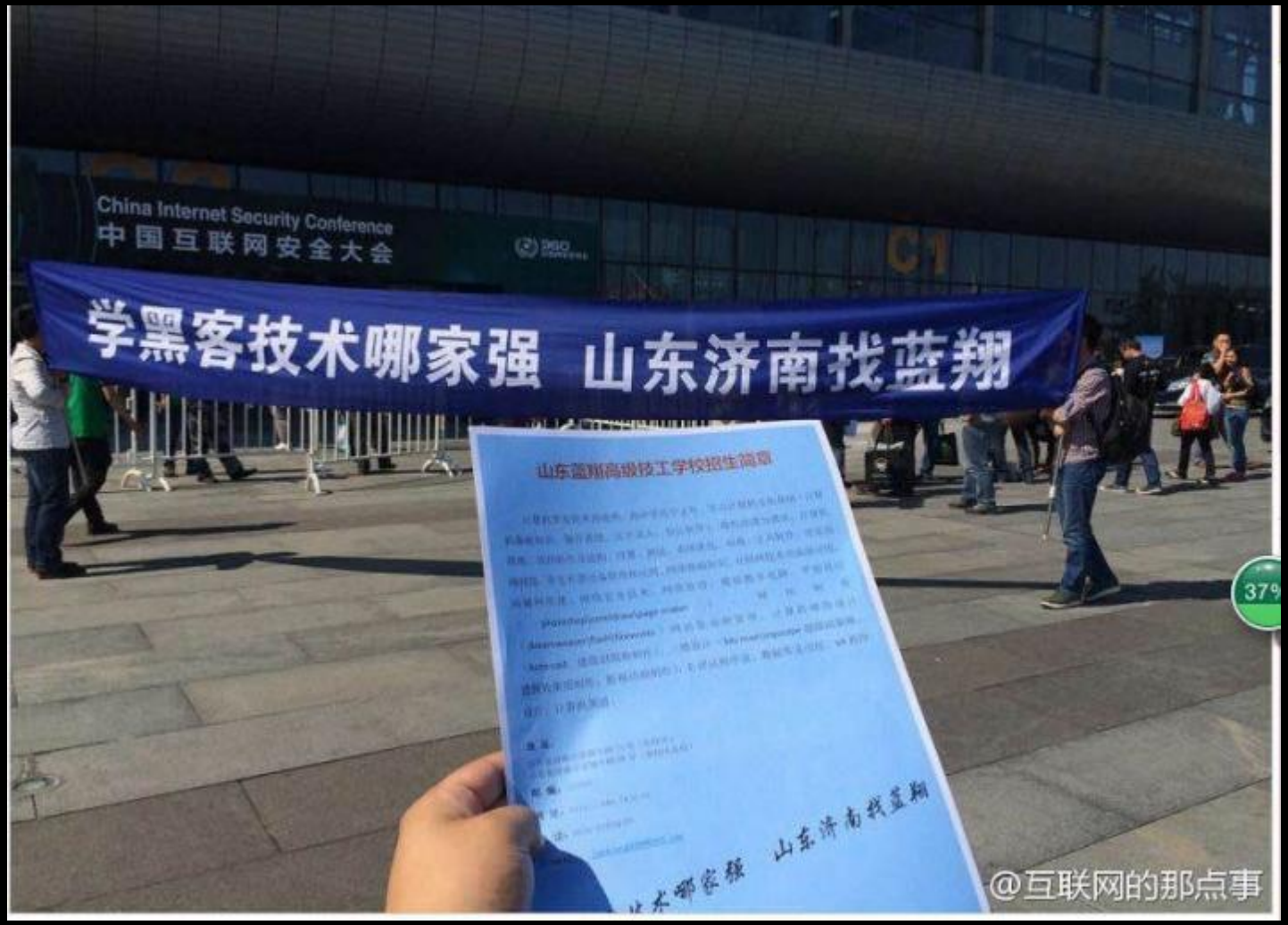
大数据运维安全

演讲人：李洪亮

职务：Qihoo 360 NETOPS Manager

日期：9/14/2014


China Internet Security Conference
中国互联网安全大会
学黑客技术哪家强 山东济南找蓝翔
山东蓝翔高级技工学校招生简章
@互联网的那点事

