C3安全峰会
CYBER | CLOUD | COMMUNICATION

未来网络架构的安全研究

陆以勤
华南理工大学

大纲

- 未来网络及其特点
- 未来网络的安全性
- 基于未来网络的安全防御体系

互联网面临新的变革

经过40多年的发展，互联网正迎来一轮新的网络变革，由于与实体经济紧密结合，为了满足实体要求对网络提出的各种要求，通过编程动态改变网络结构和形态的SDN应运而生。

产业界对未来网络的态度

- HIS最新调查：数据中心部署SDN服务提供商的数量从2015年的20%增加到2016年60%。
- AT&T 2015年4月宣布“按需网络” 扩展至100个城市，2020年75%的网络设备将由SDN/NFV等新的技术组成。
- TBR Research最新调查，全球NFV和SDN市场到2021年将增长至1580亿美元。
- 2016年6月，全球SDNFV技术大会在北京举办。我国三大运营商已将未来网络作为关键技术。可以预料，5G核心网将采用SDN技术。

SDN架构

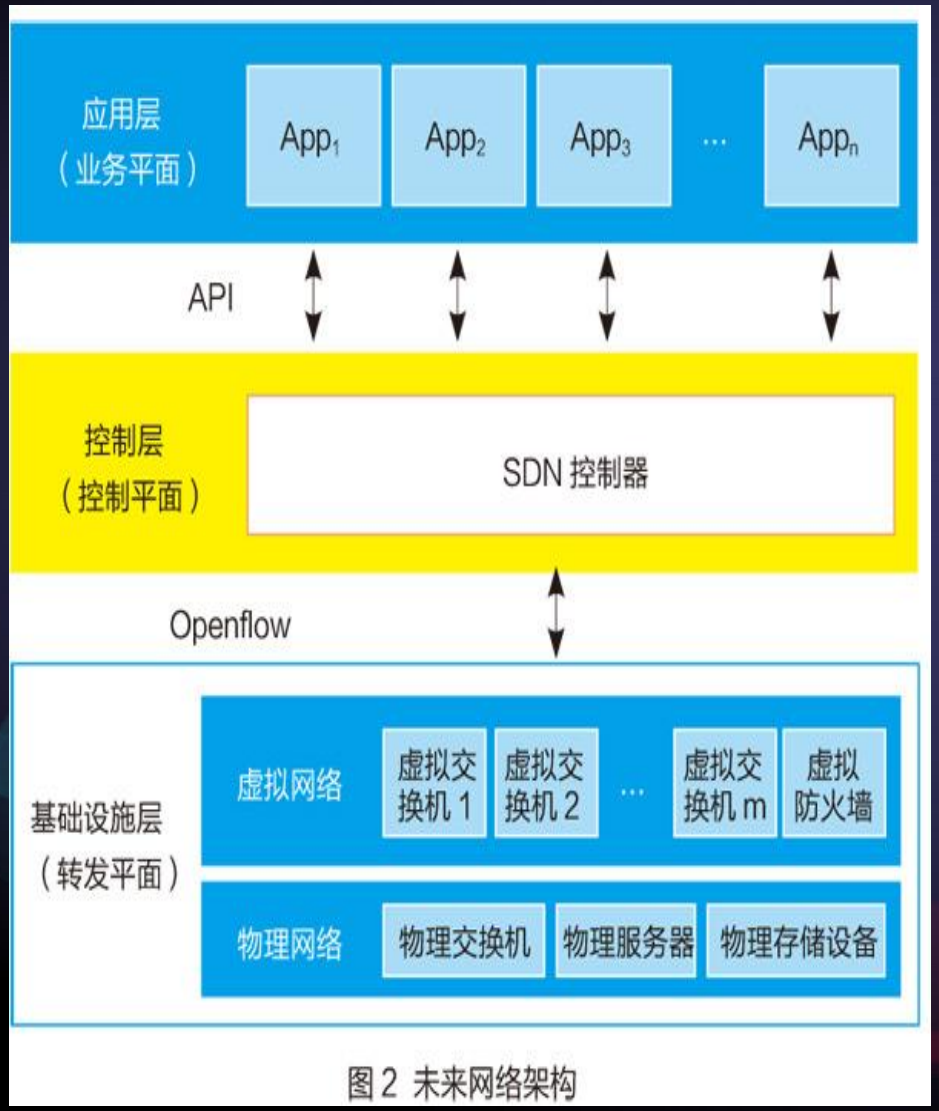


图 2 未来网络架构

“互联网 +”时代未来网络架构的发展与应用

文 / 祁琳青 陆以勤

“互联网 +”业务的发展，对网络的基础设施提出了更高的要求。互联网诞生的网络体系主要特点是设备之间的“互联”，是一种对等式的通信方式，没有主从概念，也没有全网调控的概念，但随着“互联网 +”的发展，互联网与实体经济结合，业务运行大大超越了其诞生年代的背景，传统的架构不能适应业务的发展，成为互联网产业发展的瓶颈。鉴于目前的网络架构已不适合互联网产业发展，一种根据业务需求可动态弹性分配资源、根据网络运行和安全状态快速更新策略、并向第三方开放的新网络体系结构在近两三年得到快速的发展，如同云架构改变了计算资源和存储资源的建设、运行和业务模式一样，这种新型的网络体系结构也将对网络的建设、运维和业务提供模式带来革命性影响，这种新型的网络体系结构称为未来网络架构。

未来网络架构有多种，一般目前普遍被业界认可的有软件定义网络（software defined network，SDN）和网络功能虚拟化（network function virtualization，NFV）。两者

经过十年的发展，未来网络架构开始进入了商用部署时期，国内外几乎所有的主流网络设备生产商都有 SDN 的产品，芯片生产商、网络运营商、云计算服务商、互联网应用企业等都在进行 SDN 和 NFV 的研究、试验和部署，据 Infonetics 的调研报告显示，到 2018 年全球运营商 SDN/NFV 市场规模将达到 110 亿美元。近两三年越来越多的迹象表明，未来网络正在走向现实，并且将会成为互联网产业的关键技术，对互联网产业产生革命性的影响。

未来网络的发展

为了解决互联网传统架构的资源分配弹性差、感知度颗粒度低、缺乏集中控制等问题，计算机网络专家一直在研究新的网络架构。

2005 年，CMU（卡内基梅隆大学）Albert Greenberg 等在 CCR 期刊发表的论文《A Clean slate 4D approach to network control and management》中提出：网络的关键是协同，这是控制和管理平面的事，重新构建网络的机遇和重点在控制平面。十年后的 2015 年，ACM SIGCOMM 把 Test of Time Paper Award 颁给了这篇文章，理由是：This paper led to a resurgence of interest in the topic of separated data and control planes to better manage networks that developed into Software Defined。

2007 年开始，斯坦福大学研究生 Martin Casado 联合 Nick McKeown、Scott Shenker 等人共同创建了一个网络虚拟化技术创新的公司——Nicira，并最早提出了 SDN 的概念。2011 年 Google、Facebook、Yahoo 等成立了开放网络基金会（ONF），负责制定 OpenFlow 的规范。2013 年 4 月，Cisco 和 IBM 发起成立了 OpenDaylight 计划，其范围包括一个 SDN 控制器，北向和南向 API（包括 OpenFlow）专有扩展，东西向协议用于控制器之间的互通。

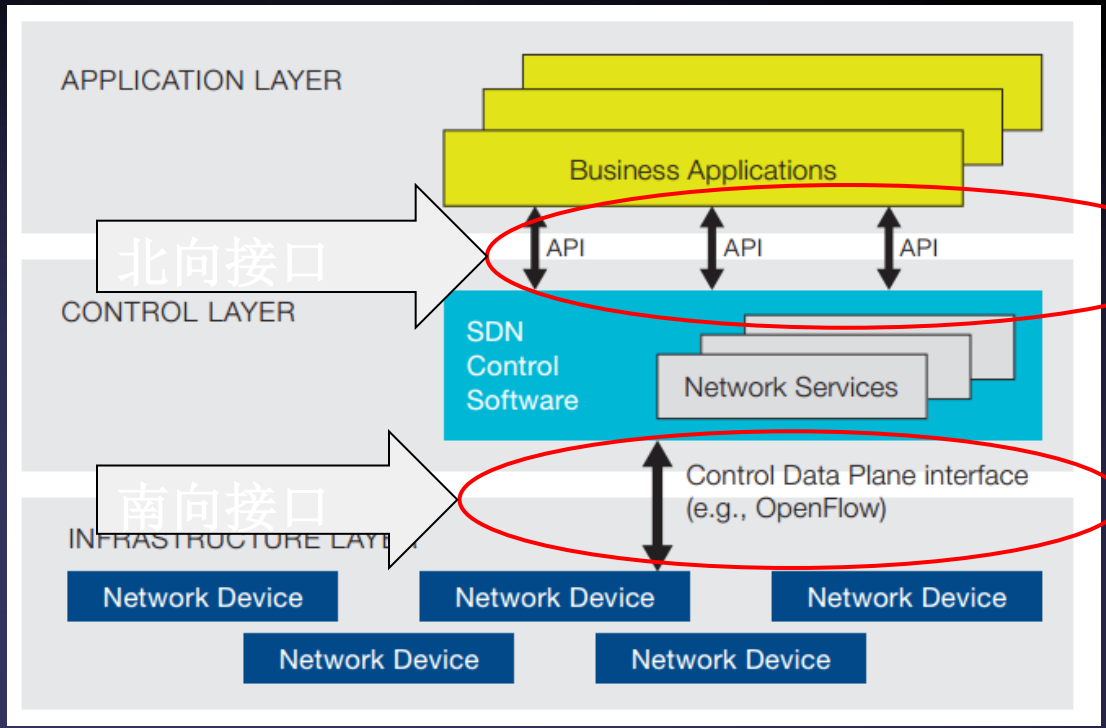
2011 年 11 月 11 日，南京市政府联合北京邮电大学、中科院计算所、清华大学共同成立中国（南京）未来网络产业创新中心，并于 2012 年 5 月正式运营。2013 年 9 月，中心升级更名为江苏省未来网络创新研究院。

