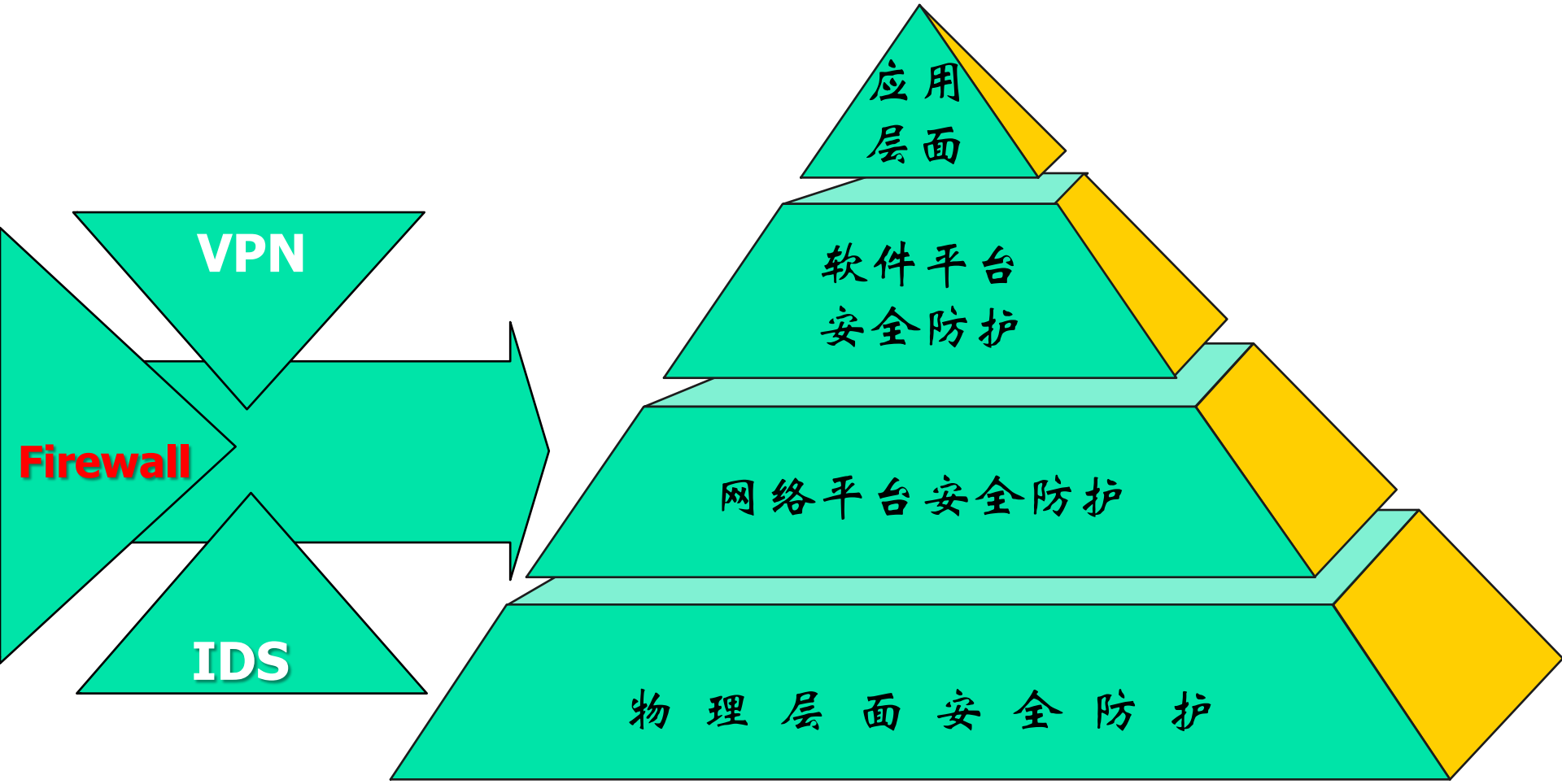
主要内容

1. 问题的引出
2. 研究内容之一:包分类
3. 研究内容之二:策略生成
4. 研究内容之三:策略分发
5. 研究内容之四:实现机制
6. 展望

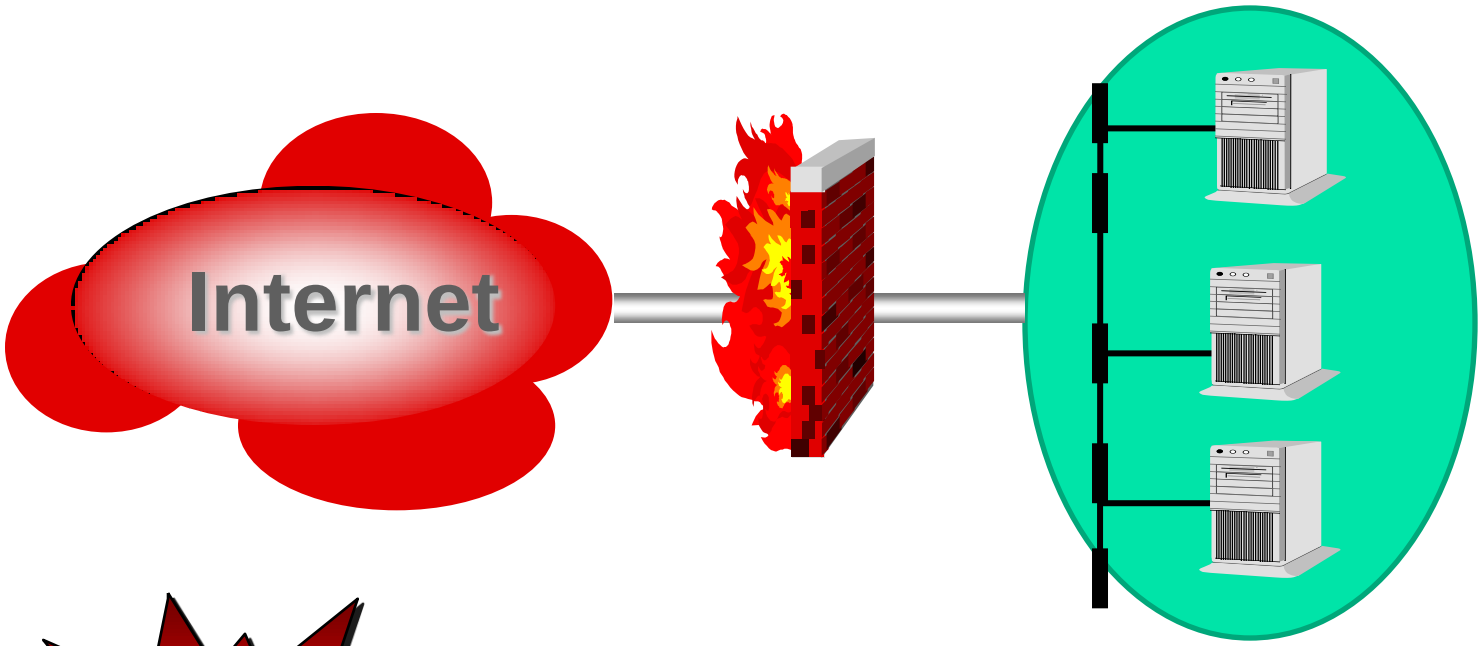
网络威胁来自何处？

- 各种恶意攻击(Virus,Trojan horse etc.)
- 系统本身的安全缺陷（patch）
- 各种应用软件的漏洞（update）

网络安全防范技术



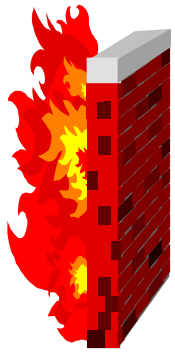
网络安全防范的对象



外部网络：
不可信任

内部网络：
可信任

集中式防火墙



