NSFOCUS

2016绿盟科技软件定义安全SDS白皮书

2016年11月25日

导读

在 2015 年中，软件定义安全大多还在探讨这个体系架构诞生的年代，还看到软件定义安全是一个新的热潮，而在今年已经可以看到自适应安全、自动化应用编排、零信任 / 微分段、体系标准化等落地应用形式，软件定义安全的发展速度由此可见一斑。

2016 绿盟科技软件定义安全白皮书，着重探讨了安全编排、资源池建设两个软件定义安全的核心部分，同时从落地实践的角度，分享三个方面的实践经验，包括面向混合云和移动办公的自适应访问控制；面向公有云的安全服务；可编排的应急响应 / 弹性服务。

需要明确的是，软件定义安全与云计算安全无论从逻辑上还是架构上都没有必然的联系。软件定义的安全方案同样也可以部署在传统 IT 环境，如果能做到开放接口，通过软件驱动底层安全设备，通过软件编排上层应用，那么这套安全防护体系也是软件定义的。相反，即使在云环境中部署了大量的安全机制，但如果仅是简单堆砌，那并不是软件定义安全。

本篇白皮书仍会重点讨论软件定义安全体系在云环境中应用，着眼于其落地交付过程，此外也会讨该体系在 BYOD、传统 IT 环境等场景可能的应用。

如需了解更多，请联系：



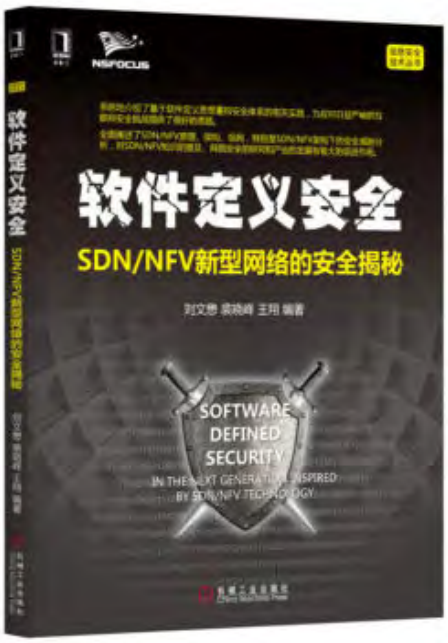
特别声明

为避免客户数据泄露，所有数据在进行分析前都已经匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

版权声明

目录

图表索引



本白皮书的作者之一，也参与了绿盟科技与华为的相关合作项目，并合作编撰了《软件定义安全》一书，概述系统的介绍了基于软件定义思想重构安全体系的相关实践，为应对日益严峻的互联网安全挑战提供了很好的思路。

一. 前言

2015 年绿盟科技发布了《2015 绿盟科技软件定义安全 SDS 白皮书》，阐述了软件定义安全的起源与发展。那么 2016 年业界在软件定义安全领域发生了什么变化，又有什么新的动态呢？本文将以去年的白皮书作为背景，重点阐述了 2016 年软件定义安全这一理念在行业内的发展情况，以及具体在落地过程中的实践。

软件定义安全本质上是一种理念，即数据与控制分离，安全管理与控制集中化，从这个意义上看其与所在环境关系不大。在《2015 SDS 白皮书》中，我们主要关注面向云环境的软件定义安全，是因为软件定义安全的理念可能最早会在云计算系统的安全防护中得到体现，原因有如下 4 点：

1. 云计算系统具备开放的应用接口（Application Programming Interface，API），安全控制平台容易与云平台对接，获取或操作云计算系统的资源，这使得安全控制平台做较少的定制，就可以演化为一个面向云环境的安全运营中心（Cloud SOC），支持面向云租户的各种安全应用；
2. 云平台借助虚拟化技术，具备了敏捷、弹性的资源池能力，可以快速准备好（Provision）虚拟化的安全设备，也可灵活地调度底层的为安全功能服务的计算、存储、网络资源，为安全功能服务；
3. 软件定义网络（Software Defined-Networking，SDN）近年来变得越来越热，很多云计算系统在规划时就加入了对 SDN 的支持，有些在实施时已部署了具有 SDN 能力的软硬件基础设施，具备了快速调度南北向和东西向流量的能力，为安全应用调整安全防护策略提供了更便捷的手段，为云环境中可实现的安全功能提供了更大的想象空间；
4. 使用云计算的租户很多是中小型企业（Small and Midsize Business，SMB），不具备规范的安全管理流程和专业的安全运营水平，无法制定完整的防护方案或管理复杂专业的安全设备。这些用户在安全方面的投入往往是防护目的驱动，而非合规性，这样会更关注安全防护系统的有效性、便捷性和灵活性。软件定义安全、安全即服务（Security as a Service，Sec-aaS）天然地匹配到了这些用户的需求。

需要明确的是，软件定义安全与云计算安全无论从逻辑上还是架构上都没有必然的联系。软件定义的安全方案同样也可以部署在传统 IT 环境，如果能做到开放接口，通过软件驱动底层安全设备，通过软件编排上层应用，那么这套安全防护体系也是软件定义的。相反，即使在云环境中部署了大量的安全机制，但如果仅是简单堆砌，那并不是软件定义安全。

本篇白皮书仍会重点讨论软件定义安全体系在云环境中应用，着眼于其落地交付过程，此外也会讨该体系在 BYOD、传统 IT 环境等场景可能的应用。

二. 背景

2016 年即将到尾声，当盘点业内安全资讯时，我们发现存在两个不同的趋势：

一方面，网络安全已成为国家战略，习总书记在 4 月 19 日在网络安全和信息化工作座谈会上的讲话 [1]，作出了重要论断：“没有网络安全就没有国家安全，没有信息化就没有现代化”，充分强调了网络安全在国家层面的重要性。11 月 7 日，全国人大通过了《网络安全法》，使得惩治网络空间领域的不法行为成为有法可依。

但另一方面，互联网上的安全事件不减反增。著名的数据泄露分析报告 Verizon DBIR[2] 在 2015 年的报告中，收集了 2122 起已确认的数据泄露事件，而在 2016 年的报告中，这一数字上升到了 3141 起，其中 89% 的数据泄露是经济利益或间谍驱动，这一观点在今年一系列针对银行 SWIFT 系统的攻击事件中得到验证，其中孟加拉央行因此造成了约 1 亿美元的损失。在间谍驱动方面，安天实验室发布了《白象的舞步：来自南亚次大陆的网络攻击》APT 报告，曝光了过去四年来自南亚具有国家背景的定向攻击，目标主要针对中国高校和其他机构。绿盟科技研究院也在去年协助客户处置了针对金融行业内多家机构的高级定向威胁。

可以说，这是一个最好的时代，网络空间安全受到了空前的重视；也可以说是一个最坏的时代，安全厂商在客户侧部署了层层安全机制：访问控制、入侵检测、身份认证、可信计算、安全管理平台（Security Operations Center，SOC）、安全信息与事件管理平台（Security Information and Event Management，SIEM）、威胁情报平台，每年都在提新的防护理念，每年都在发布新的防护产品，但依然挡不住恶意攻击者的黑手。

Gartner 的分析师提到，北美企业从安全事件发生到最终修复漏洞平均花费两周（这个数字在中国很可能更长），而攻击者从发动攻击到窃取数据往往仅需数小时。部署的安全机制不能说无效，因为在威胁发生时，安全机制第一时间捕获到了异常，例如入侵防御系统 (Intrusion Prevention System，IPS) 确实产生了告警，系统漏洞扫描系统确实报告了漏洞，流量分析系统也确实发现了异常的访问模式，但是安全管理员需要从大量的安全日志中寻找这些有用信息，如果不能有效关联起来做智能化的分析决策和自适应防护，那只能是“管中窥豹”、“盲人摸象”，不知道攻击者采

取的战术和战略，也无法了解攻击者的真实身份和意图。

要抵御日益复杂的攻击，就要求安全机制在攻击者试探、投放载荷时能够感知到异常，在攻击者得手前及时响应、阻断和隔离，甚至在攻击者开始尝试时就能预测。只要阻断攻击链的其中一环，就能挫败攻击者最终的窃取数据或破坏系统的目的。要做到以快对快，在小时级抵御攻击者的恶意行为，需要以下必备条件：

1. **连接协同**，有机结合多种安全机制，实现协同防护、检测和响应；
2. **敏捷处置**，在出现异常时进行智能化的判断和决策，自动化地产生安全策略，并通过安全平台快速分发到具有安全能力的防护主体；
3. **随需而变**，当一个安全事件爆出后，攻击者的攻击方法更新很快，以绕过防守方的安全机制，那么就要求防护者能紧跟甚至超过攻击者，以快制快，在数据泄露的窗口期内阻止攻击者。

现在业界的安全防护有两种思路：纵深防御和软件定义安全。这两种思路并不矛盾，而是有益的互补。纵深防御是根据安全需求，部署多种安全机制，层层防护，使得攻击者不能一击得手；软件定义安全则根据统一的安全需求，分析上下文安全状态，并据此做出正确决策，并通过安全策略统一驱动底层的安全资源，使得安全机制快速生效。

纵深防御不是简单地将多种安全设备或安全机制进行堆叠，软件定义也不是简单地开发几个安全应用、开放几个设备接口。应该将这两种机制根据实际场景进行有机结合，才能实现良好的防护效果。一方面，根据安全需求开发安全应用，部署相关安全机制，这些安全应用可以从安全管控平台侧获得安全设备的日志、告警，进而做出决策下发到安全设备，使得安全设备摆脱单打独斗、一一被绕过的局面；另一方面，借助虚拟化、软件定义网络等技术，安全应用可以按需部署虚拟化的安全设备，并且将流量灵活地依次调度到这些检测或防护设备，做到随时可以灵活调整的纵深防御，攻击者就不能使用一套攻击模式持续得逞，增加其攻击成本。

三．“软件定义”之百家论

软件定义安全是一种理念，业界有很多研究机构、企业借鉴了这种思想，依托软件定义的内涵，提出了自己的安全模型、架构、技术和标准，很多都体现了软件定义的内涵。我们在此列举若干，供读者参考。

3.1 自适应安全

Gartner[1] 于 2016 年提出了“自适应安全”（Adaptive Security）的防护模型，其核心思想就是不再假设防护（Protection）能实现万无一失的安全，这也是因为 Gartner 的分析师们注意到很多大企业尽管购买了很多安全产品，部署了完备的安全机制，依然发生了数据泄露和恶意攻击。可见，以往重防守、堆设备的建设思路已然不能抵御复杂攻击。

自适应安全强调了检测、响应和预测的能力。企业安全团队在检测到企业业务中断或系统遭到破坏时，应快速恢复信息系统和相关业务；当发现存在恶意攻击时，应及时隔离（Contain）和阻止恶意攻击，避免重要数据外泄。企业在构建自适应安全应遵循以下原则：一方面，要将安全策略贯穿防护、检测、响应和预测四个阶段，如图 3.1 所示；另一方面，在每个阶段要结合多种手段，例如在检测阶段需要检测事件、对事件进行确认、优先级排序，以及相应隔离；在响应阶段需要修复、对事件进行取证等。

图 3.1 自适应安全模型

1 http://www.gartner.com

Gartner 将“软件定义安全”作为 2014 年的十大信息安全技术之一，又将“自适应安全”列为 2017 年十大技术趋势之一，这两种安全防护思路都非常重要，也有一定的内在联系。Gartner 将软件定义安全作为平台革命，在 7 月发布的《2016 年新兴技术成熟度曲线》报告中，软件定义安全在成熟度曲线上已经有明显的移动，越过了成熟度曲线的最高点。对此，报告的评论是“安全供应商继续将更多策略管理从个别硬件元素移动到一个基于软件的管理平面，以便保证指定安全策略的灵活性。因此，软件定义安全为安全策略的执行带来速度和敏捷性”。可见，“软件定义安全”是实现“自适应安全”的支撑体系，只有当检测、防护的各类安全机制快速、有效地协同，才能及时发现和解决安全事件；而“自适应安全”是“软件定义安全”的一个编排原则，指明了如何使用各种安全能力解决企业遇到的现实问题。