2012 年 10 月 AT&T、BT 和

软件定义网络

Open Networking Foundation

一种新的网络架构



控制平面与转发平面分离，逻辑上集中化的网络控制

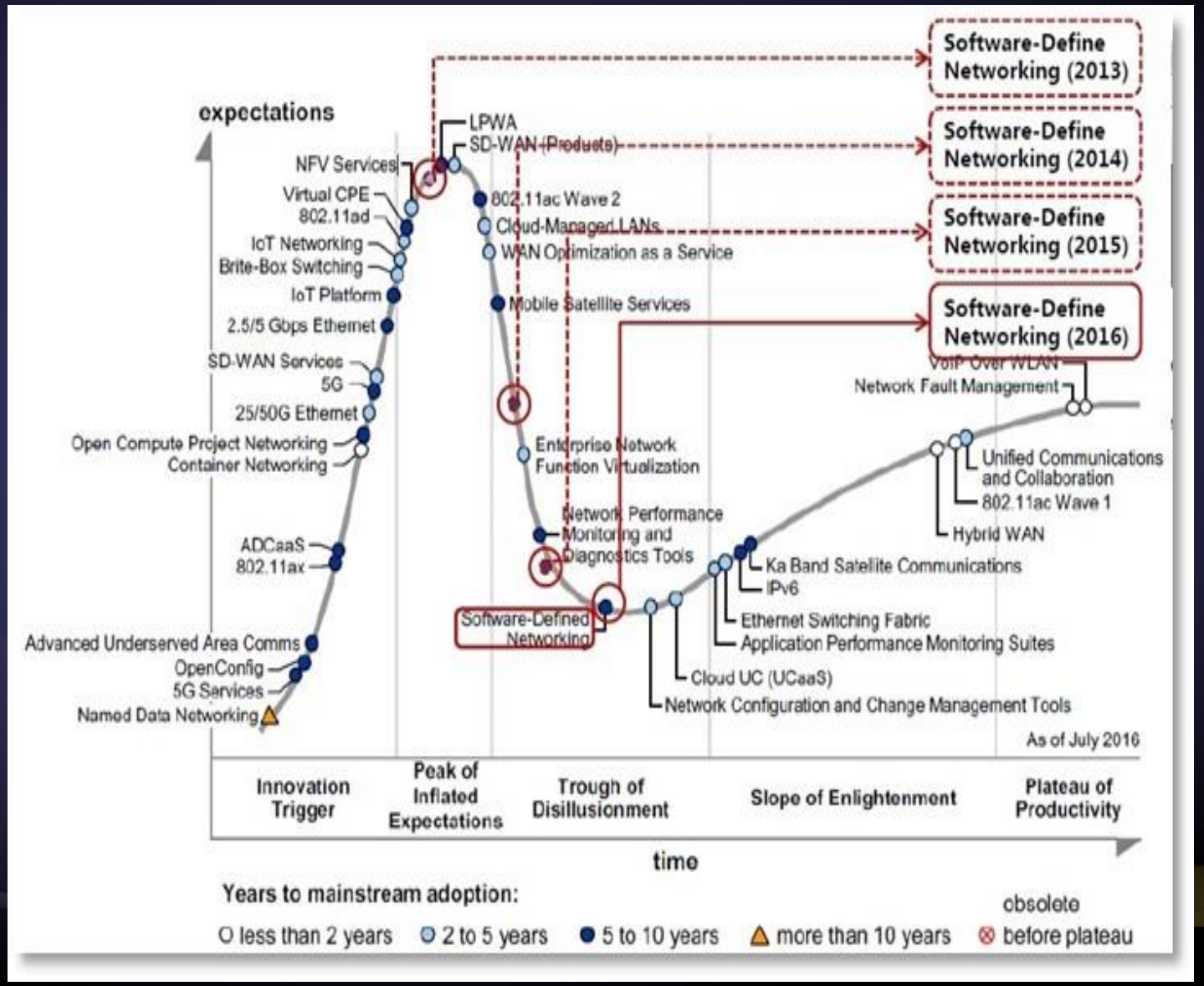
控制平面可编程、开放的编程接口

为上层应用和网络服务抽象底层转发设备

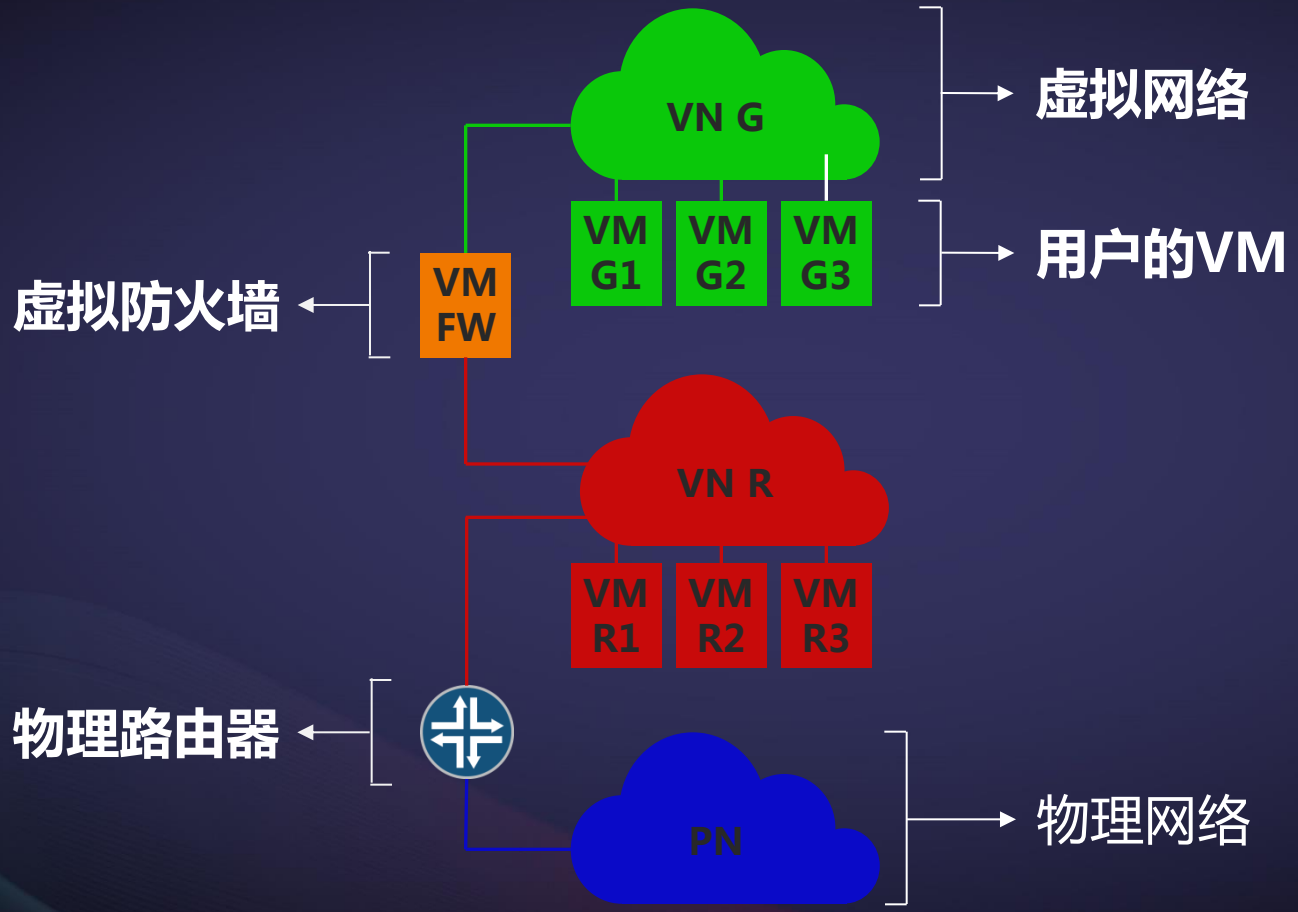
Gartner技术成熟度曲线（The Hype Cycle）

C3安全峰会
CYBER | CLOUD | COMMUNICATION

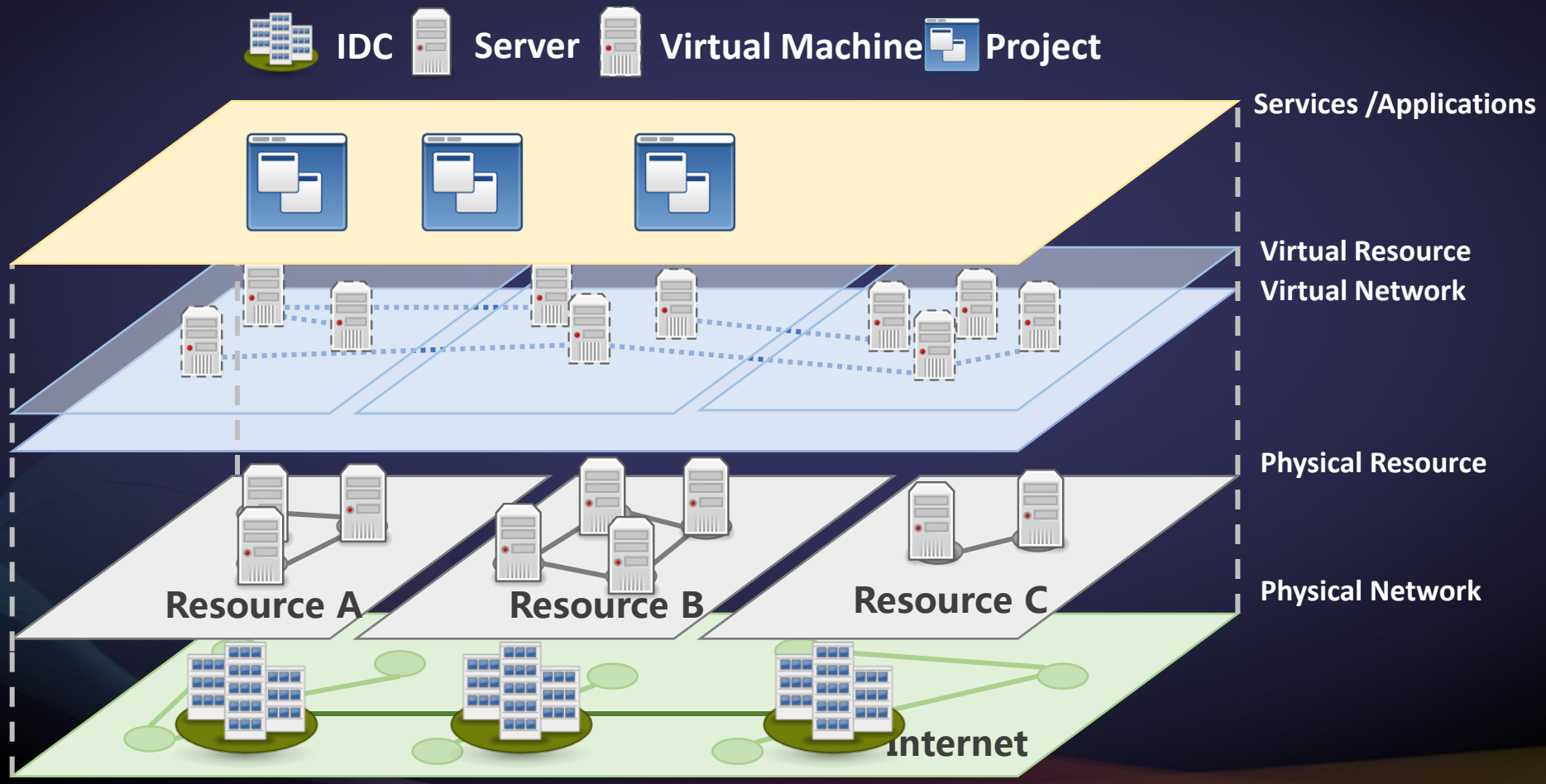
- **科技诞生的促动期** (Technology Trigger)
- **过高期望的峰值**（Peak of Inflated Expectations）
- **泡沫化的底谷期** (Trough of Disillusionment)
- **稳步爬升的光明期** (Slope of Enlightenment)
- **实质生产的高峰期** (Plateau of Productivity)



