



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

- 1 安全建设思考
- 2 安全运维之术
- 3 安全运维自动化
- 4 Q&A



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

自我研发和自动化

安全大数据

持续安全运营

3

安全高阶

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

4

安全智能

安全自适应、智能化

阻止、检测、响应、预测

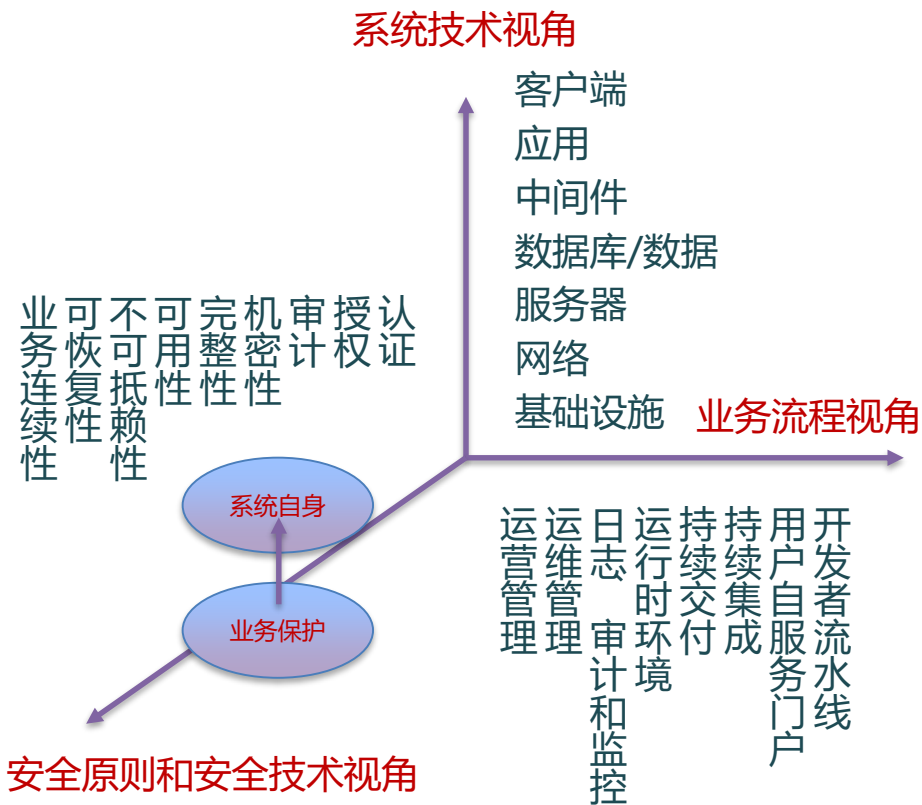
测

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

测试

真的需要测试吗?
真的不需要测试吗?

平衡

几者之间寻求平衡

品牌

怎样买到喜欢的品牌
但不被品牌绑定

容量

规划满足未来X年的容量

老板的偏好

将影响你的决定



安全运维之术

Part 2

2

Par

两个重要概念

安全运维之术

DUE
CAR
E



DUE
DILIGEN
CE

2

Par

三思而行

安全运维之术

我是这个工作的
合适人选吗？

我能控制整
个变更吗？



我有能力执行
这个任务吗？

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



谈点看法

安全运维之术



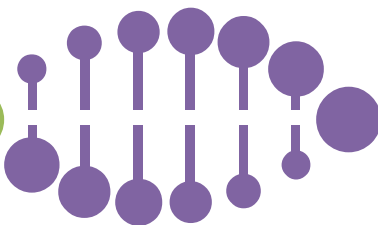
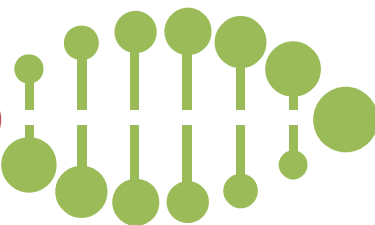
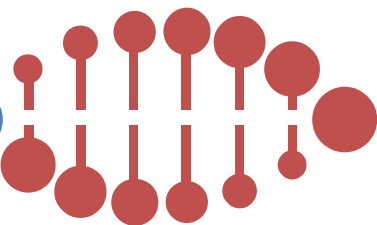
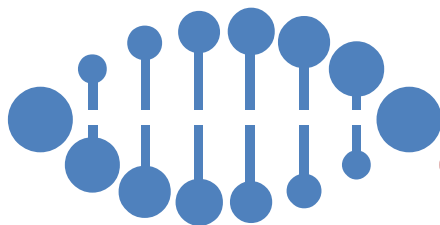
关于漏洞

