大数据运维安全

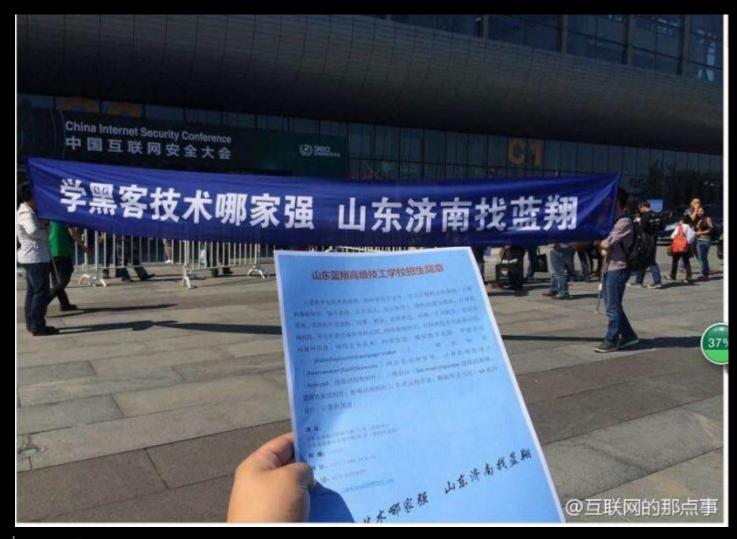
演讲人: 李洪亮

职务: Qihoo 360 NETOPS Manager

日期:9/14/2014











大数据运维安全



-网络架构的安全设计

-大数据下的安全运维实践

-IDC的物理安全

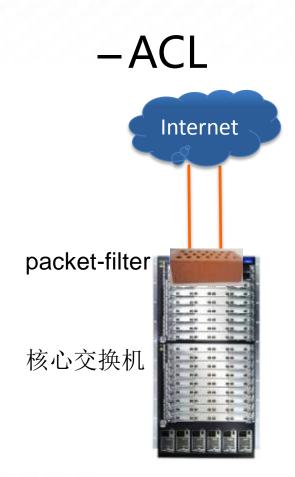


-ACL

-业务之间的隔离

-DDoS攻击的防护





ACL规则申请平台



ACL规则的自动生成与push

ACL规则的失效与老化?



