DBAplus 数据连接未来 | IT大咖说 知识分享平台

Gdevops
全球敏捷运维峰会

互联网企业安全运维实践

演讲人：田国华

2017.5.13 成都

个人简介

田国华

资深信息安全经理/上海拍拍贷

- 专注信息安全12年；
- 前携程高级网络安全经理；
- 现上海拍拍贷任职；
- CISSP、CISA、PMP、ITIL、CCNP等认证证书；
- 10余项技术发明专利；
- (ISC)² 上海分会理事；

Contents

Part 1 安全建设思考

1 Par 安全建设阶段论

安全建设思考

优先解决业务痛点
做一些基础的“保命”工作；

1 救火阶段

2 体系化建设

扎实安全基础建设
建立安全体系+少量自研工具
+商用解决方案

自我研发和自动化
安全大数据
持续安全运营

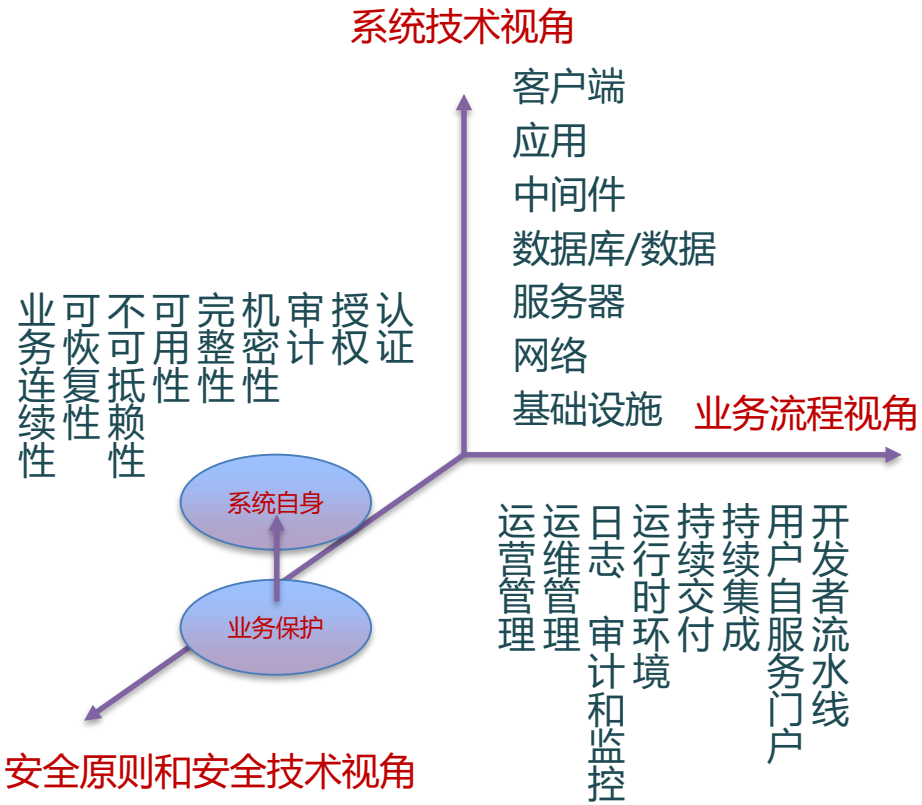
3 安全高阶

4 安全智能

安全自适应、智能化
阻止、检测、响应、预测

1 Par 系统安全架构

安全建设思考



1 Part

基本的安全理念依然重要

安全建设思考

监管	安全体系	策略	标准	风险和合规管理
身份管理	单点登录	密码强度	多因素认证	证书
数据保护	加密	密钥管理	数据防泄露	备份及存档
日志和监控	审计	衡量	关联	告警

1 Par 一些经验

安全建设思考

安全运维之术

Part 2

2 Par

两个重要概念

安全运维之术

DUE CARE

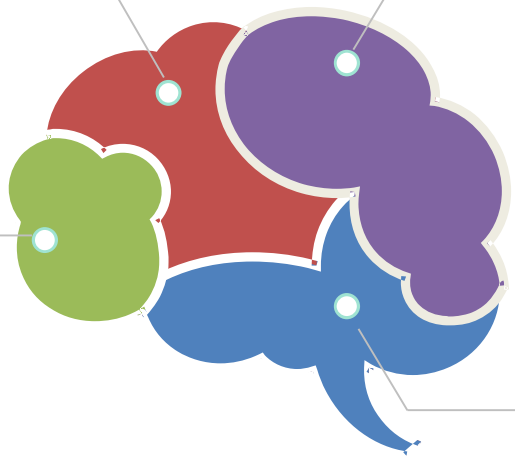
DUE DILIGENCE

2 Par 三思而行

安全运维之术

我是这个工作的合适人选吗？

我有能力执行这个任务吗？



我能控制整个变更吗？

GO!

Think Twice!

