云计算平台IaaS层网络安全架构研究与实现技术

赵淦森[1]，何文聪[2]，王海宇[1]，汤庸[1]，岳强[3]

（1.华南师范大学 计算机学院，广东 广州 510631；2.中山大学 软件学院，广东 广州 510275；
3.广东电子工业研究院，广东 东莞 523808）

摘 要：研究了现有计算平台IaaS层网络实现技术和网络安全需求，结合VLAN、Bridge、Iptables和网络虚拟化等技术，设计出一种针对IaaS云平台的网络安全架构，通过在虚拟化环境中的虚拟网络上构造面向安全的覆盖网，实现虚拟网络中网络数据的隔离。并且提出IaaS云平台网络动态安全防护的设想。提出的模型能够动态地在虚拟化环境中构造网络边界，对云计算基础设施中的不同服务的网络数据进行有效的隔离，使得虚拟网络的安全独立于物理网络的拓扑结构，满足虚拟化环境中屏蔽物理网络细节的需要，并且提升了云计算下的网络安全。

关键词：云计算；网络安全；基础设施即服务；网络虚拟化；动态网络安全

中图分类号：TP393 **文献标识码**：B **文章编号**：1000-436X(2011)9A-0108-10

On the research and implementation of IaaS network security architecture

ZHAO Gan-sen[1], HE Wen-cong[2], WANG Hai-yu[1], TANG Yong[1], YUE Qiang[3]

(1.Computer School, South China Normal University, Guangzhou 510631, China;
2.Software School, Sun Yat-sen University, Guangzhou 510275, China; 3.GDEII, Dongguan 523808, China)

Abstract: An extensive review on existing implementations of IaaS was conducted and the network security requirements of IaaS were identified. A mechanism for dynamic cloud network security was proposed, which is built on top of VLAN, Bridge, Iptables and network virtualization technology. The proposed mechanism is able to dynamically divide the virtual network of an IaaS cloud into several isolated networks, with each isolated network has its network data being confined within its own network perimeter. The dynamics of the isolated networks fits into the need of cloud computing where virtual machines may migrate from one physical machine to another at runtime. The isolation enforces the network security to a level similar to the physical networks where network perimeters are imposed by physical ports. The proposed mechanism enables network security built independent of physical network.

Key words: cloud computing; network security; IaaS; network virtualization; dynamic network security

---

收稿日期：2011-07-05

基金项目：粤港关键领域重点突破项目（20100101-5）；软件工程国家重点实验室开放基金（SKLSE2010-08-22）；广东省中国科学院全面战略合作项目（2009A0091100002，2010A090100004）；东莞市重大科技专项（2009215102001）；广州杰赛科技股份有限公司项目；广东省高等教育学会实验室管理专业委员会基金项目

Foundation Items: Canton-HK Key Field Critical Break-through Research Project(20100101-5); China State Key Lab of Software Engineering Open Fund (SKLSE2010-08-22); Canton-CAS Strategic Cooperation Project(2009A0091100002, 2010A090100004); Dongguan Key Science and Technology Research Project (2009215102001); GCI Science & Technology CO.,Ltd. R&D Project; Lab Management Committee of Guangdong Higher Education Association Fund

1　引言

云计算是一种新的计算模式，它通过网络向用户提供按需的、可伸缩的服务。通过大规模部署、灵活运作的并且弹性伸缩的虚拟化 IT 资源，能很方便的在不同用户之间共享和调整资源，同时能为用户提供不同层次的网络服务。云计算是一个服务集合，从服务模式上看，自上而下，云计算主要包括软件即服务（SaaS）、平台即服务（PaaS）、基础设施即服务（IaaS）3 种服务模式。从部署模式上看，云计算还可以分为公有云、私有云、社区云和混合云，适用于不同的应用场景和需求，不同的部署环境对云计算的性能、安全性及稳定性有不同的侧重和要求，云服务提供商可以根据实际的部署环境进行技术实现上的调整，从而使得云计算更具有针对性，产生更强的适应力。

云计算 IaaS 层服务位于云计算三层服务模型的最底端，它把 IT 基础设施（CPU、内存、存储、操作系统等）像水、电一样以服务的形式提供给用户，以服务的形式提供基于服务器和存储等硬件资源的高度可扩展和按需变化的 IT 能力[1]。现有的 IaaS 云平台，例如亚马逊的弹性计算云（EC2，elastic compute cloud）[2]，用于提供用户可定制的虚拟机，以满足用户的计算需求。IBM 的的“蓝云”云计算平台则是集软、硬件一体的平台，通过大量使用 IBM 先进的大规模计算技术并结合其软硬件系统的服务技术，提供类似于互联网的计算环境，并提供支持开放标准及开发源码的软件[3]。而 Eucalyptus 则是一种开源的软件基础结构，用来通过计算集群或工作站实现弹性的、实用的云计算服务[4]。这些现有的 IaaS 云平台，在网络安全的实现技术上各不相同，但都提供了基本的网络隔离性、及可定制的网络安全策略。但由于其主要面向提供公共云服务，其网络架构及网络安全实现方案较为复杂，在配置和应用上对管理员有较高的技术需求。

不同于传统的物理网络结构，在 IaaS 云平台中，使用虚拟化技术实现对物理硬件的池化，每个物理节点上运行一个或多个虚拟机，多个虚拟机共享同一个物理网卡与外界通信，用户需要通过网络访问虚拟机的资源。这种共享物理网卡的形式，使得虚拟机之间的网络流量在数据链路层上相互可见，导致恶意用户可以通过网络嗅探、ARP 攻击等方式窃取其他用户的信息或者破坏其他用户的网络通信，甚至对平台本身的网络通信进行破坏，对云平台的服务造成影响。