- **William Cheswick和Steve Beilovin（1994）：**

  防火墙是放置在两个网络之间的一组组件，性质：

  1. 只允许本地安全策略授权的通信信息通过
  2. 双向通信信息必须通过防火墙
  3. 防火墙本身不会影响信息的流通

集中式防火墙

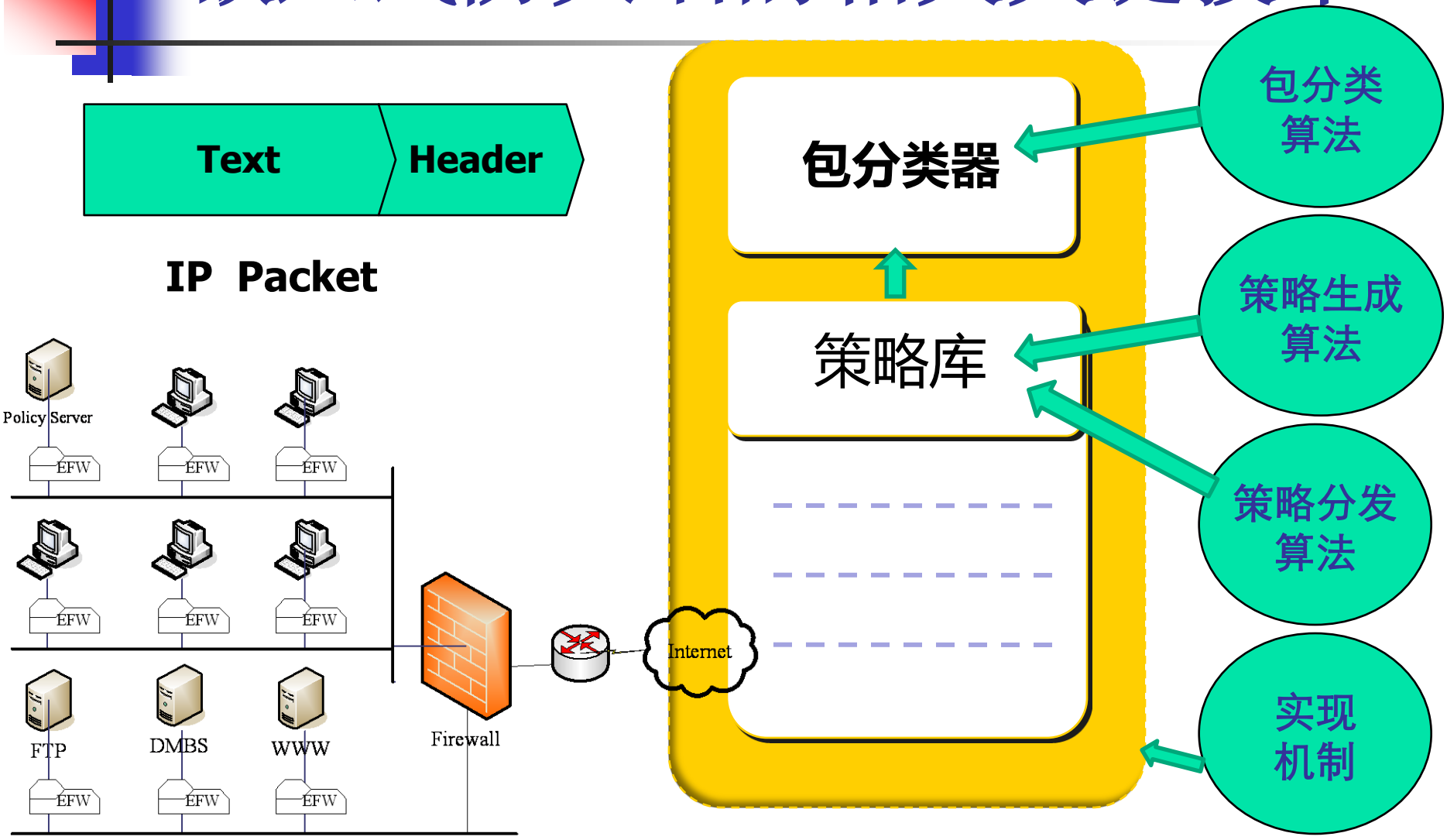
- 特别依赖拓扑结构
- 流量集中点
- 不能防止内部攻击

安全悖论？

嵌入式防火墙的引出

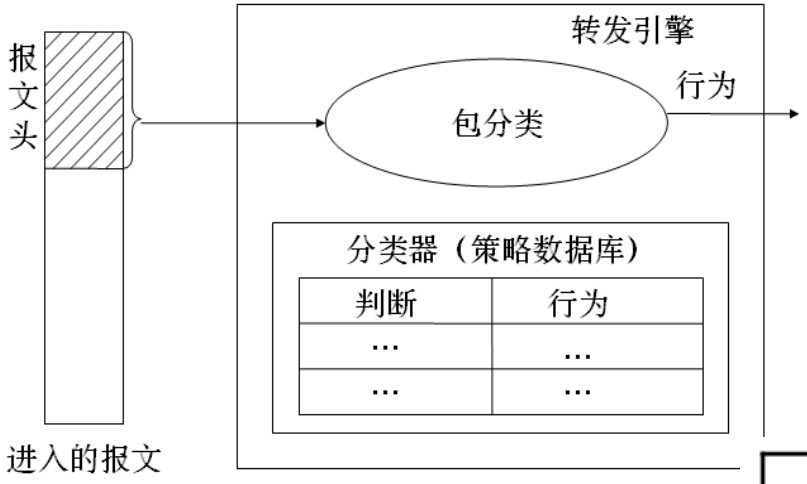
网络边界	网络及子网边界	网络边界+各节点	网络边界+各节点
保护内部网络	保护内部网络 保护各子网	防护到桌面	防护到桌面 硬件实现