2 Par 安全视野

安全运维之术

研发

运维

安全

其他

2 Par

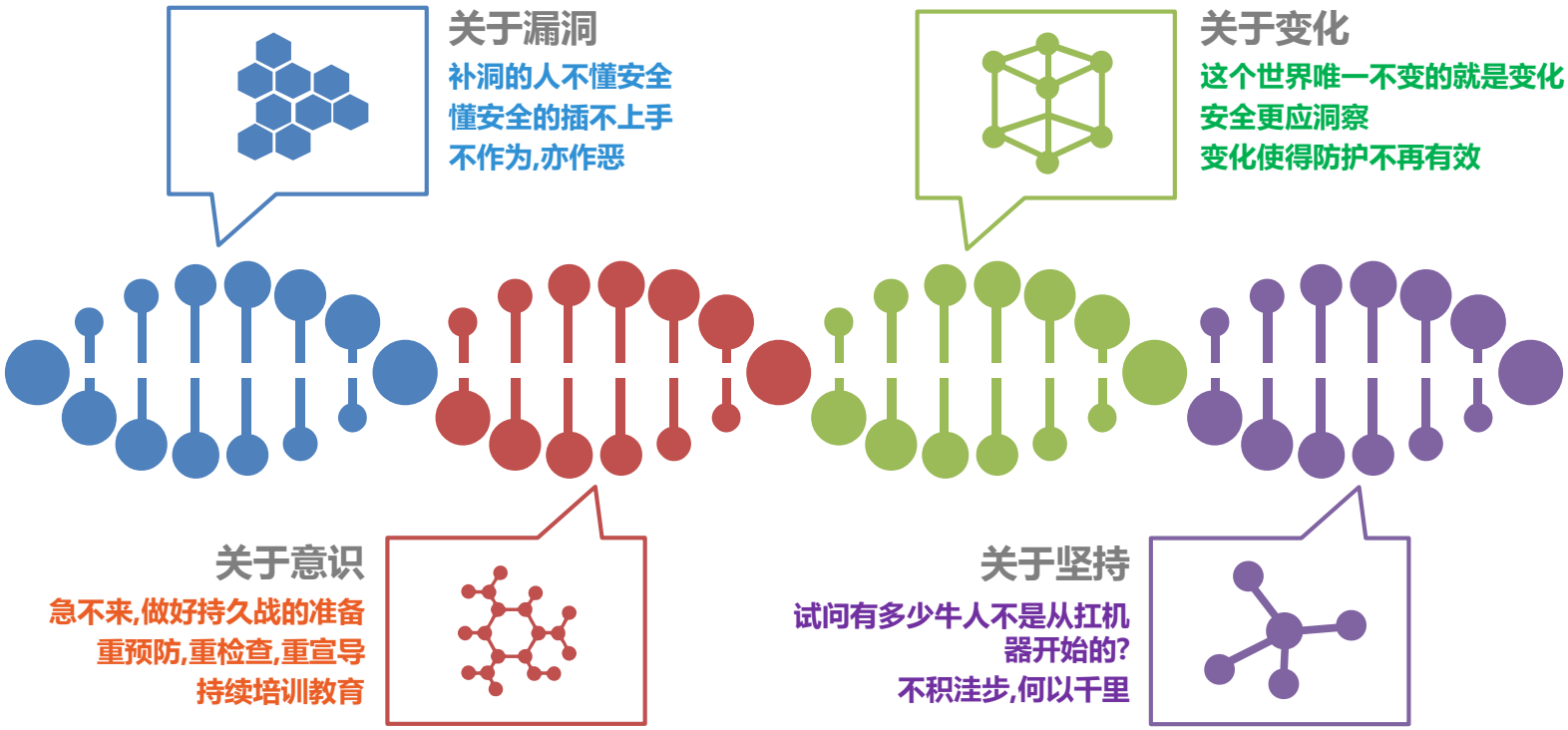
有挑战的行动

安全运维之术

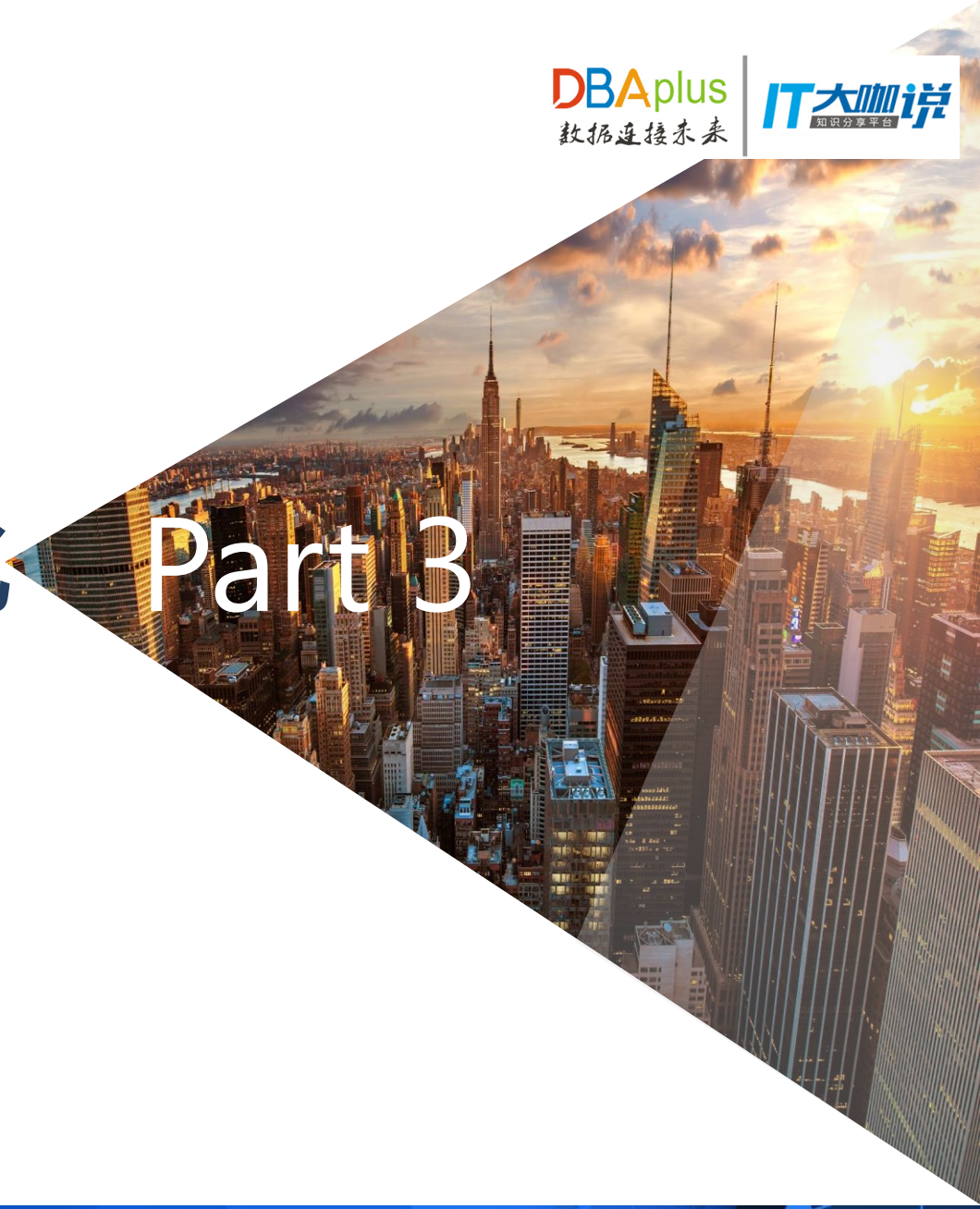
OUTAGE WINDOW

2 Pa 谈点看法

安全运维之术



安全运维自动化 Part 3



3 Par

安全运维自动化实践

安全运维自动化

3 Par

Anti-DDOS

安全运维自动化

封锁被攻击IP

与运营商联动
NOC 一键封锁

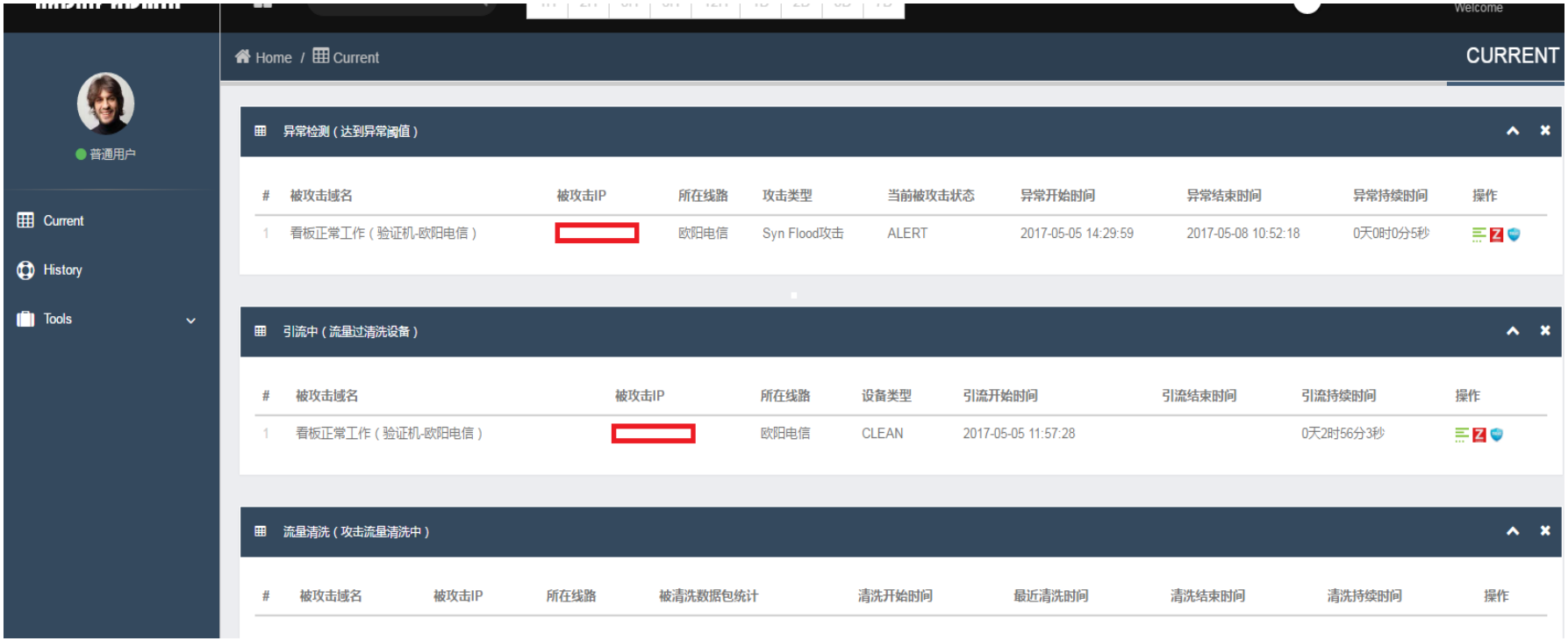
