2015 绿盟科技软件定义安全 SDS 白皮书

2015 NSFOCUS Software Defined Security Whitepaper

导读

Challenge

业界对云计算的研究及实践由来已久，但随之来而的云安全问题，需要有一套云环境中的安全建设及运维的框架和方法，同时更需要用户、云计算厂商与安全厂商多方协作实践的经验。面对这样的挑战，多年来，绿盟科技与国际云安全联盟（CSA），与全球各大开源和商用的虚拟化平台，与 SDN 控制器项目和厂商进行了深入合作，积累了一定的经验。

Content

本文着重阐述如何使用新技术和新架构，实现下一代软件定义（SDS）安全防护体系。首先介绍目前业界现状和相关工作，接着给出 SDS 架构，然后分别介绍安全应用商店、安全控制平台和安全设备的重构，最后给出若干绿盟科技的实践案例。

Benefits

读者通过本文档可以了解软件定义安全（SDS）架构的构建及实践经验，为建立适合自己的云计算平台安全中长期的方案规划、设计和管理，获取理论支撑。如果读者欲了解如何在私有云当前的体系实现安全防护，请关注绿盟科技《私有云安全技术解决方案》白皮书。

目录

图表

Note: 本文展现了绿盟科技在云安全方面的探索，本文涉及的概念、架构和相关实践工作，并不代表已有相应可销售的产品。

NSFOCUS

前言

随着网络安全已成为国家层面的对抗，国内政府、企业和各大机构对自身的信息安全日益重视。2014 年中国已成立了习近平总书记领导的中央网络安全和信息化领导小组，负责制定实施国家网络安全和信息化发展战略。各大企业也纷纷组建自己的安全团队和安全应急响应中心，通过专业化的安全运维提升自身的安全防护能力。

然而网络攻击数量逐年增加，安全形势不容乐观，很多传统的安全防护手段在新型的攻击下低效甚至失效。根据绿盟科技统计，在云计算信息系统方面，VMware 虚拟化系统共出现过 222 个漏洞，其中高危 52 个，过去一年内中披露了 11 个漏洞；全球最大的开源 IaaS 系统 Openstack 共披露了 68 个漏洞，过去一年就有 14 个漏洞，其中高危 1 个。这些漏洞无疑为外部或内部攻击者提供了极其便利的攻击手段。在 Verizon 的最新的《2015 Data Breach Investigations Report》报告中提到，一次定向攻击从开始到数据窃取平均只需数小时，而防守方从攻击开始到检测完成则需数月。可见安全界亟需改造自身的安全防护体系，以快速响应应对漏洞利用攻击，以威胁情报分析应对隐秘威胁。

不仅如此，新的技术出现也在考验原有的网络安全防护体系。云计算等技术的迅猛发展，已在深刻改变传统的 IT 基础设施、应用、数据以及 IT 运营管理。特别对于安全管理来说，一些新技术，如软件定义网络（SDN，Software Defined-Networking）、网络功能虚拟化（NFV，Network Function Virtualization），既是挑战，也是机遇。

首先，作为新技术，云计算引入了新的威胁和风险，进而也影响和打破了传统的信息安全保障体系设计、实现方法和运维管理体系，如网络与信息系统的安全边界的划分和防护、安全控制措施选择和部署、安全评估和审计、安全监测和安全运维等许多方面。其次，云计算的资源弹性、按需调配、高可靠性及资源集中化等都间接增强或有利于安全防护，同时也给安全措施改进和升级、安全应用设计和实现、安全运维和管理等带来了信息机遇，也推进了安全服务内容、实现机制和交付方式的创新和发展。

软件定义的理念正在改变 IT 基础设施的方方面面，如计算、存储和网络，最终成为软件定义一切（Software Defined Everything）。这“一切”必然包含安全，软件定义的安全体系将是今后安全防护的一个重要前进方向。

“软件定义”之百家论

最好的时代，也是最坏的时代

在近五年，互联网已发生巨大的变化，无论是基础设施，还是终端设备，无一不在重构我们的生活。

这是一个最好的时代，云计算、大数据、移动互联网和物联网等新型的 IT 基础设施和应用已在加快全球信息化步伐。随着云计算技术的不断完善和发展，云计算信息系统更加开放易用，功能更加强大丰富，接口更加规范开放，已经得到了广泛的认可和接受，许多组织已经或即将进行云计算平台建设。有调查表明，对于企业级用户，26.1%将云计算作为投资重点，而 27.4%的中小企业更偏向于选择软件定义数据中心作为未来 12 个月的投资重点[①]。

这是一个最坏的时代，随之而来的是新型环境中各种各样的安全事件，国家计算机网络应急技术处理协调中心（CNCERT/CC）在其《2014 年中国互联网网络安全报告》报告中认为，根据热点形势特点分析，移动互联网和云计算平台均为 2015 年值得重点关注的热点。

一方面，移动互联网发展迅猛，中国的手机网民已达 5.57 亿[②]，而移动互联网恶意程序在 2012 年和 2013 年呈爆炸式增长，2014 年获得恶意程序样本数量为 951059 个。一旦攻击者攻破企业员工的移动设备，就可能通过 BYOD 应用渗透入企业内网，部署在传统边界上的安全机制难以起到防护效果。

另一方面，云平台普及加大数据泄露和网络攻击风险，如网络、主机、虚拟资源管理和数据安全等方面都存在各种各样的威胁，具体威胁点可参见绿盟科技的《私有云安全技术解决方案》，此外防护措施和管理机制亟待完善。如第一章所述，作为当前

① 王丛，中国云计算演进市场和技术趋势，电脑与电信，2014

② CNCERT/CC 2014 年中国互联网网络安全报告

全球最大的商业和开源虚拟化系统，VMware 虚拟化系统和 Openstack 分别出现了 222 和 68 个漏洞，其中不乏高危漏洞。如果攻击者通过 Hypervisor 漏洞从虚拟机穿透到宿主机，那么很多安全机制就完全失效，更何况目前国内客户无论采用 VMWare Vsphere 还是 Openstack 的云计算信息系统，大部分虚拟化环境中没有采用任何安全机制，或部署任何安全设备。

总之，网络攻击的频繁化、多样化和隐蔽化，与传统安全机制检测、防护和响应的落后，造成了不可调和的矛盾，也对云计算等新型应用的发展造成了极大的阻碍。

软件定义=银弹?

随着国家和行业的监管加强，安全已经成为组织规划、设计、建设和使用云计算平台而急需解决的重大问题之一，尤其是不断出现的与云计算平台相关的安全事件让组织更加担心自身的云计算平台安全保障问题。用户对信息安全需求的不断增加，以及政府政策法规的驱动，预示着中国云计算安全市场未来潜力巨大、发展前景乐观。

自从著名咨询机构 Garnter 在《The Impact of Software-Defined Data Centers on Information Security》[①]一文中提出软件定义安全（Software Defined Security，SDS）的概念后，软件定义与安全的结合已成为业界的前沿发展热点。软件定义安全是从软件定义网络（Software-Defined Networking，SDN）引申而来，原理是将通过安全数据平面与控制平面分离，对物理及虚拟的网络安全设备与其接入模式、部署方式、实现功能进行了解耦，底层抽象为安全资源池里的资源，顶层统一通过软件编程的方式进行智能化、自动化的业务编排和管理，以完成相应的安全功能，从而实现一种灵活的安全防护。

Check Point 在 RSA 2014 大会上宣布推出软件定义防护（Software Defined Protection，SDP）革新性安全架构，可在当今日新月异的 IT 和威胁环境中为企业提供虚拟化的边界防护。赛门铁克也在 RSA 2015 提出使用软件定义网络技术对 APT 攻击进行取证，提供了一种安全事件事后快速分析的新思路[②]。Catbird 公司的软件定义安全架构[③]通过微分区（Micro-Segmentation）在虚拟环境中划分不同的域，并通过编排将安全策略下发给多种类型的安全设备，并作用在区域级别或虚拟机级别。这些方案有的具有开放性，有的具有快速响应，还有的能完成自动化安全运维，从不同层面表现出软件定义的特征。随着一些具有洞察力的安全公司提出了概念性的方案，并将其做出面向某领域的商用产品，可预见越来越多的公司的安全产品和解决方案将走向软件定义。

软件定义安全体系概述

几乎每个提出软件定义安全的厂商对该术语本身有不同的解读，导致实现的方式各有千秋。概念上，本文采用 Garnter 的定义，架构方面将会按照以下思路进行设计。

SDN 技术的出现，特别是与网络虚拟化结合，给安全设备的部署模式提供了一种新的思路。SDN 的一个特点是将网络中的控制平面与数据平面分离，通过集中控制的方式管理网络中数据流、拓扑和路由，图 1.1 是 SDN 的一个典型架构，自顶向下可分为网络应用、网络控制器和网络设备。

① https://www.gartner.com/doc/2200415/
② https://www.rsaconference.com/events/us15/agenda/sessions/1555
③ http://www.catbird.com/product/catbird-architecture