本文对 IaaS 云平台的网络安全实现技术细节做研究，通过实验验证技术路线的可行性，并针对云计算大规模部署及可管理性需求，设计一种 IaaS 云平台的网络安全架构，同时结合动态网络安全理论，初步将动态安全应用到云计算 IaaS 层的网络中。

本文安排如下，第 2 节简述 IaaS 云平台网络通信进行分析，描述基本的虚拟化网络通信方式及 IaaS 云平台的网络结构；第 3 节结合 IaaS 云平台的大规模部署特性及可管理性需求，设计一种网络安全架构并描述其架构运作；第 4 节详细描述了 IaaS 云平台网络安全实现技术，包括应用技术介绍，实现技术及配置，以及对技术实现的实验验证；第 5 节是本文的结束语。

2　IaaS 云平台网络通信分析

2.1　虚拟化环境下的网络通信

不同于现代交换网络结构中，通信节点直接与每个交换机端口相连的网络结构，在虚拟化环境下，每个物理服务器上运行着多个虚拟机实例，并且虚拟机之间会由虚拟网络相连接，再通过物理机的网卡连接到物理网络，从而构成更为复杂的网络结构。如图 1 所示[5]，在虚拟化环境下，运行在同一物理服务器上的多个虚拟机实例，在虚拟机控制器（Hypervisor）中通常存在一个虚拟交换机，将多个虚拟机的网卡连接起来，形成一个虚拟网络，同时也可以通过虚拟交换机，连接到物理服务器的网卡，从而与物理网络通信。因为处于同一台物理服务器上，一般情况下虚拟机之间能够相互通信，即同一台物理服务器上的虚拟机实例的网络流量相互可见。而在连接到物理网络后，虚拟机中的网络流量也能影响到物理网络的运行。在这种情况下，需要对整个 IaaS 云内部的网络结构进行更为复杂的设计和重新规划架构，以保证其安全性。

2.2　IaaS 云平台网络结构分析

IaaS 云平台中，由于用户需要在外部网络环境中通过远程连接的方式访问云平台提供的虚拟机实例，这要求虚拟机对外部网络是可访问的。在实现细节上看，通常是通过桥接的方式，将虚拟机的网卡桥接到云平台所在的网络中，从而实现外部网络用户的可访问，如图 2 所示。这种方式，等同于将虚拟机和物理机放置于同一个局域网中，因此虚

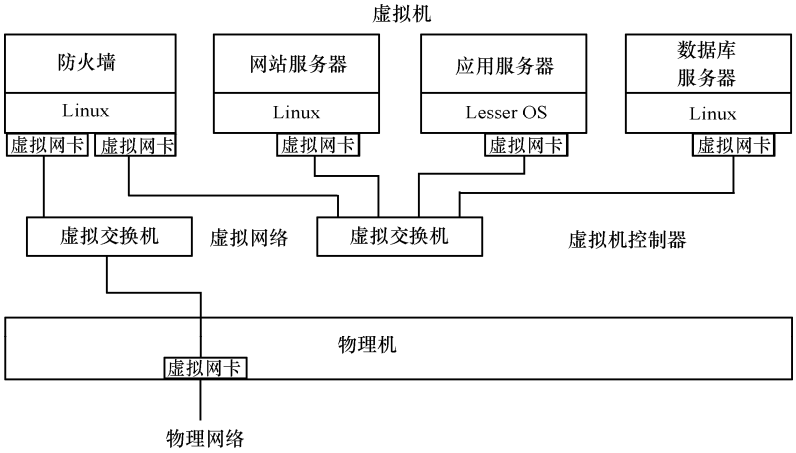


图1 虚拟化环境下的虚拟网络结构

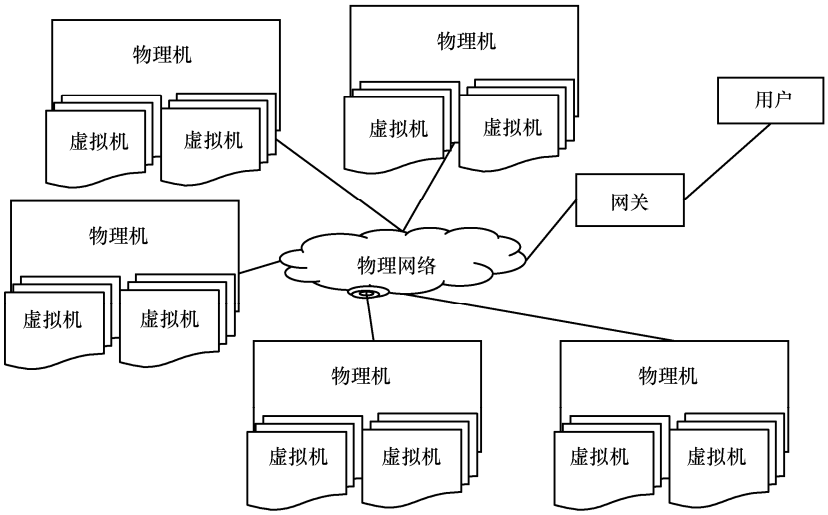


图2 IaaS 云平台的基础网络结构示意

拟机中的网络行为，将会影响到物理网络的通信。又因为虚拟机直接其实是通过虚拟网桥设备进行连接，其缺少类似物理网络交换机的网络安全特性，如 ARP 防护等功能，这又进一步导致不同用户的虚拟机以及提供不同服务的虚拟机的网络安全得不到保证。