网络功能虚拟化 (NFV)



IT资源虚拟化


IDC
Server
Virtual Machine
Project
Services /Applications
Virtual Resource
Virtual Network
Physical Resource
Physical Network
Resource A
Resource B
Resource C
Internet

未来网络的特点

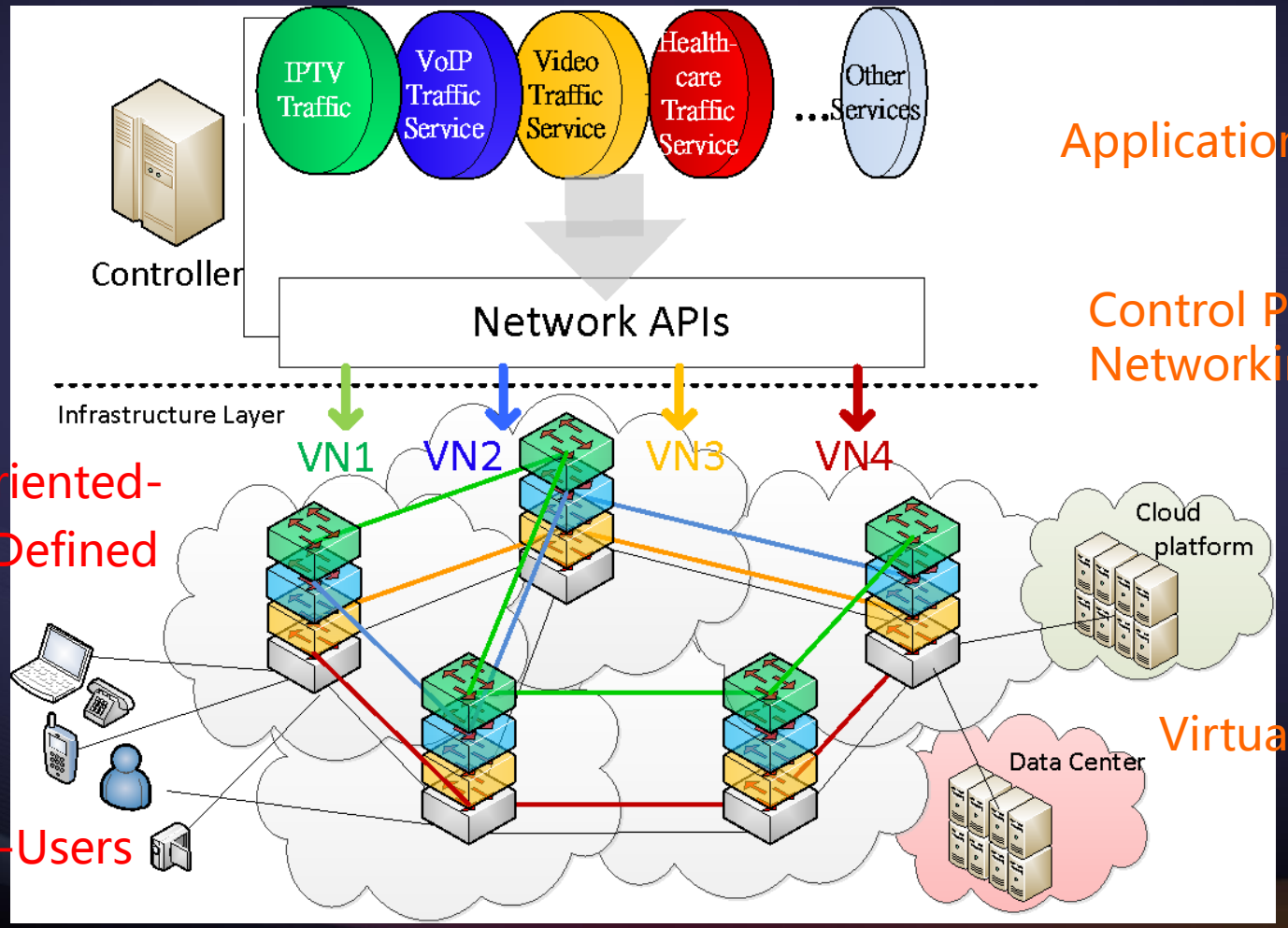
- **全网可控：**由于实现了控制和转发分离，网络具有全网集中控制性，联盟具有盟主或者分盟主，地方和中央平衡控制权，网络的感知颗粒度变得精细，使网络具备智能化的基础；
- **开放性：**网络具有统一的接口，**第三方**可以使用计算机　　的方式对网络按需进行动态设置、策略调整、资源调度，亦可以根据用户需要开发新的功能；
- **资源虚拟化：**实现计算、存储、网络等IT资源虚拟化，在物理资源层之上构建了虚拟（逻辑）资源层，用户编程可以独立于具体的物理网络，虚拟网络可以根据业务需要进行拓扑调整、配置、迁移，不受物理位置的限制。

