软件定义边界

架构指南

致谢

云安全联盟（CSA）对所有为制定本指南做出贡献和提供支持的人员表示感谢。

主要作者

Jason Garbis

Juanita Koilpillai

贡献者

Junaid Islam

Preeta Raman

Nya Murray

Michael Roza

Aaron Palermo

云安全联盟员工

Shamun Mahmud

中文翻译版说明

由中国云安全联盟(C-CSA)秘书处组织 CSA 大中华区 SDP 工作组专家对《SDP 架构指南》(SDP_Architecture_Guide)进行翻译。

参与本文档翻译的专家（排名不分先后）：

组长：陈本峰（云深互联）

组员：程长高（安全狗）、靳明星（易安联）、李钠（奇安信）、吴涛（华云数据）、余强（中宇万通）、袁初成（缔安科技）、刘德林、刘洪森、孙刚、王贵宗、杨洋、姚凯

关于 CSA 大中华区 SDP 工作组：

随着云计算和移动互联网的发展，传统的基于边界防御的企业安全模型已经无法适应需求，取而代之是 Software Defined Perimeter（软件定义边界，即 SDP）安全模型。目前，SDP 已经在国外逐渐被普遍采用，为了推动 SDP 在中国企业的应用，并根据本土市场需求制定出更适应中国市场的 SDP 实践指南，在中国云安全联盟的支持下，CSA 大中华区成立 SDP 工作组。工作组于 2019 年 3 月成立，首批参与单位有：阿里云、腾讯云、京东云、奇安信、深信服、绿盟科技、UCloud、顺丰科技、天融信、云深互联、中宇万通、华云数据、三未信安、上元信安、安全狗、易安联、联软科技、上海云盾、缔盟云、缔安科技等三十多家单位。

关于SDP工作组更多的介绍，请点击中国云安全联盟官网 https://www.c-csa.cn/ruanjiandingyibianjieSDP.html 查看，联盟联系邮箱：info@c-csa.cn。

序言

软件定义边界 Software Defined Perimeter (SDP) 是一种具有创新性的网络安全解决方案，这种解决方案又称零信任网络 Zero Trust Network (ZTN)。

SDP 或 ZTN 是基于云安全联盟 CSA 提出的理念，用安全隐身衣取代安全防弹衣保护目标，使攻击者在网络空间中看不到攻击目标而无法攻击，从而使企业或服务商的资源受到保护。

SDP 的灵感来源于中央情报局情报社区和美国国防部高度安全网络设计，因此 CSA 聘请了 CIA 原 CTO 为联盟 SDP 研究工作组组长。ZTN 灵感的最早发明者与实践者是美国微软公司，2007 年由比尔盖茨在 RSA 大会发布的微软 Anywhere Access 安全战略就是 ZTN 的实现，微软通过这项技术使公司员工甚至 Windows 使用者可以在互联网直接访问公司内网，摈弃了传统的网络边界、VPN、Firewall。

本白皮书是 CSA 贡献给业界的又一篇重磅白皮书，它是 SDP 规范之后的设计指南与参考架构，适用于企业网络环境、IaaS 云环境、IoT 车联网环境、BYOD 移动互联网环境等，不仅对 SDP 的优势与价值做了阐述，还给出了具体技术设计指导。

我代表 CSA 对大中华区参与此项翻译工作的专家们表示由衷的感谢，特别是工作组组长陈本峰投入的大量精力，及 CSA 志愿工作者们的支持。

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

目录

介绍

SDP 方案结合了技术和架构组件，可以比传统的安全工具更高效、更有效地保护网络应用程序和基础架构。

当今的网络安全体系结构、工具和平台无法应对当前安全威胁带来的挑战。无论您是在阅读主流媒体的头条新闻，还是作为网络防御者进行日常工作，或者您是安全供应商，这些潜在安全威胁都可能会影响到您。各种来源的持续攻击会影响商业企业、政府组织、关键基础设施等。

现在是时候让我们信息安全行业拥抱创新的网络安全工具，即软件定义边界（SDP）技术，将其应用于所有的网络层。SDP 方案结合了技术和架构组件，已经证明可以比传统的安全工具更好地保护网络应用程序和基础架构。由云安全联盟 CSA 于 2014 年 4 月发布的“SDP 规范 1.0”概述了 SDP 技术的基础知识：

