软件定义边界
在 IaaS 中的应用

由 SDP 工作组提交

cloud security alliance®

致谢

在此，我们由衷地感谢所有为《软件定义边界在 IaaS 中的应用》提供意见和反馈的个人，您的贡献对这份报告带来了更多的价值和意义。

谢谢您们!

主要作者:
Jason Garbis Puneet Thapliyal

SDP 联合主席:
Bob Flores Junaid Islam

编辑:
John Yeoh

共同审稿人：
Brent Bilger
Vince Campitelli
Matthew Carter
Aradhna Chetal
Gerald Greer
Kevin Fletcher
Jeff Huegel
Scott Kennedy
Juanita Koilpillai
Dan Logan
Nya Murray
Elamurian R
Vijay Rangayyan
John Reel
Reza Reza
Colin Robbins
Puneet Thapliyal
Yoshio Turner
Flavio Villanustre
Manish Yadav
Erkki Yli-Juuti
Xing Zhang

设计者:
Stephen Lumpe (封面设计者)
Kendall Scoboria

中文版翻译说明：

由中国云安全联盟(C-CSA)秘书处组织翻译《软件定义边界在 IaaS 中的应用》（Software Defined Perimeter for Infrastructure as a Service），中国云安全联盟专家委员会专家翻译并审校。

翻译审校工作专家：（按字母顺序排列）

组长：陈本峰

组员：于新宇 、马韶华 、姚凯 、沈传宝 、方伟 、莫展鹏

C-CSA 工作人员：

朱晓璐（C-CSA 研究助理）

目录

序言

随着数字化及云服务的普及，企业对网络安全产品及解决方案的需求与日俱增。软件定义边界（Software Defined Perimeter，SDP）作为新一代网络安全解决理念，最早由云安全联盟（CSA）于 2013 年提出，其整个中心思想是通过软件的方式，在移动+云时代，构建起一个虚拟的企业边界，利用基于身份的访问控制，来应对边界模糊化带来的控制粒度粗、有效性差问题，以此达到保护企业数据安全的目的。

2017 年 2 月，CSA 正式发布《Software Defined Perimeter for Infrastructure as a Service》白皮书。该白皮书全面介绍了当前 IaaS 面临的安全挑战，为什么 SDP 可以改变 IaaS 安全现状，以及 SDP 在 IaaS 中的应用场景，从而为企业了解云安全问题及如何解决问题提供了有价值的参考。中国云安全与新兴技术安全创新联盟（简称：中国云安全联盟）特组织业界专家将该白皮书翻译为中文版本，相信一定会有助于更多的中国企业和 IaaS 公司从中获益。

中国云安全联盟和云安全联盟大中华区非常感谢翻译和支持工作者们和中国云安全联盟专家委员会专家们的无私贡献。

中国云安全与新兴技术安全创新联盟常务副理事长
CSA 云安全联盟大中华区主席
李雨航 Yale Li

目标

软件定义边界（SDP）的应用正在迅速普及，[1]其有效性在许多企业和案例中得到了广泛的验证。如今，随着越来越多的企业战略性地拥抱云计算 IaaS 平台，并且迫切需要云上资源的安全访问。我们相信，致力于保护云上资源的安全架构——SDP 的时机已经到来。

本报告旨在探索和解释软件定义边界（SDP）部署于 IaaS 时，对提高安全性、合规性和运维效率的相关优势。通过本报告，读者能够清楚认识到企业 IaaS 所面临的安全挑战（基于共享责任模型），原有的 IaaS 访问控制与传统网络安全工具结合产生的安全问题，以及软件定义边界在各种场景中的解决之道。

1 Gartner 预测，到 2017 年底，使用 SDP 来保护网络服务的企业将从 1%增加到 10%，而 2021，60%的企业将用 SDP 解决方案取代 VPN。（Gartner，《迎接新时代：隔离互联网污染环境与你的网络服务》，发布于 2016 年 9 月 30 日。）市场和市场预测未来 5 年的年复合增长率为 34%（http://www.marketsandmarkets.com/PressReleases/software-defined-perimeter.asp）。其他分析师如 ESG 也预测增长：http://www.networkworld.com/article/3141930/security/goodbye-nac-hello-software-defined-perimeter-sdp.html

方法和范围

• 本报告内容主要是基于公有云的 IaaS 产品，例如 Amazon Web Services、Microsoft Azure、Google Compute Engine 和 Rackspace Public Cloud。其相关用例和方法同样适用于私有化部署的 IaaS，如基于 VMware 或 OpenStack 的私有云。

• 不管是按照 SDP 规范实现商业化的厂商，还是没有严格按照 V1 标准进行产品开发的厂商，在构建产品的过程中，都有各自不同的架构、方法和能力。在本报告中，我们对产商保持中立，并且避免头轮产商相关的能力。如果有因为产商能力产生的差异化案例，我们会使用“也许、典型的、通常”等词汇来解释这些差异，以不牺牲报告的可读性。

• 由于大多数公有云 IaaS 提供商目前只支持 IPv4，因此我们所讨论的内容在一定程度上有所束缚。不过，随着 IPv6 的应用在未来普及，在下一版本的报告中，我们将进一步完善相关内容。

• 与核心 SDP 规范相一致，我们专注用户到服务（user-to-service）的访问控制（南北方向）。服务器到服务器 Server-to-Server（也称为东西方向）通信不在本报告的范围之内（为响应市场发展趋势，在核心 SDP 规范和本报告的未来修订中，我们将会解决这一问题[2]）。服务器到服务器是核心规范 V1 中所提到的一个支持模型，但目前，该模型还未像用户到服务模型那样被高度采用。

• 高可用性和负载均衡不在本报告讨论范围之内。

• SDP 策略模型不在本报告讨论范围之内。报告中讨论的 SDP 用例和方法也可以适用于平台即服务的系统 PaaS，这取决于它们如何支持和管理网络访问控制[3]。

在撰写这份文件时，我们努力做到内容聚焦。我们考虑了很多值得探讨的话题，但这些话题要么更适合包含在整个 V2 规范中，要么我们认为与本报告无关。请参阅“增强 SDP 规范的建议”部分，这些建议提及到 V2 规范的相关重点，比 IaaS 有更广泛的适用性，其非常重要。

虽然我们避开了这些话题，但该报告的内容仍超过了目标页数，不过我们相信，在平衡内容长度和范围方面我们做出了正确的选择。该报告也将为我们下一次内容的修订提供了良好的基础。

2 注意，在 IaaS 环境中，实际上，在某些情况下，与内网环境相比，IAAS 网络安全组更容易控制东西方向流量，因为 IAAS 网络安全组默认地拒绝跨服务器流量，这必须明确启用。

3 例如，如果 PAAS 系统支持源 IP 地址限制，则它可以被配置为只接受来自 SDP 网关的访问，这样可以让 SDP 策略来控制用户访问。

执行摘要

如今，IT 和安全管理者已深刻认识到，企业和云提供商有共同的责任共同面对 IaaS 安全挑战。IaaS 与传统的内网相比，有着不同的（并且在某些方面更具挑战）用户访问需求和安全需求，然而，这些需求并不能完全由传统安全工具或者 IaaS 供应商提供的安全架构来满足。

例如，企业往往需要对用户访问网络资源进行一定程度的限制，但传统的网络访问控制（NAC）和虚拟局域网（VLAN）解决方案在 IaaS 环境中并不适用，因为它是多租户、虚拟化的网络基础设施。另一个例子：在 IaaS 环境中，所有用户都需要对云资源进行“远程访问”，最成熟的手段无它，只有 VPN。但是，随着当今移动办公、跨公司协作或动态云环境等场景广泛存在企业当中，VPN 通过管理 IP 地址和端口的访问控制并不适用。企业越来越需要以用户为中心建立安全和访问模型。

使用软件定义边界（SDP）架构，企业用户可以安全地访问他们的 IaaS 资源，且不妨碍业务用户或 IT 生产力。事实上，当正确部署时，SDP 可以成为改变网络安全在整个企业中实践的催化剂——无论是在内网还是公有云的环境。有了 SDP，企业可以有一个集中管控并且策略驱动的网络安全平台，覆盖他们的整个基础设施（无论是在内网还是公有云环境）和他们的整个用户群体，这是一个引人注目的愿景。事实上，SDP 也正在实现这一愿景。目前，世界各地的许多企业组织都在使用 SDP 来增强他们的网络安全，减少网络攻击面，增加业务和 IT 人员的生产力，并减少他们的合规负担——同时节省资金。

- 本研究的重点是如何将 SDP 部署于（IaaS）基础设施的环境中，重点为以下用例：
- 开发人员安全访问 IaaS 环境
- 业务用户安全访问内部公司应用服务
- 管理员安全访问公共对外服务
- 在创建新服务器实例时更新用户的访问权限
- 服务提供商的硬件管理后台访问
- 多企业帐户访问控制

此外，本研究报告还解释了为什么传统的网络安全方法不适用于 IaaS 环境，以及 SDP 部署在混合环境中的价值。

软件定义边界和云安全联盟提出的十二大安全威胁

云安全联盟公布了一个值得关注的网络安全威胁的报告，以此帮助企业对云计算的采用做出明智的风险管理决策。该报告反映了安全专家在 CSA 社区中就最重要的云上的安全问题所达成的一致意见：SDP 可有效减少受攻击面，缓解或者彻底消除安全报告中提到的威胁、风险和漏洞，从而帮助企业能够集中资源于其他领域。

下表列出了十二大威胁（《十二大网络安全威胁》），并分析 SDP 对于解决这些威胁的作用：

	安全威胁	SDP作用
1	数据泄露	SDP通过添加预验证和预授权层来减少公开暴露的主机的攻击面，实现服务器和网络的安全性的“最小访问权限”模型，从而有助于减少数据泄露的许多攻击方式。 剩余风险：数据泄露的几个其他攻击方式不适用于SDP，包括钓鱼、错误配置和终端保护。授权用户对授权资源的恶意访问将不会被SDP直接阻止。
2	弱身份、密码与访问管理	过去，企业VPN访问密码被盗往往导致企业数据丢失。这是因为VPN通常允许用户对整个网络进行广泛的访问，从而成为弱身份、密码与访问管理中的薄弱环节。 相比之下，SDP不允许广泛的网络访问，并限制对这些主机的访问权限。这使得安全体系结构对弱身份、证书和访问管理有更大的弹性。SDP还可以在用户访问资源之前执行强认证。 剩余风险：企业必须有一个积极的参与者来调整IAM流程，并确保访问策略被正确定义。过于宽泛的准入政策会给企业带来风险。
3	不安全的界面和API	保护用户界面不被未授权用户访问是SDP的核心能力。使用SDP，未经授权的用户（即攻击者）无法访问UI，因此无法利用任何漏洞。 SDP还可以通过在用户设备上运行的进程来保护API。目前SDP部署的主要焦点一直是保护用户对服务器的访问。 服务器到服务器的访问至今还不是SDP的一个重点，但是我们希望这将在不久的将来被包含在SDP范围内。 剩余风险：服务器到服务器API调用在这个时候不是SDP的常见用例，因此这种API服务可能不会受到SDP系统的保护。
4	系统和应用程序漏洞	SDP显著减少攻击面，通过将系统和应用程序的漏洞隐藏起来，对于未授权用户不可见。 剩余风险：授权用户可以访问授权的资源，存在潜在的攻击可能性。其它安全系统如SIEM或IDS必须用来监控访问和网络活动（见下文的内部恶意人员威胁）。