嵌入式防火墙的相关关键技术



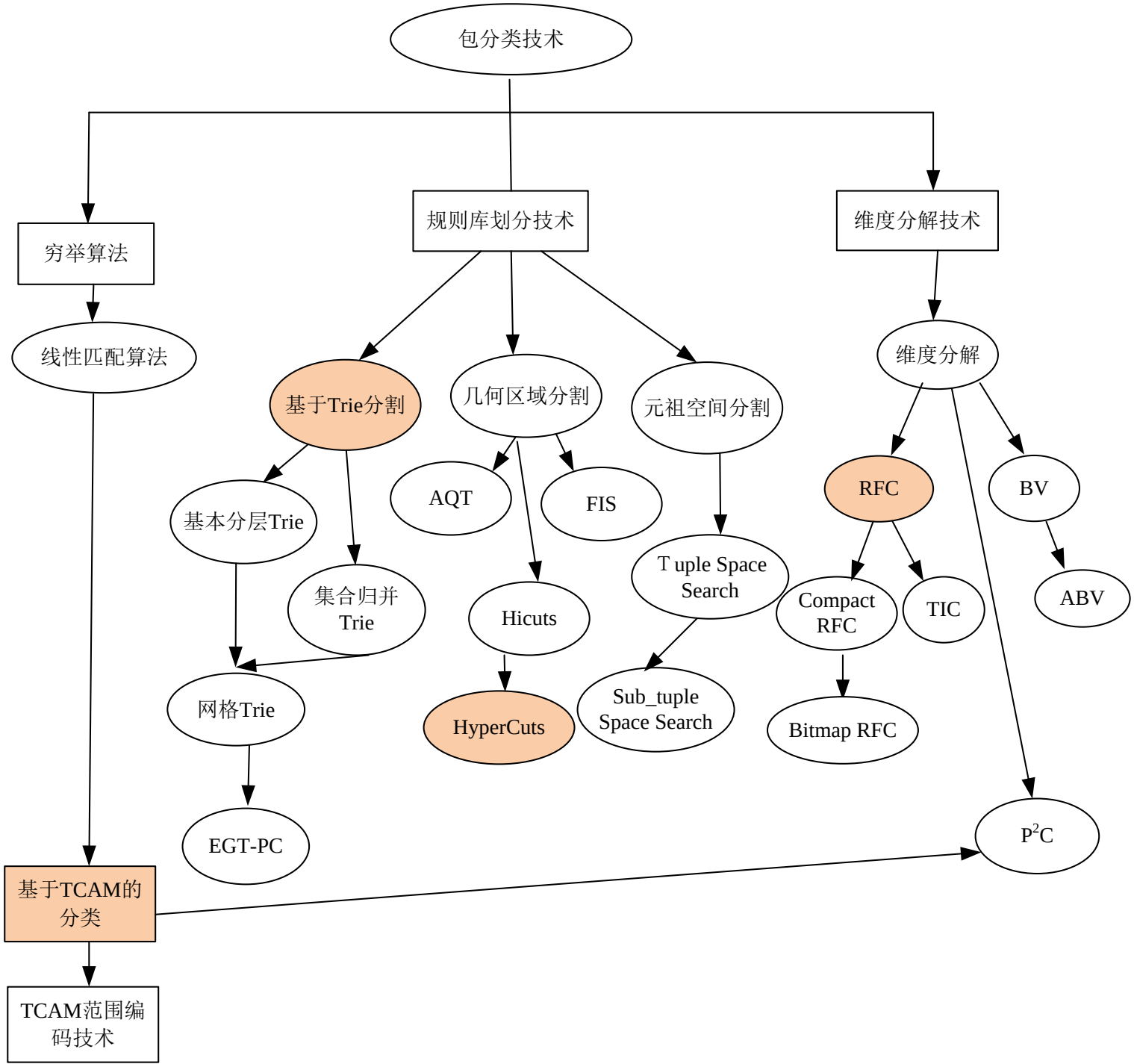
研究内容之一：包分类

- 研究目的
  - 嵌入式防火墙需要将进出网络和主机之间的分组遵循防火墙策略，进行快速的分类和处理



001	010	011

Rule#	F1	F2	F3	Action
R1	001	010	011	permit
R2	001	100	011	deny
R3	01*	100	***	permit
R4	***	***	***	permit

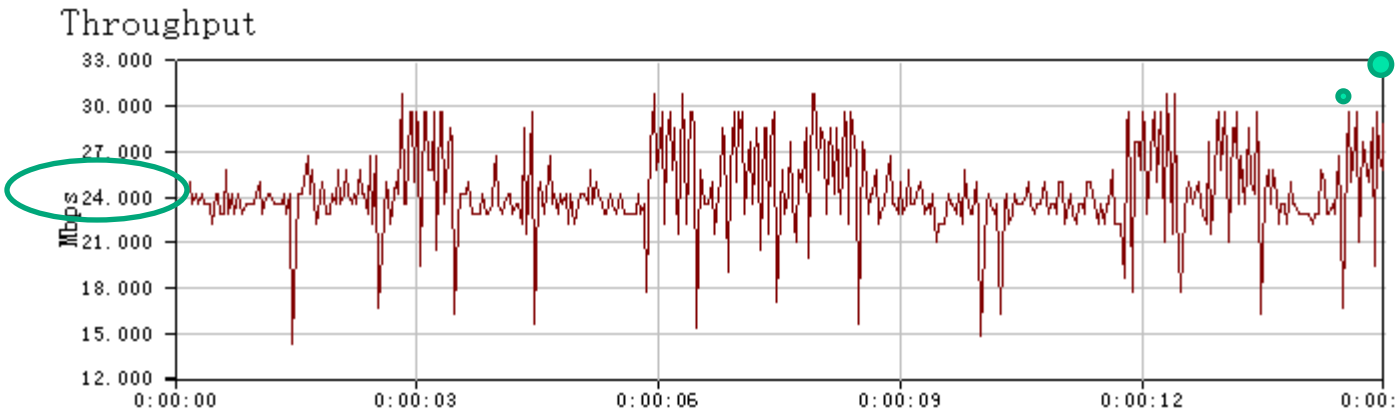

包分类技术
穷举算法
规则库划分技术
维度分解技术
线性匹配算法
基于Trie分割
几何区域分割
元祖空间分割
维度分解
基本分层Trie
集合归并Trie
AQT
FIS
RFC
BV
T uple Space Search
Compact RFC
TIC
ABV
Hicuts
网格Trie
HyperCuts
Sub_tuple Space Search
Bitmap RFC
EGT-PC
P2C
基于TCAM的分类
TCAM范围编码技术