这种情况下保证 IaaS 云平台的网络安全和服务稳定性，需要实现以下目标：

1）虚拟网络与物理网络相隔离，保证运作于物理网络的云平台通信不受虚拟机实例网络通信的影响。

2）运行于同一台物理服务器上的虚拟机实例之间可按需求隔离，即对运行在同一物理服务器但从属于不同用户或提供不同服务的虚拟机实例之间进行网络隔离和网络划分。

3）平台需提供可定制的安全策略，即可以通过管理员配置的安全策略，控制某些通信协议的数据。

3 IaaS 网络安全架构

根据上述需求及分析，本文中通过结合现有的物理网络 VLAN 技术及网络虚拟化技术，设计一种适用于大规模部署环境的云计算 IaaS 层网络安全架构。

3.1 架构分析

在 IaaS 云环境下，由于物理硬件的大规模部署，物理网络规模和复杂度大大增加。对于虚拟网络的管理，除了依靠分布式批量管理和配置外，还需要有较为清晰合理的架构。从单个节点的网络配置和规划，扩展到大规模部署环境中，主要面临以下问题。

1）网络配置调整问题

由第 3 节的实现技术分析和实验可知，要调整整个云内部虚拟机的网络通信，需要对物理节点和虚拟机的系统做许多设置和调整。这些设置和调整在大规模部署环境下，无法手工完成。这就需要云

平台内部通过自动化脚本和分布式批量管理的方式，由一个管理中心控制所有节点进行设置的调整。并且不同物理节点上的虚拟机，有可能处于同一个虚拟网络，这使得对不同物理节点的配置条件具有一定相关性，一个虚拟网络设置的调整，可能需要同时配置多个物理节点。

2）虚拟网络 IP 地址获取问题

由于虚拟化环境下，虚拟化平台主要对虚拟机的硬件（内存、CPU、硬盘、网卡等）具有高可控性和可定制性，虚拟机的 IP 地址属于虚拟机操作系统层面的配置，虚拟化平台对其可控性不高，因此通常使用外部的 DHCP 服务器对虚拟机的 IP 地址进行分配，同时可以结合虚拟机的 MAC 地址，进行固定 IP 的分配。而对虚拟机的虚拟网络进行划分和隔离，就需要不 VLAN 的虚拟机，获取到不同网络的 IP 地址，才能使得虚拟网络成功对外通信。

3）虚拟机对外通信问题

在 IaaS 平台中，用户需要远程连接到虚拟机，从而使用其计算资源。这要求虚拟机对用户在网络上是可访问的，而对云服务提供商来说，公网 IP 是有限的，甚至在企业内部部署的私有云，其原有的网络规划中，私有网络 IP 也是预先定义好的，如果云平台无法自成一个网络，对原有网络将会产生很大调整。因此云平台内部的虚拟网络必须使用私有 IP 地址进行从新规划，并且需要一个网关，将云内部虚拟机网络的私有网络地址发布到企业原有的私有网络中，从而在私有云中使用户可以访问虚拟机。而对于需要对外提供服务的虚拟机，可以使用公网 IP。

4）安全策略规划问题

由上述实验结果可知，配置虚拟网络的安全策略，主要是调整物理节点上的 LINUX 防火墙。在大规模部署的 IaaS 环境下，根据业务需求手动对虚拟机进行太细粒度的规则管理和配置不太现实，需要有可定制的安全策略，由管理员进行业务需求层面的定制，由云平台进行策略规则的调整。

3.2　架构设计

通过对 IaaS 云环境下的网络架构分析，结合虚拟化网络安全的实现技术，为解决上述提出的主要问题。一种可行的网络架构如图 3 所示。

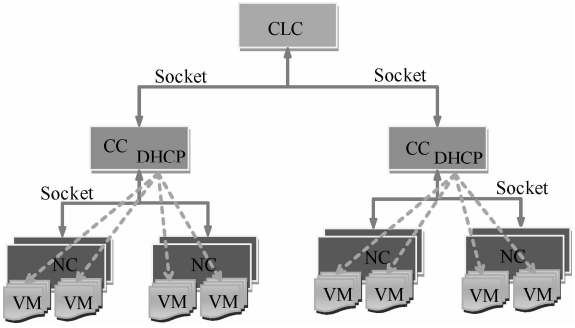


图 3　一种 IaaS 网络安全架构

如图 3 所示的 IaaS 云平台架构中，以一种 3 层架构的方式对整个云内部进行规划，最高层有一个云控制器（CLC），负责对云内部虚拟机（VM）资源的高层调度和对用户访问的控制。中间以集群的方式，对各个节点进行区域划分，用集群控制器（CC）对集群内部的资源分配，及网络调整进行控制。在各个节点上使用节点控制器（NC）对节点的配置进行直接的管理。

在网络配置上，针对大规模部署环境的配置调整问题，可以以事件驱动的形式，各个控制器之间通过 socket 进行通信，由上层的云控制器根据管理需求确定配置范围，由集群控制器转发或执行配置事件，最后在配置范围内的节点控制器负责直接执行相应的网络配置调整。其基本事件流程如图 4 所示。