在国内的实践方面，绿盟科技于 2015 年发布“智慧安全 2.0”的战略目标，意在实现自动化的安全产品闭环和安全专家运营闭环，贯穿了自适应安全的四个阶段。在产品化方面，以自研的安全管理平台（ESPC/SOC）为基础，不仅可以控制自有数十款安全产品，还支持对接第三方厂商的安全产品；同时与云服务商合作，与云管理、控制平台进行适配，向最终云用户交付易用、快捷和专业的安全应用。此外，青藤云 [2] 作为一家创业公司，从一开始就将自适应安全作为其目标，提供了自适应的安全平台，为互联网企业提供精确智能的安全服务。

3.2 自动化应用编排

自适应安全模型可以软件定义安全为支撑体系，利用北向应用编排机制进行安全资源和策略的灵活调配，实现多种防护手段的协同运作。

在 2016 年 RSA 大会的创新沙盒竞赛中，Phantom Cyber 公司展示的自动化应用编排系统 [3] 得到评委的青睐，获得了优胜奖；在 2016 年 2 月 29 日，IBM 安全收购了安全事件响应公司 Resilient Systems，以强化其弹性的灾难恢复服务。这两家公司的技术特点有不少相似性，具有软件定义安全的特征。

Phantom 认为在存在大规模攻击的场景下，会有大量的日志、告警输出，通过人工检查的方式很难发现问题，即便发现问题也很难快速解决。于是 Phantom 从应用层入手，构建自动化、可编排的安全应用体系。图 3.2 是 Phantom 的架构，它支持多种数据源和主流的 SIEM 平台，如 Splunk、Qradar 等；同时，可以让安全管理团队编写脚本 Playbook，调用相应的安全服务，实现安全运维自动化。

2 https://qingteng.cn/

3 https://www.phantom.us/product.html

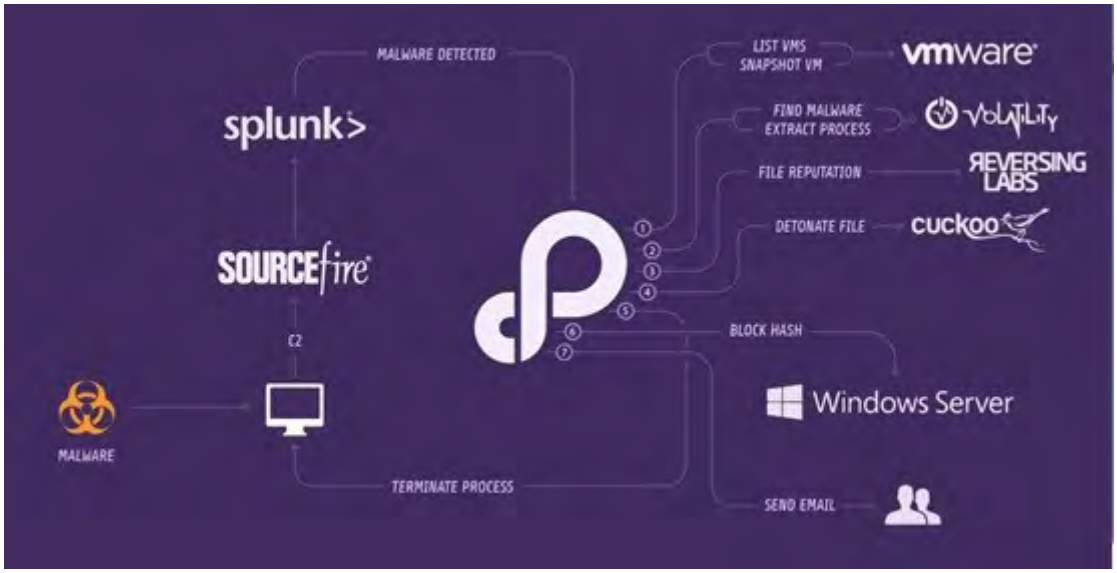


图 3.2 Phantom Cyber 的架构

Resilient Systems[4] 则通过对事件调查和响应的流程进行建模，建立了一套灵活的事件处置机制。通过软件化的设计，可以调用邮件、报表和 ticketing 系统将以前需要人工、低效、没有可视度的处置流程变得更加优化，大大缩短了安全事件处置的整体时间。

3.3 零信任 / 微分段

在安全机制的实现层面，软件定义安全的安全控制平台进行集中管控，以统一的策略控制全局的安全资源和规则。以安全设备为中心的固定边界防护和内部区域信任的传统防护思路将会发生变化，一个明显的现象是近期零信任和微分段等技术路线的兴起。

2015 年 Google 发表了一篇介绍其内网安全计划 “BeyondCorp” 的文章 [5]，内容大致是废弃防火墙。乍看出乎大多数人的意料，似乎 Google 抛弃了网络边界，也就放弃了内网安全；但细看内容，其实 Google 通过该计划彻底打破内外网之别，通过统一的访问控制引擎，管理不同用户对不同资源的访问，而不将用户和资源的位置作为决策依据。

硅谷创业公司 Skyport Systems[5] 也是为企业计算基础设施提供高效的访问控制系统。按照传统建立边界思维，攻击者在进入系统内部后就容易进一步攻击内部其他重要资源，而 Skyport Systems 提出的逻辑是，所有的资源都是零信任，即便内部某资源被攻破，从该点作为跳板进一步攻击也是困难的。通过软件定义的访问控制的理念，做到 “零信任” 条件下各处的访问控制策略快速调整。

此外，云安全联盟（Cloud Security Alliance，CSA）[6] 也提出了软件定义边界（Software Defined Perimeter，SDP）的标准，在企业内网中，可通过集中式的 SDP 控制器，对任意主客体之间的访问做

4 https://www.resilientsystems.com/
5 https://www.skyportsystems.net/
6 https://cloudsecurityalliance.org/

到一致、高效的控制。通过 SDP 标准所定义的架构，可实现 Google BeyondCorp 和 Skyport Systems 所要达到的目标。

在虚拟化场景中，VMWare 提出了微分段（Micro-Segmentation）[7] 的概念，可根据用户策略，灵活地将东西向的任意虚拟机组成区域，在这些边界间部署访问控制的规则。正是因为分段粒度、规模和策略都可以通过应用可调，所以 Gartner 也称之为软件定义分段（Software Defined-Segmentation）[6]。

上述访问控制的项目、标准和产品的实现方式各有不同，但它们的出发点类似：通过软件化、集中化的访问控制应用，实现事前零信任；通过软件定义实现全局一致、无死角的安全访问控制。

3.4 体系标准化

软件定义安全是一种理念，强调安全控制与数据分离，但同时也是一种可实现的架构，强调的是安全应用、安全控制平台和安全设备。要实现这样的架构，就要求安全控制平台能够打破厂商锁定，通过一个安全策略就能驱动不同厂家的对应安全产品。

国外的安全生态体系较为成熟，安全产品或服务多有应用接口，如 RESTful API、公开的命令行界面（Command Line Interface，CLI）等控制或配置接口，所以 Phantom Cyber 可以自行提供适配第三方厂商的驱动，最后完成更高层面的编排。用户只需编写一段通用的脚本就能实现某个安全功能，而不需要关心底层安全产品如何工作的。如果这些厂商的产品得到广泛应用，就有可能形成事实上的安全北向标准。

相对而言，国内的安全体系建设困难一些，不同厂商的安全产品对外很少提供应用接口，即便提供也是互不兼容或不公开。随着软件定义安全的兴起，分离安全数据和控制平面的原则也对控制平面的南北向 [8] 接口的开放性和标准性提出了要求。目前在南向接口标准化方面，可以看到大致分为四类：设备基本信息获取、配置操作、安全策略管理和日志告警上传，这都是比较通用的功能点。但由于每类安全设备的功能不同，所以其下发策略的应用接口都会各有不同。比如防火墙的安全策略主要是访问控制，入侵检测系统的安全策略主要是数据包载荷的匹配规则，而每类安全设备的策略语义则应该是相似的，所以一种合理的思路是针对相同安全功能的设备制定规范或标准。目前国内一些运营商研究院正在从事这方面的研究和原型开发。

能体现软件定义安全理念的业内相关工作还有很多，限于篇幅不在此展开，可以看到这一先进的理念正在得到大家的关注和重视，预期明年还会有更多具有影响力的成果。

7 http://www.vmware.com/radius/micro-segmentation-vmware-nsx/

8 南向接口是指实现安全控制平台与安全设备之间协议的应用接口，北向接口是指安全控制平台与安全应用之间协议的应用接口，下同。

四 . 安全编排：一切防护皆软件定义

4.1 应用编排：软件定义安全的灵魂

如果说软件定义安全与以往的安全架构有什么区别，那么最大的不同应该是它体现的软件化、自动化和随需而变的敏捷性，而这些特性都是通过面向不同场景的安全应用所体现的。

安全应用是以软件形态交付的，如 Web 应用、脚本或是后台守护进程等。通常每个安全应用实现一个或若干个安全功能，如 Flow 异常分析、系统脆弱性评估、用户和个体行为的画像。但在软件定义安全的设计中，安全应用对外提供可编程的应用接口，如 RESTful API、Web Service 接口、消息队列和管道等中间件接口，那么在一些复杂的场景中，可以存在更上层的安全应用，通过调用一系列其他应用的应用接口，快速有逻辑性地完成多种安全功能。

以用户行为画像为例，首先，**网络流量分析应用**可先通过对收集到的流量进行格式化、建模，建立正常访问基线；然后，**资产分析应用**评估出企业的重要资产，结合企业已有的 ERP 和 CRM 系统的 API 获得员工身份信息；接着，安全审计应用获得安全设备上传的实时日志；最后，UEBA（User and Entity Behavior Analytics）应用将上述多维度的信息和访问记录还原成可理解的用户和个体行为，从而找到如离职员工访问内网的数据库等异常事件。

可以说，安全应用的可编排特性是软件定义安全的灵魂，原因有两点：

1）安全业务的逻辑可被软件定义

安全应用提供了应用接口，也就具备了被外部软件重新定义其执行逻辑的能力，从而发挥更强大的作用。一个脆弱性评估应用不只用于日常的合规性巡查，还可成为企业安全检测 - 防护 / 修复 / 响应 / 取证的闭环中重要前导部分。这个应用与防护 / 修复应用编排，可以衍生出日常漏洞处置的应用；这个应用与响应应用编排，可以衍生出如爆发突发安全事件时打虚拟补丁的应用；这个应用与取证应用编排，可以衍生出重大安全事件出现后的快速排查应用。随着安全需求越来越多样性，安全业务的逻辑可被软件定义，企业所拥有的安全能力会越来越丰富。

2）安全应用本身可以被软件定义

如前所述，安全应用本质上与其他通用应用没有区别，都是软件形态

的。在网络上提供服务的安全应用其实就是软件即服务（Software as a Service，SaaS），其部署、升级的过程都应该可通过平台即服务（Platform as a Service，PaaS）的应用接口被软件定义。近年来随着如 Docker 等 PaaS 技术的成熟，这些应用的部署可以不考虑底层的硬件环境（Baremetal、专用硬件或预装操作系统的客户服务器），其运行环境一致可靠，同时应用的升级也可以做到实时、增量、可控。