研究内容之二：策略生成

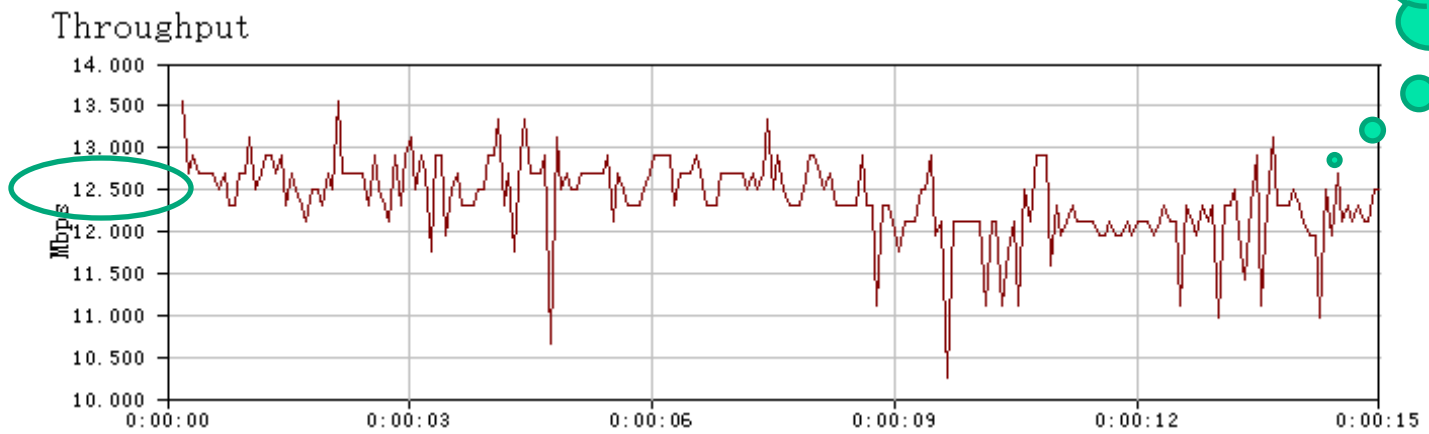
- 研究目的
  - 传统集中式防火墙：管理员在线编辑策略
  - 分布式防火墙策略
    - **Keynote：Bellovin等**
    - **IPSec：Charles等**
    - 特点：功能强，可认证和加密，运算量和网络负载影响大，资源要求高
  - 嵌入式防火墙
    - 特点：运算能力有限、节点数量多且分散，不可能对每个嵌入式防火墙进行策略设置
    - 适合于嵌入式环境下的轻型策略生成算法

IPSec对网络负载的影响

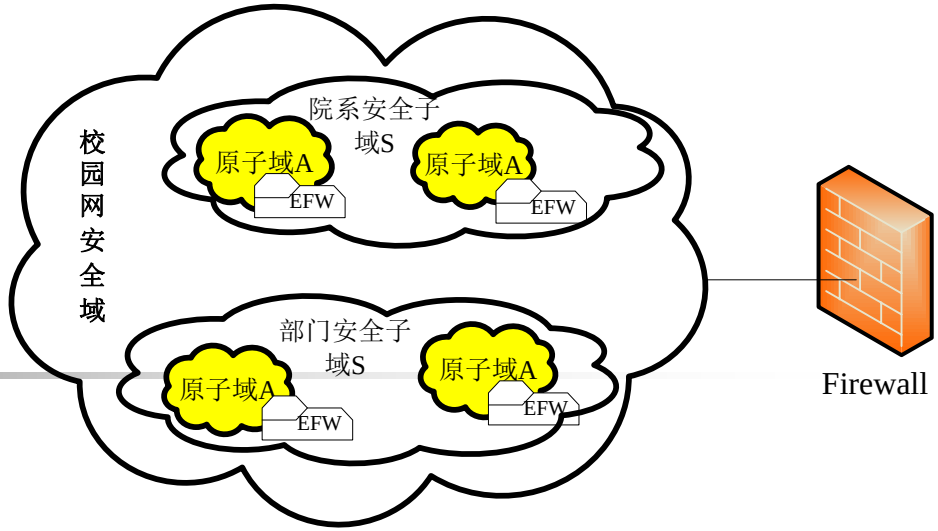
未启用 IPSec



启用 IPSec



RBAC



- 基于RBAC描述
  - 嵌入式防火墙的用户、角色和权限
- RBAC缺陷
  - 所有节点需与PS通信；无层次结构；对于不同逻辑组中的相似角色需要单独定义
- EFW需求
  - 访问规则的分发与客户端EFW本身是相关的，不能直接在嵌入式防火墙体系中应用RBAC模型，必须对RBAC进行扩展，根据各EFW特征对角色进行限制和运算，实现用户角色的动态生成
- RBAC扩展
  - 安全域、安全子域和原子域

RBAC的角色扩展

RBAC

$$D=(U,R,UA,RH,P,PA)$$

RBAC
扩展

$$D=(U,R,SR,OR,RH,P,PA)$$

U：表示全域安全系统用户集合
R：表示全域安全系统角色集合
UA：$UA\subseteq U\times R$ 表示全域安全系统用户与角色分配集合
RH：$RH\subseteq R\times R$ 表示全域安全系统角色继承关系集合，是一个偏序关系 $(RH,\geq)$
P：权限集合
PA：表示权限与角色分配集合
SR：$SR\subseteq R\times S$子域角色限制域， S表示安全子域
OR：$OR\subseteq R\times B$原子域角色限制域， B表示原子域