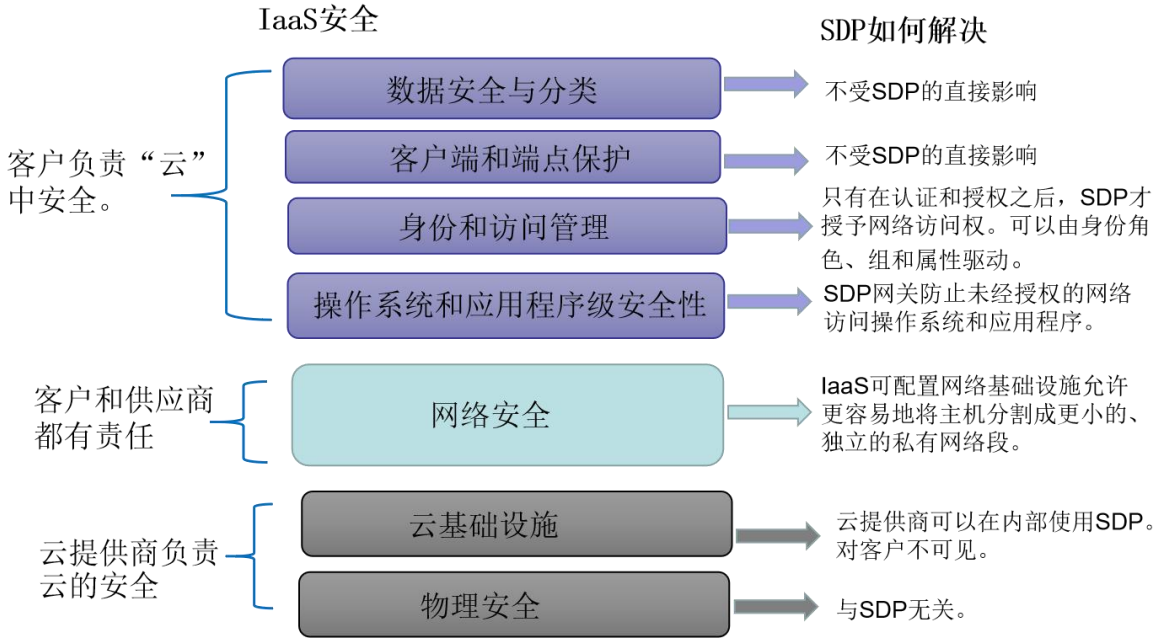
5	账号劫持	基于会话cookie的帐户劫持被SDP完全消除。如果没有预先认证和预先授权，并且携带适当的SPA数据包，应用服务器会默认拒绝来自恶意终端的网络连接请求。因此，即使网络请求中携带被劫持的会话cookie，也不会被SDP网关准入。 剩余风险：钓鱼或密码窃取仍然是一个风险，但SDP可以通过执行强身 份验证来降低这种风险，并有基于诸如地理定位等属性来控制访问的策略。
6	内部恶意人员威胁	SDP将限制内部人员造成安全威胁的能力。适当配置的SDP系统将具有限制用户仅能访问执行业务功能所需的资源，而所有其他资源都将被隐藏。 剩余风险：SDP不阻止授权用户对授权资源的恶意访问。
7	高级持续威胁攻击（APTs）	APTS本质上是复杂的、多方面的，不会被任何单一的安全防御所阻止。 SDP通过限制受感染终端寻找网络目标的能力，并且在整个企业中实施多因子认证，有效减少攻击面，从而降低APT的存在可能性和传播。 剩余风险：预防和检测APTS需要多个安全系统和过程结合起来进行深入的防御。
8	数据丢失	SDP通过执行最小权限原则，并将网络资源对未授权用户隐藏起来，来减少数据丢失的可能性。SDP还可以通过适当的DLP解决方案来增强。 剩余风险：SDP不阻止授权用户对授权资源的恶意访问。
9	尽职调查不足	SDP不适用这种情况
10	滥用和非法使用云服务	SDP并不直接适用，但SDP供应商的产品可能有能力检测和了解云服务使用状况。
11	DDoS攻击	SDP架构中的单包授权（SPA）技术使得SDP控制器和网关对阻止DDoS攻击更有弹性。SPA与典型的TCP握手连接相比可花费更少的资源，使服务器能够大规模处理、丢弃恶意的网络请求数据包。与TCP相比，基于UDP的SPA进一步提高了服务器的可用性。 剩余风险：虽然SPA显著降低了由无效SPA包所施加的计算负担，但它仍然是非零的，因此面向公众的SDP系统仍然可能受到大规模DDoS攻击的影响。
12	共享技术问题	SDP可以由云服务提供商使用，以确保管理员对硬件和虚拟化基础设施的访问管理。有关服务提供商的硬件管理控制面板访问，请参阅下面的讨论用例。 剩余风险：云服务提供商除了SDP之外，还必须使用各种安全系统和流程。

4 抗 DDoS SDP 工作组对这个问题提供了一些有趣的研究，一些正在进展中的的性能指标来对比传统 TCP 连接和 SPA 对服务器的负载的影响。值得注意的是，基于 UDP 的 SPA 甚至比基于 TCP 的 SPA 更有弹性，因为它消耗更少的服务器资源，并能更好地抵御无效的数据包流量攻击。

IaaS 安全概述

业界对云上运行的应用程序的安全性往往存在诸多误解。众所周知，如果部署恰当，基于云的应用程序比起内部部署更安全。但是，云环境遵循的是与传统内部部署不一样的安全模型，而这些不同可能无意间导致安全降低。因此，[5]向云端迁移工作业务系统不会自动让工作更安全，无论厂商还是企业都需要谨慎考量并采取行动。

IaaS 供应商通常会创建和推动“责任共享模型”，这个模型定义了 IaaS 供应商负责云的安全，而客户（企业）负责自己在云中的安全。下图是融合了几个领先 IaaS 供应商[6]的理念而创建的责任共享模型。



许多企业正在尝试拥抱云安全责任共享概念，尤其是IaaS提供商的工具集由自己创建时更是如此。这些工具倾向基于静态 IP 地址而不是基于用户（或身份），客户不能通过这种方法行之有效地管理基于用户的云资源的访问。因此，客户公司依赖应用级的身份验证来保护对这些资源的访问，致使内网里任何人都可对整个云网络进行访问。

从安全角度来看这自然存在相应风险——基于网络级的资源访问有太多可以被未经身份验证的攻击者利用的弱点。同时还有一个合规问题——企业经常要在敏感和受控环境中报告“谁访问了什么”。

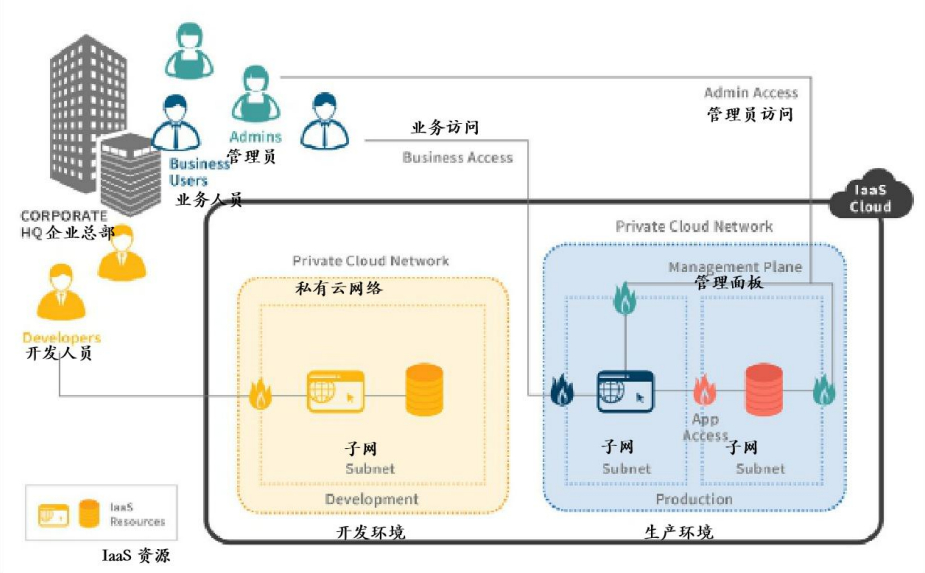
如上图所示，SDP 架构在与 IaaS 供应商的责任共享模型中有重要作用。通过 SDP，云客户可以在他们自身的安全共享控制部分采用更有效的方式

5 例如， 2017 年 1 月在不安全的、公开的 NoSQL 数据库上进行的 ransom 攻击是一个很好的例子，这些数据库大多运行在 IaaS 环境中
6 特别是这些来自于 AWS 模型 https://aws.amazon.com/compliance/shared-responsibility-model/和 Mircosoft Azure 模型 https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the-cloud-mean/

技术原理

IaaS 参考架构

本文读者对 IaaS 的组件和架构很熟悉，不需在此介绍。下图是一个对公有云和私有云部署都适用的 IaaS 环境的简化架构。



该图显示了一个包含两组 IaaS 资源（虚拟机），分成两个私有云网络的 IaaS 云环境。这些私有云网络可以对应不同的帐户，或云环境中不同的私有区域（如 AWS 虚拟私有云）。从网络访问的角度来看，这些私有云网络受到云防火墙的保护，防火墙在逻辑上控制这些网络的访问进出。对进入这些私有云网络(间)的访问控制很快就会变得复杂，不同的云提供者有不同的工具集。本文中，我们有意省略路由表、网关或 NACLs 等构件的复杂性，以便我们能够集中精力于管理用户访问 IaaS 资源所面临的挑战。

这个简单的模型不管供应商是谁，我们都可以持续地谈论云安全性和网络。具体地说，我们将在本研究中使用以下术语：

术语	描述	示例
云防火墙	控制云环境的网络流量进出的安全构件。通过将服务器实例分配给云防火墙组来进行管理。	AWS: Security Group Azure: Network Security Group
私有云网络	云环境中由单个帐户控制的独立网络区域。可能包括多个子网，并且可以由一个企业中的许多人访问。	AWS: Virtual Private Cloud Azure: Virtual Network
	IaaS 系统支持为服务器实例指派name-	AWS Tags

标签	value键值对。这些标签在 IaaS 系统中没有语义含义，但可以作为一个 SDP 系统进行访问策略决策的基础，非常有用。	Azure Tags
直接连接	IaaS供应商与电信运营商合作，提供从企业内部网络到 IaaS 环境的专用网络连接(通常使用 MPLS)。具有可靠和专用带宽的优点，通常可以将其细分为多个虚拟网络。	AWS Direct Connect Azure Express Route

为什么 IaaS 的安全性更复杂？

IaaS的网络访问存在一个重大的安全挑战。作为云安全责任共享模型的一部分，网络安全直接依赖于企业。将私有云资源公开到公共互联网通常不是一个可接受的选项——仅依赖于身份验证来保护，显然不符合安全和合规要求。因此，企业需要在网络层弥补这一差距。

由于如下几个原因，这是一个典型的复杂的安全挑战。

位置只是一个普通的属性而已

不同的开发人员（即使是座位相邻的开发者）也可能需要不同类型的网络来访问不同的资源。例如，Sally 是数据库管理员，需要访问运行数据库的所有服务器的 3306 端口。Joe 坐在 Sally 旁边，管理 Purple 项目的应用程序代码，并需要使用 SSH 连接到那些运行 Purple 项目的应用服务器。Chris 和小组其他人员不一样，他是远程工作的。他是 Purple 项目的应用程序开发员，尽管相隔千里也要求与 Joe 有相同的访问。

位置可能仅仅是访问策略需要考虑的属性之一，而非传统网络环境中网络访问层的主要驱动因素。

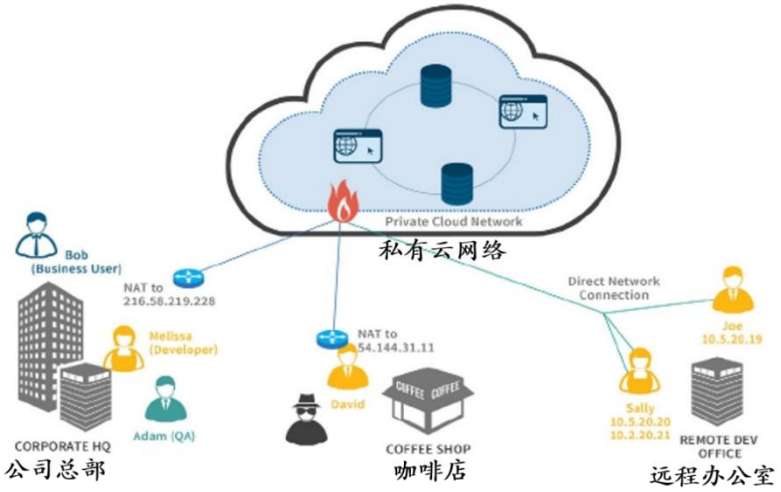
唯一不变的是变化

这是一个真理，在云环境中尤其如此。首先，IaaS 环境中的计算资源是高度动态的，服务器实例不断地被创建和销毁[7]。手动管理和跟踪这些访问几乎不可能。其次，开发者也是动态的(尽管从个人的角度来看不一定如此)——至少他们可能同时在不同项目中担任不同的角色。

这个问题在 DevOps 环境中被放大。开发、QA、发布和运维角色混合在一个团队中，对“生产环境”资源的访问可以迅速改变。

IP 地址难题

也许我们不需要传说中的网络管理员福尔摩斯 (CCIE #1)，但我们的 IPv4 世界确实面临着严峻的挑战：不仅用户的 IP 地址定期更改，用户和 IP 地址之间也没有一对一的对应关系。下图说明了当访问规则完全由 IP 地址驱动时，即使是简单的环境也会很复杂:



位置	网络设置	安全隐患
公司总部	所有用户都映射到单个 IP 地址。在此位置有许多用户需要广泛的网络访问能力	网络安全组无法区分用户，并且必须授予每个人所有资源的完全访问权限。这意味着恶意用户、攻击者或恶意软件可以从本地到云网络不受阻碍地穿越。
远程开发办公室	直接网络连接会保留每个用户的 IP 地址	IP 地址是动态分配的，并每天更改。用户还可以从多个设备访问云。 IT 运营团队不断更新安全组的规则（增加业务延迟）或网络完全对云开放（降低安全性）。
咖啡店	一个（或很少）用户需要从不同的位置远程访问，可能是 NAT的方式	来自这些位置的网络访问将会同步开放给同一网络上的任何恶意用户。IT管理员很难根据用户的位置和访问需求的变化来手动调整网络访问策略。

安全要求和传统安全工具

从根本上说，有两个问题需要解决：

- 安全地远程访问
- 用户访问的可见性和可控性

安全专业人员普遍认为向公网开放敏感服务是一个坏主意，并希望使用其中的一种或两种方法来保护敏感服务。

安全地远程访问

首先，让我们考虑安全的远程访问问题。直到今天，我们还没有发明一种将开发人员上传到云中的方法，所以，所有的云用户都是远程的，这意味着无论网络连接是公共互联网还是专用的直接连接，与云的通信都是在网络连接上发生。

企业通常通过使用 VPN 解决这一问题，通过建立站点到站点的 VPN(如上面的图中的公司总部位置蓝色线所示)，或者从用户的设备通过 VPN 集中器直接连到云。或者，结合上述两个方案，将用户从其设备通过 VPN 连接到企业网络，再从那里通过站点到站点的 VPN 进入云。

使用 VPN 在技术上解决了上面的问题的第一部分（安全地远程访问），它为从用户设备到云网络的网络通信提供了安全、加密的隧道。这有一些缺点，特别是如果所有的用户流量都需要先到公司网络，然后再去访问云，这将引入额外的延迟，造成单点故障,并可能会增加带宽成本和 VPN 授权的购买成本。通过 VPN 直接从每个用户的设备连接到云有助于解决其中的一些问题，但可能会与用 VPN 同时进入企业网络的需求（例如访问内部开发资源）发生冲突。