大纲

- 未来网络及其特点
- 未来网络的安全性
- 基于未来网络的安全防御体系

面向第三方开放的架构

An Application Oriented Model



Applications / Services

Control Plane with Networking Action

Service Oriented-Software Defined Network

Virtual Network

End-Users

SDN架构的策略冲突问题

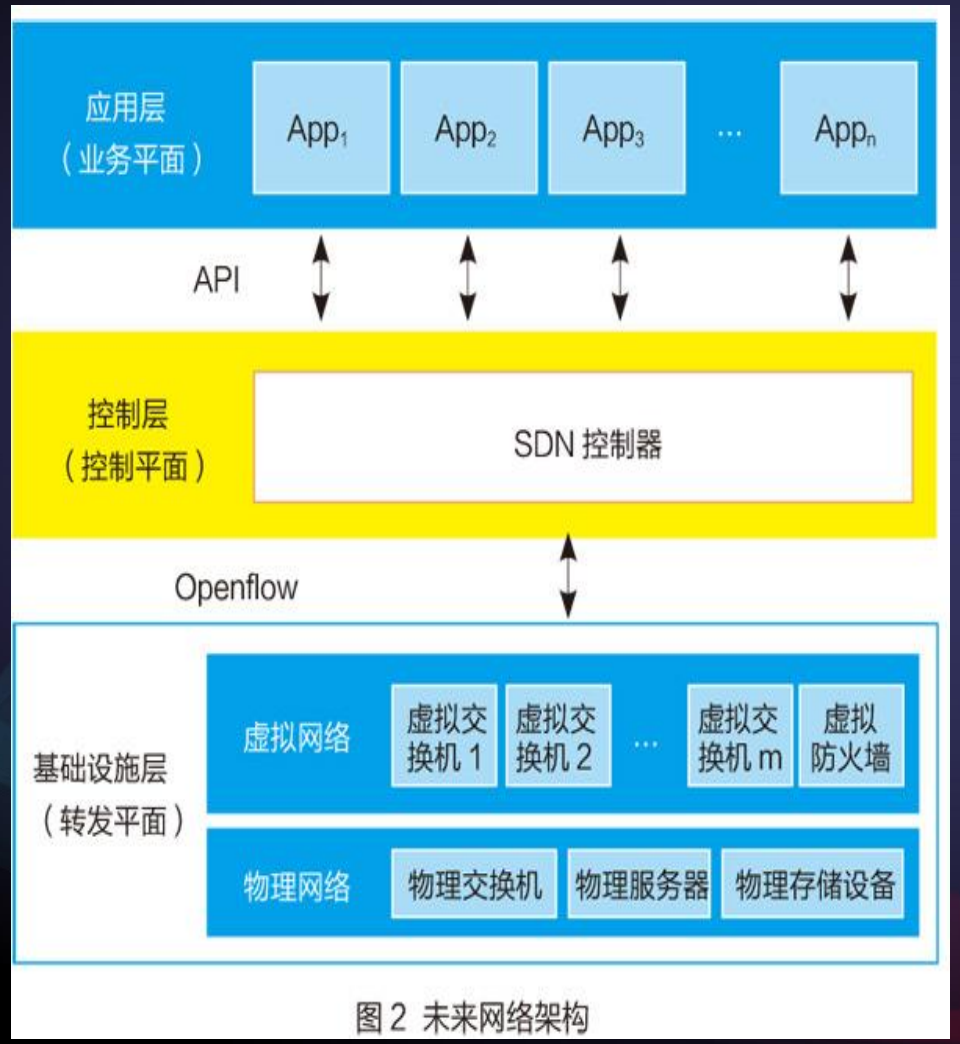
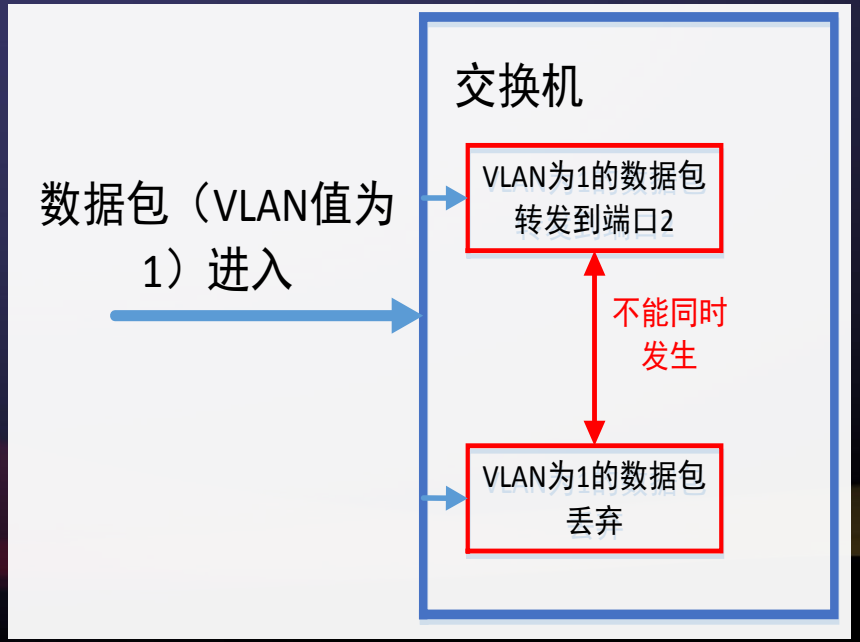
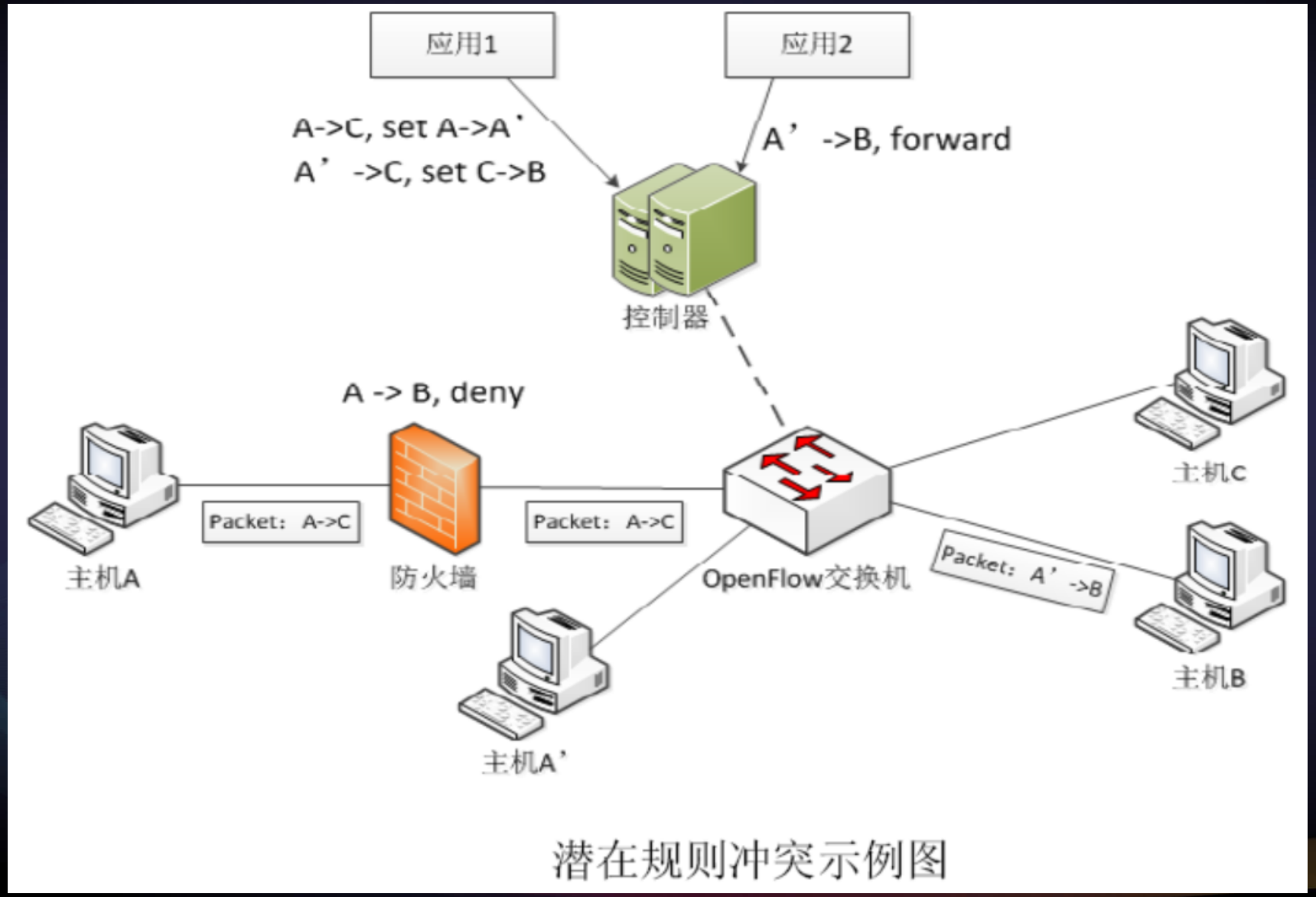


图 2 未来网络架构

由于未来网络采用对第三方开发者开放的架构，不同的开发者独立设计的策略叠加到网络运行时，一个策略的执行影响了另外策略的运行，造成了策略意图不能实现，或者导致安全问题。