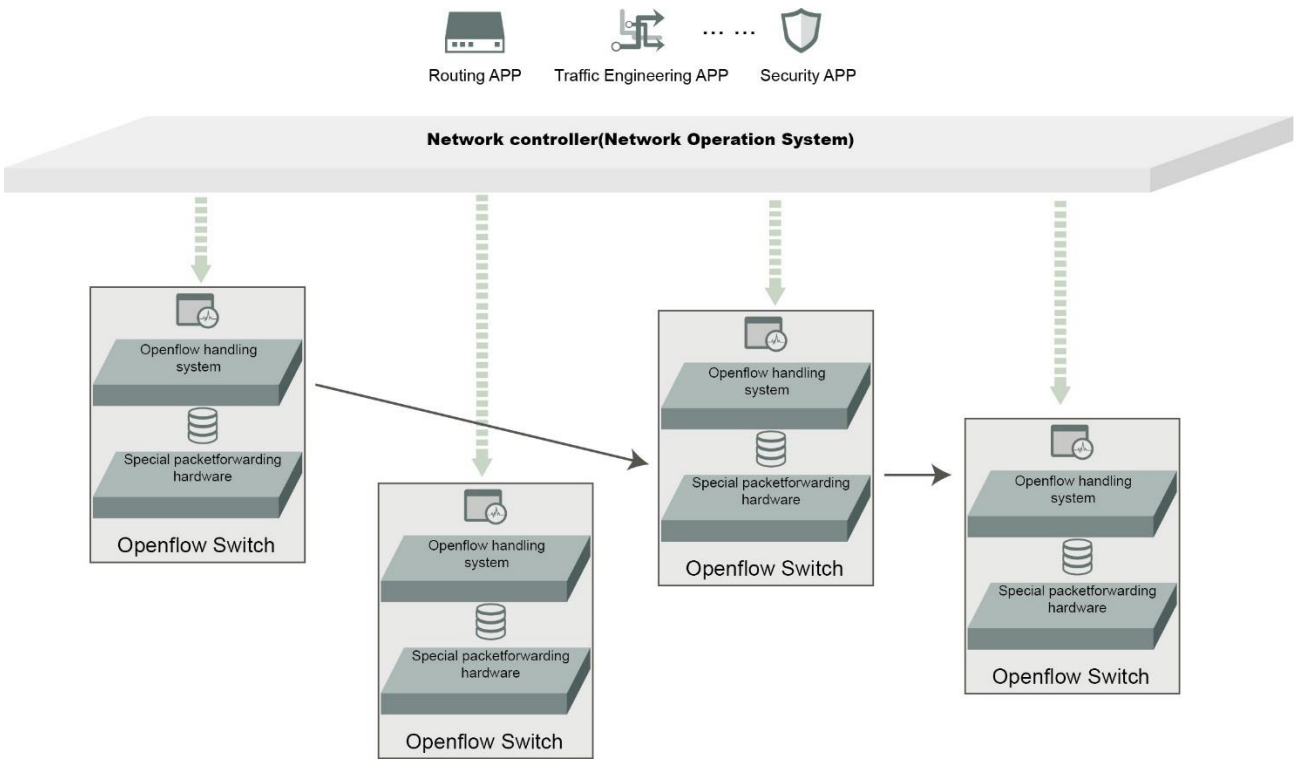

图 1.1　SDN 典型架构

那么，基于软件定义架构的安全防护体系也可将安全的控制平面和数据平面分离，架构如图 1.2 所示，可分为三个部分：用户环境中实现安全功能的设备资源池，软件定义的安全控制平台和安全应用，以及安全厂商云端的应用商店 APPStore。

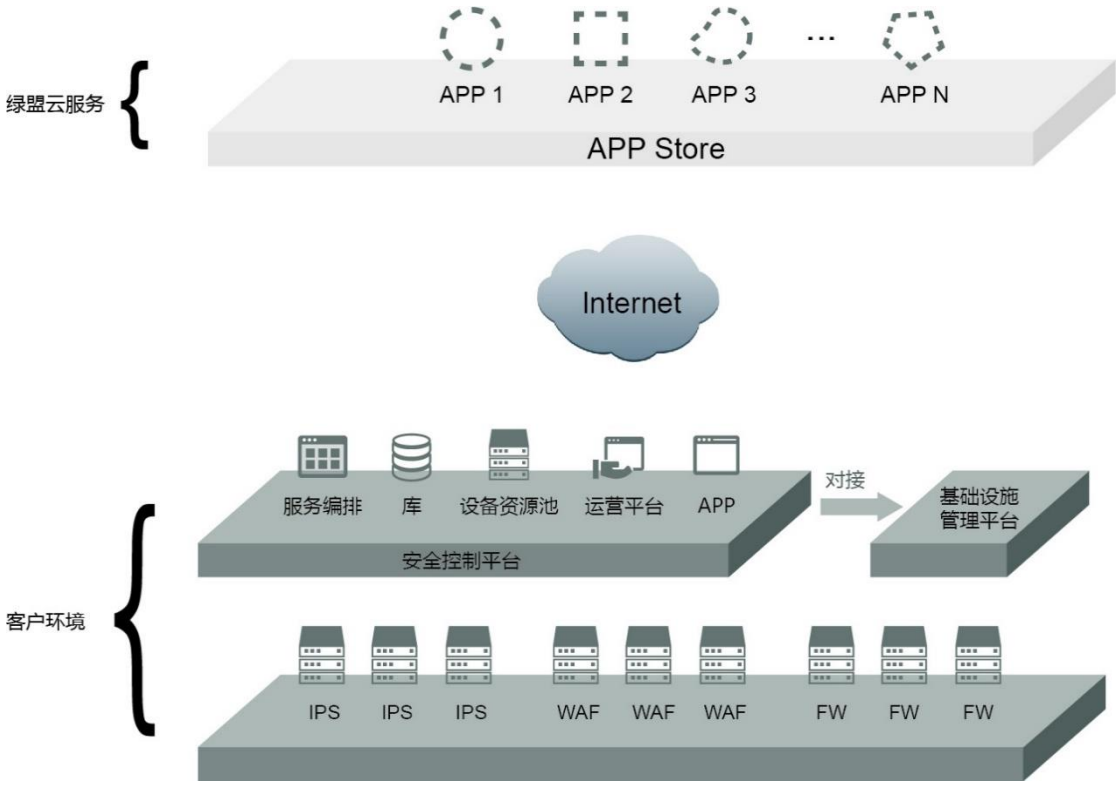

图 1.2　安全防护体系架构

- 首先，通过安全能力抽象和资源池化，安全平台可以将各类安全设备抽象为多个具有不同安全能力的资源池，并根据具体业务规模横向扩展该资源池的规模，满足不同客户的安全性能要求。
- 其次，一旦具备了底层的安全基础设施保障，安全厂商或有二次开发能力的客户可以根据特定安全业务需求，开发并交付相应的上层安全应用，以灵活调度安全资源，进行快速检测、威胁发现、防护和反馈。以往通过工程支持人员完成的人工服务，就可以通过单个安全应用或多个安全应用编排的方式交付给客户，以标准化的自动化流程完成整个项目的快速交付，在不同客户运维过程中开发的额外功能，都可孵化为该应用的标准功能，大大降低了公司的人工技术支持费用。此外，以往很多客户对产品的定制化需求往往需要花费产品线数月时间开发定制功能，但在新模式下，可由节省出的工程人员使用控制平台的应用接口开发安全应用，实现其功能，既能较快交付轻量级的应用，又能保持安全设备本身的高效、可靠。
- 此外，作为安全操作系统的安全控制平台，向上为应用提供编程接口，向下提供设备资源池化管理，东西向可适配不同的业务管理平台（如云管理平台、SDN 控制平台和客户定制的管理平台等）。在内部，从这些不同的接口的获得信息转化成标准的安全策略、资产库信息、日志告警，并利用这些信息完成任务调度、智能决策和命令推送，将以往需要人工完成或半自动完成的管理流程转换成了接近全自动化控制。
- 最后，部署在安全云上的 APPStore，将安全应用从云端直接推送到客户环境，改变了传统的线下安全交付模式。使得客户可以在非常短的时间内购买云端安全方案和安全服务，或更新原有的安全应用版本，以抵御互联网上大规模短时间内爆发的(1~n)-day 攻击。

总之，从硬件定义走向软件定义，从定制开发到轻量级应用，从传统线下交付到实时在线推送，从人力密集易错到高效自动运维，从单设备配置限制到可扩展的安全能力，从单设备功能到整体解决方案，无一不在重构安全厂商的安全防护体系。本项目的目标是构建一个可持续发展的生态系统，建立良好的客户关系，并为云端大数据分析和专家级应急响应提供支持，最终获得新的赢利增长点。

软件定义安全体系的设计

整体方案

如图 1.2 所示，基于软件定义架构的安全防护体系包括部署在绿盟云端的应用商店 APPStore，以及部署在客户环境中的安全控制平台、各类安全设备，以及各种实现安全业务的应用 APP。

其中，绿盟科技云端的 APPStore 发布自研或第三方的安全应用，客户可购买、下载和在本地部署、运行这些应用。客户环境中的核心系统是安全控制平台，负责安全设备的资源池化管理、各类安全信息源的收集和分析、与客户业务系统对接，以及相应安全 APP 的策略解析和执行。安全应用通过互联网从 APPStore 下载到安全控制平台上，然后被部署、验证、运行和升级。安全设备的交付形态有很多，但逻辑上都会在安全控制平台的管理下，形成各类资源池，具备相应的安全能力。

APPStore

APPStore 的功能需求主要有：

- 管理云端安全应用，如应用存储、下载、创建和删除等
- 用户管理，如用户注册、更新和认证等
- 支持应用编排的部署模式，即多种应用可以叠加同时实现多种业务，如编排调度、任务增加、删除和执行等
- 用户处应用管理，包括向云端注册、认证和购买，应用的搜索、更新、部署和操作。

考虑到以下三个因素：1）不同应用有完全不同的形态，如守护进程、Web 站点，或 CLI；2）一个物理机上会部署多个应用，但又需要保证应用上下文隔离；3）更新时网络带宽消耗不能过大，更新时间不能过长，建议 APPStore 的实现使用 Docker 技术，实现应用的轻量级隔离，并实现增量更新，如图 1.3 所示。

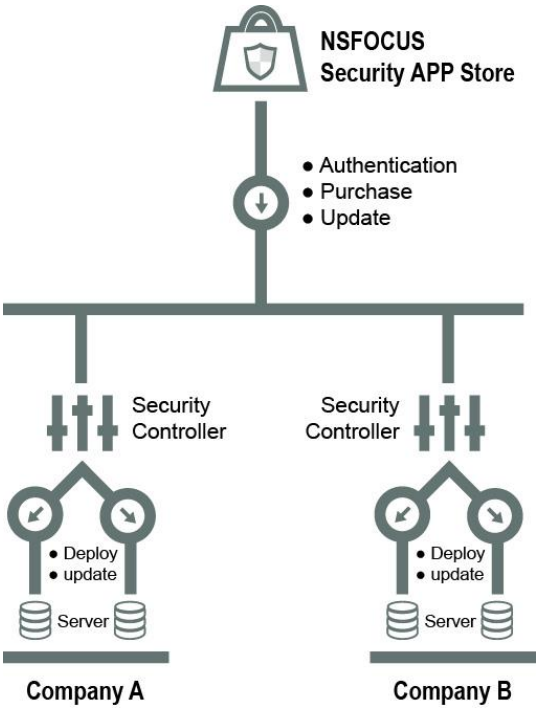

图 1.3　APPStore 设计

安全控制平台

借鉴了控制和安全数据分离的思想，设计了一个面向设施即服务（IaaS）的软件定义安全的体系，如图 1.4 所示。与软件定义网络对应的，软件定义安全体系的核心是安全控制平台（Security Controller），以下介绍平台的整体架构和主要功能模块，以及这些模块协作机制。