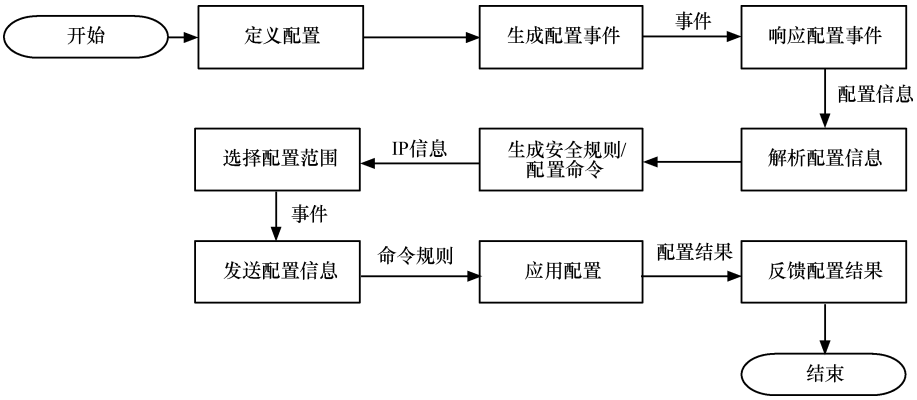


图 4　IaaS 云平台网络配置事件运作流程

针对虚拟机的IP信息获取的问题，在上述架构中，DHCP服务器部署在集群控制器中，可以通过集群控制器，根据云平台的网络配置需求操控DHCP服务器的配置，从而实现对本集群内的虚拟机的IP分配。同时，集群控制器使用双网卡，并通过LINUX系统本身的路由功能，实现对其管理的集群内部虚拟网络的流量转发和网络路由，从而使用户能实现对虚拟机的直接连接和访问。同时，对VLAN的创建等操作，也需要直接对DHCP服务器进行网络地址分配的配置和路由表的操作。其网络初始化操作的基本运作如图5所示。

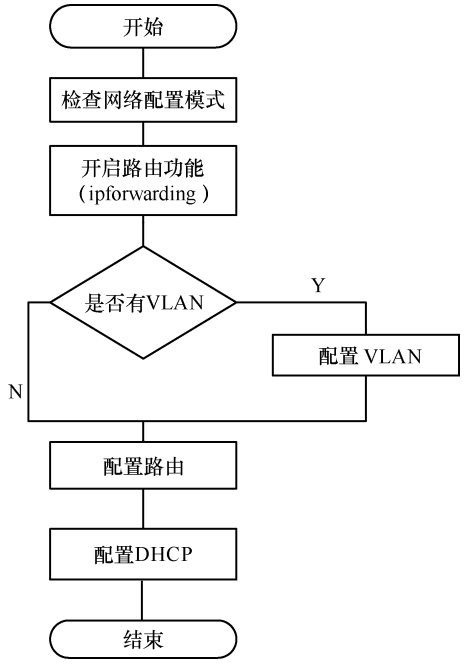


图5 集群控制器网络初始化流程

由于集群控制器使用双网卡并且开启了路由功能，只需要在连接云网络的网关路由器中，将到整个虚拟网络的路由下一跳指定到集群控制器，即可实现企业内部网络中，用户对虚拟机的直接访问。

对于安全策略的规划问题，可以引入物理网络中的ACL技术。因为从技术实现的分析上看，对虚拟网络通信的限制和调整，都是通过设置物理节点上的iptables安全规则来实现，这类似于路由器中的扩展ACL。因此，在安全策略的定制中，可以通过预定的一系列安全规则，一个服务需求层面的安全策略，再由云平台解析并执行。而iptables的规则可以抽象成，源、目的、协议和决策。因此可以实现用户定义的规则。例如某台WEB服务器，只允许外网的HTTP访问，同时只允许管理机器（10.1.1.1）的SSH连接。针对这个安全需求，管理员可以定制两条安全规则并组成一个安全策略webserver。保存在平台数据库中，针对云平台中有类似需求的服务器，直接应该该安全策略即可。云平台可以根据策略内的安全规则解析成iptables的配置命令，并根据应用的对象确定配置范围并自动配置，达到所需效果。

3.3 策略定义与规则实现

在上述网络安全架构中，安全规则与安全策略是呈现给用户直接使用的主要部分，也是系统内部实现的关键点。安全规则主要由iptables的配置语句组成，其基本的配置可以实现对某个来源和目的，同时对某个网络访问协议的控制，其配置范例如下：

```
iptables -t filter -I FORWORD 1 -s 192.168.1.1
-d 192.168.1.2 -p icmp -j DROP
```

该配置规则实现对源IP192.168.1.1到目的IP 192.168.1.2的ICMP协议通信的限制，即禁止从192.168.1.1到192.168.2.2的ICMP通信。类似的配置还可以实现对源网络地址到目的网络地址的通信限制。通过对这种配置规则的抽象，呈现给云网络安全管理员的是简单的源、目的、协议和规则4个自定义的项目。管理员仅仅需要了解自己的安全需求，而无需关心iptables的配置细节。因此，安全规则是管理员对某个范围内通信进行控制的细节定义。

而在更高层的应用当中，管理员往往面对的是一种业务需求，例如对Web服务器的安全配置。这种需求往往是需要配置多条安全规则才能实现，同时也会存在一些通用的需求，例如针对多个Web服务器的安全配置。因此，本文参考类似路由器中的ACL机制，提出安全策略的概念。安全策略，是针对特定需求预先定义的一组安全规则，可重复应用到不同对象和范围中。因此，对云安全管理员来说，如果云网络中有大量的虚拟机实例担当WEB服务器的角色，并且它们由同一台管理机（IP：192.168.1.1）负责管理，那么他只需要定义一组安全规则，组成一个安全策略，并应用到所有服务器即可。其安全策略描述如下。

策略名：Web服务器安全

策略规则：

源：all 目的：all 协议：HTTP 决策：ACCEPT

源：192.168.1.1 目的：all 协议：SSH 决策：

ACCEPT

源：all 目的：all 协议：all 决策：DROP

根据 iptables 从上自下优先匹配的原则，实现对 HTTP 协议和 SSH 的可访问性，同时拒绝其他网络协议的访问，实现安全性配置。

同时，安全规则与安全策略的设计形式，可以更好的结合动态网络安全设计，实现对云计算 IaaS 层网络的动态安全防护。在动态安全设计中的 P2DR 模型，其安全策略可以由管理员预先定义。云安全管理员定义了针对不同攻击类型的一系列安全策略，网络安全系统通过策略提供的攻击类型与反应策略的匹配，在遇到攻击时自动选择适当的策略，实现对网络安全的动态响应。例如，针对 DOS 攻击，管理员定义如下安全策略，简要实现对受攻击实体的隔离：

