微隔离如何颠覆防火墙

严雷　　蔷薇灵动创始人

2018 ISC 互联网安全大会 中国·北京
Internet Security Conference 2018 Beijing·China
（原中国互联网安全大会）

目录

云安全产品部署的三个环境约束

永远不要忘记你是在一个极其庞大，极其复杂，变化极快的环境下思考产品

特别多，特别乱，总在变

- 规模
- 复杂
- 变化

量变引起质变

为什么不能用资源池解决东西向流量问题

- 东西向流量是南北向的20倍不止
- 微服务架构让情况更严峻
- 绝对不能采用大范围引流
- 绝对不能制造瓶颈点

为什么要考虑TCO

- 购买成本：必须考虑单点价格，因为不是一次性采购！
  成本随着云规模的扩展而线性增长
- 部署成本：必须改变购买“大盒子” 的偏好
- 单点开销每增长一个百分点，都可能意味着上百万的部署成本。
- 运维成本：安装必须自动化
  管理必须是软件定义的

你保护不了你看不见的东西

- 安全开始于对业务的理解

  哲学三问：你是谁？你从哪里来？要到哪里去？

- 虚拟化架构使得业务很难被准确观察

  计算在哪里发生？

  虚机之间容器之间如何交互？

  数据在哪里存储？

瞬息万变的云

- 不再有一成不变的策略

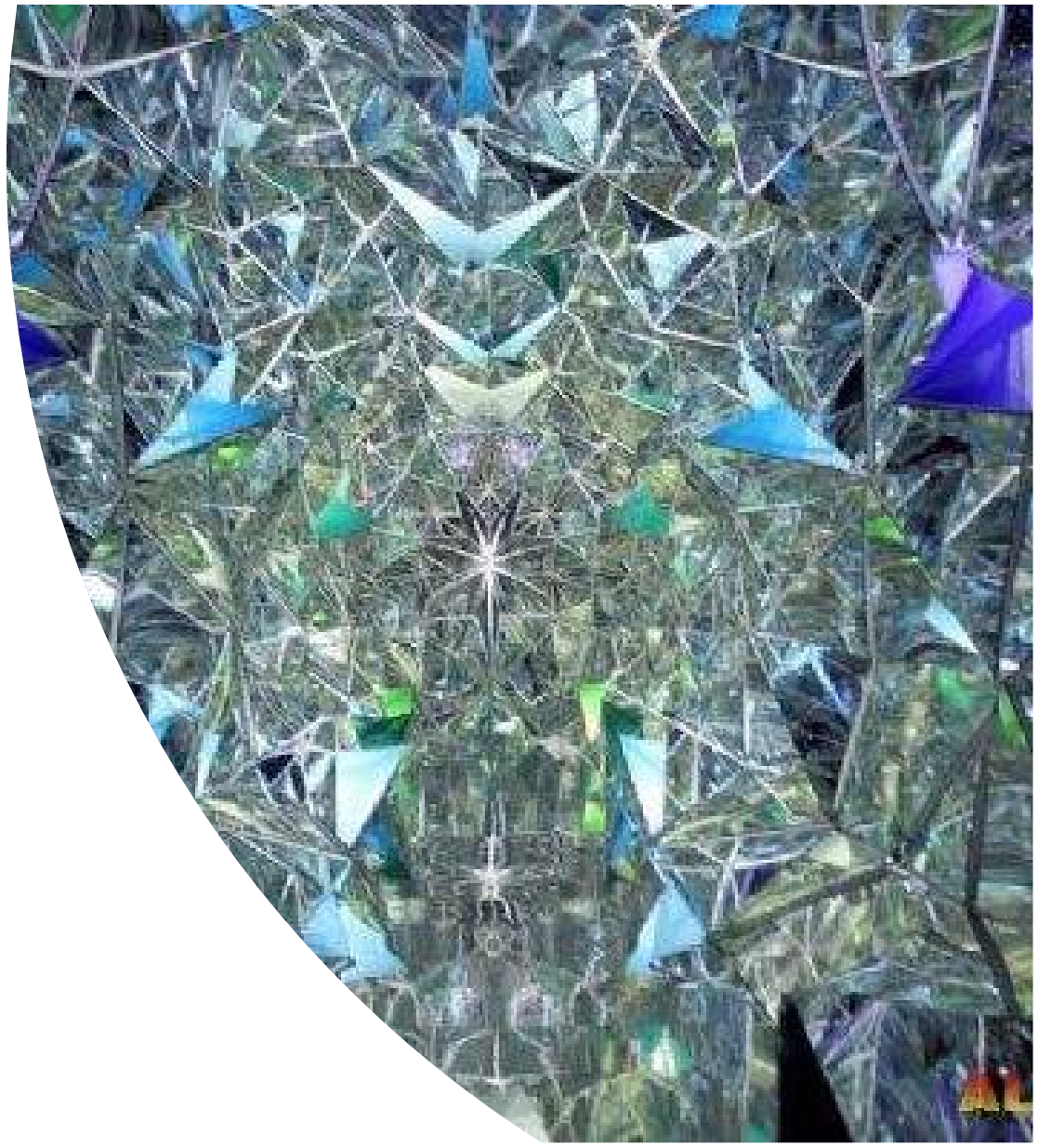
  漂移，扩容，迁移，弹性扩展，业务上下线

- 超短的资源生存周期

  从几个月到几分钟都有可能

  各种资源完全动态分配

- 你的安全基础架构必须跟得上云的脚步



云安全技术发展的三个方向

全面理解，全面控制，全面自动化

- 业务可视
- 负载控制
- 软件定义

业务可视

- 云内安全没有可视化就没法做
- 不要尝试手工的业务分析，量太大，而且变化太快。
- 可视化的价值不是监控而是策略设计的依据
- 好的可视化能做业务分析
- 更好的可视化可以辅助策略设计甚至自动生成策略

负载控制

- 安全不能只是侦测，你必须要有控制点（enforcement point）
- 只有控制才能有效下降风险，并对安全事件做应急处置
- 云安全的发展方向是白名单。
- 控制点要分布的足够广泛，最好是部署在工作负载之内
- 控制点要足够便宜和轻量级