普遍来说,如果 VPN 上应用程序通讯协议已经是加密的，例如 HTTPS 和 SSH，并不会增强安全的保密性和完整性，

VPN 可以提供价值的一个方面是安全的可用性，因为被 VPN 保护的资源可以确保不会公开可见，从而防止 DDoS 一类的攻击。

这是我们下一节的一个很好的话题，在这里我们谈及查看和控制用户访问的需求，而这点 VPN 无法帮助到企业用户。

用户访问的可见性和控制

不管用户如何进入 IaaS 环境的（无论是否通过 VPN），安全团队仍然需要控制（并监视和报告）在 IaaS 环境中哪些用户可以访问哪些资源。

IaaS 平台提供了内置的工具来管理这一点，例如 AWS 中的安全组和 Azure 中的网络安全组（在本文中我们称为云防火墙），基于 IP 地址控制对服务器的访问。

这是**安全访问面临的最基础的挑战**——企业需要解决用户访问问题，但只被赋予了基于 IP 地址的访问控制工具。

让我们来看一个关于云防火墙的例子：

类型	协议	端口范围	源地址
HTTP	TCP	80	173.76.247.254/32
HTTP	TCP	80	50.255.155.113/32
HTTP	TCP	80	73.68.25.221/32
HTTP	TCP	80	98.217.113.192/32
HTTP	TCP	80	209.64.11.88/32
HTTP	TCP	80	172.85.50.162/32
HTTP	TCP	80	68.190.210.117/32
RDP	TCP	3389	173.76.247.254/32
RDP	TCP	3389	110.142.238.207/32
RDP	TCP	3389	50.255.155.113/32
RDP	TCP	3389	73.68.25.221/32
RDP	TCP	3389	98.217.113.192/32
RDP	TCP	3389	209.64.11.88/32

上述的防火墙配置片段展示了IaaS平台提供的简单IP地址规则方法。所有被分配到此防火墙组的虚拟机实例都将继承这个规则集，允许网络访问特定的端口。任何IaaS的用户都可以证明这种方法存在以下几个问题：

- 它提供对此云防火墙中所有服务器的粗粒度访问
- IP 地址不能与用户对应
- 没有任何策略的概念，也没有解释为什么指定的源 IP 地址会在这个列表中。因此，依照用户的访问控制策略去实现任何一种复杂的访问控制都是相当困难和耗费时间的。
- 上述列表是静态的，不能依据用户位置和权限的变化而做出相应的变化。
- 上述方法没有考虑任何信任的概念（比如身份验证强度，设备配置文件或客户端行为），

并相应调整访问权限。

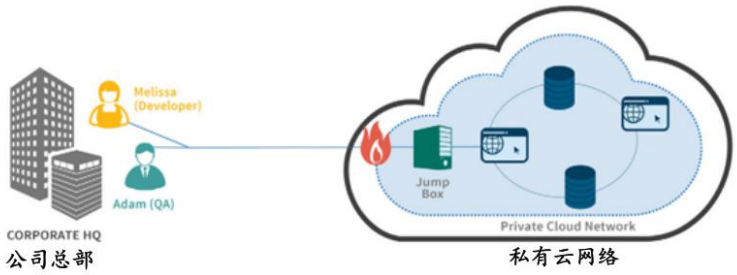
- 任何更改都需要对管理对 IaaS 账户进行管理访问，将导致以下两种之一发生：
    - 需要进行集中化处理，因而导致性能下降
    - 需要对更多用户设置管理员访问权限，从而产生安全性、合规性和操作性问题

在IaaS环境下，安全远程访问控制已经不再是一个特殊场景。所有用户都是“远程的”，因此，网络安全团队需要关心所有用户是如何访问资源的，而不仅仅是用户的一个子集。也就是说，安全的远程访问控制必须成为一个核心关注点，并且是采用IaaS的任何企业的整体策略的一部分。

注意：除了上述方法（将多个源 IP 地址添加到单个云防火墙）以外，在另外一些云平台上，你可以使用略微有所差异的方法——创建多个云防火墙（例如，针对每个用户的 IP 创建一个防火墙），或者每个云服务器实例关联多个云防火墙。这些都与上述方法具有相同的逻辑效果。虽然可以给防火墙分配有意义的名字（例如“Sally home and work”）让它能行之有效，但是这会带来额外的开销，并且这仍然是个静态的解决方案。

跳板机：三思而后行

跳板机，也被称作跳转服务器或跳转主机，使不安全区域的用户访问在更安全区域中运行的服务器或服务。对于本文档，使用跳板机的场景是使用跳板机来代理访问云环境中的服务器。



如上图所示，跳板机的网络访问可以是公开的，通过直接连接或者VPN来访问。访问跳板机桌面本身需要用户认证（多因子）。跳板机通过用对受管理的服务的强制单点访问，来控制云资源的访问。然而，跳板机中的诸多限制使得它不适合用于海量的云资源访问控制：

• 它不是典型的多用户系统，用于单用户访问受保护的服务器

• 它是为特殊场合的访问控制设计的，比如系统管理员访问，而不是为持续的访问控制设计的

• 它只能对跳板机网络中的所有服务器一刀切地提供“要么全有，要么全无”的网络访问控制

• 它是一个非常有价值的攻击目标。一旦攻破一个跳板机，或者一台可以访问跳板机的用户设备，就对攻击者开放了整个网络

• 难以跟踪用户访问以实现合规性检查

很显然，跳板机不是云系统用户访问控制的合适解决方案。

为什么是 SDP 而不是 VPN

VPN是一种广泛用于安全远程用户访问控制的普遍技术。但是为什么企业不能继续使用这种被验证过的技术呢？

VPN很好地为远程用户提供对虚拟局域网或网段的安全访问，就好像他/她们实际物理地存在于企业网络一样。这种技术，在与多因子身份认证结合时，对于具有传统边界的企业以及静态用户和服务器资源来说效果很好。但是正如Gartner的调研报告所说，“DMZ和传统VPN是为上世纪90年代的网络设计的，由于缺乏保护数字业务所需的敏捷性，它们已经过时。”[8]

VPN有两个缺点，使它们不适合当今的需求。首先，它们对所分配的网络提供非常粗粒度的访问控制。它们的目标是让远程用户的行为就像在本地网络上一样，这意味着所有用户都可以对整个虚拟局域网VLAN进行完全的网络访问。尝试配置VPN以为不同用户提供不同级别的访问是不现实的。它们也不能很容易地适应网络或服务器集群的变化。VPN根本无法跟上当今的动态发展的企业的需要。

其次，即使公司对VPN所提供的控制级别感到满意，但VPN只是一种控制远程用户的竖井式解决方案——它们不会帮助保护本地内网中的用户，这意味着组织需要一组完全不同的技术和策略来控制本地用户的访问。这将使协调和匹配这两个解决方案所需的工作量成倍增加。而且，随着企业采用混合和基于云计算的计算模型，VPN就更难被有效地使用。

Gartner 指出：“到 2021 年，60%的企业将逐步淘汰 VPN，换而使用软件定义边界（SDP），（尽管 2016 年 SDP 的使用量不到 1%）。”[9]

虚拟桌面基础设施（VDI）

虚拟桌面基础设施（VDI）是一组技术，可以让企业在企业数据中心的集中式服务器机群中托管大量的桌面操作系统实例。这些实例可以是桌面操作系统的虚拟化实例，也可以是许多用户并发登录到的桌面操作系统的多用户版本。与VPN一样，VDI一直是企业用来远程访问其网络和应用程序的一种重要机制。

总的来说，在今天的云计算和移动世界中，VDI有一些缺点。首先，远程桌面的用户体验往往在小型的移动设备上表现不佳。它不会以一种响应的方式呈现，而且非常难以使用，因此会阻碍生产力。

其次，很多基于桌面的客户端/服务器（C/S）应用程序已经被重新编写为Web应用程序，从而减少了VDI的价值。第三，VDI集群的采购成本很高，尤其是如果它们是基于硬件的。最重要的是，随着越来越多的工作业务系统转移到云上，企业已经意识到VDI并不能解决远程应用程序的用户访问的问题。

事实上，VDI确实解决了部分远程访问问题——通常通过对从客户端设备到VDI服务器的流量进行加密，但它不能帮助解决核心的用户访问问题——控制一个特定用户可以访问的网络资源。在某些情况下，VDI会使多个用户出现在一个多用户操作系统中，从而使这个问题变得更加困难。在这种情况下，通过传统的网络安全解决方案进行网络访问控制实际上是不可能的。

VDI 无疑是有一定的好处，但是它并不是为了控制用户对云网络和服务器资源的访问而设计的，因此在某些方面甚至会使这个问题变得更加困难。

SDP 怎么解决这个问题？

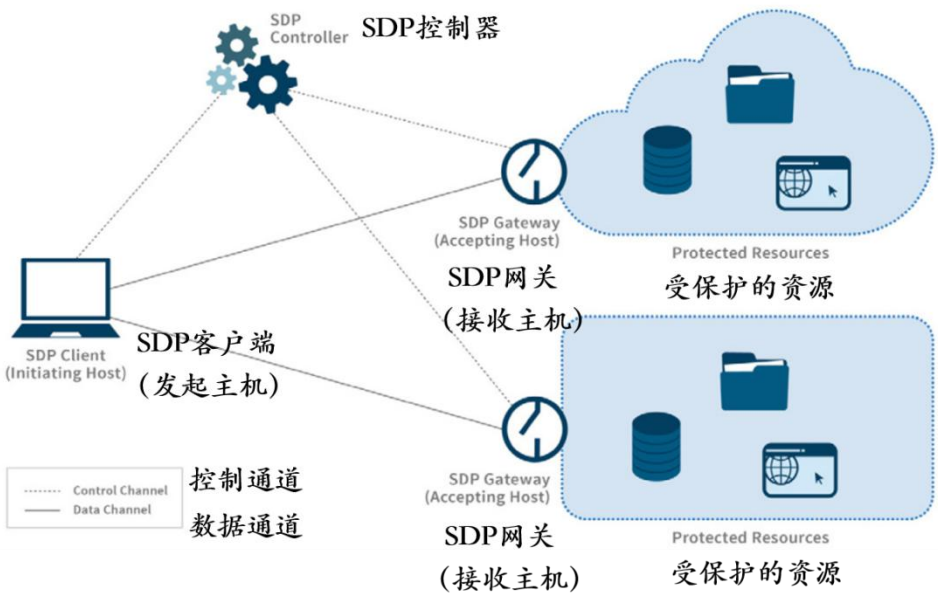
SDP可以解决上面讨论的所有安全问题，为企业提供对IaaS环境的安全远程访问，并对用户访问做到细粒度的可见性和控制。

通过使用SDP，企业的云资源对于未经授权的用户完全不可见。这样完全消除了许多攻击方式，包括暴力攻击；网络流量攻击，以及TLS漏洞攻击，如著名的“心脏出血Heartbleed漏洞” 和 “贵宾犬Poodle漏洞”。SDP通过在企业的服务器周围建立一张“暗网”，帮助它们成功地为云计算安全负责。

SDP 以预认证和预授权作为它的两个基本支柱。通过在单数据包到达目标服务器之前对用户和设备进行身份验证和授权，SDP 可以在网络层上执行最小权限原则，可以显著地缩小攻击面。

什么是软件定义边界（SDP）？

软件定义边界[10]（SDP）架构由三个主要组件组成，如下所示：



CLIENT 客户端（发起主机）	每个用户的设备上运行的客户端
CONTROLLER 控制器	用户身份认证的组件（可选择性地与用户身份管理系统集成），并在授予每个用户个性化的网络权限之前对其进行验证
GATEWAY 网关（接收主机）	网关代理访问受保护的资源。客户端的流量通过加密的通道发送到每个网关，在那里它被解密并发送到适当的应用程序（受保护的资源）。如上图所示，SDP 体系结构支持多个分布式网关，每个网关保护一组应用程序或系统资源。

用SDP术语来说，客户端（用户设备）指的是发起主机，网关指的是接收主机。在通过控制器进行身份验证后，客户端为每个网关建立加密的隧道（上面的图表显示了两个分布式网关，每个网关保护一组不同的资源，由单个控制器管理）。

SDP规范中的一个重要元素是单包授权（SPA）。使用这种技术，客户端基于一个共享密钥（seed）创建一个基于HMAC的一次性口令，并将其提交给SDP控制器和网关，作为连接建立过程发送的第一个网络数据包。（它也用于网关与控制器的连接建立）

因为 SDP 控制器和网关拒绝无效的数据包（可能来自未经授权的用户），所以它们可以防止和未经授权的用户或设备建立 TCP 连接。由于非法的客户端可以通过分析单个数据包来区分，所以 SDP 控制器和网关所产生的计算负载是最小的。这极大降低了 DDoS 攻击的有效性，并使得 SDP 服务可以在面向公众的网络中可以更安全、更可靠地部署。

基于用户而不仅仅是 IP 地址策略

由于 SDP 系统是以用户为中心的（也就是说，在允许任何访问之前，它们先验证用户和设备），因此它们允许企业基于用户属性创建访问策略。通过使用诸如目录组成员、IAM-分配的属性和角色等机制，公司可以以一种对业务、安全和合规性团队有意义的方式定义和控制对云资源的访问。相比之下，传统的网络安全系统完全基于 IP 地址，根本不考虑用户。

SDP 的优势

部署 SDP 的企业将在改善安全性的几个维度受益，我们希望在本文档的其余部分中清楚地表达出来。SDP 的其他好处包括运维效率、简化的合规性工作和降低成本等。下面我们将进行一一探讨。