当然应用编排也存在一些问题，例如应用对外提供的应用接口没有通用标准，这也需要安全行业的厂商一起协作，开放自有的接口，并制定统一的规范，形成良性的生态。

4.2 在线商店：交付革命

互联网自诞生伊始就在深刻地改变世界，“工业 4.0”、“物联网”、“O2O”、“BYOD”这些流行词都是互联网与工控体系、嵌入式系统、百姓日常生活和企业办公等场景结合后诞生的新模式，可以说互联网的敏捷、开放和丰富的资源给这些传统事物带来了新的变革。

软件定义安全本质是借助应用的灵活逻辑实现安全方案的“软化”，那么这些应用从何而来，这些应用的逻辑因何而变？在软件定义安全发展到应用成熟的阶段，这些问题就会被提出。

可预见到，软件定义安全的体系与互联网结合几乎是必然的。没有互联网支撑的应用交付，任何精妙的安全体系终究会落后于日益变更的业务系统，或败在日益变化的攻击手段。安全应用（Security APP）会演化成安全即服务，使得安全应用时刻处于最有效和最新的状态。从这个角度看，提供安全平台即服务的在线商店（Security APPStore）的概念也是顺理成章。

应用商店有以下优点：

1）应用交付便捷快速

设想现在的安全产品交付过程，用户首先需要通过销售了解产品功能介绍，与售前人员沟通后，根据需求确定部署方案，以及产品规格和配置，然后下单购买。根据库存和生产情况，通常经过数周到数月产品才能到货，厂家再安排工程实施人员布线、加电、配置和调试，此时宣告交付完成。如果运行时遇到硬件故障等无法解决的问题，还需要退换货，通常又要花上数周甚至数月的时间。这里还不涉及人工的例行系统更新和遇到安全事件时的紧急补丁应用的开销。由此可看出传统模式有三个问题：时间开销大；售前售后人员成本高；运维难度高、受人员素质影响大。

如果安全应用通过在线应用商店交付，客户可以浏览、搜索在线应用，找到感兴趣的应用，即可点击试用或购买，如图 4.1 所示。

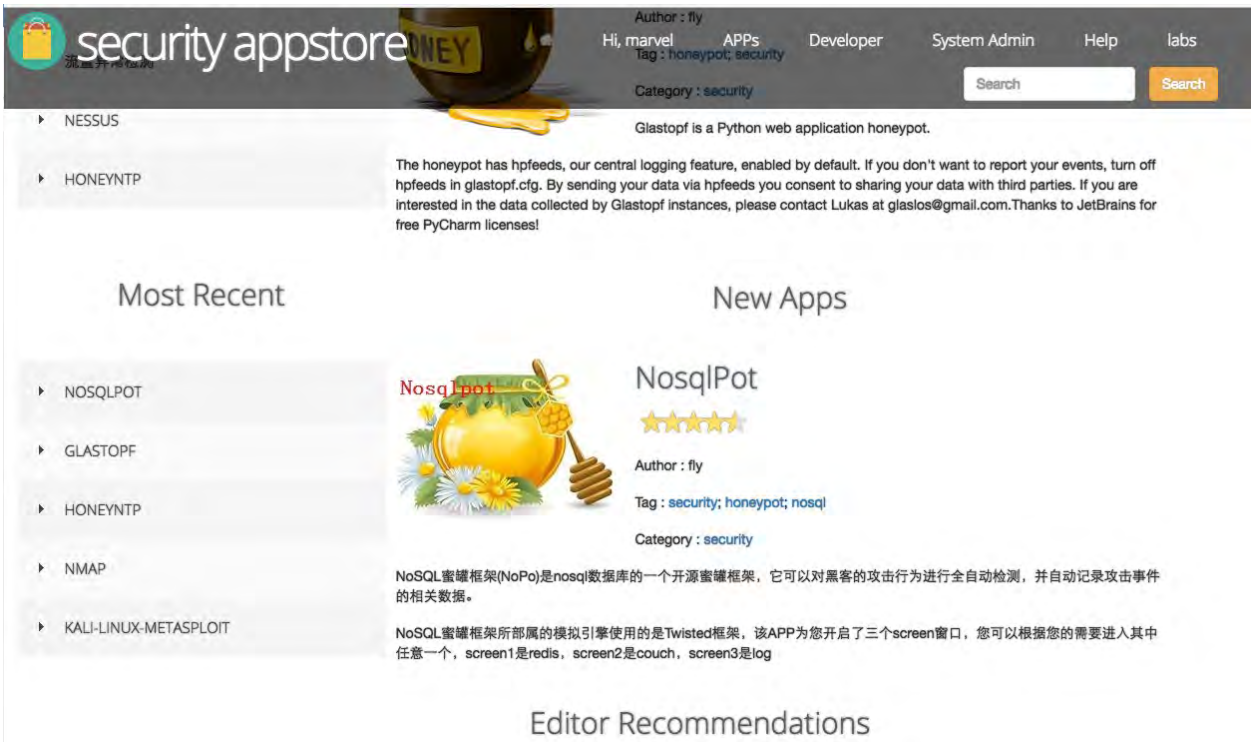


图 4.1 安全 APPStore

通过这种方式，安全应用可很快下载并部署到客户环境的服务器上，整个过程通常在分钟到小时级，如图 4.2 所示。因为应用的研发和运行环境一致，所以应用下载之后就能正常运行，节省了大量配置的时间开销。

应用更新也是类似，通过增量更新的方式，花费时间更短。可见这种方式大大缩短了安全应用交付、部署和运维的时间开销。

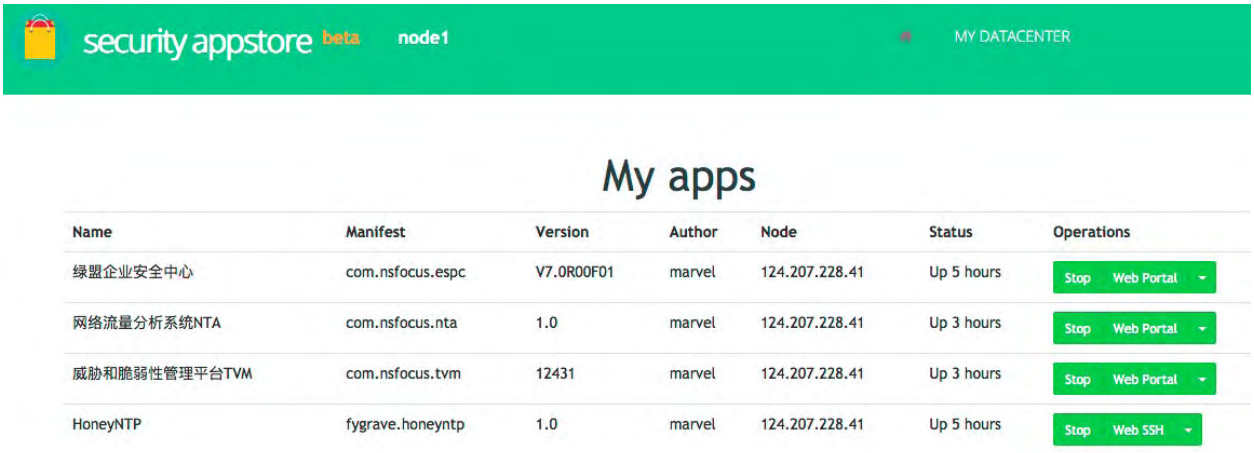


图 4.2 客户端部署的安全应用

2）应用研发成本低

应用商店中的安全应用通常是面向行业客户通用的需求研发的，所以面向的场景是相似的。尽管不同客户业务环境存在一些差异，但技术上采用容器化等 PaaS 技术，每个安全应用都是标准化的，从研发、调试到客户侧部署，其运行环境、软硬件配置、依赖关系没有变化，即插即用，避免了大量定制化的方案制定和工程实施开销，而且整体的运行稳定性也能得到保证。

标准化加 SaaS 化的云端应用商店，大大降低了交付的边际成本，因为购买 1 个应用的成本与购买 100 个应用的边际成本几乎相当，节约了大量的人工成本。

安全应用商店这种模式不仅为客户提供了时间、产品质量等方面的良好体验，还降低安全厂商的成本，提高了生产效率。

此外，应用商店也可构建一个安全生态，容易通过标准的方式规定应用的规格和接口，从而实现 4.1 节中的应用编排，进一步强化了已有的安全能力 [9]。

9 事实上惠普公司也推出过面向 SDN 应用的应用商店，足以见得它在 SDx（Software Defined Everything）发展的必然阶段。

五 . 资源池：按需而变的安全能力

如 3.1 节中所述，Gartner 将软件定义安全移至技术成熟度曲线最高点右侧，也就是幻想破灭期，这表示其愿景虽好，但在应用中会遇到很多困难，迫使人们对其态度更加趋于实用。事实上，在国内的一些云安全的实验性项目中，我们发现研发和运营一个软件定义的安全系统是有难度的。经过了一系列的实践，我们发现安全资源池（Security Fabric）是实践软件定义安全理念一个比较好的途径。

5.1 理想主义的困境

“软件定义”有敏捷、高效和开放等诸多优点，一个系统达到可以被软件所定义的程度显然是一种理想状态：软件定义网络 SDN 是网络运维的理想目标，软件定义数据中心（Software Defined Data Center，SDDC）是云计算的理想目标，软件定义安全 (Software Defined Security，SDS) 则是企业安全体系的理想目标。软件定义安全可能最早会在软件定义数据中心，特别是各种云计算信息系统中部署。因为软件化的安全体系与虚拟化、SDN 化的云环境可以天然地互补：借助虚拟化的安全产品和 SDN 化的流量引导，安全平台很容易快速具备安全防护能力。

但从另外一个角度看“理想状态”，往往意味着实现这个目标不会一帆风顺。据笔者观察，近两年一些公司部署面向云计算的安全解决方案已经有软件定义的特性了，但这些方案的落地却并不容易。原因有很多，其中最本质的因素是安全始终是要适应业务系统，而大部分云计算系统在开始设计时就没有充分考虑到安全因素，造成这些系统与安全厂商集成时困难重重。即便是如 VMWare 和 Palo Alto[10] 这样的业界先进的虚拟化平台厂商和安全厂商也遇到了诸多问题，VMWare NSX 中安全防护的 API 历时良久才于今年发布。

具体来说，安全厂商的解决方案在云平台落地有如下问题：

1. 安全产品的虚拟化及适配云平台 Hypervisor 较为困难。出于性能考虑，很多安全产品都会对网卡等设备做优化，如果云平台的 Hypervisor 不提供兼容的方案，那么这些安全产品即便虚拟化后，也无法直接运行在 Hypervisor 上。又如，有些需要工作在透明模式下的安全产品需要多块网卡连接到同一个虚拟子网且不带网络

10 https://www.paloaltonetworks.com/

地址，这在如 Openstack 环境下是不被支持的；很多云平台不支持虚拟实例启动时挂载多个硬盘，也导致一些安全设备无法正常启动。

2. 安全设备的证书体系在云平台中不能直接适用。安全厂商为了控制安全产品的知识产权不外泄和安全服务的有效期，往往会通过一些认证和授权机制（如证书验证等），以保证安全产品能够正常工作。但是在云环境中会有一些变化，传统加密狗等硬件证书的方式在虚拟机随时生成销毁的虚拟化平台下就变得低效不可用；另外，同一类的虚拟化安全设备都是从虚拟镜像启动，这些虚拟安全实例之间本质上是相同的，彼此无法区分，如果使用虚拟机的硬件参数（如网卡物理地址），又依赖于云平台不能事先颁发，故也对证书分发和验证造成了困扰。
3. 安全方案无法控制云平台的内部流量。正如第一点中提到，很多主流云平台在设计伊始就没有考虑到安全运维时对网络控制的需求，没有提供可控制内部虚拟网络流量的应用接口，即便部分提供商有 SDN 方案，但没有考虑到安全防护所需要的相关流量控制操作，所以安全方案很难利用云平台自身的接口将内部流量做调度到安全设备做进一步处理。

