探索软件定义的新型防护体系

绿盟科技
刘文懋 资深研究员 博士

密级：公开使用

Agenda

1 新型网络的安全防护体系

2 软件定义的安全防护实践

3 学术成果

Network management is pain

Distributed Network Management

CLI , Serial

WEB portal

Unmatch

Distributed Compute& Storage Management

Perl, Expect

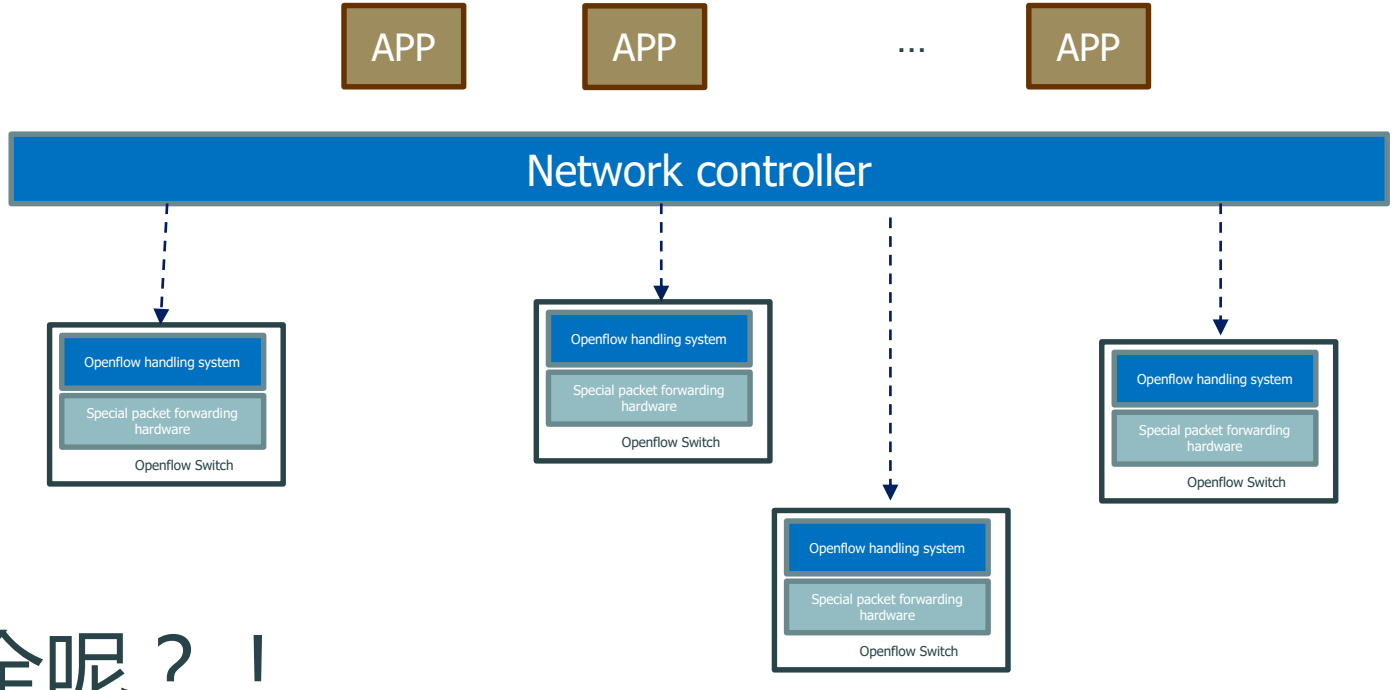
Puppet

Hadoop,

Storm…

软件定义计算、存储、网络 vs 安全

- SDN是未来网络的希望之路

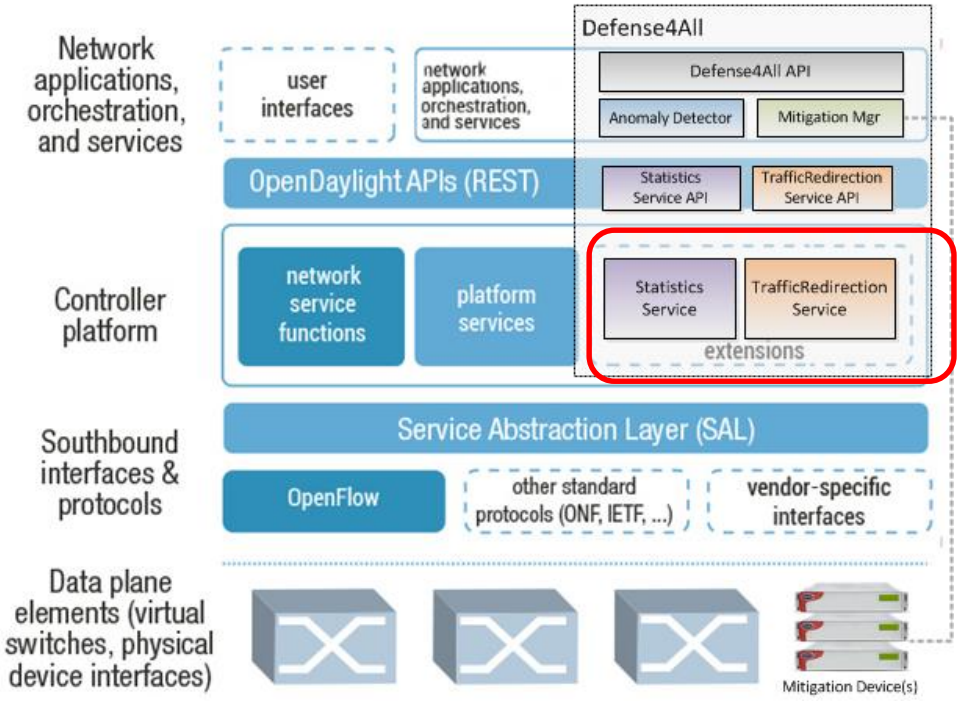


- 安全呢？！
  - 能否在SDN网络中部署现有的安全产品？
  - 能否使用软件定义的理念重构我们的安全解决方案？

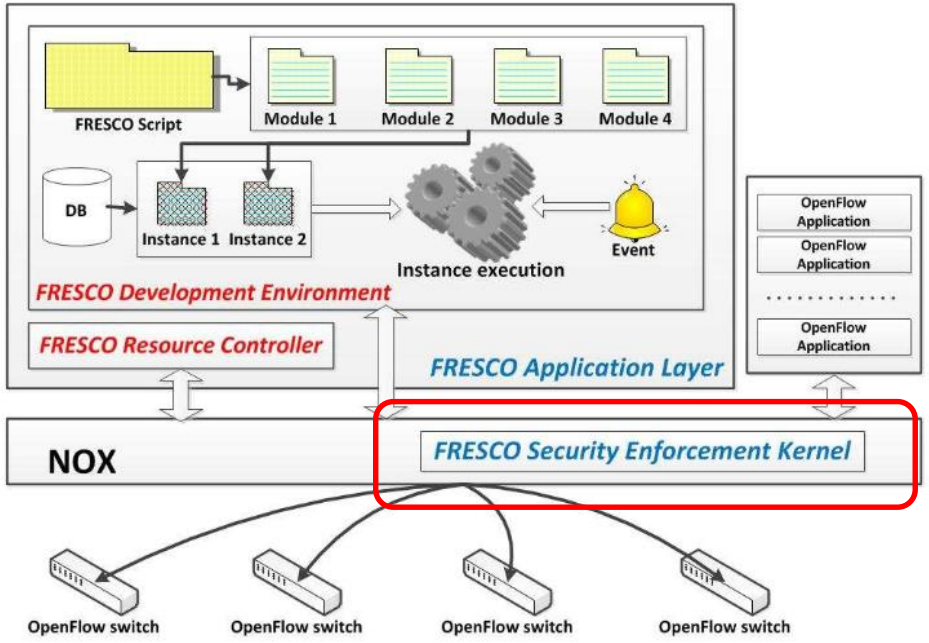
SDN安全的相关工作

- Flow-level security
  - Lightweight DDoS flooding attack detection using NOX/OpenFlow [2]
  - Source address validation solution with OpenFlow/NOX architecture [3]
- Packet-level security
  - FleXam, a flexible sampling OpenFlow extension [4]
- Architecture
  - FRESCO[1]
  - Defense4All in Opendaylight, radware
  - …