大数据运维安全

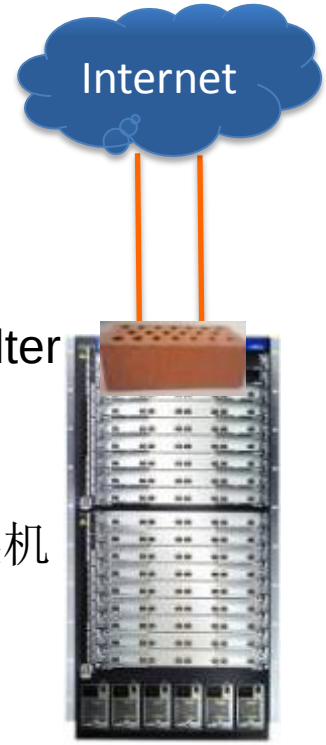
- 网络架构的安全设计
- 大数据下的安全运维实践
- IDC的物理安全

网络架构的安全设计

- ACL
- 业务之间的隔离
- DDoS攻击的防护
- 流量的分析与检测

网络架构的安全设计

– ACL



ACL规则申请平台

ACL规则的自动生成与push

ACL规则的失效与老化?

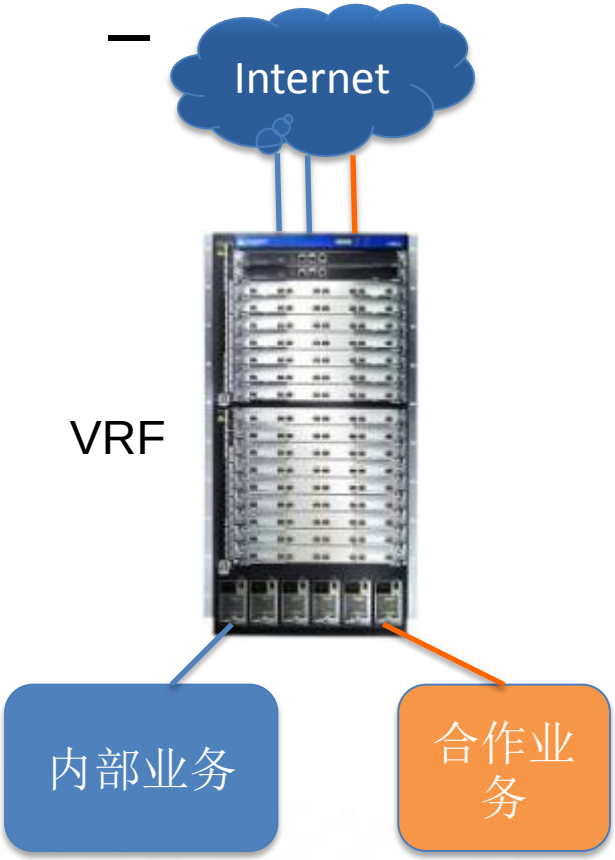
网络架构的安全设计

