2015 绿盟科技云安全解决方案

2015 NSFOCUS Cloud Security Solution

目录

图表

关键信息

本方案首先研究了云计算系统的典型结构，分析了云计算系统面临的安全威胁、安全需求和挑战，进而对云安全防护总体架构，包括保障内容和实现机制、部署方法进行了设计和详细阐述，并介绍了云安全相关的安全技术服务内容和范围，最后给出了典型的云安全防护场景。

其中关于软件定义安全体系架构，在之前发布的《2015 绿盟科技软件定义安全 SDS 白皮书》中有详述。

NSFOCUS

随着云计算技术的不断完善和发展，云计算已经得到了广泛的认可和接收，许多组织已经或即将进行云计算系统建设。同时，以信息/服务为中心的模式深入人心，大量的应用正如雨后春笋般出现，组织也开始将传统的应用向云中迁移。同时，云计算技术仍处于不断发展和演进，系统更加开放和易用，功能更加强大和丰富，接口更加规范和开放。例如软件定义网络（简称 SDN）技术、NFV（网络功能虚拟化）等新技术。这必将推动云计算技术的更加普及和完善。

云计算技术给传统的 IT 基础设施、应用、数据以及 IT 运营管理都带来了革命性改变，对于安全管理来说，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问题和挑战，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。

根据调研数据，信息安全风险是客户采用云计算所考虑重大问题之一，且国家和行业安全监管愈加严格，安全已经成为组织规划、设计、建设和使用云计算系统而急需解决的重大问题之一，尤其是不断出现的与云计算系统相关事件让组织更加担心自身的云计算系统安全保障问题。

本方案基于绿盟科技长期对云计算安全的探索和研究，借鉴行业最佳实践，结合绿盟科技近期云计算安全建设经验，提出了云计算安全保障框架和方法。

一 云计算典型体系结构

云计算主要是通过网络，将 IT 以抽象化的方式交付给客户，为基于 IT 的服务交付模式带来了巨大变革。云计算的一些独特优势，使其广为接受，包括：大规模资源池化、资源弹性、按需分配、自动化部署、高可靠性、高运营效率及技术和 IT 的高透明度。

云计算平台的实现主要包括两个方式：虚拟化构成的云和应用程序/服务器构成的云，其中后者的安全防护与传统方式基本相同，不再赘言，这里主要对虚拟化构成的云进行讨论。

目前，计算虚拟化已经成熟，并为组织所广泛采用，如 VMware vSphere、Citrix Xen 等。另外，一些用户开始尝试采用 SDN、NFV 等新型技术，旨在通过软件控制方式解决现网中遇到的存储、网络不能自动部署和分权分域管理问题。

云计算系统分类

根据 NIST 发布的相关规范，云计算系统按照部署方法可分为私有云、公有云、社区云、混合云。为了便于说明，以下内容将主要以私有云为例进行说明。

云计算系统所采用虚拟化技术的不同，对安全防护设计和部署具有一定影响。根据有无才采用 SDN、NFV 技术，可分为两类：原生虚拟化系统和基于 SDN 技术的虚拟化系统。如无特别说明，下述描述均指原生虚拟化系统。

云计算系统典型物理架构

下图给出了一个典型的云计算系统的典型架构。

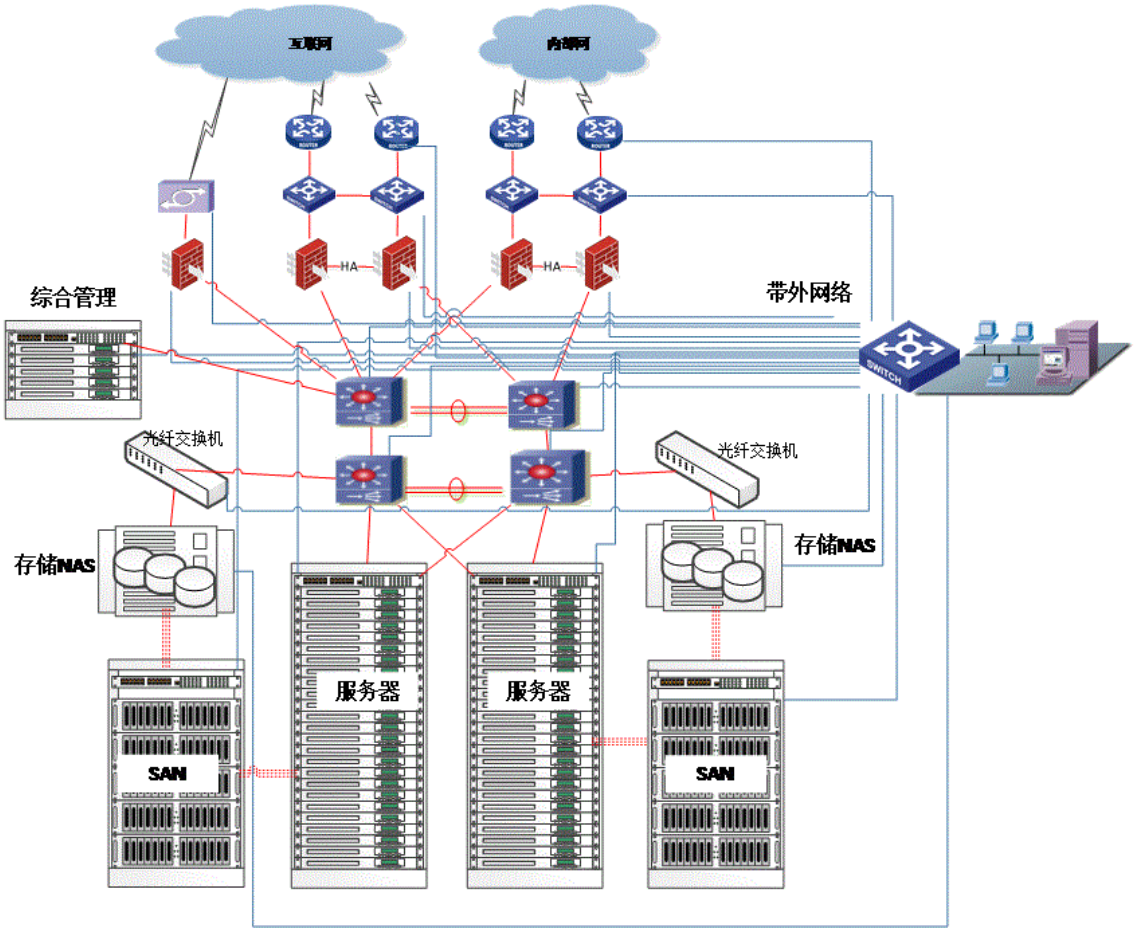

图 一.1 云典型架构

云计算系统通常具有以下特征：

- 核心交换机一般采用高性能数据中心级交换机搭建，支持虚拟化技术，并提供 Internet、内部网络、外部专用网络的接入。通过汇聚交换机（支持虚拟化）提供 x86 服务器、小型机等服务器的接入。
- 与互联网相关，可以提供 VPN 接入，外发访问，以及公众用户对云的访问。
- 与内部网络相同，可以提供内部用户对云的访问，以及和内部其他系统进行信息交互。
- 都有大量的刀片式服务器，并通过虚拟化软件，实现对计算资源的抽象和池化。
- 具有 SAN、NAS 存储系统。具有独立的存储网络。
- 具有独立的综合管理平台，实现对云的运营管理。
- 具有带外网管系统，实现对整个云的运维管理。

云计算系统逻辑结构

云计算系统 一般都包括三个层次两个平台：基础设施即服务(IaaS)、平台即服务（PaaS）、云软件即服务（SaaS）、云管理平台和运维管理平台。如下图所示：

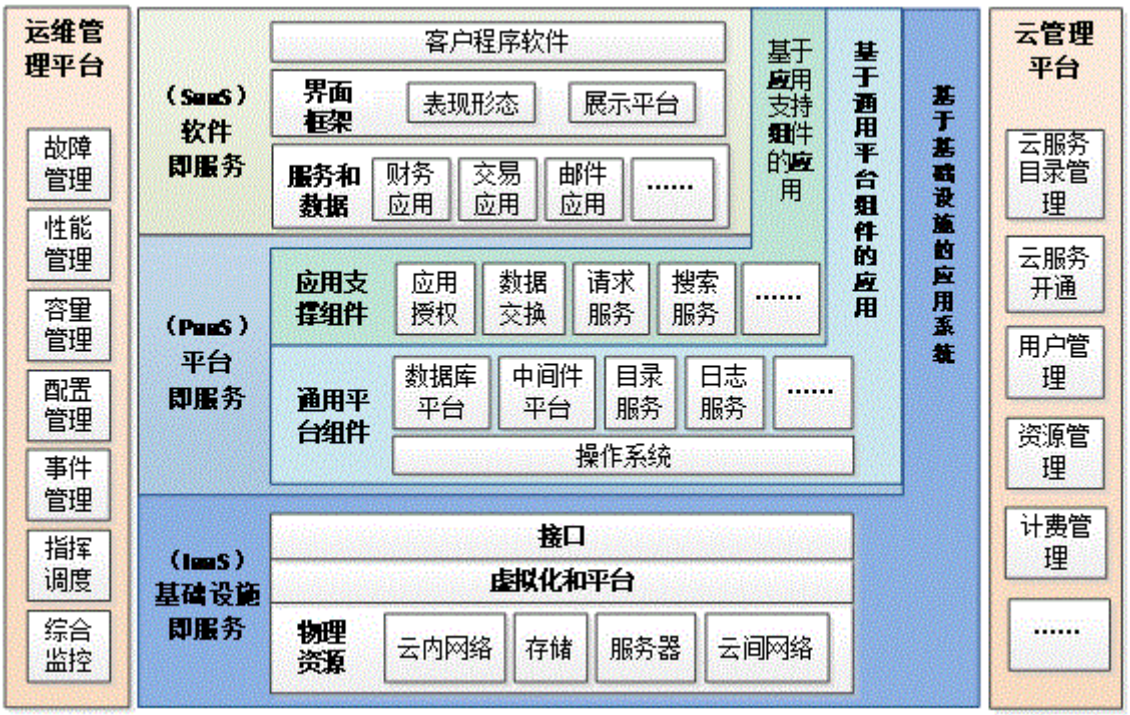

图 一2 云典型逻辑结构

简单说明如下：

- 基础设施即服务层（IaaS）：包括了各种服务器、存储、网络设备、链路等各种物理资源，以及虚拟化管理程序和对外提供服务的接口。可以基于此层对外提供虚拟主机服务；
- 平台即服务层（PaaS）：包括了各种系统、平台、应用软件，可以提供应用软件的开发、测试、部署和运营环境；
- 软件即服务（SaaS）：包括各一系列的应用软件，以及提供各客户/用户使用的交互展示程序。可以通过网络向用户交付相应的应用服务；
- 云管理平台：负责云计算服务的运营，并对云计算资源池系统及其中的各类资源进行集中管理，主要功能包括云服务开通、用户管理、计价管理等功能。通常云管理平台通过与资源池系统之间的资源管理接口下发资源管理指令，并通过网管接口向云维管理平台（网管系统）提供资源池系统内各类设备的管理和监控信息；
- 运维管理平台：实现对虚拟设备、系统、网络的技术维护和管理工作，包括容量、配置和事件管理等功能。一般通过带外网络与各种资源进行互联

二 云计算安全威胁和需求分析

云计算模式通过将数据统一存储在云计算服务器中，加强对核心数据的集中管控，比传统分布在大量终端上的数据行为更安全。由于数据的集中，使得安全审计、安全评估、安全运维等行为更加简单易行，同时更容易实现系统容错、高可用性和冗余及灾备恢复。但云计算在带来方便快捷的同时也带来新的挑战。

安全威胁分析

CSA 在 2013 年的报告中列出了九大安全威胁。依排序分别为 1.数据泄露 2.数据丢失 3.帐户劫持 4.不安全的接口（API） 5.拒绝服务攻击（DDoS） 6.内部人员的恶意操作 7.云计算服务的滥用 8.云服务规划不合理 9.共享技术的漏洞问题。把云计算环境下的安全威胁细化，并按**云计算环境下等级保护**的基本要求进行对应，可得到如下的云计算环境下的具体安全威胁：

- 网络安全部分
  - 业务高峰时段或遭遇 DDoS 攻击时的大流量导致网络拥堵或网络瘫痪
  - 重要网段暴露导致来自外部的非法访问和入侵
  - 单台虚拟机被入侵后对整片虚拟机进行的渗透攻击，并导致病毒等恶意行为在网络内传播蔓延
  - 虚拟机之间进行的 ARP 攻击、嗅探
  - 云内网络带宽的非法抢占
  - 重要的网段、服务器被非法访问、端口扫描、入侵攻击
  - 云平台管理员因账号被盗等原因导致的从互联网直接非法访问云资源
  - 虚拟化网络环境中流量的审计和监控
  - 内部用户或内部网络的非法外联行为的检查和阻断
  - 内部用户之间或者虚拟机之间的端口扫描、暴力破解、入侵攻击等行为
- 主机安全部分：
  - 服务器、宿主机、虚拟机的操作系统和数据库被暴力破解、非法访问的行为
  - 对服务器、宿主机、虚拟机等进行操作管理时被窃听
  - 同一个逻辑卷被多个虚拟机挂载导致逻辑卷上的敏感信息泄露
  - 对服务器的 Web 应用入侵、上传木马、上传 webshell 等攻击行为
  - 服务器、宿主机、虚拟机的补丁更新不及时导致的漏洞利用以及不安全的配置和非必要端口的开放导致的非法访问和入侵
  - 虚拟机因异常原因产生的资源占用过高而导致宿主机或宿主机下的其它虚拟机的资源不足
- 资源抽象安全部分
  - 虚拟机之间的资源争抢或资源不足导致的正常业务异常或不可用
  - 虚拟资源不足导致非重要业务正常运作但重要业务受损
  - 缺乏身份鉴别导致的非法登录 hypervisor 后进入虚拟机
  - 通过虚拟机漏洞逃逸到 hypervisor，获得物理主机的控制权限
  - 攻破虚拟系统后进行任易破坏行为、网络行为、对其它账户的猜解，和长期潜伏
  - 通过 hypervisor 漏洞访问其它虚拟机
  - 虚拟机的内存和存储空间被释放或再分配后被恶意攻击者窃取
  - 虚拟机和备份信息在迁移或删除后被窃取
  - hypervisor、虚拟系统、云平台不及时更新或系统漏洞导致的攻击入侵
  - 虚拟机可能因运行环境异常或硬件设备异常等原因出错而影响其他虚拟机
  - 无虚拟机快照导致系统出现问题后无法及时恢复
  - 虚拟机镜像遭到恶意攻击者篡改或非法读取
- 数据安全及备份恢复
  - 数据在传输过程中受到破坏而无法恢复