上述三个问题，都与云服务商的平台相关，试想安全厂商如果与一家家云服务商适配，势必投入巨大的精力，边际成本极高，事实上也产生了“合作厂商锁定”的问题。结果就是安全厂商因为技术上的限制很难将安全方案完整地部署到云平台上。如果安全方案难以部署，软件定义的先进理念就无法变成实现，各种理想目标也就无从谈起。

5.2 资源池：打通最后一环

可以说，突破云环境中的虚拟化系统和网络控制体系的限制是实现云中软件定义安全的最重要一环，如何打破这个僵局，各家厂商也是八仙过海，各显其能。但有意思的是经过两年左右的探索，主流厂商都提出了基于安全资源池的方案，可见技术发展有其必然性。

虽然很多厂商提出的安全资源池是将硬件设备变成虚拟化实例，结合与云平台对接的管控系统，形成一个解决方案，但其目的只是将自身的方案应用于云环境。当然这些想法是合理的，不过这些面向云计算的原生资源池不是软件定义，而是厂商的无奈之举。

我们发现软件定义安全同样也需要资源池：控制平台通过安全应用的策略体现出处置的智能度，通过资源池体现出处置的敏捷度。软件定义的安全资源池可以让整套安全体系迸发出强大的活力，极大地提高了系统的整体防护效率。

还是以 4.2 节中提到的产品交付为例，通常用户需要花上数月做预算准备，并再花上较上一段时间做产品购买、部署和上线的准备。但是当发生新的攻击时，现有的安全防护手段在短时间内无法有效防护。例如某 Web 站点的客户采购了一台 WAF 做 Web 应用的安全防护，但如果出现大规模的拒绝服务攻击时，单台 WAF 就很难抵挡住攻击，此时部署新的设备已经来不及了。

但如果使用资源池的方式，安全厂商交付的虽然也是硬件设备，但里面的能力是软件定义的，如

果用户在应用商店购买了 Web 防护应用，就会在盒子中部署虚拟的 WAF，并配置好安全策略、网络流量导向等。如果出现流量型分布式拒绝服务（Distributed Denial of Service，DDoS）攻击，则可以在盒子里部署虚拟的流量清洗设备，与虚拟 WAF 一起工作；如果整体流量扩大时，可以对虚拟 WAF 做弹性扩容。

可见，软件定义的资源池对外体现的是多种安全能力的组合、叠加和伸缩，可应用于云计算环境，也可应用于传统环境，以抵御日益频繁的内外部安全威胁。当然，在云环境中，软件定义的资源池不仅可以解决云安全的落地，而且能发挥虚拟化和 SDN 等先进技术的优势，实现最大限度的软件定义安全。

5.3 资源池架构

与数据中心中的计算、存储和网络资源相似，各种形态、各种类型的安全产品都能通过控制和数据平面的池化技术，形成一个个具有某种检测或防护能力的安全资源池。

从架构上看，安全资源池处于软件定义安全的偏南位置，包括安全控制平台中的资源池化控制组件，以及数据平面上的多个资源池，如图 5.1 所示。

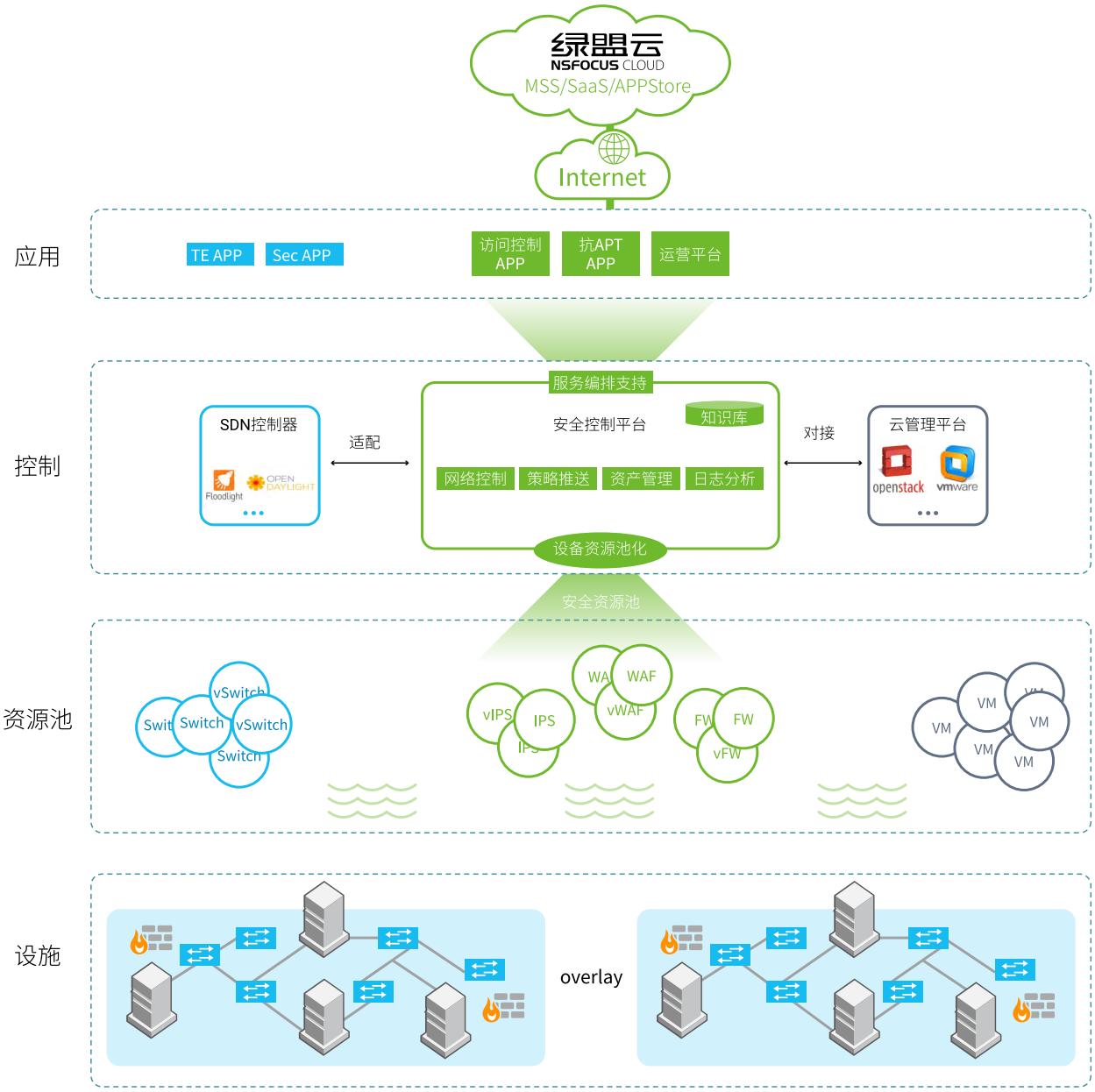


图 5.1 基于资源池的安全体系

这样，设备资源池化组件对上层提供了多种安全能力，如图中的 IPS 资源池提供了入侵防护的能力，WAF 资源池提供了 Web 防护的能力，防火墙资源池提供了访问控制的能力。资源池中的资源可以是厂商甲的，也可以是厂商乙的；可以是硬件安全设备，也可以是虚拟化的。只要这些资源提供标准的对外描述、管理和控制接口，就可以统一管控。

因而，安全应用可以根据控制平台的北向接口描述，动态调用这些能力，而无需关心到底是调用了谁家的安全设备或是哪类安全设备，更不用关心如何部署或配置这些设备。

目前资源池中的资源形态主要有如下四类，如图 5.2 所示：

1. 虚拟机设备形态，部署在客户的计算节点上。安全控制平台的设备资源池化组件借助云平台的 Hypervisor 和网络管理组件进行控制这些虚拟安全设备。这种形态的优点是不需要购置新的硬件产品，安全能力也可随着计算节点的规模弹性扩展，安全处理在计算节点内部避免了数据传输的时间和带宽开销，缺点是安全虚拟机需要适配多个云计算系统，比较困难。
2. 硬件内置虚拟机形态，技术路线与虚拟机设备形态很相似，安全设备也是虚拟化的实例，不同之处在于底层的 Hypervisor 是安全厂商可控的，处理性能和网络流量调度可以做得非常高效。
3. 硬件虚拟化形态，通过硬件虚拟化的技术，可以实现在一个硬件设备中虚拟出多达数千个虚拟系统，每个虚拟系统独立运行，可做到租户隔离。与 2) 相比，这种方式更轻量，以较少的硬件成本就能部署在大规模的环境中，缺点是单个硬件只能启动同一类型的虚拟安全设备。
4. 硬件原生引擎形态，这是一种将原有硬件设备加入资源池最简单的方式，主要是提供必要的应用接口支持，此外在一些 overlay 网络中，需要加入隧道管理和对数据包加解隧道头的功能。优点是不需要做太多改动，缺点是部署与网络拓扑有关，不能快速横向扩展。

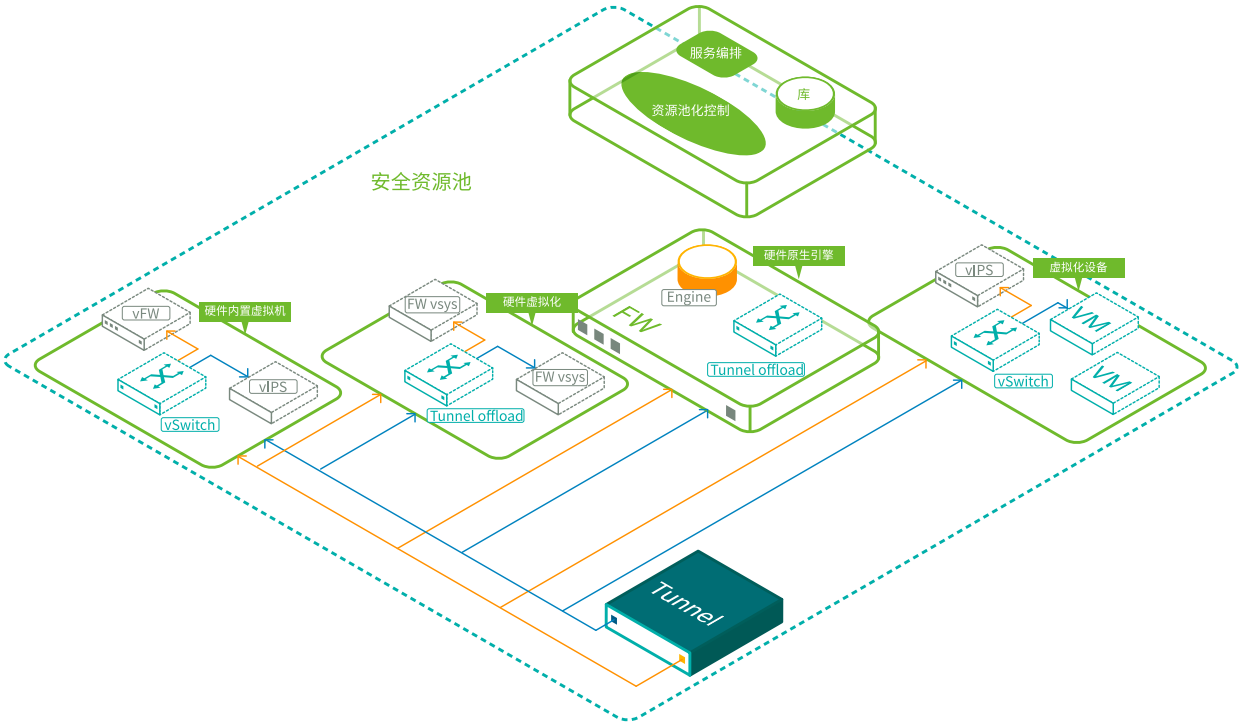


图 5.2 支持服务链的安全设备交付模式

其中形态 1. 交付的是镜像文件，形态 2. -4. 交付的是硬件设备，外部形态看似与传统的安全设备没有太多区别，但内部实现各有不同。随着技术的发展，除了上述 4 种外，很可能还有其他的形态的安全产品组成资源池，例如安全即服务。不过万变不离其宗，只要资源池化控制组件与资源池之间的应用接口保持一致，那么无论哪种形态的资源池，都能对外提供相应的安全能力。