策略名：DOS 防护

攻击类型：DOS 攻击

策略规则：

源：192.168.1.1 目的：all 协议：SSH　决策：ACCEPT

源：all 目的：all 协议：all 决策：DROP

此时在受到 DOS 攻击时，安全系统在得到 IDS 的通知后，选择该策略进行应用，可以立刻隔绝受攻击的目标的网络访问，同时留有管理机的网络入口，方便管理员进行登录处理。

最后，因为策略规则的适用范围主要根据 IP 地址和网络地址进行限制，所以可以在安全系统内部通过结合应用实例的 IP 信息进行自动调整，从而实现基本的可推导性。例如，　云网络中某个网段（例如：192.168.3.0）被黑客入侵并成为肉鸡发布恶意流量，安全系统可以根据 IDS 汇报的入侵范围，推导隔绝 192.168.3.0 网段的安全规则：

源：192.168.3.0 目的：all 协议：all 决策：DROP

并自动应用到该网络内的所有机器，实现动态安全防护。在更智能的情况下，可以直接根据攻击的类型，推导出需要隔绝的网络协议，进行更细粒度的调控。

3.4　动态安全设计

由于网络通信动态的行为特征，网络安全具有不确定性与动态变化的性质，对网络安全的防范也从传统的静态安全机制转变为动态安全防范。网络安全模型，是动态网络安全过程的抽象，目前主要有两种动态网络安全理论模型，即 PDR 模型和 P2DR 模型。

PDR 模型通过防护（protection）、探测（detection）和响应（response）3 种方式来保证网络系统整体的安全性，如图 6 所示。而 P2DR 模型是在 PDR 模型上的扩张，通过增加策略（policy），在安全策略的指导下及时发现问题并迅速响应，满足对网络动态安全防护的更高要求，其模型示意图如图 7 所示[6]。

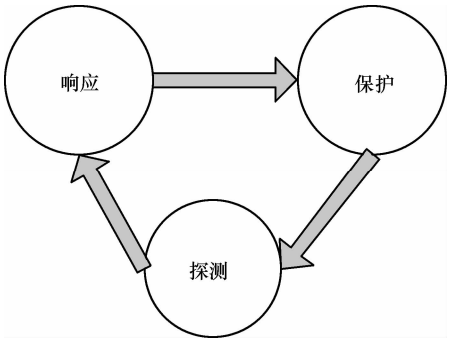


图 6　PDR 模型

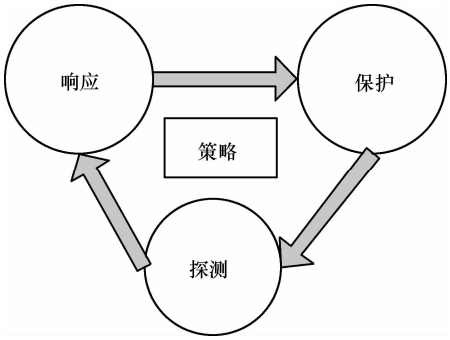


图 7　P2DR 模型[6]

在 IaaS 云平台中，使用动态安全网络模型，可以充分利用云平台的灵活性及自动化特性，对网络安全威胁能更迅速做出响应。

通过对上述网络安全架构的设计和分析，由于其能够自动完成 VLAN 调整及安全策略应用等操作，假设在云平台内部有一个 IDS（intrusion detection systems），便可以结合云内部网络的安全调整功能，实现基于 P2DR 模型的动态安全防护。针对 IaaS 平台网络安全的动态安全模型设计如图 8 所示。

如图 8 所示，云平台的网络安全模块中，预留一个接口（Listener），负责监听 IDS 的结果，IDS 在检测到网络中出现攻击时，立刻通知 Listener，Listener 对收到的通知发出警报并做出响应，同时立刻调度云网络控制器（CLCnetMgr）进行处理，

CLCnetMgr根据攻击类型，选择适当的策略，并解析其操作，根据操作事件触发CCnetMgr、NCnetMgr进行网络配置调整。最终在NCnetMgr的操作返回同时，CLCnetMgr像Listener汇报处理结果。在发生攻击和处理的过程中所有组件都会通过日志记录所进行的操作，方便管理员在事后进行查询。

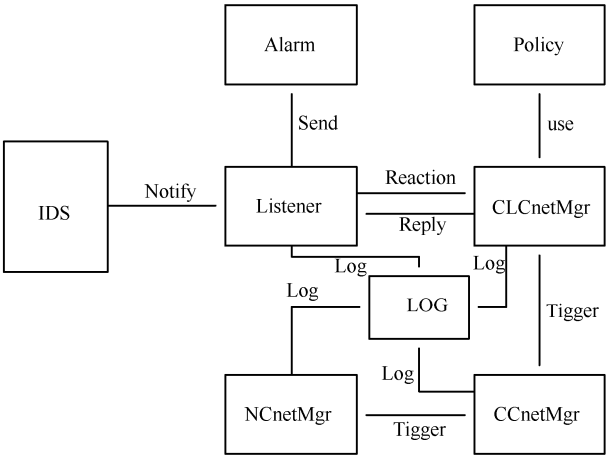


图8 vebula动态安全模型

假设假设云内部的某一台虚拟机VM1，对整个虚拟网络和物理网络发起了攻击。此时IDS检测到攻击，并通知Listener。此时，动态安全机制启动，假设默认对此类攻击的处理策略是进行隔离。则其响应的顺序图如图9所示。