- 在虚拟环境传输的文件或者数据被监听
- 云用户从虚拟机逃逸后获取镜像文件或其他用户的隐私数据
- 因各种原因或故障导致的数据不可用
- 敏感数据存储漂移导致的不可控
- 数据安全隔离不严格导致恶意用户可以访问其他用户数据

为了保障云平台的安全，必须有有效的抵御或消减这些威胁，或者采取补偿性的措施降低这些威胁造成的潜在损失。当然，从安全保障的角度讲，还需要兼顾其他方面的安全需求。

安全需求和挑战

从风险管理的角度讲，主要就是管理资产、威胁、脆弱性和防护措施及其相关关系，最终保障云计算平台的持续安全，以及其所支撑的业务的安全。

云计算平台是在传统 IT 技术的基础上，增加了一个虚拟化层，并且具有了资源池化、按需分配，弹性调配，高可靠等特点。因此，传统的安全威胁种类依然存在，传统的安全防护方案依然可以发挥一定的作用。综合考虑云计算所带来的变化、风险，从保障系统整体安全出发，其面临的主要挑战和需求如下：

- 法律和合规
- 动态、虚拟化网络边界安全
- 虚拟化安全
- 流量可视化
- 数据保密和防泄露
- 安全运维和管理

针对云计算所面临的安全威胁及来自各方面的安全需求，需要对科学设计云计算平台的安全防护架构，选择安全措施，并进行持续管理，满足云计算平台的全生命周期的安全。

三 云安全防护总体架构设计

云安全防护设计应充分考虑云计算的特点和要求，基于对安全威胁的分析，明确来各方面的安全需求，充分利用现有的、成熟的安全控制措施，结合云计算的特点和最新技术进行综合考虑和设计，以满足风险管理要求、合规性的要求，保障和促进云计算业务的发展和运行。

设计思路

在进行方案设计时，将遵循以下思路：

- 保障云平台及其配套设施
  - 云计算除了提供 IaaS、PaaS、SaaS 服务的基础平台外，还有配套的云管理平台、运维管理平台等。要保障云的安全，必须从整体出发，保障云承载的各种业务、服务的安全。
- 基于安全域的纵深防护体系设计
  - 对于云计算系统，仍可以根据威胁、安全需求和策略的不同，划分为不同的安全域，并基于安全域设计相应的边界防护策略、内部防护策略，部署相应的防护措施，从而构造起纵深的防护体系。当然，在云平台中，安全域的

边界可能是动态变化的，但通过相应的技术手段，可以做到动态边界的安全策略跟随，持续有效的保证系统的安全。

- 以安全服务为导向，并符合云计算的特点
  - 云计算的特点是按需分配、资源弹性、自动化、重复模式，并以服务为中心的。因此，对于安全控制措施选择、部署、使用来讲必须满足上述特点，即提供资源弹性、按需分配、自动化的安全服务，满足云计算平台的安全保障要求。
- 充分利用现有安全控制措施及最新技术
  - 在云计算环境中，还存在的传统的网络、主机等，同时，虚拟化主机中也有相应的操作系统、应用和数据，传统的安全控制措施仍旧可以部署、应用和配置，充分发挥防护作用。另外，部分安全控制措施已经具有了虚拟化版本，也可以部署在虚拟化平台上，进行虚拟化平台中的东西向流量进行检测、防护。
- 充分利用云计算等最新技术
  - 信息安全措施/服务要保持安全资源弹性、按需分配的特点，也必须运用云计算的最新技术，如 SDN、NFV 等，从而实现按需、简洁的安全防护方案。
- 安全运营
  - 随着云平台的运营，会出现大量虚拟化安全实例的增加和消失，需要对相关的网络流量进行调度和监测，对风险进行快速的监测、发现、分析及相应管理，并不断完善安全防护措施，提升安全防护能力。

安全保障目标

通过人员、技术和流程要素，构建安全监测、识别、防护、审计和响应的综合能力，有效抵御相关威胁，将云平台的风险降低到企业可接受的程度，并满足法律、监管和合规性要求，保障云计算资源/服务的安全。

安全保障体系框架

云平台的安全保障可以分为管理和技术两个层面。首先，在技术方面，需要按照分层、纵深防御的思想，基于安全域的划分，从物理基础设施、虚拟化、网络、系统、应用、数据等层面进行综合防护；其次，在管理方面，应对云平台、云服务、云数据的整个生命周期、安全事件、运行维护和监测、度量和评价进行管理。云平台的安全保障体系框架如下图所示：

图 三.3 云平台安全保障体系框架

简单说明如下：

- **物理环境安全：**在物理层面，通过门禁系统、视频监控、环境监控、物理访问控制等措施实现云运行的物理环境、环境设施等层面的安全；
- **虚拟化安全：**在虚拟化层面，通过虚拟层加固、虚拟机映像加固、不同虚拟机的内存/存储隔离、虚拟机安全检测、虚拟化管理安全等措施实现虚拟化层的安全；
- **网络安全：**在网络层，基于完全域划分，通过防火墙、IPS、VLAN ACL 手段进行边界隔离和访问控制，通过 VPN 技术保障网络通信完全和用户的认证接入，在网络的重要区域部署入侵监测系统（IDS）以实现对网络攻击的实时监测和告警，部署流量监测和清洗设备以抵御 DDoS 攻击，部署恶意代码监测和防护系统以实现对恶意代码的防范。需要说明的是这里的网络包括了实体网络和虚拟网络，通过整体防御保障网络通信的安全；
- **主机安全**：通过对服务主机/设备进行安全配置和加固，部属主机防火墙、主机 IDS，以及恶意代码的防护、访问控制等技术手段对虚拟主机进行保护，确保主机能够持续的提供稳定的服务；
- **应用安全：**通过 PKI 基础设施对用户身份进行标识和鉴别，部署严格的访问控制策略，关键操作的多重授权等措施保证应用层安全，同时采用电子邮件防护、Web 应用防火墙、Web 网页防篡改、网站安全监控等应用安全防护措施保证特定应用的安全；
- **数据保护：**从数据隔离、数据加密、数据防泄露、剩余数据防护、文档权限管理、数据库防火墙、数据审计方面加强数据保护，以及离线、备份数据的安全；
- **安全管理：**根据 ISO27001、COBIT、ITIL 等标准及相关要求，制定覆盖安全设计与获取、安全开发和集成、安全风险管理、安全运维管理、安全事件管理、业务连续性管理等方面安全管理制度、规范和流程，并配置相应的安全管理组织和人员，并建议相应的技术支撑平台，保证系统得到有效的管理

上述安全保障内容和目标的实现，需要基于 PKI、身份管理等安全基础支撑设施，综合利用安全成熟的安全控制措施，并构建良好的安全实现机制，保障系统的良好运转，以提供满足各层面需求的安全能力。

由于云计算具有资源弹性、按需分配、自动化管理等特点，为了保障其安全性，就要求安全防护措施/能力也具有同样的特点，满足云计算安全防护的要求，这就需要进行良好的安全框架设计。

安全保障体系总体技术实现架构设计

云计算平台的安全保障技术体系不同于传统系统，它也必须实现和提供资源弹性、按需分配、全程自动化的能力，不仅仅为云平台提供安全服务，还必须为租户提供安全服务，因此需要在传统的安全技术架构基础上，实现安全资源的抽象化、池化，提供弹性、按需和自动化部署能力。

总体技术实现架构

充分考虑云计算的特点和优势，以及最新的安全防护技术发展情况，为了达成提供资源弹性、按需分配的安全能力，云平台的安全技术实现架构设计如下：

图 三4 云平台安全技术实现架构

说明：

- **安全资源池**：可以由传统的物理安全防护组件、虚拟化安全防护组件组成，提供基础的安全防护能力；
- **安全平台：**提供对基础安全防护组件的注册、调度和安全策略管理。可以设立一个综合的安全管理平台，或者分立的安全管理平台，如安全评估平台、异常流量检测平台等；
- **安全服务**：提供给云平台租户使用的各种安全服务，提供安全策略配置、状态监测、统计分析和报表等功能，是租户管理其安全服务的门户

通过此技术实现架构，可以实现安全服务/能力的按需分配和弹性调度。当然，在进行安全防护措施具体部署时，仍可以采用传统的安全域划分方法，明确安全措施的部署位置、安全策略和要求，做到有效的安全管控。对于安全域的划分方法详见第五章。

对于具体的安全控制措施来讲，通常具有硬件盒子和虚拟化软件两种形式，可以根据云平台的实际情况进行部署方案选择。

与云平台体系架构的无缝集成

云平台的安全防护措施可以与云平台体系架构有机的集成在一起，对云平台及云租户提供按需的安全能力。

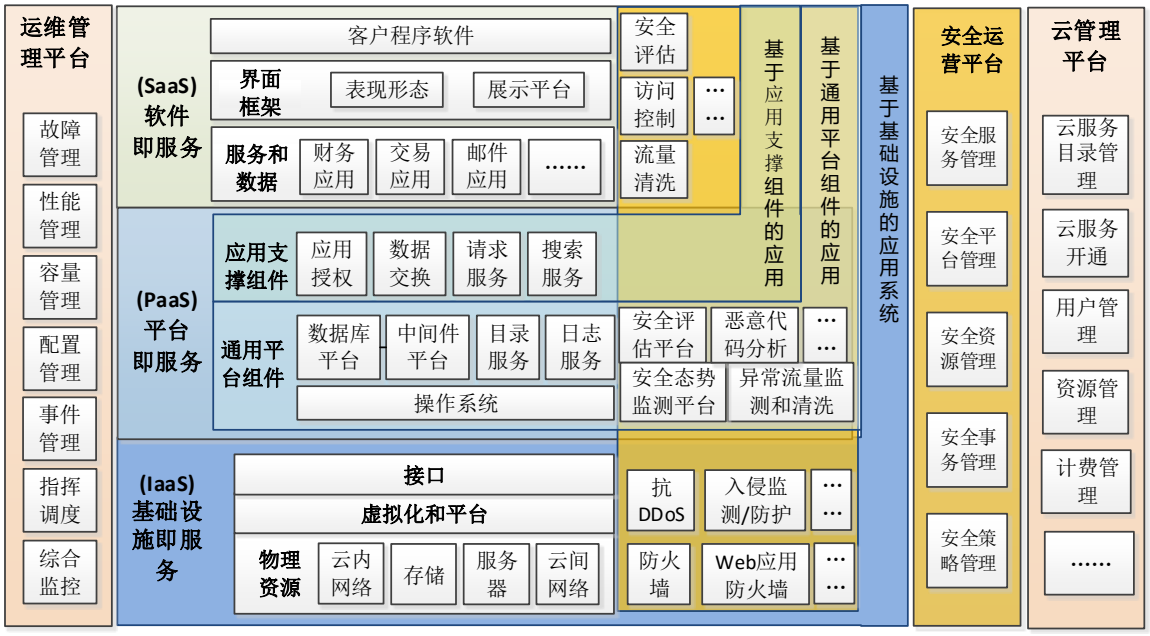

图 三.5 具有安全防护机制的云平台体系架构

工程实现

云平台的安全保障体系最终落实和实现应借鉴工程化方法，严格落实“三同步”原则，在系统规划、设计、实现、测试等阶段把落实相应的安全控制，实现安全控制措施与云计算平台的无缝集成，同时做好运营期的安全管理，保障虚拟主机/应用/服务实例创建的同时，同步部署相应的安全控制措施，并配置相应的安全策略。

四 云平台安全域划分和防护设计

安全域是由一组具有相同安全保护需求、并相互信任的系统组成的逻辑区域，在同一安全域中的系统共享相同的安全策略，通过安全域的划分把一个大规模复杂系统的安全问题，化解为更小区域的安全保护问题，是实现大规模复杂信息系统安全保护的

有效方法。安全域划分是按照安全域的思想，以保障云计算业务安全为出发点和立足点，把网络系统划分为不同安全区域，并进行纵深防护。

对于云计算平台的安全防护，需要根据云平台安全防护技术实现架构，选择和部署合理的安全防护措施，并配置恰当的策略，从而实现多层、纵深防御，才能有效的保证云平台资源及服务的安全。