运维效率

与达到特定级别的安全性所需的手工工作相比，SDP 的自动化策略执行在运维上体现了显著的好处。从另一个角度来看，一个企业可以通过 SDP 轻松获得的安全性级别实际上是不可能通过传统的安全工具实现的。

简化的合规性工作

SDP的实施产品通常提供每个用户访问权限和活动的详细记录，这是由于网关对所有客户端网络流量进行日志记录和控制。因此，SDP可以根据这些细节提供自动化的合规性报告。

而且，由于 SDP 支持对用户访问的细粒度控制，企业通过将其网络分割成更小的、隔离的部分来获得降低合规性需要的范围。

降低成本

SDP可以帮助企业以多种方式降低成本。首先，对访问策略的自动执行减少了为响应用户

或服务器更改而手动更新和测试防火墙规则的需求。在较大的企业中，这通常是其IT人员日常工作的一部分，因此这提供了一个减少工作量和人工成本的机会（特别是在外包模型中）。它还将提高业务和技术人员的生产效率，同时也可以有效降低硬成本（特别是对于小时工或外包的工人）。

其次，简化的合规性工作将减少准备和执行审计所需的时间和精力。这两项活动都需要第三方咨询师，节省的每一小时都是直接的成本节约。

最后，SDP 还可以给企业带来一种替代其他技术的方案，从而降低成本。例如，我们已经看到一些企业在考虑升级传统 NAC 的网络交换机时选择了 SDP，这为他们节省了数十万美元的资本支出。

SDP 作为变革的催化剂

我们特别欣慰的是，SDP可以成为变革的催化剂。我们相信，SDP代表了安全架构的突破，并将很快成为广泛被采用的保护网络服务的方法。

我们越来越多地看到企业公开支持 SDP 作为它们实施安全的新方式，并将其作为一个机会来取代传统的安全技术，如 VPN、NAC、或 DMZ，因为它是一种更有效、更动态、更安全的替代品。

SDP、身份及访问管理

SDP、身份及访问管理（IAM）在很多方面都是互补的。首先，SDP 能实现对已经部署的 IAM 系统进行身份验证，这可以加速 SDP 的上线。这种身份验证可能通过连接到本地 LDAP 或 AD 服务器，或者使用 SAML 之类的标准来实现。

其次，SDP实施产品通常使用IAM用户属性（如目录组成员、目录属性或角色）作为SDP策略的元素。例如，一个SDP策略可能会定义为“目录组中的所有销售用户都可以在443端口上访问销售门户的服务器。”这是一个很好的例子，说明SDP系统如何为现有的IAM系统增值（并扩展能力）[12]

最后，SDP系统也可以包含在由IAM系统管理的身份生命周期中。通常被称为“加入，移动，离开”流程，IAM系统管理着与用户帐户和访问权限相关的业务和技术流程。部署SDP的企业应该将SDP管理的网络权限包含到它们的IAM供应系统中。例如，当IAM系统在应用程序X中为Sally Smith创建一个新帐户时，SDP系统应该同时创建相应的网络权限。

综上所述，这种集成很好地支持了第三方用户访问SDP系统。SDP控制器信任第三方IAM系

统提供的身份验证和用户身份生命周期的所有权管理。因此，当第三方用户在它们的IAM系统中被禁用时（这对企业的用户禁用流程非常关键），用户将自动无法访问SDP保护的资源，因为他们不能通过关联进行身份验证。这个关联很好地解决了第三方访问的一个常见问题。

关于 SDP 和 IAM 如何一起工作还有很多内容要写，但是这样的分析在这个文档中是不可能的（尽管我们很喜欢这两种技术）。我们正在考虑将其纳入 SDP v2 规范中。

8 Gartner:G00315586，《迎接新时代：隔离互联网污染环境与你的网络服务》，2016 年 9 月 30 日

9 如上

10 SDP 版本 1.0 规范在这里提供：https://cloudsecurityalliance.org/download/sdp-specification-v1-0/

11 防 DDoS SDP 工作小组对这个主题有一些有趣的研究，还有一些正在研究的性能指标，对比了使用传统 TCP 连接和 SPA 在服务器负载上的区别。请注意，基于 UDP 的 SPA 比基于 TCP 的 SPA 更有弹性，因为它消耗的服务器资源更少，并且能够更好地抵御无效的数据包流量攻击。

12 这个例子是一个真实的策略，但是它在一些更大的环境中可能会面临挑战。供应商应该考虑支持参数化的策略，例如，一个使用身份和系统属性的策略有效地声明“只有部门中的用户可以访问他们在端口 443 上的部门门户”。

IaaS 使用场景

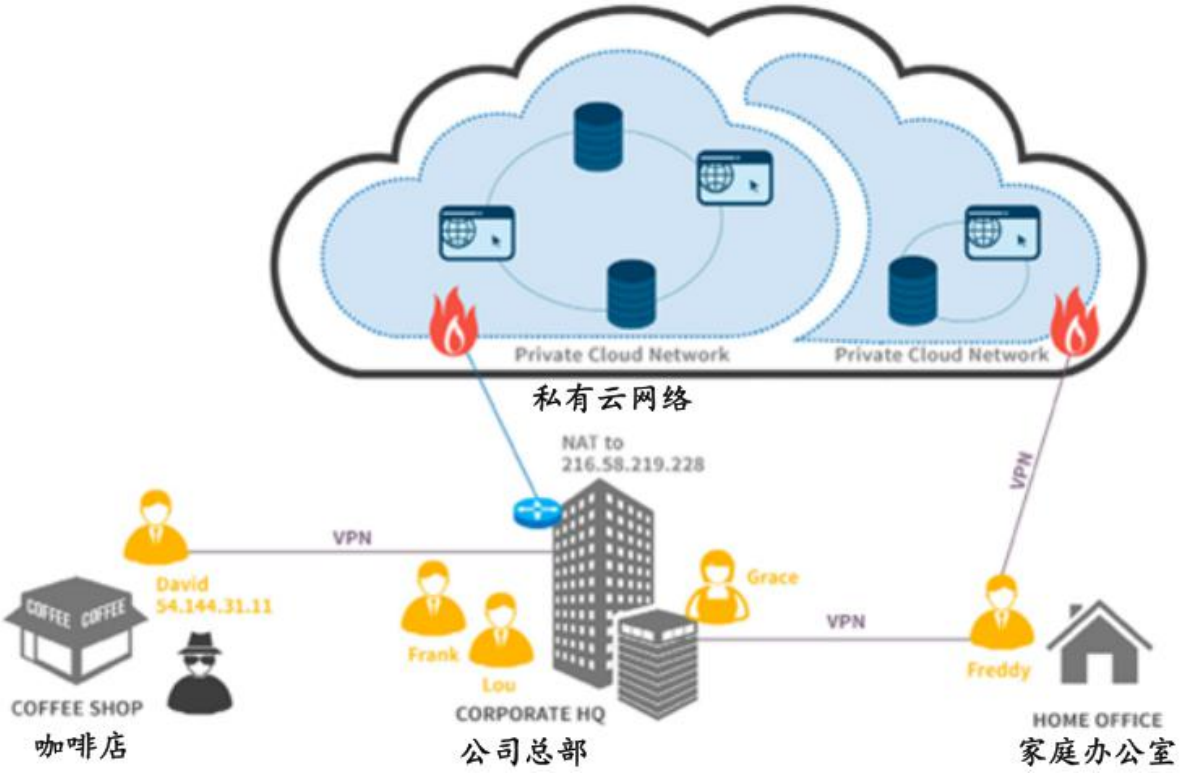
本节包含六个用例，代表了 SDP 可以为 IaaS 访问的核心需求提供帮助。

用例场景：开发人员安全访问 IaaS 环境

开发人员需要访问IaaS资源，用于开发，测试和部署工作。这些用户需要访问各种协议和端口，以及访问不断变化的IaaS资源。

开发人员可能会处理敏感数据，在 DevOps 环境的生产系统中工作。因此，在安全性和合规性的需求下，组织对系统访问行为必须是可视而且可控的。

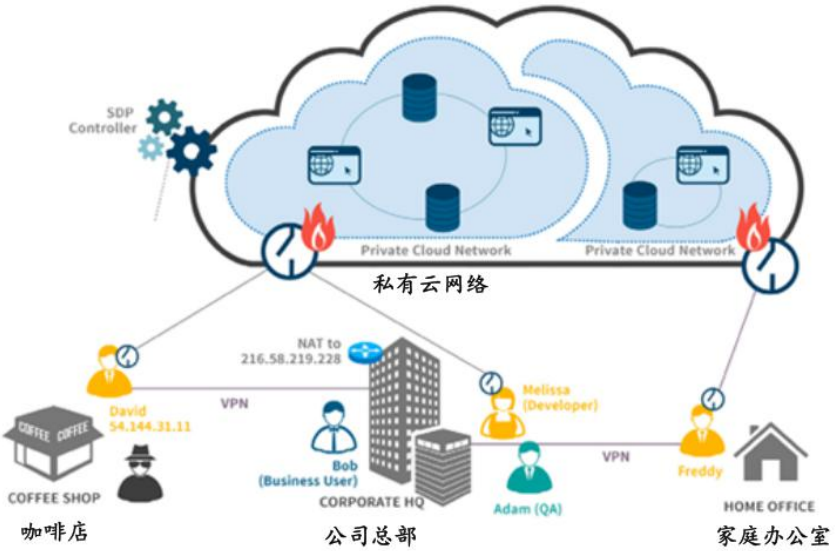
不使用 SDP 的访问



如上图所示，各种开发人员需要访问两个私有云网络环境。这些开发人员具有不同的访问要求，并且处于不同的位置。云防火墙是网络流量的唯一控制点，实质上是一个包含所有授权连接的简单表格。表格包含源 IP 地址到目标服务器和端口的映射。

使用 SDP 的访问

SDP部署如下。控制器（如下页图所示）在所有用户均可访问的位置运行（为了清楚起见，连接未在图中显示）。它可能在云端的公共可访问位置运行，或者可能在总部的DMZ区运行。访问控制器受单包授权（SPA, Single-Packet Authorization）保护，因此将其暴露在互联网并不会显著增加风险。



用户通过 SDP 控制器正确验证身份后，他们通过 SDP 网关访问私有云网络上的资源。网关也受 SPA 保护，所有用户流量都通过互联网上的加密隧道传输。网关对每个用户执行访问控制策略，以实现最小权限原则。网关位于每个私有云网络的入口点，并控制所有入站流量。

对照

需求：Grace，Lou和Frank在总部工作，需要通过应用程序进行协作，在多个服务器实例上访问端口22（SSH），443（HTTPS），3306（MySQL）和3389（RDP）。

挑战：总部的所有系统都 NAT 到单个 IP 地址 216.58.219.228

不使用 SDP	使用 SDP
方法：必须将防火墙配置为允许从216.58.219.228到私有云网络中的所有服务器上的所有服务器上的所有端口的流量通过。这些服务器必须分配可公开访问的IP地址。	**方法：**每个用户建立一个从其设备（发起主机）到SDP网关互相认证的隧道，然后再通过网关连接到云中的目标资源。 云防火墙配置变得更简单： • SDP网关对整个互联网的所有流量开放。因为它只允许通过SPA连接，所以它可以在一定程度上减轻DDoS和其他攻击。[13] • 受保护的资源位于SDP网关后面的私用IP地址上，无法

	从互联网访问。云防火墙配置为只接受来自网关IP地址的访问连接。
效果：公司网络上的所有用户和系统都可以完全访问私有云网络，违反了最小权限原则，增加了攻击面。云网络可以被扫描并且可以被攻击者利用漏洞进行攻击。服务器访问仅通过身份验证保护，而不受网络级别的保护。密钥管理可能成为开发人员的负担。合规性检查更加困难，因为所有用户都可以访问所有系统。	**效果：**因为每个用户到 SDP 网关的连接都是单独建立并经过高强度认证的，与源 IP 地址是否经过 NAT 不再相干。SDP 网关可以以细粒度的方式对每个用户实施对云资源的访问控制。组织可以定义与用户、设备和角色相关的策略。

需求：David是一名远程开发人员，他必须定期从不安全的网络（如咖啡店）访问云端系统中的多个服务器。他还需要访问总部网络上的开发资源。这些服务使用多个协议和端口（22,443,3389）。

挑战：咖啡店网络 NAT 到单个 IP 地址 54.144.131.11。

不使用 SDP	使用 SDP
方法：开放云防火墙使其面向整个互联网访问是不能接受的，甚至允许来自 54.144.131.11 的所有流量都具有太大的安全风险，因此 David 首先将 VPN 连接到办公网络，然后像访问云网络那样访问企业局域网	**方法：**David 的设备向 SDP 控制器进行身份验证，然后授予访问受 SDP 网关保护的资源的权限。David 不再需要 VPN 进入办公网络，从而提高网络性能并减少网络带宽使用成本。
效果：David 需要通过 VPN 连接到总部网络（他需要访问本地资源），所有流量都必须回到公司网络，从而增加延迟和带宽成本。该解决方案变成了上面表格中的要求，即允许企业网络上的所有用户和设备都可以完全访问云网络。	**效果：**由于流量是从 David 的设备加密到网关，因此他即使使用公共无线网络或公共互联网也没有太大风险。云防火墙的配置不必改变 – 网关对互联网开放（但受 SPA 保护） – 所以 David 无论身在何处都可以高效工作，并且安全基础架构无论位于何处都能始终如一地工作。

13 有关更多信息，请参阅防 DDoS 工作组的 SDP 研究以及 CSA 赞助的年度 SDP Hackathons。

需求：Freddy 是一位在其家里工作的开发人员，需要访问与其团队其他成员分开的私有云网络。这个环境包含敏感的，受管制的信息，所以他建立了一个 VPN 来进行访问。他还需要访问总部网络上的开发资源。