由攻击响应的顺序图可知，在Listener触发CLCnetMgr做出反应之后，CLC提取出的安全策略，直接转化成对网络的配置调整，即后续的操作都采用网络架构本身的功能。

由此可知，只需在设计中将Listener模块的接口设计好，与IDS进行对接，即可通过本身的配置机制，实现动态安全扩展。同时，在策略上的调整和完善，可以使整个云网络对攻击的响应更加智能。

4 IaaS云平台网络安全实现技术

为了验证上述架构的技术可行性，实现IaaS云平台的网络安全，本文从单个节点上的虚拟网络进行分析，简要介绍VLAN、Bridge、VDE及netfilter/iptables等技术，通过实验验证对同一物理服务器上虚拟机网络通信的流量隔离及安全配置。

4.1 实现技术简介

在本文提出的技术方案中，为了实现对虚拟化网络的数据链路层隔离，从传统物理网络中引入VLAN技术，通过按照IEEE 802.1Q的标准，通过对以太网数据链路层的数据帧添加VLAN标记

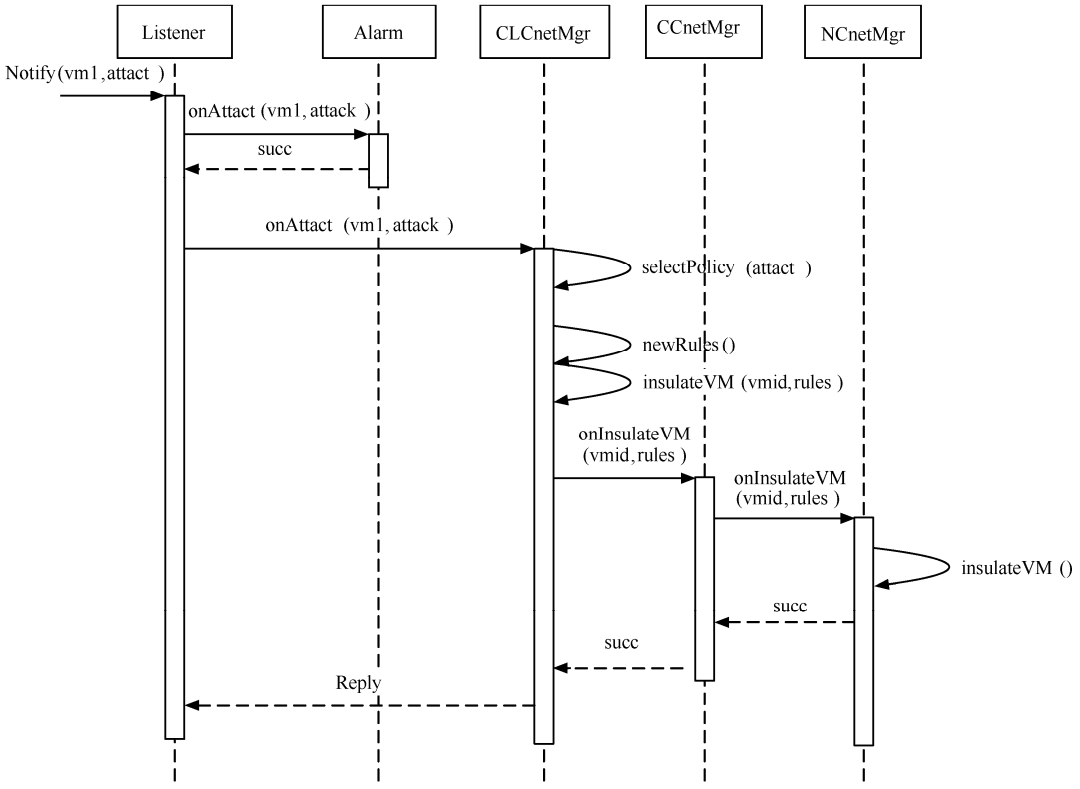


图9 攻击响应顺序

（VLAN tags），实现在数据链路层的广播域隔离，以实现对不同局域网中的主机进行逻辑分群管理和通信限制[7]。而为了实现与物理网络拓扑结构无关的虚拟网络划分，通过网络虚拟化技术，使用 VDE（virtual distributed ethernet）[8]虚拟交换机提供一个虚拟以太网络，使得运行在不同物理机上的虚拟机可以相互通信。为了实现安全策略的定制，可以通过 netfilter/iptables[9]设定一系列规则来管理网络数据包的流动和传送规则实现对虚拟机网络层上的通信限制与隔离。

4.2　实现配置分析及实验验证

在对整个 IaaS 网络安全架构进行设计前，先通过对单个节点和两个节点上的网络进行分析和配置，实现最基本的网络安全需求配置，并通过几个方面的实验进行技术验证。基本的实验环境如下。

操作系统：Ubuntu Linux 10.10

虚拟化环境：qemu-kvm 0.12.5

虚拟化管理环境：libvirt 0.8.3

软件环境：vlan，vde2

通过 qemu-kvm 结合 libvirt，在 libvirt 本身虚拟网络的基础上，实现以下配置实验，验证所用技术的配置效果及可行性。

1）单节点上通过 VDE 的 VLAN 功能实现虚拟机的网络隔离。

通常要使虚拟机对外部网络可见，一般使用桥接的方式将虚拟机的网卡桥接到物理网络中，为了实现在基本桥接网络模式下，虚拟机之间在数据链路层的隔离性，VDE 虚拟交换机本身的 VLAN 功能实现对不同的网络流量进行 VLAN 标记，从而达到网络划分的目的。实验如下。