补洞的人不懂安全
懂安全的插不上手
不作为,亦作恶



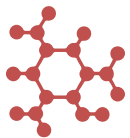
关于变化

这个世界唯一不变的就是变化
安全更应洞察
变化使得防护不再有效



关于意识

急不来,做好持久战的准备
重预防,重检查,重宣导
持续培训教育



关于坚持

试问有多少牛人不是从扛机器开始的?
不积跬步,何以千里





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

IP一键扔黑洞

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
超出设定阈值告警

云端联动

云端防护

需要开放API接口
DNS切换部分自动化

攻击看板自动告警

Anti-DDOS

安全运维自动化

The screenshot displays a dashboard with a left sidebar containing navigation options: Current, History, and Tools. The main content area is titled 'CURRENT' and shows three sections of data:

- 异常检测 (达到异常阈值)**: A table listing detected anomalies. The first entry shows a 'Syn Flood攻击' (Syn Flood attack) on '2017-05-05 14:29:59' with a status of 'ALERT'. The '被攻击IP' (Attacked IP) is highlighted with a red box.
- 引流中 (流量过清洗设备)**: A table showing traffic diversion. The first entry shows '引流开始时间' (Diversion start time) as '2017-05-05 11:57:28' and '引流持续时间' (Diversion duration) as '0天20时56分3秒'. The '被攻击IP' is highlighted with a red box.
- 流量清洗 (攻击流量清洗中)**: A table for traffic cleaning, currently empty.

异常检测 (达到异常阈值)									
#	被攻击域名	被攻击IP	所在线路	攻击类型	当前被攻击状态	异常开始时间	异常结束时间	异常持续时间	操作
1	看板正常工作 (验证机-欧阳电信)	[Red Box]	欧阳电信	Syn Flood攻击	ALERT	2017-05-05 14:29:59	2017-05-08 10:52:18	0天0时0分5秒	[Icons]

引流中 (流量过清洗设备)								
#	被攻击域名	被攻击IP	所在线路	设备类型	引流开始时间	引流结束时间	引流持续时间	操作
1	看板正常工作 (验证机-欧阳电信)	[Red Box]	欧阳电信	CLEAN	2017-05-05 11:57:28		0天20时56分3秒	[Icons]

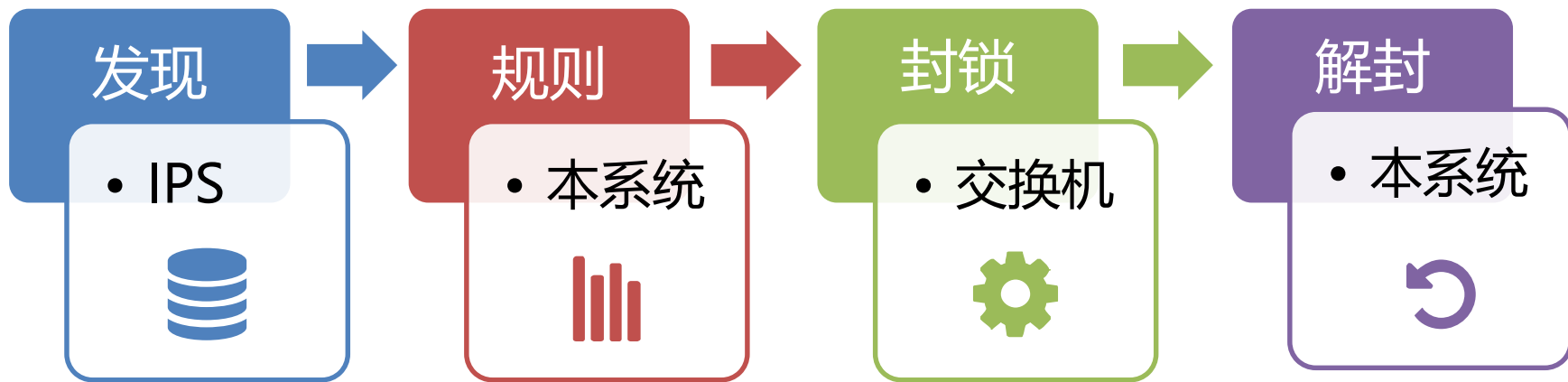
流量清洗 (攻击流量清洗中)									
#	被攻击域名	被攻击IP	所在线路	被清洗数据包统计	清洗开始时间	最近清洗时间	清洗结束时间	清洗持续时间	操作