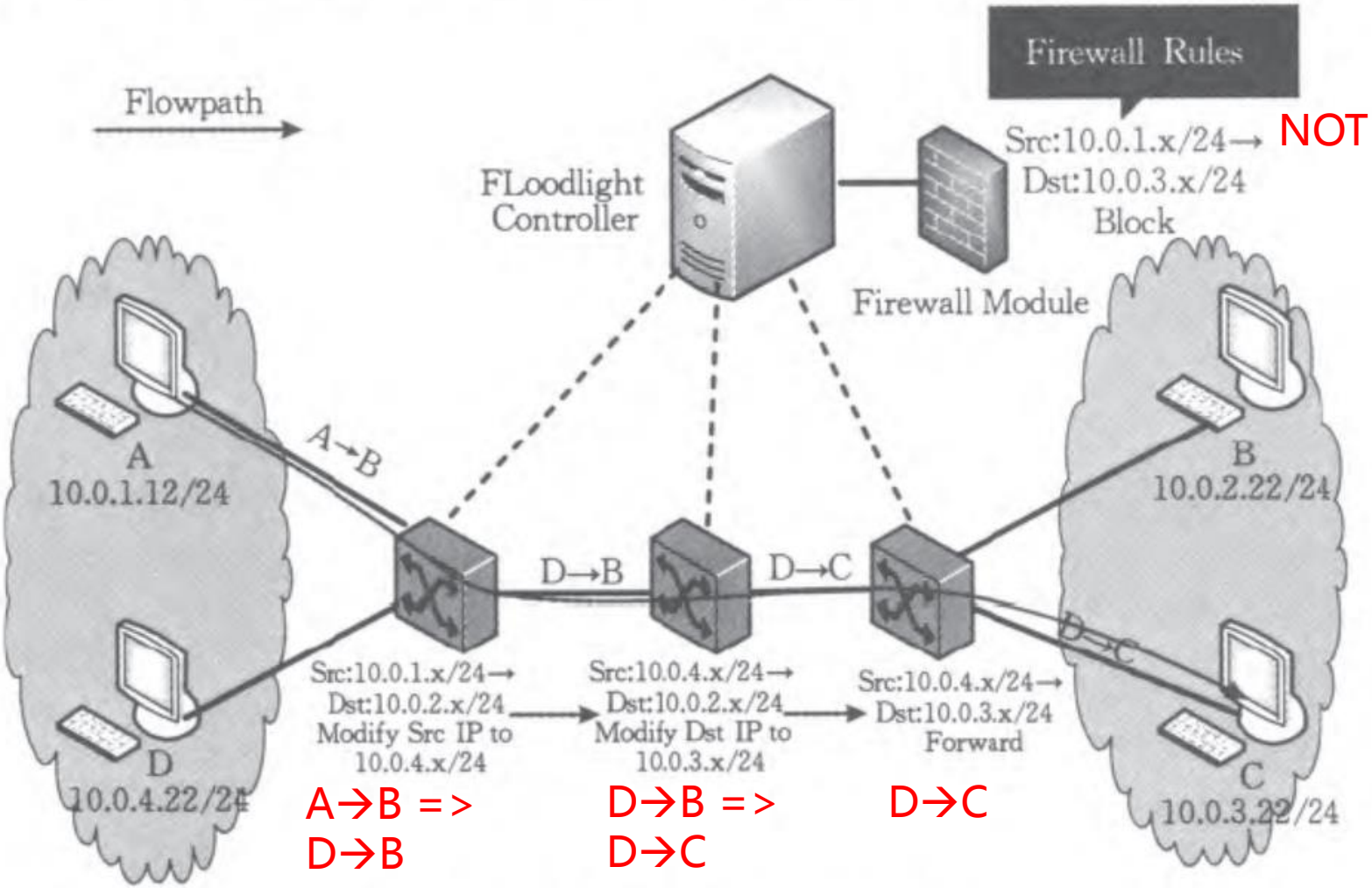
SDN的策略冲突引起的安全问题



潜在规则冲突示例图

资料来源：王航远，《SDN应用策略冲突检测方法研究》

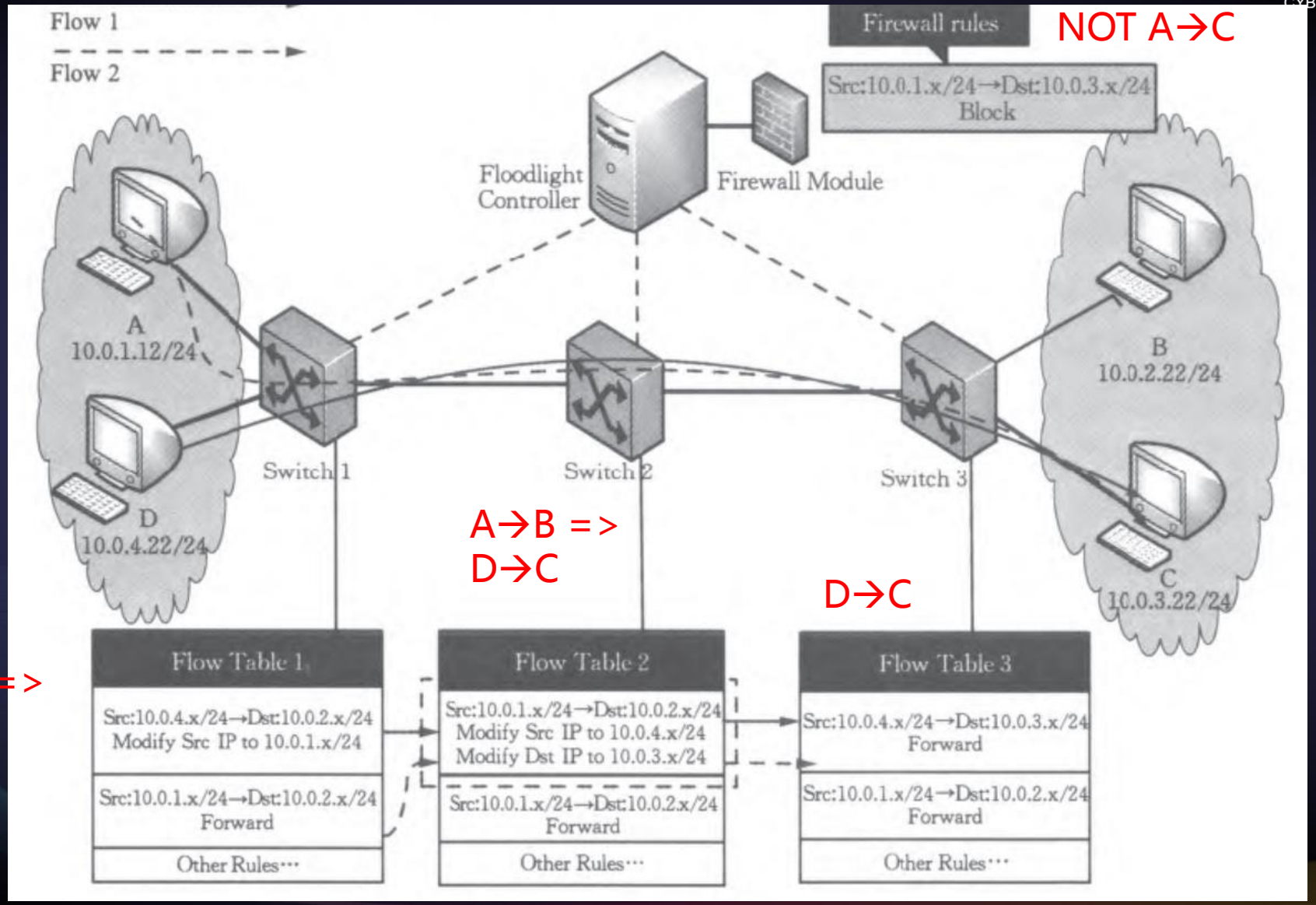
对地址的重写操作导致安全策略被绕过



重写操作导致安全策略被绕过

资料来源，王鹃等，一种基于OpenFlow的SDN访问控制策略实时冲突检测与解决方法《计算机学报》

策略冲突造成路径错误



资料来源，王鹃等，一种基于OpenFlow的SDN访问控制策略实时冲突检测与解决方法《计算机学报》

电信业务冲突问题

1996 年 12 月
第 12 卷第 12 期
电 信 科 学
TELECOMMUNICATIONS SCIENCE
Vol.12 No.12
December 1996

电信系统的业务交互*

陆以勤 韦岗
(华南理工大学 广州 510641)

摘要 本文综述了电信业务交互问题产生的原因以及研究的背景、方法和发展,并以作者的研究成果为例说明如何用形式方法处理业务交互。

关键词 电信系统 业务交互 Petri 网 不变量守恒变换

1 电信系统的业务交互问题

随着通信技术的发展,业务的加速集成不仅成为可能,而且在国外已成为一种趋势。在国内,除了原有的新业务如"呼叫等待(call waiting)"、"呼叫转移(call transfer)"等外,邮电部门还投入大量资金引进或研制专用的业务增值设备。1995 年 5 月我国第一个智能平台——大唐 EN2000 通过邮电部鉴定,作为主干机型,在 1995 年 9 月实现了全国八大城市联网。1995 年 8 月广州和深圳引进了爱立信公司和 AT&T 公司的智能网设备,进行集中付费(free phone)、虚拟专用网(VPN)、个人通讯(UPT)、电子投票(VOT)4 种业务为期一年的增值

策略冲突检测

- 由于第三方策略设计者之间不一定会互间沟通，甚至，不一定知道自己设计的两个策略之间执行时会否互相影响。

策略冲突检测

- **规则冲突检测**：检测两个规则间是否冲突，运用静态检测和逻辑表示的方法。
- **不变量违反检测**：意图的满足性测试，例如无环，可达性测试，通常使用模型检测和理论验证器的方法。

现有检测方法需要解决的问题

匹配域修改

SDN中匹配域修改动作能修改数据包的头域，现有大部分文献中基于传统网络分析方法忽略分析，或者由于其复杂性放弃分析，使得很多模型不适用现有的SDN网络架构。

全网一致

SDN中要求全网考量，大部分文献中只检测单一规则，不考虑功能一致（例如选路和相互有依赖的规则），一旦冲突发生，余下的规则会对网络造成不良影响。

优先级分配

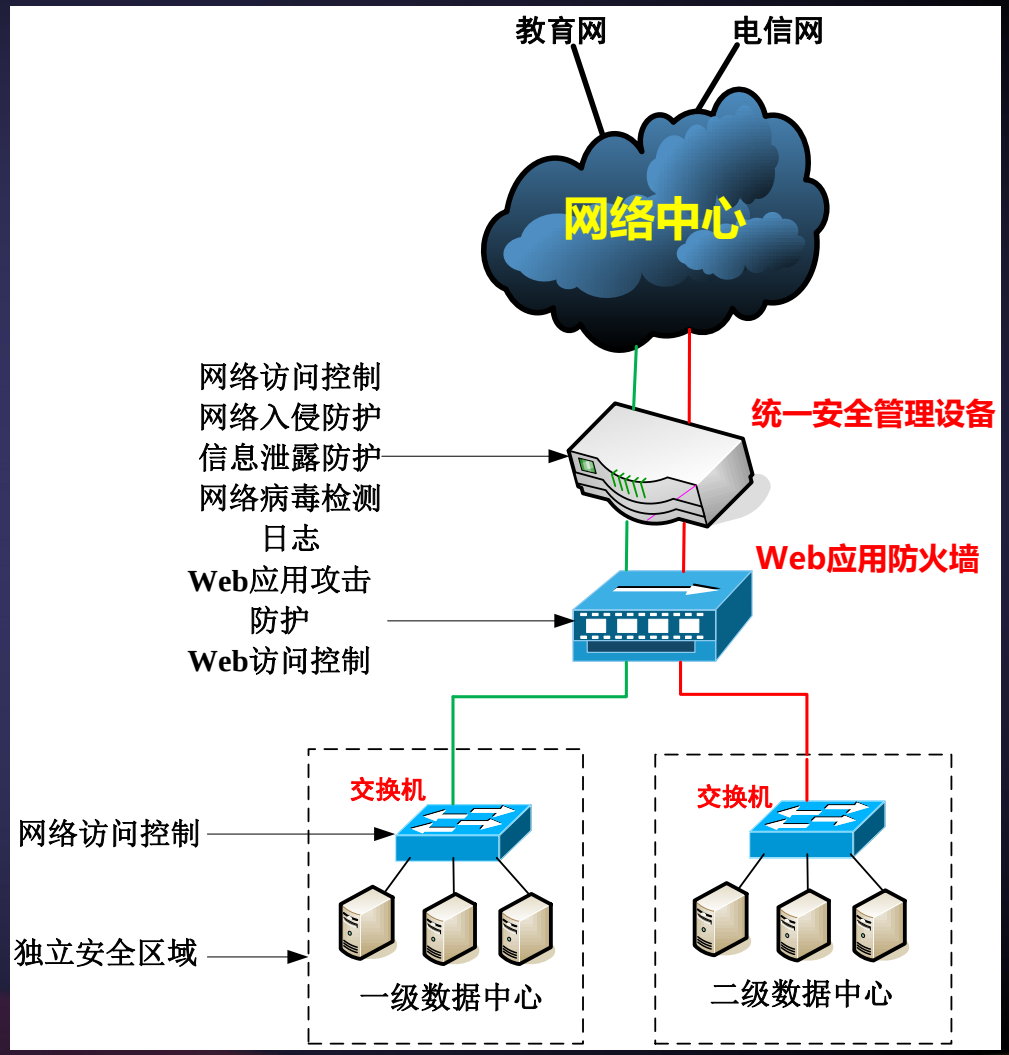
冲突发生后处理阶段，大部分文献的处理人为分配优先级，工作量大，极易错误的。

大纲

- 未来网络及其特点
- 未来网络的安全性
- 基于未来网络的安全防御体系

现有网络安全防御体系存在的问题

- 安全设备部署在网络边缘，对内部感知颗粒度粗，难以防范来自内部的攻击；
- 部署在系统内部的安全设备采用游兵散勇式的防御方法，没有进行信息共享和协同防御；
- 基于漏洞/后门具体特征等先验信息的检测方法难以有效应对未知漏洞/后门；
- 基于网络行为的异常分析方法不够灵活，需要定义各种参数，不能够适应变化的网络环境。