安全域划分

安全域划分的原则

- 业务保障原则：安全域方法的根本目标是能够更好的保障网络上承载的业务。在保证安全的同时，还要保障业务的正常运行和运行效率；
- 结构简化原则：安全域划分的直接目的和效果是要将整个网络变得更加简单，简单的网络结构便于设计防护体系。比如，安全域划分并不是粒度越细越好，安全域数量过多过杂可能导致安全域的管理过于复杂和困难；
- 等级保护原则：安全域划分和边界整合遵循业务系统等级防护要求，使具有相同等级保护要求的数据业务系统共享防护手段；
- 生命周期原则：对于安全域的划分和布防不仅仅要考虑静态设计，还要考虑云平台扩容及因业务运营而带来的变化，以及开发、测试及后期运维管理要求

安全域的逻辑划分

按照纵深防护、分等级保护的理念，基于云平台的系统结构，其安全域的逻辑划分如下图所示：

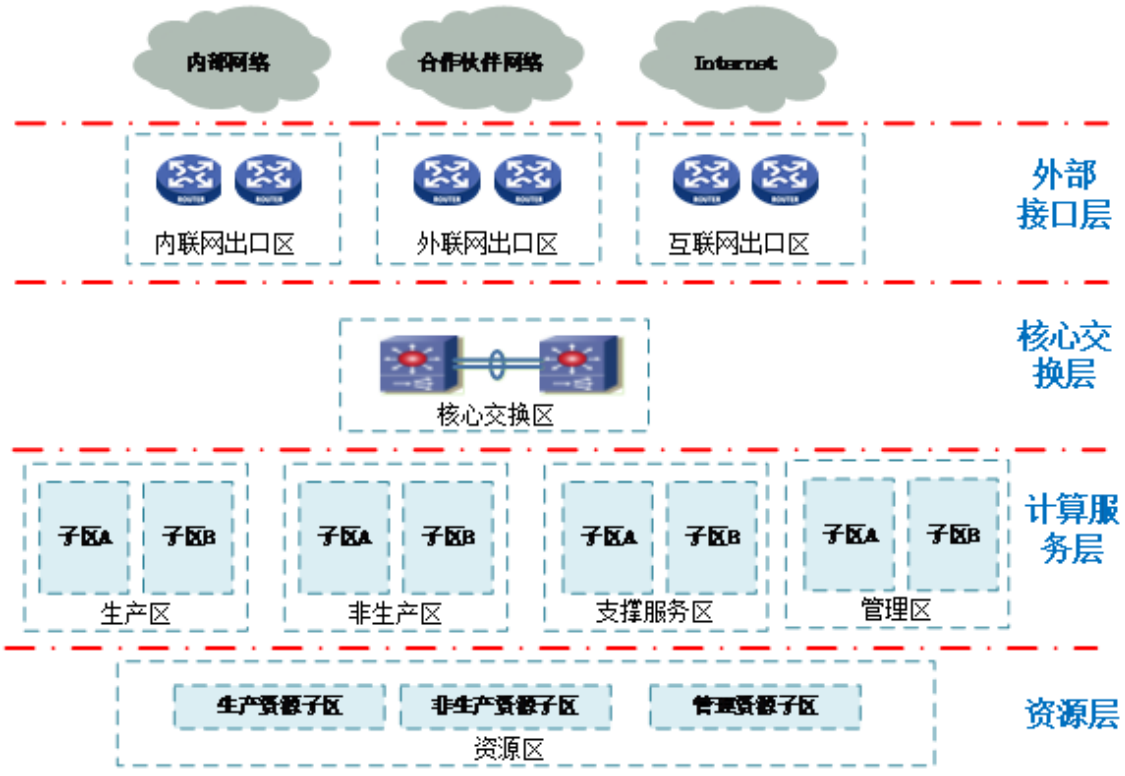

图 四.6 云平台安全域逻辑划分

按照防护的层次，从外向内可分为外部接口层、核心交换层、计算服务层、资源层。根据安全要求和策略的不同，每一层再分为不同的区域。对于不同的区域，可以根据实际情况再细分为不同的区域。例如，根据安全等级保护的要求，对于生产区可以在细分为一级保护生产区、二级保护生产区、三级保护生产区、四级保护生产区，或者根据管理主体的不同，也可细分为集团业务生产区、分支业务生产区。

对于实际的云计算系统，在进行安全域划分时，需要根据系统的架构、承载的业务和数据流、安全需求等情况，按照层次化、纵深防御的安全域划分思想，进行科学、严谨的划分，不可死搬硬套，下面给出一个安全域划分的示例，可参考。

安全域的划分示例

根据某数据中心的实际情况及安全等级防护要求，安全域划分如下图所示：

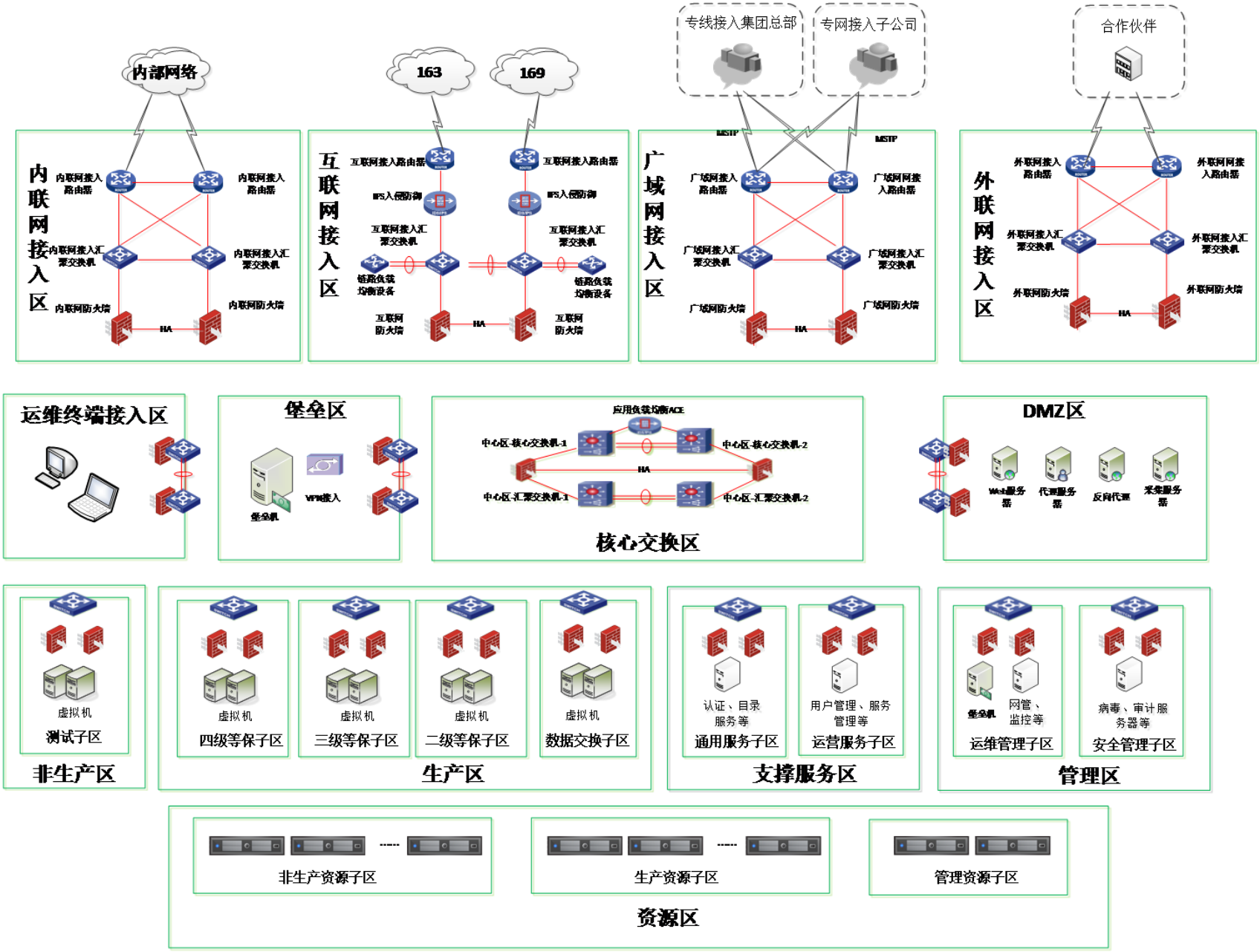
内部网络
163
169
专线接入集团总部
专网接入子公司
合作伙伴
内联网接入区
互联网接入区
广域网接入区
外联网接入区
运维终端接入区
堡垒区
核心交换区
DMZ区
非生产区
生产区
支撑服务区
管理区
资源区
测试子区
四级等保子区
三级等保子区
二级等保子区
数据交换子区
通用服务子区
运营服务子区
运维管理子区
安全管理子区
非生产资源子区
生产资源子区
管理资源子区

图 四.7 安全域划分示例

说明如下：

- **互联网接入区**：主要包括接入交换机、路由器、网络安全设备等，负责实现与 163、169、CMNET 等互联网的互联；
- **内联网接入区**：主要包括接入交换机、路由器、网络安全设备等，负责实现与组织内部网络的互连；
- **广域网接入区**：主要包括接入交换机、路由器、网络安全设备等，负责与本组织集团或其他分支网络的接入；
- **外联网接入区**：主要包括接入交换机、路由器、网络安全设备等，负责本组织第三方合作伙伴网络的接入，如银行、合作网络等；
- **核心交换区**：由支持虚拟交换的高性能交换机组成。负责整个云计算系统内部之间、内部与外部之间的通信交换；
- **生产区**：主要包括一系列提供正常业务服务的虚拟主机、平台及应用软件，使提供 IaaS、PaaS、SaaS 服务的核心组件。根据业务主体、安全保护等级的不同，可以进行进一步细分。例如：可以根据保护等级的不同，细分为四级保护子区、三级保护子区、二级保护子区。另外，为了保证不同生产子区之间的通信，可以单独划分一个负责交换的数据交换子区；
- **非生产区**：非生产区主要为系统开发、测试、试运行等提供的逻辑区域。根据实际情况，一般可分为系统开发子区、系统测试子区、系统试运行子区；
- **支撑服务区**：该区域主要为云平台及其组件提供共性的支撑服务，通常按照所提供的功能的不同，可以细分为：
  - 通用服务子区：一般包括数字证书服务、认证服务、目录服务等；
  - 运营服务子区：一般包括用户管理、业务服务管理、服务编排等；
- **管理区**：主要提供云平台的运维管理、安全管理服务，一般可分为：
  - 运维管理子区：一般包括运维监控平台、网管平台、网络控制器等；
  - 安全管理子区：一般包括安全审计、安全防病毒、补丁管理服务器、安全检测管理服务器等。
- **资源区**：主要包括各种虚拟化资源，涉及主机、网络、数据、平台和应用等各种虚拟化资源。按照各种资源安全策略的不同，可以进一步细分为生产资源、非生产资源、管理资源。不同的资源区对应不同的上层区域，如生产区、非生产区、管理区等；
- DMZ **区**：主要包括提供给 Internet 用户、外部用户访问代理服务器、Web 服务器组成。一般情况下 Internet、Intranet 用户必须通过 DMZ 区服务器才能访问内部主机或服务；
- **堡垒区**：主要提供内部运维管理人员、云平台租户的远程安全接入以及对其授权、访问控制和审计服务，一般包括 VPN 服务器、堡垒机等；
- **运维终端接入区**：负责云平台的运行维护终端接入

针对具体的云平台，在完成安全域划分之后，就需要基于安全域划分结果，设计和部署相应的安全机制、措施，以进行有效防护。

云平台不同于一般的 IT 系统，会涉及多个网络，下面对此进行简要说明，再讨论云平台的安全防护。

网络隔离

为了保障云平台及其承载的业务安全，需要根据网络所承载的数据种类及功能，进行单独组网。

- **管理网络**　物理设备是承载虚拟机的基础资源，其管理必须得到严格控制，所以应采用独立的带外管理网络来保障物理设备管理的安全性。同时各种虚拟资源的准备、分配、安全管理等也需要独立的网络，以避免与正常业务数据通信的相互影响，因此设立独立的管理网络来承载物理、虚拟资源的管理流量；
- **存储网络**　对于数据存储，往往采用 SAN、NAS 等区域数据网络来进行数据的传输，因此也将存储网络独立出来，并于其他网络进行隔离；
- **迁移网络**　虚拟机可以在不同的云计算节点或主机间进行迁移，为了保障迁移的可靠性，需要将迁移网络独立出来；
- **控制网络**　随着 SDN 技术的出现，数据平面和数据平面数据出现了分离。控制平面非常重要，关于真个云平台网络服务的提供，因此建议组建独立的控制网络，保障网络服务的可用性、可靠性和安全性

上面适用于一般情况。针对具体的应用场景，也可以根据需要划分其他独立的网络，

安全防护设计

云计算系统具有传统 IT 系统的一些特点，从上面的安全域划分结果可以看到，其在外部接口层、核心交换层的安全域划分是基本相同的，针对这些传统的安全区域仍旧可以采用传统的安全措施和方法进行安全防护。如下图所示：