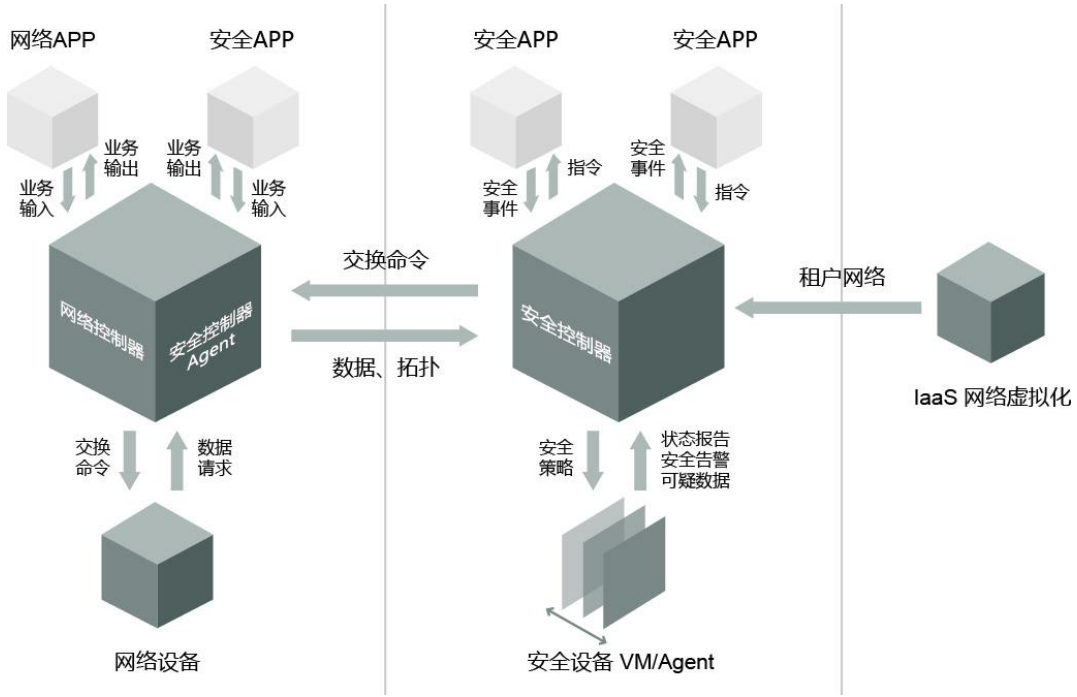

图 1.4　基于安全控制平台的软件定义安全架构

安全控制平台的内部模块组成和总体架构如图 1.5 所示，主要由若干个核心模块和面向不同场景的定制模块组成的。每个模块与控制平台内部的模块或外部的安全或网络主体进行交互，生成的数据保存到缓存或数据库中，形成若干个库，如 APP 库、设备库、流库和策略库等。

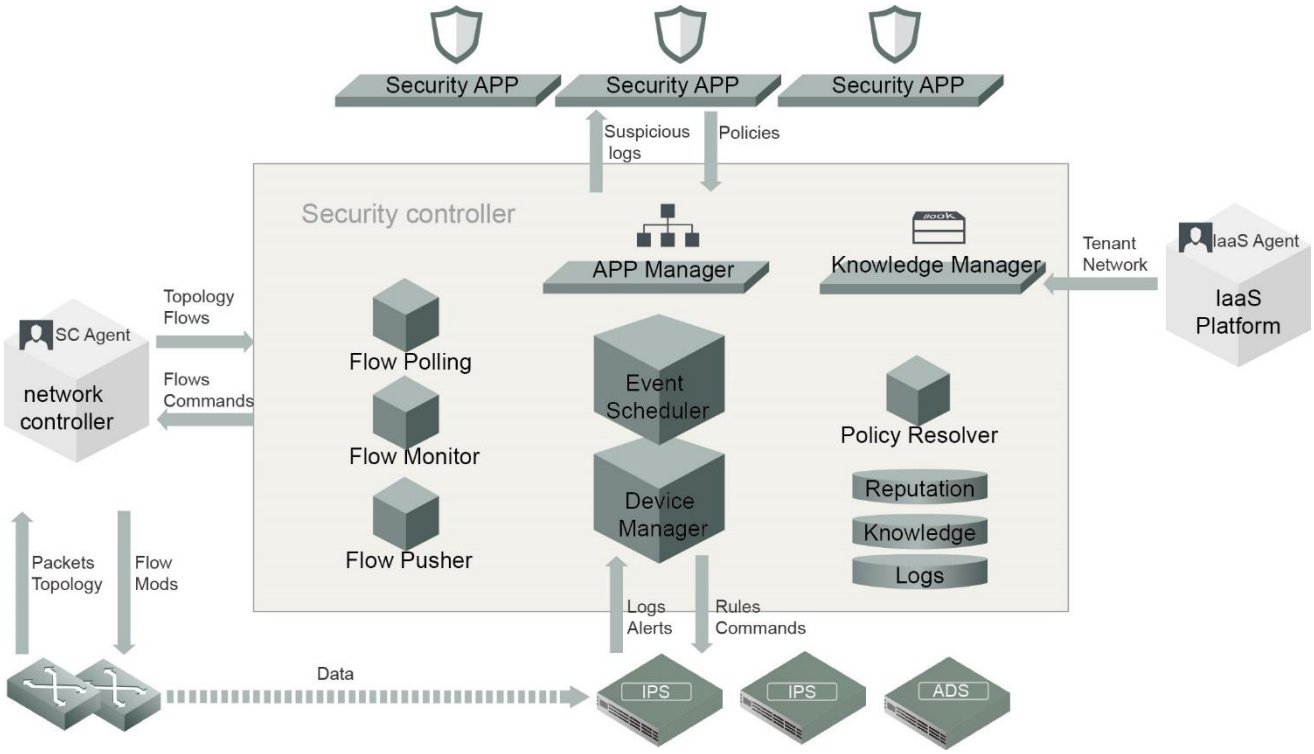

图 1.5　安全控制平台的结构

其中核心模块包含：

- 分布式事件调度（Event Scheduler）　接受各模块注册事件，将需处理的事件分发给相应模块，触发事件处理机制；
- 应用管理（APP Manager）　管理北向的安全应用信息，接受应用的可疑数据订阅，推送满足条件的可疑数据
- 设备管理（Device Manager）　管理南向的设备应用信息，在策略解析器等模块中提供所需的安全设备
- 策略解析（Policy Resolver）　将安全 APP 的抽象策略分解为网络设备或安全设备可执行的具体命令

此外，还有一些重要的模块，如数据收集、可疑数据监控和命令推送，在不同场景有特定的实现，称之为定制模块。例如在 OpenFlow/SDN 的环境中，还有流表获取（Flow Polling）、流量监控（Flow Monitor）和流指令推送（Flow Pusher）三个模块。

安全控制平台实现的功能是由上述若干模块的协作完成的，基本的工作流为数据收集模块从东西向获得网络数据，数据监控模块根据安全应用的订阅条件寻找粗粒度的可疑数据，通过安全应用管理模块推送给安全应用；后者根据细粒度的算法进行决策，将命令通过安全应用管理模块下发给策略解析模块，后者根据语义解析成网络控制器或安全设备可理解的命令，最终由数据推送模块下发到控制器或安全设备。

在具体场景中，可能会存在额外的安全模块，例如日志记录和分析等，工作流也可能存在一些差异。但每个模块实现自己的功能，相对独立，这种模块的设计有以下特点：

- 各模块均提供开放、标准的 WEB API
  - 例如 APP Manager 和 Device Manager 等都可通过 RESTful 接口进行访问，支持 CRUD 操作，从而实现应用和设备的增加、更新和删除等功能。
- 模块之间是松耦合的，部署比较方便

- 管理员可以调用接口启用或禁用某些组件，安全控制平台也会根据相应的应用场景，调用相应的模块；安全管理员也可以很容易根据需要编写新的模块对安全功能进行扩展。

由于整个安全系统强调的是在松耦合的系统中，提供简单的资源操作原语，使得安全管理员可以通过设计一组相关的 Web 调用，就能完成一系列一致性的操作，实现复杂的安全功能。

整个系统要点在于协作控制，它贯穿了安全控制平台内部模块间，以及安全控制平台与安全应用、设备间的交互设计。下面我们先介绍南北向的设备和应用如何与安全控制平台进行交互，接着说明安全控制平台内部的模块通信协作机制，然后介绍安全控制平台与安全应用协作的可疑数据订阅机制，最后分析将安全应用下发的策略解析成相应命令的策略解析机制。

安全设备资源池化

如果将安全架构部署云计算环境中，那就有可能使用虚拟化技术，实现安全设备的资源池化，并通过控制平台与 SDN 控制器的协同，对流量按需调度，实现服务链（Service Chain），此外根据应用所需的安全需求就可以从资源池中找到相应资源，而不用关心物理上安全设备部署在哪里，也不需要考虑如何布线划区。

此外，通过控制与数据分离，安全设备可以做到逻辑简单、处理高效，并保证了系统的稳定性。

要实现上述目标，就需要产品线从设备形态、设备部署形式和设备功能进行，实现以下的任务：

- 面向设备引擎提供可适应多种环境的统一平台，最终交付安全设备形态，如图 1.6 中的可处理隧道协议的单引擎模式、多类型虚拟设备组成的服务链、硬件虚拟化和 Hypervisor 集成的虚拟化等。在提供了底层支撑平台后，各产品线只需将自己的引擎部署在这些平台上，就可以快速交付可扩展的设备资源池；
- 架构需定义统一的安全设备类型、能力、应用接口等；
- 产品线需开放设备的应用接口，简化各种定制的模块，提高稳定性。

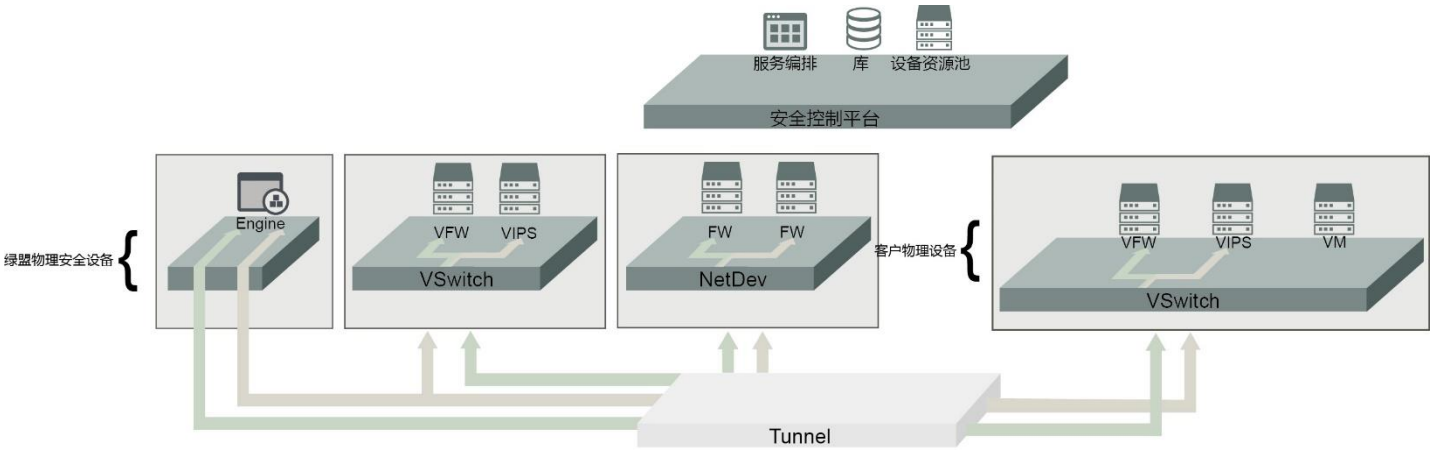

图 1.6　多种形态的安全设备资源集成

安全设备重构

正如上节所述，当安全设备完成资源池化后，对上层应用呈现出的只有安全能力，表现形式就是应用接口 API。从设备的角度看，当自身实现只需通过若干接口即可交付。

从功能上看，当安全控制平台实现了策略管理、安全分析、安全状态机和各类知识库和资产库，上层的应用就可以基于这些公共中间件实现各种功能，满足客户的不同需求。

这种设计模式避免了很多出于各种原因所不得不做的定制开发，极大解放了研发团队的人力资源，以便集中资源强化和优化设备自身的功能。

整体设计如图 1.7 所示，以防火墙为例，安全控制平台中的知识库中包含了各类地址的信誉、主机资产间的关系和资产归属信息，并根据上下文决定当前的黑白名单。相应的规则通过控制平面的南向接口传输到设备的规则库，那么防火墙运行时只需要判断逻辑匹配规则库的规则，当匹配时执行决策逻辑，所有规则都不匹配时执行默认决策逻辑。当判断逻辑和决策逻辑实现的非常高效，且应用功能满足需求时，整个系统就能高效、可扩展的运行。