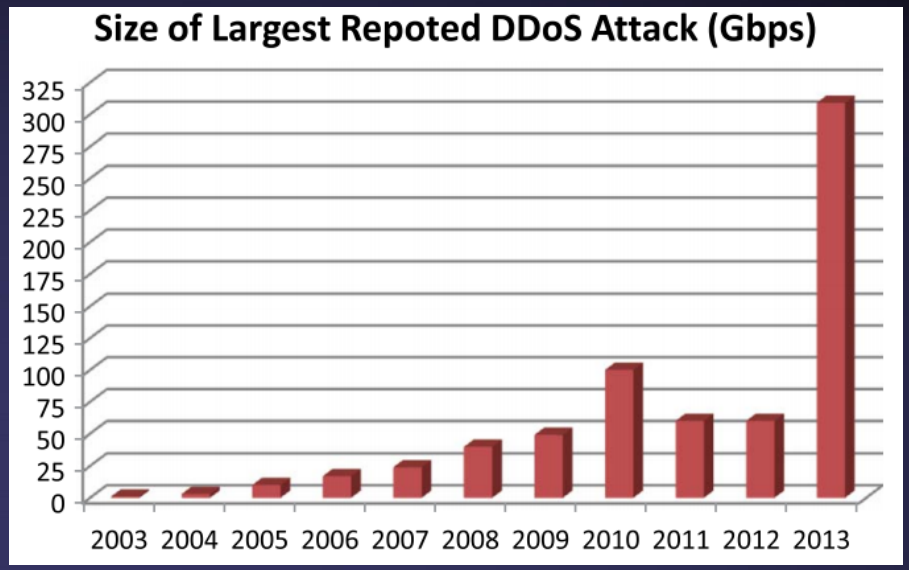


攻击方式的改变

C3安全峰会
CYBER | CLOUD | COMMUNICATION

1、云计算平台超宽带网络接入使DDoS攻击的强度异常巨大：300Gbps

Arbor Networks报告



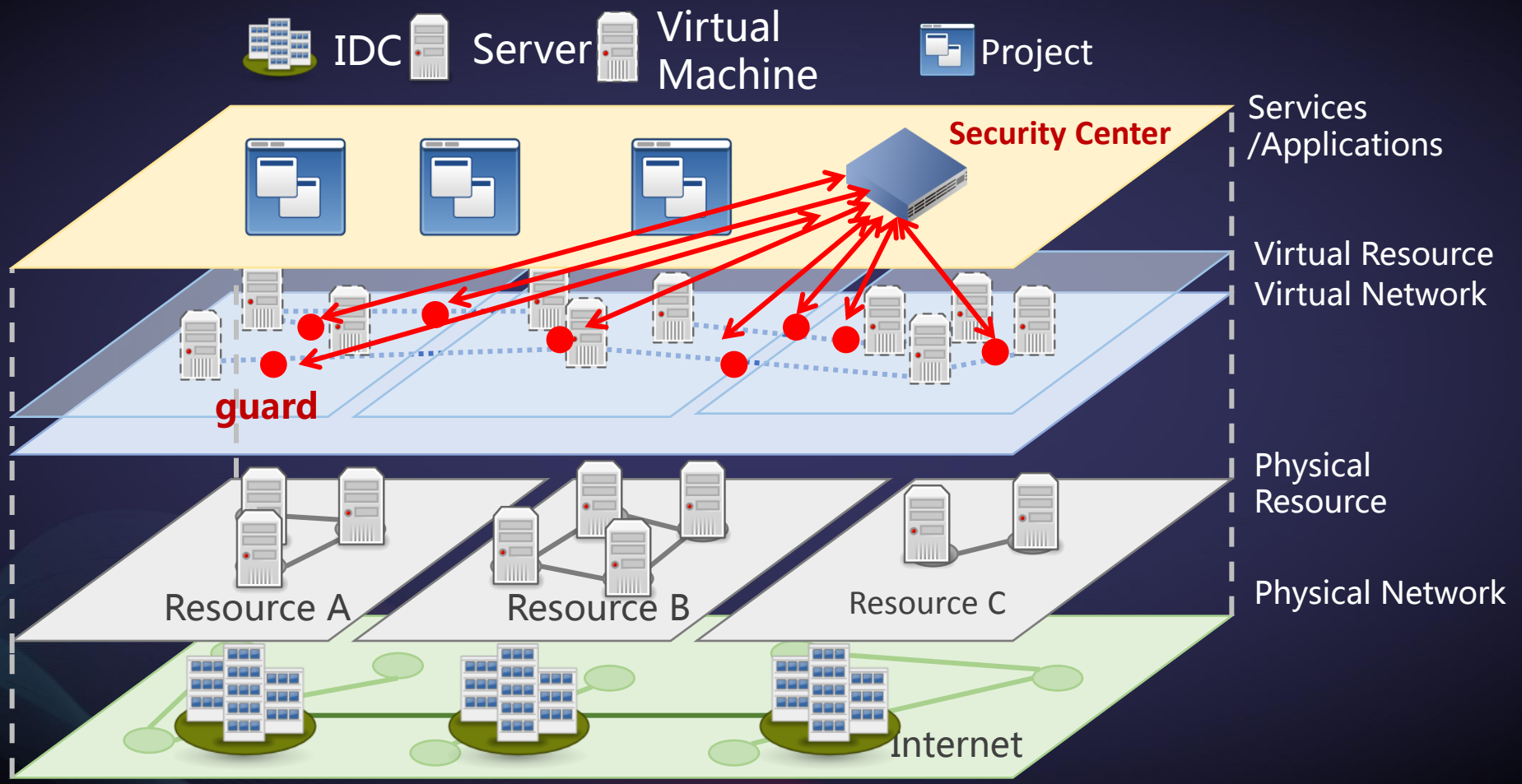
2、云资源的快速弹性交付使得恶意软件即服务成为现实:DDoS攻击即服务

调查表明：只需1000美金左右就可以购买具有10000个计算机节点的僵尸网络

3、由于多租户的共存，一次攻击可以泛化指向云端多个攻击目标

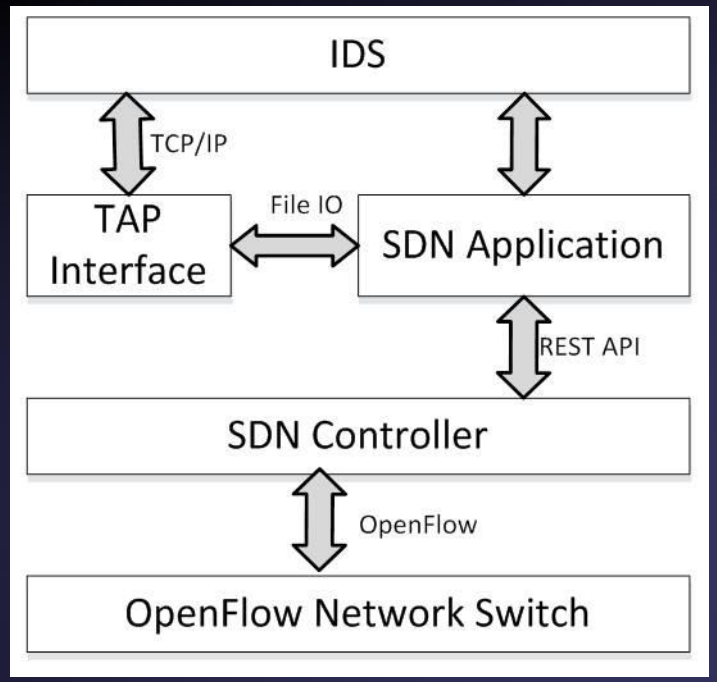
4、虚拟化技术为攻击者研究攻击目标的弱点提供了样本

协同防范体系



将安全感知的神经延伸到网络空间内部，细化信息收集的颗粒度，突破传统单点防御和边缘防御模型在传统网络和云计算环境的缺陷

SDN架构的IDS



（1）SDN控制器通过Packet_in消息等手段从底层OpenFlow交换机汇集网络流量；