3

Par

交换机封IP

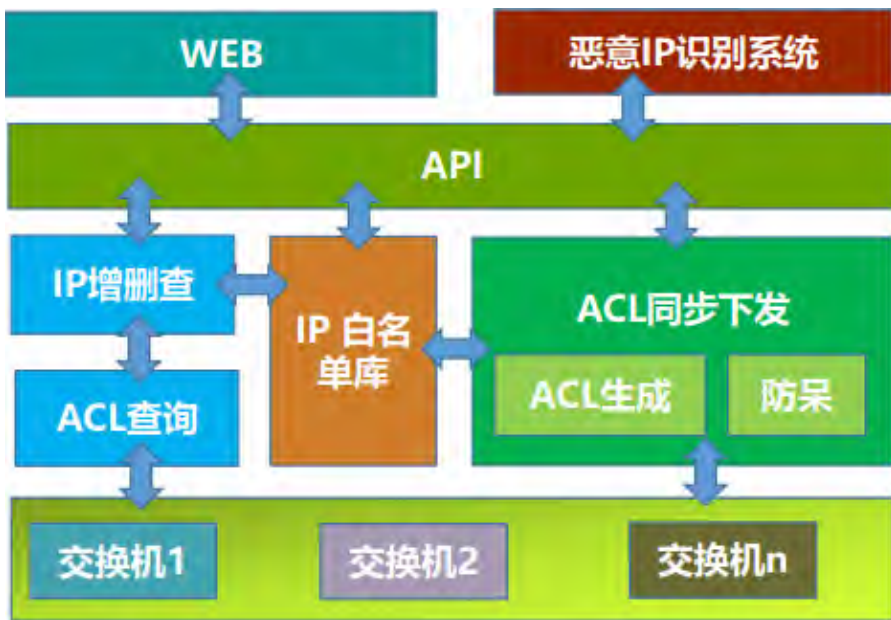
安全运维自动化



● 恶意IP输出 ● 规则匹配 ● 执行操作 ● 恢复IP访问

3 Par

交换机封IP 安全运维自动化

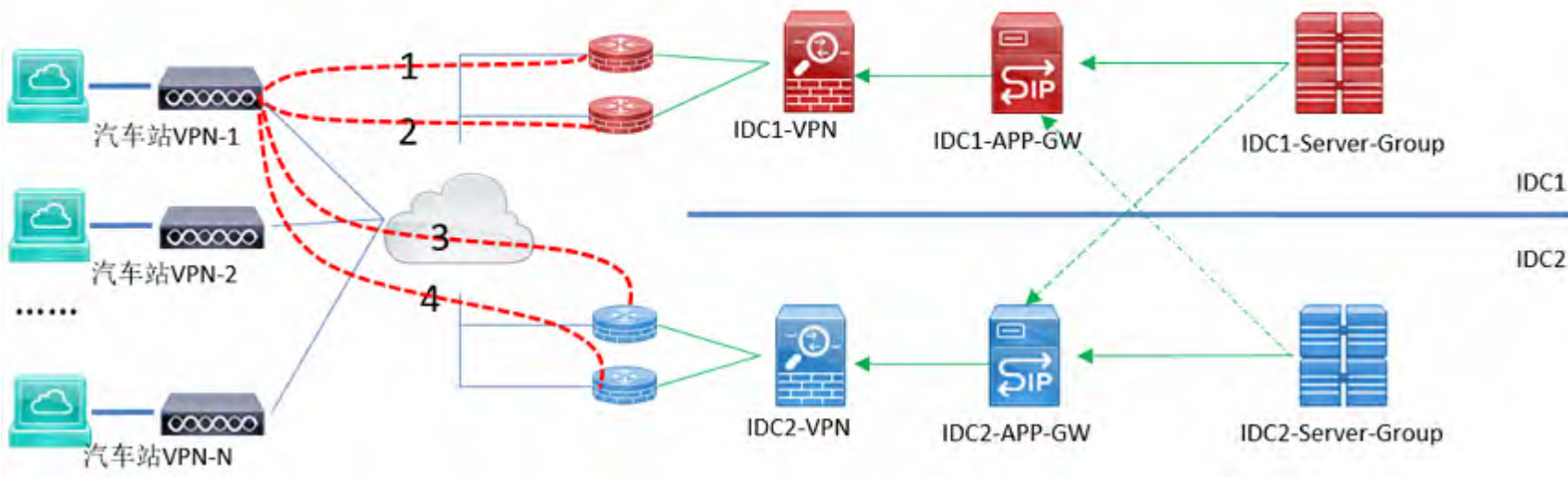


The screenshot shows a web form titled '增加交换机黑灰名单'. It includes a text input for 'ip地址' (IP Address) with a note: '请输入需要封锁的ip地址；批量增加ip请用换行符分隔，单次不能超过10个。' (Please enter the IP address to be blocked; for bulk addition, use line breaks, and no more than 10 per batch). Below this is a '持续时长' (Duration) section with a text input '最大14天' (Maximum 14 days) and a dropdown menu set to '小时' (Hours). A checked checkbox reads '不进行订单校验 (勾选就不会走订单校验流程)' (Do not perform order verification (checking will skip the order verification process)). A '描述' (Description) text area is labeled '详细描述，1-50字符' (Detailed description, 1-50 characters). At the bottom right are '取消' (Cancel) and '保存' (Save) buttons.

