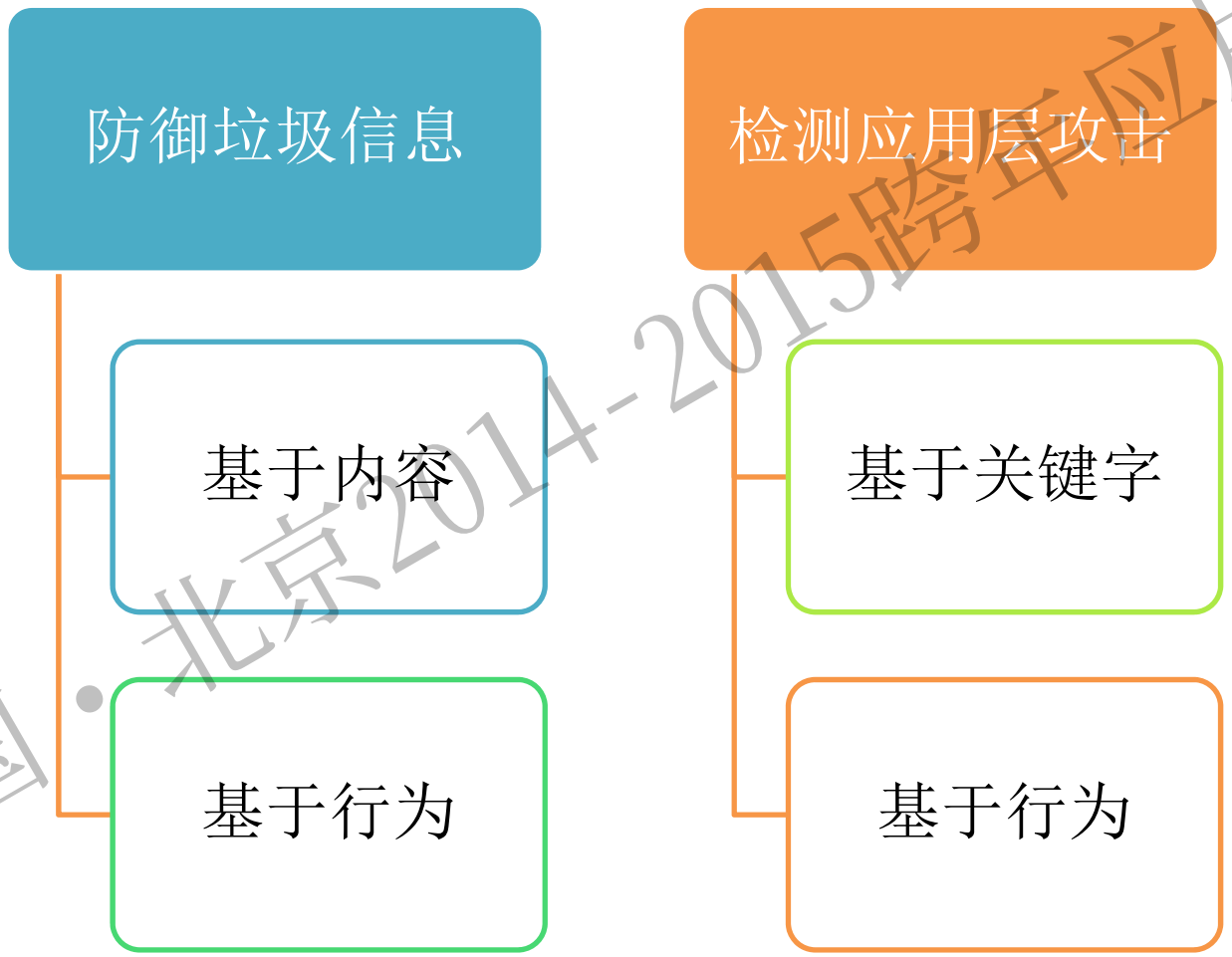
分布式垃圾信息拦截系统

分布式入侵检测系统

目录

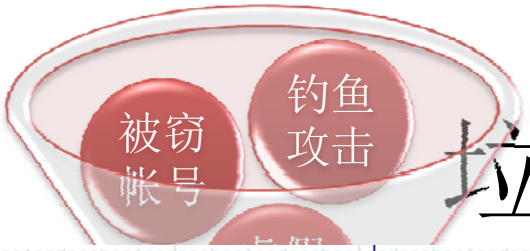
- 垃圾信息 V.S. 应用层攻击
- 攻击方式对比
- 反垃圾信息系统
- 应用层攻击检测系统