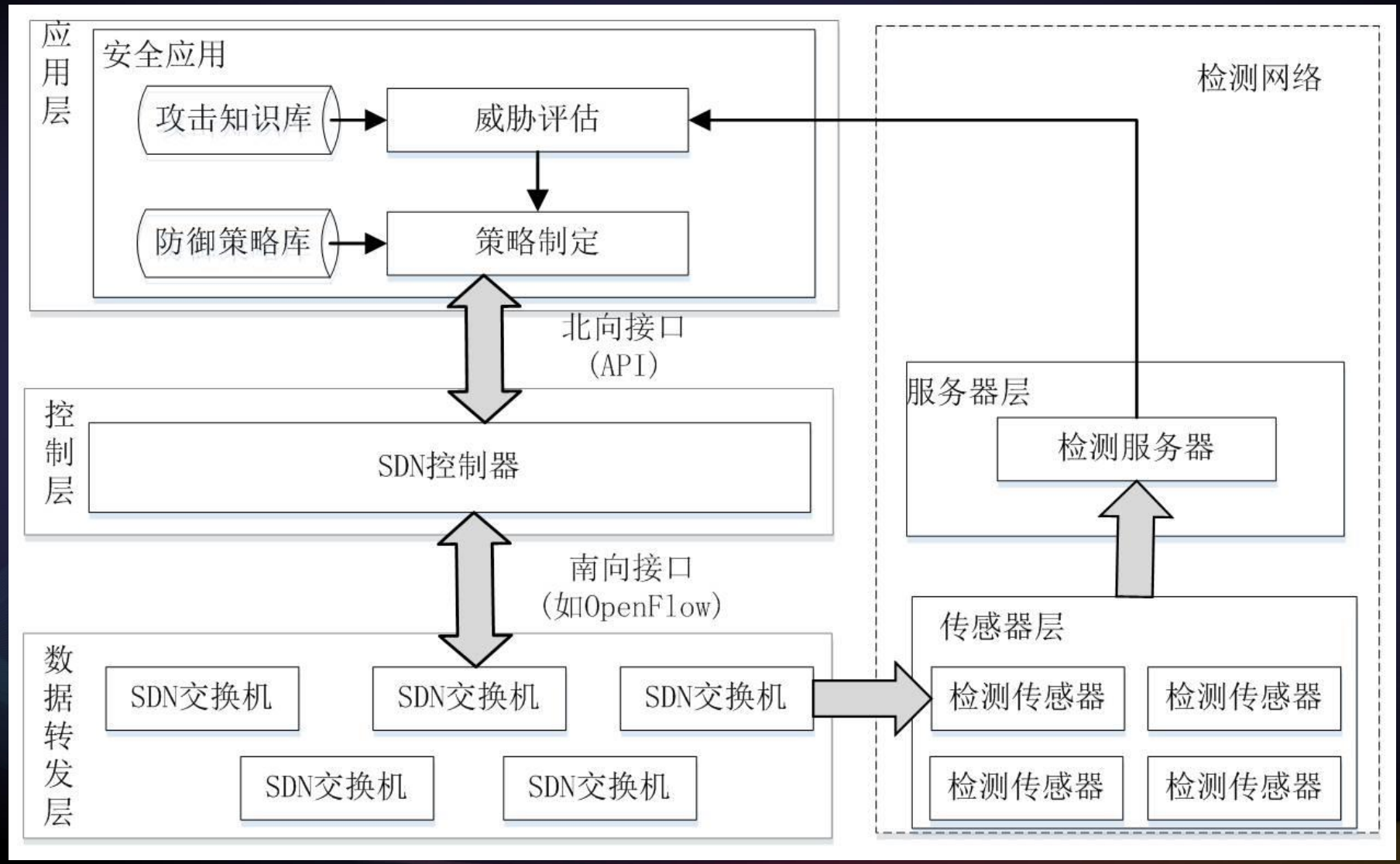
（2）SDN应用将控制器获取的网络流量送入部署的IDS检测引擎中进行入侵检测，并将检测结果返回给安全应用；

（3）SDN安全应用根据IDS检测结果，制定对应的防御流表项；

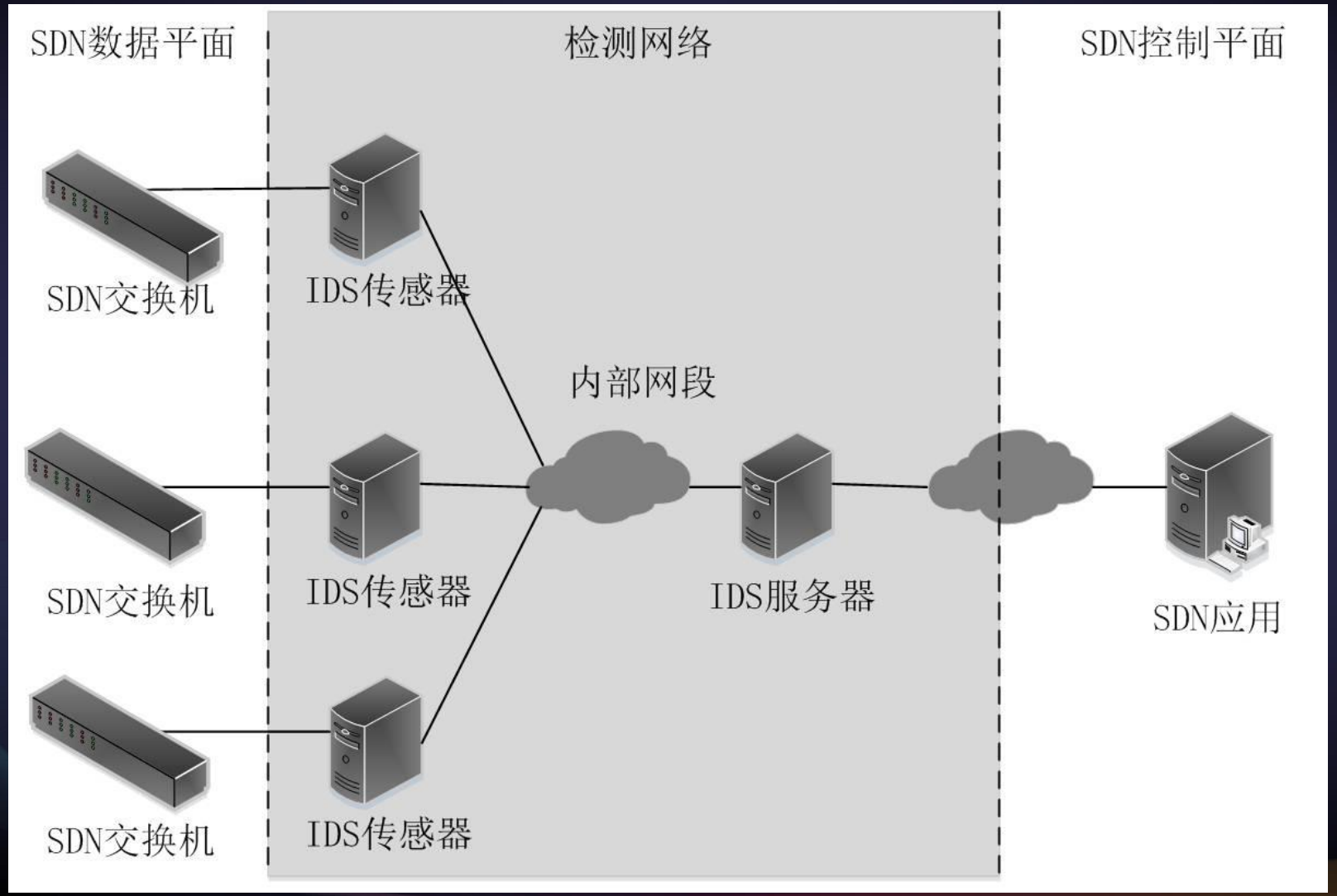
（4）SDN安全应用通过REST API指示控制器将防御项下发部署到底层的OpenFlow交换机；

（5）OpenFlow交换机则根据所部署的防御流表项阻断网络攻击，保护网络的安全。

SDN架构的独立的检测网络



具有独立检测网络的IDS系统



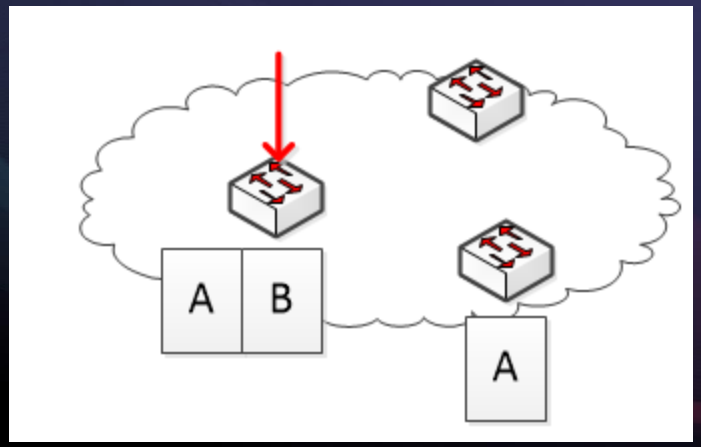
1、解决原始数据采集的问题：采用分布式的流量样本信息采集方法，从网络全局的角度监控网络流量

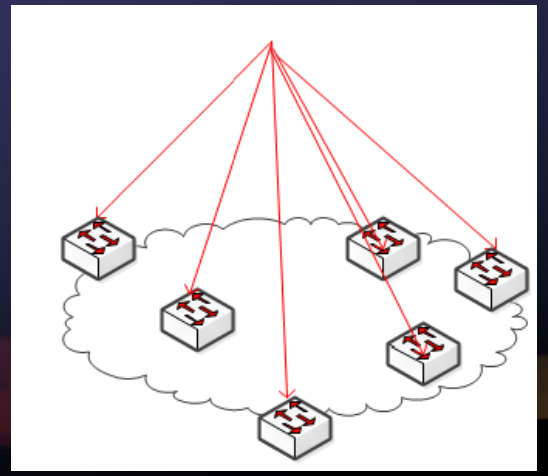
从网络全局网元设备处实时获取可定义的高细粒度流量统计信息，从整网角度建立分布式的流量统计信息采集方法。