挑战：Freddy 的位置不变，但他需要持续访问云和总部资源。出于安全目的，需要安全的网络连接。但他不能在同一台机器上同时运行两个 VPN。

不使用 SDP	使用 SDP
方法：Freddy 通过他的开发机器上的不同环境访问这些资源 。他通过虚拟机进入云端网络，并通过运行在他的自己主机操作系统上的 VPN 访问总部网络	**方法：**Freddy 建立到 SDP 网关的安全连接，以访问受保护的云资源。
效果：这种方法会影响到Freddy的工作效率，因为他的一些工具和开发任务需要从同一个系统访问这两个环境。 由于 Freddy 是目前唯一访问此环境的人员，因此合规性和审计报告不成问题。但他知道，几个星期后，随着其他团队成员加入该项目，他将会面临跟踪和报告所有人的访问行为以及管理这些访问权限的问题。他还不知道他将如何启用这种访问。他应该向办公室的每个人开放云防火墙吗？ 那么远程开发人员呢？他需要管理每个人的 VPN 访问吗？	**效果：**他可以同时使用自己的VPN连接到办公室网络，与访问云资源没有冲突或问题，因为SDP连接看起来像是常规网络连接，而不是VPN。所以Freddy的工作将更高效。 Freddy 可以通过他设计的一系列策略轻松控制和报告对这些资源的访问行为。提供对新用户的访问只需编辑他的策略或编辑用户属性即可，使他能够以细粒度的方式控制访问。

总结

对于这个用例，SDP为企业提供了强大的优势：

- 无论位置如何，都可确保开发者的访问需求
- 通过服务和端口精确控制每个开发人员可以访问的服务
- 更简单的合规报告
- 更简单的安全策略配置
- 提高开发人员的生产力

用例场景：保障业务人员访问内部企业应用系统的安全

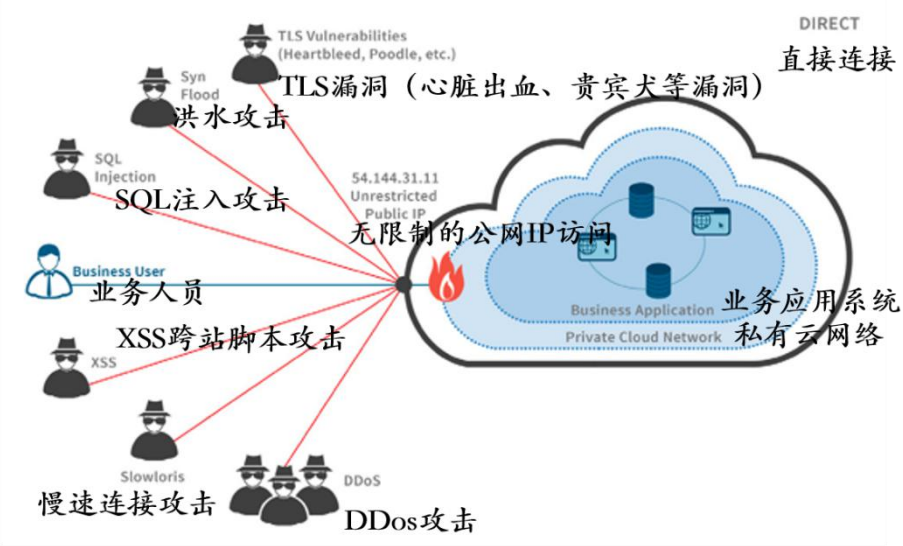
业务人员需要安全访问在IaaS环境中运行的企业应用系统，如人力资源管理系统、财务、采购、费用、供应链等。这些应用可能是供应商提供的系统，可能是内部IT开发人员开发的应用系统，也可能处于生产环境或者测试/QA环境。

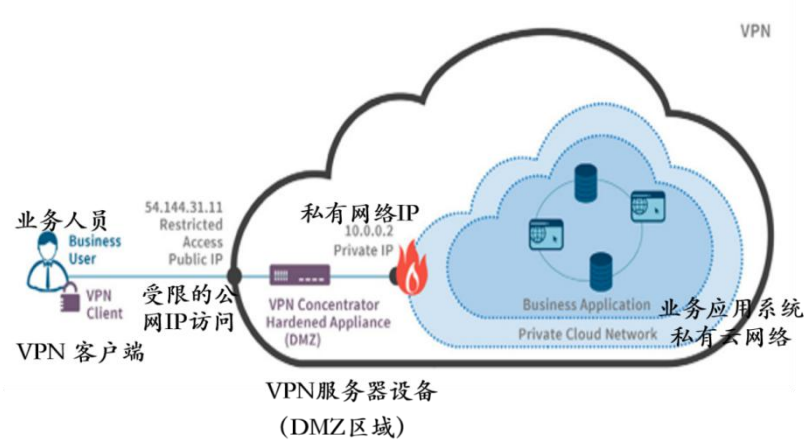
在这些情况下，业务人员通常不需要考虑网络或计算机的底层访问协议（例如SSH或RDP）。

不使用 SDP 的访问

向业务人员提供应用系统的安全远程访问有三种常见方式 ： 1）直接连接、2）VPN 和3）VDI。

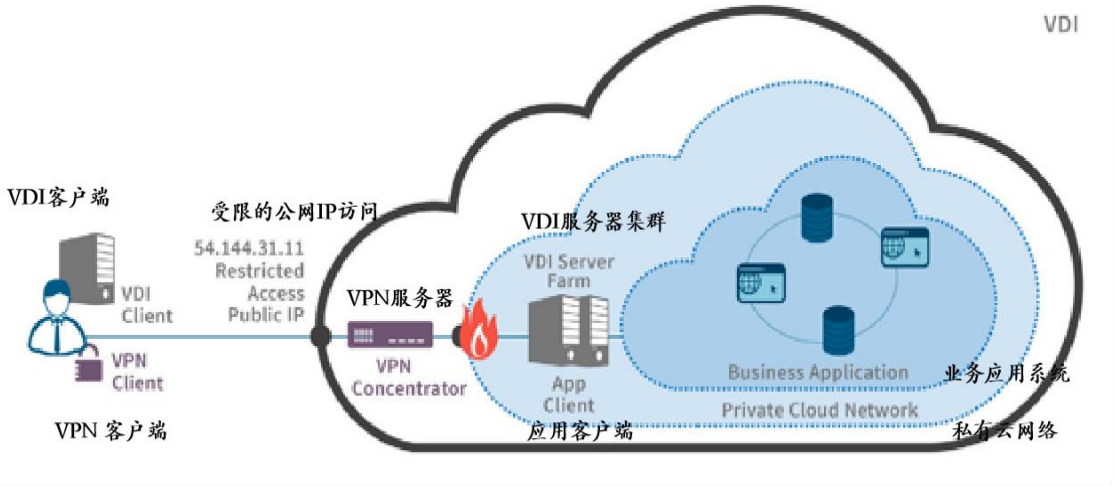
直接连接：在直接访问的情况下，应用系统通常是一个Web应用程序，配置到公共互联网环境下，不考虑访问限制。在这些情况下，应用系统会暴露于各种因素（安全威胁）下，容易受到各种形式的攻击，包括暴力破解，DDoS，XSS和任何TLS漏洞（如心脏出血漏洞Heartbleed或贵宾犬漏洞Poodle）。





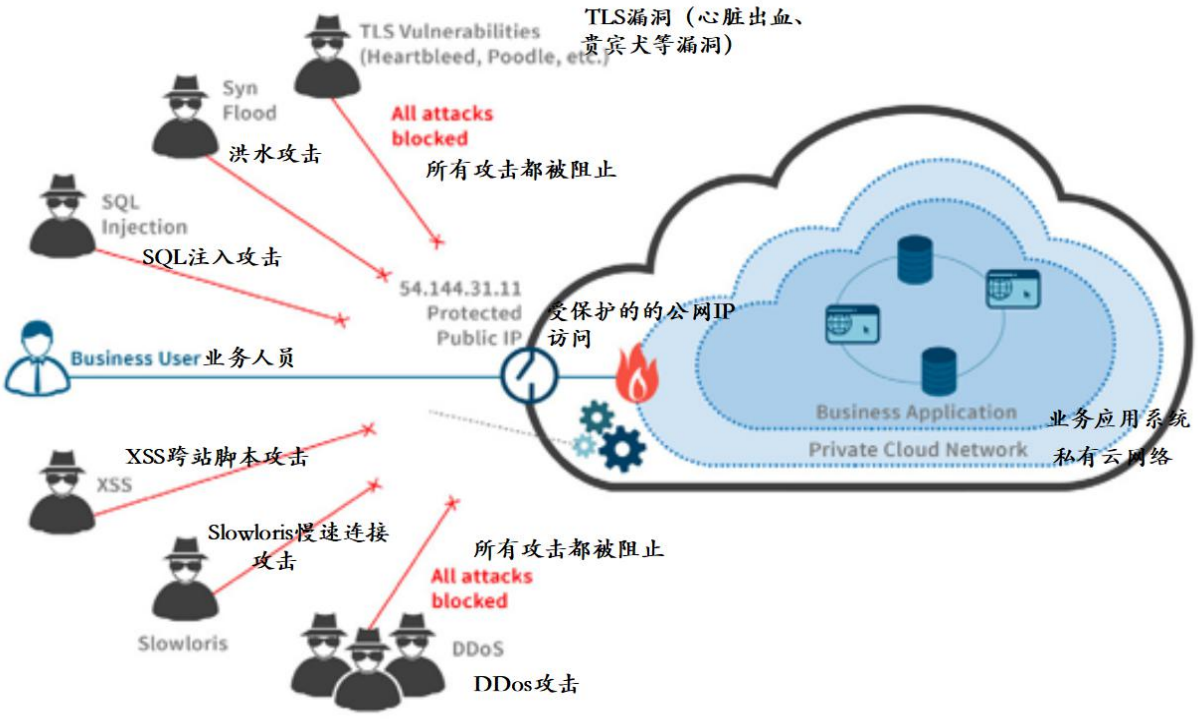
VPN：通过VPN，内网及其所有的资源都将对该业务人员的设备开放。

VDI：通过VDI，业务人员可以操作虚拟计算机（通常是Windows操作系统），这个虚拟机可以用作企业应用系统的启动平台。业务应用系统通常是一个需要“厚Windows客户端”（较多在客户端及服务器端的运算，较少的通信链接）的客户端/服务器应用程序。



使用 SDP 的访问

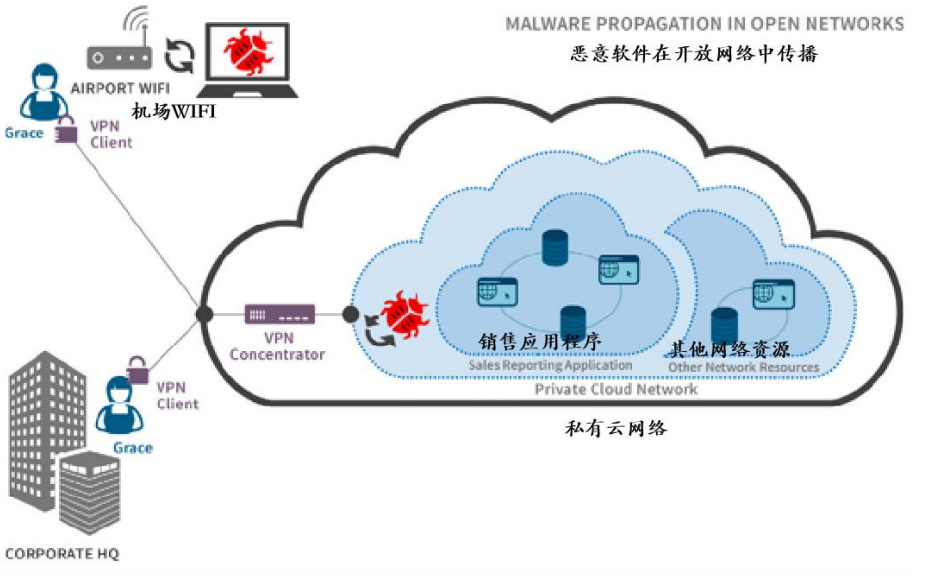
通过SDP解决方案，只有授权用户才能访问业务应用系统。实际上，未经授权的用户甚至无法访问SDP网关 – 因为它受到单包授权SPA的保护，所以对攻击者来说实际上是完全不可见。

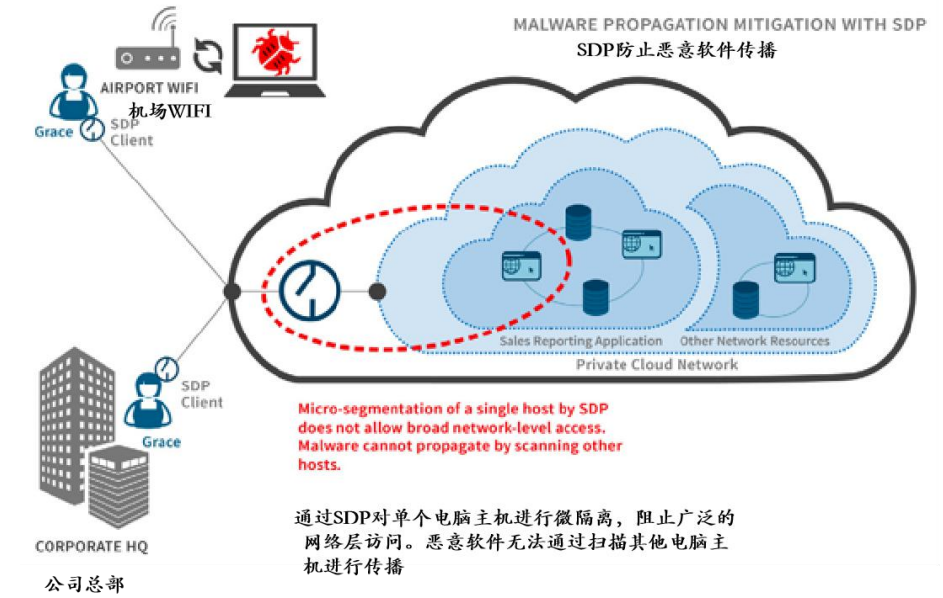


我们来看看不同的用户的访问需求，以及如何管理这种访问。

需求：Grace在公司总部的销售部门工作。她需要通过由IT团队开发的新销售报告系统访问重点客户销售报告。她经常拜访不同地方的客户，需要远程运行报告，且该应用系统托管在Amazon AWS上。