“SDP 背后的原理并非全新。美国国防部（DoD）和美国情报体系（IC）内的多个组织在网络访问之前已经实施了基于认证和授权的类似网络架构。通常用于机密或高端网络（由国防部定义），每台服务器隐藏在远程访问网关设备后面，用户必须先通过该设备身份验证，才能查看授权服务并进行访问。SDP 利用分类网络中使用的逻辑模型，并将该模型纳入标准工作流程中。在获得对受保护服务器的网络访问之前，SDP 要求端点进行身份验证并首先获得授权。然后在请求系统和应用程序基础架构之间实时创建加密连接。[14]”

14 https://downloads.cloudsecurityalliance.org/initiatives/sdp/SDP_Specification_1.0.pdf

目的

作为一个安全从业者和解决方案提供商组成的组织，我们对信息安全和网络安全充满热情。我们相信 SDP 是一个重要的创新解决方案，可以应对我们所有人面临的安全威胁。

自“SDP 规范 1.0”发布以来，我们作为一个由软件供应商、系统、安全架构师和企业组成的工作组，已经构建并部署了许多符合这些准则的系统。同时，我们了解了很多关于 SDP 实现的知识-特别是在缺乏原始规范的领域。

通过本指南，我们将帮助企业和从业人员获取有关 SDP 的信息；展示其可提供的经济和技术效益；并帮助用户在其组织中成功实施 SDP。如果实现以下目标，我们将认为此文档是成功的:

- 提高 SDP 的市场认知度、可信度和企业采用率
- 提高人们对 SDP 在不同环境中的应用的理解
- 提升企业使用 SDP 解决问题的动机
- 使用本文档向内部业务相关者介绍 SDP
- 企业根据本白皮书中的体系结构建议成功部署 SDP 解决方案。

受众目标

本文中的信息将使考虑或正在组织机构中实施 SDP 项目的安全性、体系结构和技术网络团队受益。

主要受众包括从事信息安全、企业架构和安全合规角色的专业人员。这些人员主要负责 SDP 解决方案的评估、设计、部署和运营。

此外，作为解决方案提供商、服务提供商和技术供应商的人员也将从本文提供的信息中获益。

概述

软件定义边界（SDP）简介

SDP 旨在利用基于标准且已验证的组件，如数据加密;、远程认证（主机对远程访问进行身份验证）、传输层安全（TLS，一种加密验证客户端信息的方法）、安全断言标记语言（SAML），它依赖于加密和数字签名来保护特定的访问及通过 X.509 证书公钥验证访问。将这些技术和其它基于标准的技术结合起来，确保 SDP 与企业现有安全系统可以集成。

自云安全联盟（CSA）首次发布软件定义边界（SDP）规范以来，CSA 已经看到了 SDP 无论在知名度还是在企业的 SDP 创新应用方面都取得了巨大的增长。虽然传统的网络安全方法在所有行业中似乎都让 IT 和安全专业人员感到身心疲惫，但 SDP 技术使用和兴趣却在不断增加，例如：

- 五个 SDP 工作组在其重点领域取得了重大进展，包括用于 IaaS 的 SDP、防 DDoS 攻击和汽车安全通信。[14]
- 已经有多个供应商处提供多种商业 SDP 产品，并已在多个企业中被使用。
- 针对 SDP 的防 DDoS 用例实施了开源（参考 [15]）。
- 已举办四个针对 SDP 的黑客松，并且攻破成功率保持为零。
- 行业分析师报告已开始将 SDP 纳入研究和演示。

14 SDP-for-IaaS: https://cloudsecurityalliance.org/download/sdp-for-iaas/
Anti-DDoS: http://www.waverleylabs.com/open-source-sdp/
Software-Defined Perimeter Working Group Initiatives: https://cloudsecurityalliance.org/ group/software-defined-perimeter/#_initiatives