当前SDN安全架构案例

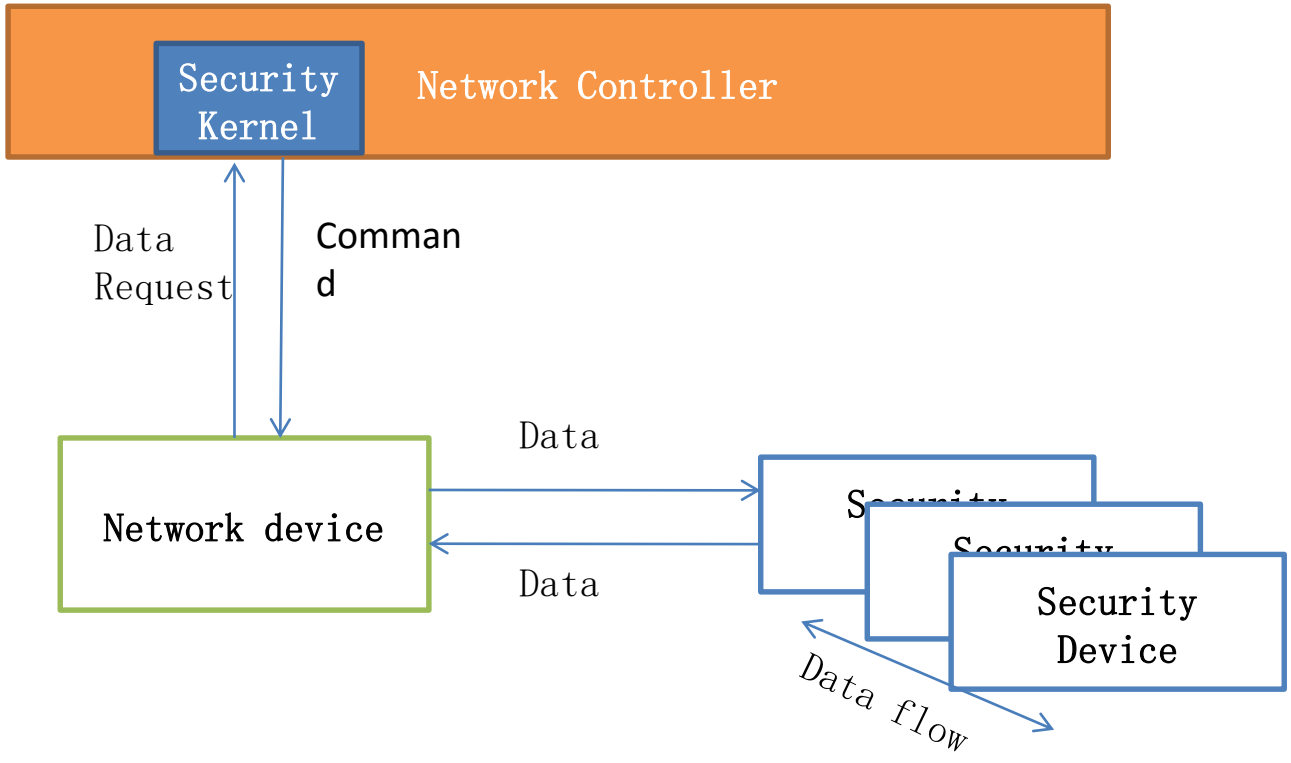


Defense4All

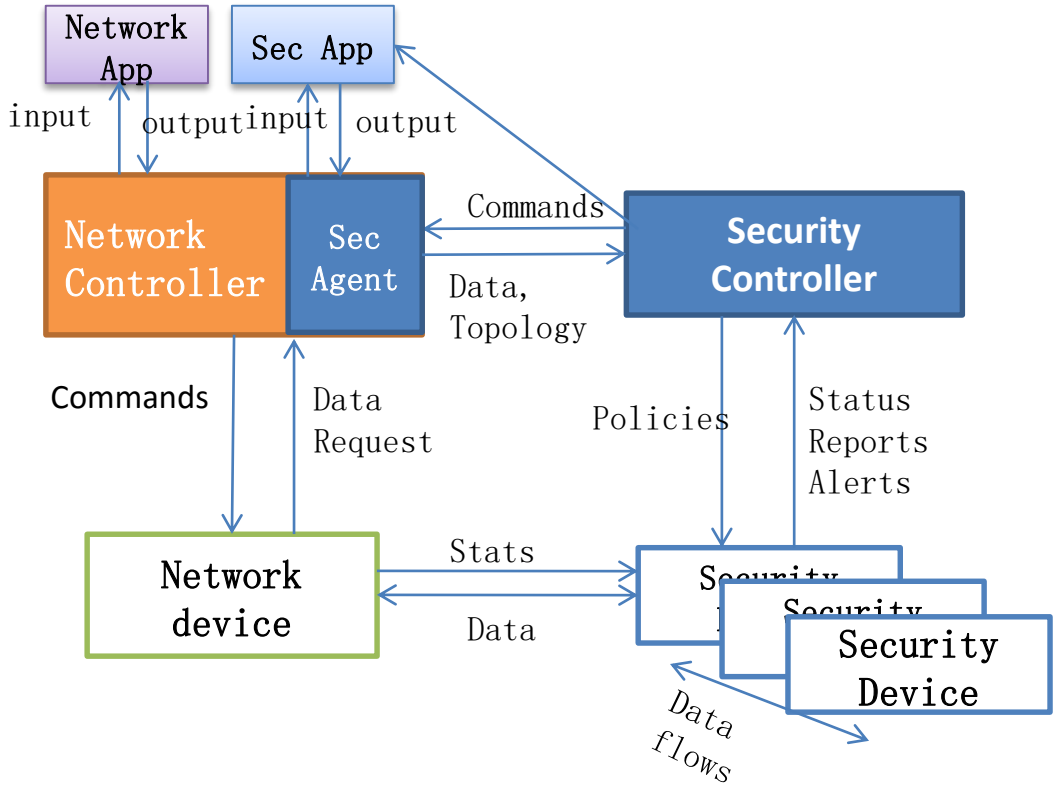


Fresco

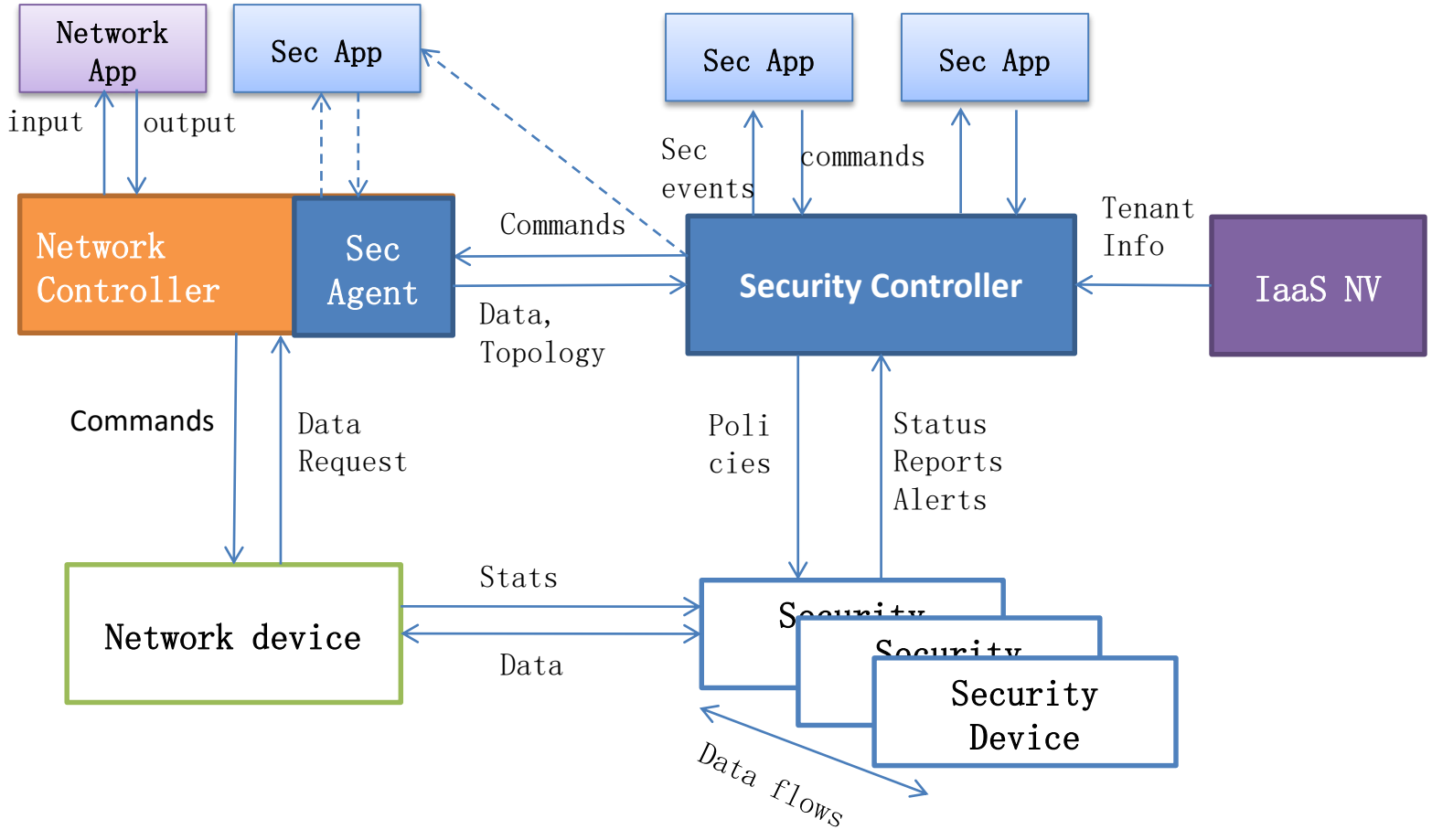
形式化的当前SDN安全架构



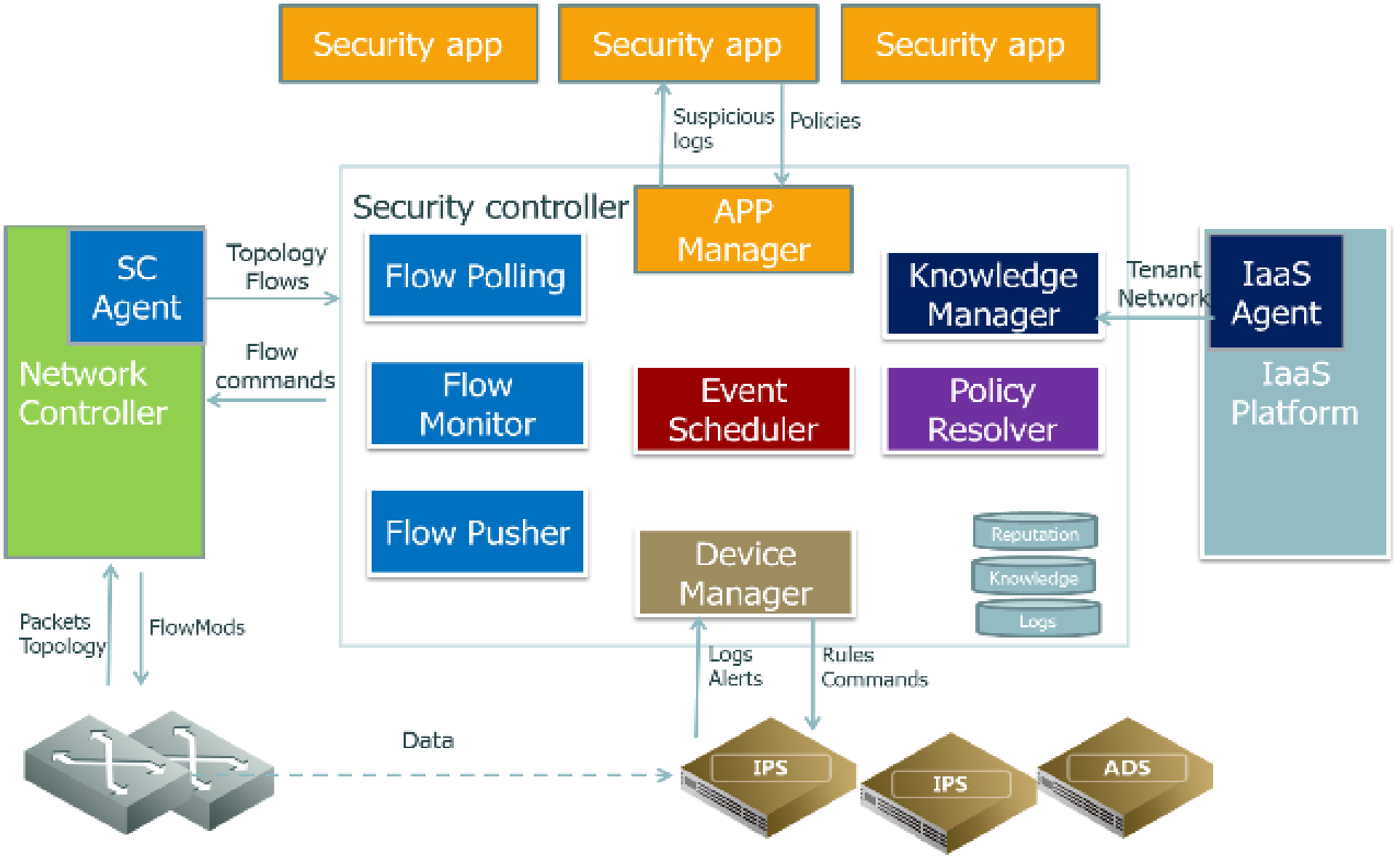
The SDSA Architecture I



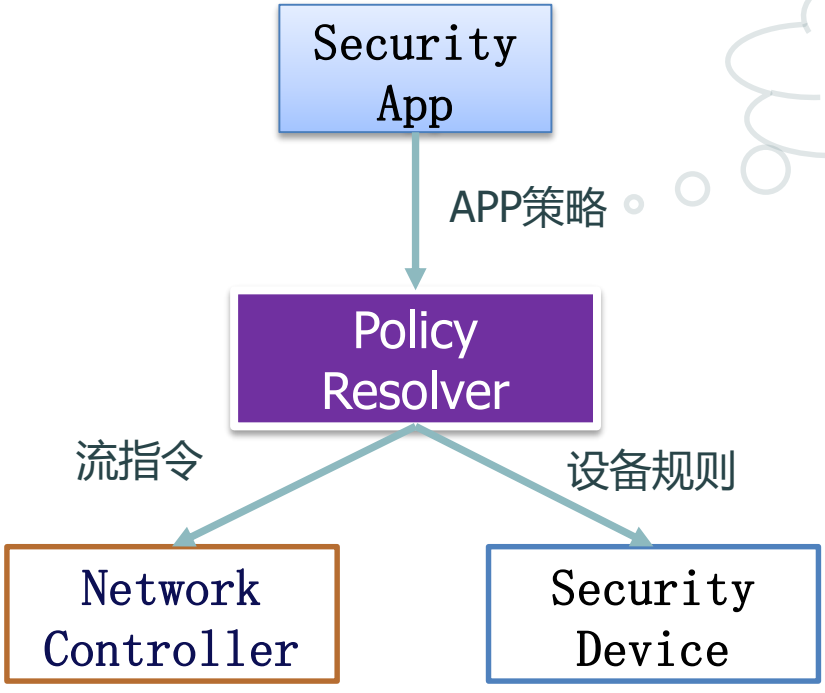
The SDSA Architecture II

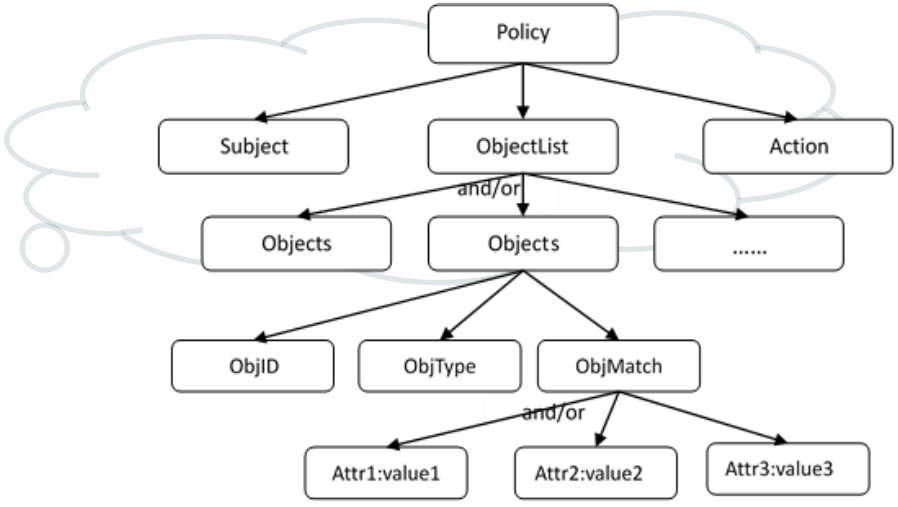


The SDSA controller



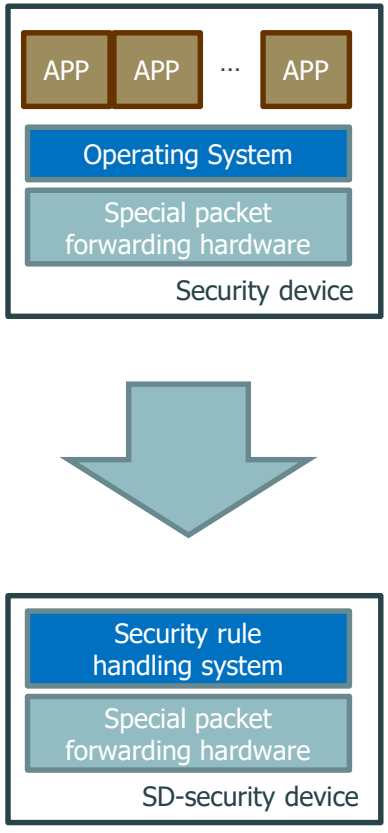
策略解析

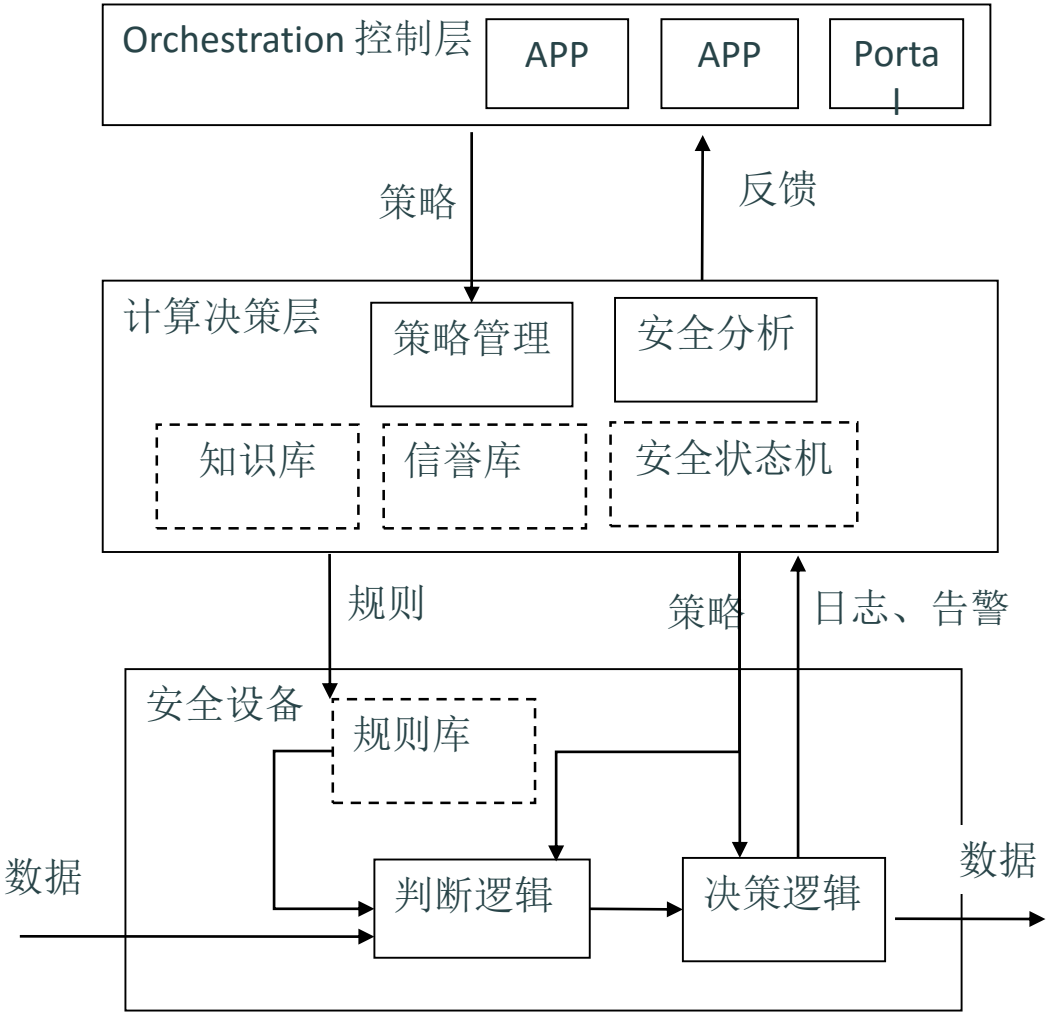




- **Subject** is the policy executor: a SC module, a security device, or the network controller
- **Action** is a verb denoting how to deal with objects: {BLOCK, CLEAN, LOG…}
- **Objects** a collection of tenants, VMs or networks flows. Each has a unique identifier *ObjID*, its type ObjType, and a compound matching expression ObjMatch.

重构安全设备


APP
APP
…
APP
Operating System
Special packet forwarding hardware
Security device
Security rule handling system
Special packet forwarding hardware
SD-security device


Orchestration 控制层
APP
APP
Porta
策略
反馈
计算决策层
策略管理
安全分析
知识库
信誉库
安全状态机
规则
策略
日志、告警
安全设备
规则库
数据
判断逻辑
决策逻辑
数据