图 5.3 给出了各种形态安全设备组成的完整资源池示意图。当安全设备以硬件存在的时候（如硬件虚拟化和硬件原生引擎系统），可直接连接硬件 SDN 网络设备接入资源池；当安全设备以虚拟机形态存在的时候（如虚拟机形态和硬件内置虚拟机形态），可部署在通用架构（如 x86）的服务器中，连接到虚拟交换机上，由端点的 agent 统一做生命周期管理和网络资源管理。

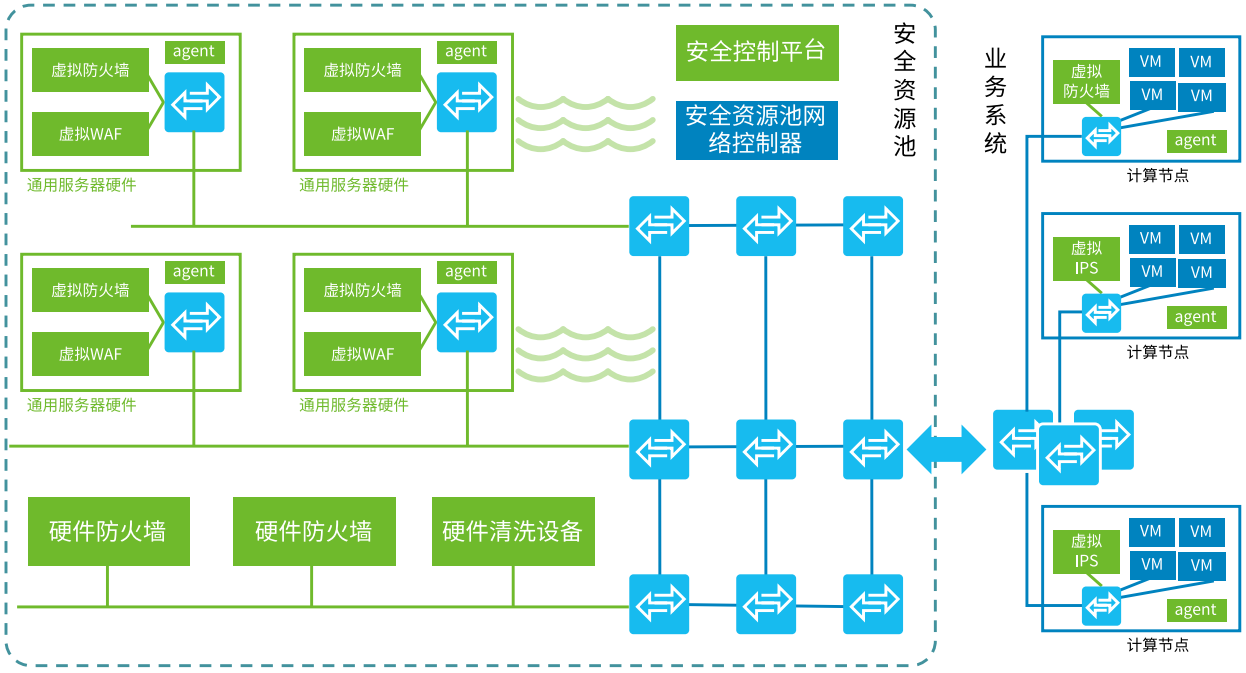


图 5.3 安全资源池示意图

在具体的项目中，可以根据业务系统的云平台和网络部署情况，选择合理形态的安全设备，构建出统一的安全资源池。例如，当安全性能要求较高时，推荐使用硬件虚拟化形态设备组成的安全资源池；当云平台的资源和应用接口存在较多限制时，在计算节点中部署虚拟化安全设备就很难实现快速复杂的防护功能。从实践来看，划分一块专用的计算、存储和网络区域作为安全资源池，在这个可控的环境中可以完成如服务编排、负载均衡、高可用等功能。

具体来说，专有安全资源池的数据平面由各类安全设备和支持 SDN 的软硬件交换机组成，形成了弹性的防护能力。资源池的控制平面由安全控制平台和网络控制器组成，两者通过松耦合分别控制专有区域内部的安全资源和网络流量，同时与业务系统的控制平面进行对接，实现域间流量互通。

根据租户业务特点，安全控制平台对安全资源、安全 / 网络策略进行统一管理，向上输出相应的

安全能力，使得安全应用不需要关心执行安全功能的是什么类型的设备、是哪台设备、在哪里部署，或是如何配置策略，极大减轻了安全应用与环境的耦合度；同时使得安全应用的编排效率大大提高。

根据安全策略需要，资源池的网络控制器对内部流量进行统一调度，从业务系统过来的流量进行分流、引流，到达某个或某些安全设备；进行相应处理后，再由资源池的网络出口输出。目前不少主流的 SDN 解决方案都支持这种网络 Fabric 的结构和功能。借助网络 Fabric 的能力，安全控制平台可以将流量调度到任意硬件或虚拟安全设备处置，还可快速建立、拆除安全服务链，使得安全防护方案灵活度大大提高。

安全资源池提供的安全能力可应用于多种应用场景，5.4 节介绍如何将资源池部署在云计算系统中，其中根据网络流量特征，又可分为处理南北向流量的资源池和处理东西向流量的资源池；5.5 节介绍资源池在传统的 IT 环境中中的部署。

5.4 云计算环境的安全防护

上节描述提到，云计算环境中存在南北向流量和东西向流量，资源池化的防护方案对这两种流量均可实现有效防护。本节将分别介绍这两种流量的防护方法。

1．南北向流量的安全防护

云计算环境中的南北向流量是指跨不同网络之间的流量，这些流量可以在路由器或三层交换机处获取到，所以可以将资源池部署在这些网络的交界点处理南北向流量。

南北向流量可分为两类：第一类是物理网络的边界流量，从物理环境进出虚拟云环境；第二类是虚拟网络间的边界流量，即从一个虚拟网络通过虚拟路由器进入到另一个虚拟网络中。

对于第一类物理网络的边界流量，可以采用由若干硬件设备组成安全资源池的方式，旁挂在数据中心入口处的路由器或三层交换机上，对物理环境进出虚拟云环境的流量进行处理。另外，在资源池内部可根据安全策略的需要，对各种安全应用进行按需编排，实现敏捷、协调、按需而变。

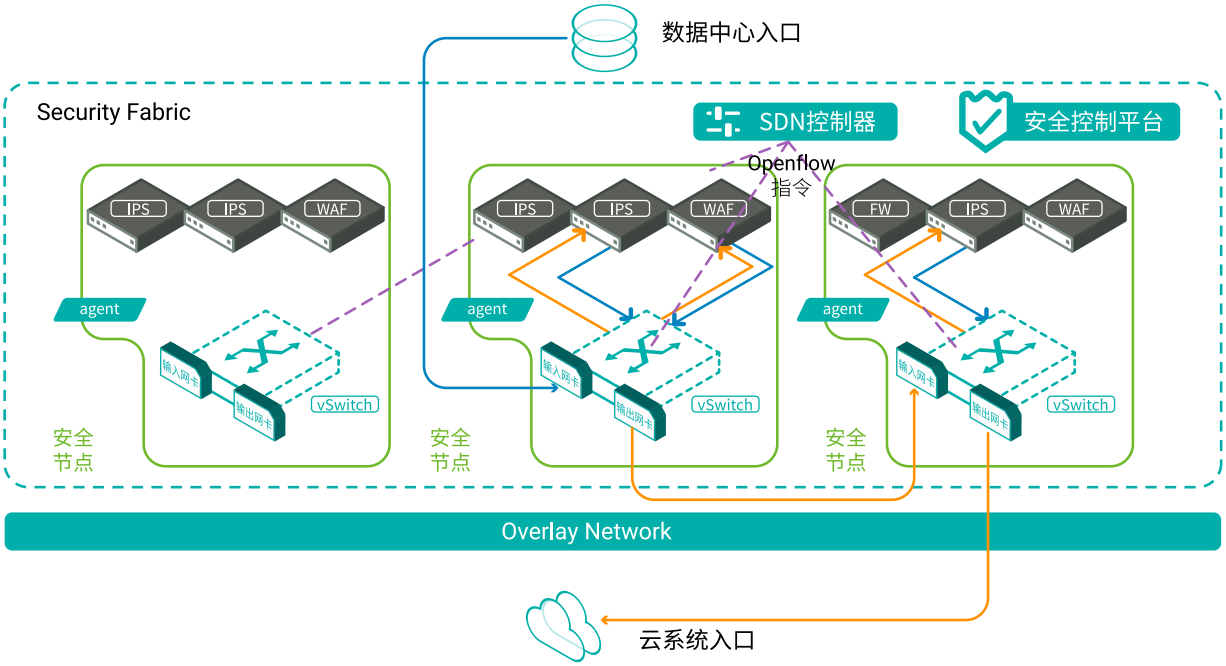


图 5.4 处理南北向流量的安全资源池部署方式

对于第二类虚拟网络间的边界流量，其安全资源池化方式可与前面的情形相同，但需要加入隧道管理和对数据包加解隧道头的功能，以解决虚拟网络间隧道式的流量问题。

2．东西向流量的安全防护

云计算环境的东西向流量存在于虚拟网络内部，对其安全防护可以采用上述多种方式的某一种或者多种混合的安全资源池化的方式，当然前提是这些安全资源都支持软件定义安全平台的 API 接口。

对于虚拟化网络，要将东西向流量引入安全资源池可采用以下两种方法：

1. 利用 SDN 网络技术，对支持 SDN 技术的虚拟交换机 / 路由器下发流表，将流量引入到安全资源池；
2. 在业务系统的计算节点内部，内置网络访问代理，通过配置网络策略可将需处理的流量由网络访问代理转发到安全资源池。

待安全资源池处理完毕后，根据安全策略配置，将流量转发到相应的目的节点。

与南北向流量防护类似，在对东西向流量做安全防护时，安全资源池内也可以运行各类安全应用，根据不同的安全检测、分析、响应、处置策略，进行灵活的安全业务编排，实现安全防护的协同、敏捷、按需而变。

需要说明的是，在云计算环境实现安全防护时还需要考虑多租户支持、安全应用间隔离的问题，可以通过虚拟化和 SDN 技术实现，在此不再赘述。

5.5 传统环境的安全防护

企业网络中部署的一般是传统安全设备，每个安全设备执行各自的安全功能，性能高但功能比较固定。当前企业面临快速、多变、持续性的安全威胁，亟需安全防护方案具有快速、强大、按需而变的能力，而这恰恰是传统单个安全设备所无法满足的。

此外更重要的是，从成本上看，要达到相同的性能，由低端安全设备、网络 Fabric 组成的安全资源池的成本远低于单个高端安全设备的成本。

当客户有较高安全性能需求时，安全资源池会成为一种很好的选择。而对于一般的 SMB 企业而言，即便没有很高的性能需求，但如果通过少数几个安全节点，就能输出丰富安全防护功能，而不需要购置独立单一功能的专有硬件安全设备，无疑也是有很大的吸引力 [11]。