K

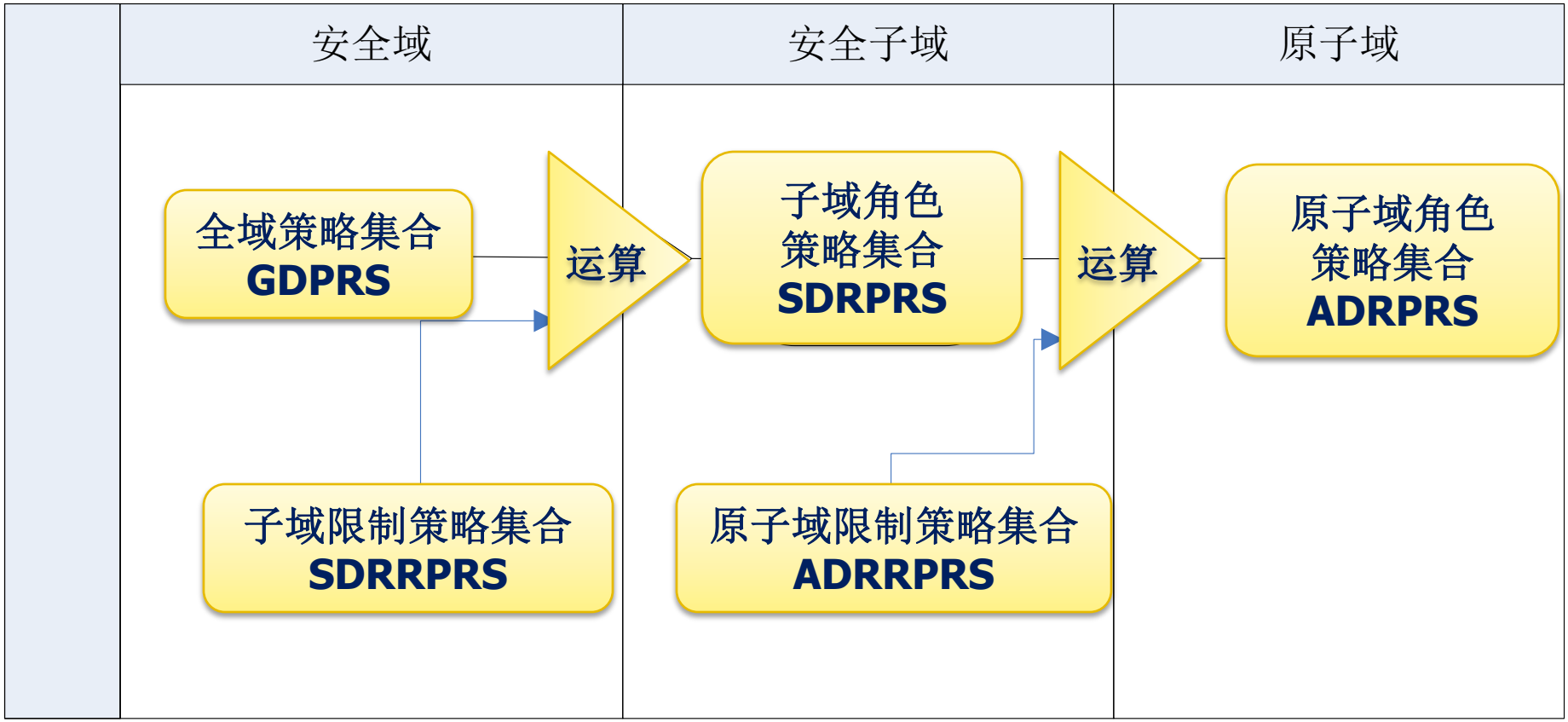
角色限制域与扩展角色

- 角色限制域：继承关系，层次关系
- 扩展角色：处于角色限制域中的角色，可继承，所有扩展角色组成的继承关系，构成层次关系

  - 自反性 $\forall k \in K \Rightarrow k \geq k$
  - 反对称性 $\forall k_1, k_2 \in K, k_1 \geq k_2 \wedge k_2 \geq k_1 \Rightarrow k_1 = k_2$
  - 传递性 $\forall k_1, k_2, k_3 \in K, k_1 \geq k_2 \wedge k_2 \geq k_3 \Rightarrow k_1 \geq k_3$

- 子域角色继承于全域角色，拥有全域角色 的所有属性，且可以扩展；
- 原子域角色继承于子域角色，拥有子域角色的所有属性，且可以扩展

子域/原子域角色策略的生成



子域/原子域角色策略的生成

子域角色策略

- **sRS**禁止访问安全子域内的任何客户端的策略集合
- **dRS**禁止安全子域内的客户端访问的远程站点或网络范围的策略集合
- **oRS**表示角色策略集合中不属于**sRS**和**dRS**的其它规则

原子域角色策略：

- **inRS**中的规则负责检验进入**EFW**的数据
- **outRS**中的规则负责检验从**EFW**中发出去的数据

$$SDRPRS = sRS \cup dRS \cup oRS$$

且：$sRS \cap dRS = \varnothing$

$dRS \cap oRS = \varnothing$

$sRS \cap oRS = \varnothing$

结合**EFW**特点：
对网络内部和外部的访问控制；
网络分组进出的方向

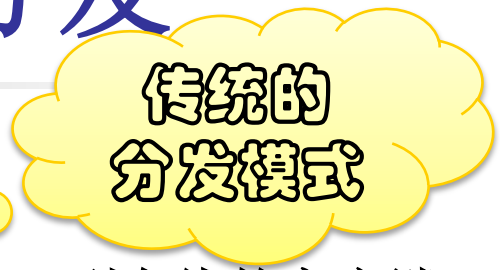
$$ADRPRS = inRS \cup outRS \quad 且 \quad inRS \cap outRS = \varnothing$$

特点

- 对传统RBAC进行角色扩充
- 通过角色限制生成子域/原子域角色策略
- 结合嵌入式防火墙特性
  - 对网络内部和外部的访问控制子集划分
  - 网络分组进出方向子集的划分

不管是子域策略集合还是原子域策略集合，都继承于全域策略，子域或原子域可在此基础上进一步扩展策略，以对子域或者原子域进一步访问控制，保证了各嵌入式防火墙策略的完整性、安全性和全局的一致性

研究内容之三：策略分发



- 研究目的
  - “推”方式是指策略服务器有新的策略后，“推”到在线的客户端防火墙，易引起短时间内的爆发流，策略服务器负载急剧上升
  - “拉”方式是指各客户端防火墙定期向策略服务器发送请求，下载新的策略，易造成策略服务器的负载较大
  - **SOAP + XML**，适用于分布的边界防火墙
  - 去除**Policy server**，采用**P2P**思想，节点之间的信任？

策略分发算法

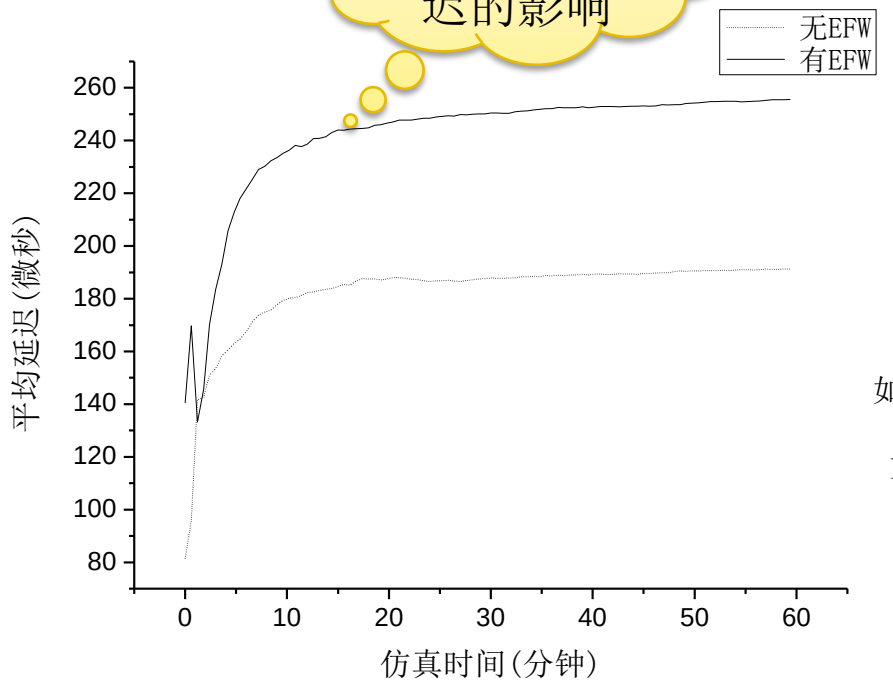
- 改进的策略分发过程
  - 客户端嵌入式防火墙将策略保存在非易失存储器中
  - 策略服务器检测到版本更新后，发送广播通知客户端主动更新
  - 正在运行的客户端收到版本更新广播后，为减少并发性，通过一个随机延迟后再进行策略拉取
  - 策略服务器端使用一个队列来存放等待下载的客户端请求，丢弃重复请求