软件定义

- 统一的管理与分散的控制
- 纯软件化定义安全策略
- 自动化的策略下发与调整能力
- 最好具备自适应能力

微隔离是如何颠覆防火墙的

颠覆的意思就是，以一种全新的产品，彻底替代对过去产品的需求，意味着完全不同的技术理念，完全不同的业务逻辑，以及完全非对称的竞争优势。

防火墙的世界是酱紫的

1 网络是静态的

网址一旦分配就不再变化

网络地址与计算资源有稳定的对应关系

2 内部是可靠的

网络可以分为不同的区域

边界防御，枪口对外

3 有个叫网关的地方

所有的流量都会经过这个里

如果没有的话可以造一个

4 业务是已知的

根据明确的业务需求设计策略

如果不知道，就用黑名单

云计算的现实是酱婶儿的

1 经常性变化的网络

漂移总在发生

网址总在变化

2 多租户多应用混合部署

网段没有了

防火墙失去了表达方式

3 看不见的流量

虚机间甚至于容器间流量根本不出现在网络上

内网没有关键路径，也就是说没有网关这种地方了

大范围引流又不现实

和酱婶儿的

4 业务交付要求极高

每天都可能上线新的业务

业务内部的通信关系极其复杂

无法预先设计安全策略

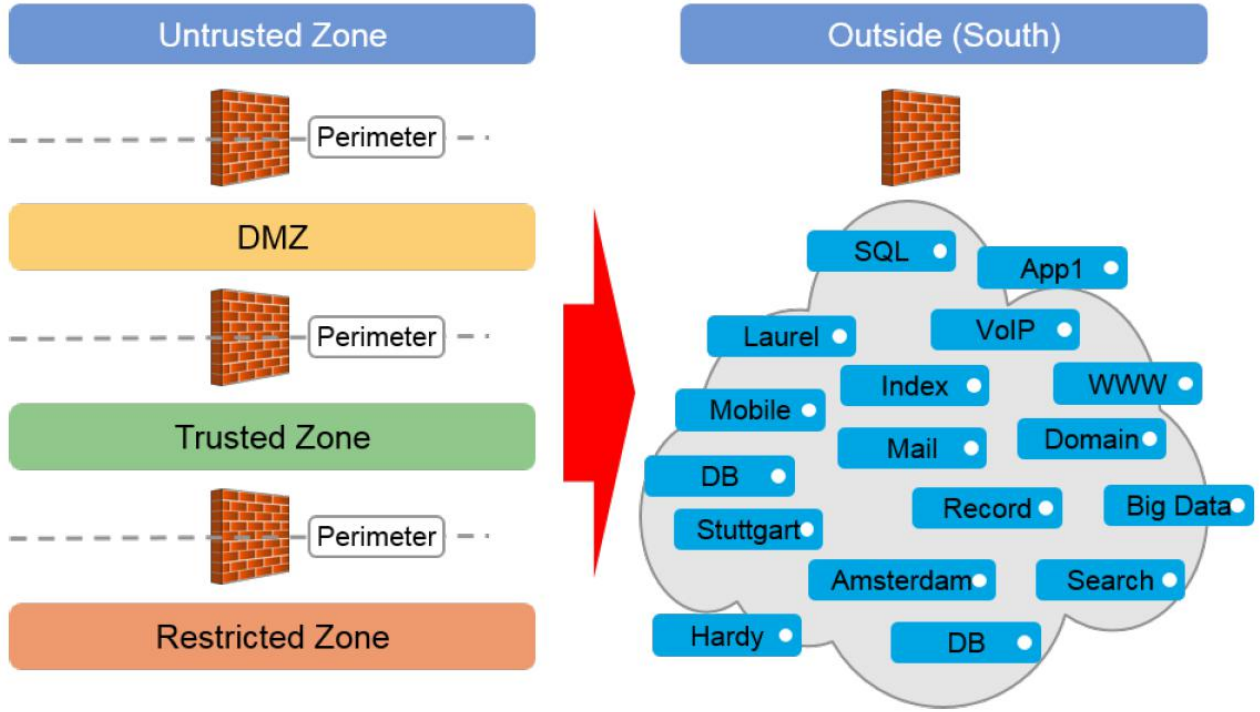
5 防火墙太重了

成千上百的虚防火墙（安全组）管理起来就是个噩梦

计算开销可能是个大问题

云计算时代的网络安全革命：微隔离

微隔离（microsegmentation）最早由Gartner在其软件定义的数据中心（SDDC）的相关技术体系中提出，用于于提供主机（容器）间安全访问控制（区别于过去的安全域间的安全访问控制）,并对东西向流量进行可视化管理。是云安全的核心技术模块。