事实上，基于软件定义安全而构建的安全体系也可以为传统环境的 IT 系统提供更强大、敏捷、智能的安全防护能力。具体实现方式与云计算环境中 5.4 节中南北向流量防护方案类似，这里不再赘述。

11 这种小规模资源池与 UTM（Unified Threat Management）不同，本身具备更多的检测和防护功能，还可以通过增加硬件（可以是客户自己的服务器）适应业务需求。

六 . 软件定义安全实践

本章介绍安全应用如何借助安全控制平台进行多种环境下的快速安全防护。

6.1 面向混合云和移动办公的自适应访问控制

随着降低办公和运营成本的需求越来越普遍，很多企业开始搭建私有云，也在尝试购买一些互联网上的基础设施即服务（Infrastructure as a Service，IaaS）（如阿里云 Web 服务器）和 SaaS（如 ERP 等应用），或者部署无线网络，鼓励员工携带自有手机、平板电脑进行移动办公。所以可预计，混合云和 BYOD 会成为未来几年企业 IT 环境常见的基础设施。

目前混合云常见的部署方式是通过虚拟专用网络（Virtual Private Network，VPN）等隧道技术将客户原有系统与云系统相连接，图 6.1 是一个典型混合云的 Overlay 网络，某企业拥有已建成的企业网络，同时作为租户 A 租用了某公有云的虚拟私有云（Virtual Private Cloud，VPC）。该企业网络的物理网关 / 防火墙（GW/FW1）通过 VPN 等隧道技术与公有云网关（GW/FW2）后的租户 A 虚拟路由器 / 防火墙服务 12 相连，云计算系统的物理网关防火墙（GW/FW2）跟云系统的管理网络和租户的虚拟网关 / 防火墙相连。

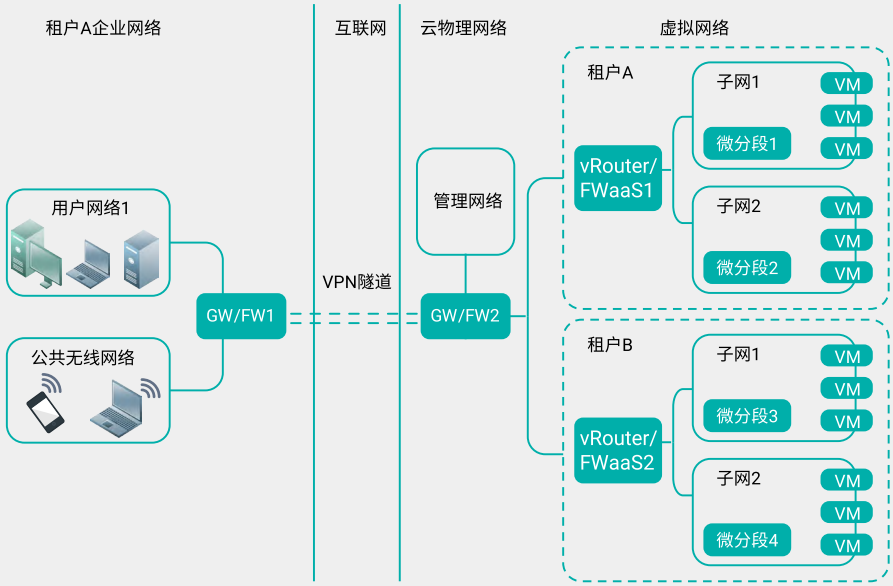


图 6.1 混合云的访问控制架构

12 不同云计算系统中的访问控制机制略有不同，本文以 Openstack 为例，虚拟网络中的防火墙为防火墙即服务（Firewall as a Service，FWaaS），下同。

在大型企业内部还会部署私有云，网络结构与公有云 VPC 类似，分支机构会通过 VPN 或专线接入数据中心的私有云。

企业网络中不仅包括办公网络，还有延伸到公司各个角落的无线网络。

员工在这样的环境中办公，访问的网络资源不仅仅限于内部网络（如私有云虚拟网络内部的服务器间通信），还存在于不同网络间（如在办公环境访问公有云的文件存储服务，在无线网络访问私有云的即时通信服务器）。随着企业规模变大和业务快速发展，通过管理员手动控制这些访问规则变得低效且容易出错。

通过软件化的方式，面向不同的网络环境可部署统一的访问控制策略，将用户企业网络的网关、云物理网络的网关、租户虚拟网关和租户虚拟子网微分段处的防火墙设置一致的规则：

1. 租户 A 的企业网络防火墙 FW1 与防火墙服务 FWaaS1 的规则应一致；
2. 企业网络防火墙 FW1 应与企业的 BYOD 认证系统关联，保证公共无线网络中的设备可提供相应身份，并仅能访问其已被授权的云端 VM；
3. 云计算数据中心的物理网络防火墙 FW2 应保证控制网络和数据网络的隔离，特别是严格控制互联网到云管理网络的流量；
4. 用户需根据业务划分相应的微分段，并通过 FWaaS1 和安全组控制自租户企业网络进出的南北向流量和不同微分段间的东西向流量，对如数据库 DB 等段的流量进行严格限制。

一般而言，可通过基于角色（Role-Based Access Control，RBAC）或基于属性（Attribute-Based Access Control，ABAC）等传统方法制定访问控制规则，但这些规则总体而言较为固定，缺少上下文感知，在发生威胁时无法快速调整控制规则。很多高级持续性威胁（Advanced Persistent Threat，APT）攻击的场景中，恶意攻击者通过社工或木马，获得了内部用户的身份，绕过了边界检查机制，从而能够访问内部资源。仅仅依靠访问控制列表（Access Control List，ACL）显然是不能抵御这些看似合法的攻击。

在云环境中攻击会发生在很短时间中，要想在攻击者达到目的前阻止其行为，就要求策略调整非常迅速：通过服务链，可以按需地在虚拟或物理位置部署各种深度包检测（Deep Packet Inspection，DPI）安全设备，根据上层应用的策略将流量依次牵引经过若干设备，当 DPI 设备发现可疑攻击时，通知防火墙或 SDN 平台实时隔离可疑流量，或调整服务链做进一步的检测或防护。

通过软件定义的安全控制平台，一方面安全应用可建立统一的访问控制机制，覆盖 BYOD、企业网络和云端虚拟网络的各处边界；另一方面可利用 SDN 和网络功能虚拟化（Network Function Virtualization，NFV）等服务链技术，动态根据上下文风险调整防护级别。

需要说明的是，概念上自适应访问控制关注的是访问控制策略的动态调整，我们将其放在软件定义安全实践中是因为这种策略的调整是可被软件定义的：用户只需聚焦于安全应用的防护策略，而不

需要关注底层负责访问控制的具体驱动，到底是网络设备通过流表实现的，还是防火墙通过安全策略实现的，或者是别的软件的 ACL 实现的。从实践来看，企业物理网络采用 SDN 技术可以极大提高策略的控制和调整粒度，实现全局实时的流量控制，而且越来越多的企业正在考虑部署 SDN 网络，所以在下面的案例中我们假定企业已部署了 SDN 网络。

整个系统的架构如图 6.2 所示，网络架构分为企业网络、互联网和云系统网络三部分。

其中，企业网络包括以下组件：

1. SDN 交换机，与部署在物理环境中的无线路由器桥接，并通过外部网关接入互联网，与云环境的租户虚拟网关通过隧道打通；
2. 认证服务器，企业网络中提供如轻量目录访问协议（Lightweight Directory Access Protocol，LDAP）、数据库等员工用户名密码的认证支持；

云环境网络是指部署在企业中的私有云或公有云的 VPC 系统，包括以下组件：

3. 租户虚拟网关，与企业网络通过隧道连接，同时为云环境的内部虚拟网络提供路由和三层访问控制服务；
4. 微分段，在虚拟子网内部提供二层访问控制服务；
5. NFV，防火墙、入侵检测系统（Intrusion Detection Systems，IDS）和其他应用层防火墙，提供 DPI 和行为层面的控制机制。

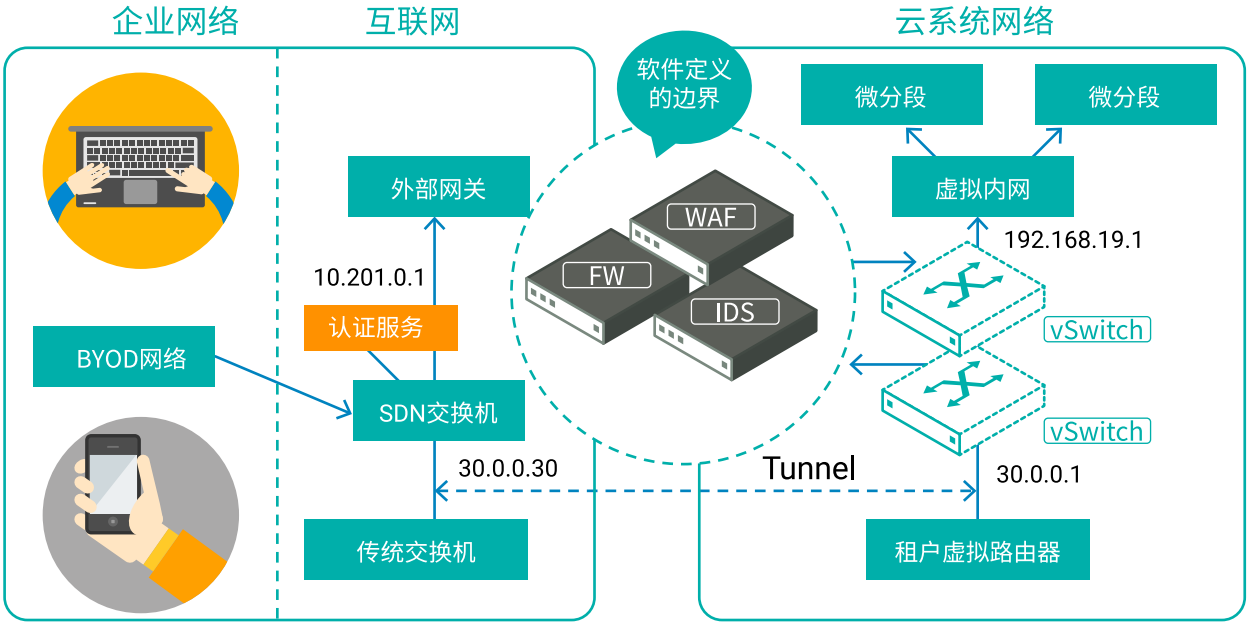


图 6.2 混合云与 BYOD 环境访问控制示意图

主要流程分为三个部分：

1. 用户认证，利用 SDN 技术将 HTTP 流量牵引到认证服务器上，实现全局网络上的用户接入认证；
2. 访问控制，在企业网络和云环境针对该用户部署统一的访问控制策略；
3. 自适应控制，通过服务链部署相应的安全机制，根据上下文调整控制策略。

在初始化阶段，SDN 控制器向 (1) 中 SDN 交换机下发以下 OpenFlow 流指令：

1. 允许所有 DHCP 和 DNS 的数据包；
2. 将所有 HTTP 的数据包牵引到 (2) 中认证服务器 auth.server；
3. 拒绝其他所有数据包。

运行时，用户连接上无线路由器后，通过浏览器访问任何 HTTP 网站，都会被重定向到认证服务器，后者通过将请求页面重写为认证页面，如原请求 http://www.a.com/hello.php?key=value 被改写为 http://auth.server/login?key=value。从而用户可以在该页面输入自己的用户名密码进行认证，理论上认证后端支持任何协议，所以可以兼容企业原有的认证服务。