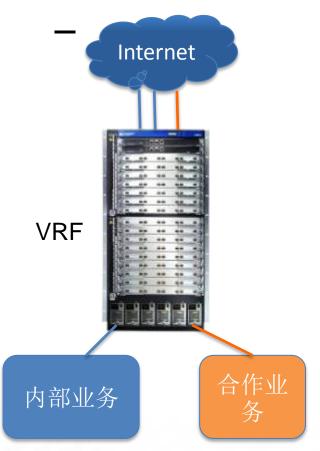
-ACL

-业务之间的隔离

-DDoS攻击的防护



- 业务之间的安全隔离



Vlan方式隔离,会增加ACL复杂度

VRF或vPC(cisco)能提供更加简便的隔离方案

在不具备VRF的环境,建议通过策略路由方式将流量抛出



-ACL

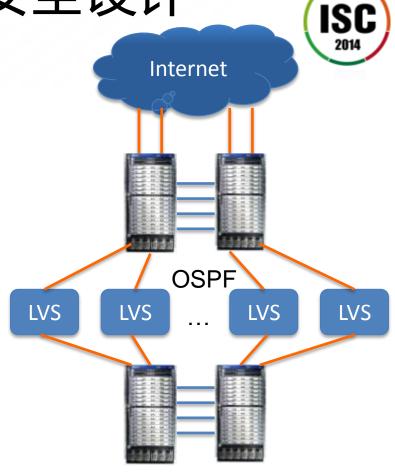
- 业务之间的隔离

-DDoS攻击的防护

-DDoS攻击的防护

LVS的fullNAT模式,具备良好的扩展性

LVS提供block ip接口,对攻击ip进行屏蔽













广告时间



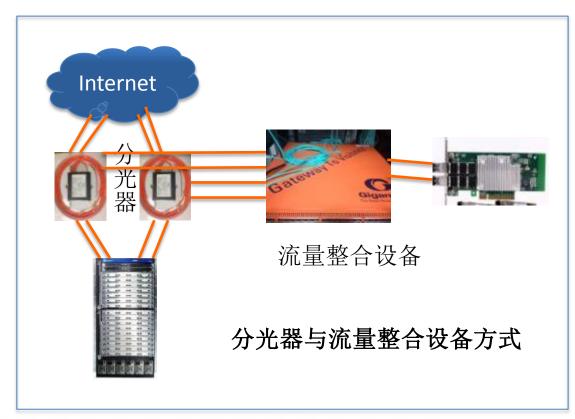
-ACL

-业务之间的隔离

-DDoS攻击的防护









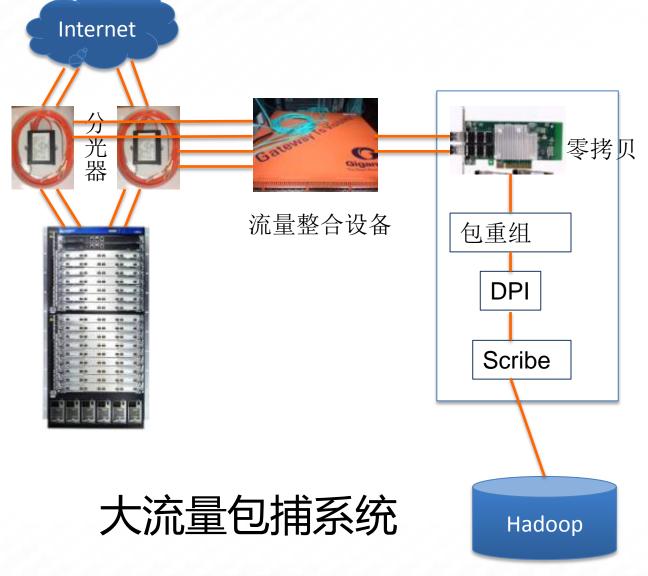
-大流量包捕系统

-分布式存储与并行计算系统

- 机器学习与规则提取系统

_





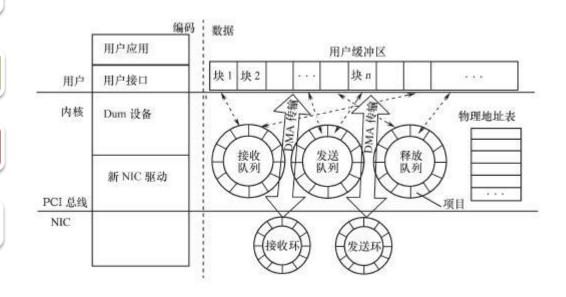


避免数据拷贝

按CPU数分配队列

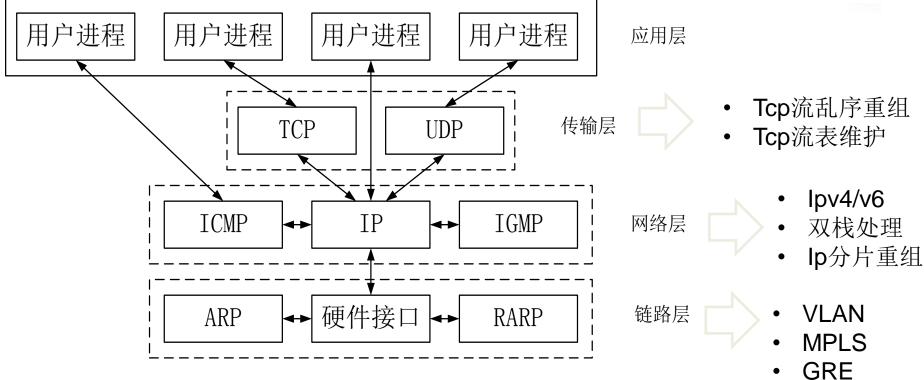
将多种操作结合

直接IO



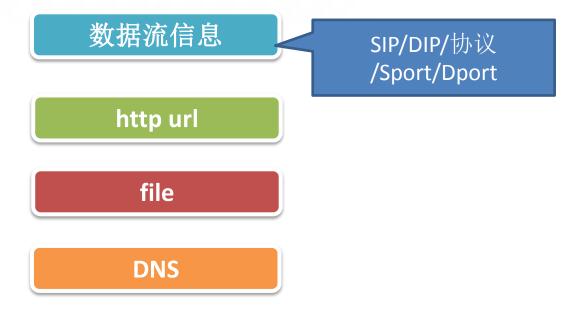
大流量包捕系统—零拷贝





大流量包捕系统—数据包重组





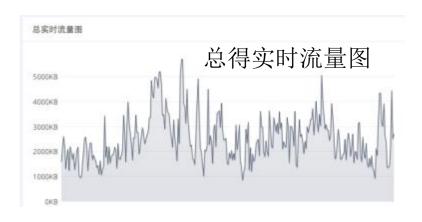
大流量包捕系统—DPI



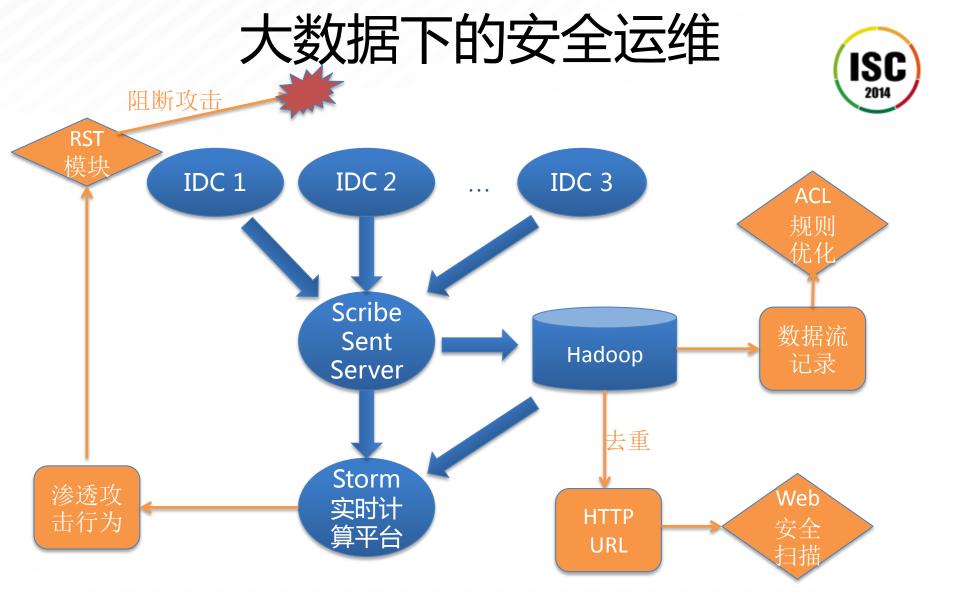




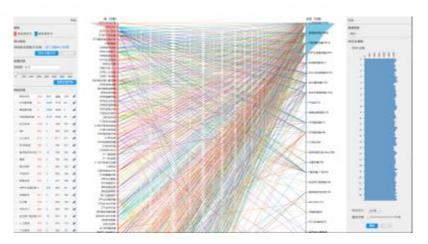




大流量包捕系统——功能展示









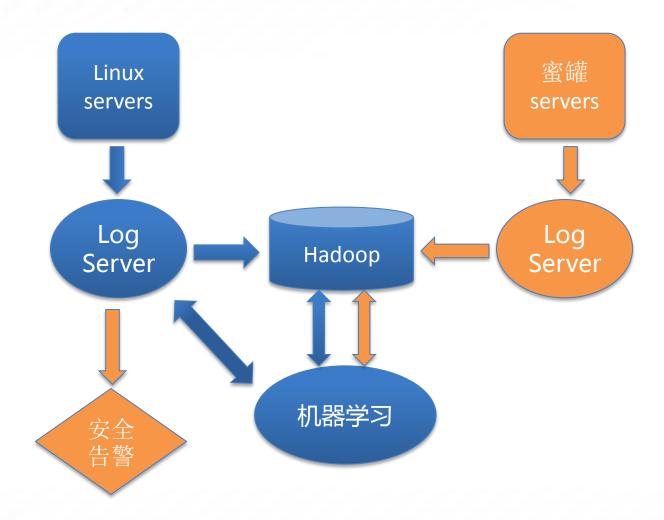
覆盖10个数据中心

每天60T的存储量