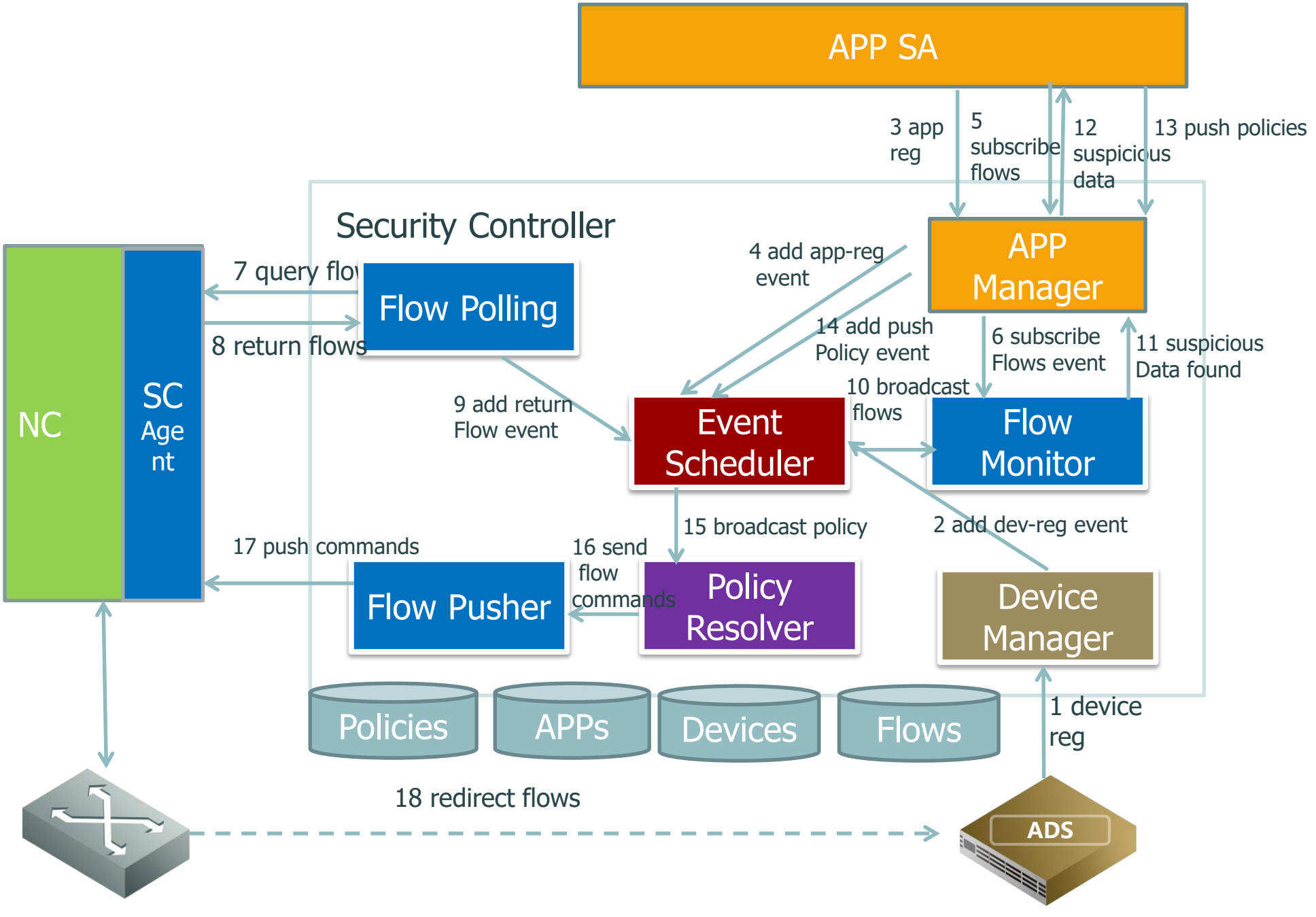
Agenda

1 新型网络的安全防护体系

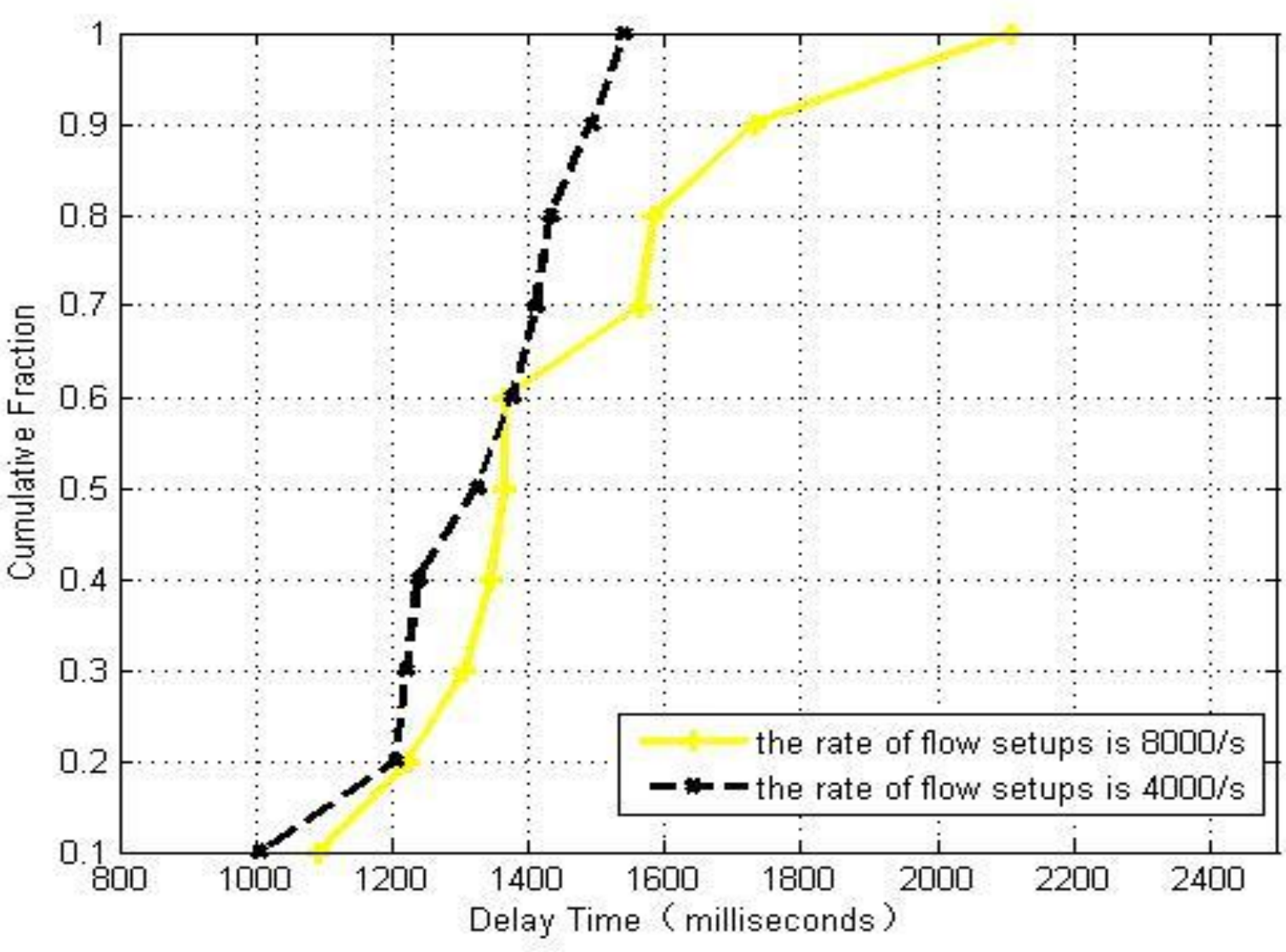
2 软件定义的安全防护实践

3 学术成果

软件定义的DDoS防护

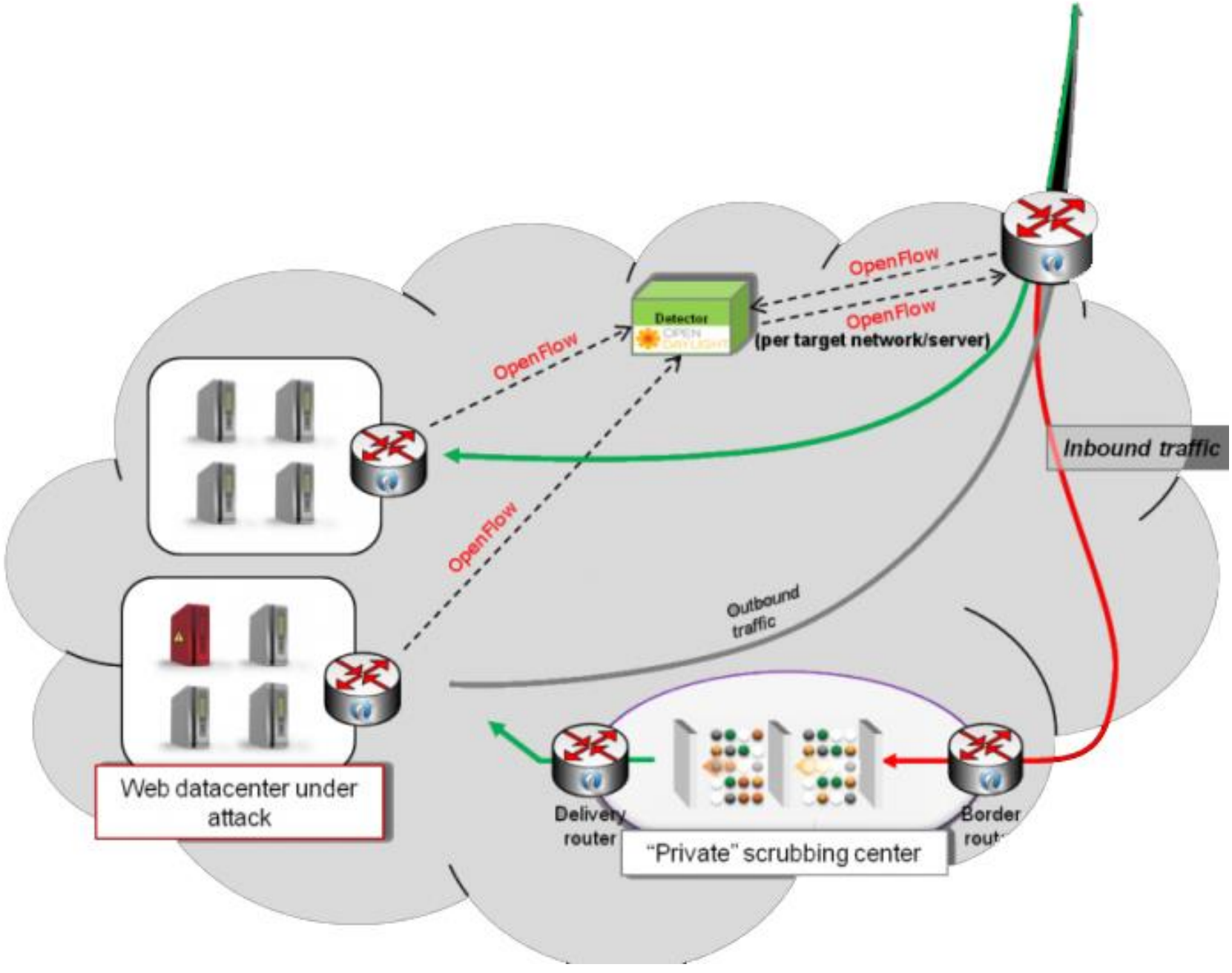


实验结果



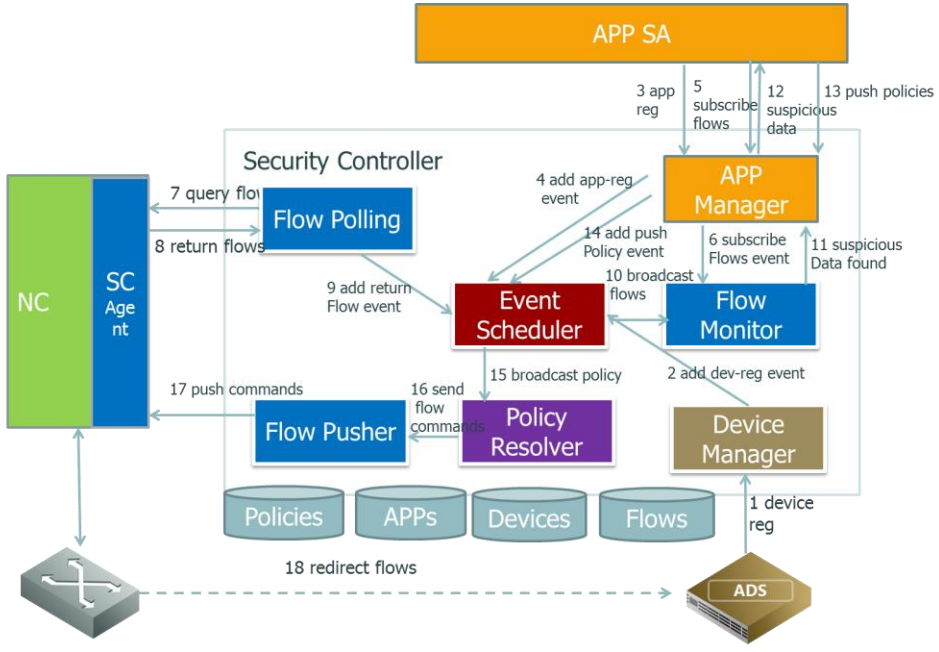
- 4000 flows/s ， 90% detected within 1.5s

Related works : Defense4ALL



Related works：Defense4ALL

- ONS 2014 IDOL :Real-time SDN Analytics for DDoS mitigation - Broadcade
- 绿盟-NTA设备docker化后的软件定义抗DDoS防护



绿盟软件定义的DDoS检测原型架构

绿盟云监护抗拒绝服务系统凭借优质DDoS清洗服务产品获得美国知名杂志《信息安全产品指南》金奖

Case: 端口扫描

Table1 Normal port scan

Scan type	Live ports	Unestablished rate	I
TCP scan	735	98.28%	4.573
TCP SYN scan	970	98.22%	6.023
Normal	3	19.15%	0.026

Table2 Slow port scan

Scan type	Live ports	Unestablished rate	I
Slow syn scan	208	11.16%	1.384
Normal	3	1.6%	0.02

$$I = \frac{x\sum U_i}{nR} + \frac{(1-x)\sum A_i}{nC}$$

Table3 Detection overhead

Scan overhead (μs/pkt)	TCP SYN scan	TCP scan	Slow scan
Flow monitor	0.1356	0.1620	0.0013
Snort plugin	2.00	2.02	2.34

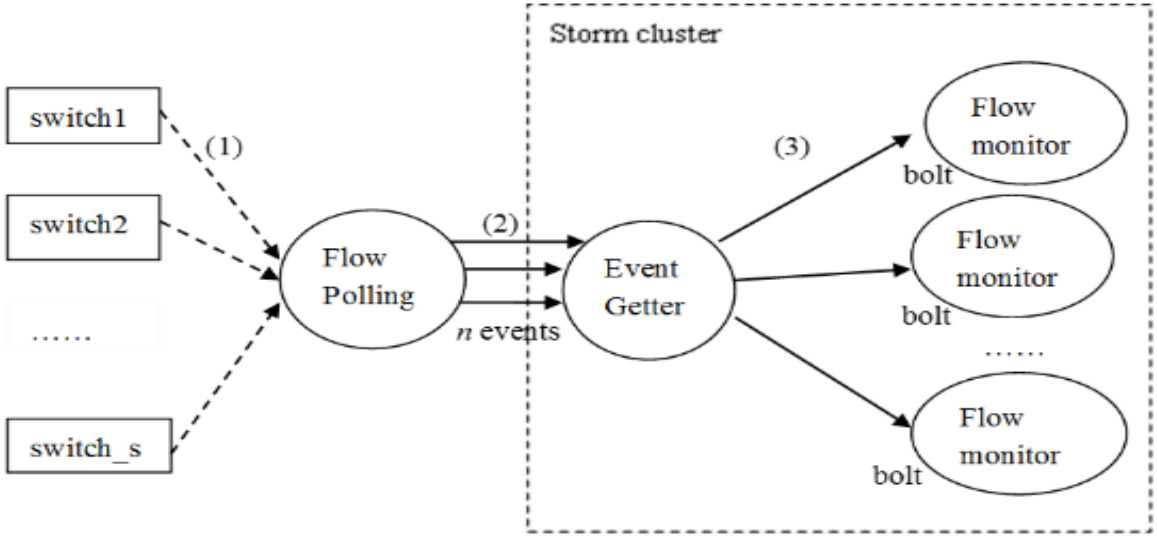


Figure 6: Distributed flow processing.