挑战：Grace 在出差期间在机场和咖啡店访问多个免费网络。过去，IT 安全部门发现了她的笔记本电脑上的恶意软件，他们担心当 Grace 通过 VPN 访问新的重点客户销售报告或返回公司总部时，恶意软件可能会传播到 AWS 基础架构中（“星期一恶意软件”）。



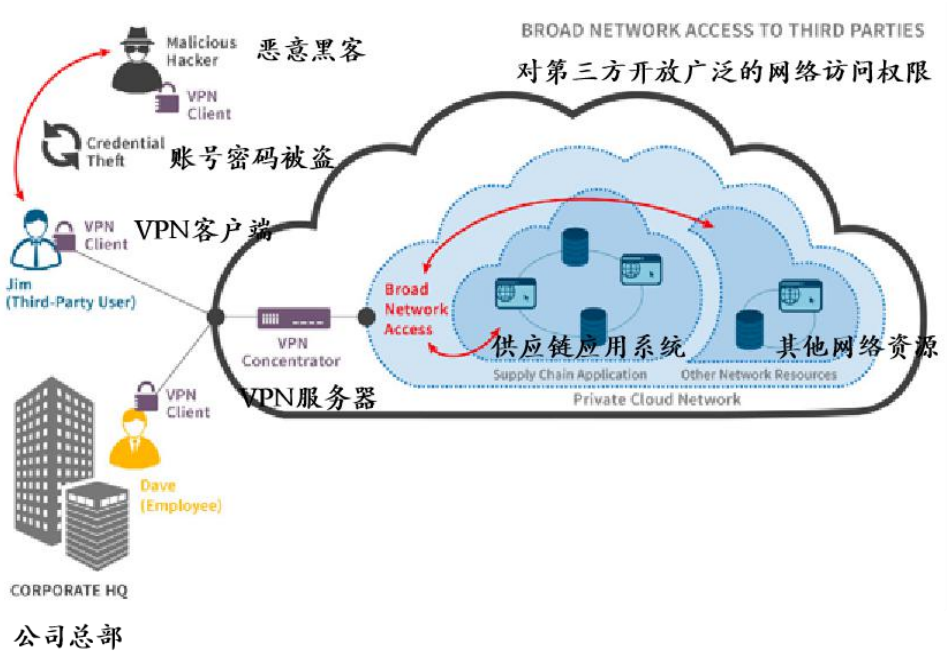


不使用 SDP	使用 SDP
方法：恶意软件不应该能够在网络内传播。因此，IT 安全人员创建了一个网络分段以隔离 AWS 上的应用服务器。	**方法：**SDP 提供的好处能够将网络隔离到单个服务器（而不是整个网络）。SDP 为 Grace 提供安全的远程访问，同时防止恶意软件通过公网访问带入[14]（例如 VPN）。
效果：使用传统网络工具创建微分段很复杂。随着应用程序数量的增长，ACL 记录的数量往往呈指数增长[15]。很快，网络管理员由于需要支持数千个 ACL 而负担过重。每个新建的 ACL 请求都需要数天才能分析和处理。生产力降低，IT 失去敏捷性，新应用的部署会变慢。	**效果：**业务人员现在可以完全访问托管在公有云网络上的企业应用系统。SDP在默认情况下提供有限制的网络访问，因此不违背最小权限访问的原则。 网络管理员能够阻止通过公网访问带入的恶意软件，不会因公司日益复杂的网络问题而负担过重。

需求：Dave负责IT部门的供应链应用系统。新的业务流程要求其供应商员工Jim在货物发运后立即在其供应链应用系统中输入货件的详细信息。

挑战：这需要授予第三方供应商的一部分人员对应用系统的访问权限，这些业务人员（例如Jim）不是公司的员工，而Dave对其安全策略及安全培训等方面的控制是有限的。

Dave 不希望授予他们进入公司内网的广泛网络访问权限（VPN），他担心如果供应商端的账号被盗，他的整个公司网络将会受到伤害。他该如何限制“爆炸半径”?



14 使用 SDP 控制东西向流量将在 v2 SDP 规范中得到实质性解决。如本文档其他地方所述，这是 IaaS 环境与内部部署相比较容易解决的问题。

15 从技术上讲，0（n ^ 2）是为了建立应用程序到应用程序的连接模型。

不使用 SDP	使用 SDP
方法：Dave 为这一个应用服务器创建一个虚拟内网 VLAN，这样就能将其与其它网络隔离。但是，供应链应用系统非常复杂，并已集成到网络中的其他几个系统中。这里存在跨 VPC 的连接和防火墙规则，以及网络层访问控制表。因此，维护复杂的网络配置非常麻烦，因为任何系统中的 IP 地址更改都可能会导致整个供应链应用程序无法运行。	**方法：**使用 SDP 的情况下，他们可以从针对单个服务器进行网络隔离中获益（而不是隔离整个网络）。远程连接不会向供应商暴露任何其他网络资源。恶意的攻击者无法进行嗅探或探索网络中的其他漏洞或者易攻陷的资源。Dave 选择使用 SDP 来为供应商人员提供安全和保密的远程接入。
效果：Dave不再向第三方供应商提供应用系统访问权限，因为从网络安全角度来看其过于复杂且存在风险。 供应链用户希望他们能更好的规划来自供应商的供应。这样做的影响是，上下游不再能够看到即将到来的发货数据，业务面临错误订单和延迟发货的风险。	**效果：**尽管 Dave 无法控制第三方供应商业务人员执行安全最佳实践和培训，但通过 SDP 他可以在发生账号失窃时限制影响范围。授予第三方访问权限变得更安全，不仅提高了供应链的效率而且同时保证业务增长。

需求：Jim每周都会准备一份业务分析报告，生成报告的是一个只能在Windows系统上运行的客户端/服务器(C/S)应用程序。所以IT部门为Jim和他的团队部署了一个VDI解决方案。Jim每次需要通过VDI登录远程桌面，然后启动报告程序。

挑战：这个（C/S）报告程序是从一个大型供应商处购买的打包的应用程序。建议的部署模式仅是“私有部署”，即供应商建议不要通过公共互联网访问应用程序的服务端，因为其并不稳定/安全。也就是说，服务器必须与客户端在同一网络内。

因此，对于远程用户，IT安全团队决定使用VDI，其中客户端和服务器始终保持在同一网络中。但是，构建和维护VDI服务器的成本非常高，并且会随着远程/出差雇员数量的增加而增加。

组织面临的挑战是如何安全地开放（C/S）应用程序的服务器部分，以便业务用户可以直接在他们自己的 Windows 笔记本电脑上运行客户端。

不使用 SDP	使用 SDP
方法： Jim 持续增加更多基础设施来支持 VDI 集群	**方法：** 使用SDP，Jim可以安全的向经过认证/授权的选定业务用户开放服务器/端口。对于其他人而言，服务器保持“不可见” Jim 选择使用 SDP 来为有需求的业务分析用户提供 C/S 应用的安全远程接入。
效果： 建立一个大型的VDI集群既增加了用于硬件的资本支出，也增加了用于维护和保养VDI服务器的运营支出。 因此，IT 部门必须削减其他重要项目的预算，而 VDI 集群正在耗尽所有的资金。	**效果：** 使用SDP方法减少了维护VDI基础架构的成本。业务人员变得更加高效，因为他们运行应用程序之前省去了日常登录远程桌面的步骤。 不久以后，VDI 集群就可以淘汰，从而为其他设施腾出 IT 预算。

总结

在这个使用场景中，SDP为为企业提供了强大的优势：

- 为远程业务用户提供安全访问企业应用的途径
- 精确控制用户可以访问的应用程序。
- 增加第三方业务集成。
- 更简单的合规报告
- 降低VDI相关基础设施成本
- 更简单的安全策略配置
- 提高业务流程的生产效率

使用场景：安全的管理面向公众的服务

当一个应用程序在云端提供服务时，系统管理员、开发人员以及其他高级用户都需要远程访问它的很多后端服务。这些服务可能包括：

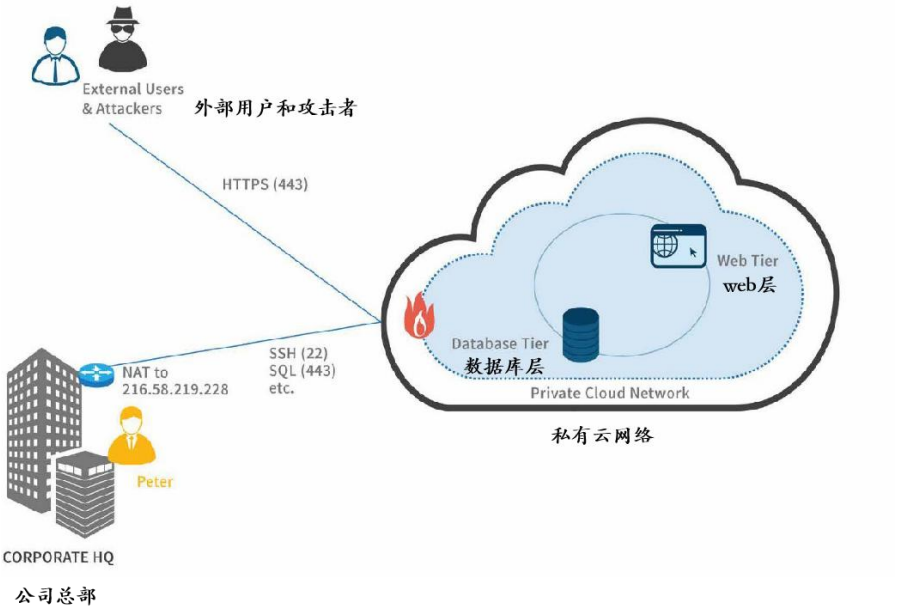
- 通过SQL接口来访问数据库层（例如SQL Navigator for Oracle, PgAdmin for Postgres等）
- 通过SSH访问服务器

• 应用程序的管理员界面（例如WordPress博客的管理界面）

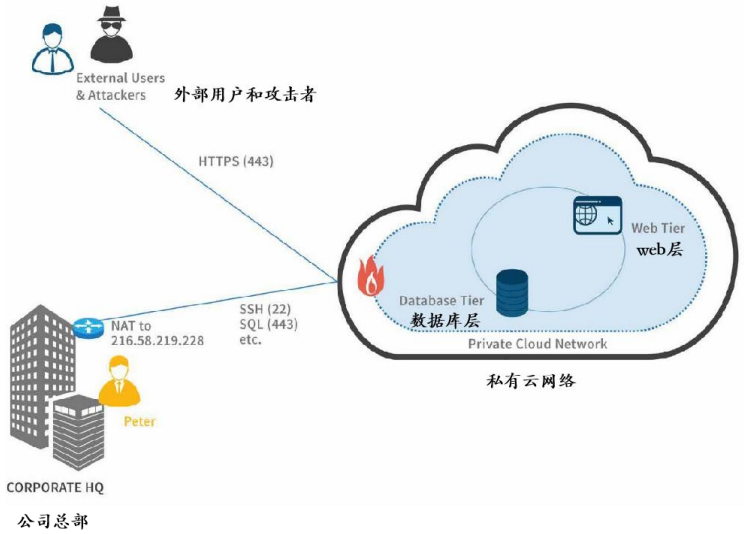
• 通过HTTPS访问数据库工具（例如PhpMyadmin for MySQL）

• 在这些案例中，在公共互联网上允许这些服务不受限制的访问是不明智的。暴露这些服务会导致暴力破解、错误配置、0day利用等攻击的几率上升。

不使用SDP时，这些后端服务需要被暴露到公共互联网，或者在云防火墙上手动维护限制某些源地址访问，但即使如此也有可能将服务暴露给许多用户。



当使用 SDP 方案时，只有那些需要公共访问的服务（如 HTTPS）才会暴露于互联网。所有其他服务都被 SDP 网关所隐藏，而且访问受到接入策略的控制，不需要接入额外的 VPN。



需求：Peter是一个财务应用系统的数据库管理员。他的公司已经将他们的基础设施转移到一个行业领先的IaaS上。Peter负责调整数据库SQL查询以改善应用性能。所以，他通过防火墙开放了数据库端口并且使用SQL浏览工具连接数据库来完成优化计划。

挑战：现在数据库端口对外开放，恶意的自动机器人会迅速发现开放端口，并且尝试暴力破解管理员密码。他们有可能在几天内通过字典破解口令并获得公司的重要财务数据，也可能发现默认密码，或者利用已知的数据库平台漏洞（未被修复）进行攻击。