在用户实现了认证后，安全控制平台在策略库中将该终端设为已认证，同时向云系统的防火墙服务下发允许该地址访问云中资源的规则，同时向企业网络的交换机下发以下 OpenFlow 流指令：

1. 将通过认证的用户终端发出的流量处理行为设为 action=CONTROLLER；
2. 之后该终端发出的数据包首次出现会送到 SDN 控制器，后者判断：

   2.1 如果目的地址为云环境的内网普通虚拟机，则允许通过，并根据安全策略将流量经过 (5) 中若干安全设备；

   2.2 如果目的地址为互联网，则允许通过；

   2.3 如果目的地址为企业内网服务器或云环境的内网重要资源，则根据认证用户的身份判断其是否有访问该资源的权限；

3. SDN 控制器将 2) 中处理结果推送到相关网络设备，后者可处理该流后续的所有数据包；
4. 通过 SDN 和 NFV 技术，根据访问类型按需在虚拟路由器后按需部署多种类型的防护或检测设备，组成服务链；
5. 根据上下文感知该终端环境的安全度，当 DPI 或行为分析引擎中的发现周围出现疑似攻击，安全应用则相应地将策略调严，将该策略转换企业网络交换机的流表或云中防火墙访问的规则，反之调松下发，实现自适应的访问控制。

上述访问控制与 Gartner 提出的自适应访问控制是一致的，如将 IDS 引入服务链可实现对数据包载荷的检测，将文件沙箱（如 NSFOCUS TAC）引入服务链可实现对文件运行时的行为检测，诸如此类。

当某种安全机制触发告警后，可调高当前的安全级别，对相关的访问控制做限制、隔离和阻断；反之亦然。

6.2 面向公有云的安全服务

公有云和私有云的安全需求有很大差异，所以对应的防护思路也是不同的。简单而言，私有云的安全聚焦于安全管理，管理员要考虑的一个重要安全需求是合规性，传统的安全机制也需要在私有云中有相应强度的部署；而公有云的安全主要集中在业务安全，用户考虑的重要需求是保证其对外提供的服务运行正常，以及采购安全产品过程的快捷性、使用安全产品的便捷性和整体防护流程的效率等。

所以，安全厂商在私有云的安全防护的方案中，提供（虚拟化）安全设备和安全管理平台为主，而在公有云的防护方案中，则以提供安全产品即服务（Security as a Service）为主。从安全厂商的角度来看，前者与传统的交付方式相似，但后者需要考虑到对安全了解不多的用户的使用方式，以及与云平台的各种对接，挑战更大。

在 2015 年的软件定义安全白皮书中，我们在“软件定义安全的实践”一章中，也单独列出了 Web 安全应用，其中给出了绿盟科技在融合 IaaS 和 SDN 的 Web 防护应用和一体化的 Web 安全应用两种场景中所做的工作。今年我们在一些公有云项目中，扩展了这些应用，提供了 Web 防护、Web 脆弱性评估、VPC 入侵检测等安全应用，这些安全应用基于安全控制平台，为公有云租户提供对内和对外的安全防护。用户可以通过云平台上快速开通并使用这些服务，在使用过程中，应用只提供易于理解的界面和功能，而安全平台和安全设备在后台将这些安全功能转换成了复杂、专业的安全规则。

例如，在 Web 安全应用中，用户只需要选择被防护站点，设置开启防护的功能，如图 6.3 所示。此时安全应用通过安全控制平台准备好了虚拟 WAF，并向该虚拟 WAF 下发防护策略，最后通过 SDN 控制器下发流表将流量牵引到虚拟 WAF。用户不需要关心如何布线、如何配置，在运维时只需登录安全应用即可获知网站当前的状态和防护的详情，如图 6.4 所示。

图 6.3 Web 安全防护应用 - 策略下发

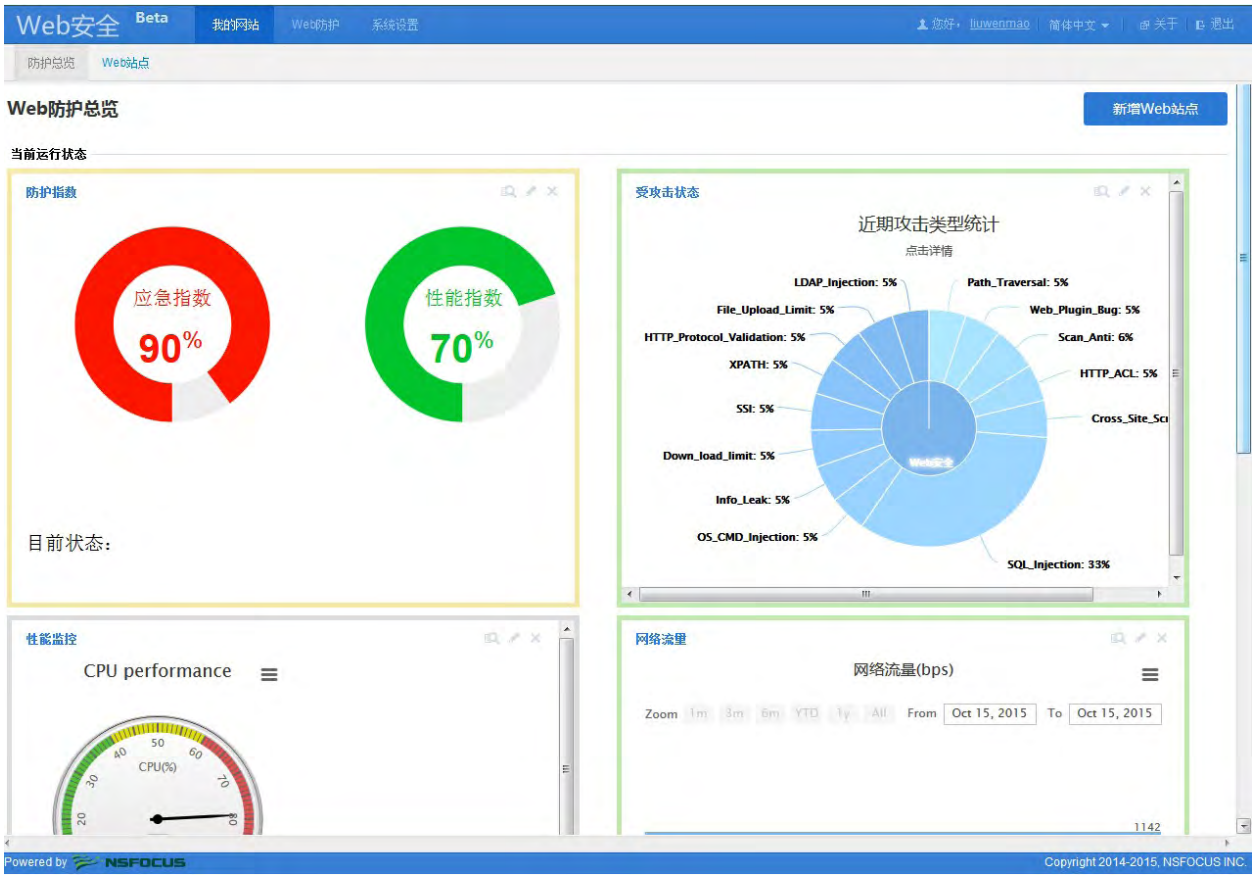


图 6.4 Web 安全防护应用 - 运营界面

借助软件定义安全的架构，这些面向公有云的安全应用，可以不做修改部署在多种公有云平台，使得普通云上用户能方便快捷地获得所需的安全能力。

6.3 可编排的应急响应 / 弹性服务

随着互联网的快速发展，重量级的漏洞从曝光到大规模利用时间从以天计算到以小时计算，大企业的严重安全事件也是层出不穷，安全防护所遇到的挑战也越来越大。Gartner 提出的自适应安全模型，基于的假设就是即便是安全防护体系完备的 TOP500 大企业，其 IT 基础设施也是会被攻破的。但即便如此，也可以通过增强检测和响应的安全机制，使系统在很短时间内恢复，数据最终不会被泄露。

所以，安全厂商应该提供弹性服务（Resilient Service），为企业提供预测、防护、检测和响应服务，通过模板提供自动化的处置流程，应对各种类型的安全事件，缩短整体处理时间。Phantom 的 Playbook 事实上提供了自动化处理的引擎，IBM 收购的 Resilient System 也提供了弹性服务，可大大缩短安全事件处置周期。

弹性服务包括两个部分，安全厂商的云端应急响应支撑和客户侧的本地（on-premises）应急响应服务。前者是由安全厂商完成从漏洞 / 安全事件的发现到相应处置方案交付的整个过程；后者是客户

发现安全事件到最终解决的整个过程。虽然侧重点、参与角色和处理机制不同，但流程是相似的。为了简单起见，本文着重讲述云端提供的应急响应服务。

从功能上看，云端应急响应服务提供了从发现到样本分析、发布处置方案、升级产品，到客户在安全事件全周期全方位感知，如图 6.5 所示。云端的应急响应服务包括内部团队的应急响应组件、提供安全功能的 SaaS/MSS 组件和面向终端客户的安全服务组件。这些组件利用云端的各种基础设施、中间件和人力资源，进行工作流的流转、切换、等待和恢复。

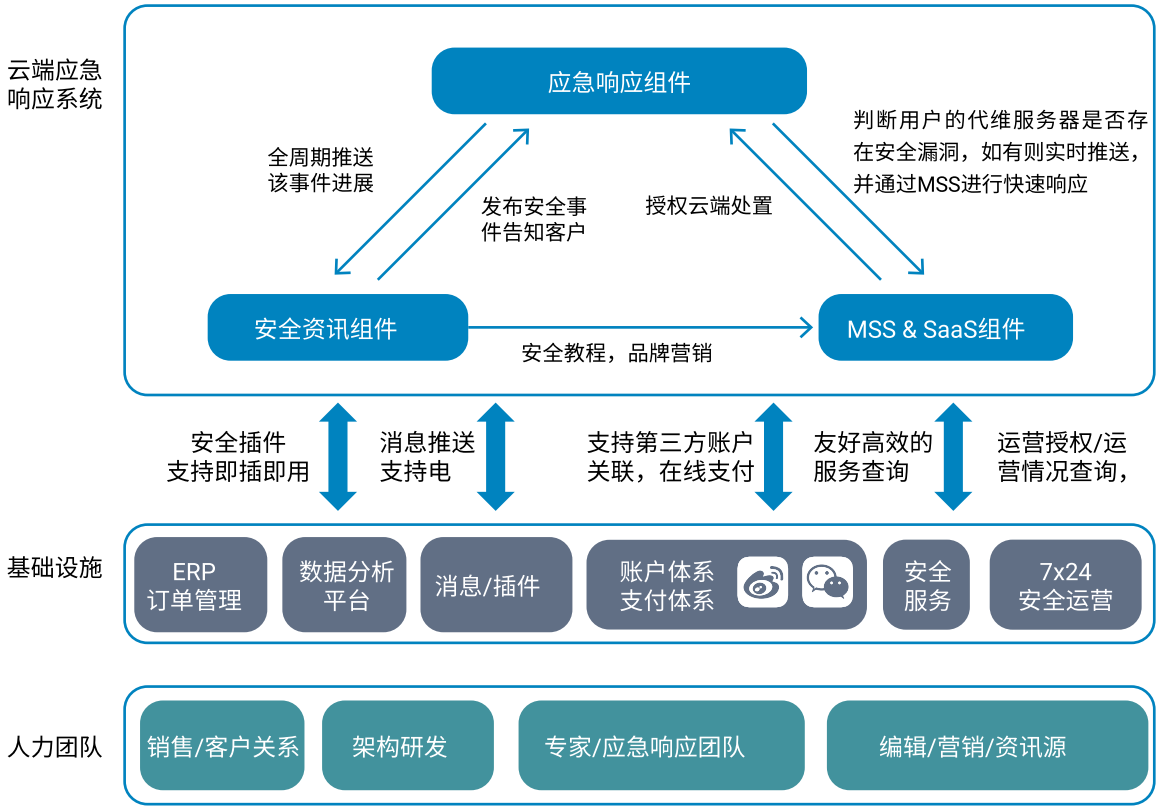


图 6.5 云端应急响应示意图

要针对大规模突发的互联网重大安全事件做到小时级响应，整个过程就必须持续高度自动化；流程上还需要灵活定义在每个处置节点的数据输入输出流，节点处置中允许人工参与和程序运行混合进行，流程就必须做到细节可视、成果可量化。安全厂商每天处置的安全事件数量巨大、类型不同，涉及的影响范围又非常广，每个处置流程的不同阶段又涉及到多部门、大量用户，通过软件定义的流程编排就能大大提高处置效率。