要完成上述体系，但还需研发团队对产品本身功能进行梳理，可能会对产品的实现架构进行重构，需要较多的人力投入，但其带来的,后继的研发、测试和运维成本的节省无疑是巨大的。

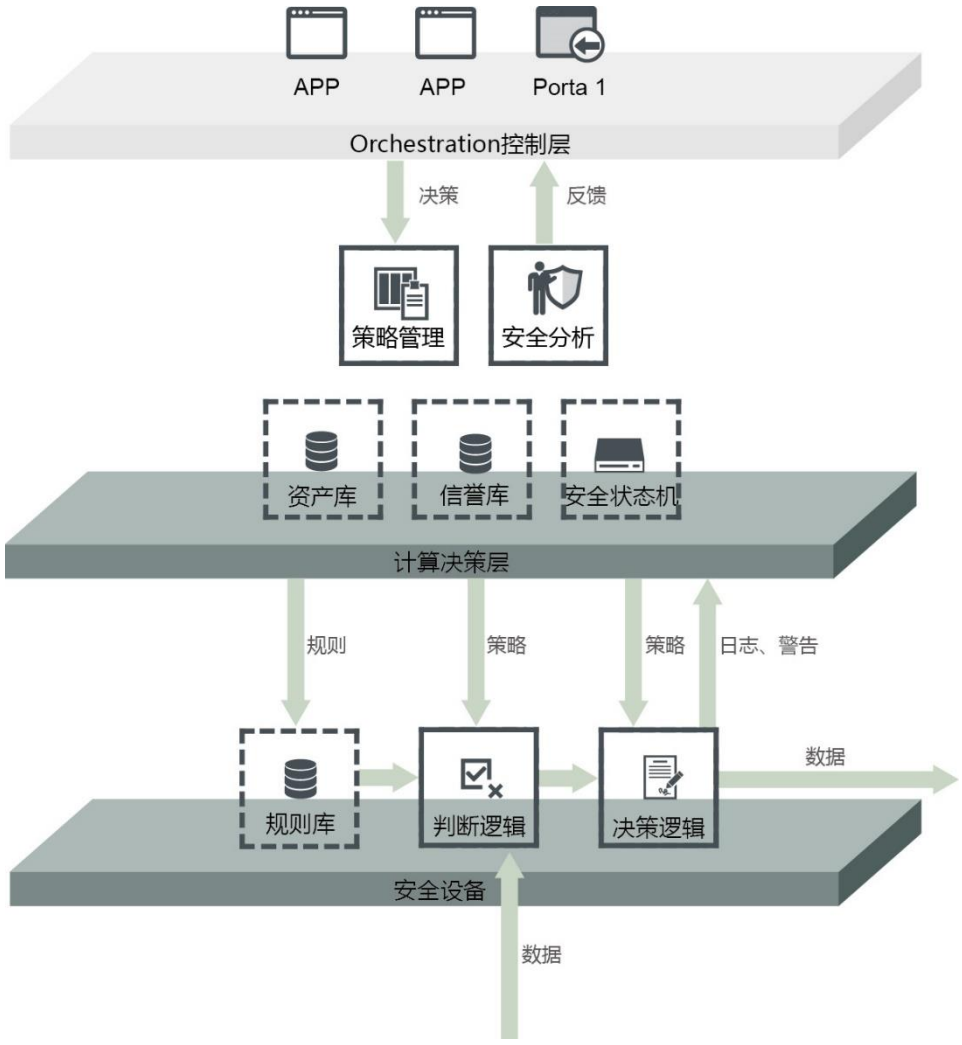

图 1.7　面向安全控制平台的安全设备重构

软件定义的云安全实践

第三章中的软件定义的安全体系是较为通用的架构，在第四章中我们给出了一个可行的架构设计，绿盟科技利用该架构实现了一个安全系统。本章将介绍该系统的部署和交付情况，以及该系统在若干常见的云环境场景中如何工作。

部署模式

本节主要阐述在在一个典型应用场景中，所需要的设备资源情况，以及如何将这些资源部署到整个项目。

假定在早期部署阶段有 100 位客户的控制平台接入，APPStore 部署于绿盟的云端，需要 8 台服务器，其中包括 1 台前端 Web 服务器，1 台认证服务器， 5 台后台处理服务器，1 台磁盘阵列服务器作为机群。

在一个中等规模客户的云计算业务系统中，包括 25 个机架，每个机架部署 2 台安全节点，共需要 50 台物理安全设备，这些设备涵盖防火墙、入侵检测系统、入侵防护系统、Web 防火墙、安全审计系统、数据库审计系统、抗拒绝服务检测和清洗系统等方面。

在安全控制平台部署在客户环境中，以虚拟安全设备组成服务链为例，资源池规模在 500 台安全虚拟设备左右，每个机架部署 1-2 个物理安全设备（即安全节点，下同）。安全控制平台通过分布式的方式部署，包括 1 台数据库服务器、1 台消息通信服务器、1 台负责策略、设备管理和应用管理的服务器，以及 1 台部署安全应用的服务器。总体的部署方案如图 1.8 所示。

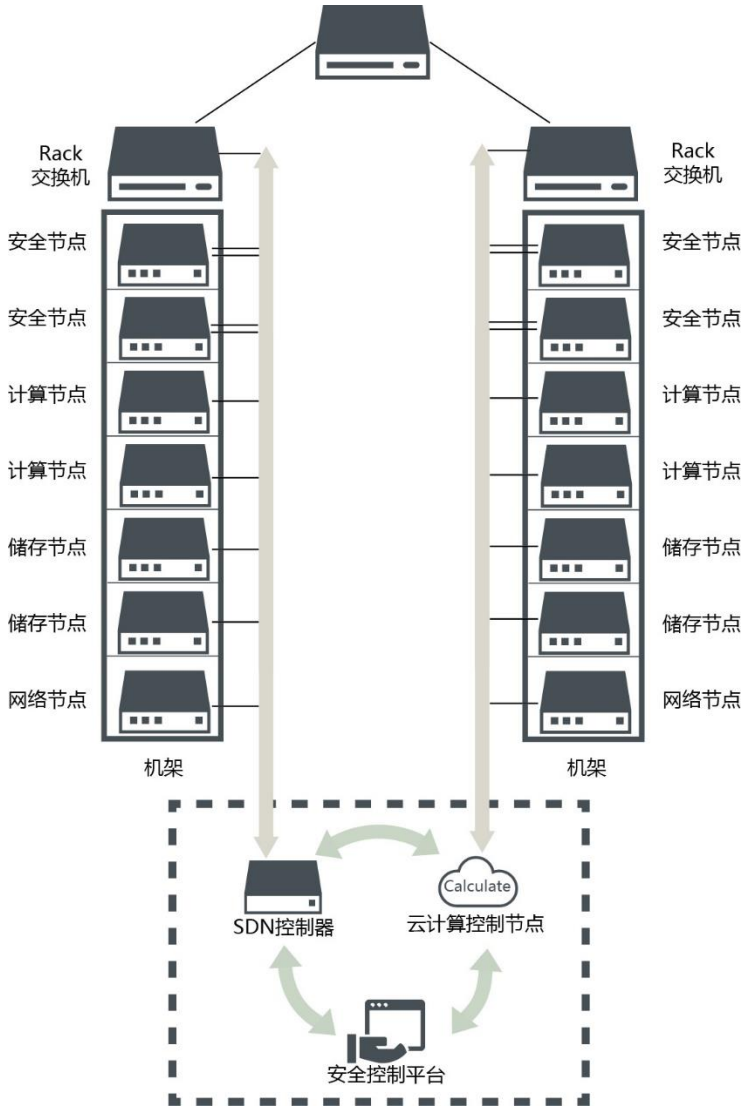

图 1.8　安全设备部署图

如图 1.9 所示，虚拟安全设备可以部署在计算节点上，也可以部署在独立的安全节点上，安全设备可以是工作在二层网络，也可以工作在三层网络。域内计算节点和安全节点内 Hypervisor 的虚拟交换机（Virtual Switch，VSwitch）连接到 SDN 控制器，安全管理平台通过 SDN 控制器开放的北向接口与之连接。