基于VPN链路容灾

安全运维自动化

基于VPN的网络链路容灾系统及方法

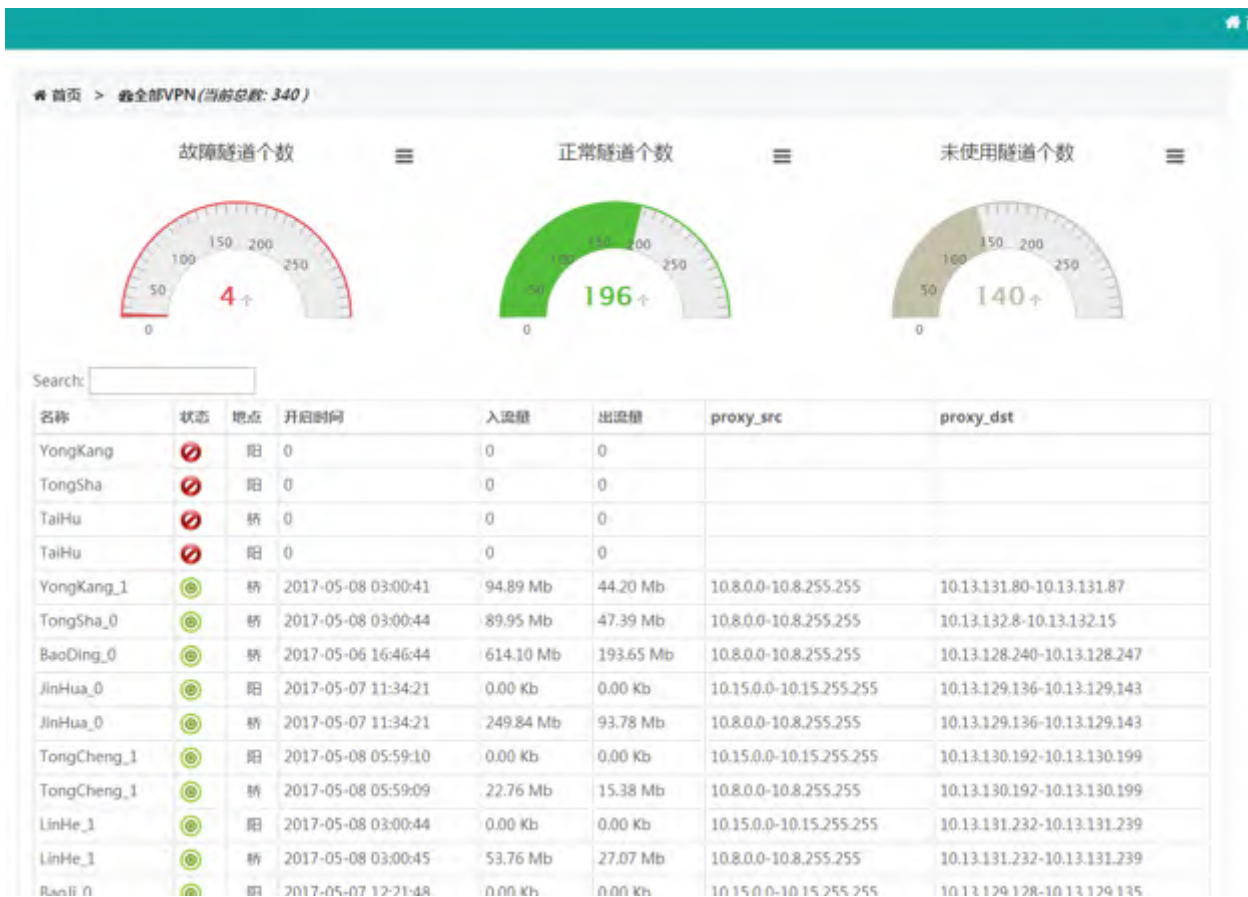


3

Par

基于VPN链路容灾

安全运维自动化

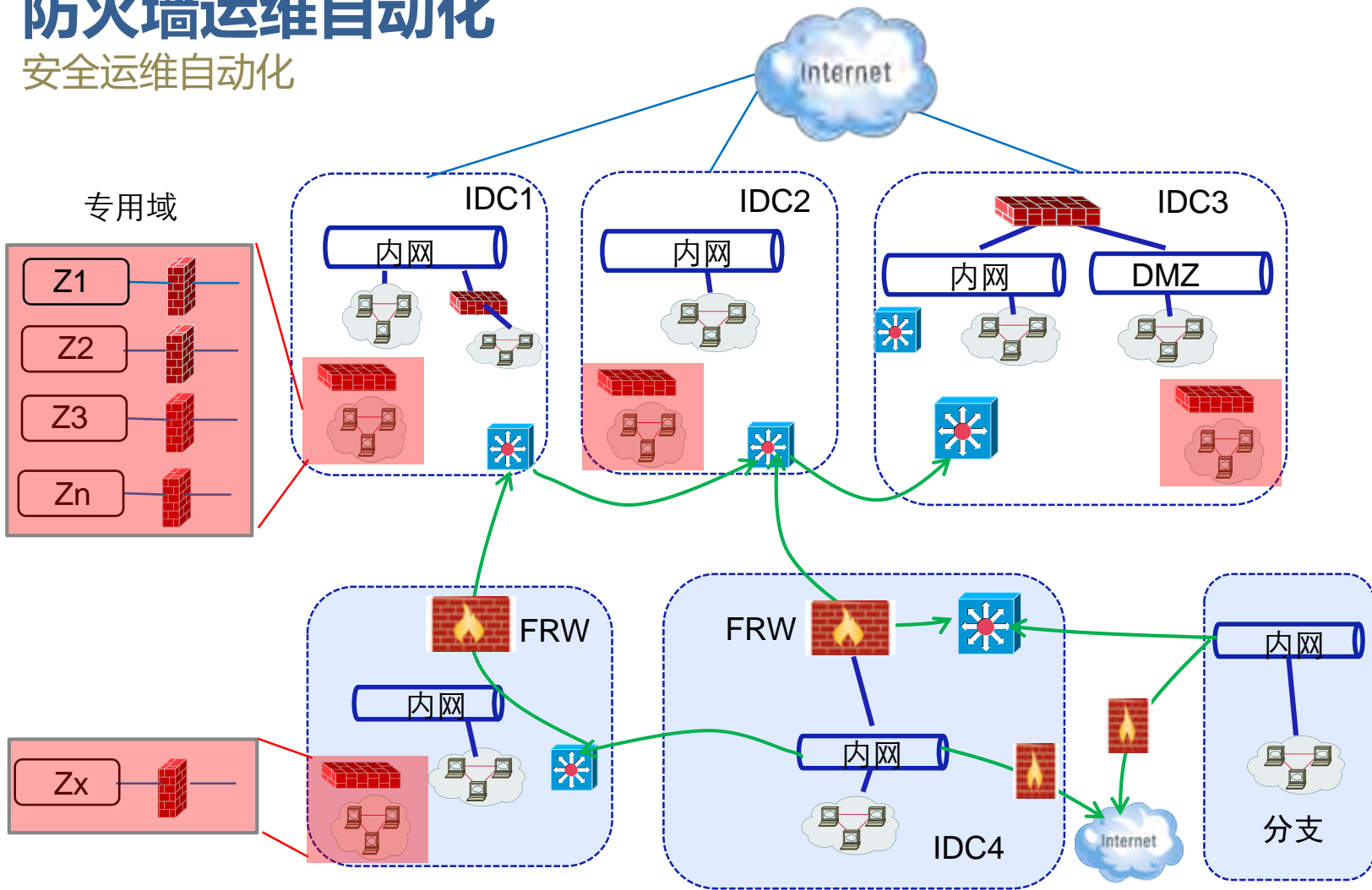


3

Par

防火墙运维自动化

安全运维自动化

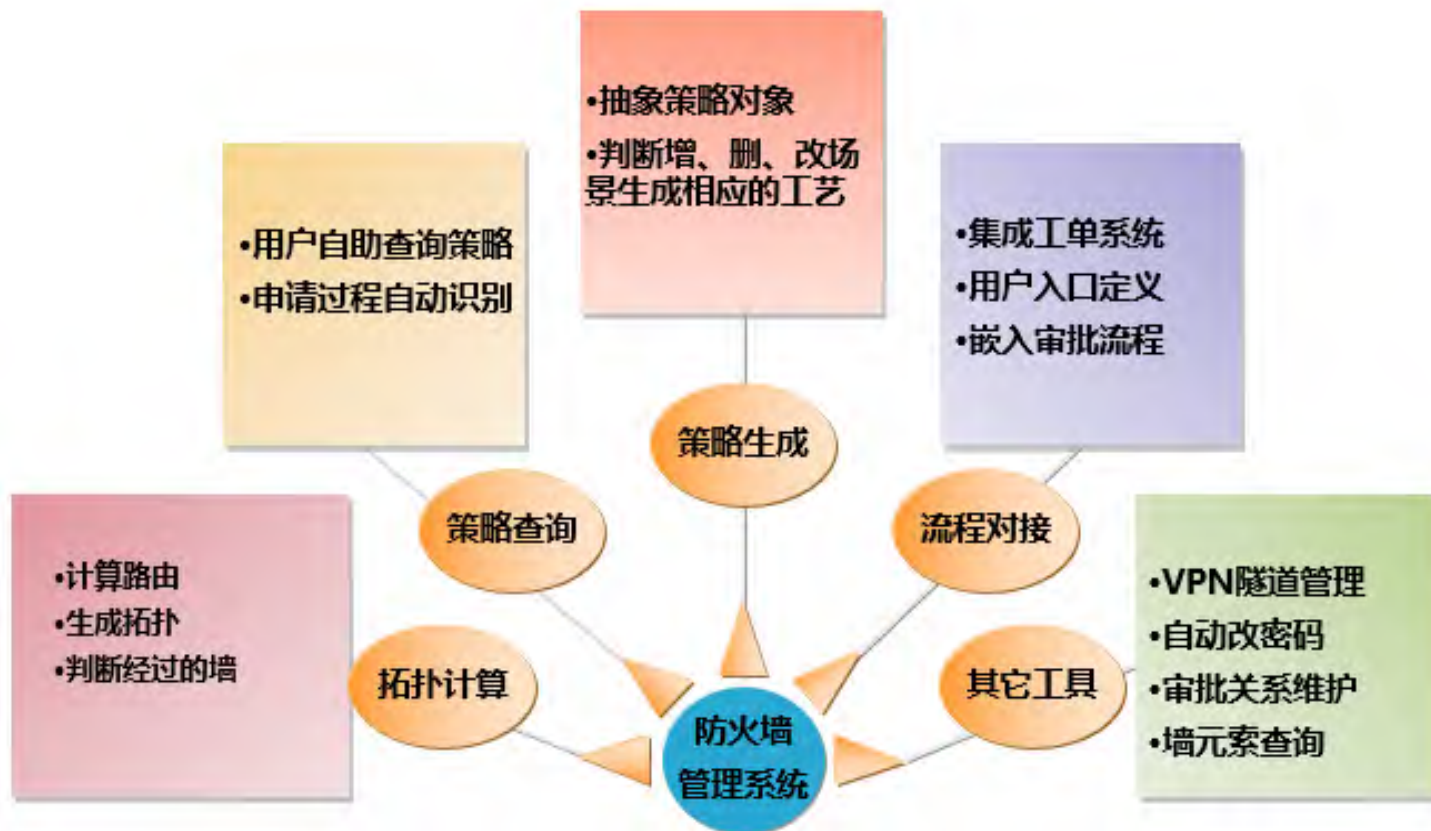


3

Par

防火墙运维自动化

安全运维自动化