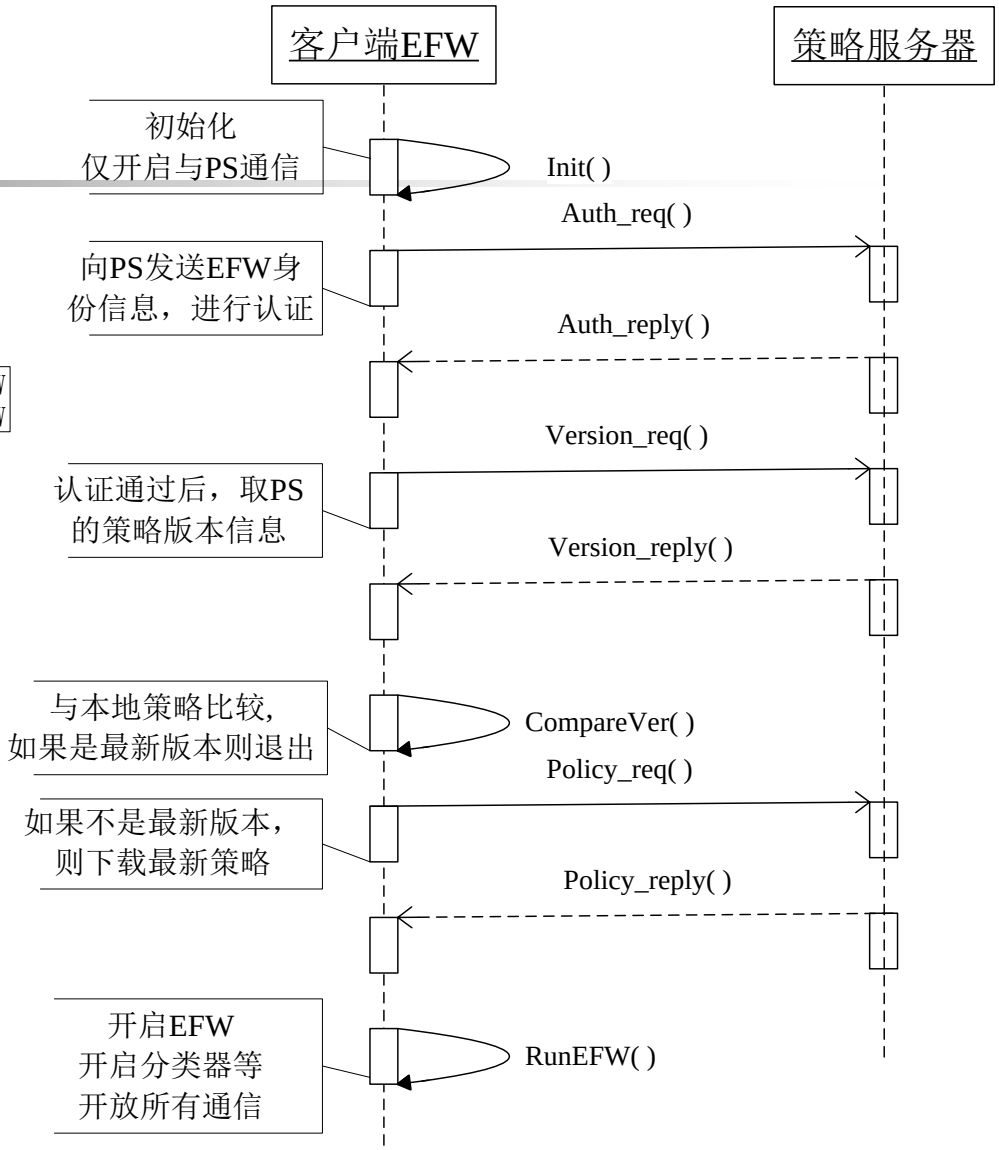
推拉结合

初始化算法
策略更新算法

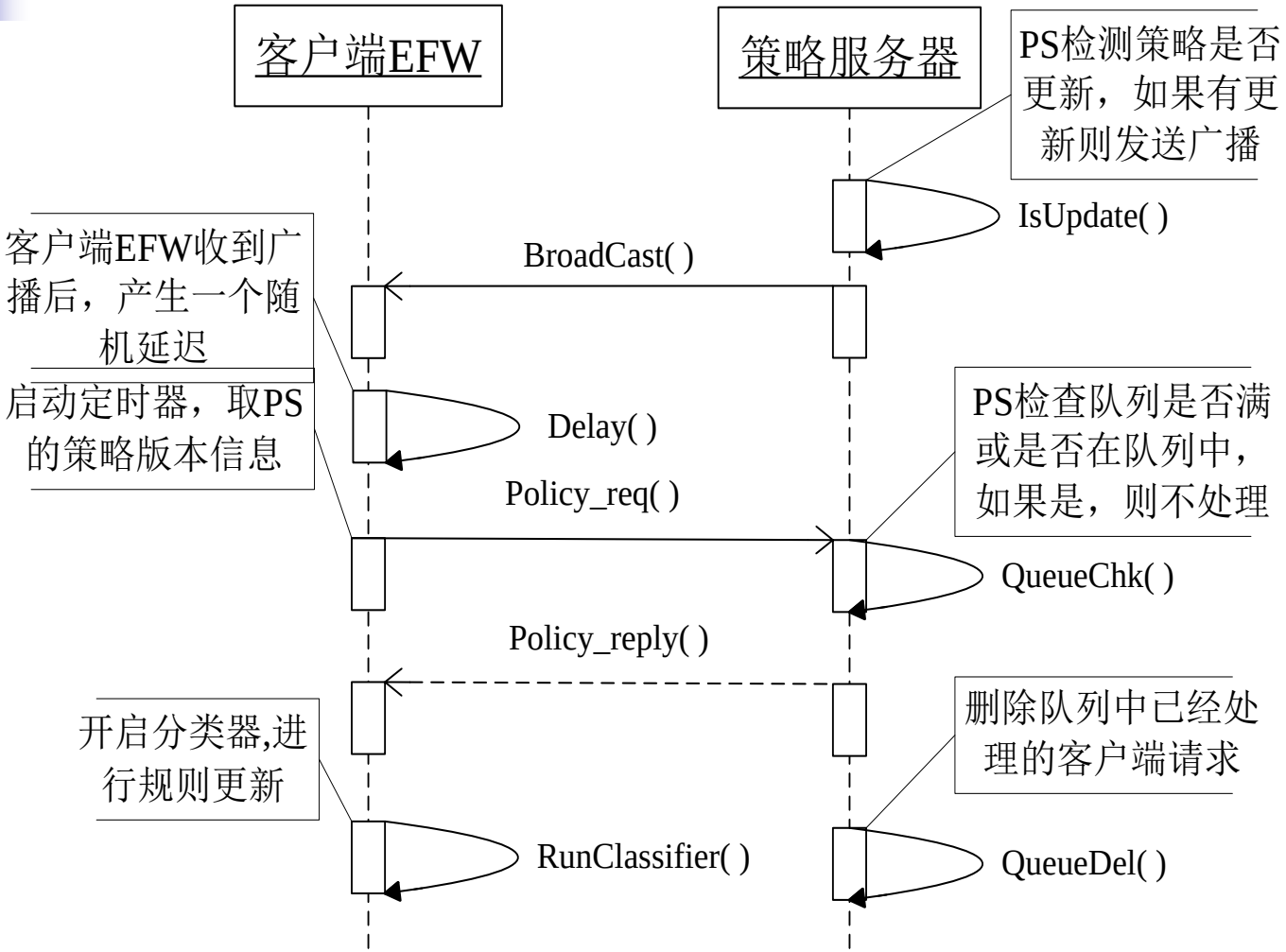
初始化算法

串联EFW
对网络延
迟的影响



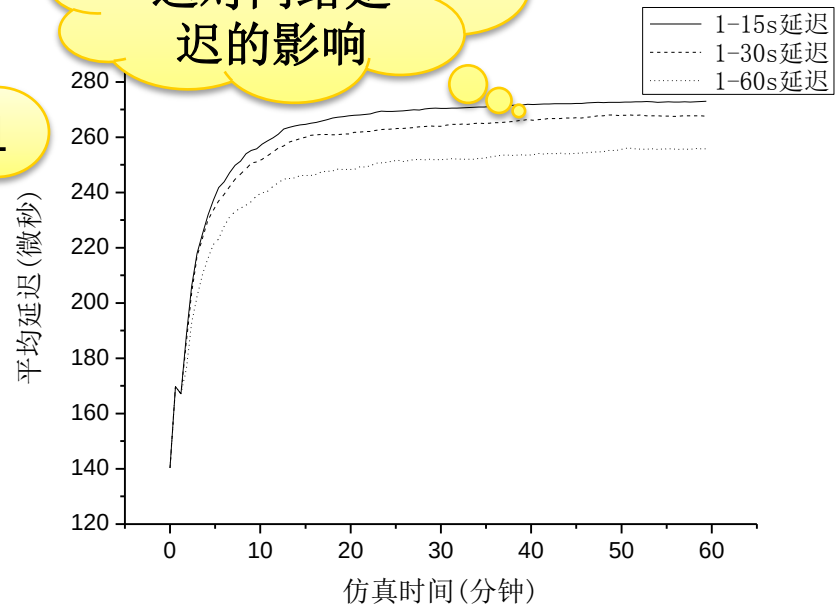


策略更新算法


客户端EFW
策略服务器
PS检测策略是否更新，如果有更新则发送广播
IsUpdate( )
BroadCast( )
客户端EFW收到广播后，产生一个随机延迟
启动定时器，取PS的策略版本信息
Delay( )
Policy_req( )
PS检查队列是否满或是否在队列中，如果是，则不处理
QueueChk( )
Policy_reply( )
开启分类器,进行规则更新
删除队列中已经处理的客户端请求
RunClassifier( )
QueueDel( )