15 http://www.waverleylabs.com/open-source-sdp/

SDP 安全优势

- SDP 通过最小化攻击面来降低安全风险。
- SDP 通过分离访问控制和数据信道来保护关键资产和基础架构，使其中的每一个都看起来是“黑”（不可见）的，从而阻止潜在的基于网络的攻击。
- SDP 提供了一个集成的安全体系结构，这个体系结构是现有安全产品（如 NAC 或反恶意软件）难以实现的。SDP 集成了以下独立的架构元素:
  - » 用户感知的应用程序
  - » 客户端感知的设备
  - » 网络感知的防火墙/网关
- SDP 提供了基于连接的安全架构而不是基于 IP 的替代方案，因为当今 IP 环境的爆炸式增长和云环境中的边界缺失使得基于 IP 的安全性变得脆弱。
- SDP 允许根据预先审查谁可以连接（从哪些设备、哪些服务、基础设施和其他参数）来控制所有连接。

SDP 商业优势

SDP 提供了许多业务优势，我们在这里概述这些优势以供您快速参考。我们期待与 SDP 社区合作，在未来的出版物中对这些益处进行深入的定性和定量检验。

业务领域	实施 SDP 的优势
节省成本及人力	使用 SDP 替换传统网络安全组件可降低采购和支持成本。 使用 SDP 部署并实施安全策略可降低操作复杂性，并减少对传统安全工具的依赖。 SDP 还可以通过减少或替换 MPLS 和租用线路利用率来降低成本，因为组织机构可以减少或消除对专用主干网的使用。 SDP 可以为组织机构带来效率和简便性，最终有助于减少人力需求。
提高 IT 运维的灵活性	IT 流程可能会拖累业务流程。相比之下，SDP 的实现可以由 IT 或 IAM 事件自动驱动。这些优势加快了 IT 的速度，使其更快地响应业务和安全需求。
GRC 好处	与传统方法相比，SDP 降低了风险。 SDP 可以抑制威胁并减少攻击面，防止基于网络或者应用程序漏洞被利用的攻击。 SDP 可以提供并响应 GRC 系统（例如与 SIEM 集成），以简化系统和应用程序的合规性活动。
合规范围增加及成本降低	通过集中控制从注册设备上的用户到特定应用程序/服务的连接，SDP 可以改进合规性数据收集、报告和审计过程。 SDP 可为在线业务提供额外的连接跟踪。 SDP 提供的网络微隔离经常用于减少合规范围，这可能会对合规报告工作产生重大影响。
安全迁移上云	通过降低所需安全架构的成本和复杂性，支持公有云、私有云、数据中心和混合环境中的应用程序，SDP 可以帮助企业快速、可控和安全地采用云架构。 与其他选项相比，新应用程序可以更快地部署，且有更好的安全性。
业务的敏捷性和创新	SDP 使企业能够快速、安全地实施其优先任务。例如： • SDP 支持将呼叫中心从企业内部机构转换为在家办公的工作人员 • SDP 支持将非核心业务功能外包给专业的第三方 • SDP 支持远程第三方网络和位置上用户自助服务的设备 • SDP 支持将公司资产部署到客户站点，与客户建立更强的集成并创造新的收入

SDP 主要功能

SDP 的设计至少包括五层安全性：（1）对设备进行身份认证和验证；（2）对用户进行身份验证和授权；（3）确保双向加密通信；（4）动态提供连接；（5）控制用户与服务之间的连接并且同时将这些连接隐藏。这些和其他组件通常都包含在 SDP 实现中。

信息/基础设施隐藏		
SDP 架构组件	**减轻或减少安全威胁**	**额外效益**
服务器“变黑”	所有外部网络攻击和跨域攻击	SDP 组件（控制器、网关）在尝试访问的客户主机通过安全协议（如单包授权（SPA））进行身份验证授权之前，不会响应任何连接请求。
减少拒绝服务（DoS）攻击	带宽和服务器 DoS 攻击（但请注意，SDP 应该通过 ISP 提供的上游反 DoS 服务来增强。）	面向 Internet 的服务通常位于“拒绝所有”SDP 网关（充当网络防火墙）后面，因此能够抵御 DoS 攻击。 SPA 可以保护 SDP 网关免受 DoS 攻击。
检测错误包	快速检测所有外部网络和跨域攻击。	从任何其他主机到接受主机（AH）的第一个数据包是 SPA 数据包（或类似的安全构造）。如果 AH 收到任何其他数据包，则将其视为攻击。