垃圾信息 V.S. 应用层攻击

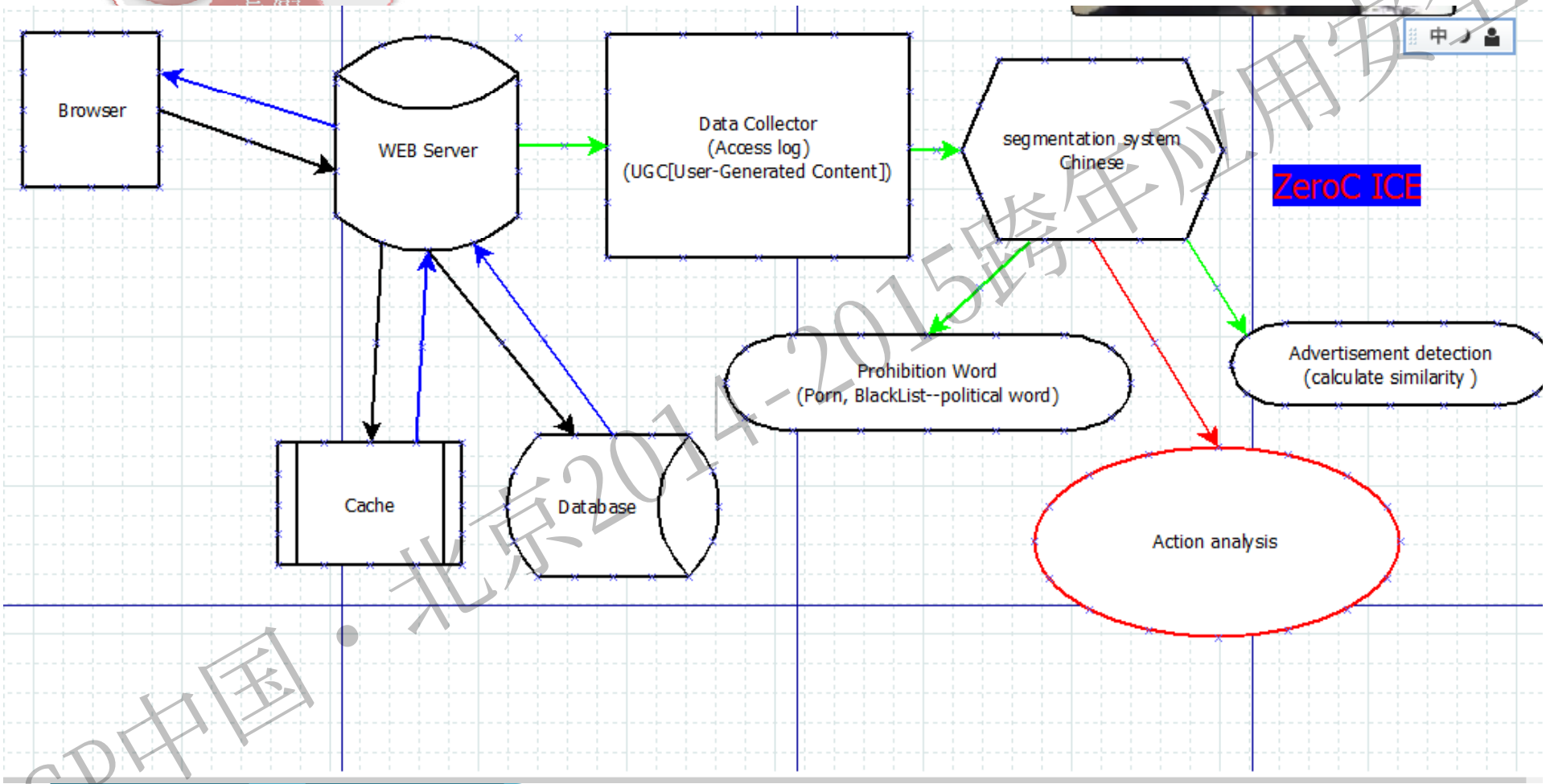


攻击方式对比

垃圾信息	WEB攻击	检测方式
发送广告内容	扫描、注入、XSS	基于特征字符串
冒充他人发送诈骗信息	扫号、信息窃取	基于行为特征
帐号劫持、虚假帐号	异常登录	基于登陆特征