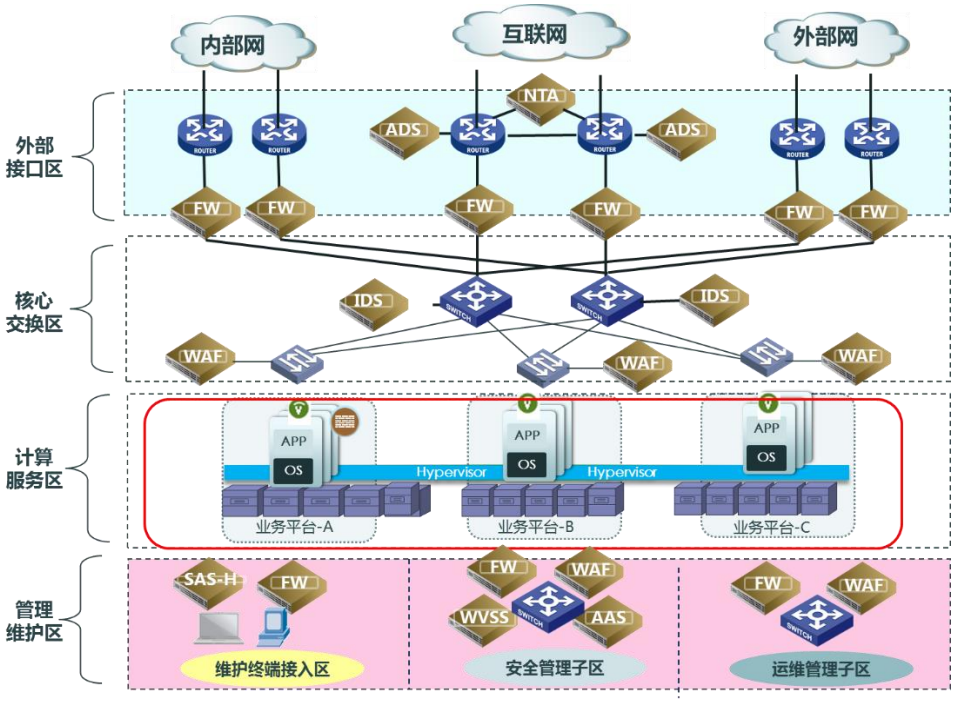

图 四.8 传统安全措施的部署

当然，从上面的安全域划分结果可以看到，相对于传统的网络与信息系统来讲，云平台由于采用了虚拟化技术，在计算服务层、资源层的安全域划分与传统 IT 系统有所不同，这主要体现在虚拟化部分，即生产区、非生产区、管理区、支撑服务区、堡垒区、DMZ 区等。下面在对这些采用了虚拟化技术的区域进行重点设计。当然，对于不同的区域，应按照根据 4.3 节安全保障技术框架的要求，选择、落实适用的安全控制措施，下面重点说明。

生产区

生产区部署了虚拟化主机、软件平台、应用层，应基于虚拟化技术实现，因此其安全防护应考虑虚拟化安全、网络安全、主机安全、应用安全、数据安全等内容。

虚拟化安全

虚拟化安全主要涉及虚拟化组件及其管理的安全，包括了虚拟化操作系统、虚拟化交换机、虚拟主机、虚拟存储及虚拟化安全管理系统的安全。

对于虚拟化安全主要采用的是安全配置和加固、虚拟化映像防护等。详细内容参见第七章介绍。

网络安全

网络安全主要涉及防火墙、异常流量检测和清洗、网络入侵检测、恶意代码防护、VPN 接入、安全审计等内容。

防火墙及边界防护

安全域需要隔离，并需要采取访问控制措施对安全域内外的通信进行有效管控。通常可采用的措施有 VLAN、网络设备 ACL、防火墙、IPS 设备等，这里主要对防火墙的功能、部署进行说明

功能

访问控制系统的安全目标是将云计算中心与不可信任域进行有效地隔离与访问授权。访问控制系统由防火墙系统组成，防火墙在网络入口点或者安全域的边界，根据设定的安全规则，检查经过的通信流量，在保护内部网络安全的前提下，对两个或多个网络之间传输的数据包和联接方式按照一定的安全策略进行检查，来决定网络之间的通信是否被允许。

产品形态

对于云计算环境的边界隔离，主要采用传统防火墙、虚拟化防火墙。

部署

对于云平台，防火墙需要实现对传统网络环境中的安全域的隔离，也需要实现对虚拟化环境中的安全域（如生产域及其子区、生产域及其子区、支撑服务域及其子区、管理域及其子区、DMZ 域及其子区等）的隔离。对于传统网络环境中的安全域可采用传统防火墙、传统的部署方式即可，而对于虚拟化环境中的安全域可采用虚拟化防火墙实现。

以 VMWare ESXi 虚拟化平台为例，虚拟化防护墙的部署方式如下图所示：

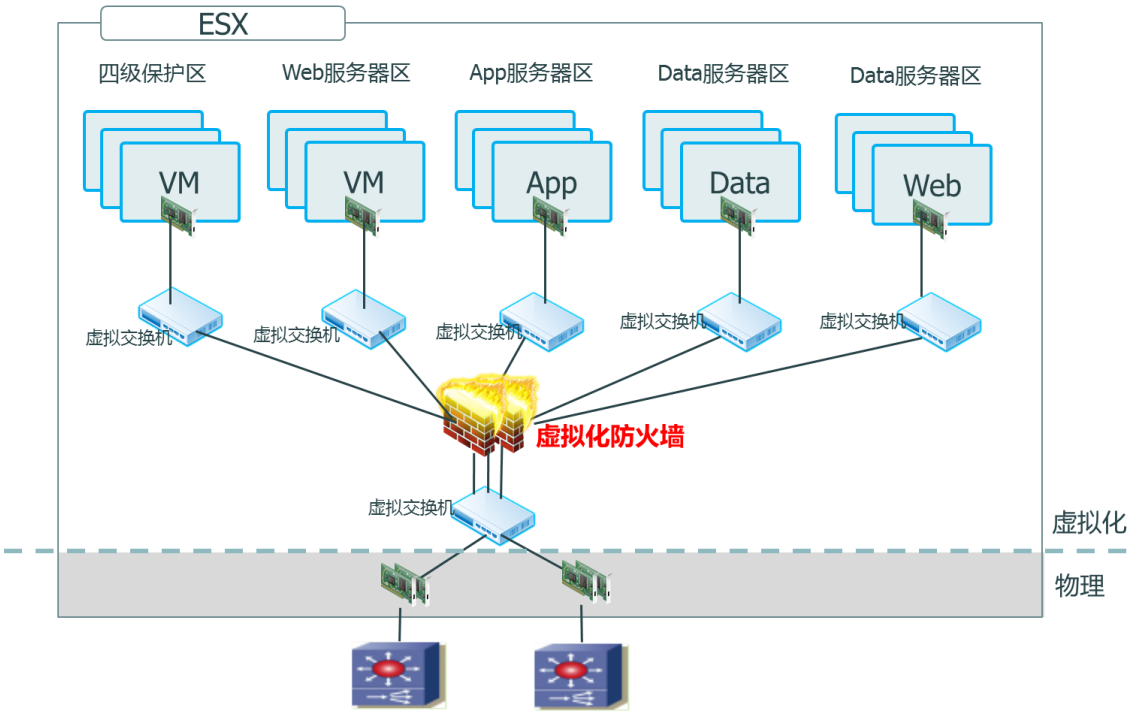

图 四.9 虚拟化防火墙部署

网络异常流量监测与分析

云计算中心部署的应用和业务非常丰富，如基于流媒体的音视频服务， VPN 业务等等，必然会受到各种网络攻击，如 DDOS，进而出现大量异常流量。在这种流量成分日益复杂，异常流量海量涌现的情况下，对网络流量进行实时监测和分析，从而全面了解流量的各种分布以及变化趋势就显得十分必要了。

功能

网络流量分析系统在云计算中心运营维护中的作用体现在两个方面：异常流量监测分析和流量统计分析。由于互联网上存在大量的异常流量，尤其是大流量的抗拒绝服务（DDoS）攻击经常造成链路拥塞，以至于网络无法正常提供服务甚至造成整个网络环境完全瘫痪。因此异常流量监测分析是网络流量分析系统的首要任务，下面详细阐述流量统计分析和异常流量检测分析的功能。

- 流量统计分析　　流量统计分析的任务是实时监控进出云计算中心流量的地域分布，应用组成分布、变化趋势，并生成相应的统计报表。统计对象的粒度可以为 IP 地址、IP 地址段、用户（用 IP 地址或地址段的组合来定义）。流量的地域分布显示对某个主机（或地址段、用户）的访问流量来自哪些地域。流量统计结果对流量工程具有很重要的参考价值。应用组成分布显示云计算中心内部各种业务的开展情况，结合地域分布的信息，也可以指导流量工程。流量的变化趋势显示流量随时间的变化规律以及峰值时段对带宽的占用情况，这些数据有助于进行云计算中心容量规划。
- 异常流量监测分析
  - 双向异常流量监测　　异常网络流量分析系统应对网络中的由内至外、由外至内的流量进行双向监测，即可监测外发异常流量，也可监测外来异常流量；
  - 异常流量定位　　异常网络流量分析系统应对网络中的流量进行持续监控和实时分析，并对异常流量进行及时的发现、告警和定位，使网管人员能够准确的发现异常流量进入网络的端口和攻击目标；
  - 异常流量分析　　异常网络流量分析系统对异常流量进行详细的分析，对异常流量的行为进行记录和分析，使网管人员能够准确的了解异常流量的行为特征；
  - 异常流量防范　　异常网络流量分析系统能够针对网络中的异常流量提供防范方法和建议，使网管人员能够快速应对网络中的异常流量，将异常流量对网络和用户的影响减少到最低；
  - 异常流量记录　　异常网络流量分析系统应对网络中发生的异常流量进行记录，网管人员可以查询系统的历史记录，分析网络异常流量的类型、特点和趋势，总结长期预防异常流量的手段和方法；
  - 异常流量过滤　　异常网络流量分析系统能够根据异常流量的特点、方向，通知其他安全设备对异常流量进行过滤、清洗或压制。或者通知运维人员进行手动处理，以防止或减少云计算中心受异常流量的影响

目前业界的通常解决方案是异常流量检测分析系统与抗拒绝服务攻击系统联动部署实现异常流量分析和过滤，异常流量检测分析系统将异常告警信息实时通告给抗拒绝服务攻击系统，由抗拒绝服务攻击系统实施异常流量过滤净化，将净化后的流量回注。抗拒绝服务攻击系统的在后面的章节详细阐述。

产品技术选型

目前网络流量分析产品主要有两大类型：

- 类型一：基于流（FLOW）信息的流量分析产品，流（FLOW）信息由网络中的路由器和交换机产生，流量分析设备根据流（FLOW）信息进行流量分析；
- 类型二：基于应用层分析的深度包检测产品（DPI），采用端口镜向或分光方式将需要分析的数据流转发给流量分析设备

基于流（FLOW）信息的流量分析产品具有如下特性，1）采用旁路方式进行部署，不会影响业务；2）能够支持大流量大范围网络的分析需求，由于流（FLOW）数据是对网络实际转发数据流的聚合与抽象，相对于 DPI 设备投资较少；3）对于大流量监测来讲，其检测准确率可以达到 99.99%。

对于云平台，其数据流量较大，且内置的虚拟交换机可以直接输出 Netflow 数据流，因此建议在云计算中心采用基于流（FLOW）信息的流量分析产品。

系统组成和形态

基于 Netflow 技术安全检测与分析系统主要包括异常流量检测系统和综合分析平台。

对于异常网络流量监测系统，其产品形态目前主要有传统物理设备形态，以及虚拟化产品形态。考虑的设备的性能以及与流量清洗设备联动的要求，可同时采用两种形态。

部署建议

综合分析云计算中心的实际情况，其异常流量主要来自互联网、第三方网络、企业广域网，还包括虚拟机之间互相攻击的异常流量。因此需要在云平台的互联网出口、外联网出口、广域网出口，以及生产区域边界、DMZ 区域边界上部署异常流量监测系统（旁路部署 Netflow 流量采样检测模块），实现流量统计分析、路由分析、异常流量检测。它既可以作为流量监控分析产品对网络流量进行深入分析，从而全面了解各类流量的分布以及变化趋势；也可分析诸如 DDoS 攻击、网络滥用误用、P2P 流量等异常流量。

异常流量检测系统基于 Netflow 数据，其采集点是主要物理/虚拟交换机上，可根据需要灵活部署。以 VMWare ESXi 虚拟化平台为例，一般部署情况如下图所示：

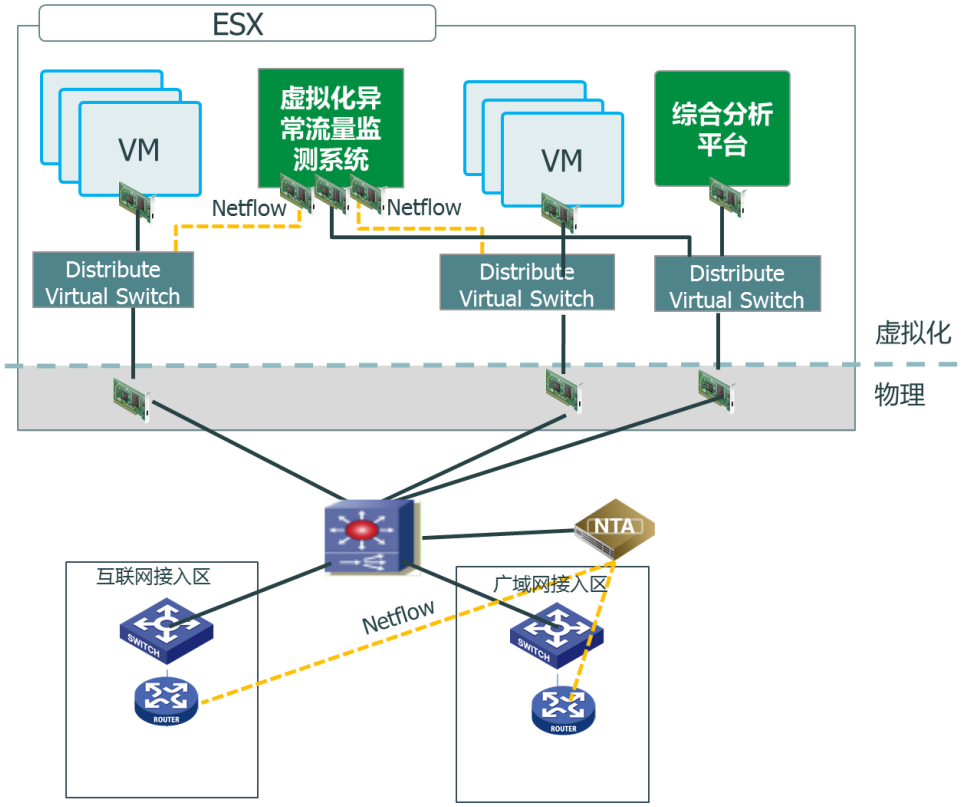

图 四.10 异常流量监测系统部署

网络入侵检测

云计算对外提供服务，完全面向互联网，所面临的威胁被无限放大，在云计算中心网络出口采用入侵检测机制，收集各种信息，由内置的专家系统进行分析，发现其中潜在的攻击行为。由网络入侵检测系统捕获分析网络中的所有报文，发现其中的攻击企图，根据事先制定的策略通知管理员或自行采取保护措施。