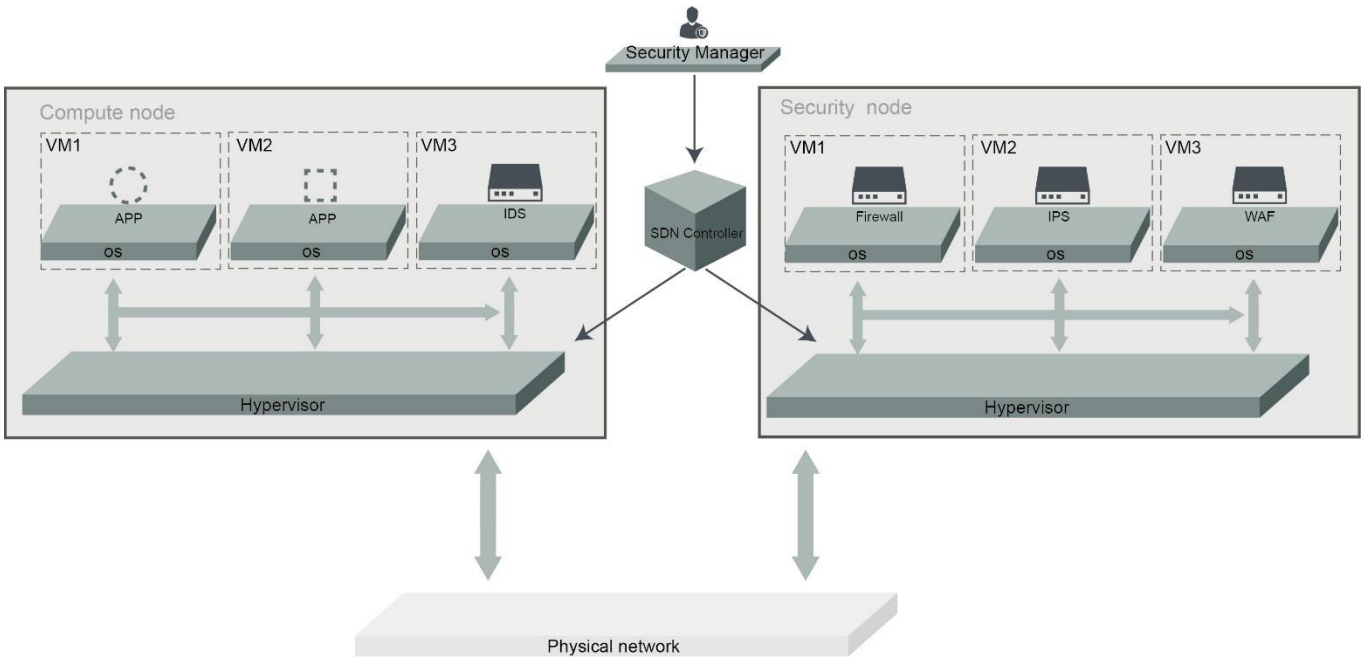

图 1.9　使用 SDN 技术的安全设备部署图

当接收并解析安全策略后，安全管理平台通过 SDN 控制器，向虚拟交换机下发流表，依次在源节点的虚拟交换机、源目的节点间的隧道和目的节点的虚拟交换机之间建立一条路径，这样原来虚拟机 VM1 通过源节点虚拟交换机直接到 VM2 的流量，就沿着上述指定路径先到了目的节点的虚拟安全设备，当处理完毕之后，数据流从安全设备的输出网卡返回到最终的目的虚拟机 VM2。图 1.10 展示了在开源虚拟化系统 Openstack+开源 SDN 控制器 Floodlight 环境下部署 IPS 的情况。

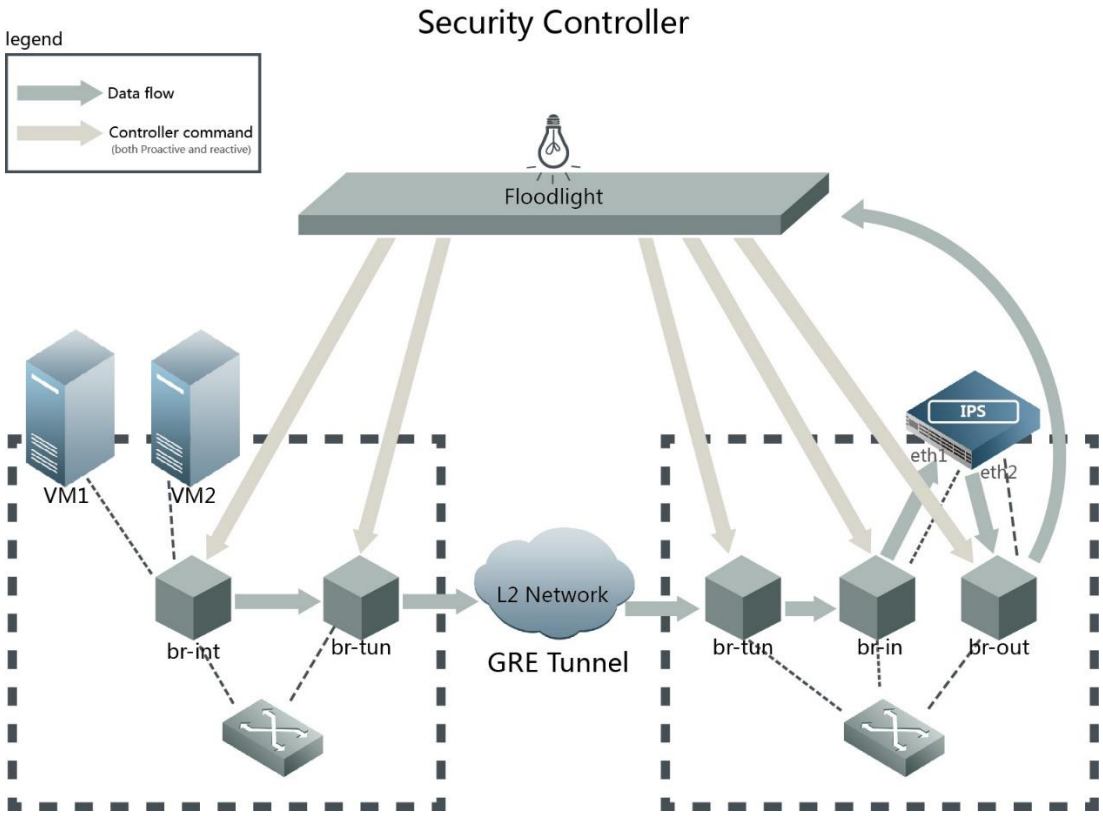

图 1.10　使用 SDN 技术实现流量牵引的原理图

当需要多种类型的安全防护时，数据流就会依次经过多个安全设备，形成一条服务链（Service Chain），如图 1.11 所示。在这种部署模式下，安全设备的部署情况如下表所示。

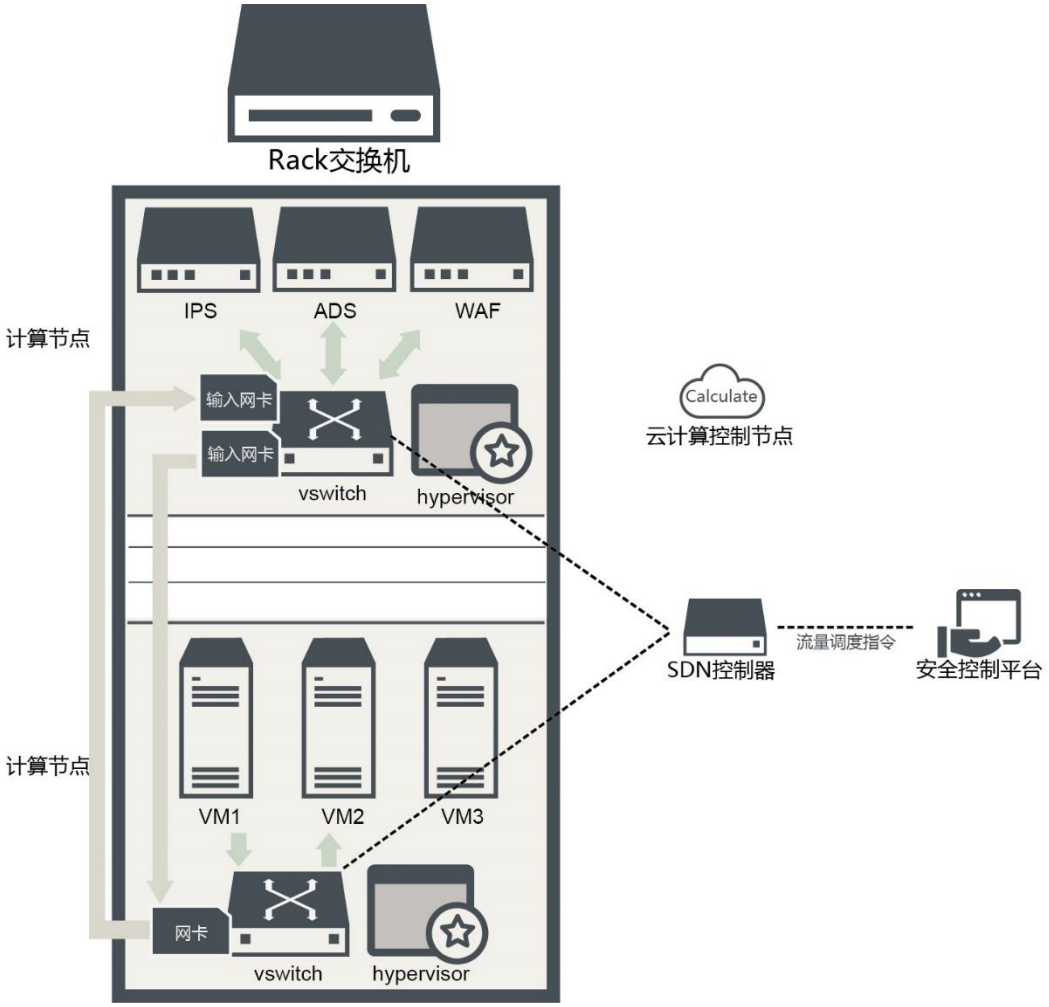

图 1.11　使用 SDN 技术实现服务链

使用 SDN 技术集成模式的设备部署

设备类型	安全设备	部署模式	说明
检测防御	防火墙	二层防火墙	通过 SDN 控制器牵引流量
		三层防火墙	直接路由
	网络入侵防护系统 IPS	旁路部署	通过 SDN 控制器镜像流量
		串联部署	通过 SDN 控制器牵引流量
	网络入侵检测系统 IDS	旁路部署	通过 SDN 控制器镜像流量
	高级威胁分析	旁路部署	通过 SDN 控制器镜像流量
	Web 防火墙	反向代理	正常部署在网络可达处
		透明代理	通过 SDN 控制器牵引流量
	拒绝服务流量监测 NTA		正常部署在网络设备可达处
	流量清洗系统 ADS	物理部署	对于从外向内的恶意流量需部署在物理边界处；防护内部恶意流量通过 SDN 控制器牵引流量
		串联部署	
安全评估	系统扫描器	独立部署	需到物理或虚拟主机网络可达，在网络不直接可达处可通过 SDN 控制器打通两点间路径
	WEB 扫描器	独立部署	需到物理或虚拟主机网络可达，在网络不直接可达处可通过 SDN 控制器打通两点间路径
	配置核查系统	独立部署	需到物理或虚拟主机网络可达，在网络不直接可达处可通过 SDN 控制器打通两点间路径
安全监管	数据库审计	旁路部署	通过 SDN 控制器镜像流量
	安全审计	旁路部署	通过 SDN 控制器镜像流量
	堡垒机	旁路部署	通过 SDN 控制器牵引流量