耳	> Webscan	> A							
0	3001001		LI O		WEIST IN LAND	CALLA SELFANISCE MEMORIAL	71,73 TO, AUTH, U JAIR.	7177 10, 2019, 1.01 8.11.	Ħ
	3087001	https	1101	notice	500 Internal Server Error(POST)	该真面发生了内部错误(POST)	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:58 a.m.	未处 理
	3087001	https	1101	notice	500 Internal Server Error(POST)	该页面发生了内部错误(POST)	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:58 a.m.	未处 理
	3086996	http:	080	notice	Possible Sensitive File	可能是敏感文件	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:55 a.m.	2.0
	3086996	http:	080	notice	Possible Sensitive File	可能是敏感文件	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:55 a.m.	5.0
	3086996	https	080	notice	500 Internal Server Error(POST)	该真面发生了内部错误(POST)	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:56 a.m.	5.0
	3086996	https	080	χź	十辛龄	茶取的	九月 18, 2014, 9 p.ハ	単 クー 7:55 a.m.	忽略
	3086989	https	0					7LH 19, 2014, 7:11 a.m.	未提 理
	3086989	http:	o	no a	ep女	全扫描	九月 18, 2014, 9 p.m.	九月 19, 2014, 7:11 a.m.	調拍

大数据日志统计展现







蜜罐获取黑客特征

主机安全日志的展现

Shell训练数据标定

chmod 777 ajax.php -Rf

总共 93

.* which.*

.*exp.*

.*wtmp.*

.*secure[\W].*

.*echo.*php.*

."HACK."

."www.exploit-db.com."

cp fengerbolmd5infos.zip search/

B.ft 150070 1 2 3 4 ... 1500 1501

/home/s/var/proc/ -x 2011041622 > /dev/null &

python feedback-7.py 1000 10000 user_trust.levels3

php load_data.php /home/xiemingqiang/level-dist-md5.txt

 sudo -u cloud nohup (homels/appsiCloudSafeLine/cloudMID)parserimid_parser -f. (homels/appsistatdata/midlog/ 4 /homels/appsiCloudSafeLine/cloudMiD(parsericonfl/qlog.ini -S.db76.safe.ffc.qihoo.net.4730,db78.safe.ffc.qihoo.net.4733 -D

主机智能告警的人工训练

User

Rank

13

11

12

12

12

11

11

11

IDC的物理安全



监测中心

- 机房的温湿度监控与报警







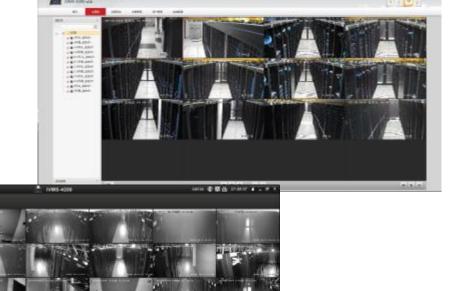
IDC的物理安全



重要机房的视频监控

本地存储/异地备份

动态内容保存







谢谢