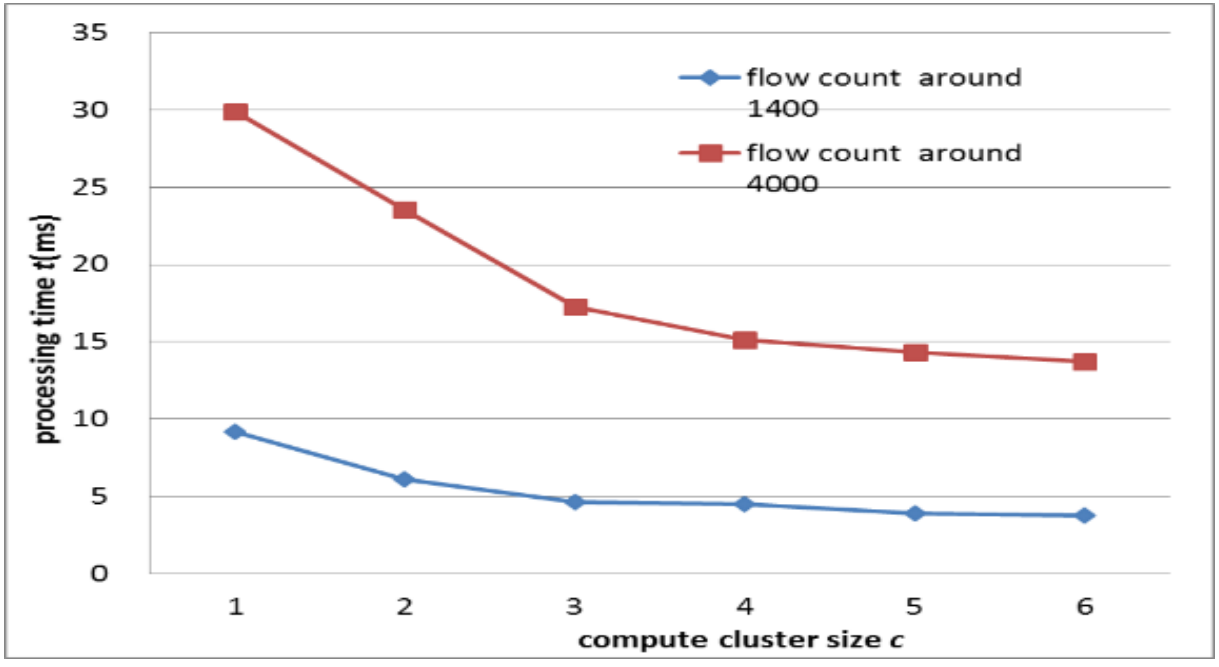
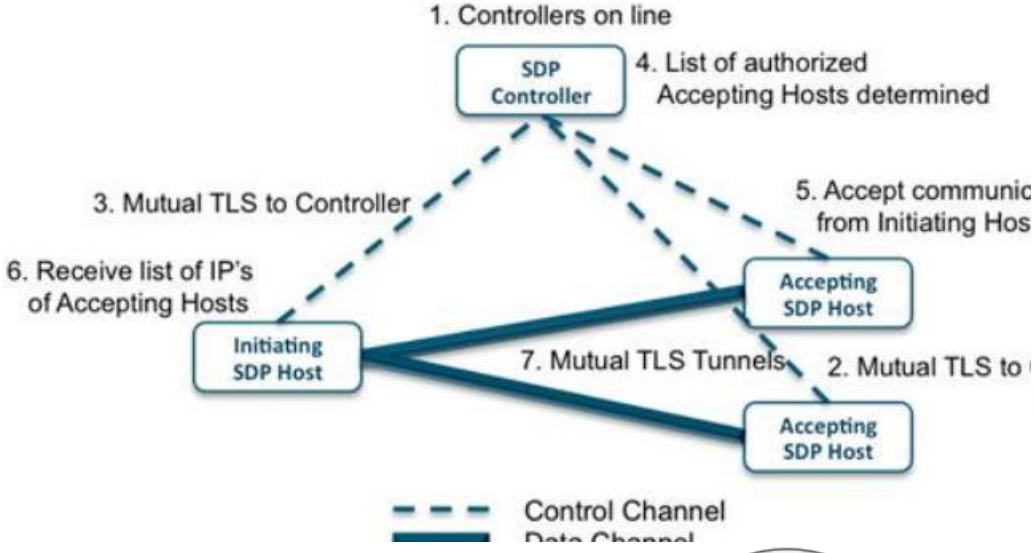


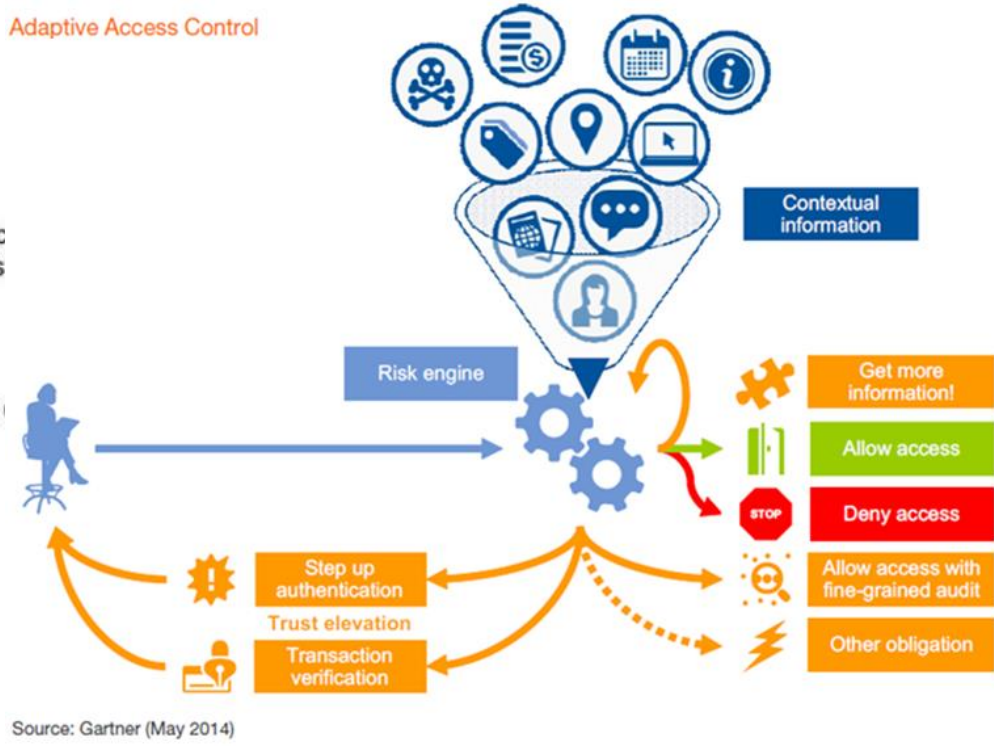
Figure 7: Cluster time consuming comparison.

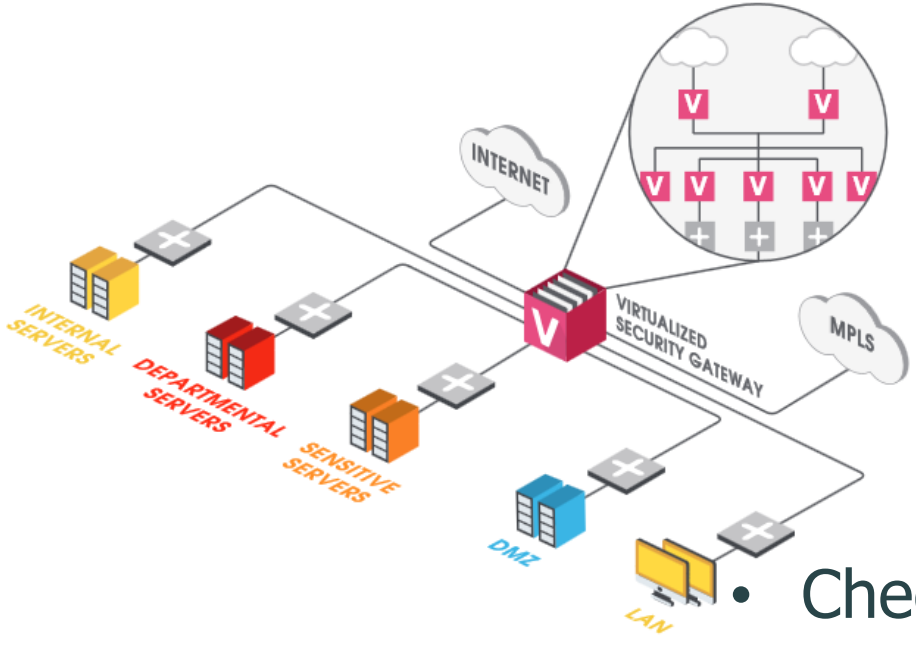
Access control in SDN

- CSA:SDP(Perimeter)



- Garnter: Adaptive Access Control





- Checkpoint：SDP(Protection)

Case: Software defined access control in BYOD

10.201.10.222

Internet

NSFOCUS Intranet

外部网关

10.201.0.1

软件定义的边界

内部网关

192.168.19.1

br-ex

br-int

br-tun

NF

WAF

ADS

CONTROLLER

SDN交换机

30.0.0.30

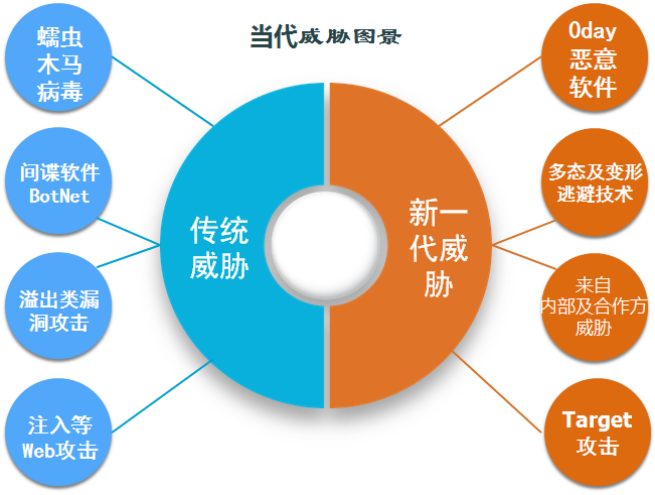
30.0.0.1

GRE Tunnel

传统交换机

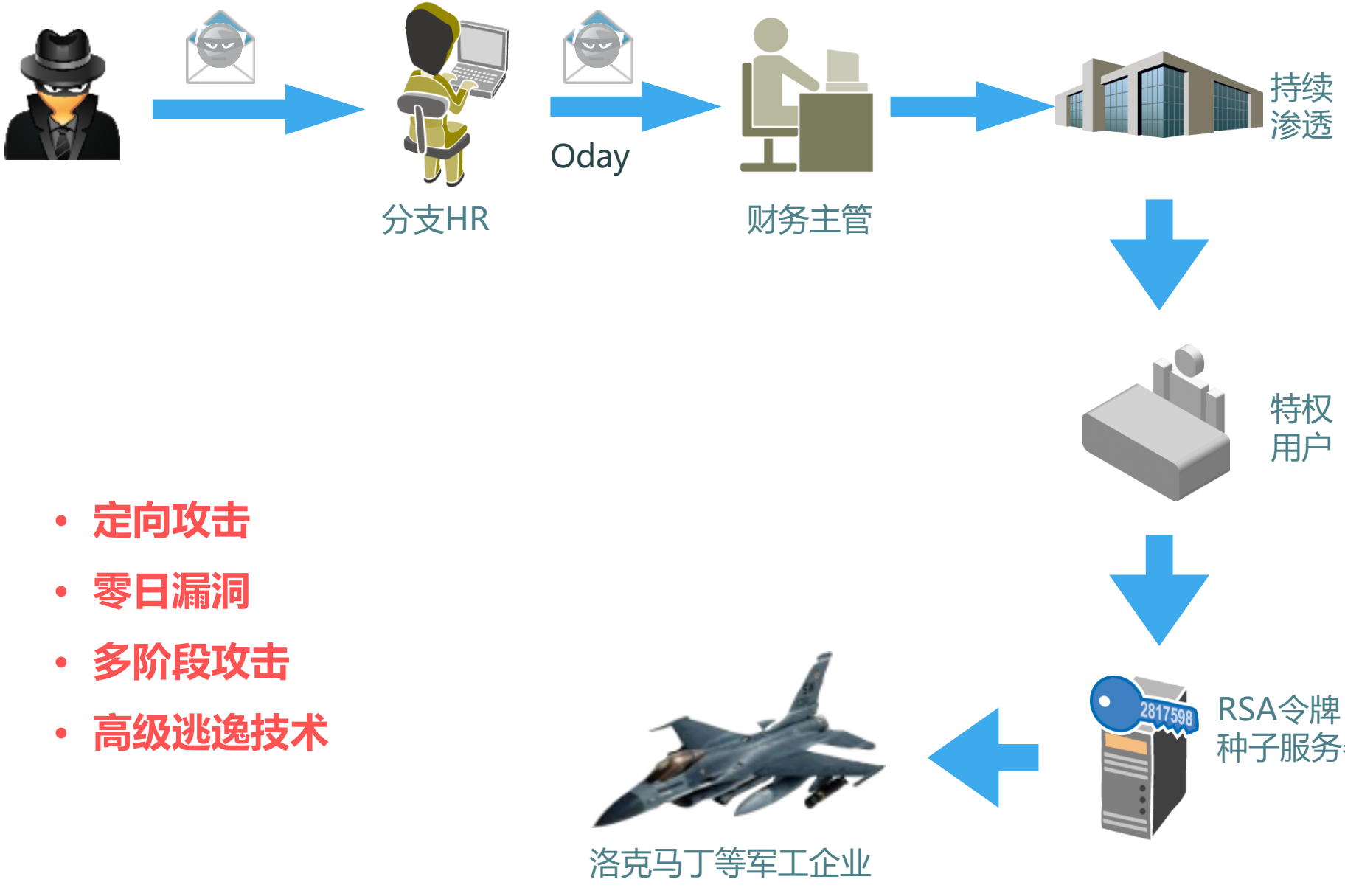
10.201.10.223

“下一代威胁”来势汹汹


当代威胁图景
蠕虫
木马
病毒
间谍软件
BotNet
溢出类漏
洞攻击
注入等
Web攻击
传统
威胁
新一
代威
胁
0day
恶意
软件
多态及变形
逃避技术
来自
内部及合作方
威胁
Target
攻击