微隔离的基本逻辑

1 去网络化

- 不利用ip地址作为策略语言
- 不利用网段作为分组手段（这一点很重要）

2 零信任

- 点到点访问控制
- 基于白名单的策略设计

3 自学习

- 业务关系自学习
- 安全策略自动生成

4 控制点在工作负载上

- 在每一个工作负载上（CLOUD WORKLOAD）进行访问控制
- 不需要网关，不需要引流，没有瓶颈点
- 当网络规模发生变化时安全能力不受影响

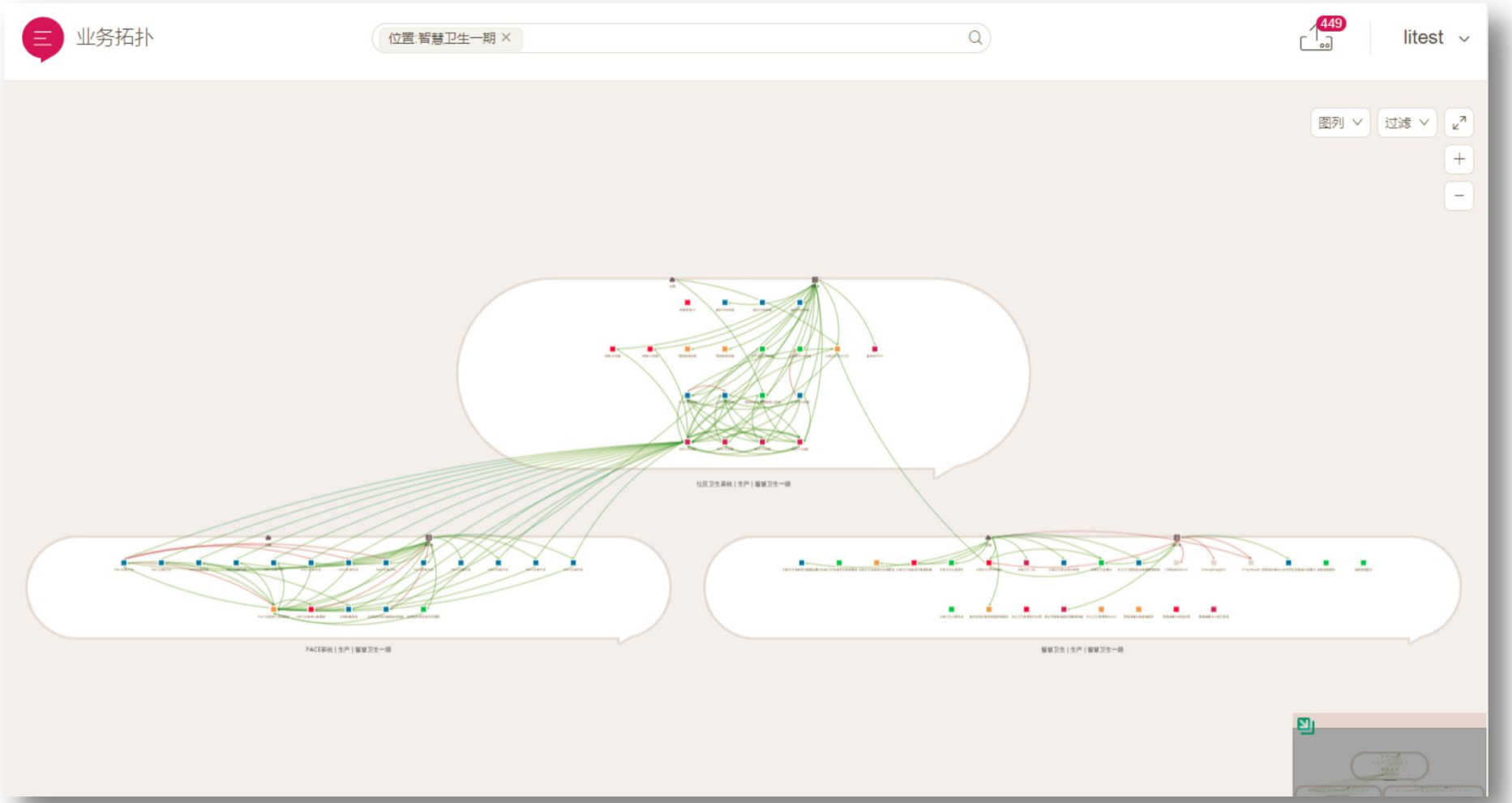
5 软件定义

- 分散的控制点与统一的管理平台
- 一套用于策略管理软件语言
- 彻底的API化

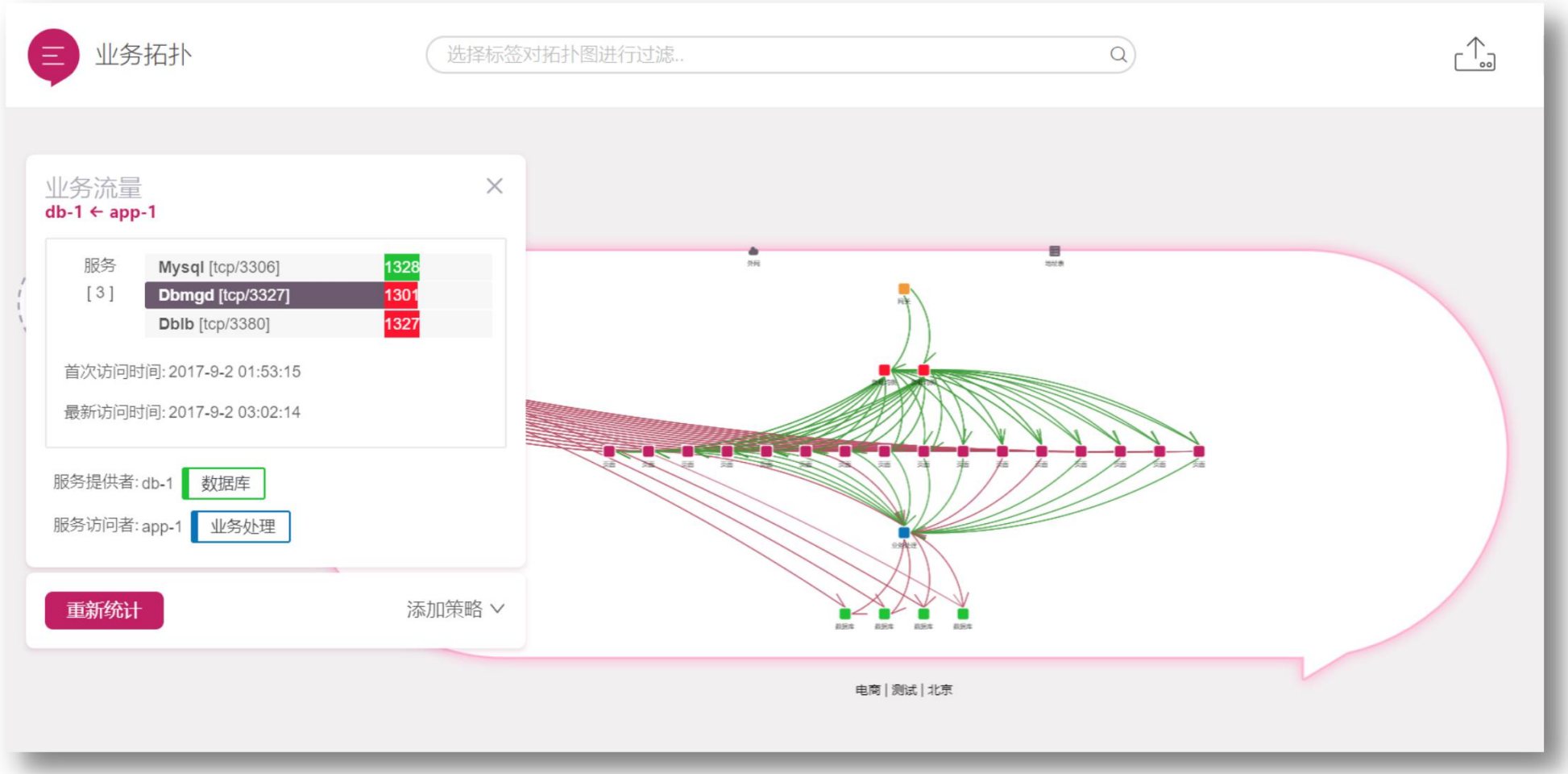
6 自适应

- 对迁移，弹性扩展，网址变化能够感知
- 能够进行策略重算
- 能够自动进行策略调整

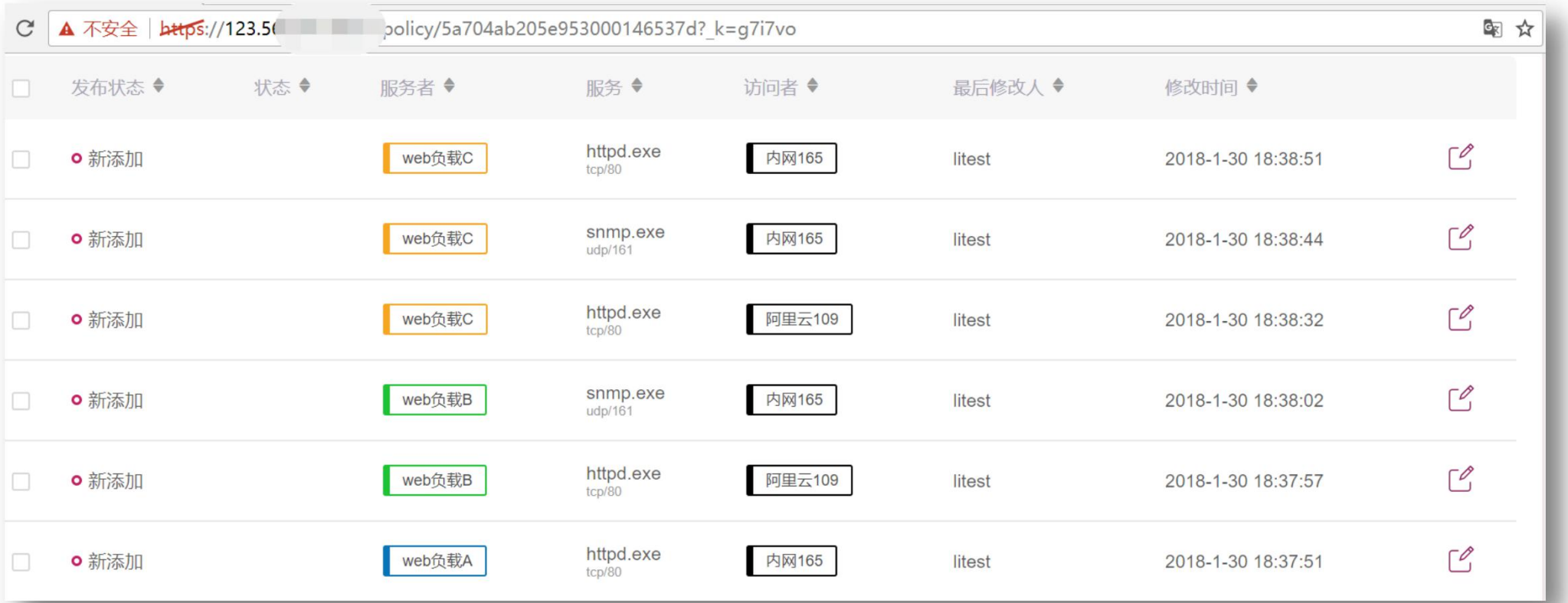
举个栗子



可视化能力


业务拓扑
选择标签对拓扑图进行过滤..