安全设备的交付形态

绿盟科技的《私有云安全解决方案》中提及的安全设备交付形态有 4 类：支持解隧道的单引擎硬件模式、支持服务链的硬件设备、支持硬件虚拟化的硬件设备，以及虚拟设备镜像，然而本文主要讨论使用新技术实现软件定义的安全方案，所以如不加特殊说明，本章讨论的场景中主要为支持服务链的硬件设备这种交付模式。其特点如下：

当安全设备自身能实现虚拟化后，通过资源池化，可在多个物理安全设备中启动多种及多个虚拟安全设备的实例，再经过服务编排，将流量依次进过一个或多个物理安全设备中的虚拟安全设备，可以完成相应功能的服务链。

如图 1.12 中的客户物理设备中的虚拟机流量，可以依次进过虚拟防火墙、虚拟 IPS 和虚拟 TAC 设备，完成访问控制、数据包分析和行为检测。这种交付模式比较灵活，一个物理安全设备就能完成多种安全功能，整体的安全功能还可以得到横向扩展，但是对整体的安全服务编排提出了很高的要求。

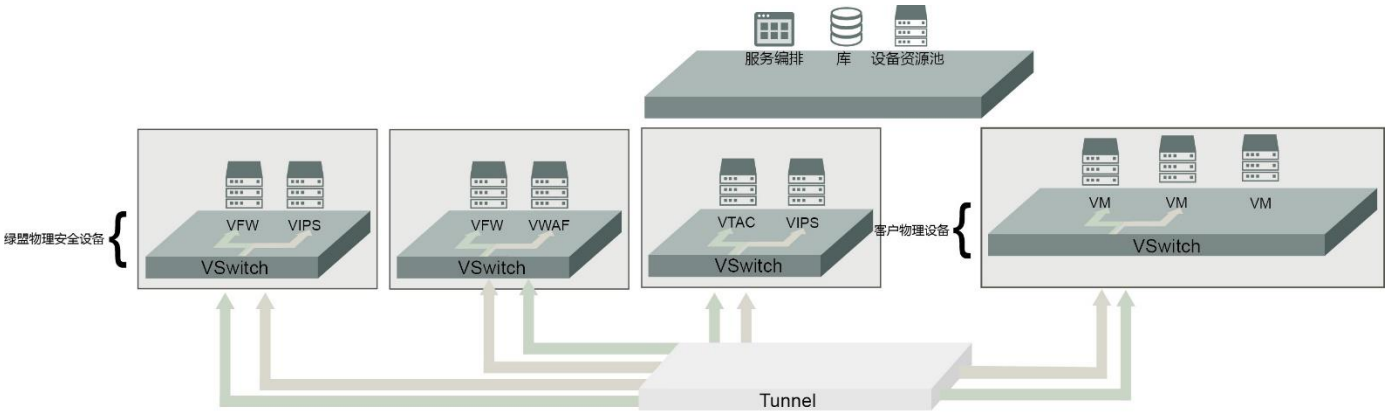

图 1.12　支持服务链的硬件交付模式

DDoS 检测清洗

使用 SDN 技术可以从交换机上获取流量统计信息，并根据特征值判断是否存在恶意攻击，Radware 和 Broadcade 均在 ONS 2014 大会上做过展示类似的方案。

利用相似的思路，可借助安全控制平台中的流相关的组件，从 SDN Network Controller（NC）中获得相应的流量，并根据抗 DDoS 应用订阅的恶意流特征进行检测，发现恶意流量后，应用可根据细粒度的检测判断是否出现恶意攻击，如是则下发实时清洗的流指令，即可将恶意流量牵引到清洗设备 ADS 上。

整个过程如图 1.13 所示，从功能上，安全应用等同于绿盟的网络流量分析设备 NTA，但该应用可使用 NTA 的引擎，并可根据云平台的虚拟资产信息进行细粒度检测，同时可以直接从 APPStore 上获得，所以整体方案的交付和运行效率较传统方案加速效果非常明显。

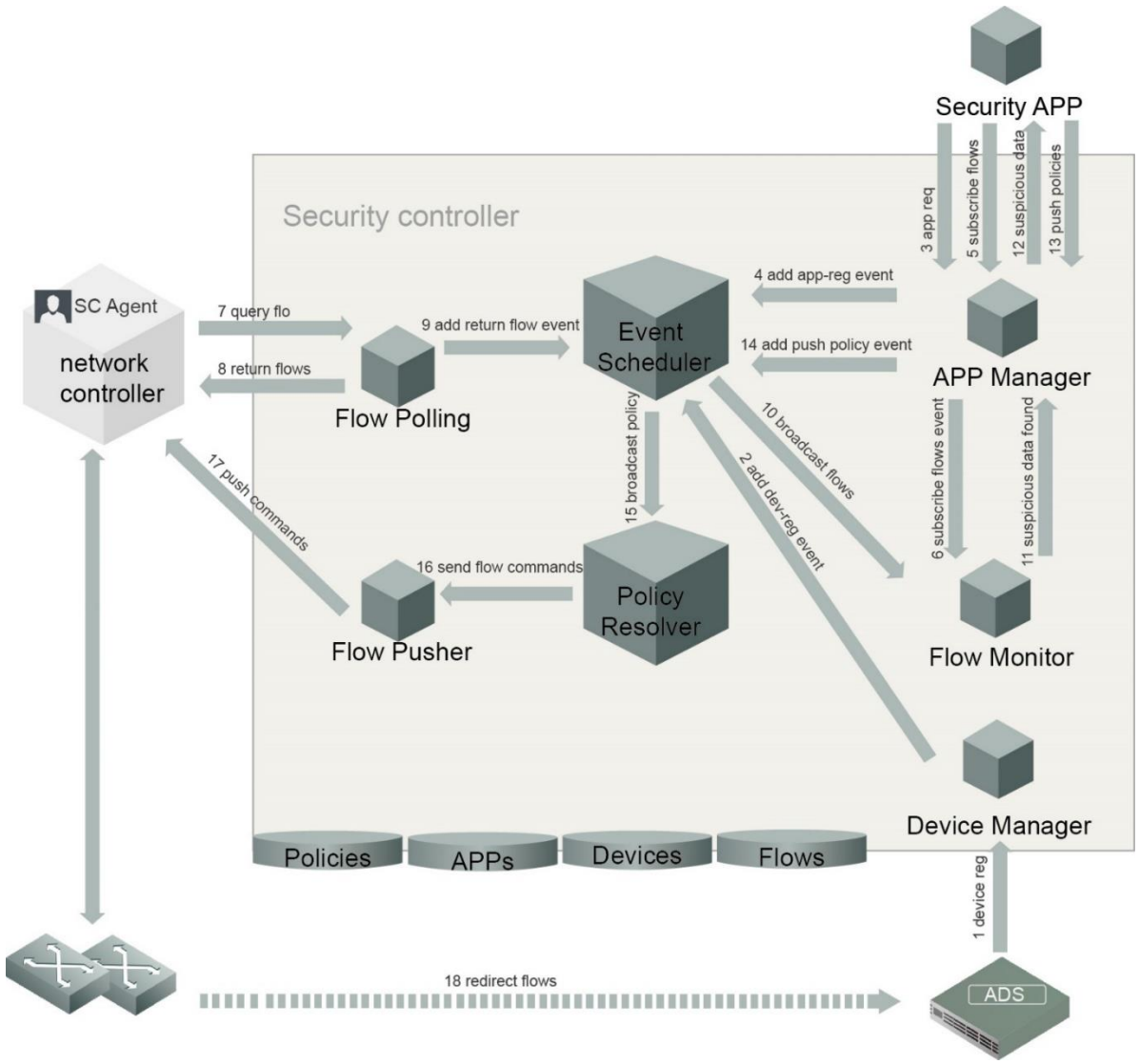

图 1.13　使用安全控制平台实现 DDoS 检测和清洗

测试表明（如图 1.14 所示），攻击者发动 DDoS 攻击时，当流建立速度为 4000 新流/秒时，安全控制器的处理时延为 1-1.5 秒，当流建立速度为 8000 新流/秒时，时延增加为 1-2.2 秒。总体而言，基于流的检测速度相对较快，当流检测使用分布式实时处理框架 Strom 后，流检测模块可部署在多个节点上运行，整体处理效率也较高。

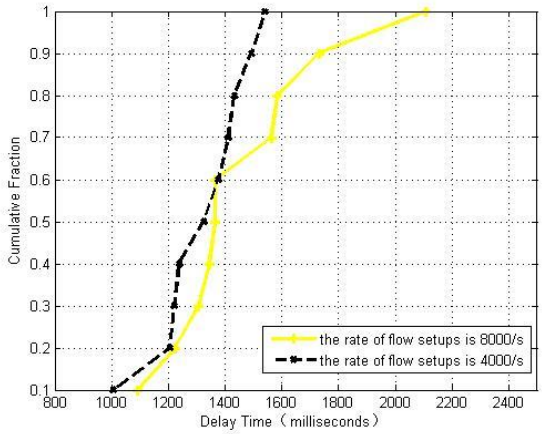

图 1.14　处理延迟的累计概率函数

APT 攻击检测和防护

传统安全防御机制在 APT 攻击下缺乏必要的检测和可视化能力，因此近年来有大量的建有较完善防御机制的企业被恶意攻击者成功入侵。例如：2009 年极光行动：通过 APT 攻击 Google 和其它科技公司，目的似乎是试图获取存取权限并可能尝试修改应用代码；2011 年 RSA 公司的部分 SecurID 动态密码生成器被窃取，攻击者进一步攻击使用 SecurID 双因子认证的客户，窃取其机密信息；2014 年美国零售巨头 Target 因为供应链服务商被攻破，导致其内部的 4000 万客户的信用卡信息被盗取。当很多公司开始部署私有云提高生产效率的同时，攻击面扩展到了企业物理区域以外，防护边界变得模糊；另安全产品虚拟化的滞后、安全设备检测点不易部署和整体安全方案的复杂，导致整体的安全机制不完善，特别是公有云用户往往是中小企业，无法在安全方面大量投入。这类攻击导致云中用户资料泄密、篡改，企业的业务中断乃至声誉受损、竞争力丧失。

当前有一些公司开始研究抵御 APT 攻击，如美国 FireEye 公司的 APT 防护方案在 2013 年捕获了 14 个 0Day 漏洞，但美国将其列为对华禁运的高科技安全产品，国内无法获取相关技术。绿盟科技于 2013 年开始研制抵御 APT 攻击的威胁分析系统 TAC，除集成已知威胁检测技术外，使用动态检测技术，可不依赖传统签名技术检测未知威胁，具有详尽的报警信息和极少的误报率。虽然深度检测设备可分析高级复杂的攻击模式，但需要较多资源，整体效率较低；而 IPS 或者 NBA 产品检测会有很高的误报率。