云端防护

需要开放API接口
DNS切换部分自动化

自研DDOS攻击看板

支持移动端
实时显示受攻击IP及流量情况
超出设定阀值告警

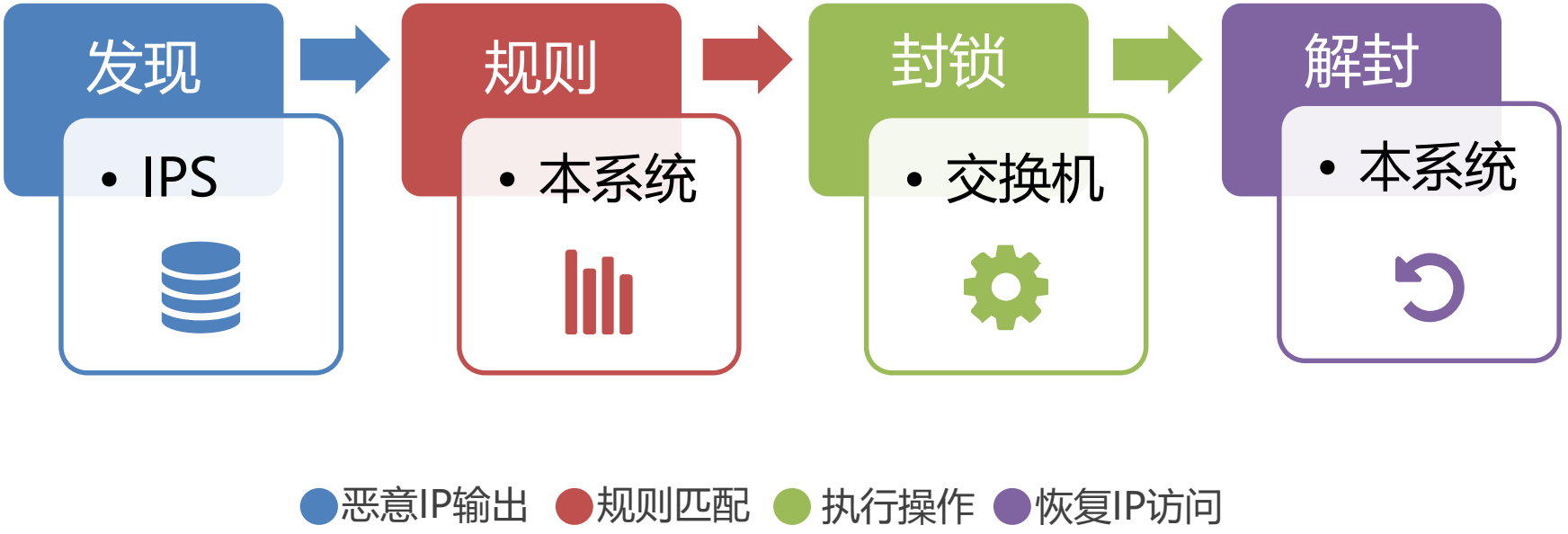
3 Par Anti-DDOS
安全运维自动化



3 Par

交换机封IP

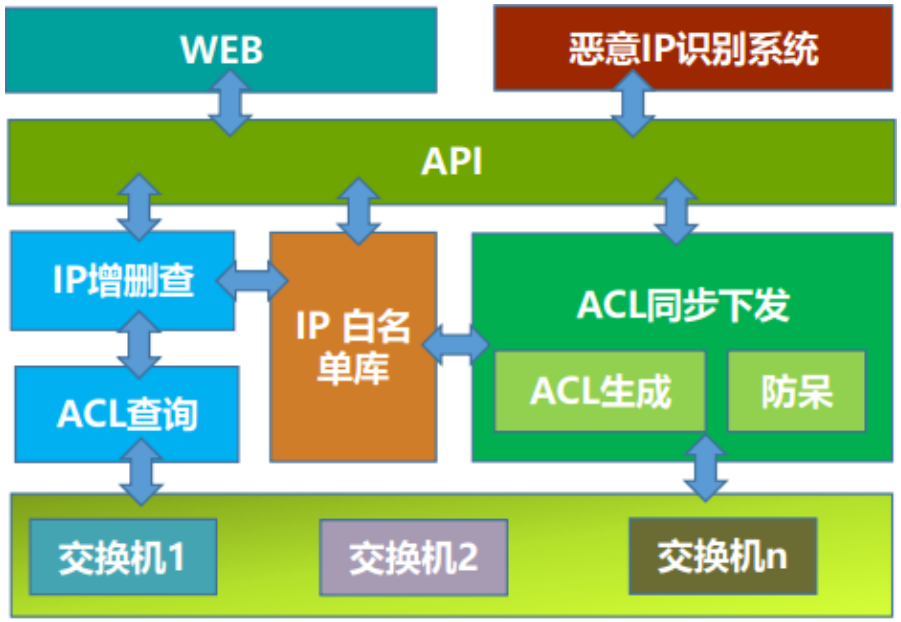
安全运维自动化



3 Par

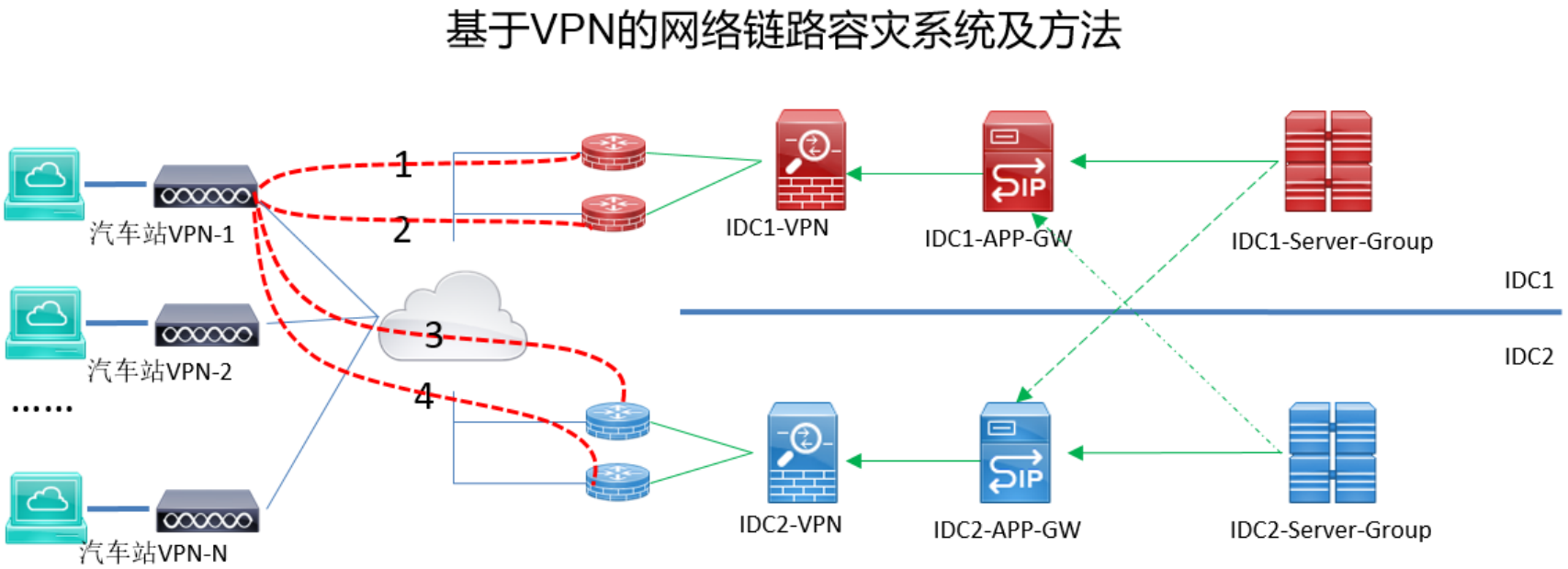
交换机封IP

安全运维自动化



3 Par 基于VPN链路容灾