不使用 SDP	使用 SDP
方法：Peter 为云端网络设立 VPN	**方法：**使用 SDP，Peter 可以让端口对其他地方保持关闭。恶意黑客不会意识到数据库服务正在运行。数据库端口只能通过授权和认证后从 Peter 的设备访问。
效果：Peter 不得不在另一个不是他们原有数据中心私有网络上设立 VPN。他不得不在他的设备上配置两个不同的 VPN 并且每次访问网络资源时都需要选择连接到哪个 VPN。Peter 是一位 SQL 开发人员，并不是 IT 管理员，他不完全了解 VPN 配置。他并不喜欢会拖慢他的 VPN。	**效果：**Peter 不需要切换不同配置，也不需要配置网络安全策略就可以安全地访问数据库。

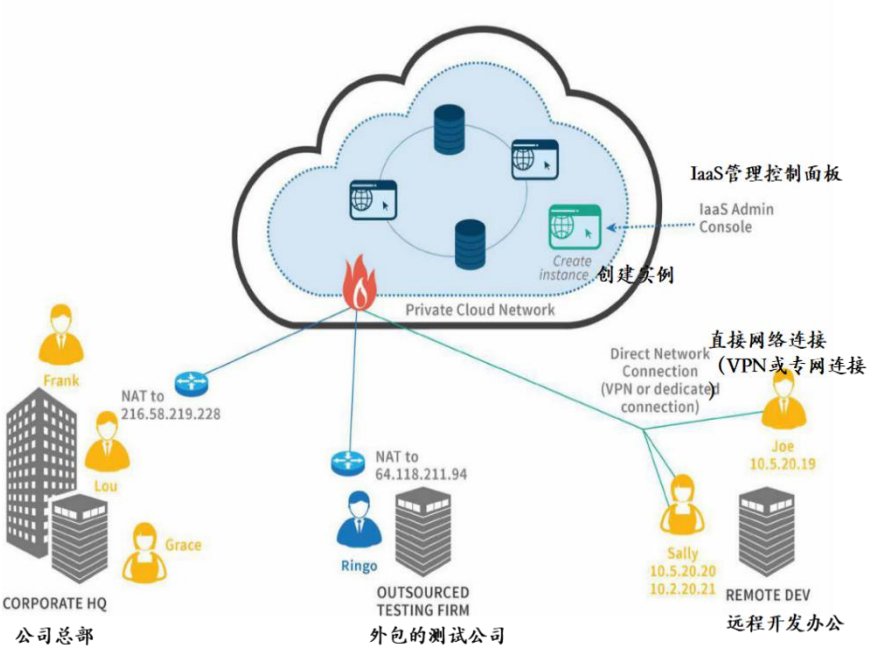
使用场景：当新服务实例创建时更新用户访问权限

云环境本质上是动态的，实际上，大多数企业利用IaaS的这一特点来提高其开发速度和敏捷性。特别是在IaaS环境中，创建和销毁服务器实例非常简单，所以企业可以频繁地(如果不是连续的)创建和销毁服务器实例[16]。

如下图所示，一个人使用IaaS控制台（或者调用API接口的系统）创建一个新的服务器实例。所需的网络更改取决于其位置，云连接类型和需求，并在以下页面的表中讨论。

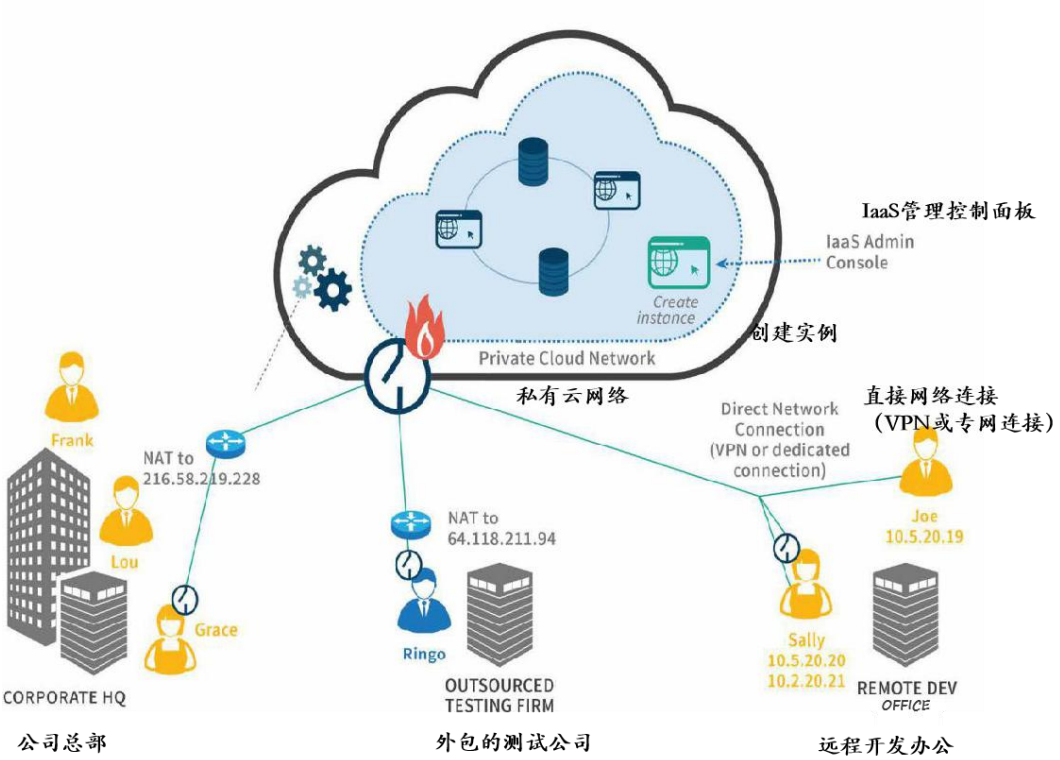
*16 备注 1：*对于这个用例，我们所描述的是由 IaaS 管理控制台手动启动的服务器实例，或者从开发或部署脚本通过 IaaS API 启动的服务器实例。此处不讨论 IaaS 基础架构自动扩展的服务器实例（例如，基于 CPU 负载阈值）。访问这些示例已在已有用例的覆盖范围内，因为它们实际上是纯粹用于负载平衡和扩展目的的已运行资源的克隆。对它们的访问将由与控制池中服务器核心集相同的访问策略来管理，本文档中的其他使用场景将对此进行介绍。

*备注 2：*由于通过将实例分配给云防火墙组来授予网络访问权限，因此在实例终止时无需执行任何操作即可移除访问权限。云防火墙并不授予特定服务器地址访问权限，因此也不存在由于 IP 地址重用导致错误继承访问权限。



使用 SDP 接入

云服务器全部受 SDP 系统保护，网关充当私有云网络的唯一网络入口点。新的服务器实例具有元数据（标签）。



需求：Grace启动一个实例并且只需要SSH访问（端口22）

挑战：Grace 位于一个通过 NAT 地址访问云的网络

不使用 SDP	使用 SDP
方法：这个实例必须分配一个公网 IP 地址，并且云防火墙必须授予 NAT 地址 216.58.219.228 或者整个互联网（0.0.0.0）对实例的完全访问。	**方法：**访问新的服务器实例必须通过SDP网关，SDP网关可公开访问并且受SPA的保护。 SDP 系统检测到这个新的服务器实例，并根据其元数据（标签）自动授予 Grace 对端口 22 的访问权限。
效果：虽然云防火墙不需要立即进行更改，但对任何用户或在公司网络中的设备来说，访问此服务器都是不受限的。这代表着重大的安全风险。由于 IP 地址是 NAT 的，因此不可能将网络访问权限限制为单个用户或单个端口。因此，安全团队要求通过单独的密钥来控制对这些实例的 SSH 访问。管理和跟踪这些密钥文件是一件令人头疼的事情，并且对开发者来说也存在安全风险。	**效果：**Grace 会自动获得生产所需的最低访问权限，而无需任何手动重新配置或 IT 部门参与操作。

需求：Sally 启动一个实例，并需要从她的所有设备上访问 HTTPS，RDP 和 MySQL 端口。

挑战：Sally 通过她直连到云的办公室网络来访问云端——这些资源就好像在本地网络一样。

不使用 SDP	使用 SDP
方法：如果目的是只允许 Sally 访问，云防火墙则必须更新以允许 Sally 当前 IP 地址访问这个特定的服务器实例。如果目标是不产生任何延迟的情况下授予 Sally 访问权限，则必须将实例配置为允许所有本地网络上的设备访问新服务器实例的所有端口。	**方法：**SDP 系统检测到这个新的服务器实例，并根据其元数据（标签）自动授予 Sally 适当的端口访问权限。
效果：要求对云防火墙进行持续更改是大多数企业不愿意承担的运营负担，因为这会增加时间和成本。大多数企业授予开放式网络访问权限，而仅依靠认证进行控制。	**效果：**Sally 会自动获得必要的最低访问权限，无需任何手动重新配置或 IT 部门参与操作。

需求：Ringo 作为一个外包的测试人员，需要 Web 访问（443 端口）才能测试这个新实例。

挑战：Ringo 的办公室网络被 NAT 转换为一个不会改变的单一公共 IP 地址。由于 Ringo 在另一个时区，他有时必须在家工作实时与团队协作。

不使用 SDP	使用 SDP
方法：云防火墙必须允许 Ringo 从特定的公共 IP 地址访问。通过特定服务器分配给此云防火墙组，可以将其限制为特定的服务器实例。防火墙还必须允许 Ringo 从家用 IP 地址（定期更改）访问。	**方法：**SDP 系统检测到这个新的服务器实例，并根据其元数据（标签）自动授予 Ringo 对端口 443 的访问权限。
效果：用户启动的这个新服务器实例必须将其分配给允许从 Ringo 的 NAT 地址访问的安全组。所有使用 Ringo 的家用网络的用户也都可以通过端口 443 访问此实例。 每次 Ringo 的家用 IP 地址变化时，他必须向 IT 部门申请更新云防火墙更新。这可能需要长达 24 小时，并影响整个团队的生产效率。	**效果：**Ringo 自动获得必要的最低访问权限，无需任何手动重新配置或 IT 部门介入操作。 因为访问权限是授予作为用户的 Ringo，所以不会绑定到他的 IP 地址。这意味着 Ringo 能立即工作，并且无论他在哪里工作，都具有相同的安全访问权限。

总结

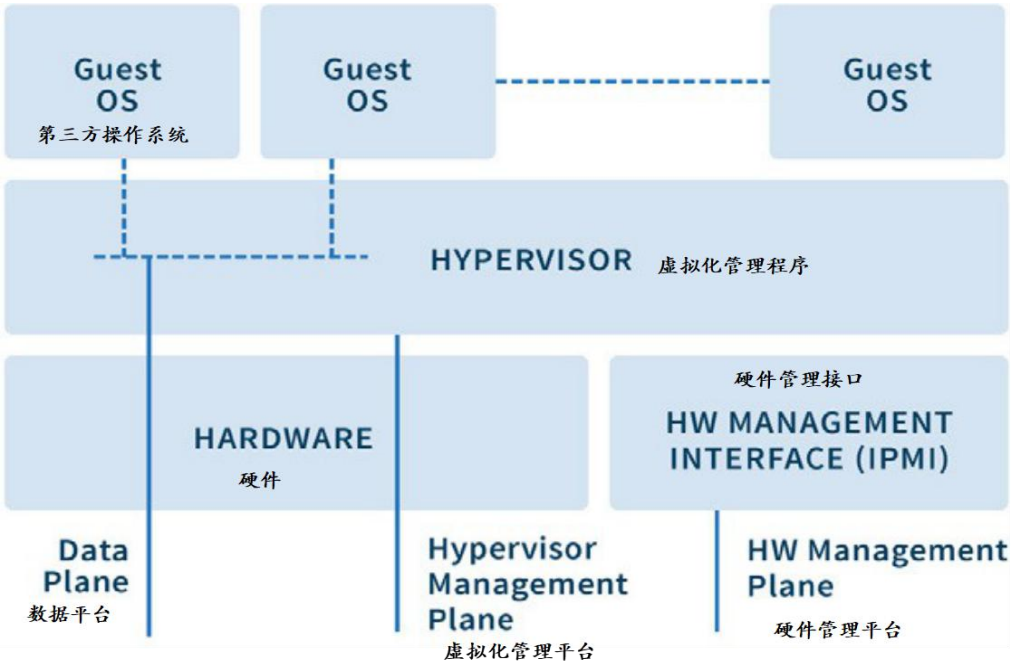
在这个使用场景中，SDP 为企业提供了强大的优势：

- 自动检测新服务器实例，并根据实例元数据自动分配用户访问权限
- 无论位置如何，都可确保开发者安全访问
- 完全的高效生产-不用等待网络访问控制更改的延迟
- 由策略驱动的访问控制，而不是基于云防火墙配置
- 减少 IT 运营工作量和成本

使用场景：对于服务提供商的硬件管理平台访问

尽管我们提出了一个无限可扩展且完全虚拟化的平台概念，但它实际上是运行在某个层面上的网络和计算硬件上。当然，这些硬件必须由服务提供商管理，无论他们是提供私有云平台的内部IT部门、服务器托管商或共址提供商、还是商业IaaS供应商。

下面的逻辑图说明了要管理的网络访问路径：



Data Plane数据平台是用于访问第三方操作系统实例的标准网络。我们在整个文档中的讨论都集中在这个网络上。

Hardware Management Plane 硬件管理平台是内置于许多硬件平台的网络，通常基于称为IPMI（智能平台管理接口）的英特尔规范构建。这可以通常称为底板管理控制器，或者非正式地称为“熄灯网络”。大多数服务器制造商通过具有其自身物理网络连接的嵌入式硬件卡，比较著名的如Dell服务器的DRAC）和HP的ILO for ILO都支持此功能。[17]