功能

入侵检测作为一种积极主动地安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵。从网络安全立体纵深、多层次防御的角度出发，入侵检测理应受到更高的重视。

入侵检测系统可实时监控云计算中心网络中的数据访问和系统事件，及时发现攻击行为并作为分析证据并对可疑的访问行为进行自动响应。

利用入侵检测系统的攻击结果判定功能重点关注攻击成功的安全事件。针对某些特定的安全规则单独设定安全策略，针对云计算中心业务特点过滤一些低风险或者不可能成功的攻击行为，从而减少管理员关注日志告警的工作量，也使得重要攻击行为能够得到重点体现。

同时，可以针对业务特点自定义某些特定的安全规则。如敏感内容信息过滤，设置自定义的关键字过滤检测规则，通过与防火墙的联动或自身发送的 TCP Killer 数据包，将涉及敏感信息的 TCP 会话阻断，防止信息泄露或者一些非法的网络信息传递。

产品组成和形态

网络入侵检测系统一般包括网络入侵检测设备和综合分析平台。网络入侵检测设备主要有传统硬件网络入侵检测设备（NIDS）和虚拟化网络入侵检测设备（vNIDS）两种产品形态。

部署建议

入侵检测系统应部署在已被入侵的高危区域或者关键区域。包括互联网接入区、外联网接入区，以及关键的计算服务域。

对于互联网接入区、外联网接入区，可采用传统的 IDS，而对于位于虚拟化平台上的关键计算服务域可以用虚拟化入侵检测系统，并可部署一套综合分析系统，对系统所有入侵检测日志进行统一存储、分析和呈现。以 VMWare ESXi 虚拟化平台为例，一般部署情况如下图所示：

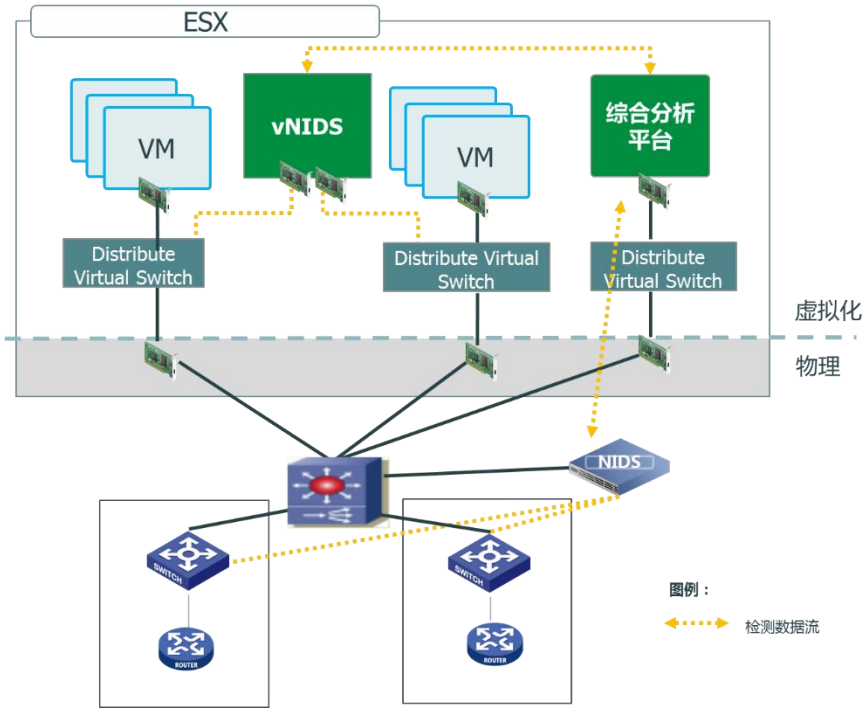

图 四.11 网络入侵检测系统部署图

主机安全

主机安全与传统安全相同，这里不再赘述。

Web 应用防护

云计算中心一般都是采用 Web 的方式来对外提供各类服务，特别是在 Web 2.0 的技术趋势下，75%以上的攻击都瞄准了网站（Web）。这些攻击可能导致云计算服务提供商遭受声誉和经济损失，可能造成恶劣的社会影响。Web 应用防护技术通过深入分析和解析 HTTP 的有效性、提供安全模型只允许已知流量通过、应用层规则、基于会话的保护，可检测应用程序异常情况和敏感数据（如信用卡、网银帐号等）是否正在被窃取，并阻断攻击或隐蔽敏感数据，保护云计算平台的 Web 服务器，确保云计算平台 Web 应用和服务免受侵害。

Web **防护技术**

与传统防火墙/IPS 系统相比较，Web 应用防护技术将提供一种安全运维控制手段，基于对 HTTP/HTTPS 流量的双向分析，为 WEB 应用提供实时的防护。

- 对 HTTP 有本质的理解：能完整地解析 HTTP，包括报文头部、参数及载荷。支持各种 HTTP 编码（如 chunked encoding）；提供严格的 HTTP 协议验证；提供 HTML 限制；支持各类字符集编码；具备 response 过滤能力；
- 提供应用层规则：WEB 应用通常是定制化的，传统的针对已知漏洞的规则往往不够有效。WAF 提供专用的应用层规则，且具备检测变形攻击的能力，如检测 SSL 加密流量中混杂的攻击；
- 提供正向安全模型（白名单模型）：仅允许已知有效的输入通过，为 WEB 应用提供了一个外部的输入验证机制，安全性更为可靠；
- 提供会话防护机制：HTTP 协议最大的弊端在于缺乏一个可靠的会话管理机制。WAF 为此进行有效补充，防护基于会话的攻击类型，如 cookie 篡改及会话劫持攻击

Web 应用防护技术将以一个可闭环又可循环的方式去降低潜在的威胁，对于事中疏漏的攻击，可用事前的预发现和事后的弥补，形成环环相扣的动态安全防护。事前是用扫描方式主动检查网站并把结果形成新的防护规则增加到事中的防护策略中，而事后的防篡改可以保证即使疏漏也让攻击的步伐止于此，不能进一步修改和损坏网站文件，对于要求信誉高和完整性的用户来说，这是尤为重要的环节。

产品形态

对于网络应用防火墙，其产品形态目前主要有传统物理设备形态，以及虚拟化产品形态。在虚拟化的环境中，应选择虚拟化产品形态，并可以实现和网站安全检测系统、Web 安全扫描系统进行联动。

产品部署

Web 应用防火墙应部署在 Web 服务器之前，并逻辑串联。根据需要可选择透明模式、路由模式或者反向代理模式。

以 VMWare ESXi 虚拟化平台为例，其部署方式如下图所示：

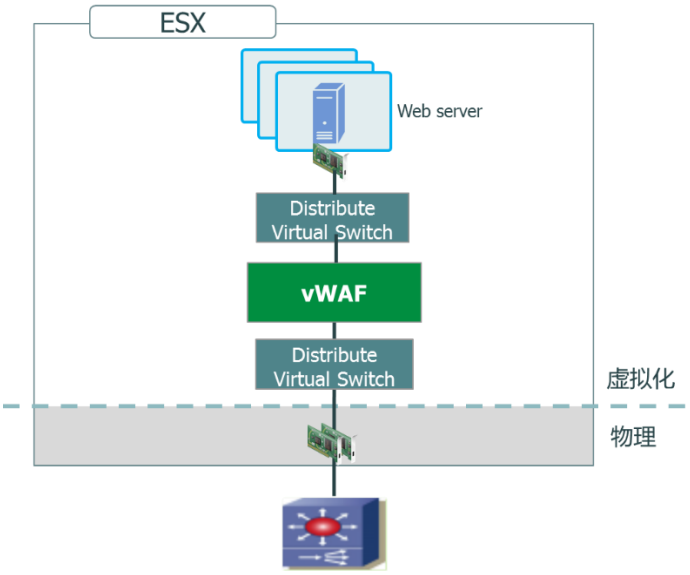

图 四.12 虚拟化 Web 应用防火墙部署

网页防篡改

网页防篡改系统可以仍旧部署在 Web 服务上，实现防篡改功能，其功能、技术实现与部署与传统方式相同，这里不再赘述。

网站安全监测技术

见安全管理区的描述。

数据安全

对于数据安全，需要涉及数据的产生、传输、存储、使用、迁移、销毁以及备份和恢复的全生命周期，并在数据的不同生周期阶段采用数据分类分级、标识、加密、审计、擦除等手段。另外，在采用了这些基础防护技术措施之外，还应考虑数据库审计、数据防泄露以及数据库防火墙的手段，最大限度地保证云平台中的数据安全。

非生产区

对于非生产区部署的主机、应用一般与生产区基本相同，因此，对于非生产区的安全防护可以借鉴生产区的防护方法，这里不再赘述。

DMZ 区

DMZ 区主要部署了生产区核心应用的一些代理主机、web 主机等，其直接面向来自互联网的网络访问，受到的威胁程度高，应进行重点防护。

对于 DMZ 区的安全防护可以借鉴生产区的防护方法，这里不再赘述。需要说明是的：为了保证系统安全防护的可靠性，其安全防护措施，如防火墙，应与网络接入区、生产区等防护措施形成多层异构模式。

堡垒区

VPN 接入

VPN 接入可以采用传统 VPN 接入设备，也可以采用虚拟化的 VPN 接入设备。其实现方式与传统方式基本相同，这里不再赘述。

堡垒机

云平台的管理运维人员、第三方运维人员以及租户需要多云计算平台的主机、应用及网络设备进行管理、维护操作。为了发现和防止不当操作、越权操作的发生，需要对此类用户进行认证、授权、访问控制和审计。堡垒机就是完成上述功能的关键设备，典型应用场景如下图所示：

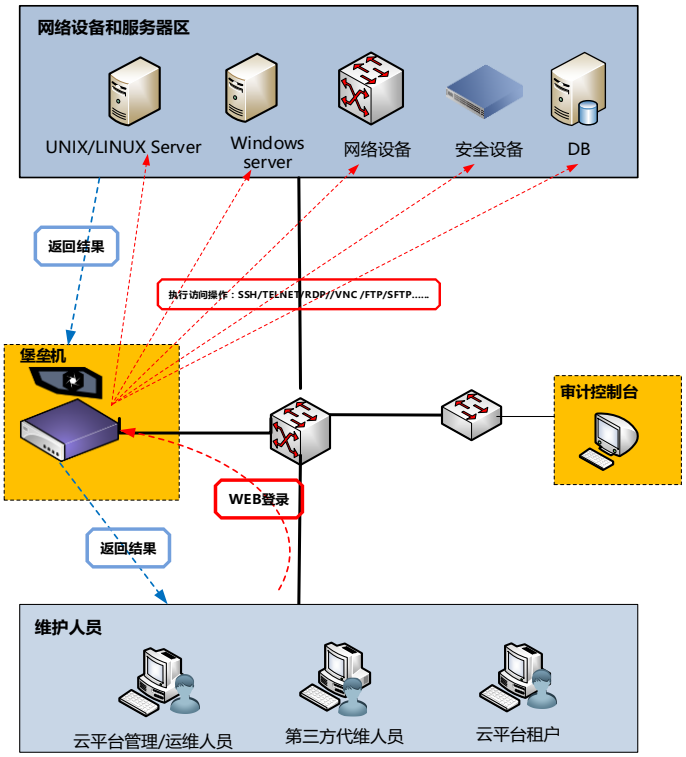

图 四.13 堡垒机应用场景

功能

堡垒机可以提供一套先进的运维安全管控与审计解决方案，目标是帮助云计算中心运维人员转变传统 IT 安全运维被动响应的模式，建立面向用户的集中、主动的运维安全管控模式，降低人为安全风险，满足合规要求，保障企业效益，主要实现功能如下：

- 集中账号管理　　建立基于唯一身份标识的全局实名制管理，支持统一账号管理策略，实现与各服务器、网络设备等无缝连接；
- 集中访问控制　　通过集中访问控制和细粒度的命令级授权策略，基于最小权限原则，实现集中有序的运维操作管理，让正确的人做正确的事；
- 集中安全审计　　基于唯一身份标识，通过对用户从登录到退出的全程操作行为进行审计，监控用户对目标设备的所有敏感操作，聚焦关键事件，实现对安全事件地及时发现预警，及准确可查

产品形态

对于堡垒机，其产品形态目前主要有传统物理设备形态，以及虚拟化产品形态。根据需要可以选择相应的产品形态。

部署

云计算平台的管理用户类型主要包括：云平台运维管理人员、第三方管理人员以及云平台租户。从网络访问途经讲，有内部网络访问和来自互联网的访问。堡垒机部署在管理终端和被管理设备之间，并实现逻辑上的串联部署，同时，堡垒机应部署在管理平面，实现和用户数据的隔离。