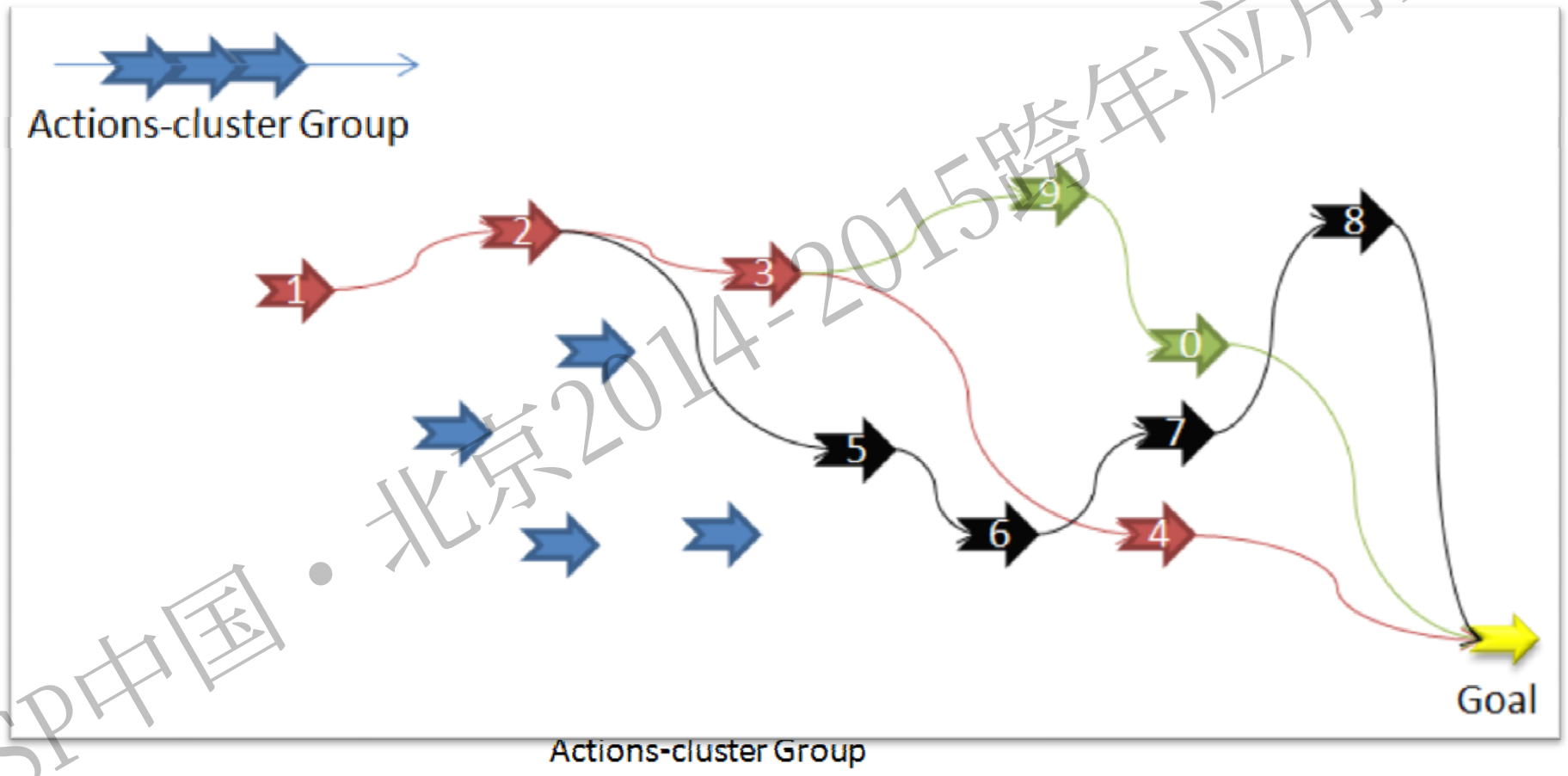


垃圾信息过滤系统

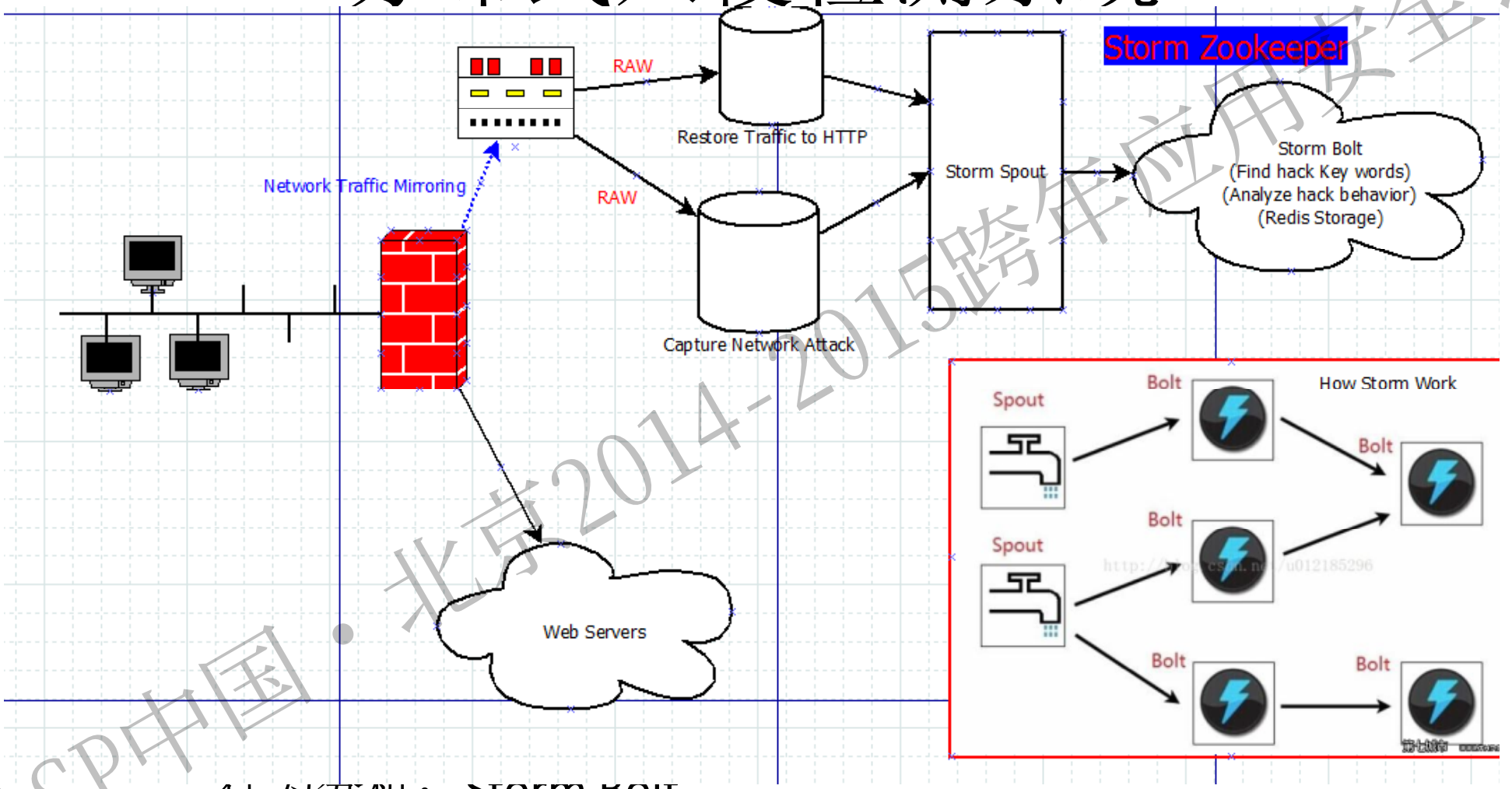


实时拦截：
IP,URL,其他特征

基于行为的分析



分布式入侵检测系统



- 行为分析：Storm Bolt

基于URL的异常检测

- 类型一
  - Hostname被替换成了IP地址+端口的形式.
- 类型二
  - 一个看似合法的域名，包含了跳转特征：比如，包含跳到另外一个域名的关键字
- 类型三
  - 合法的域名后面跟了一大串字符串，比如：../../../../../etc/passwd
- 类型四
  - 包含了敏感内容的URL,比如:admin等

一切还在进行中

谢谢