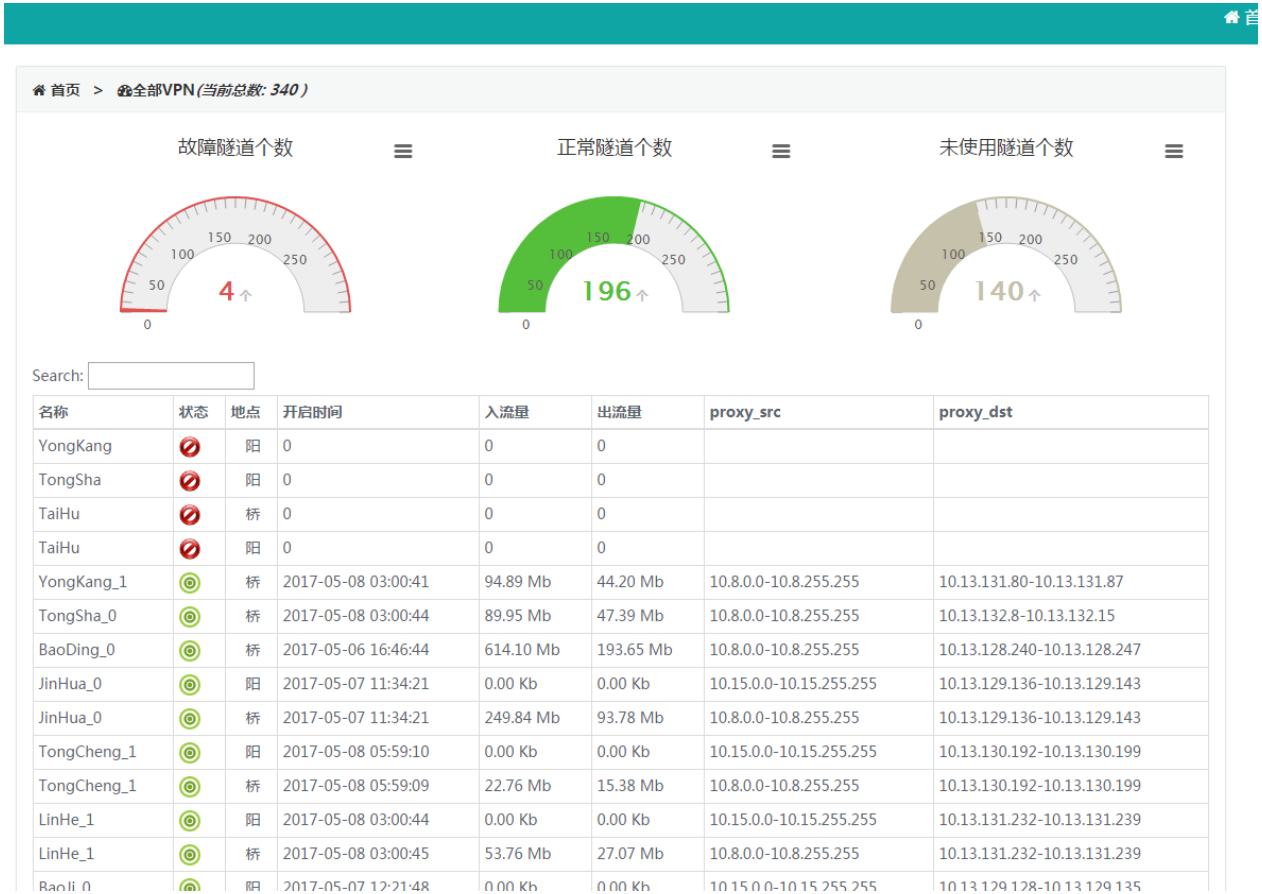
安全运维自动化



3 Par

基于VPN链路容灾

安全运维自动化

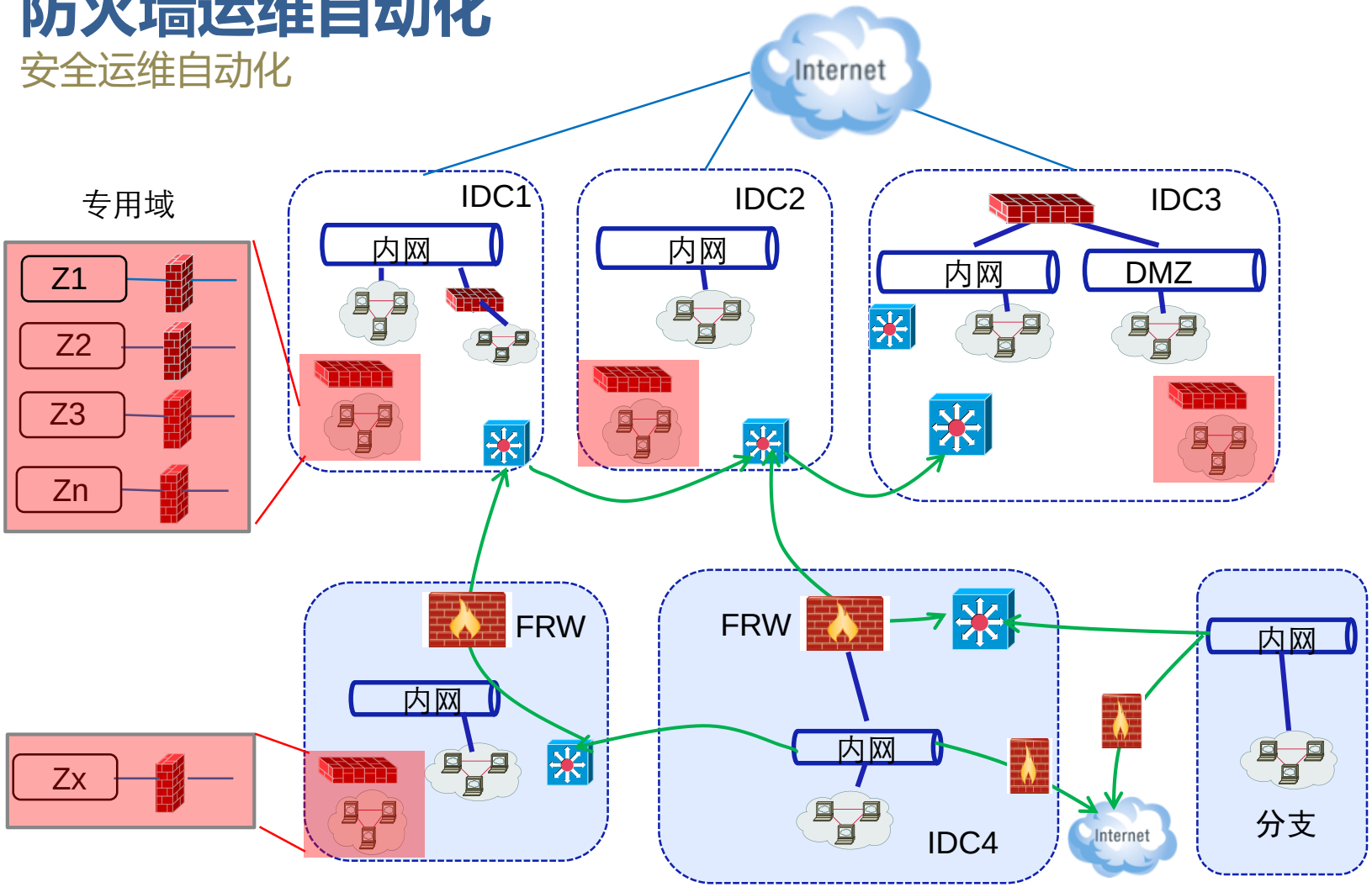


名称	状态	地点	开启时间	入流量	出流量	proxy_src	proxy_dst
YongKang		阳	0	0	0		
TongSha		阳	0	0	0		
TaiHu		桥	0	0	0		
TaiHu		阳	0	0	0		
YongKang_1		桥	2017-05-08 03:00:41	94.89 Mb	44.20 Mb	10.8.0.0-10.8.255.255	10.13.131.80-10.13.131.87