但是，这些IPMI服务因许多漏洞而众所周知，包括不修改的默认账号密码以及无法抵御简单攻击。

Hypervisor Management Plane 虚拟化管理平台是管理员通过GUI控制台或API访问读虚拟化进行管理。虽然虚拟机管理程序通常具有比IPMI系统更好的访问控制，但它们仍应配置为仅通过单独的网卡，在物理上独立的网络或虚拟局域网VLAN上进行访问，并受SDP保护。下面的讨论虽然侧重于IPMI，但也适用于虚拟化管理平台。

安全管理员访问各种端口上的IPMI网络接口。此访问必须具有强身份验证，并且出于安全性和

合规性报告目的而被记录。理想情况下，管理员需要全天候访问到这个网络。但是，这种按需访问通常具有时间敏感性，因为IT可能会响应服务器中断。同时应该有业务流程 – 例如请求和批准 – 来控制访问，并且使用闭环机制确保一旦不再需要访问就被删除。

IPMI 有许多已知的弱点，从可利用的漏洞到有限的管理功能。IPMI 需要单独的网络，无论是物理上分离还是通过 VLAN。

不使用 SDP	使用 SDP
方法：强烈建议不要使用默认方法，即依赖IPMI系统中的默认账号密码，并将访问IPMI网络的权限仅限于授权用户。 较好的方法虽然会产生很大的开销，但却是单独管理每个服务器的访问账号。 更好的方法是将 IPMI 身份验证与企业的 LDAP / RADIUS 系统联通。	**方法：**使用SDP，IPMI服务器可以简单地放置在受SDP网关保护的网段上。也就是说，除非SDP策略允许，否则任何网络流量都无法到达任何IPMI接口。 SDP 系统可以利用各种用户和系统属性 – 例如组成员资格、设备配置文件、位置或时间。
效果：这些解决方案都不够完善 – 保留IPMI系统的默认账号密码是在自讨苦吃 – 恶意攻击者很容易获得对网络的访问权限，例如通过错误的配置。 在每个服务器的基础上配置用户访问账号可以提供更好的安全性，但在任何规模的环境中都是行不通的 ，因为需要较多的手动工作和账号跟踪就来实现这一点。 利用组织的 LDAP / RADIUS 系统进行身份验证要好得多，但仍然要求任何可能在某些时候需要 IPMI 访问权限的用户始终可以完全访问 IPMI 网络。通过防火墙规则控制网络访问在技术上是可行的，但会引入过多的进程开销，并会延迟对服务器的管理员访问。	**效果：**用户对 IPMI 接口的访问可以由策略驱动，并且可以根据即时的“按需授权”策略轻松动态调整。例如，SDP 系统可以在允许用户访问之前，验证工单系统中是否存在特定用户和特定服务器的需求。这很容易支持对敏感授权的请求、批准等流程。 并且，SDP系统可以基于位置实施访问规则，例如仅允许从本地公司网络访问，以及阻止来自远程位置的任何访问。 SDP 还可以与组织的 IAM 系统集成，以实施强身份验证。

总结：

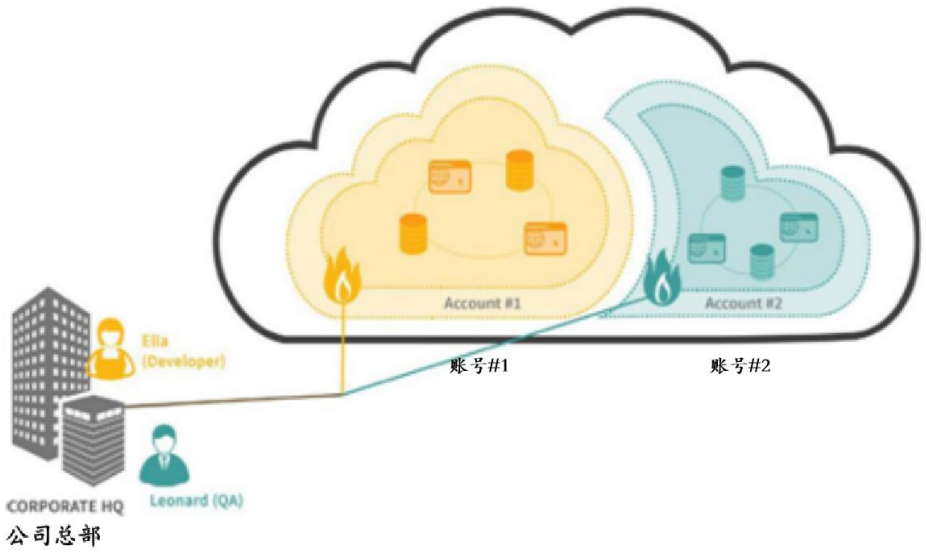
对于此场景，SDP 提供以下好处：

- 安全可控地访问高风险和易受攻击的 IPMI 网络
- 细粒度控制哪些用户可以访问这些系统，以及何时访问
- 通过简单的、以用户为中心的策略进行控制
- 通过与 IAM 集成实施强身份验证
- 在保障安全性或合规性的情况下，实现紧急服务器中断情况的快速访问
- 全面详细的日志，了解谁可以访问哪些系统（以及何时）以实现合规性
- 随着数据中心的增长和动态而扩展的解决方案

17 参考 https://en.wikipedia.org/wiki/Intelligent_Platform_Management_Interface 来了解更多信息。
18 参考 https://community.rapid7.com/community/metasploit/blog/2013/07/02/a-penetration-testers-guide-to-ipmi

使用场景：通过多企业账号控制访问

在此场景中，一个企业在IaaS上具有多个不同的帐户。出于安全性或合规性原因，这可能是故意的，或者由于不同的组独立设置帐户而偶然发生的的。下图显示了两个帐户的情况，但企业通常还有更多帐户，例如，如果他们采用了“一系统一个帐户”策略，则会有更多帐户。



从企业到云的连接（如上图中的墨绿色部分所示）可以通过共享云直连（实际上是专用站点到云的 VPN）或通过 Internet 进行连接。在任何一种情况下，都有相同的挑战，如上图所示。

要求：针对不同用户设置不同的访问权限，并且在该用户的所有帐号上保持一致。

挑战：虽然有多个单独的帐户可能在计费或访问云控制台，但它们不共享云防火墙。

不使用 SDP	使用 SDP
方法：如果企业试图严格控制用户对资源的访问，上述用例中提到的问题仍然存在，并且实际上随着帐户数量越来越严重。 他们可能会尝试通过使用云 API 来更新安全组策略以自动执行一些操作，但最终仍然面临着以 IP 地址为中心的云防火墙模型被应用到以用户为中心的安全控制的问题。	**方法：**通过在每个云防火墙前部署 SDP 网关，企业可以立即简化并提高其安全性。每个帐户的云防火墙可以简化为一个简单的规则 - 仅允许从 SDP 网关到受保护服务的连接。
效果：结果是企业实际上向网络上的所有用户开放所有云资源，只是依赖身份验证来保护它们。正如我们上面所述，这不是一个强有效的安全或合规的方案。	**效果：**无论使用的云帐户的数量或类型如何，都可以始终如一地应用 SDP 策略。这些策略提供完整的合规性跟踪，并始终与企业的 IAM 系统集成。

总结：

对于此例，SDP体现出明显的优势：

- 在不会牺牲安全性前提下，允许使用多个云提供商的账号
- 简化云防火墙规则相关的手动管理工作
- 始终对所有用户群实施所有帐户的访问策略

增强 SDP 规范的建议

在进行这项研究的整个过程中，我们有意地从一个从业者的角度来看SDP，查看实际可行的用例，这些案例通常是由可行的SDP实现和体系结构所支持的。因为这些很有必要，所以这些用例和需求超出了当前（V1）SDP规范。

在我们的辩论、对话和写作中，我们会记录那些我们认识到的一个完整的SDP实现所需的领域（如SDP供应商产品已经解决的问题所证明的）。

这些话题中的许多超出了IaaS，它们是整个SDP规范的必要一部分，然而我们决定它们不在本文档的范围内，而是放到当前正在进行的V2规范中。我们期待着接下来的创作，就以下主题进行讨论：

- 网络权限的策略模型
- IAM 集成
- 目录属性和 SAML 验证作为策略模型的一部分
- 逐步认证触发器
- 高可用性和负载均衡方法
- 除了 HTTP 外的网络协议支持（如 SSH、UDP）
- 深度包检测和会话代理
- 增量部署到现在的企业环境
- 实例元数据和云环境自动探测
- SDP 成本节约/ROI 模型
- 探讨服务器与服务器之间的流量微隔离（东西向流量）
- 遗留的风险和潜在的 SDP 系统威胁（例如，中间人攻击、控制器或网关攻击）

混合云以及多云的环境

在可预见的未来中，多数企业都拥有一个复杂的IT环境。安全团队与其将此看成是一个需要消除的问题，不如去拥抱这种丰富的场景，因为这是商业与生俱来的复杂性。不同行业的商业有不同需求，我们可以非常负责任地预测，世上没有“放之四海而皆准”的IT架构可以适用所有的企业。

这表明安全团队需要寻找正确类型的工具和技术来为不同的环境提供持续的安全保障。虽然总是有不少平台强关联的工具，例如系统管理、自动化、或者是终端管理，但我们相信从安全的角度来说，企业在不同平台上建立统一的以用户为中心的策略和流程是非常关键的。

例如，企业肯定非常希望有一个统一的平台，他们可以定义并且执行“谁可以访问什么系统”的策略和流程。这个平台必须是统一管理内网部署的、多地部署的、物理的、虚拟的、私有云的、公有云的资源。如果不是这样，企业将面临增加的复杂性、风险、以及运维成本。

我们相信 SDP，因为它以用户为中心、平台无关、网络层访问控制强制执行的能力，是今天企业解决复杂环境下安全问题的正确选择。

替代计算模型和 SDP

我们看到“无服务器”计算模型的可用性和采用率正在稳步提高，云提供商在其功能线中添加了新的‘PaaS’。这些是对传统（如关系数据库或消息队列）的“as a service”转变到更新颖的“function as a service”（例如AWS Lambda、Azure Functions、以及 Google Cloud Functions），以及其他许多新的以物联网为中心的业务。

所有这些共同点是它们不向客户公开传统操作系统，这意味着要解决的网络访问控制问题可能与IaaS平台相关的问题不同。

在某些情况下，这些服务完全符合我们在此讨论的IaaS场景。例如，作为服务的关系数据库恰好是受SDP保护的服务类型。实际上，许多IaaS提供商使用相同的网络访问模型来控制对其IaaS实例的关系实例的访问，因此我们在此描述的SDP方法是完全相关的。

在其他情况下，其中一些服务使用其他安全模型。例如，“function as a service ”通常可以通过公开暴露的URL或通过某种API网关访问。由于客户端到网关到服务器的模型没有任何意义，今天可能与SDP方法不兼容。我们相信这些模型将会像SDP一样发展，并且这将成为未来一个有趣的领域。

无论如何，如果您的企业正在使用（或考虑）其中一些替代计算模型，请确保您和您的安全团队与开发人员进行互动，以了解该工具的安全模型，以及如何与您的安全架构向适应。

容器和 SDP

容器是另外一个正在快速发展的趋势，许多企业采用它们作为基础技术，实现高速的DevOps方案/周期。容器带给他们一些有趣的新的安全和访问挑战。对于不同的容器和集群技术，当然有不同的网络访问模型，但为了简化起见，它们映射到以下方面：

- 每个 pod 群集（单个 OS 进程中的一组容器）获取一个由其容器共享的公共 IP（Kubernetes 模型）

- 每个容器都有一个私有 IP，它被 NAT 连接到 pod 群集的公共 IP（Docker 模型）。

在这两种情况下，SDP都可以有效地应用。pod群集和它们的容器可以放在SDP网关后面，SDP制定策略来控制用户对服务的访问。受保护的服务对应于容器内动态解析的IP地址或元数据，就像IaaS环境一样。从端口到容器的任何特定于pod群集的映射都可以在SPD网关后面工作，添加SDP没有任何影响。

当然，还有其他方法可以在容器内联网，因此请仔细查看您的团队使用的工具。但总的来说，上面列出的主流方法与SDP兼容，实际上可以很好地与SDP配合使用。这是另一个未来研究和验证的领域。

结论与下一步计划

无论你是一个企业、一个服务提供者、还是一个独立的实践者，我们都希望这项研究能够给您带来帮助。该文档将提高您对与IaaS环境相关的特定网络访问所面临的挑战，并通过软件定义边界SDP来帮助您解决这些问题。

我们希望您能够不仅仅将IaaS资源视为内部网络的扩展。拥抱云有很多好处，但往往需要很多改变才能充分利用。我们希望这篇研究能帮助您对云有不同的看法，并且改变用户访问这些资源的方式，使其更安全、更灵活、更高效。

我们相信SDP在安全方面是一个重要的进步——这是第一次使动态的、以身份为中心的安全性被应用在网络层上，并且我们热衷于看到它更广泛地被企业所接受，以满足当今的安全和业务需求。正如Gartner所说的那样：

“连接复杂性使得旧的安全体系不可持续，这需要一种新的方法来满足数字业务对复杂性、大流量和灵活性的需求，同时避免从旧模型中继承漏洞。”[19]

当然，SDP并不能解决所有的安全问题——有很多信息安全问题并不在SDP的范围内，也有可能会从特定产品中产生残余风险，或者由企业实施的细节产生。

但是总的来说，软件定义边界作为一种新的方法，不仅适用于当前的IaaS环境，而且正在重塑下一代网络安全解决方案。

19 Gartner：《迎接新时代：隔离互联网污染环境与你的网络服务》，2016 年 9 月 30 日。