我们提出的安全控制平台和安全设备协同机制，可依次从全局数据流、满足某些特征的数据包和某个软件行为三个方面逐级加强对数据和行为的检测，整体流程如图 1.15 所示。分析全局流量可避免设备的检测死角并提高检测效率，使用传统检测和深度检测结合的方式，一方面筛除了大量正常的数据流，减轻检测系统负担，另一方面使用静态检测加动态运行检测的方式有效检测出未知恶意行为，大大减少了误报率。安全控制器通过流量调度和安全设备动态部署，提高了整体的检测性能。

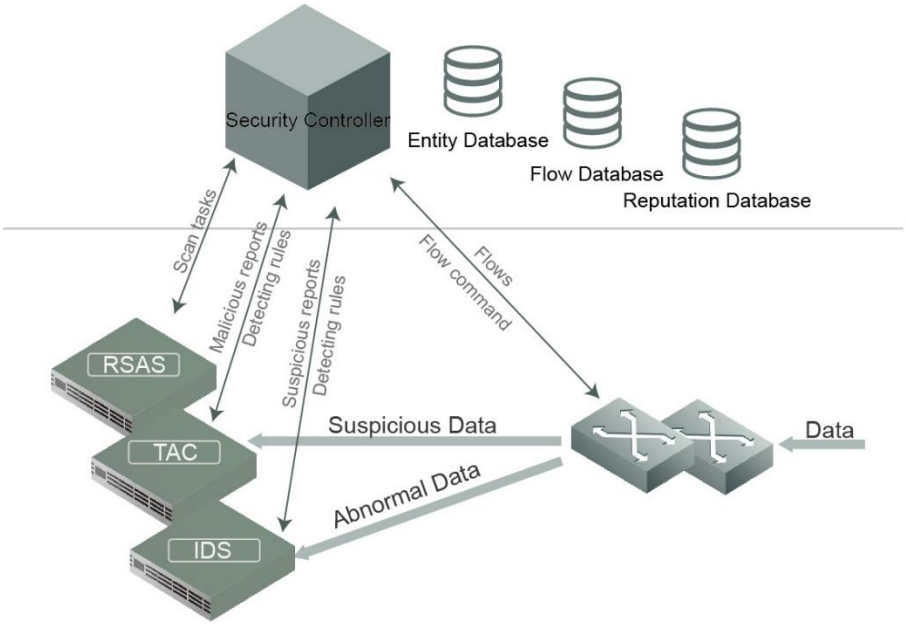

图 1.15　软件定义的 APT 防护流程

安全控制平台可结合 SDN 和虚拟化云平台，在详细的全局知识视图下对异常流量和异常行为进行检测和决策，可进行准确的处置，进一步结合设备的历史告警和日志对外部和被攻破的内部虚拟用户进行恶意行为追溯。 具体地，安全控制平台的模块可根据局部网络设备上的流表信息构建全局的数据流知识库，即可掌握全局范围内所有历史时刻的数据流在每个网络设备的流向。一旦某时刻出现异常的流（访问可疑目的地、流量异常等），即可将可疑流牵引到 IPS 设备上做数据包的深度检测，出现疑似恶意行为即可向上提交告警，以便安全控制器调度其他安全资源，如 TAC 设备做行为检测，或扫描器查找所有受影响的主机，并做隔离或应用虚拟补丁等。

可见，当发现安全威胁后，具体执行何种操作，完全是通过安全控制平台之上的安全应用，根据客户的安全需求，或威胁的具体类型，按需弹性的进行决策，整个过程都是可通过软件定义的。例如图 1.16 给出的检测防护方案是通过全局流量分析建立

历史时刻的全局流表，建立访问模式的安全基线，当检测出异常方式时，将流量牵引到 IPS 设备做防护。这就是一个强化流检测，简化数据包处理的方案，同样也适用于很多场景。

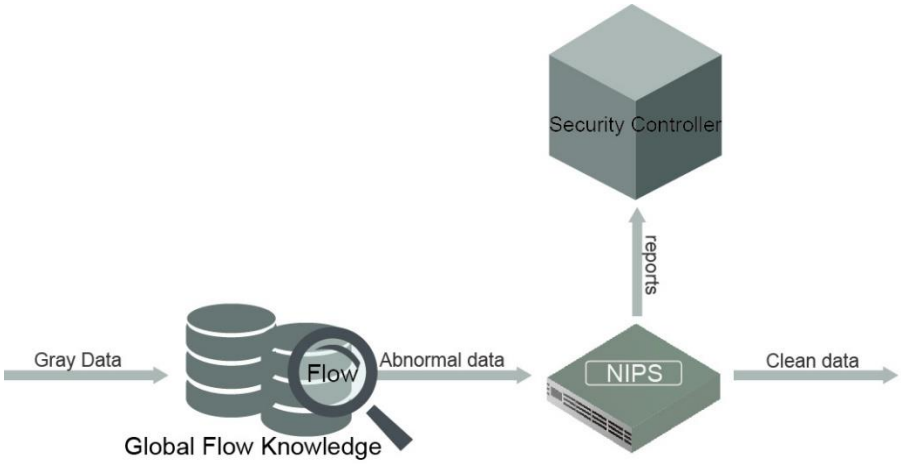

图 1.16　流检测和数据载荷检测的协同

Web 安全应用

云计算中比例最大的应用当属 Web 类：Web 站点、Web 服务和 Web 应用。很多 Web 类应用直接对外开放，考虑到 DDoS 攻击商业化，SQL 注入、XSS 注入和跨站等攻击手法以工具化简单化，所以这些应用很容易受到攻击。云环境中需要一种能够快速部署、灵活调度的 Web 安全服务。

融于 IaaS/SDN 的 Web 安全

本节阐述如何在支持 SDN 技术的云环境中部署 Web 安全应用，此处以 Openstack 为例，安全应用可集成到 Openstack 的管理前端 Horizon 中，如下图所示。

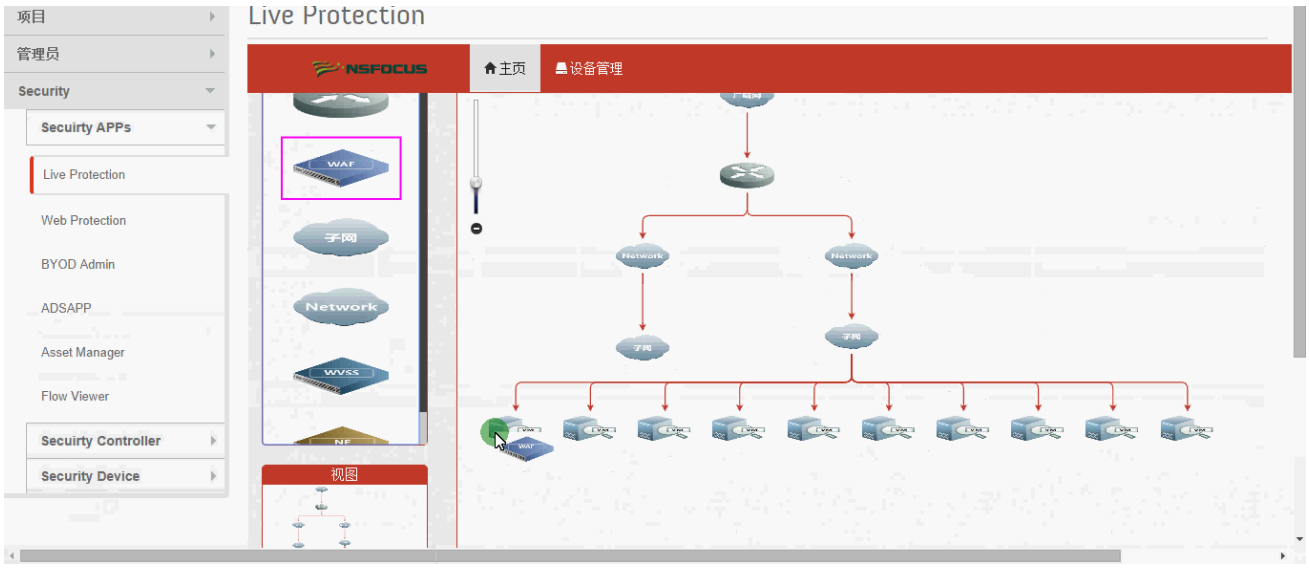

图 1.17　在线的 Web 防护界面

整体工作流如图 1.18 所示，当用户需要部署 WAF（Web 应用防火墙）时，可以在安全应用的管理层侧将 WAF 拖到相应的被防护虚拟机上，配置好 WAF 的部署模式、管理地址等，点击确定。此时，安全控制平台自动完成三个任务：1）通过守护进程准备好并启动相应的 WAF 虚拟机，2）通过 SDN 将流量牵引到 WAF 的入口，3）向 WAF 下发防护站点的策略。

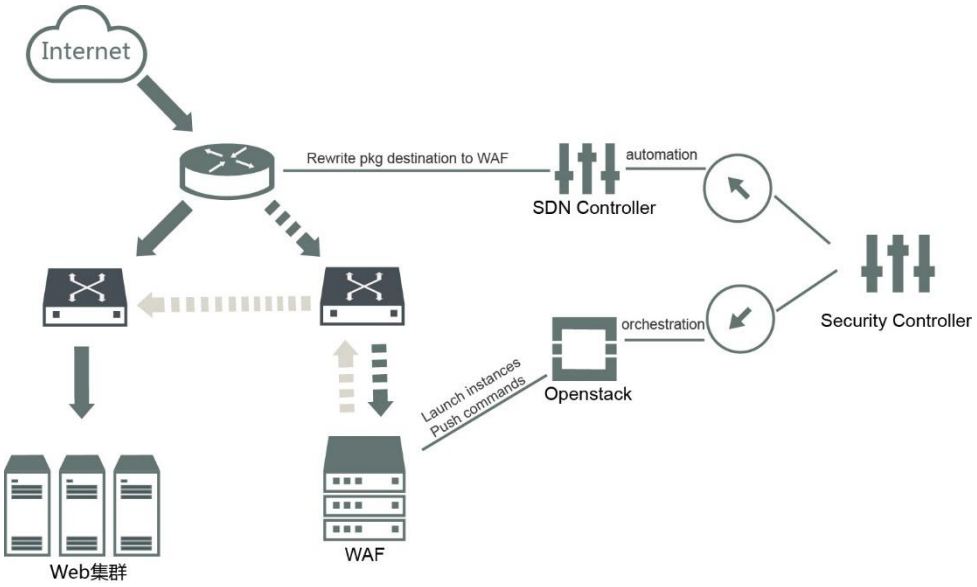

图 1.18　在线的 Web 防护流程

这种部署方式客户仅仅需了解少量信息即可，不像以往需要了解 WAF 的部署模式、规则配置、拓扑规划等，所有这些工作均有安全控制平台、SDN 控制器和虚拟化系统完成。