2、研究原始数据的预处理方式：定义基于多点信息的检测度量标准

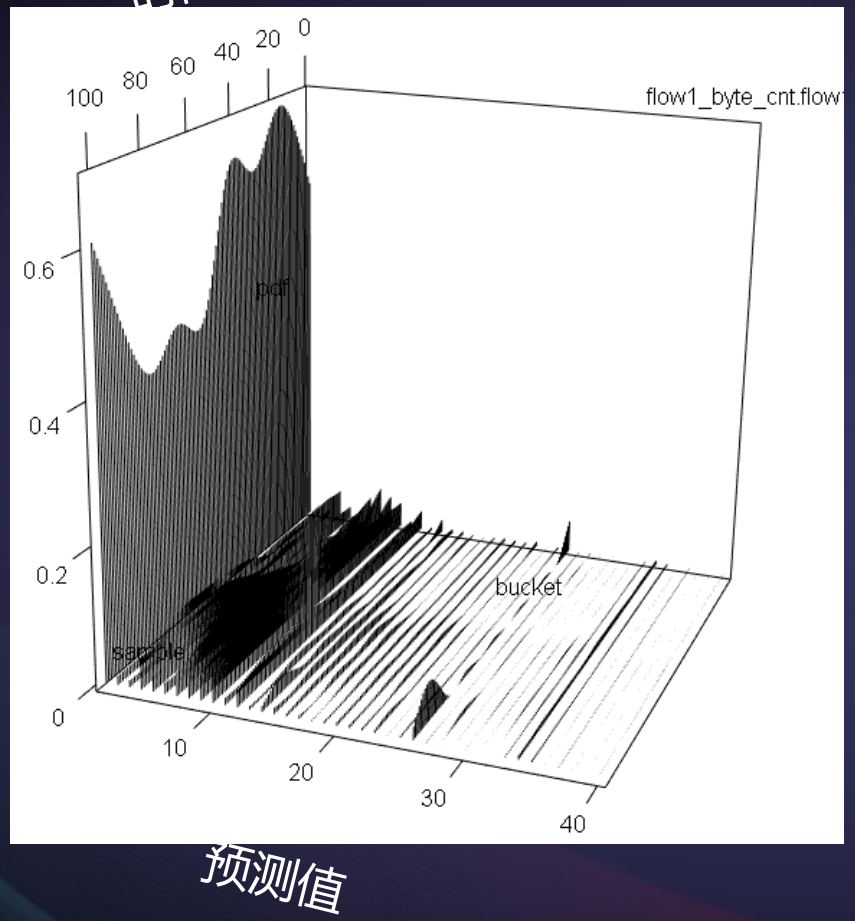
基于单点信息的检测度量标准通常基于局部的汇聚流信息建立度量模型，挖掘网络汇聚点处流量内包含的流模式特征信息，例如基于目的地址的熵、平均每条流的报文数、对称流所占比例等。这种度量在云计算网络下难以从租户的逻辑网络视角进行测度。

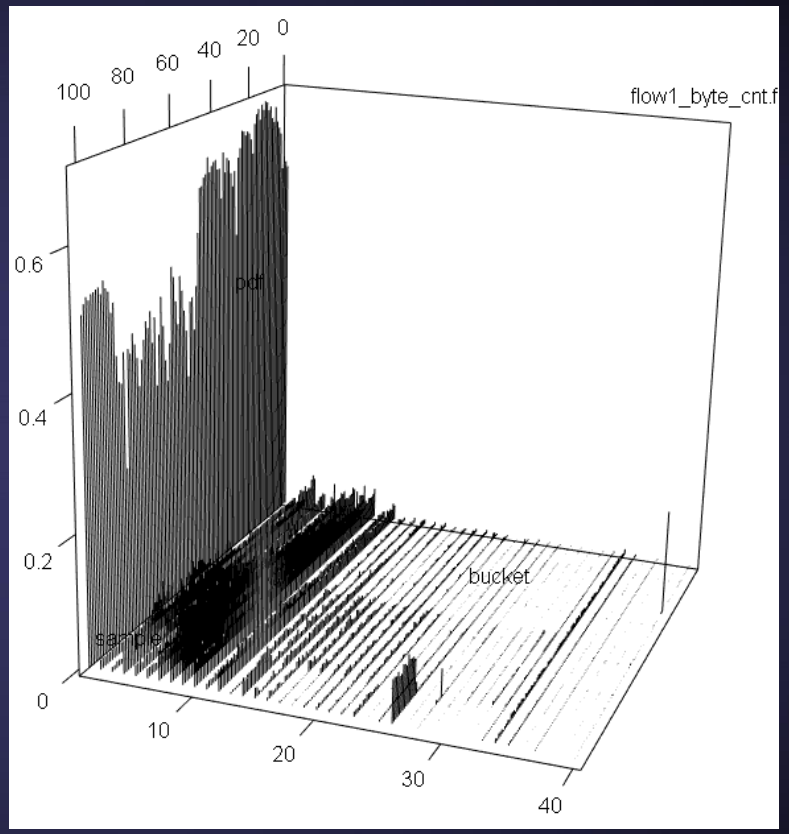
需要重新设计对来自多点的原始数据的预处理方式，定义新的检测度量标准，对局部得到的流量信息进行汇总后提炼出检测方法需要的输入数据





预测模型是时间、分布刻度、预测值的三维。



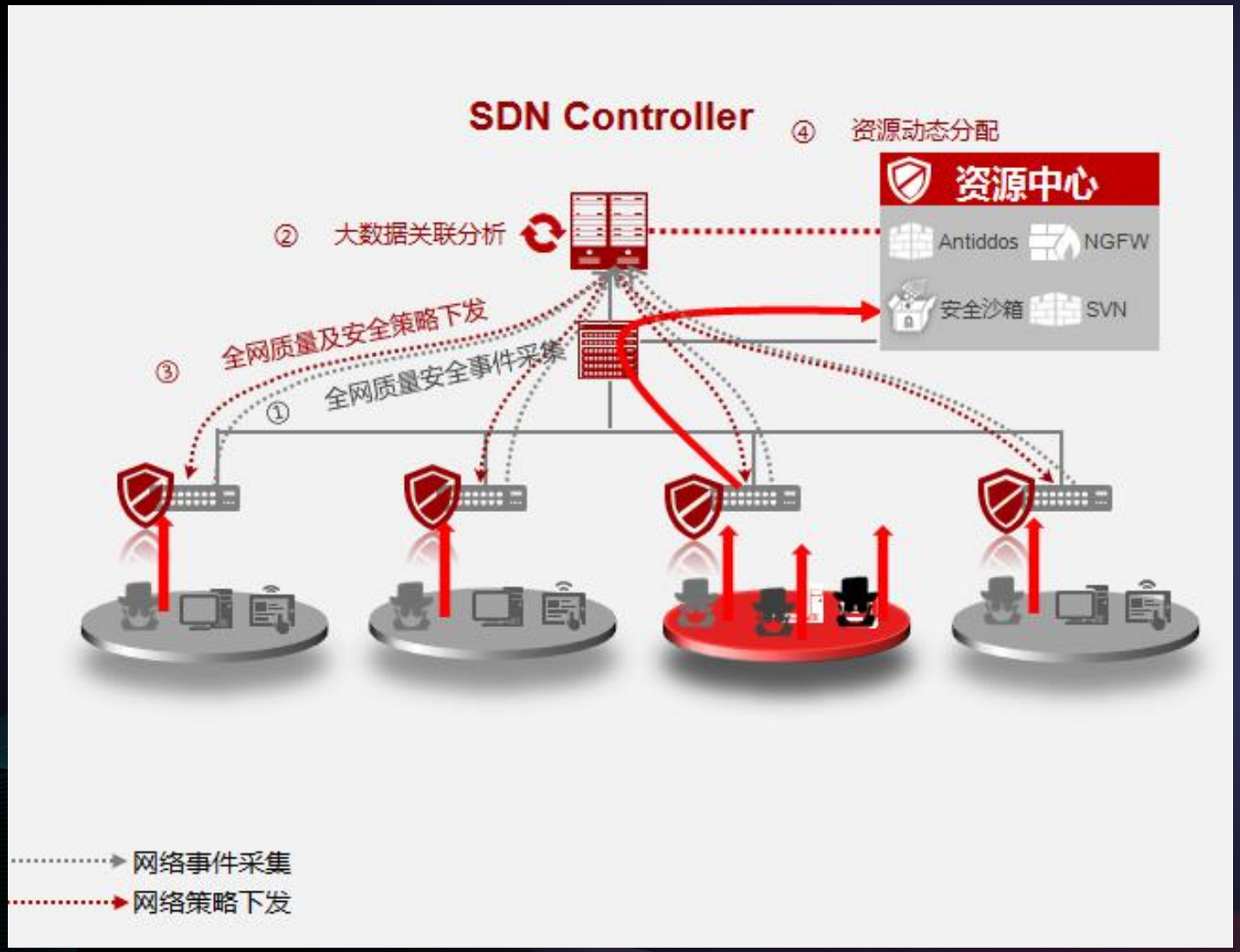


SDN和传统网络下DDoS攻击防御机制的

	传统网络	SDN
控制方式	分布式控制	集中控制
数据获取	从自治域的边界网元设备获取汇聚的流量信息	分布式的从网路全局的网元设备获取流量信息
检测方法	1、基于信号处理的检测方法：统计学、熵模型等 2、基于机器学习的检测方法：神经网络、贝叶斯模型等	目前的方法基本继承传统网络下的检测方法，根据数据的差异性定义了新的测度度量
响应机制	在边界网络设备执行策略（例如过滤、队列、流清洗或DPI）	根据检测提供的信息从网络全局角度下发特定的策略
部署方式	专用的设备、性能要求高、部署代价大	以软件的方式运行在通用服务器上，敏捷灵活

各自为营的散兵游骑难以阻挡组织完善的正规军，SDN相对于传统网络应对DDoS攻击这种精心组织的攻击具有先天性的优势。

基于SDN的安全防御体系



1、全网事件采集

网络、安全设备日志、终端用户行为及流量异常数据等

2、大数据关联分析

SDN Controller对海量数据进行关联分析，发现安全隐患

3、全网策略下发

SDN Controller下发调整后的安全策略至全网相关设备

4、资源动态分配

SDN Controller将全网的安全设备虚拟为资源池，并根据区域、用户、安全事件动态分配网络资源

5、重复执行1，直至故障或安全威胁消除

C3安全峰会
CYBER | CLOUD | COMMUNICATION

Thank you