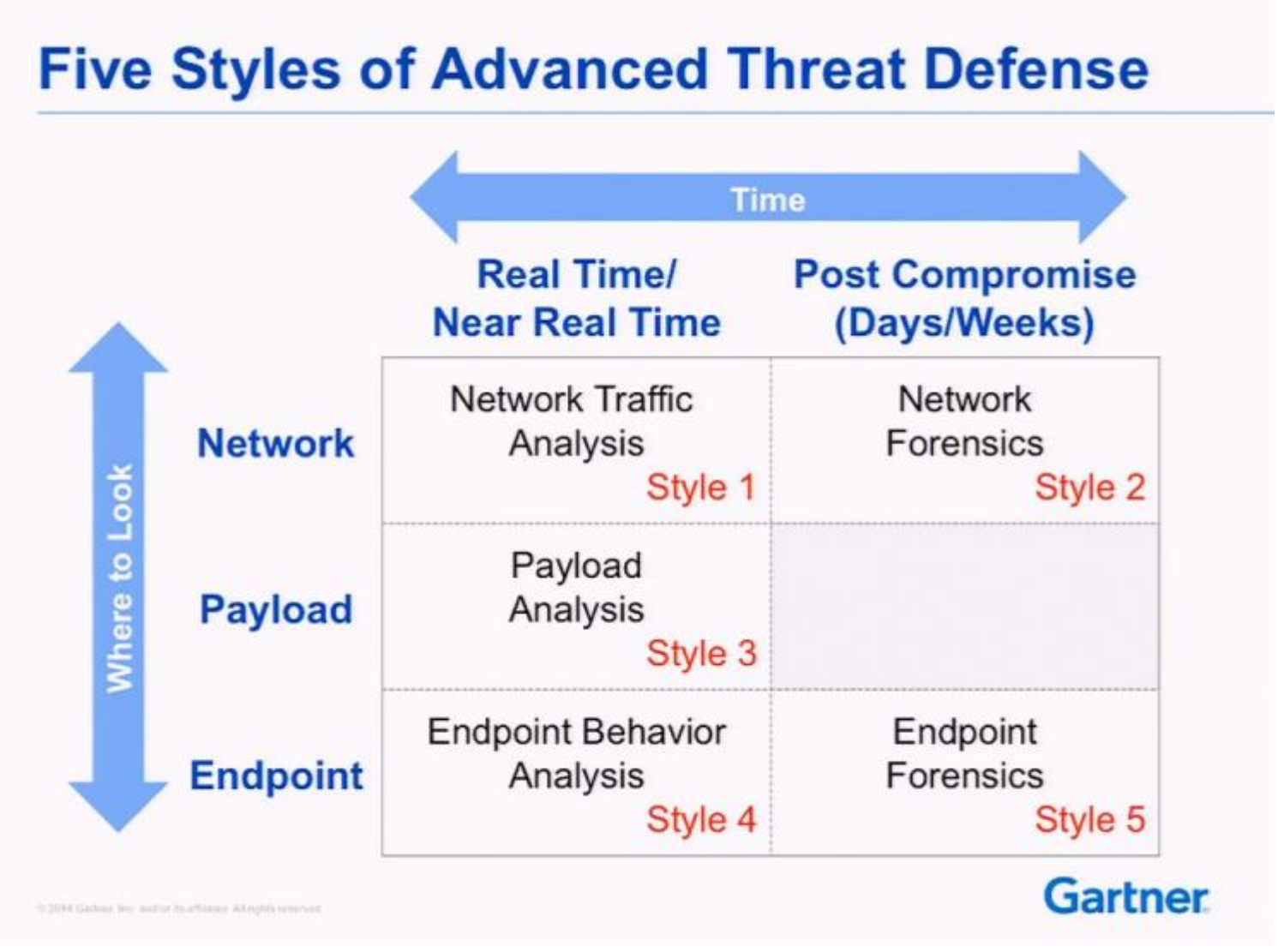
零日
攻击
骇客发现漏洞后，往往不再公布，而是长时间利用进行漏洞攻击
多态及变形
恶意软件
1、造成恶意软件样本的快速膨胀，McAfee及Sysmantec的样本库数量过亿
2、同时这种恶意软件可能很难提取特征码
社交网络
及混合攻击
1、利用社交网站或邮件系统，进行钓鱼攻击.
2、往往多种传播方式：邮件、网络、USB等
APT
攻击
利用以上手段，攻击个人得手后，长期在其网络潜伏，窃取重要信息
传统威胁
蠕虫
木马
病毒
间谍软件
Botnet
溢出类
漏洞攻击
注入等
Web攻击

RSA SecruID攻击



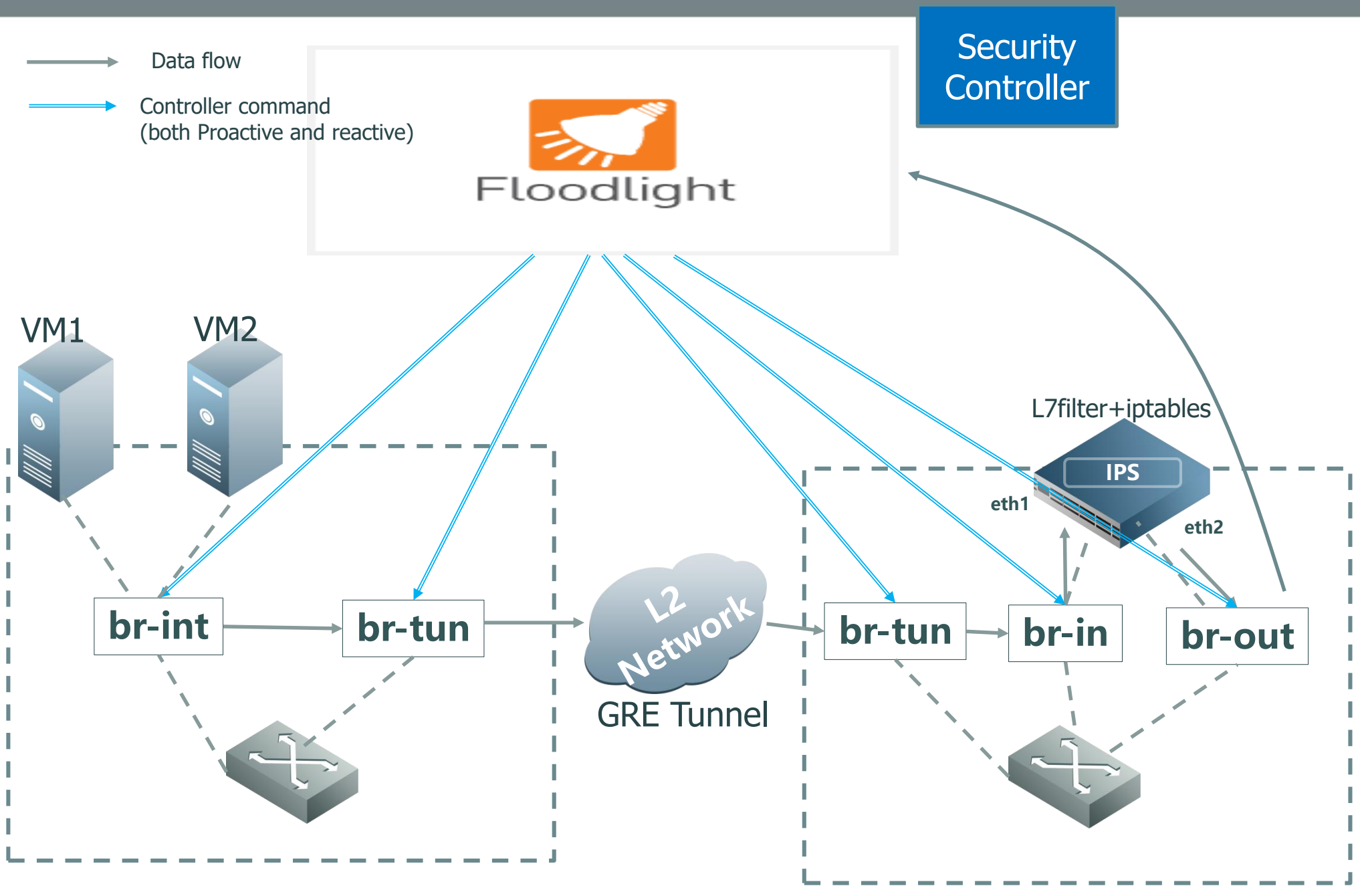
- **定向攻击**
- **零日漏洞**
- **多阶段攻击**
- **高级逃逸技术**

Anti-APT(Advanced persistent threat)