- ACL
- 业务之间的隔离
- DDoS攻击的防护
- 流量的分析与检测

网络架构的安全设计

–业务之间的安全隔离

–



Vlan方式隔离，会增加ACL复杂度

VRF或vPC(cisco)能提供更加简便的隔离方案

VRF

在不具备VRF的环境，建议通过策略路由方式将流量抛出

网络架构的安全设计

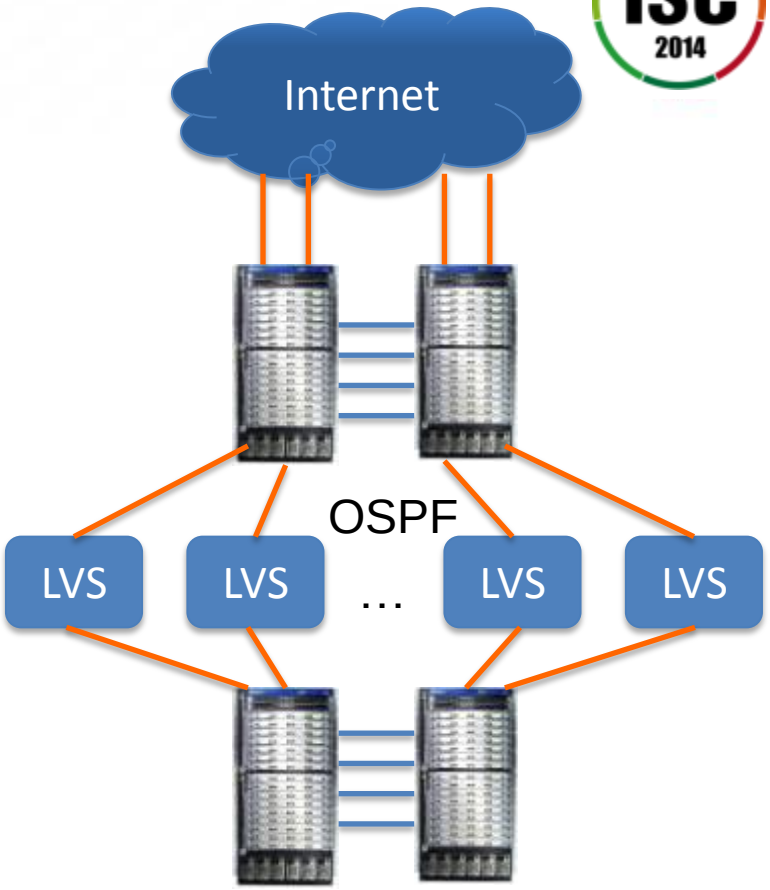
- ACL
- 业务之间的隔离
- DDoS攻击的防护
- 流量的分析与检测