双向加密的连接		
SDP 架构组件	**减轻或减少安全威胁**	**额外效益**
验证用户和设备身份	来自未授权用户和设备的连接	所有主机之间的连接必须使用相互身份验证来验证设备和用户是否是 SDP 的授权成员。
不允许伪造证书	针对身份被盗的攻击	相互身份验证方案将证书固定到由 SDP 管理的已知且受信任的有效根目录。
不允许中间人攻击	中间人攻击	相互握手技术可以防止在撤销服务器证书之利用在线证书状态协议（OCSP）响应的中间人攻击。

“需知（NEED TO KNOW）”访问模型		
SDP 架构组件	**缓解或降低的安全威胁**	**额外效益**
取证简化	恶意数据包和恶意连接	对所有恶意数据包进行分析和跟踪，以便进行取证行动。
细粒度访问控制	来自未知设备的外部用户的数据窃取	只允许授权用户和设备与服务器建立连接。
设备认证	来自未授权设备的威胁；证书窃取	密匙被证实由请求连接的适当合法设备持有。
保护系统免受已被入侵设备的攻击	来自被入侵设备的“内网漫游”的威胁	用户只能访问授权的应用程序（而非整个网络）。

动态访问控制		
SDP 架构组件	**缓解或降低的安全威胁**	**额外效益**
动态的、基于会员认证体系的安全隔离区	基于网络的攻击	通过动态创建和删除访问规则（出站和入站）来启用对受保护资源的访问。

应用层访问		
SDP 架构组件	**缓解或降低的安全威胁**	**额外效益**
取消广域网接入	攻击面最小化； 消除了恶意软件和恶意用户的端口和漏洞扫描	设备只能访问策略允许的特定主机和服务，不能越权访问网段和子网。
应用程序和服务访问控制	攻击面最小化； 恶意软件和恶意用户无法连接到资源	SDP 控制允许哪些设备和应用程序可访问特定服务，例如应用程序和系统服务。

SDP 潜在应用领域

因为 SDP 是一种安全架构，所以它能够很好提供多种不同级别的安全，无法简单把它归类到现有的安全常见类别。下表列出了部分可由 SDP 实施保护的几种场景。

网络场景	现有技术的局限性	SDP 优势
基于身份的网络访问控制	传统的网络解决方案仅提供粗粒度的网络隔离，并且以 IP 地址为导向。即使 SDN 这样的新平台，企业仍然难以及时实现以身份为中心且精确的用户访问控制。	SDP 允许创建与组织相关的以身份为中心的访问控制，且访问控制是在网络层实施。例如，SDP 支持仅允许财务用户只能在公司允许的受控设备上通过 Web 访问财务管理系统。SDP 还允许只有 IT 用户才能安全地访问 IT 系统（SSH）。
网络微隔离	通过传统的网络安全工具，使用微隔离服务来提高网络安全性，是一种劳动密集型工作。	SDP 能够实现基于用户自定义控制的网络微隔离。通过 SDP 可以自动控制对特定服务的网络访问，从而消除了手动配置。
安全的远程访问（VPN 替代）	VPN 为用户提供安全的远程访问，但范围和功能有限。这种方式不保护本地用户，并且通常仅提供粗粒度访问控制（访问整个网段或子网）。这种安全和遵从风险通常违反最小权限原则。	SDP 可以保护远程用户和本地用户。公司组织可以使用 SDP 作为整体解决方案，摒弃 VPN 解决方案。而且，SDP 解决方案还专为细粒度访问控制而设计。用户无法访问所有未经授权的资源，这符合最小权限原则。
第三方用户访问	安全团队通常尝试通过 VPN，NAC 和 VLAN 的组合来控制第三方访问。这些解决方案通常是孤岛式的，无法在复杂环境中提供细粒度或全面的访问控制。	保护第三方访问权限使企业能够进行创新和适应。例如，用户可以从公司办公过渡到家庭办公以降低成本或者有时可以远程工作，而且某些功能可以安全地外包给第三方专家。SDP 可以轻松控制和保护第三方用户的本地访问。
特权用户访问安全	特权用户（通常是管理员）访问通常需要更高的安全性、监控和合规性监督。一般特权访问管理（PAM）解决方案通过凭证加密存储来管理访问，但是该凭证加密存储不提供网络安全性、远程访问或敏感内容访问。	对特权服务的访问可以限制为授权用户，并在网络层受到保护，并且可以向未经授权的用户隐藏特权服务，从而限制攻击范围。SDP 确保只有在满足特定条件时（例如，在定义的维护窗口期或仅从特定设备）才允许访问，然后可以记录访问日志以进行合规性报告。
高价值应用的安全访问	目前，对具有敏感数据的高价值应用程序提供细粒度授权可能需要对多个功能层进行复杂且耗时的更改。（例如：应用程序、数据外部访问。）	可以通过集成用户/身份感知，网络感知和设备感知在不暴露完整的网络的情况下限制对应用程序的访问;并依靠应用程序或应用程序网关进行访问控制。SDP 还可以促进应用程序升级，测试和部署，并为 DevOps CI / CD 提供所需的安全框架。