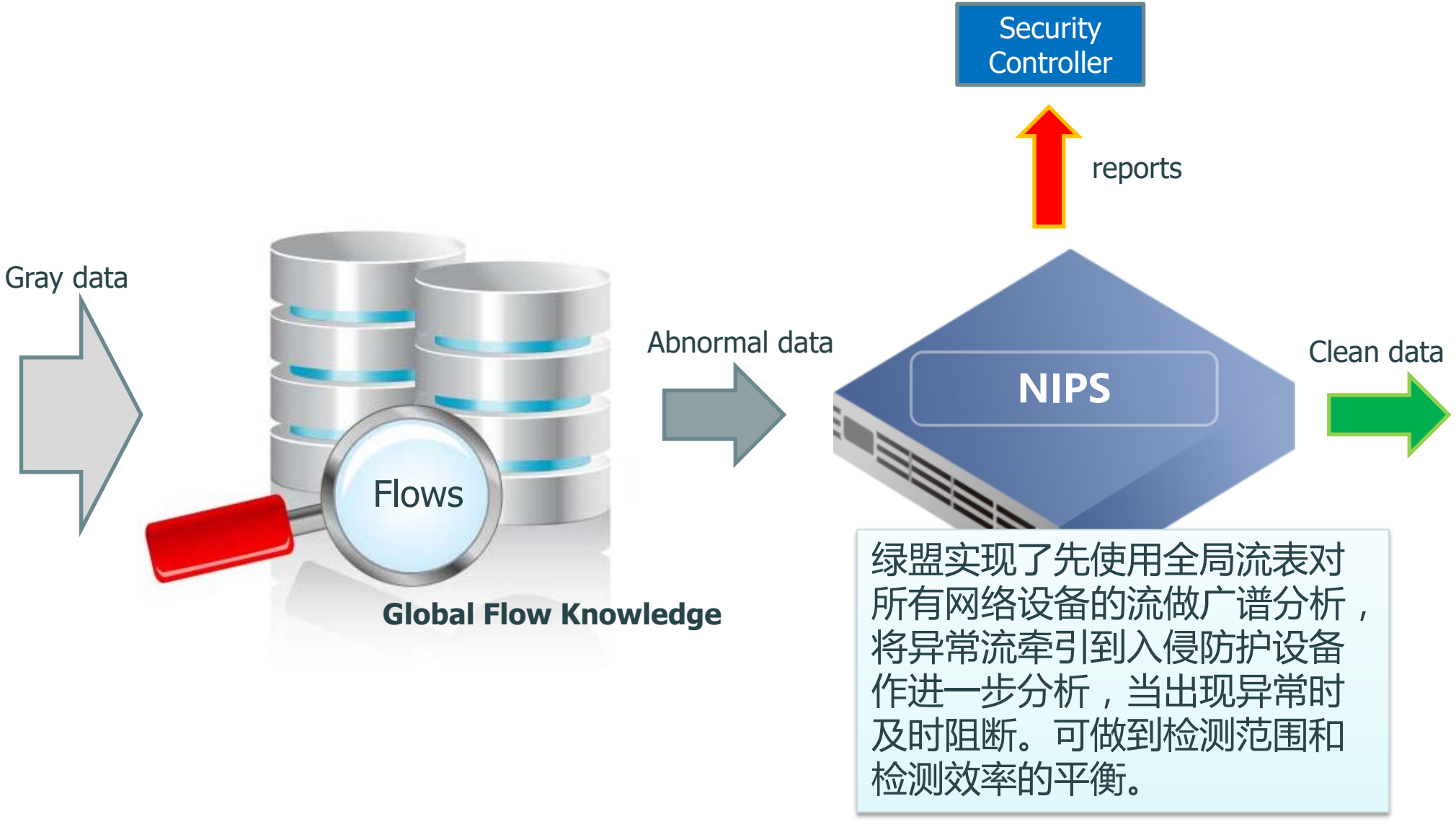


- To the point: the five style of advanced threat defense, Lawrence Orans, Gartner

IPS示例


Data flow
Controller command
(both Proactive and reactive)
Security Controller
Floodlight
VM1
VM2
L7filter+iptables
IPS
eth1
eth2
br-int
br-tun
L2 Network
GRE Tunnel
br-tun
br-in
br-out