与传统的 Web 安全云服务相比，如安全宝、加速乐，这种方案通过 SDN 技术可将流量做地址变换，直接将到路由器上到 Web 服务器的流量通过 2 层网络牵引到 WAF 设备，而无需让用户手动修改域名的指向，从而在保证技术可靠性的前提下，提供了便利性和提高了防护速度。

一体化的 Web 安全应用

软件定义安全的概念本身与 SDN 或虚拟化技术是彼此独立的，强调的是安全控制和数据分离，从而改善设备间的协同性，提高防护效率。所以本节给出一个传统网络环境中软件定义的 Web 安全应用，下图中展现的页面是该应用的前端，用户可以实时感知其 Web 站点的运行安全状态。

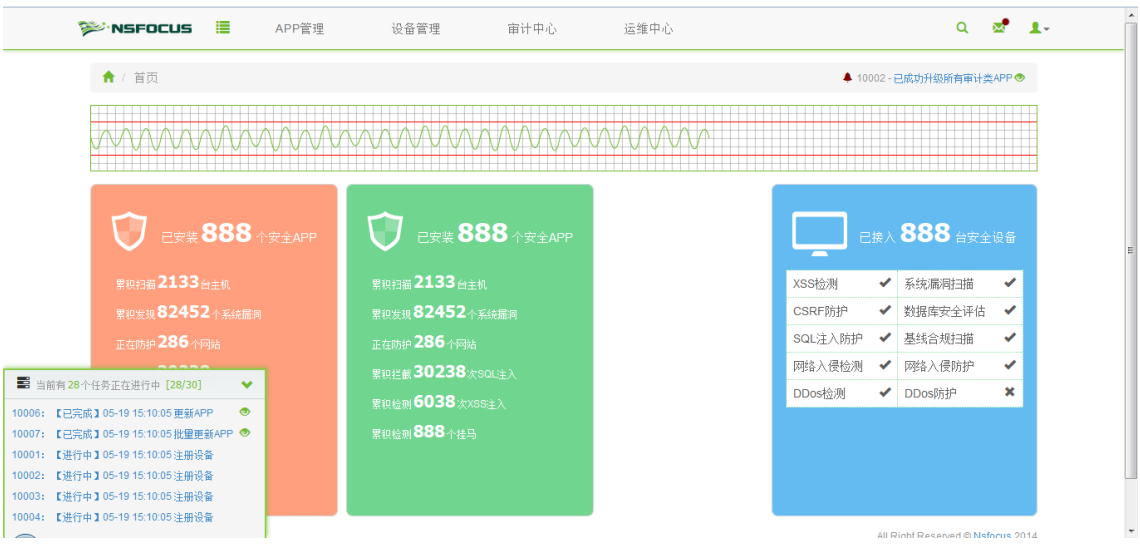

图 1.19　多设备协同的 Web 安全应用

当用户点击对某站点进行体检时，安全控制平台即向 Web 漏洞扫描器 WVSS 下发扫描任务，如下图所示。

图 1.20　Web 应用脆弱性评估

扫描结束后，客户会收到一份关于该站点的脆弱性报告， 如下图所示。

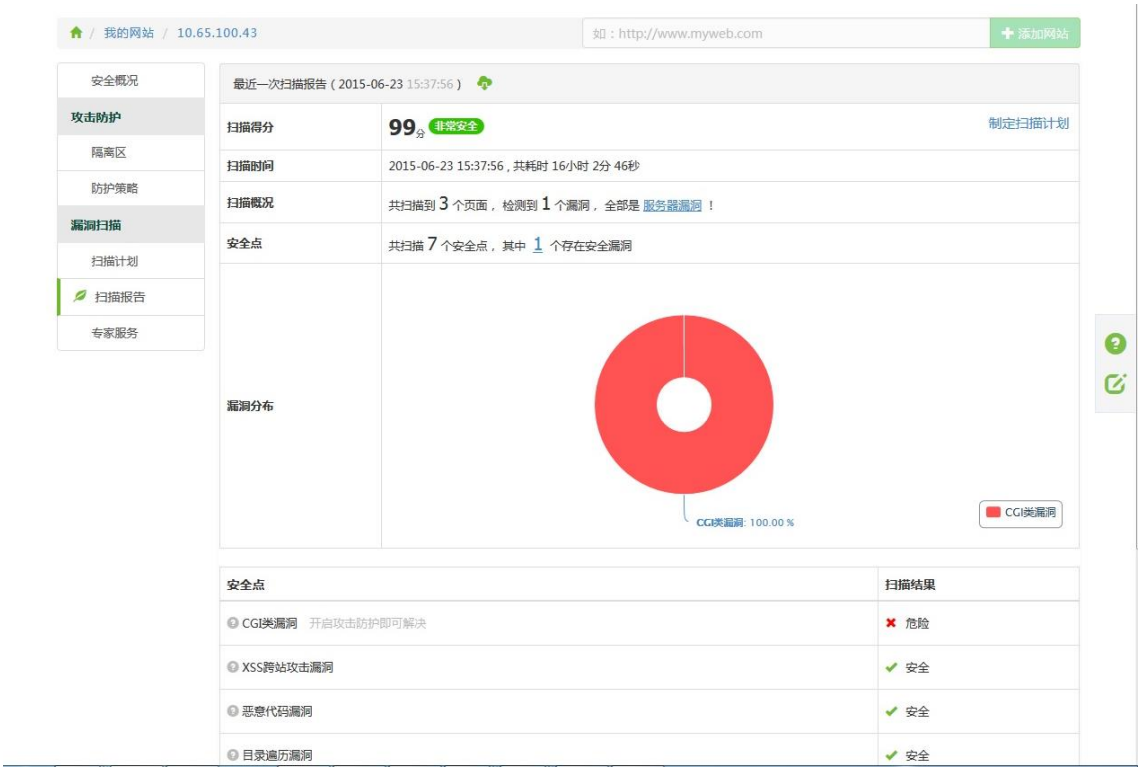

图 1.21　Web 应用脆弱性评估报表

如果用户发现该站点存在漏洞，则可直接启用防护，如下图所示；随后安全控制平台根据知识库中的漏洞与防护方法的对应关系，找到相应的虚拟补丁，将其作为策略下发到防护 WAF 中。

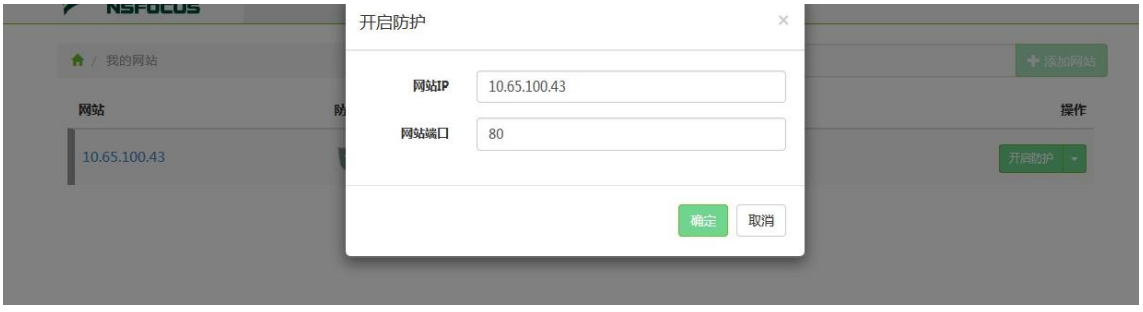

图 1.22　扫描网站出现漏洞后可启用防护

当启用防护后，用户可对网站重新扫描，以确定之前启用的防护规则是否生效。如此迭代地形成“扫描”-“防护”的闭环，直到所有的漏洞都被防住。该流程如图 1.23 所示。

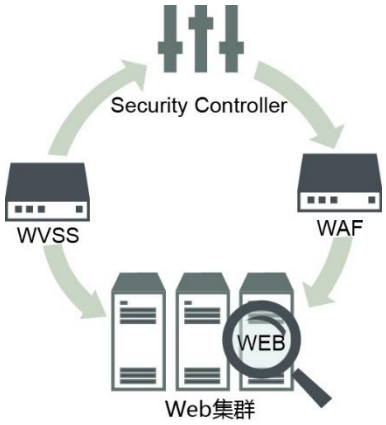

图 1.23 Web 安全应用协同原理

在整个过程中，用户感知到的始终是一个 Web 应用，提供网站体检和网站防护的功能，而不需要关心底层的 WVSS 或 WAF 等安全设备，包括这些设备的形态（虚拟还是实体）、部署模式，以及发现漏洞到应用补丁之间的内在关联。所以软件定义使用户摆脱了以往复杂的部署、配置和运维的体验，并且缩短了漏洞从发现到修复的宝贵时间窗口。

软件定义安全 SDS

SECURITY⊕

软件定义安全（SDS）不一定是应对新型安全威胁的银弹，因为软件定义从原理上没有解决传统安全不能解决的新问题。然而，新型威胁挑战的是传统防护体系臃肿、低效、部署受限、反应迟钝、可视化差等弱点，软件定义正是以开放、高效、灵活、快速等特性，以快速响应应对漏洞，以应用协同应对持续威胁，以自适应灵活部署安全机制应对可能的绕过渗透。

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。在此基础上，绿盟科技在业界率先提出了软件定义安全的架构，并通过若干场景下的实践，验证了软件定义安全的理念确实可以极大改善用户体验、提高防护效率，真实解决客户的安全问题。《软件定义安全 SDS》的推出，即是对软件定义安全架构及实践的总结，给大家提供参考。

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 大会与云杉网络演示的公有云异常流量分析与可视化展现，以及与绿网科技的 GNFlush 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。

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，并正在参与编写《信息系统等级保护云计算安全设计技术指南》中的边界和通信安全部分。

诚然，软件定义安全不是一蹴而就的，安全生态圈的建立、安全应用的协同、安全设备的重构，均非一朝一夕能实现的。不过为解决客户的真正问题，迎战互联网安全企业的挑战，各大安全企业应抛开成见、去除壁垒，实现安全能力的开放，以自身的安全经验积累通过安全应用实现分析、检测、防护和反馈等一系列高效的安全体系。

作者和贡献者

刘文懋，绿盟科技　　Email：liuwenmao@nsfocus.com

关注软件定义安全 SDS

如果您希望与我们一起持续关注这个项目，请关注：

- 绿盟科技安全报告：http://www.nsfocus.com.cn/research/report.html
- 绿盟科技官方微博：http://weibo.com/nsfocus
- 绿盟科技官方博客：http://blog.nsfocus.net/
- 绿盟科技官方微信：

  搜索公众号 绿盟科技

扫描二维码，在线看报告

关于绿盟科技

北京神州绿盟信息安全科技股份有限公司（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 30 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，绿盟科技在网络及终端安全、互联网基础安全、合规及安全管理等领域，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专业安全服务。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS