



GOPS2017
Beijing




GOPS

全球运维大会

2017



指导单位:  数据中心联盟
Data Center Alliance

主办单位:  高联运维社区
GreatOps Community

 开放运维联盟
OpenOps Alliance

大会时间: 7月26-30日

大会地点: 北京朝阳悠唐皇冠假日酒店



云时代网络边界管理实践及安全体系建设

翟耐栋 安全工程师



GOPS2017
Beijing

目录



1

安全防护理念

2

自动化运维实践



GOPS2017
Beijing

云时代网络边界管理面临的挑战

1. 业务网络庞大

- 几百个办公网VLAN
- 几十个IDC
- ...

2. 个人权限需求差异

- 运维管理员
- 业务使用人员
- ...



安全防护的理念



GOPS2017
Beijing

1. 全网访问控制统一集中管理

- 网络入口管理
- 安全域管理





2. 网络接入管控

- 终端安全管理
- 安全基线管理



GOPS2017
Beijing

3. 业务流量分析

- 全流量镜像，违规流量分析
- 威胁情报检测





GOPS2017
Beijing

目录

1 安全防护理念

➔ 2 自动化运维实践



GOPS2017
Beijing

如何高效的进行安全运营

1. ACL管理

- ACL需求多样
- ACL配置繁琐
- ACL失效管理

2. 网络管理

- 可视化管理
- 安全审计记录

高效安全



用户、应用拥有者



网络运维



安全



GOPS2017
Beijing

业务应用应用视角

业务需求
业务流
连通性
管理
用户绑定

安全可靠
易部署
变更管理
自动化

安全策略
动态细粒度
安全域
可视化
安全审核
安全审计

网络访问控制策略

访问控制矩阵



	办公网服务器区	办公网工作区	办公网测试区	IDC服务器区	Internet	...
办公网服务器区	-	X	X			
办公网工作区	http/https Ssh 定义服务	-		光纤定义服务		
办公网测试区	特定资源		-	特定服务		
IDC服务器区				-	any	
Internet				http/https		
...						

高效自动化ACL变更管理



GOPS2017

- ACL策略申请审批开通失效处理业务流
- 自动化管理，精细粒度控制，控制到人
- 实时掌控ACL开通，到期情况和使用情况

The screenshot shows a network diagram with nodes and connections, and a table of ACL rules. The table has columns for ID, Name, Action, and Status.

ID	名称	动作	状态
100	2017-07-24 14:01	允许	已生效

The screenshot shows a list of devices and their ACL configurations. The table has columns for Device Name, Version, Configuration Type, Change Time, and Effective Time.

设备名称	版本号	配置类型	变更时间	接收时间
[Redacted]	22 详情	运行	2017-07-24 10:06:46	2017-07-24 10:09:03
[Redacted]	58 详情	运行	2017-07-24 10:05:00	2017-07-24 10:08:34
[Redacted]	21 详情	点注意配置项	2017-07-24 09:38:55	2017-07-24 10:05:17
wangshen-asa	758 详情	运行	2017-07-24 09:38:26	2017-07-24 10:04:30
办公网核心交换机	990 详情	运行	2017-07-24 09:37:49	2017-07-24 10:01:15
办公网核心交换机	989 详情	运行	2017-07-24 09:37:38	2017-07-24 09:49:23
办公网核心交换机	252 详情	配置	2017-07-24 09:37:07	2017-07-24 09:41:13
办公网核心交换机	988 详情	运行	2017-07-24 09:37:07	2017-07-24 09:37:18
办公网测试网ASA	305 详情	运行	2017-07-24 09:36:27	2017-07-24 09:38:36

全网安全策略和安全边界可视化



GOPS2017
Beijing

- 三层网络设备边界可视化
- 安全域可视化
- 访问控制策略自定义定义可视化
- ACL实时分析优化
- 违规流量实时监测
- 用户和权限管理，安全审计管理，确保所有操作可追溯

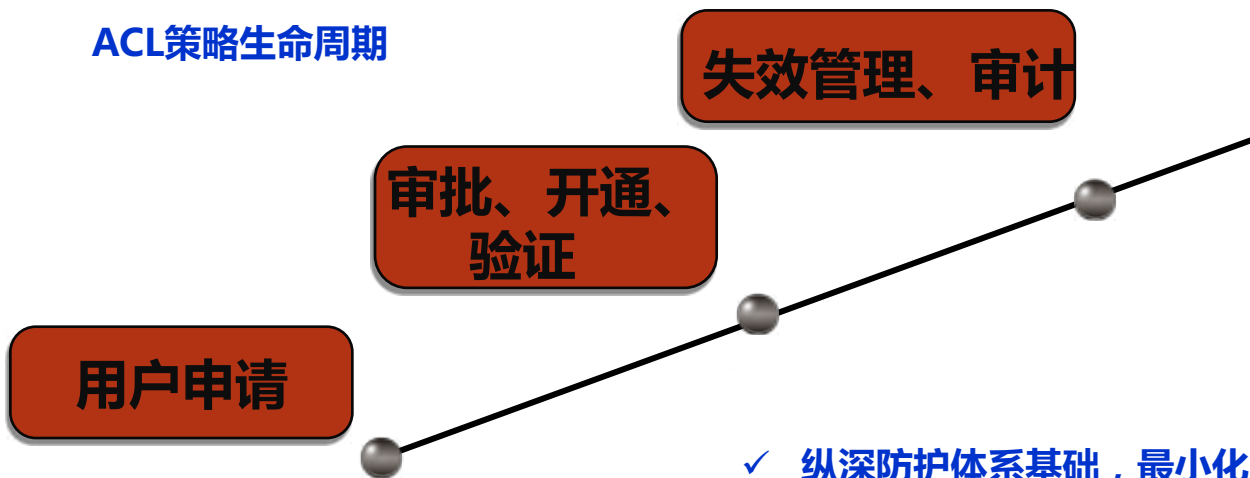


设备：办公网核心交换机 ACL规则列表

ACL名	业务网段数	源地址数	可命中规则数	命中流量	最近命中时间
sa-h (3026)	261	0	45		
haha (3025)	196	0	2		
haha (3002)	194	3	15		
kuoshengjingshafe-h (3040)	188	0	34		
weishengquan-h (3032)	171	0	16		
weishengquan-h (3021)	169	0	21		
weishengquan-h (3181)	134	0	11		
weishengquan-h (3040)	127	0	14		
weishengquan-h (3120)	107	0	18		

按需访问控制管理

ACL策略生命周期



失效管理、审计

审批、开通、
验证

用户申请



- ✓ 纵深防护体系基础，最小化网络攻击面，窄带
- ✓ 统一管理LAN和IDC网络，无需关心底层网络
- ✓ 隔离网段管理最基本策略，特殊业务、第三方服务
- ✓ 细粒度按需部署访问控制策略



GOPS2017
Beijing

网络流量采集器

数据集群

- ✓ 镜像流量
- ✓ 出口流量



- ✓ telnet
- ✓ ssh
- ✓ netconf



违规流量监测
失效ACL流量监测

撤销命令执行

管理服务器

有效期
真实访问流量
自动撤销

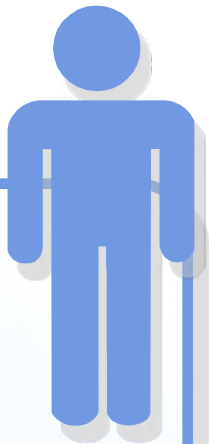


总结



访问控制

- ✓明晰网络边界
- ✓白名单方式ACL管理，默认全部deny
- ✓业务优先，自动化流程化高效
- ✓按需开通，最小权限，
- ✓ACL全生命周期管理
- ✓针对具体业务制定具体ACL策略（恶意代码分析）



安全域

- ✓VLAN划分，VLAN管理，信息可展示
- ✓统一集中管理，未用标记
- ✓云端边界开放端口与服务扫描
- ✓策略路由
- ✓针对具体业务划分隔离网段（测试、第三方）



资产划分

需要有明确的资产分类；
区分业务的核心资产



安全审计
定期的安全审计



exp



安全域

需要有明确的安全域的划分

基于人的管理

只有基于人这唯一标示，
才能实现灵活的终端管
控





高效运维社区
GreatOPS Community



GOPS2017
Beijing

会议

- 8月18日 DevOpsDays 上海
- 全年 DevOps China 巡回沙龙
- 11月17日 DevOps金融上海

培训

- EXIN DevOps Master 认证培训
- DevOps 企业内训
- DevOps 公开课
- 互联网运维培训

咨询

- 企业DevOps 实践咨询
- 企业运维咨询



商务经理：刘静女士
电话 / 微信：13021082989
邮箱：liujing@greatops.com



GOPS2017
Beijing

谢谢!