以 VMWare ESXi 虚拟化平台为例，一般部署情况如下图所示：

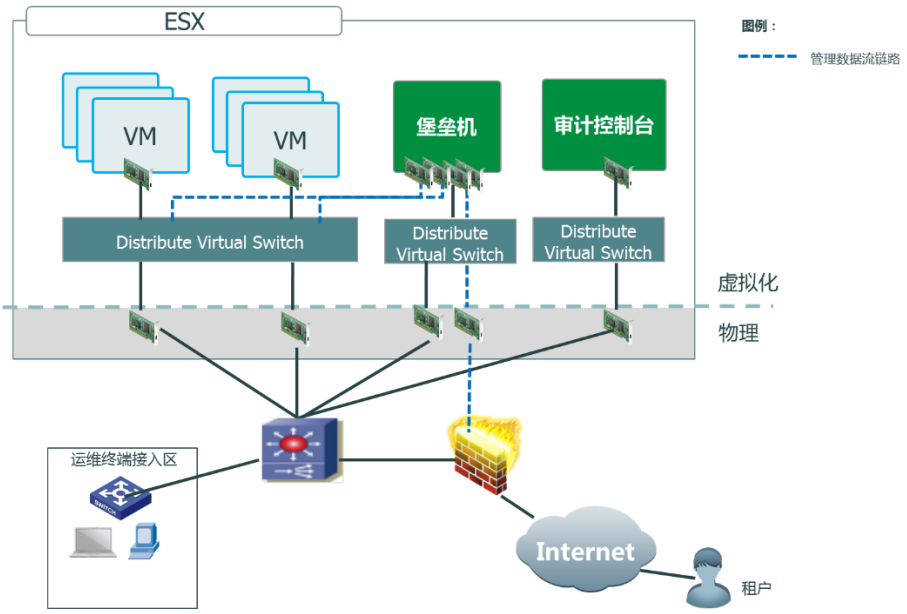

图 四.14 堡垒机部署图

支撑服务区

支撑服务区的安全防护与传统 IT 系统的支撑服务区相同，主要部署防火墙、入侵检测等防护、数据库审计、信息防泄露等防护措施，这里不再赘述。

管理区

管理区可以细分为运维管理子区、安全管理子区。运维管理子区主要部署虚拟化管理平台、云运维管理平台、网络管理平台等，其防护与传统的 IT 系统基本相同，不再赘述。

对于安全管理子区，一般会集中化部署安全防护措施的管理服务器、提供通用安全服务的服务平台，如综合安全管理服务器、防病毒服务器、安全检查/评估系统、安全态势监测系统等，实现“大院式”防护，降低防护成本。

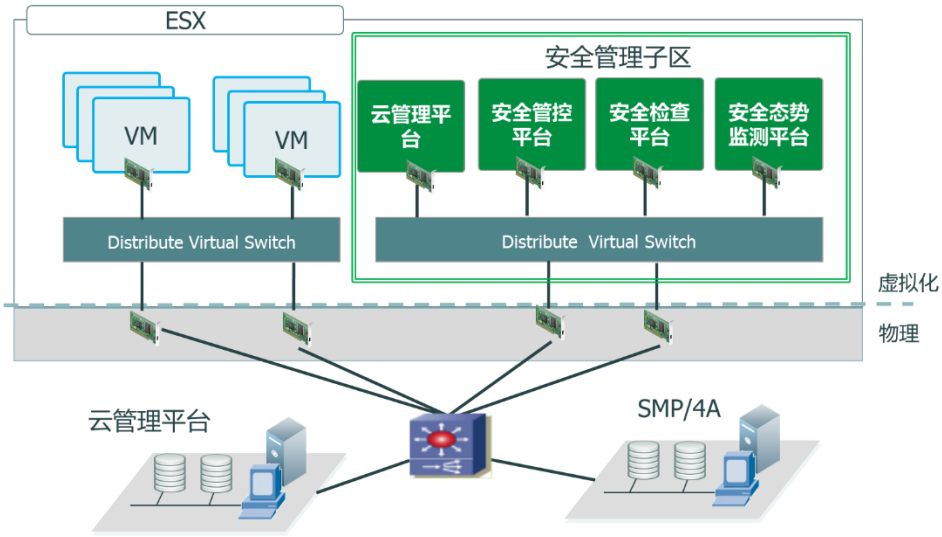

图 四.15 安全管理子区

对于云平台来讲，这里采用的安全防护措施可与虚拟化管理平台、云管理平台有机集成，如实现虚拟机配置/活动信息的获取、租户信息的获取、虚拟机所部署应用的信息的获取等，以实现全程自动化实现。

安全检查/评估系统

所有的 IT 组件都会有安全漏洞或者配置弱点，需要部署安全检查/评估系统对系统进行持续安全检查、扫描，并自动化分析系统存在的问题，给出应对策略。

功能

安全扫描技术主要是用来评估计算机网络系统的安全性能，是网络安全防御中的一项重要技术，其原理是采用模拟攻击的形式对目标可能存在的已知安全漏洞/配置弱点进行逐项检查。安全扫描系统可对云平台主机/设备/应用进行定期扫描、评估，分析客户业务系统当前的设置和防御，指出潜在的安全漏洞，以改进系统对入侵的防御能力。扫描的目标包括工作站、服务器、路由器、交换机、数据库应用等各种对象，根据扫描结果向系统管理员提供安全性分析报告，为提高网络安全整体水平产生重要依据。

产品形态

对于安全评估系统，其产品形态目前主要有传统物理设备形态，以及虚拟化产品形态。根据需要可以选择相应的产品形态。

部署建议

在共享式工作模式下，只要将安全评估系统接入云平台安全管理子区网络并进行正确的配置即可正常使用，其工作范围可以覆盖到云平台网络地址可达之处。运维人员可以从任意地址登录安全评估系统并下达扫描任务。

网站安全监测技术

云计算平台所部署了大量网站，需要对这些网站进行持续、动态侦测，提早发现问题和漏洞，增强客户访问体验。

技术原理与功能

传统的网站安全监管方式通常是采用 Web 应用安全扫描工具周期性的对网站进行安全扫描与评估，然后根据评估结果进行安全加固和风险管理。这种安全检查工作是一种静态的检查工作，能够反映站点被检查那一时期站点的安全问题，但是缺少风险的持续监测性。

网站安全监测技术根据网站系统监管要求，通过对目标站点进行页面爬取和分析，为用户提供透明模式的远程集中化安全监测、风险检查和安全事件的实时告警，并为用户提供全局视图的风险度量报告，非常适用于为租户提供安全增值服务。

网站安全监测技术具体包括 Web 爬虫与链接智能分析、Web 页面预处理与分级检测、网页木马检测与分析，实现网站漏洞扫描、网页挂马监测、网页敏感内容监测、网页篡改监测、网站平稳度监测、网站域名解析监测等功能，能够从站点的脆弱性、完整性、可用性三方面全方位的对站点的安全能力要求进行监管，并且可为一个大型的站点群同时提供安全监测的能力。

产品形态

对于网站安全检测，其产品形态目前主要有传统物理设备形态，以及虚拟化产品形态。根据需要可以选择相应的产品形态。

部署

网站安全监测系统可根据云计算平台网站的规模进行独立部署和分布式部署。独立部署方式就是在网络中部署一台同时具备监测及数据分析能力的设备，即一台设备实现所需要的监测能力。系统具有管理网口和扫描网口，管理口可接入用户内容，用于用户对监测任务的管理。扫描口接入外网，对重要网站进行监测。分布式部署方式，即采用单台控制中心，多台引擎的

分布式部署方式。控制中心和引擎之间的通信采用管理口，引擎与被监测网站可采用扫描口连接。分布式部署方式，即满足了对大量网站高频率的监控，也可对各网站的监测数据进行汇总分析，方便用户对所有网站进行集中管理。

对于云计算平台，建议采用分布式部署方式，并采用软件形态，这样可以资源的弹性。

五 云计算安全防护方案的演进

目前，云计算技术在快速发展、完善中。在虚拟化技术之后，尤其是 SDN、NFV 技术的采用，为存储、网络资源的自动化部署和分权分域管理提供了技术手段。另外，大数据技术的出现和应用，也会存储资源的敏捷性应用提供支撑手段。

同时，云计算的安全防护体系技术体系和实现方法也跟随着云计算的技术演进步伐，不断演进和完善。这主要体现在安全防护措施的部署、安全防护技术体系架构、安全运营等方面。

虚拟化环境中的安全防护措施部署

在云计算环境中，为了适应虚拟化环境，以及对对虚拟机之间的流量、跨安全域边界得流量进行监测和访问控制的需要，安全设备在保持架构和功能的基础上，在产品形态和部署方式发生了一定的变化。

在产品形态方面，主要体现是由硬件变化了软件。在部署方式方面，主要通过合理设计虚拟化网络逻辑结构，将虚拟化安全设备部署在合理的逻辑位置，同时保证随着虚拟主机的动态迁移，能够做到安全防护措施和策略的跟随。

从实现逻辑上讲，可以将控制措施分为：

- 检测类：捕获相应的数据流量，但不再进行转发。如 vNIDS、网络流量检测等；
- 控制类：拦截网络流量，并进行安全处理后进行转发。如防火墙、Web 应用防火墙等

对于这两类设备的部署方式，已经在前面进行了描述，这里不再赘述。应当说明的是，这种部署方式由于需要一定的配置工作，并不能实现安全措施（也可以抽象为安全资源）的自动化部署、分权分域管理。随着，SDN、NFV 技术的采用，基于 SDN 技术的安全技术体系架构实现了这些需求。

软件定义安全体系架构[①]

体系架构

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，下图是 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]软件安全体系架构的详细说明参见《2015 绿盟科技软件定义安全 SDS 白皮书》

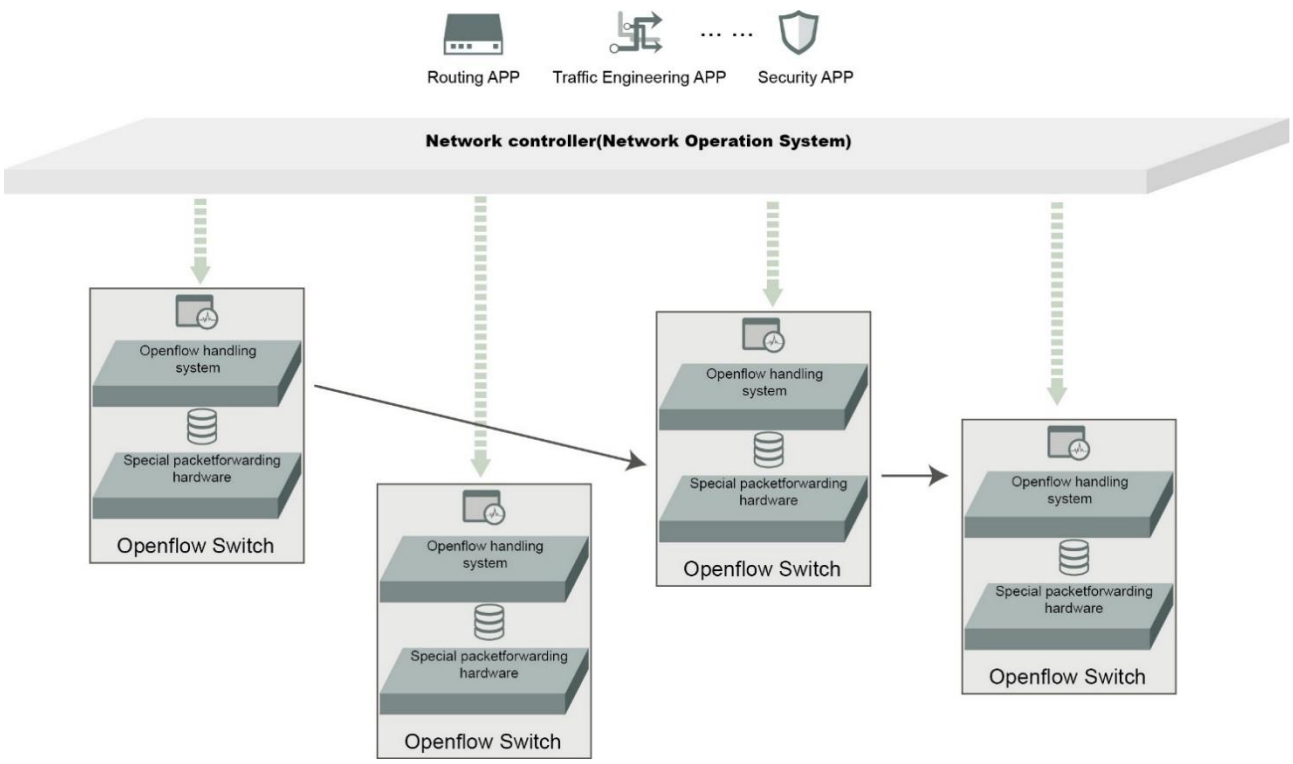

图 五.16 SDN 典型架构

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 0 所示，可分为三个部分：实现安全功能的设备资源池，用户环境中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。