TongSha_0		桥	2017-05-08 03:00:44	89.95 Mb	47.39 Mb	10.8.0.0-10.8.255.255	10.13.132.8-10.13.132.15
BaoDing_0		桥	2017-05-06 16:46:44	614.10 Mb	193.65 Mb	10.8.0.0-10.8.255.255	10.13.128.240-10.13.128.247
JinHua_0		阳	2017-05-07 11:34:21	0.00 Kb	0.00 Kb	10.15.0.0-10.15.255.255	10.13.129.136-10.13.129.143
JinHua_0		桥	2017-05-07 11:34:21	249.84 Mb	93.78 Mb	10.8.0.0-10.8.255.255	10.13.129.136-10.13.129.143
TongCheng_1		阳	2017-05-08 05:59:10	0.00 Kb	0.00 Kb	10.15.0.0-10.15.255.255	10.13.130.192-10.13.130.199
TongCheng_1		桥	2017-05-08 05:59:09	22.76 Mb	15.38 Mb	10.8.0.0-10.8.255.255	10.13.130.192-10.13.130.199
LinHe_1		阳	2017-05-08 03:00:44	0.00 Kb	0.00 Kb	10.15.0.0-10.15.255.255	10.13.131.232-10.13.131.239
LinHe_1		桥	2017-05-08 03:00:45	53.76 Mb	27.07 Mb	10.8.0.0-10.8.255.255	10.13.131.232-10.13.131.239
BaoJi_0		阳	2017-05-07 12:21:48	0.00 Kb	0.00 Kb	10.15.0.0-10.15.255.255	10.13.129.128-10.13.129.135