每个应急响应服务的组件，本质上都是安全应用，这些组件可以通过编排系统调用各种 IT 基础设施，对移动用户推送安全事件，或通过 MSS 云端人工服务抵御客户侧的安全威胁，或通过 SaaS 在云端进行日志分析。而这些安全应用在不同的安全事件处置中，有相互交互，按照应急预案进行有序的协同。

在设计编排系统时，进一步将这些组件按照安全事件的生命周期进行分解，并结合使用应急响应服务的团队，可作出图 6.6。可以看到每一个角色都会参与若干个处置步骤，每个过程都会存在前置和后置过程，通过工作流相连。

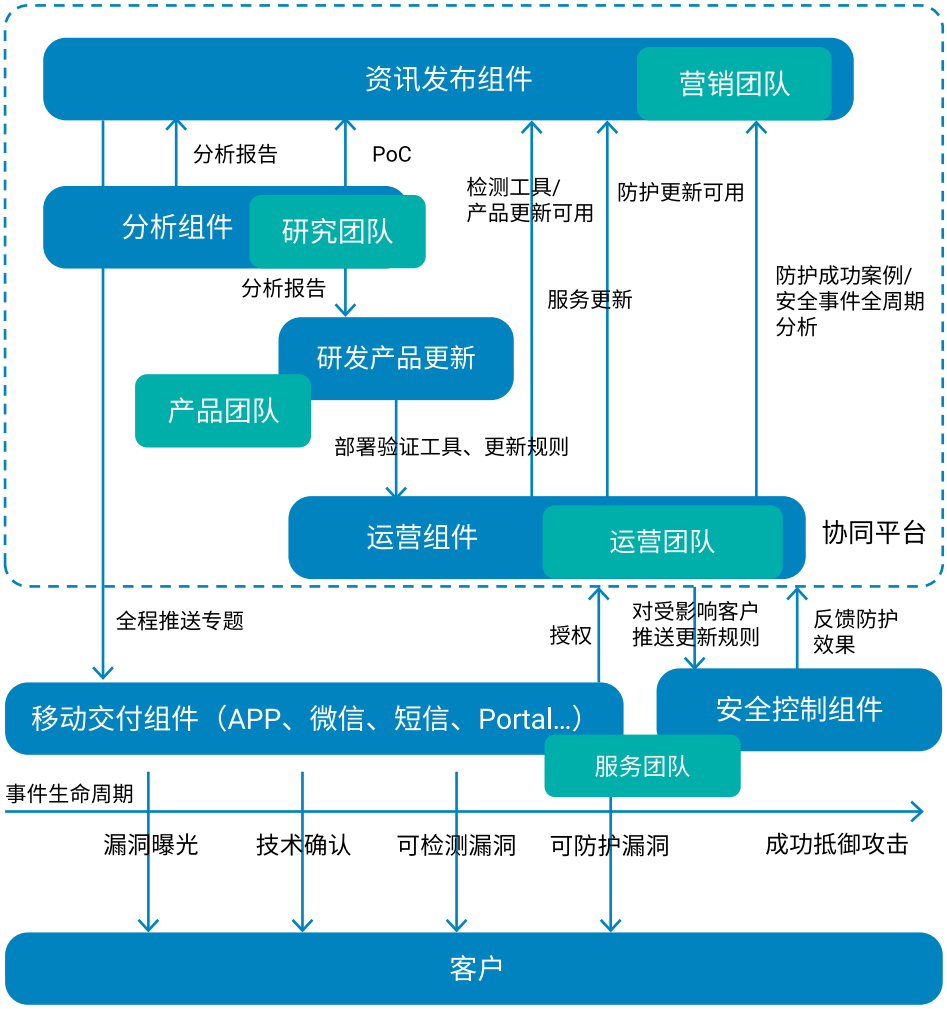


图 6.6 应急响应编排的时序图

我们抽象该流程抽，将处理流程中的每个步骤变成节点，每个节点主要由触发、执行行为（包括工作下发、告知客户、对资产的控制命令下发等）、结束三部分组成。前一个节点的结束将是下一个节点的触发，对多个节点进行编排形成编排链。图 6.7 给出了一个样例，其中含有三条编排链。

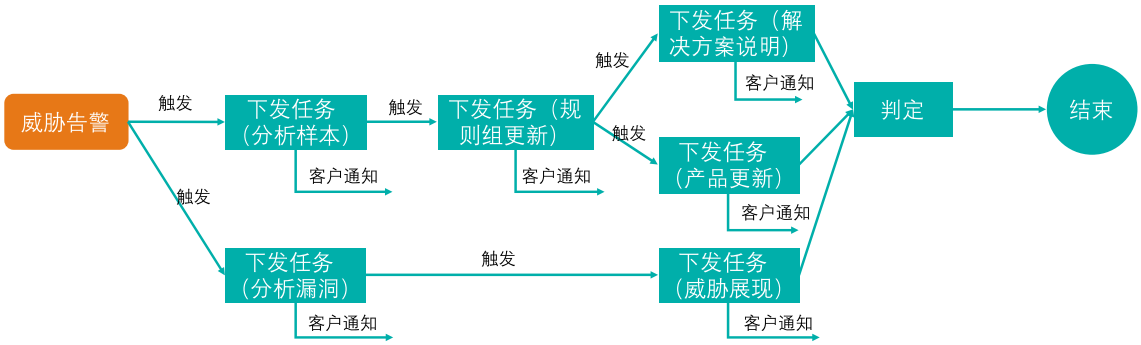


图 6.7 应急响应编排的时序图

初始设置时，管理员利用以往的安全事件处置步骤，按照引导对每个步骤填入关键信息，将步骤节点按一定顺序生成编排任务，将编排任务下发给后台的编排链解析模块。编辑好的编排任务，其中任务下发、客户通知、判定是定义好的步骤。

在运行时，编排系统在后台对接收的编排任务进行解析，过程中每个步骤会被解析成具有规定执行顺序的多行为编排链。这些编排链按照步骤编排的顺序组成最终可执行的处置步骤序列。

对于人工参与的步骤，编排系统通过计时器倒计时中断的方式将工作流从输入切换到输出；对于自动化的步骤，编排系统监听程序运行结果的通知，并将运行结果作为输入转交给下一个节点。以往人与人通过即时消息、邮件交互变成了通过角色、关系、资产、流程、步骤、行为、事件和输入输出等要素构成的编排系统，系统中每个节点都可以自动有序运行，大大降低了因某个关键节点阻塞导致服务无法推进的风险。

通过编排系统，应急响应的云端处置体系在软件定义后，使得整个流程趋于自动化、智能化，大大缩短了安全事件从发现到客户侧处置的周期。

七 . 结束语

软件定义安全已越过了技术成熟度曲线的最高点，国内外的关注度会越来越多。2016 年是软件定义安全发展的重要一年，很多初创公司和成熟公司的安全产品很好地诠释了这一点。

软件定义安全从架构上看，北向的要点是安全应用的有效协作和快速交付，前者利用应用编排技术形成安全策略的灵活组合，适配于不同的场景；后者借助全新的在线应用商店构建良好的生态环境，加快安全应用的交付速度，应对日益激烈的攻防对抗。南向的要点是能根据多变的安全策略，快速输出相应的安全能力，资源池技术不仅解决了安全体系与云平台集成的可行性问题，还有助于将异构的安全设备抽象统一，形成可快速就绪、弹性的安全能力。可以预计，未来几年这三个技术将会得到快速的发展，成为推动软件定义安全的强大支撑动力。

本文从宏观角度分析了软件定义安全在 2016 年的新动向，文中更多技术细节可参考《软件定义安全：SDN/NFV 新型网络的安全揭秘》一书。

参考文献

[1] 习近平，在网络安全和信息化工作座谈会上的讲话，
http://politics.people.com.cn/n1/2016/0426/c1024-28303544.html

[2] Verizon, DBIR 2016,
http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/

[3] 安天，白象的舞步：来自南亚次大陆的网络攻击，
www.antiy.com/response/WhiteElephant/WhiteElephant.pdf

[4] 通信世界网，《Gartner2016 年度新兴技术成熟度曲线》全解读，
http://www.cww.net.cn/news/html/2016/8/19/2016819853335793.htm

[5] Google, BeyondCorp: A New Approach to Enterprise Security,
https://static.googleusercontent.com/media/research.google.com/en/us/pubs/archive/43231.pdf

[6] Gartner, Hype Cycle for Infrastructure Protection, 2015,
https://www.gartner.com/doc/3110721/

八 . 关于绿盟 - 巨人背后的专家

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

基于多年的安全攻防研究，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及安全运营等专业安全服务。

绿盟科技通过挖掘各行业客户的安全需求，在前瞻性的研究成果基础之上，不断拓展市场销售网络，覆盖国民经济的多个行业，尤其在政府、运营商、金融、能源、教育、医疗等重点行业。绿盟科技提供的产品及解决方案，具有高安全性、高可用性及可管理性，能够满足日益复杂的客户安全需求。自 2007 年起，绿盟科技开始积极拓展海外市场。现已在日本东京和美国硅谷设立子公司，并在欧洲、东南亚设立分支机构，深入开展全球业务。绿盟科技正在为保障全球客户的网络与业务的平稳运行而持续努力。

2009 年，绿盟科技成为国际云安全联盟（CSA）在亚太区的首家企业成员。2010 年，绿盟科技发起成立国际云安全联盟中国区分会（CSA Greater China Chapter）。绿盟科技在云安全和虚拟化安全、软件定义安全的新型安全服务、安全度量、安全信誉、安全智能等前沿安全领域进行了积极的研究探索并积累了丰富的经验。目前，绿盟科技已经实现了各类虚拟化的安全产品，并推出基于软件定义安全的云安全解决方案。该解决方案已在一些合作伙伴中获得验证，如 2015 年全球 SDN 大会与云杉网络 [1] 演示的公有云异常流量分析与可视化展现，以及与华为 SNC[2]、绿网科技 GNFlush[3] 等一系列业界 SDN 控制器集成，在 BYOD 环境中验证了软件定义的访问控制；在 2016 年华为全连接大会上，展示的定义抗拒绝服务攻击防护系统获得华为开发者生态最佳解决方案奖。

绿盟科技还积极推动各类科研课题的研究和云安全标准制定，参加了 863 课题《云计算环境中恶意行为检测与取证技术研究》的软件定义取证架构，并在参与编写《信息系统等级保护云计算安全设计技术指南》的边界安全部分。

1 http://www.yunshan.net.cn/

2 http://carrier.huawei.com/cn/products/fixed-network/carrier-ip/service-gateway-controller/snc

3 http://www.greenet.net.cn/product.php?id=17

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，
为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供
具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。
在这些巨人的背后，他们是备受信赖的专家。

www.nsfocus.com