Video Demo：流+数据包层协同防护



绿盟实现了先使用全局流表对所有网络设备的流做广谱分析，将异常流牵引到入侵防护设备作进一步分析，当出现异常时及时阻断。可做到检测范围和检测效率的平衡。

服务链简介I

Rack交换机

计算节点

IPS

ADS

WAF

输入网卡

vswitch

输出网卡

hypervisor

Openflow指令

SDN控制器

安全控制平台

计算节点

VM1

VM2

VM3

vswitch

网卡

hypervisor

云计算控制节点

Rack交换机

计算节点

IPS
ADS
WAF
vswitch
输入网卡
输出网卡
hypervisor

计算节点

VM1
VM2
VM3
vswitch
网卡
hypervisor

Openflow指令

SDN控制器

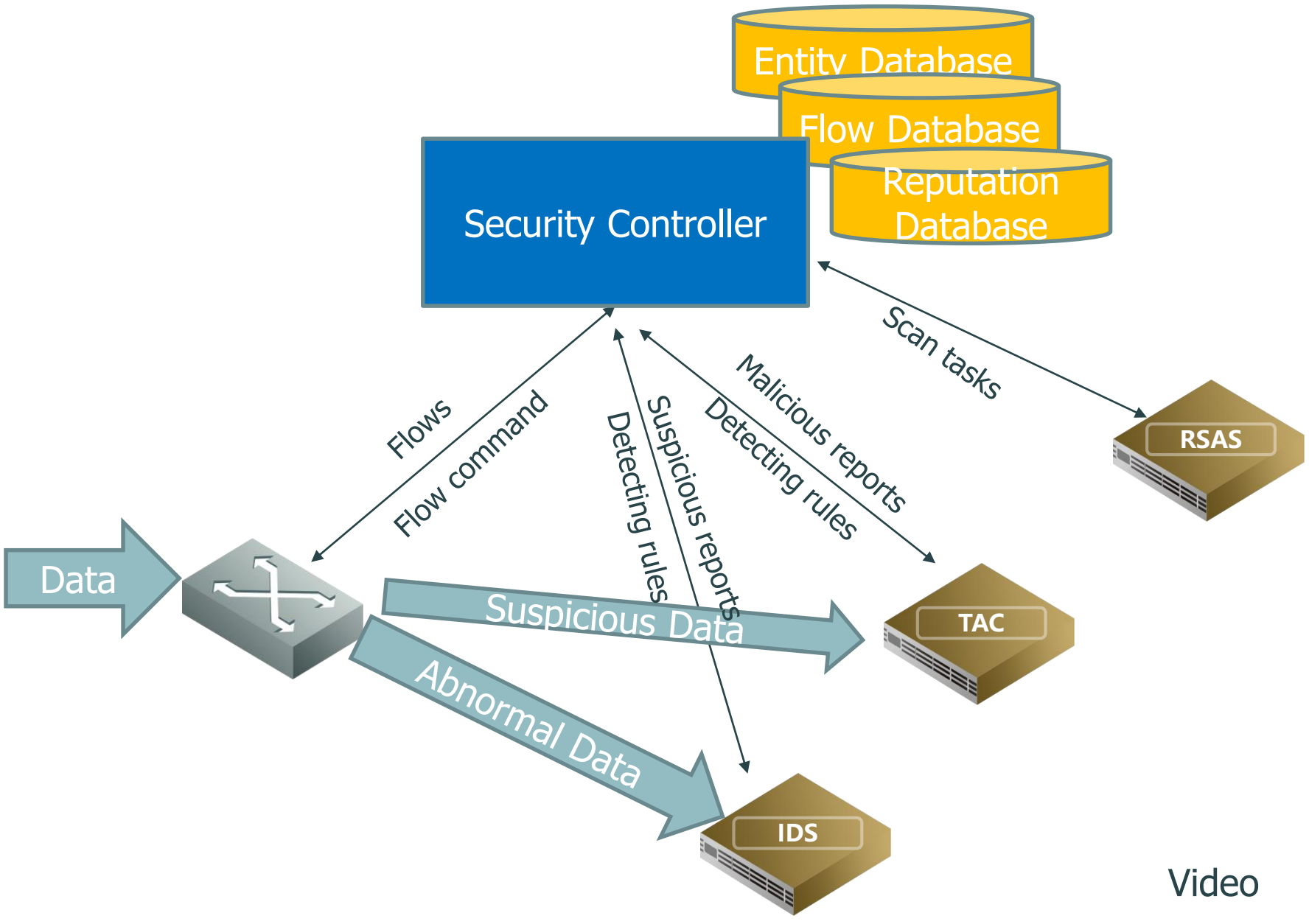
流量调度指令

安全控制平台

云计算控制节点

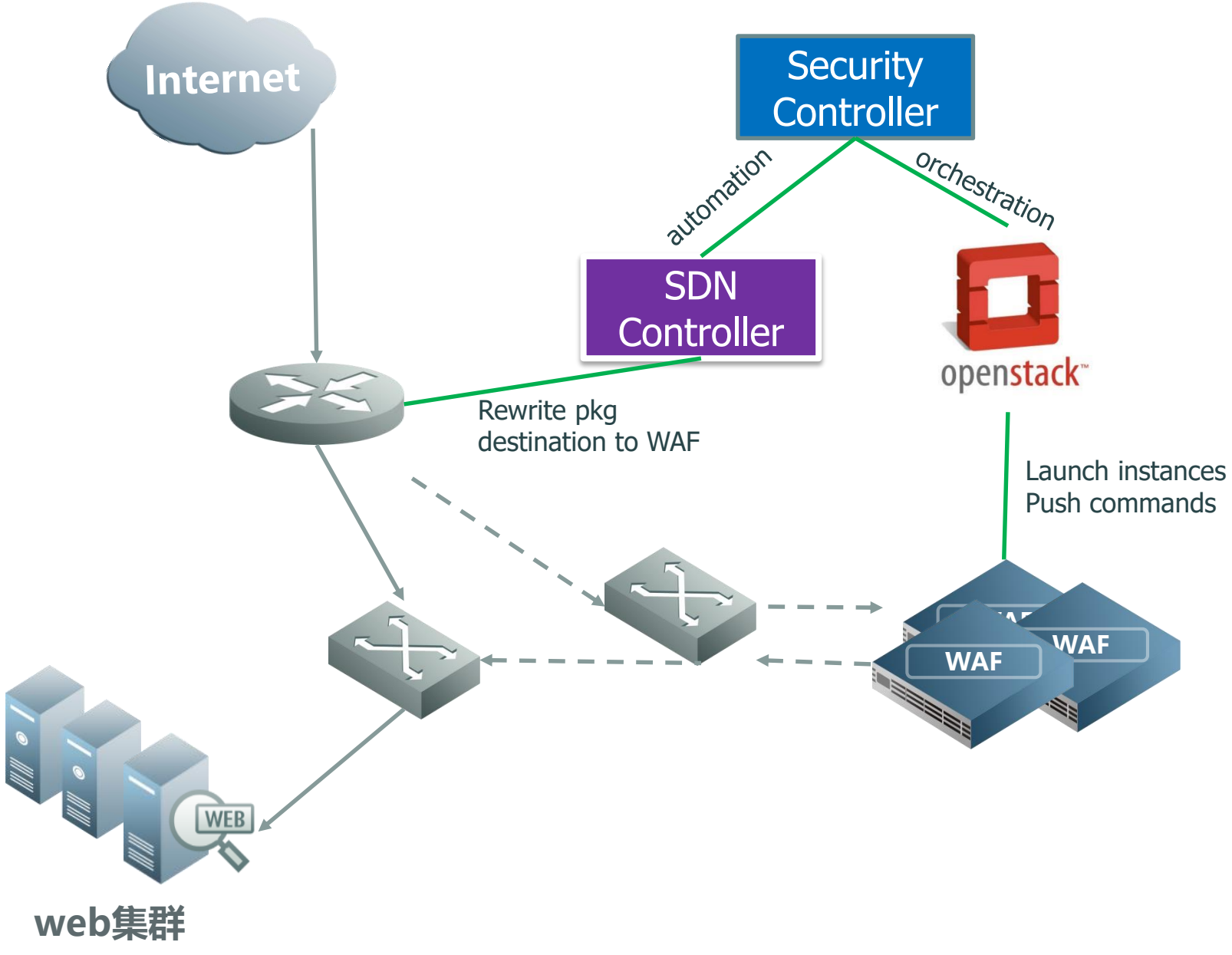
Demo：多种Web安全设备协同

Case: Software defined Anti-APT solution

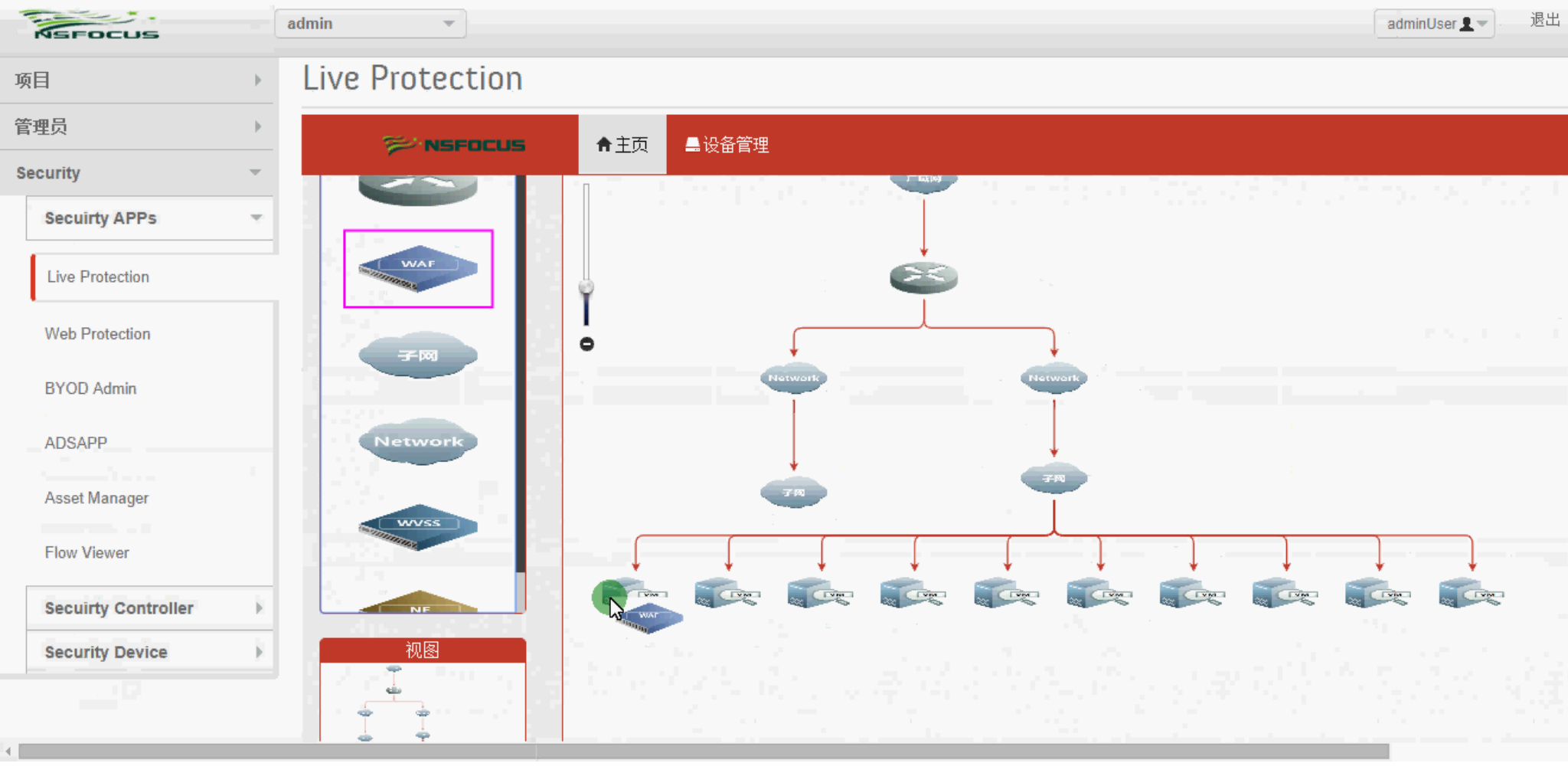


Video

Case：Live protection for Openstack web servers



Demo：WAF VM+Openstack+SDN controller



Video

Agenda

1 新型网络的安全防护体系

2 软件定义的安全防护实践

3 附录

云杉LiveCloud+绿盟安全服务发布会

国科数据中心　云杉网络 Yunshan Networks

LiveCloud弹性私有云服务&国科可信云 发布会

2014年8月15日 14:00-16:00
苏州国际科技园创新俱乐部

发布仪式	LiveCloud & 国科可信云发布
主题演讲	国科数据中心：国科云，可信云 云杉网络：SDN，助力数据中心云服务
合作伙伴演讲	盛科网络：高速互联，支撑云网络 绿盟科技：安全防护，云中生命线 宏杉科技：高速存储，迎接大数据

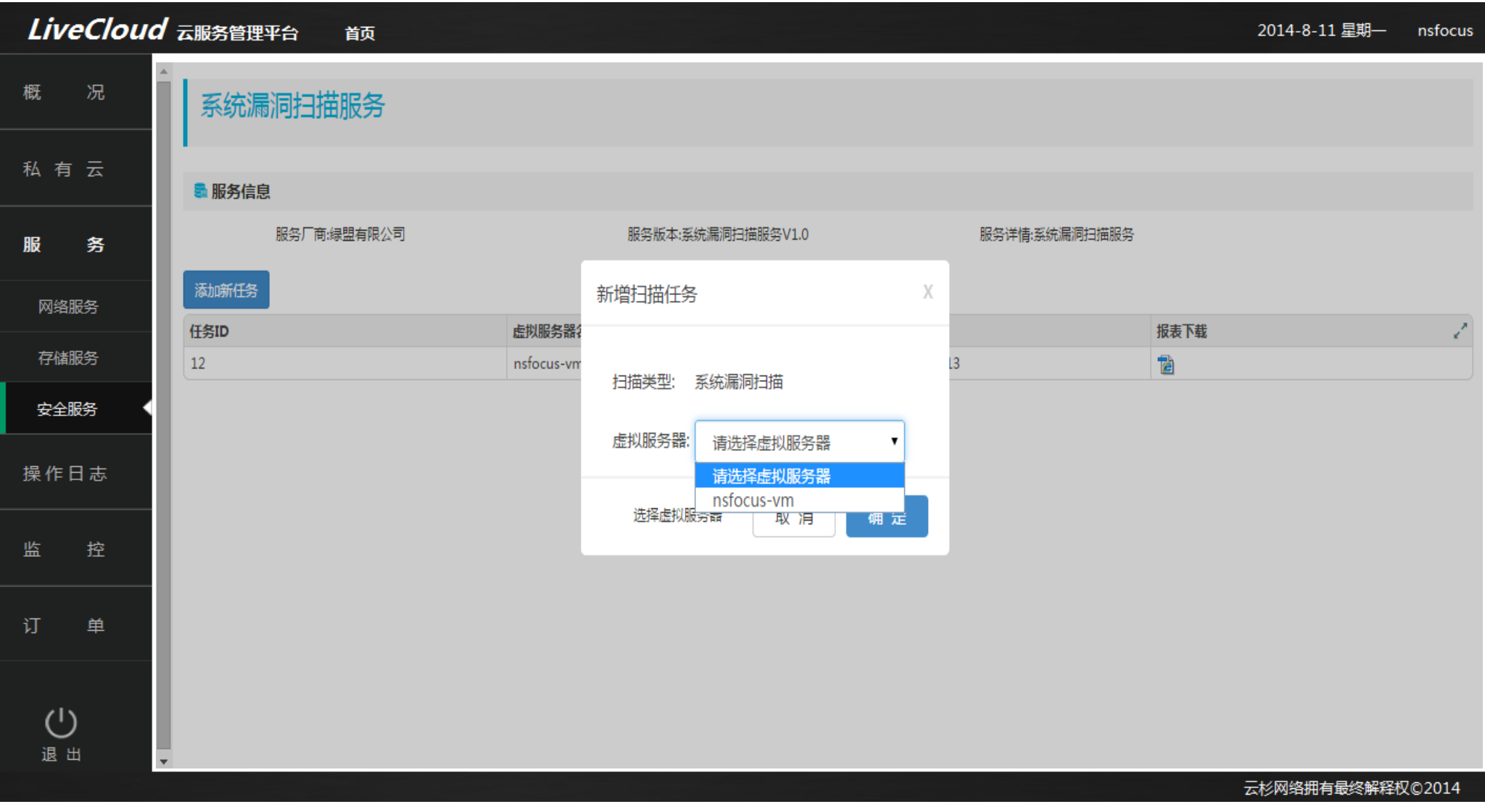
苏州工业园区星湖街328号
国际科技园五期1幢101室
创新俱乐部（蒲公英创业吧）

主办 国科数据中心 \ 云杉网络
协办 苏州工业园区科技发展有限公司

报名&现场
原小姐 18610244868
常小姐 13951117674

与LiveCloud的合作 - WAF

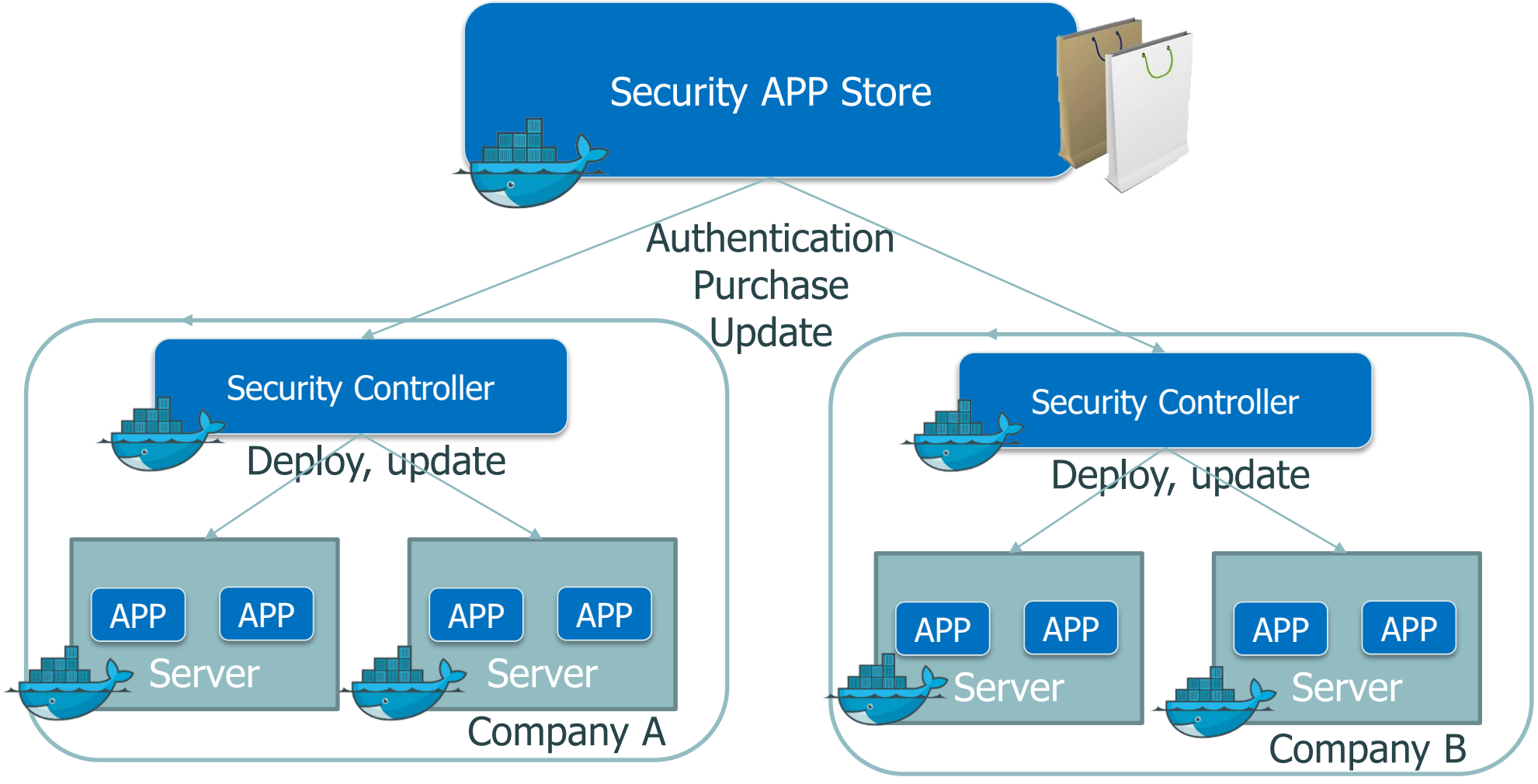
与LiveCloud的合作 - 漏扫服务



- 基于SDN技术的恶意行为监测系统

APPStore：安全交付模式的革命

- 用户云端认证，快速部署、更新应用
- 实现应用容器级的隔离，增量更新




NSFOCUS SECURITY
APP S
Most Popular
TOP1 NMAP
TOP2 NTA
TOP3 TEST
download client
operation
192.168.19.13
deploy
App下载
App操作
App查看
App部署
APP ORCHESTRATION
IF
NMAP
192.168.19.13
THEN
EMAIL
sicexpn@163.com
Add
APP NMAP
Author: xpn
manifest: nmap
level:
download
description
manage
init
start
stop
status
update

谢谢！

@marvel 新浪微博
liuwenmao@nsfocus.com