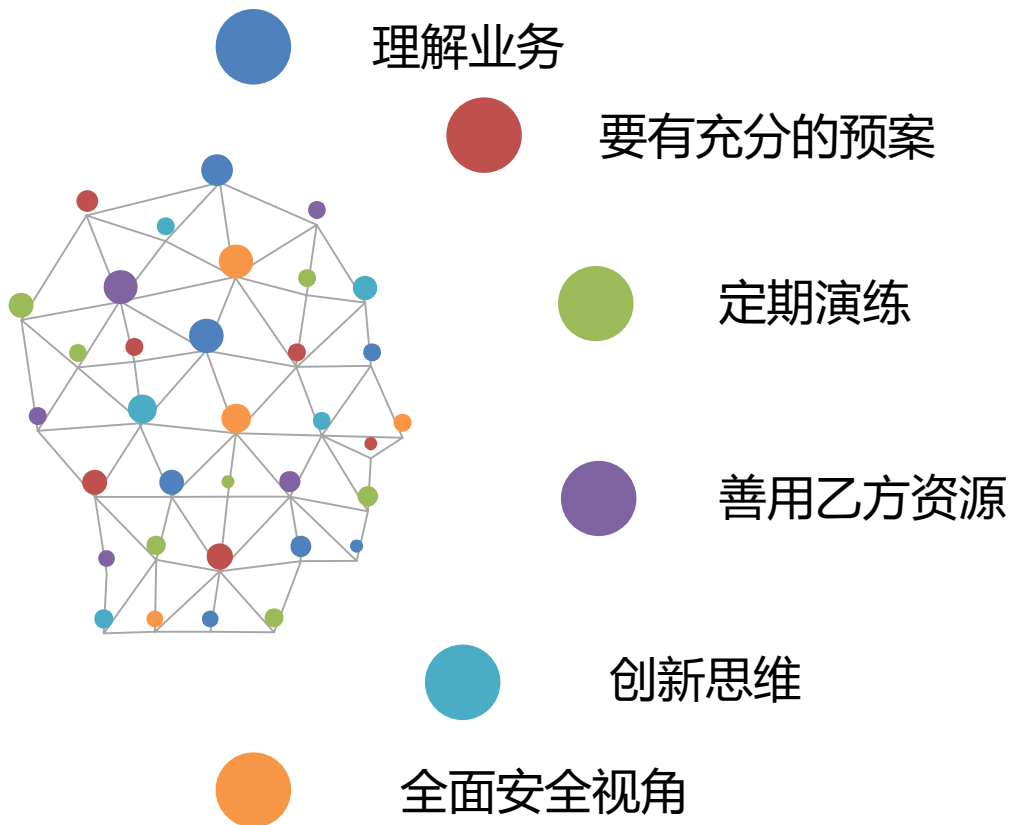


3

Par

一点感想

安全运维自动化





G*devops*

全球敏捷运维峰会



THANK YOU !