3 Par

防火墙运维自动化

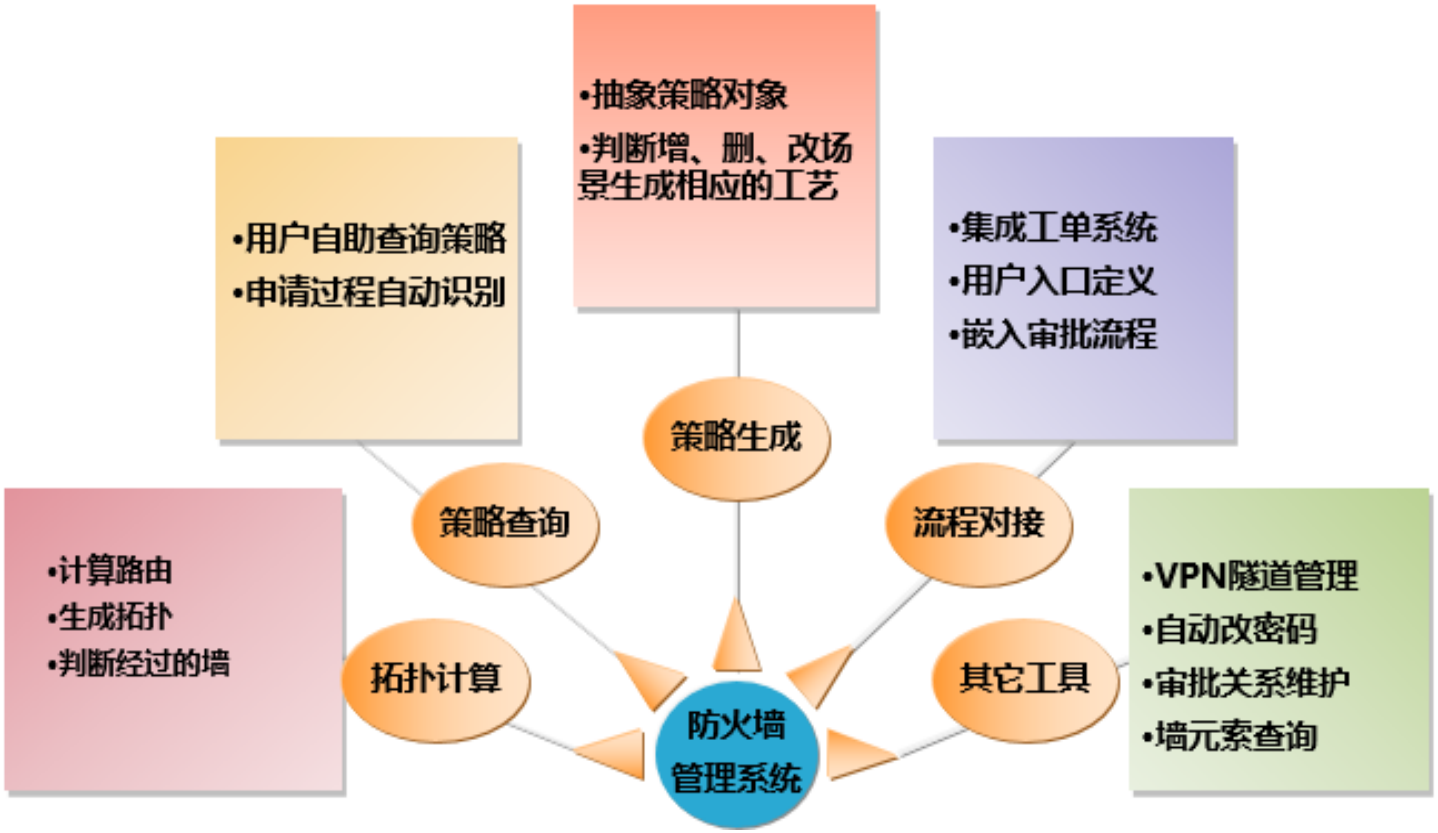
安全运维自动化



3 Par

防火墙运维自动化

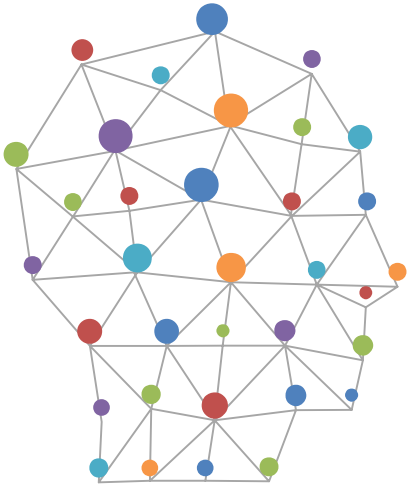
安全运维自动化



3 Par

一点感想

安全运维自动化



- 理解业务
- 要有充分的预案
- 定期演练
- 善用乙方资源
- 创新思维
- 全面安全视角

DBAplus 数据连接未来 | IT大咖说 知识分享平台

Gdevops

全球敏捷运维峰会

THANK YOU！