业务流量
db-1 ← app-1
服务
[3]
Mysql [tcp/3306] 1328
Dbmgd [tcp/3327] 1301
Dblb [tcp/3380] 1327
首次访问时间: 2017-9-2 01:53:15
最新访问时间: 2017-9-2 03:02:14
服务提供者: db-1 数据库
服务访问者: app-1 业务处理
重新统计
添加策略
电商 | 测试 | 北京

软件定义



发布状态	状态	服务者	服务	访问者	最后修改人	修改时间
新添加		web负载C	httpd.exe tcp/80	内网165	litest	2018-1-30 18:38:51
新添加		web负载C	snmp.exe udp/161	内网165	litest	2018-1-30 18:38:44
新添加		web负载C	httpd.exe tcp/80	阿里云109	litest	2018-1-30 18:38:32
新添加		web负载B	snmp.exe udp/161	内网165	litest	2018-1-30 18:38:02
新添加		web负载B	httpd.exe tcp/80	阿里云109	litest	2018-1-30 18:37:57
新添加		web负载A	httpd.exe tcp/80	内网165	litest	2018-1-30 18:37:51

为什么是颠覆

- **策略总数降低95%**
  - 能看懂
  - 易维护

策略极简：

- **整体开销0.5%**
  - 安全投入更低
  - 对业务影响更小

开销极小：

- **策略运维全自动**
  - 极大提升工作效率
  - 极大减少运维开销

效率极高：

- **业务与安全同步**
  - 安全不再阻挡业务
  - 业务不必牺牲安全
  - 符合DEVOPS要求

交付极快：

ISC 2018
ISC互联网安全大会

360互联网安全中心

谢 谢！

2018 ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原中国互联网安全大会）

360技术

IT大咖说 知识共享平台