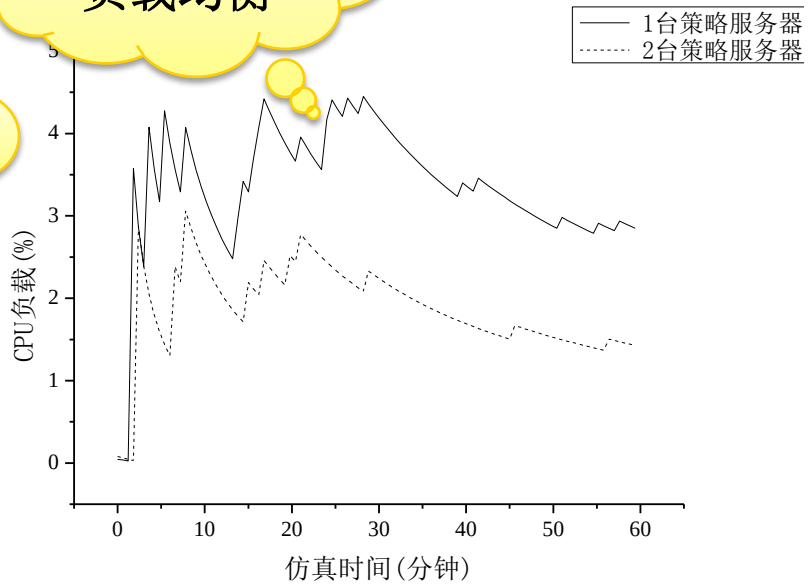
策略拉取延迟对网络延迟的影响

1

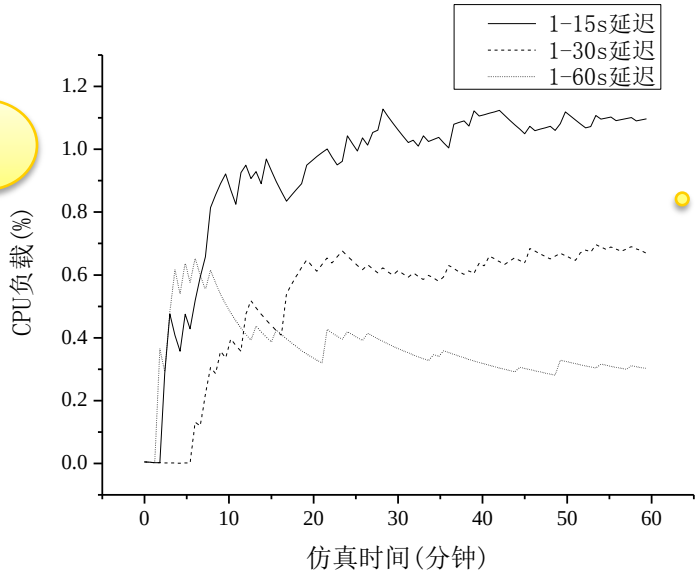


多服务器负载均衡

3



2



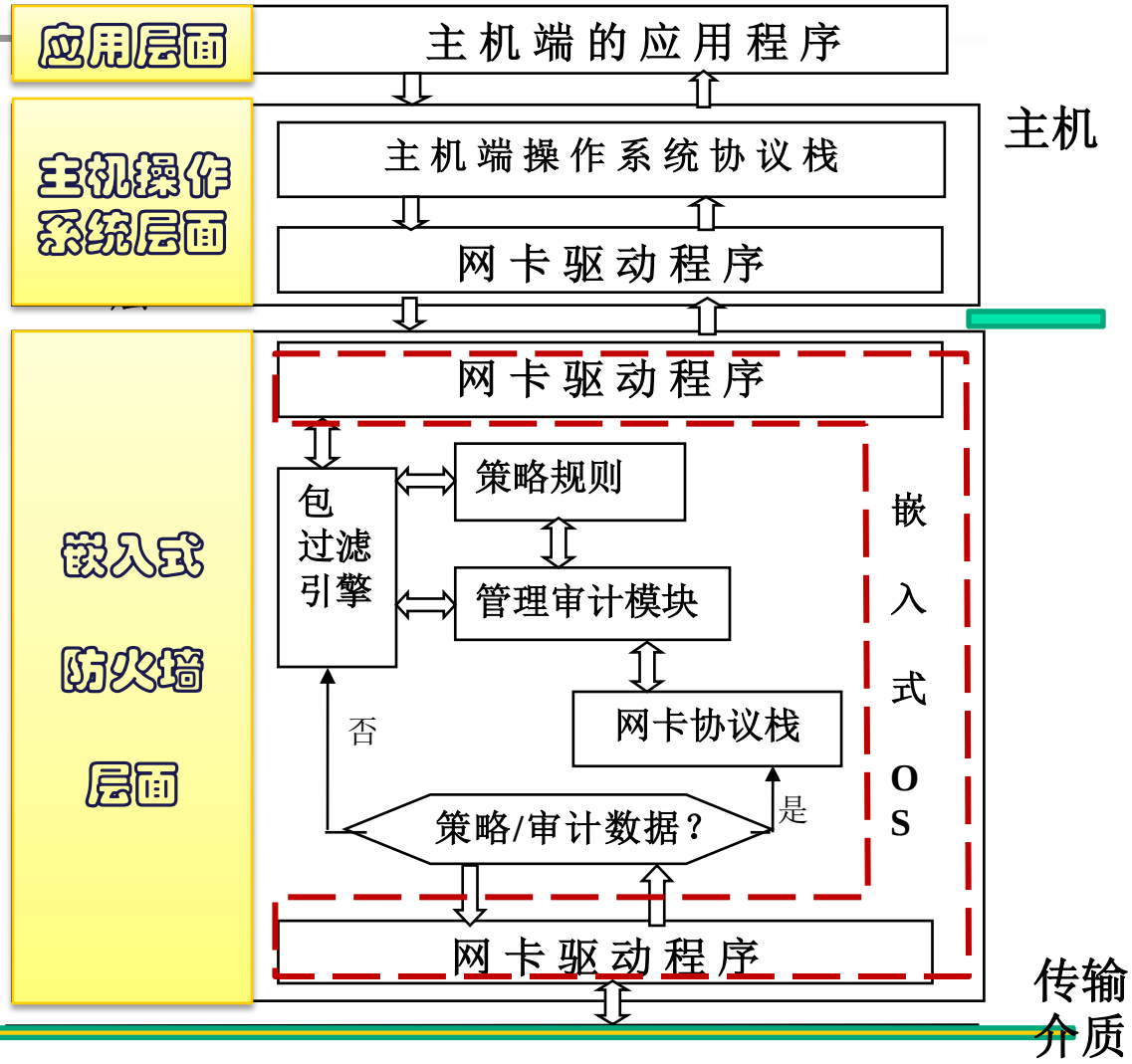
策略拉取延迟对服务器CPU的影响

研究内容之四：具体实现机制

- 研究目的
  - 基于软件的实现方法
    - 与OS的悖论
  - 多种基于硬件的实现方法
    - **ASIC**：周期长，成本高
    - **FPGA**：可编程，在线更新策略困难
    - **NP**：速度快，适用于路由器，交换机，集中式防火墙
    - **ARM**：便于控制和扩展，易部署到桌面级，成本低廉

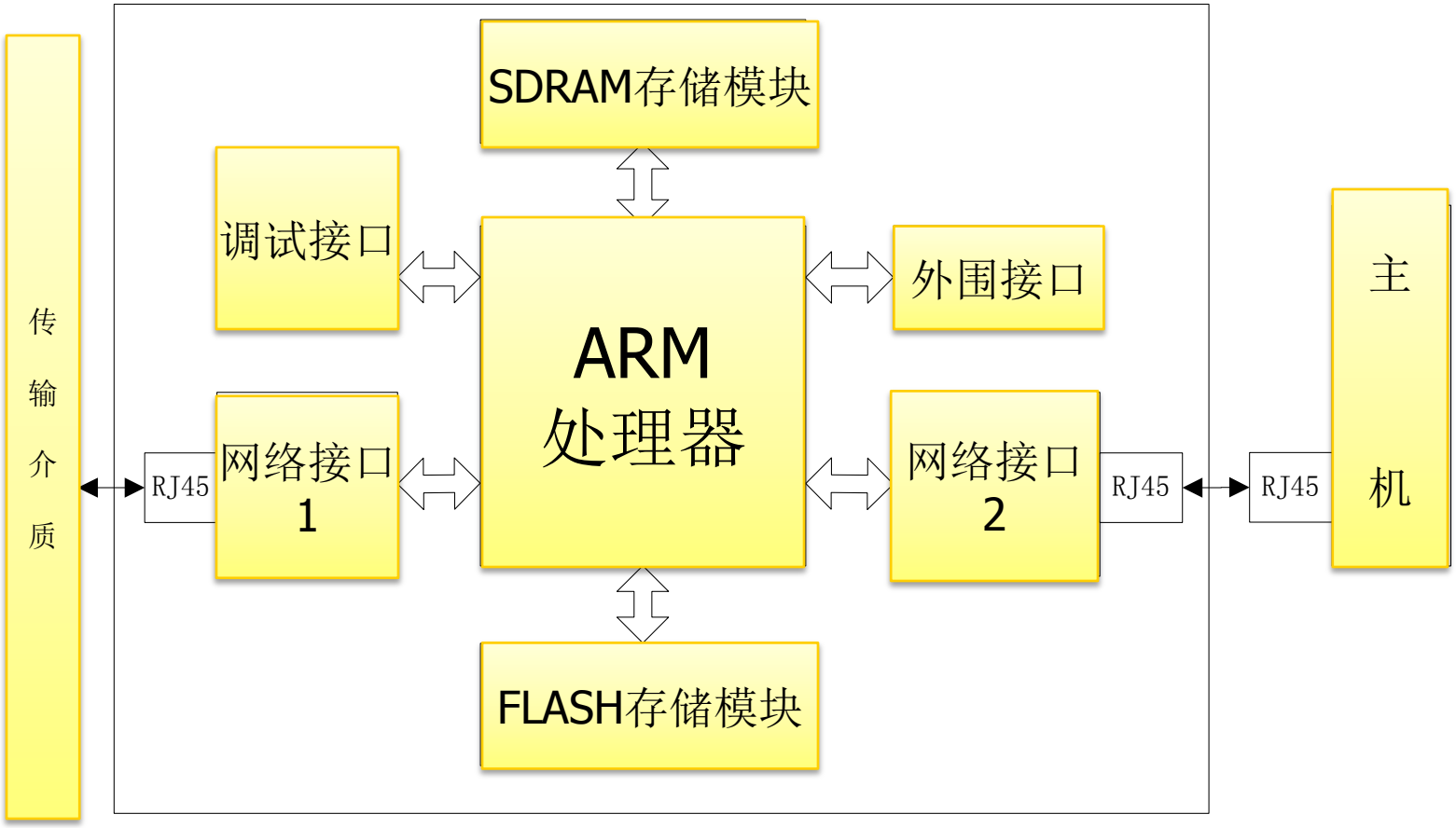
总体架构

- 嵌入式防火墙通过RJ45接口连接到受保护主机
- 所有进出主机的数据流经由嵌入式防火墙处理
- 管理和应用的平台：移植嵌入式Linux



硬件架构

- 模块化：核心、存储、网络接口、调试、外围电路
- 单独的处理器，不受主机OS控制
- 单独的存储器，“存储-转发”
- 单独的OS，开发各种安全应用



软件架构


软件层
硬件层
应用层
包分类器、策略更新、IDS等
OS层
嵌入式操作系统
驱动层
网卡驱动、串口等
Bootloader
嵌入式防火墙硬件

展望

- 对策略进行优化处理，检测并减少策略冲突
  - 保证全域策略的一致性、完整性和紧凑性
- 在策略分发方面，可考虑采用应用层组播方法，实现节点之间的协同工作
  - PS+节点协同
- 基于嵌入式防火墙平台开发相关安全应用系统
  - IDS、IPS、VPN、加解密等

谢谢