① 实验准备条件：2 台 windows xp 虚拟机 vm1 和 vm2（包括配置 xml 文件，镜像文件），2 台 vm 分别关闭 windows 系统防火墙，并设置同一个网段的固定 IP：

vm1：192.168.1.1

vm2：192.168.1.2

② 关键配置步骤：

a）用 libvirt 命令启动 vm1，vm2（virsh create vm1.xml；virsh create vm2.xml）。

b）创建 2 个虚拟网桥 br1，br2（sudo brctl addbr br1；sudo brctl addbr br2）。

c）创建 2 个虚拟网卡 tap1，tap2（sudo vde_tunctl t tap1；sudo vde_tunctl-t tap2）。

d）启动虚拟网桥和虚拟网卡（sudo ifconfig br1 up；sudo ifconfig br2 up；sudo ifconfig tap1 up；sudo ifconfig tap2 up）。

e）将虚拟机分别接入虚拟网桥（sudo brctl addif br1 vnet0；sudo brctl addif br2 vnet1）。

f）将虚拟网卡接入虚拟网桥（sudo brctl add if br1 tap1；sudo brctl addif br2 tap2）。

g）启动 VDE 虚拟交换机（vde_switch-d-s /tmp/vde-M /tmp/mgmt）。

h）将虚拟网卡接入 VDE 虚拟交换机（vde_plug2tap-d-s /tmp/vde tap1；vde_plug2tap-d-s /tmp/vde tap2）。

i）配置 VDE，创建 2 个 VLAN（vlan1，vlan2）并将 tap1，tap2 所接的 VDE 端口分别加入 VLAN1，VLAN2 中

③ 通信验证测试：

a）在完成配置步骤 i）前，使用 virt-manager 图形管理界面打开 vm1，并尝试用 ping 命令与 vm2 进行 ICMP 通信测试，此时可以成功 ping 通 vm2。

b）完成配置步骤 i）后，vm1 中无法 ping 通 vm2。

④测试结论：

可以通过 VDE 提供的 VLAN 功能，实现在同一台物理服务器上，两台虚拟机之间的网络隔离。

2）单节点上通过 netfilter/iptables 对虚拟机通信进行控制。

为了验证实现安全策略配置，对虚拟机直接的通信进行网络协议级别的通信控制。通过在单个节点上对 netfilter/iptables 的配置控制 2 个虚拟机之间的通信，验证配置和技术方案可行性。实验如下。

①实验准备条件：2 台 windows xp 虚拟机 vm1 和 vm2（包括配置 xml 文件，镜像文件），两台 vm 分别关闭 windows 系统防火墙，并设置同一个网段的固定 IP：

vm1：192.168.1.1

vm2：192.168.1.2

②关键配置步骤：

a）用 libvirt 命令启动 vm1，vm2（virsh create vm1.xml；virsh create vm2.xml）。

b）在 vm2 配置 windows 文件共享，共享一个文件夹并测试在 vm1 上是否可访问。

c）默认启动 vm1，vm2 时，由于通过 libvirt 启动，vm1 和 vm2 被接入同一个虚拟网桥 virbr0 中。

d）配置 iptables，阻止 vm1 到 vm2 的 ICMP 通

信(sudo iptables-t filter-I FORWORD 1-s 192.168.1.1 -d 192.168.1.2-p icmp-jDROP)。

e) 在vm1上ping vm2的IP,验证配置的结果。

③通信验证测试:

a) 在完成配置步骤c之前,使用virt-manager图形管理界面打开vm1,并尝试用ping命令与vm2进行ICMP通信测试,此时可以成功ping通vm2,同时在vm1上打开网络邻居,可以看到vm2的共享文件夹。

b) 完成配置步骤c后,vm1中无法ping通vm2,但vm1仍然可以访问vm2的共享文件。

④测试结论:

可以通过netfilter/iptables的配置,实现对同一个物理节点上虚拟机直接网络通信的控制。

3) 2个节点上物理网络结构无关的虚拟网络划分。

为了验证在大规模部署时,可以通过VDE实现与物理网络结构无关的虚拟网络划分,通过以下实验验证其可行性。实验如下。

① 实验准备条件:

2台物理机(Node1, Node2)使用上述基本配置,并连接到同一个物理交换机中,IP分别为:

Node1:192.168.6.1

Node2::12.168.6.2

2台windows xp虚拟机vm1和vm2(包括配置xml文件,镜像文件)分别在Node1,Node2上,2台vm分别关闭windows系统防火墙,并设置同一个网段的固定IP:

vm1:192.168.1.1

vm2:192.168.1.2

② 关键配置步骤:

a) 在Node1, Node2上用libvirt命令启动vm1,vm2 (virsh create vm1.xml; virsh create vm2.xml)。

b) 根据实验1中的步骤,在Node1,Node2分别创建VDE虚拟交换机vde1和vde2并创建虚拟网桥及虚拟网卡,将虚拟机的虚拟网卡接入到vde1, vde2中。

c) 通过VDE cable将两台机器上的VDE交换机互联(dpipevde_plug /tmp/vde1 = ssh cloud@192.168.6.2 vde_plug /tmp/vde2 &)。

d) 在vm1上ping vm2的IP,验证配置的结果。

③ 通信验证测试:

在Node1上的vm1 ping Node2上的vm2,可以成功通信。

将Node2上的配置换成另外台在远程网络的物理主机。

Node3(ip:192.168.54.17),在配好相应的vm2, vde交换机后,再次使用vde交换机互联dpipevde_plug /tmp/vde1 = ssh cloud@192.168.54.17 vde_plug /tmp/vde2 & 。

此时在使用vm1 ping vm2,可以成功通信。

④ 测试结论:

可以通过VDE的远程互联功能,实现与物理网络无关的虚拟网络划分,只需要底层的物理网络是可通信的,处于不同物理机中的虚拟机可以通过VDE交换机通信。

通过上述实验可知,在单个节点上及2个节点之间完全可以通过文中所述的技术和配置,达到所需要的安全隔离效果。同时结合架构设计上对大规模部署的考虑,证明了本文所述网络安全架构实现的可行性。

5 结束语

本文在IaaS环境下,通过结合VLAN、VDE、网络虚拟化以及Netfilter/iptables等网络安全技术,对IaaS云平台的网络安全实现技术进行分析和实验验证,同时结合云平台大规模部署的特性,对IaaS云平台的网络环境和需求进行分析,设计一种可行的IaaS云平台网络安全架构,同时在此基础上结合动态网络安全理论,探讨了IaaS云平台实现动态安全防护的可行性。

本文中使用的技术,主要是在传统物理网络中广泛使用的网络安全技术,同时结合了网络虚拟化的实现技术。文中设计的网络安全架构,与Eucalyptus在主要结构上基本相同,但本文的网络安全架构及实现,更偏向于在企业私有云中使用,相对来说网络安全的实现更为简易,同时因为结合了VDE虚拟交换机,在实现VLAN的时候不依赖于物理网络拓扑结构,这是对Eucalyptus的改进。在安全策略的设计上,文中提出的类似路由器ACL配置的安全策略设计,比Eucalyptus的安全组功能更为通用,同时也更符合现实中的配置需求。本文末尾提出的动态安全实现设想,只是在IaaS云平台中使用动态安全的初步尝试,使用动态安全对于性能及平台运作上的影响尚未完全考虑,而引入更智

能的动态安全模型，如何更好的结合 IDS 进行安全防护，这些是本文努力的方向。同时，在共享网卡产生的流量及带宽影响上，本文尚未讨论，在未来可以结合支持 QoS 的虚拟交换机如 Open Vswitch[10]，实现对带宽的分配和限制。

本文的工作解决了 IaaS 平台在企业私有云部署环境下对网络安全配置的基本需求，在网络安全的自动化调整和动态安全响应等方面留有了较大的扩展余地，这对于企业私有云的自主扩展和定制具有较大优势。同时，本文的安全架构和实现技术主要基于虚拟化网络的相关技术，在物理网络的基础上构造一个虚拟网络的覆盖网，构造虚拟化网络层的多个网络边界，以实现网络流量和访问的约束。此设计和实现能够独立于具体的物理网络环境，满足云计算基础设施中的动态调整的需求。

本文工作的主要不足之处在于，未对所设计的方案进行量化的安全测评和性能测评，未能提供具体量化的安全指标以及性能指标。此部分工作目前正在开展，相关结果将于后续论文中发表。

参考文献：

[1] 朱近之，智慧的云计算[M]. 电子工业出版社，2010.
ZHU J Z. Intelligent Cloud Computing[M]. Electronic Industry Press, 2010.

[2] Amazon[EB/OL]. http://aws.amazon.com/ec2/, 2011.3.28.

[3] 陈康，郑纬民. 云计算：系统实例与研究现状[J]. 软件学报，2003，20(5):1337-134.
CHEN K, ZHENG W M. Cloud computing: system instance and state of the art[J]. Journal of software, 2003, 20(5):1337-134.

[4] Eucalyptus 官网[EB/OL]. http://www.eucalyptus.com/, 2011.3.25.
Eucalyptus official website[EB/OL]. http://www.eucalyptus.com/, 2011.3.25.

[5] JONES M T. Linux 中的虚拟网络[EB/OL]. https://www.ibm.com/developerworks/cn/linux/l-virtual-networking/, 2010.12.1
JONES M T. Virtual network in Linux[EB/OL]. https://www.ibm.com/developerworks/cn/linux/l-virtual-networking/, 2010.12.1

[6] 侯小梅，毛宗源，张波. 基于 P2DR 模型的 Internet 安全技术[J]. 计算机工程与应用，2000.1-5.
HOU X M, MAO Z Y, ZHANG B. Internet security technology based on P2DR model[J]. Computer Engineering and Applications, 2000.1-5.

[7] 维基百科，虚拟局域网[EB/OL]. http://zh.wikipedia.org/wiki/VLAN, 2011.4.3.
Wikipedia, virtual LAN[EB/OL]. http://zh.wikipedia.org/wiki/VLAN, 2011.4.3.

[8] VirtualSquare[EB/OL]. http://wiki.virtualsquare.org, 2011.4.5.

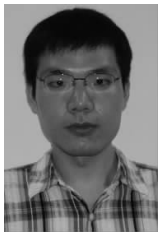
[9] 维基百科，Iptables[EB/OL]. http://zh.wikipedia.org/wiki/Iptables, 2011.4.3.
Wikipedia, Iptables[EB/OL]. http://zh.wikipedia.org/wiki/Iptables, 2011.4.3.

[10] Open vSwitch[EB/OL]. http://openvswitch.org/, 2011.3.28.

作者简介：

赵淦森（1977-），男，广东东莞人，华南师范大学教授，主要研究方向信息安全和云计算。

何文聪（1988-），男，广西崇左人，主要研究方向为计算机网络和云计算网络安全。



王海宇（1988-），男，河南新乡人，华南师范大学计算机学院硕士生，主要研究方向为云安全。

汤庸（1964-），男，湖南张家界人，博士，华南师范大学计算机学院院长、教授，主要研究方向为协同计算、时态数据库和云计算。

岳强（1963-），男，黑龙江望奎人，博士，广东电子工业研究院云计算与产业研究所所长，主要研究方向为涉及计算机体系结构、嵌入式操作系统、分布式计算、网格计算、云计算等。