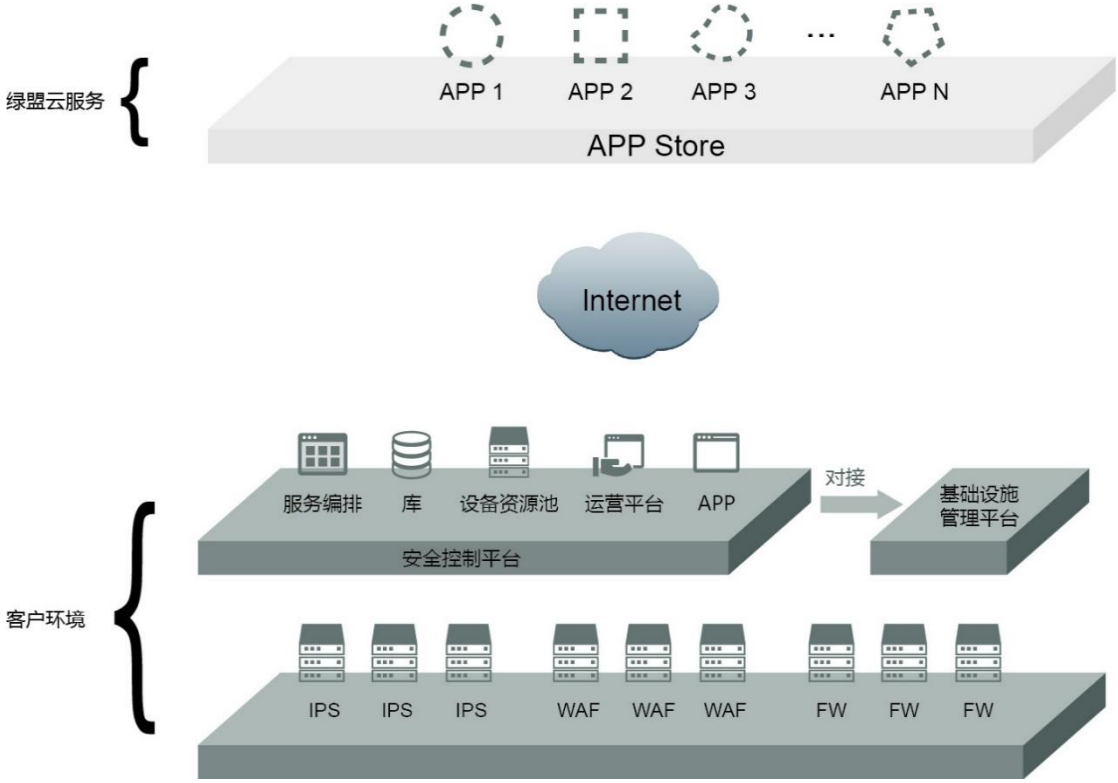

图 五.17 软件定义安全防护体系架构

说明：

- **安全资源池**：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；
- **安全控制平台：**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、与云计算基础设施的对接，以及相应安全 APP 的策略解析和执行。并通过与 SDN 控制器的对接，实现网络逻辑拓扑的改变、数据流的调度；
- **安全应用：**安全应用是使用底层安全资源池完成特定安全功能的组件，租户可以从应用商店选择、下载，并自动化部署、设置和管理；
- **应用商店：**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

技术实现原理

在 SDN 架构中，网络控制器可实现流量特征收集、底层网络拓扑学习、路由路径计算和流指令下发等功能，而指令的生成、决策都是由上层 APP 实现的。安全控制平台作为的一个具体应用，可以负责信息安全防护的决策、判断及流调度策略，进而实现对网络流量的自有调度，使虚拟化环境中的流量经过特定安全防护设备，实现安全检测、过滤等功能。

使用安全控制平台的安全设备部署如下图所示。

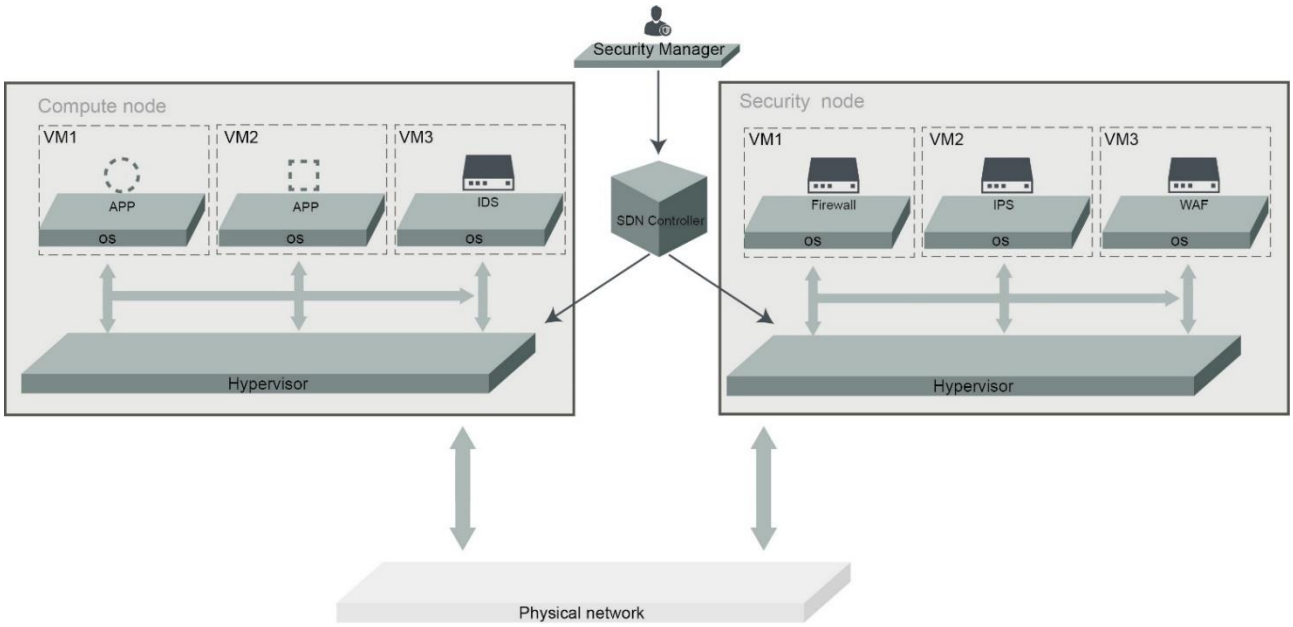

图 五.18 使用 SDN 技术的安全设备部署图

云平台内的计算节点和安全节点内 Hypervisor 的虚拟交换机连接到 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。

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。

下图展示了在开源虚拟化系统 Openstack+开源 SDN 控制器环境下部署 IPS 的情况。

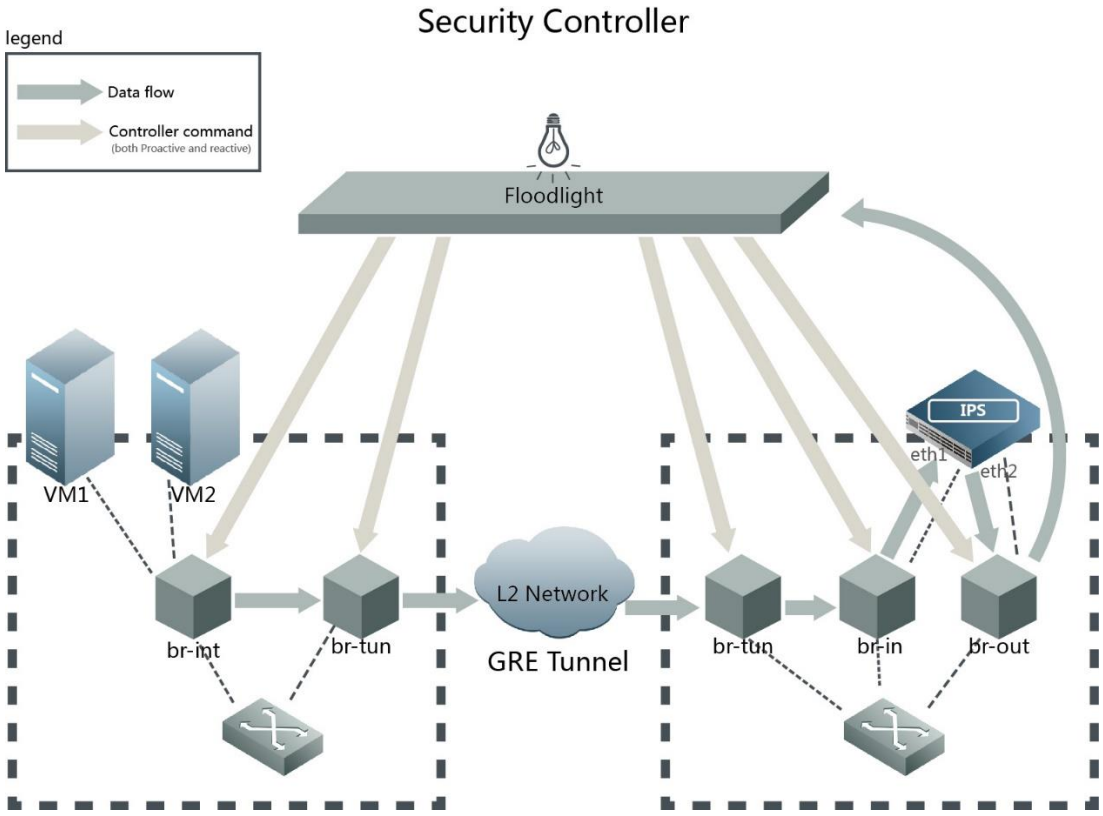

图 五.19 使用 SDN 技术实现流量牵引的原理图

当需要多种类型的安全防护时，可是使数据流就会依次经过多个安全设备，进而达成多种防护的目的。

方案演进

绿盟科技的云计算安全解决方案可以实现无缝演进。在原生虚拟化环境中部署的安全设备可以通过软件升级，实现和 SDN 网络控制器的接口、安全控制平台的接口，并进一步抽象化、池化，实现安全设备的自动化部署。同时，在部署时通过安全管理策略的更变租户可以获得相应安全设备的安全管理权限、达成分权分域管理的目标。

在安全控制平台部署期的过渡阶段，可以采用手工配置流控策略的模式，实现无缝过渡。在这种部署模式下，安全设备的部署情况与基于 SDN 技术的集成部署模式相似，只是所有在使用 SDN 控制器调度流量处，都需要使用人工的方式配置网络设备，使之执行相应的路由或交换指令。

的 IPS 防护为例，可以由管理员手动配置计算节点到安全节点中各个虚拟网桥的流表，依次将流量牵引到 IPS 设备即可。如下图所示：

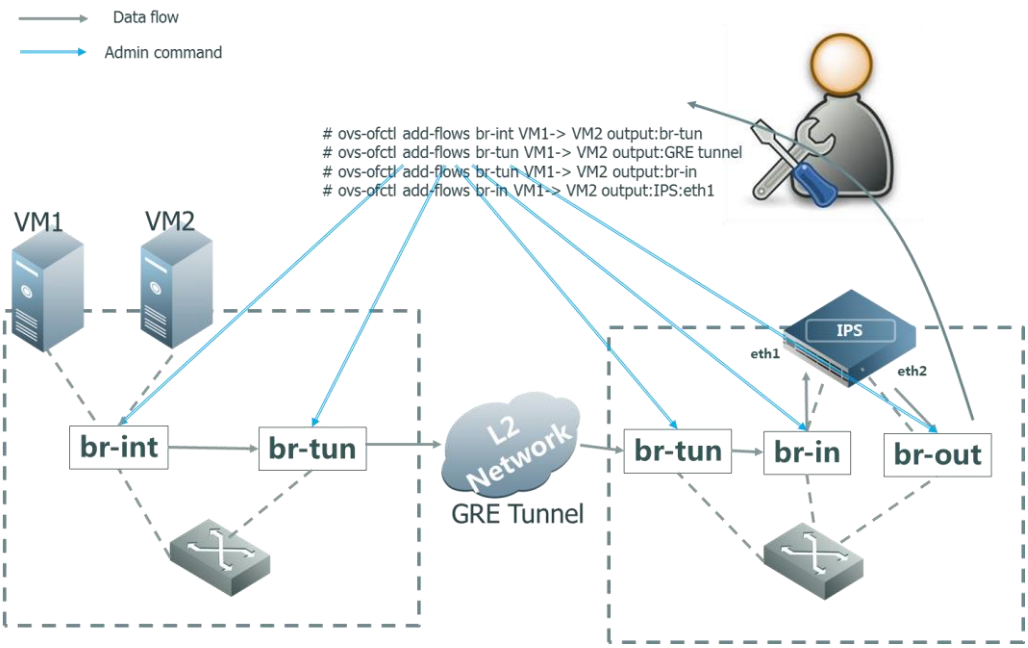

图 五.20 基于手工配置的 IPS 防护模式

安全运营

对于安全防护，关键是在系统运行期间，对系统的持续安全检测、防护，并对突发事件进行处理，这需要安全运维人员具有较高的安全知识和技能。对于云计算中心的租户，由于其安全知识和技能不足，需要购买安全代维服务，对云平台的提供商来讲，就需要提供安全运营服务。

绿盟科技的云计算安全解决可以提供安全运营支持。通过在安全管理子区部署的集中化的安全检测/评估平台、安全管理平台等可以实现对租户提供安全运营服务。

另外，绿盟科技提供了云端的安全服务，可以为云平台服务商提供设备代维、网站检测、恶意代码分析和更新、安全威胁分析和安全情报等服务。

六 云安全技术服务

私有云安全评估和加固

风险评估服务

针对云计算中心的风险评估将在针对国内外信息安全风险评估规范和方法理解的基础上开展，遵循 ISO27005 以及 NIST SP800-30 的基础框架，并且将针对云计算的资产识别、威胁分析、脆弱性识别和风险评价融入其中，是云计算中心进行安全规划建设、法规遵从、运营安全状态分析等安全日常活动的重要依据。

此方案的设计思路是针对云计算中心的安全现状而做出的，因此在对云计算中心的安全体系设计具有一定的局限性和不确定性。为了使最终采用的安全管理、安全技术手段充分贴合云计算中心的实际安全需求，需要通过安全建设中的重要手段——风险评估来实现。通过风险评估可以更加清晰、全面的了解云计算中心系统的安全现状，发现系统的安全问题及其可能的危害，为后期安全体系建设中的安全防护技术实施提供依据。

