以用户的名义重新定义NGFW

演讲人：袁沈钢

职务：网康科技创始人、CEO

日期：2014.9.23

防火墙的发展

1990年，CheckPoint
- 基于IP、端口的访问控制
- 检查数据包头的异常特征
- 较强的三、四层转发能力

2004年，IDC
- 基于IP、端口的访问控制
- 检查数据包头及载荷部分
- 较高的性能衰减

2009年，Gartner
- 基于应用特征的访问控制
- 检查数据包头及载荷部分
- 较理想的性能衰减

Stateful Firewall → UTM → NGFW

- 禁止越权访问以及非法连接的建立是防火墙的核心目标和基本功能
- 防火墙技术的历次升级是为了在新的安全背景下更好的实现其功能

防火墙的进化逻辑

始终通过三大能力的增强提升用户的安全性

数据通信

- 网关产品的必要条件

访问控制

- 防火墙的最核心目标

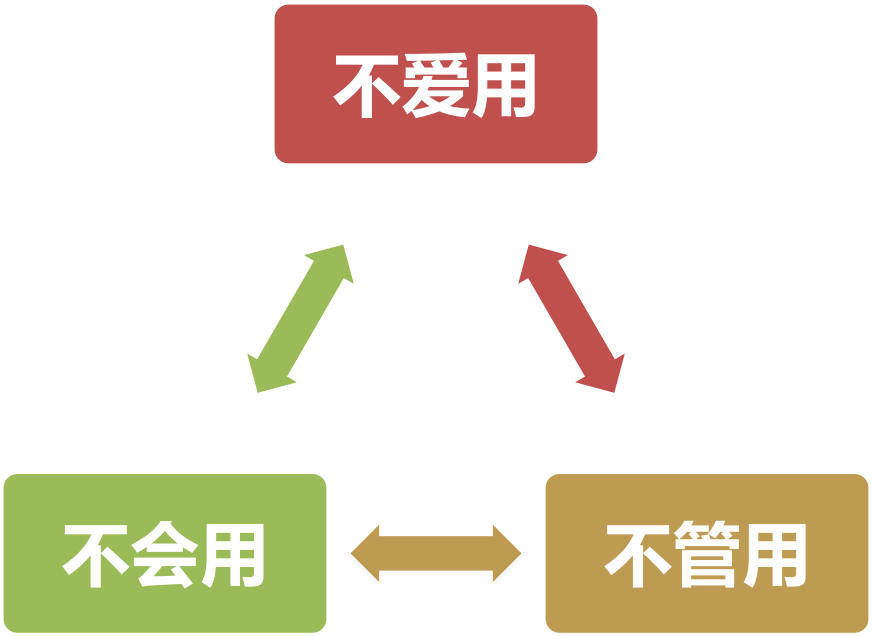
特征匹配

- 为了更好的访问控制

- NGFW的能力体现
  - 数据通信：较高的性能、IPv6、虚拟防火墙等
  - 访问控制：由元组控制提升为人、应用、内容控制
  - 特征匹配：病毒、木马等应用层威胁的识别和防御

防火墙用户的“怪现状”

从不登录的防火墙，何谈三分技术、七分管理？



- 75%的防火墙用户在最近三个月内没有登录过防火墙设备
- 80%的在线防火墙仅配置了一条“any any any permit all”的策略
- 更多的IT管理者在网络出现问题后束手无策

改配置？千万别断网！

安全吗？该如何安全？ 为了业务，全部放通！

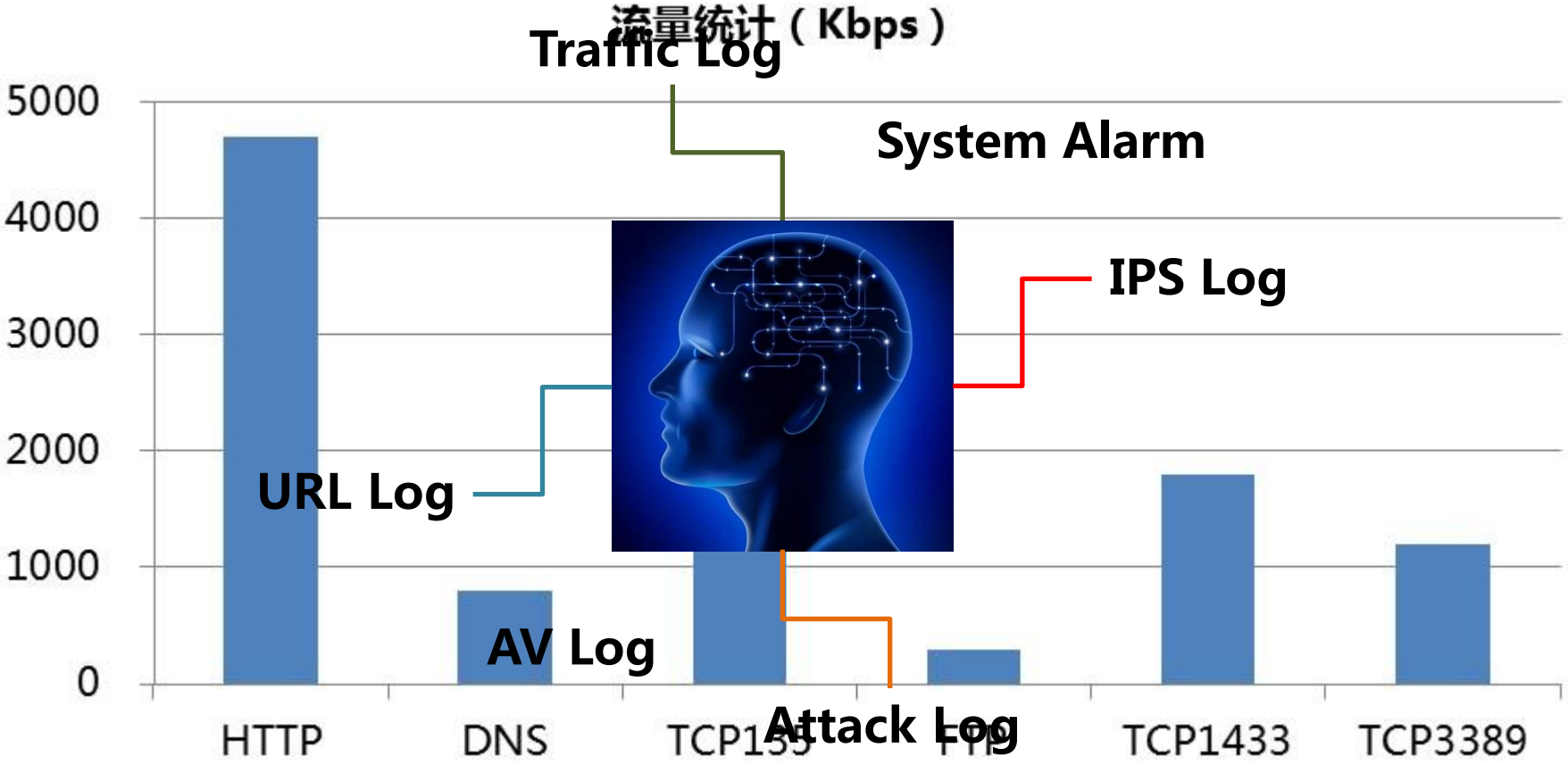
根因分析：关键信息未知

看不清、看不懂、看不全让安全举步维艰

- 决策阶段
  - 缺乏基本信息的了解
- 执行阶段
  - 缺乏合理的安全建议
- 响应阶段
  - 缺乏及时的效果反馈

洞察力：被忽略的第四大能力

看看本质：这样的数据是如何形成的？



NGFW 的全网洞察力


网康科技
NETENTSEC
详情
常规
会话ID: 2151411542
时间: 2014-04-09 15:42:52
应用: 二进制文件下载
IP协议: TCP
策略: 允许
动作: 阻断
威胁类型: 防病毒
威胁名称: HEUR/Malware.QVM11.Gen
威胁分类/内容: 9.rar
严重性: 严重
源
源用户: 10.198.20.100
源IP: 10.198.20.100
源端口: 52967
源国家: 10.0.0.0-10.255.255.25
源区域:
目的
目的用户: 未定义账号
目的IP: 42.121.254.142
目的端口: 80
目的国家: 中国
目的区域:
事件溯源
关联日志
时间 日志 类型 应用 动作 策略 总字节数 包数 严重性 分类 URL/文件名
2014-04-09 15:42:45 网址过滤 二进制文... 允许 允许 网络资源 files.cnblogs.com/cfdown/9.rar
2014-04-09 15:42:45 数据过滤 文件过滤 二进制文... 告警 允许 ocx 9.rar
2014-04-09 15:42:52 威胁 防病毒 二进制文... 阻断 允许 严重 9.rar
2014-04-09 15:43:32 流量 连接结束 二进制文... 允许 允许 68542 86

机器视角 VS 用户视角

IP_A在访问IP_B的TCP80端口 ✗

张某某在访问Sina的微博应用 ✓

A访问B的流量中发现了病毒 ✗

张某某访问B网站下载的X.rar文件中捆绑了病毒 ✓

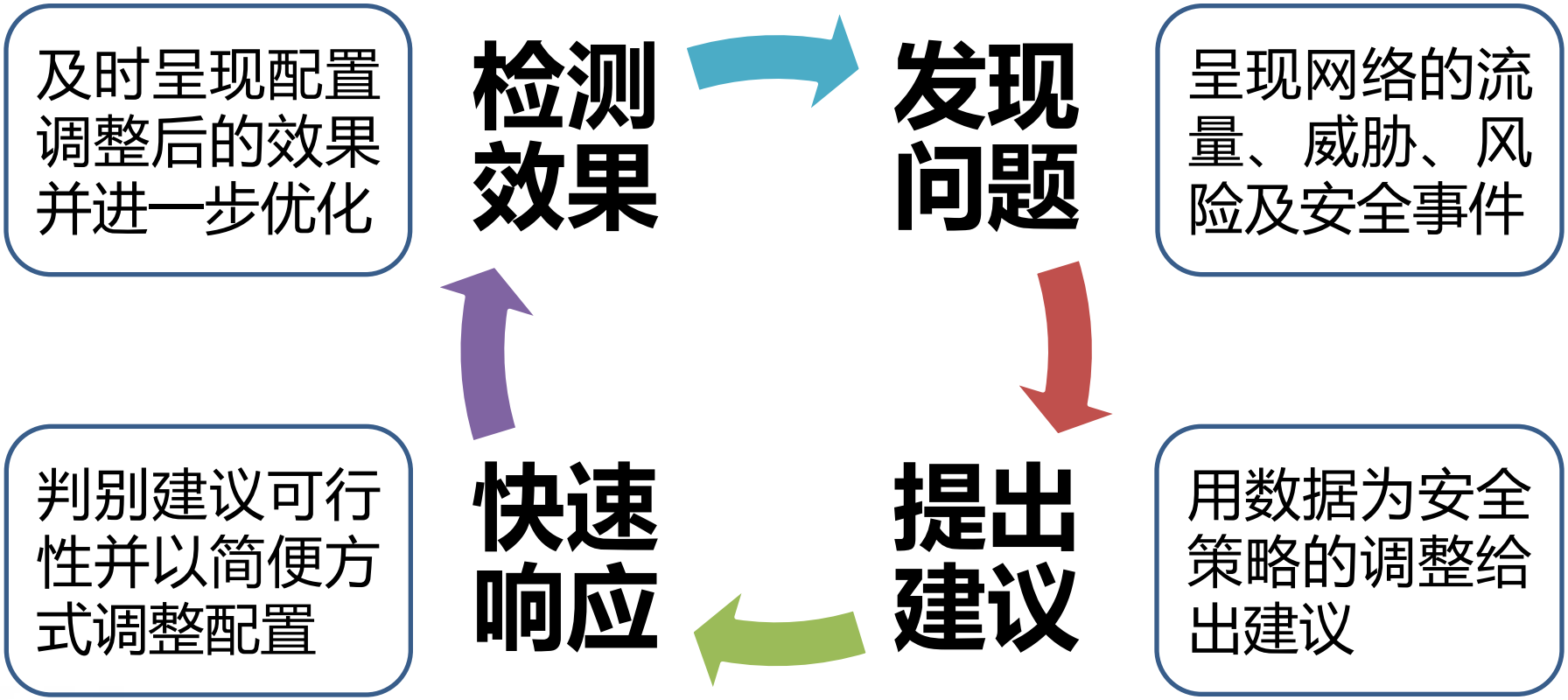
A当前占用的下行带宽为10M ✗

张某某当前占用的下行带宽为10M是平时的5倍 ✓

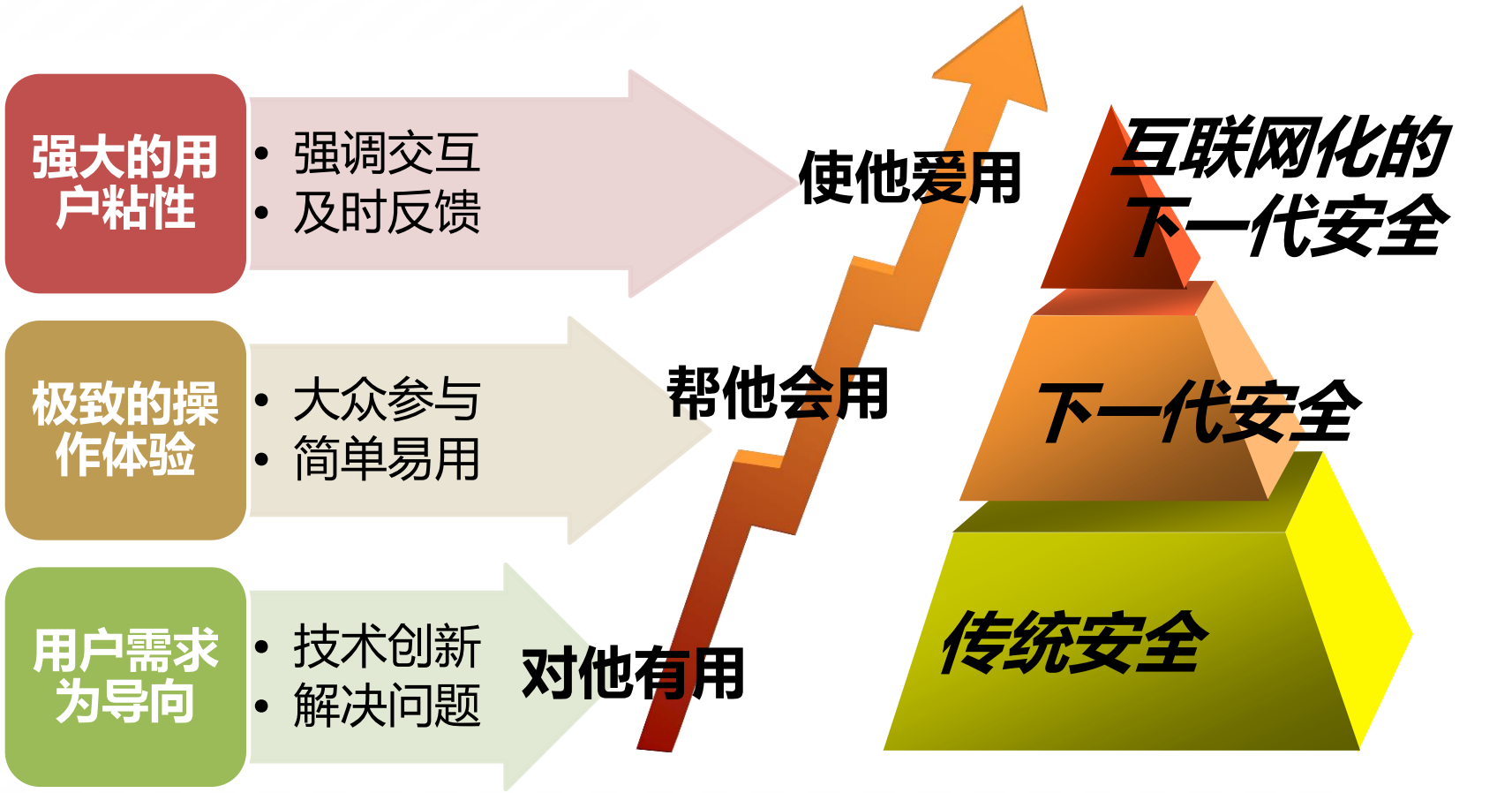
A当前与100个IP建立了连接 ✗

张某某与100个IP建立了连接，目标分属10个国家 ✓

重构防火墙的使用逻辑


发现问题
呈现网络的流量、威胁、风险及安全事件
提出建议
用数据为安全策略的调整给出建议
快速响应
判别建议可行性并以简便方式调整配置
检测效果
及时呈现配置调整后的效果并进一步优化

用互联网思维武装传统安全



以用户的名义重新定义NGFW

有用

- 融合必要的安全功能，能够防御更加复杂、隐蔽的威胁

会用

- 能够用数据支撑用户建立并持续高效运行安全管理闭环

爱用

- 简约的人机交互和及时的正反馈激励，极致的用户体验

新安全 新体验

安全从此触手可及

Thanks!