网络架构的安全设计

–DDoS攻击的防护

LVS的fullNAT模式,具备良好的扩展性

LVS提供block ip接口,对攻击ip进行屏蔽



网络架构的安全设计

网络架构的安全设计

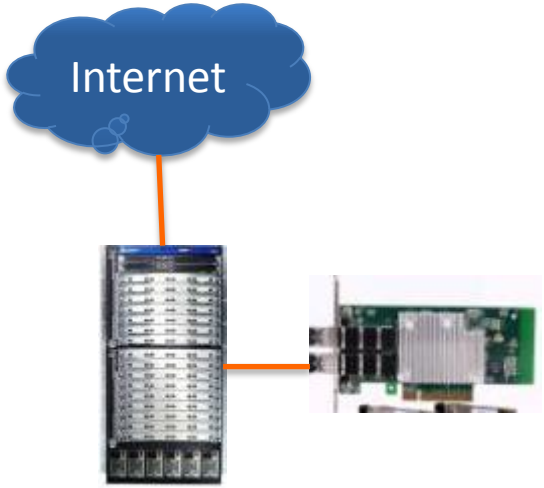
广告时间

网络架构的安全设计

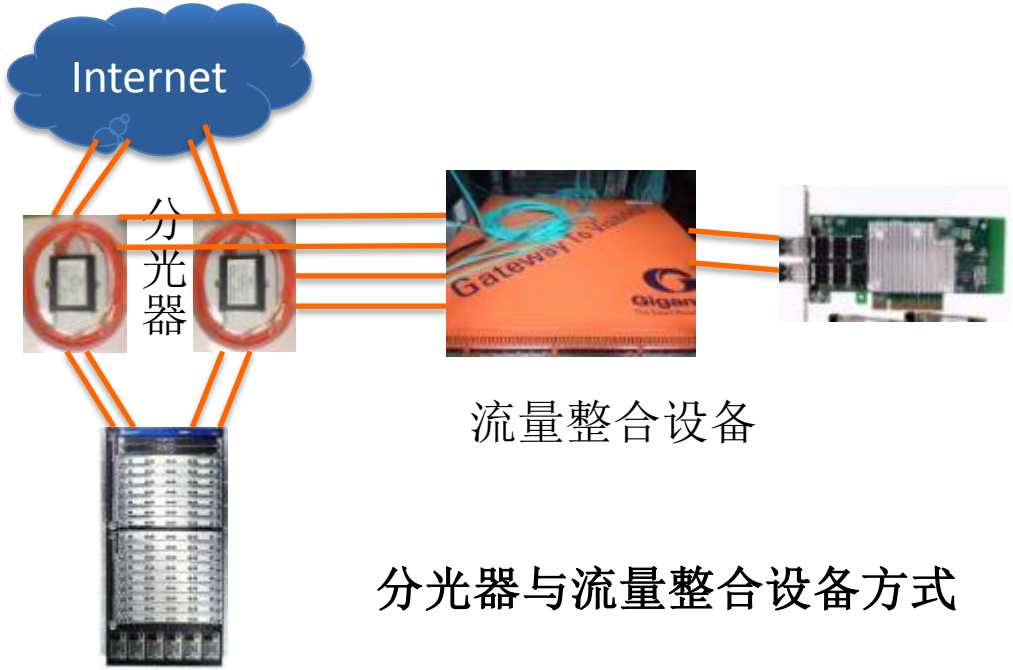
- ACL
- 业务之间的隔离
- DDoS攻击的防护
- 流量的分析与检测

网络架构的安全设计