风险评估对现有网络中的网络架构、网络协议、系统、数据库等资产安全现状进行发现和分析，确定系统在具体环境下存在的安全漏洞、隐患，以及被黑客利用后会造成的风险和影响。在此基础上对实施流程进行规划：即针对云计算中心的具体情况制定适合于自身的安全目标和安全级别，在充分考虑经济性的基础之上设计和实施相应的安全建设方案。

安全测试服务

安全测试是以绿盟科技在漏洞挖掘、分析、利用等领域的理论依据和多年实践经验为基础，对云计算平台进行深入、完备的安全服务手段。安全测试内容将包括如下内容：

- **源代码审计：**源代码审计（Code Review，后简称为代码审计）是由具备丰富的编码经验并对安全编码及应用安全具有很深刻理解的安全服务人员，根据一定的编码规范和标准，针对应用程序源代码，从结构、脆弱性以及缺陷等方面进行审查；
- **模糊测试：**模糊测试是一种通过提供非预期的输入并监视异常结果来发现软件故障的方法，是一个自动的或半自动的过程，这个过程包括反复操纵目标软件并为其提供处理数据。模糊测试方法的选择完全取决于目标应用程序、研究者的技能，以及需要测试的数据所采用的格式；
- **渗透测试：**渗透测试（Penetration Testing）是由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，找出未知系统中的脆弱点和未知脆弱点。渗透测试服务的目的在于充分挖掘和暴露系统的弱点，从而让管理人员了解其系统所面临的威胁

私有云平台安全设计咨询服务

参考标准和规范

云计算虽然是信息技术革命性的新兴领域，但是在国际和国内也有权威性的组织或者机构，针对该领域的信息安全风险控制制定并发布了指导具体实践活动的标准和规范，这些标准和规范，不仅可以为云计算服务平台的建设者和运营者提供全面有效的信息安全风险控制措施指南，也是云计算安全咨询服务提供者的主要参考和依据。

GB/T 31167/31168-2014

我国在 2014 年发布了两个云计算安全的国家标准，分别是《GB/T 31167-2014 云计算服务安全指南》和《GB/T 31168-2014 云计算服务安全能力要求》。

GB/T 31167 是针对政府行业策划、选择、实施、使用公有云服务的整个外包生命周期给出信息安全管控指南，而 GB/T 31168 面向云服务商，提出了云服务商在为政府部门提供服务时应该具备的安全能力要求。以上两个标准虽然是面向政府行业使用公有云服务而提出，但是 GB/T 31168 中提出的安全控制能力要求，对于其他行业使用公有云服务，以及建立私有云计算平台的组织来说，同样具备重要的参考意义。

GB/T 31168 给出了不同的云服务模式下，服务提供者与客户之间的安全控制职责范围划分，如下图所示：

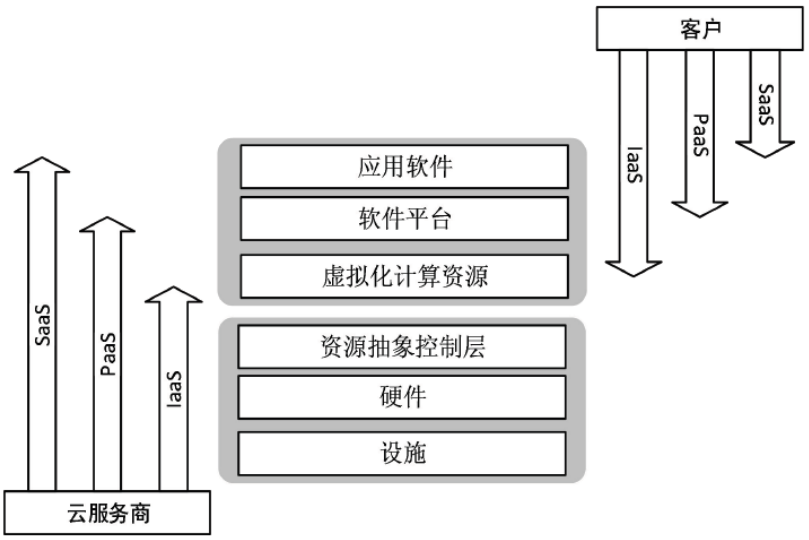

图 六.21 服务提供者与客户之间的安全控制职责范围划分

GB/T 31168 对云服务商提出了基本安全能力要求，分为 10 类，每一类安全要求包含若干项具体要求。

- **系统开发与供应链安全（17 项）**：云服务商应在开发云计算平台时对其提供充分保护，对信息系统、组件和服务的开发商提出相应要求，为云计算平台配置足够的资源，并充分考虑安全需求。云服务商应确保其下级供应商采取了必要的安全措施。云服务商还应为客户提供有关安全措施的文档和信息，配合客户完成对信息系统和业务的管理；
- **系统与通信保护（15 项）**：云服务商应在云计算平台的外部边界和内部关键边界上监视、控制和保护网络通信，并采用结构化设计、软件开发技术和软件工程方法有效保护云计算平台的安全性；
- **访问控制（26 项）**：云服务商应严格保护云计算平台的客户数据，在允许人员、进程、设备访问云计算平台之前，应对其进行身份标识及鉴别，并限制其可执行的操作和使用的功能；
- **配置管理（7 项）**：云服务商应对云计算平台进行配置管理，在系统生命周期内建立和维护云计算平台（包括硬件、软件、文档等）的基线配置和详细清单，并设置和实现云计算平台中各类产品的安全配置参数；
- **维护（9 项）**：云服务商应维护好云计算平台设施和软件系统，并对维护所使用的工具、技术、机制以及维护人员进行有效的控制，且做好相关记录；
- **应急响应与灾备（13 项）**：云服务商应为云计算平台制定应急响应计划，并定期演练，确保在紧急情况下重要信息资源的可用性。云服务商应建立事件处理计划，包括对事件的预防、检测、分析和控制及系统恢复等，对事件进行跟踪、记录并向相关人员报告。云服务商应具备容灾恢复能力，建立必要的备份与恢复设施和机制，确保客户业务可持续；
- **审计（11 项）**：云服务商应根据安全需求和客户要求，制定可审计事件清单，明确审计记录内容，实施审计并妥善保存审计记录，对审计记录进行定期分析和审查，还应防范对审计记录的非授权访问、修改和删除行为；
- **风险评估与持续监控（6 项）**：云服务商应定期或在威胁环境发生变化时，对云计算平台进行风险评估，确保云计算平台的安全风险处于可接受水平。云服务商应制定监控目标清单，对目标进行持续安全监控，并在发生异常和非授权情况时发出警报；
- **安全组织与人员（12 项）**：云服务商应确保能够接触客户信息或业务的各类人员（包括供应商人员）上岗时具备履行其安全责任的素质和能力，还应在授予相关人员访问权限之前对其进行审查并定期复查，在人员调动或离职时履行安全程序，对于违反安全规定的人员进行处罚；
- **物理与环境保护（15 项）**：云服务商应确保机房位于中国境内，机房选址、设计、供电、消防、温湿度控制等符合相关标准的要求。云服务商应对机房进行监控，严格限制各类人员与运行中的云计算平台设备进行物理接触，确需接触的，需通过云服务商的明确授权

CSA CMM&GUIDE

云安全联盟 CSA 是由多厂商组成的云计算安全权威性国际组织，该组织自成立起就致力于为云计算服务商提供信息安全风险控制方面的指南，其中主要的成果包括《云安全控制矩阵 CCM》和《云计算关键领域安全指南》白皮书。

最新升级的 CSA CCM V3.0，融合了多个行业公认的安全标准，条款，和控制框架，例如 ISO 27001/27002, 欧盟网络与信息安全局(ENISA)信息担保框架，ISACA(国际信息系统审计协会)对信息和相关技术的控制条款，支付卡行业数据安全标准，和联邦风险和授权管理程序等，为云服务商提供了覆盖 16 个领域 133 项安全控制措施要求：

图 六.22 云计算关键领域安全

其它指南与认证

除了上述国家标准和云安全联盟标准之外，还有其它的组织或机构对云计算安全风险控制体系进行了探索和实践，包括：

- 美国国防部 DOD 云计算安全需求指南
- 欧盟网络与信息安全局 ENISA 云计算安全白皮书
- 英国标准协会 BSI 云计算安全管理体系 STAR 认证
- 国内数据中心联盟可信云服务认证

咨询服务思路

绿盟科技为云服务商客户（包括各种服务交付模式和运营部署模式）提供信息安全咨询服务的整体思路如下图所示：

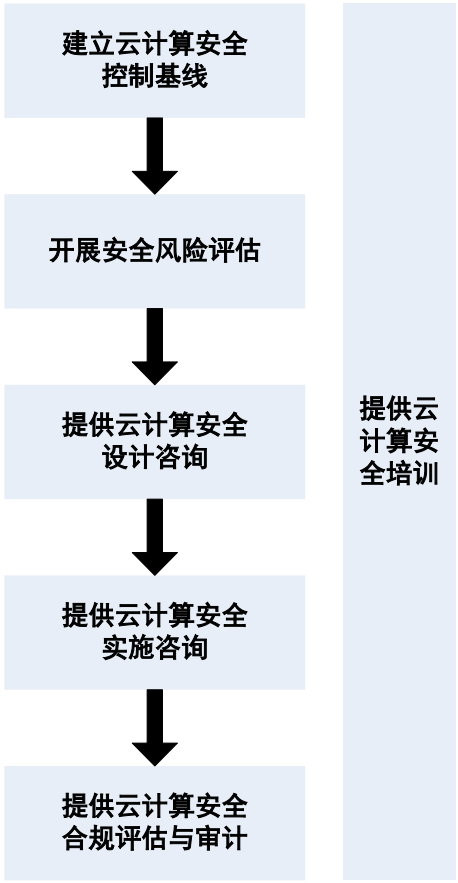

图 六.23 安全咨询服务思路

首先综合参考当前的国际/国内标准规范，建立一套具备普遍适用意义的、面向云计算平台的信息安全控制措施基线，该基线由不同领域不同类别的安全控制措施组成，涵盖安全技术与安全管理控制措施，基本全面覆盖云计算平台所面临的信息安全风险。

然后，面向云计算平台的设计、建设、运营的完整生命周期，提供安全风险评估、安全控制体系设计、安全控制体系实施建设、以及安全控制体系合规评估和咨询等多项咨询服务，协助云服务商客户建立和运营既全面有效控制信息安全风险，又能够满足合规要求的云计算服务平台。

同时，我们还向客户提供与云计算安全有关的各类培训服务，实现知识、经验、能力向客户方人员的交付和转移。

咨询服务内容

云计算安全设计咨询服务

基于风险评估的结果，以及合规性要求，可以全面识别云计算平台的信息安全控制需求，绿盟科技向云服务商客户提供云计算平台的安全控制设计咨询服务，协助客户在云计算平台的设计阶段，同步完成安全控制体系的设计任务，安全控制体系设计方案能够全面响应和落实所识别出的安全控制需求，从根本上为客户的云计算安全服务平台具备充分的安全保证能力提供保证。

云计算安全实施咨询服务

面向按照安全控制设计方案进行云计算平台的建设和部署过程，绿盟科技向客户提供以下的实施咨询服务：

- 安全策略的制订和部署
- 安全策略有效性测试

- 安全渗透性测试

云计算安全合规审计服务

云服务商客户的安全合规审计需求可能来自于外部合规要求，例如具备 BSI STAR 认证所要求的年度监督审计，也可能来自于客户自身成熟度较高的管理要求。

按照信息安全风险管理要求，云计算平台的信息安全风险管理过程应该包括持续性的风险监测、周期性的风险评估，以及可能来自于合规性目的的周期性安全专项审计。绿盟科技向云服务商客户提供信息安全合规外部审计服务，根据客户云服务平台的实际情况，如服务交付模式、运营模式、具备的认证资质等，为客户制订审计实施范围，并建立审计监督基线，通过实施合规审计，从而能够准备认知云服务平台的安全合规水平，识别存在的不足和问题，并制订后续的加固整改行动计划。

云计算安全培训服务

绿盟科技还向客户提供与云计算安全有关的各类培训，包括如何解读各项标准规范，如何构建安全控制基线，如何实施安全风险评估，如何进行安全体系设计与实施，以及如何对云计算安全体系进行持续的评估和监督审计，提升客户方人员的知识水平，以及增强客户云计算平台信息安全管理的成熟度。

七 云安全解决方案

SECURITY

云平台的安全建设是一个长期的任务，需要随着技术的发展和业务的更新，及时地制定设计新的安全方案，调整已有的安全策略。

目前，云计算技术也在快速发展和演进，云计算平台的体系结构也在不断变化，需要持续跟踪、研究最新的技术应用情况及存在的问题，并结合云平台体系结构的实际情况，对安全保障体系不断地评估、改进和完善。

作者和贡献者

作者

李国军，绿盟科技　　Email：liguojun@nsfocus.com

刘文懋，绿盟科技　　Email：liuwenmao@nsfocus.com

贡献者

朱博，绿盟科技　　Email：zhubo@nsfocus.com

张智南，绿盟科技　　Email：zhangzhinan@nsfocus.com

何财发，绿盟科技　　Email：hecaifa@nsfocus.com

罗爱国，绿盟科技　　Email：luoaiguo@nsfocus.com

庞南，绿盟科技　　Email：pangnan@nsfocus.com

王永孝，绿盟科技　　Email：wangyongxiao@nsfocus.com

关注云安全解决方案

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/category/securityreport/
- 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

八 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