–流量的分析与检测



流量镜像方式



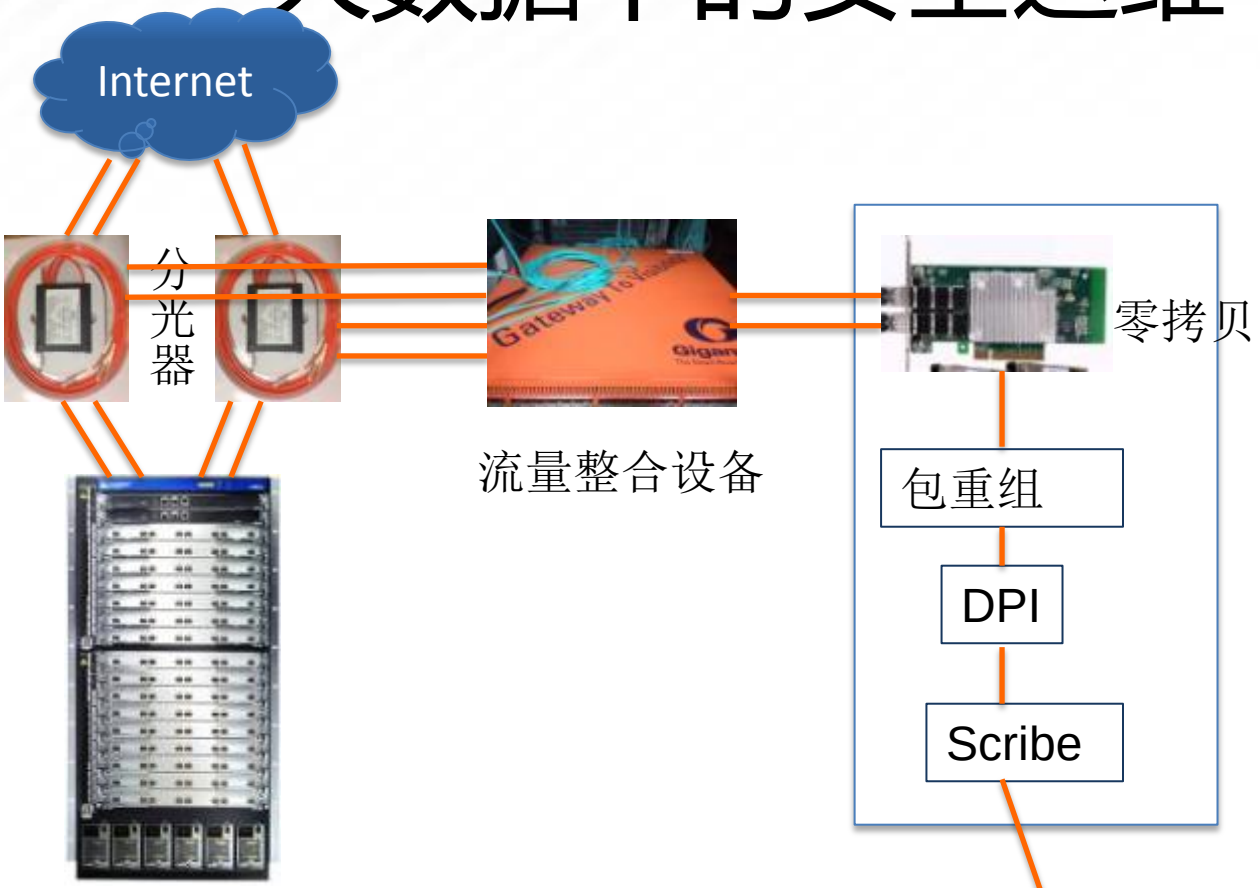
流量整合设备

分光器与流量整合设备方式

大数据下的安全运维

- 大流量包捕系统
- 分布式存储与并行计算系统
- 机器学习与规则提取系统
-
-
-

大数据下的安全运维



大流量包捕系统

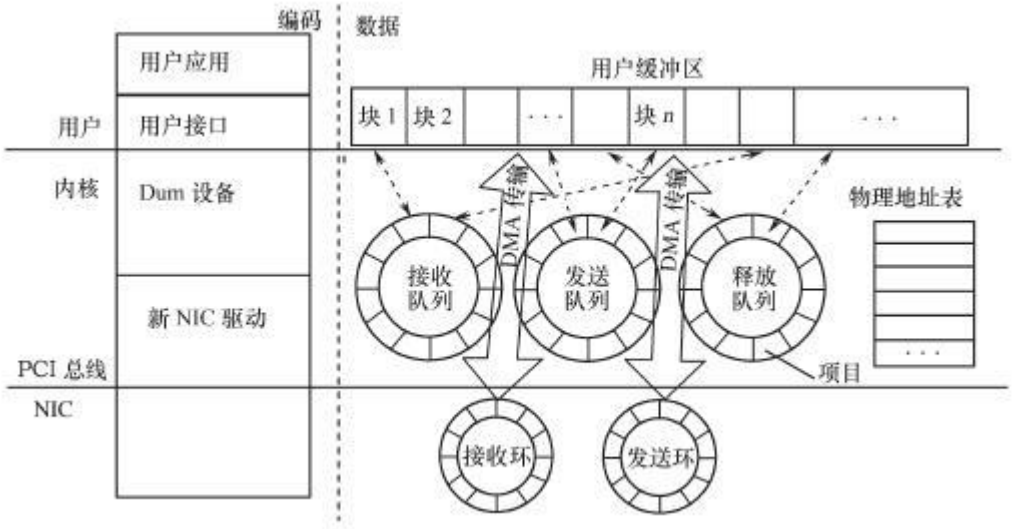
大数据下的安全运维

避免数据拷贝

按CPU数分配队列

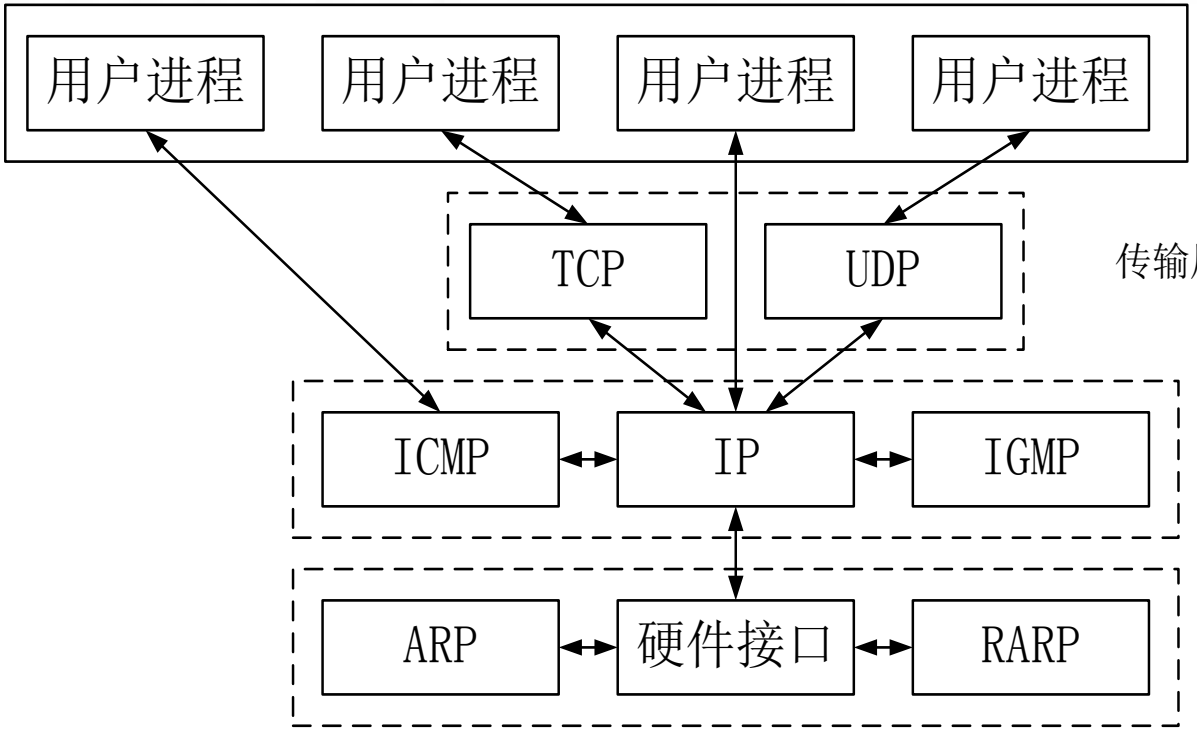
将多种操作结合

直接IO



大流量包捕系统—零拷贝

大数据下的安全运维



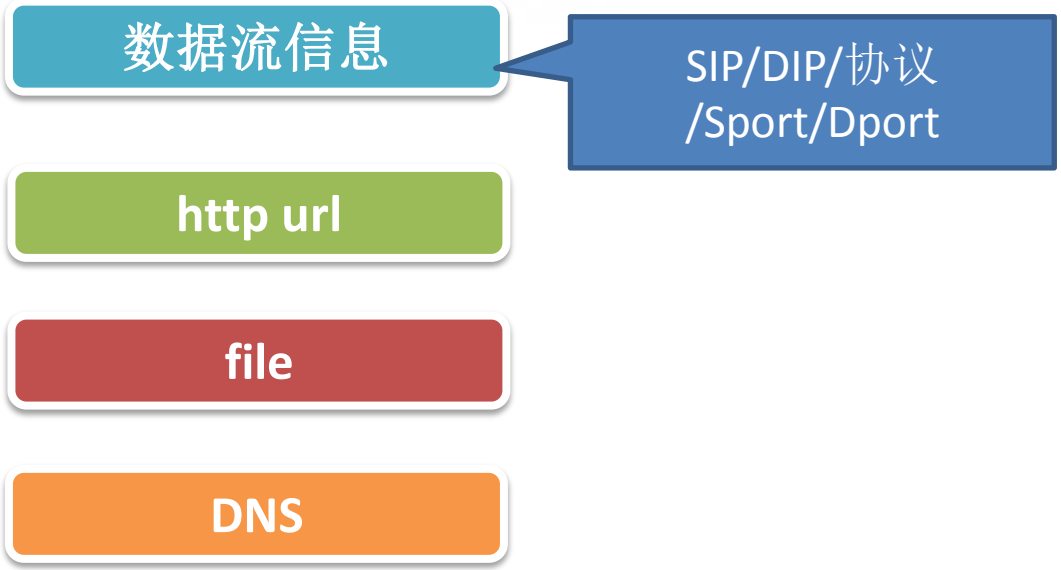
- Tcp流乱序重组
- Tcp流表维护

- Ipv4/v6
- 双栈处理
- Ip分片重组

- VLAN
- MPLS
- GRE

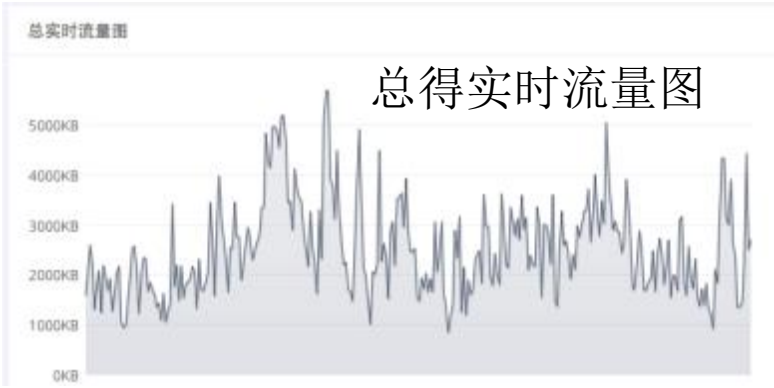
大流量包捕系统—数据包重组

大数据下的安全运维



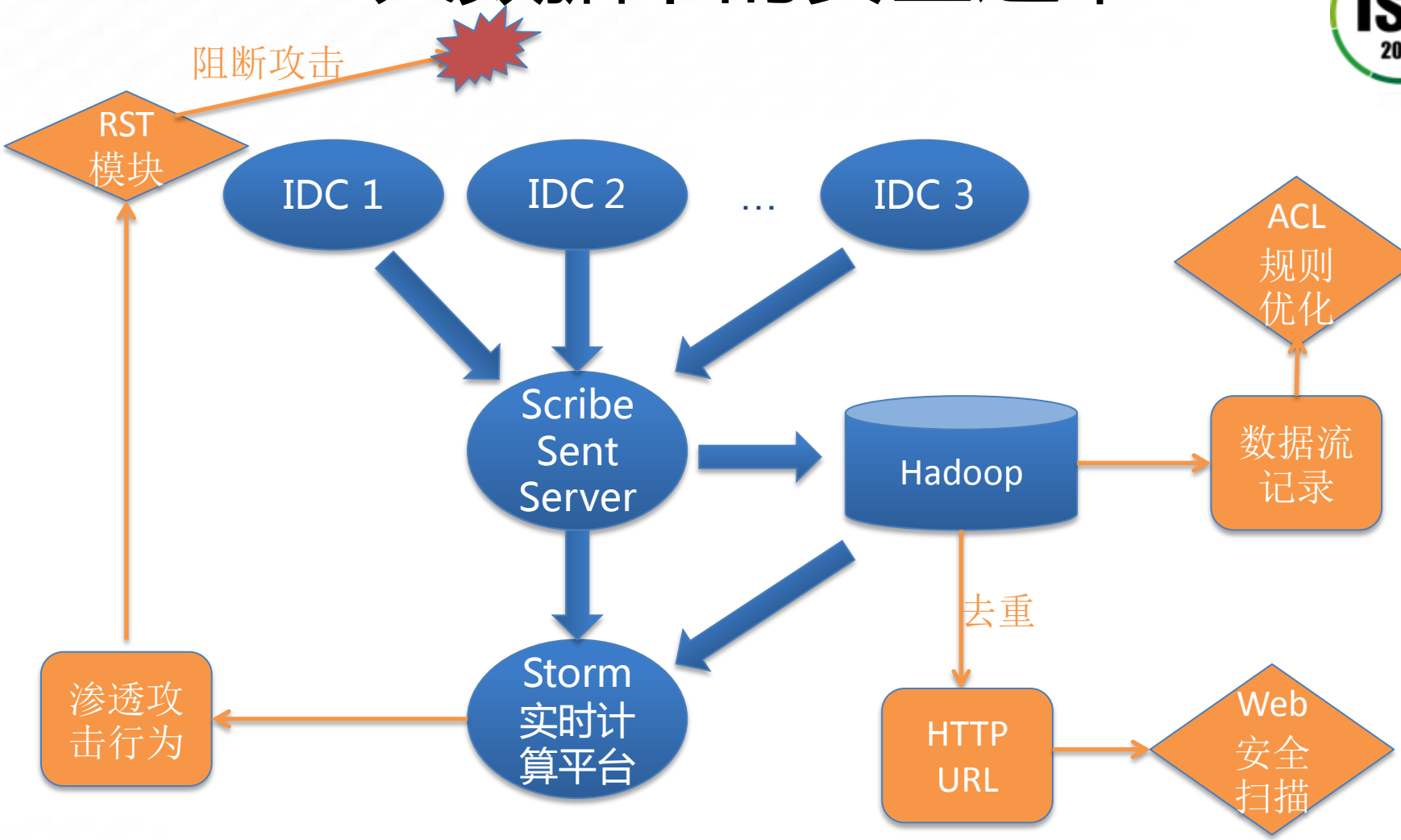
大流量包捕系统—DPI

大数据下的安全运维

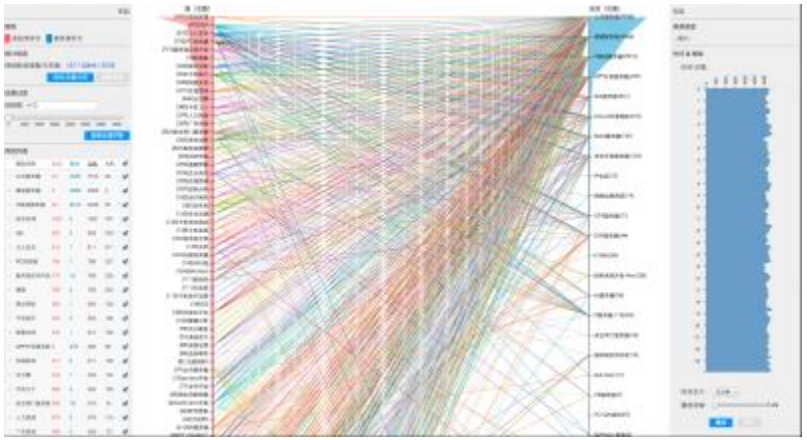


大流量包捕系统—功能展示

大数据下的安全运维


阻断攻击
RST
模块
IDC 1
IDC 2
…
IDC 3
ACL
规则
优化
Scribe
Sent
Server
Hadoop
数据流
记录
去重
渗透攻
击行为
Storm
实时计
算平台
HTTP
URL
Web
安全
扫描

大数据下的安全运维



核对ACL的过期情况

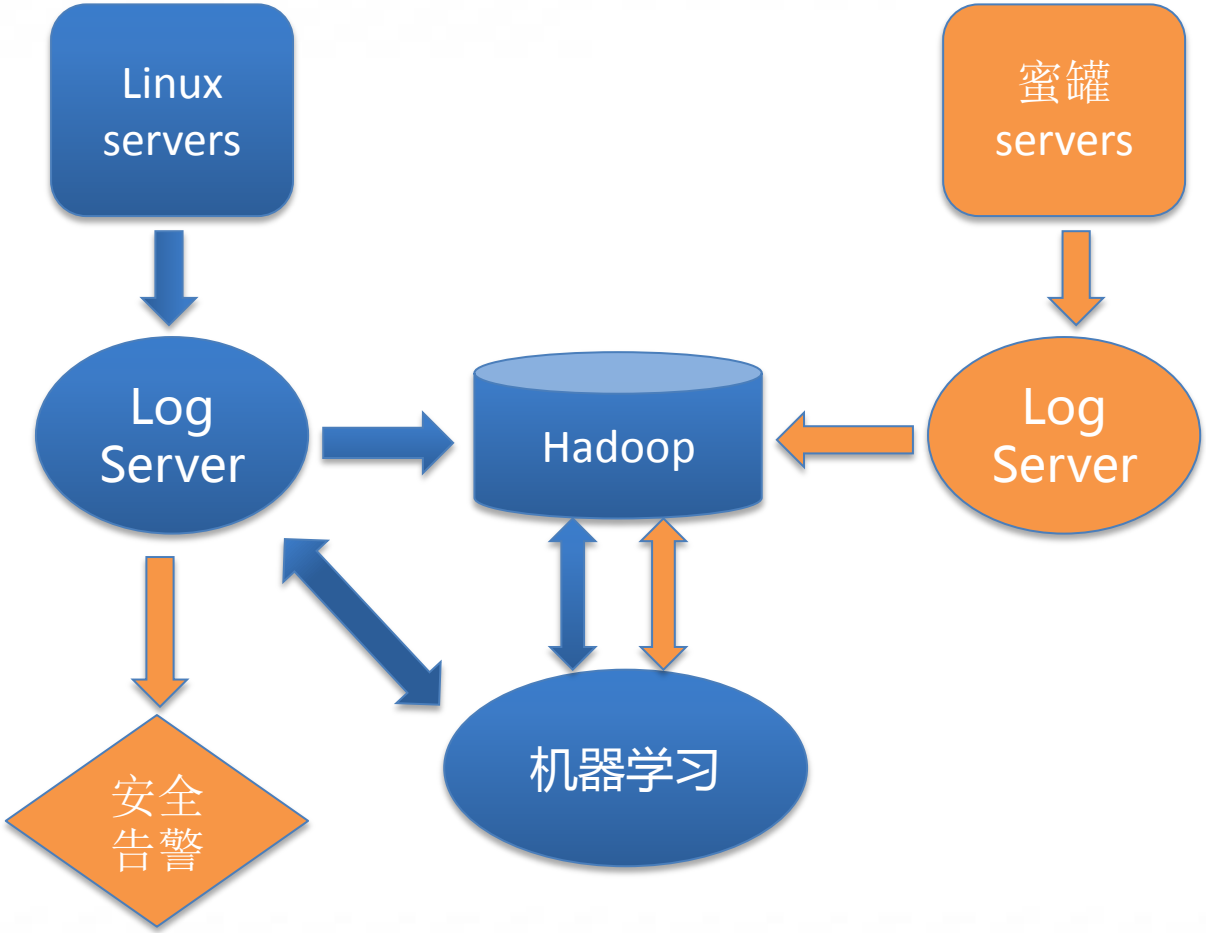
覆盖10个数据中心

每天60T的存储量

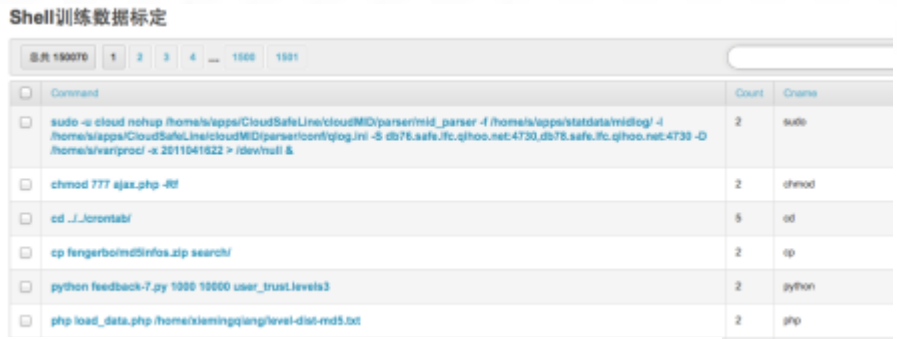
对旁路获取的url进行web安全扫描

大数据日志统计展现

大数据下的安全运维


Linux servers
蜜罐 servers
Log Server
Hadoop
Log Server
安全告警
机器学习

大数据下的安全运维



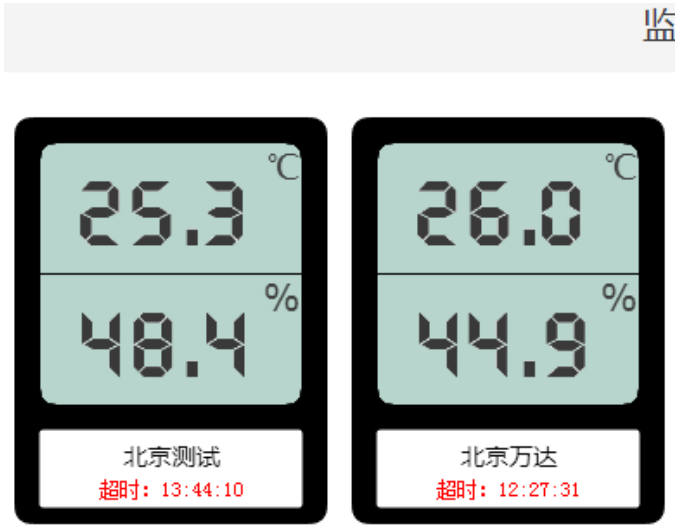
主机智能告警的人工训练

蜜罐获取黑客特征

主机安全日志的展现

IDC的物理安全

–机房的温湿度监控与报警



IDC的物理安全

重要机房的视频监控

本地存储/异地备份

动态内容保存

大数据下的安全运维

谢谢