网络场景	现有技术的局限性	SDP 优势
托管服务器的访问安全	在托管安全服务提供商（MSSP）和大型 IT 环境中，管理员可能需要定期对在重叠 IP 地址范围的网络上对托管服务器进行网络访问。这一点通过传统的网络和安全工具很难实现，并且要求繁琐的合规性报告。	可以通过业务流程来控制对托管服务器的访问。SDP 可以覆盖复杂的网络拓扑、简化访问，同时记录用户活动以满足合规性要求
简化网络集成	要求组织定期快速集成之前不同的网络，例如，在并购或灾难恢复方案中	借助 SDP，网络可以快速无中断地互连，而无需进行大规模更改
安全迁移到 IaaS 云环境	采用基础架构即服务（IaaS）的组织急剧增加，但许多安全性问题仍待解决。例如，IaaS 访问控制可能与企业原有的访问控制无法衔接，范围仅限于云提供商环境内部。	SDP 方案改进了 IaaS 安全性。不仅将应用程序隐藏在默认防火墙之外，还会对流量进行加密，并且可以跨异构企业定义用户访问策略。请参考《SDP 在 IaaS 中的应用》白皮书。
强化身份认证方案	对已有的应用程序在安全性和合规性上可能需要额外的 2FA。但这在非网络应用和不易更改的程序上是很难实现的。	SDP 需要在对特定应用程序授予访问权限之前添加 2FA。并通过部署多因素身份验证（MFA）系统来改善用户体验，并可以添加 MFA 以增强遗留应用程序的安全性。
简化企业合规性控制和报告	合规性报告需要 IT 团队付出极其耗时且成本高昂的工作。	SDP 降低了合规范围（通过微隔离），并自动执行合规性报告任务（通过以身份为中心的日志记录和访问报告）.
防御 DDoS 攻击	传统的远程访问解决方案将主机和端口暴露在 Internet，并受到 DDoS 攻击。所有的完整的数据包都被丢弃，而且低带宽 DDoS 攻击绕过了传统的 DDoS 安全控制。	SDP 可以（让服务器）对未经授权的用户不可见，并通过使用 default-drop 防火墙，只允许合法的数据包通过。

4 具体来说，我们正在讨论用于远程企业用户访问的 VPN，而不是站点到站点 VPN 或消费者 VPN 方案。
5 在 Gartner 于 2016 年 9 月 30 日发表的一篇论文中，作者写道：“到 2021 年，60％的企业将逐步淘汰数字商业通信的网络 VPN，转而采用软件定义边界，而 2016 年不到 1％“。

“现在是时候将你的服务从互联网沼泽中隔离出来了”
https://www.gartner.com/doc/3463617/time-isolate-services-internet-cesspool。

SDP 架构

SDP 架构的主要组件包括客户端/【发起主机（IH）】，服务端/【接受主机（AH）】和【SDP 控制器】，AH 和 IH 都会连接到这些控制器。【SDP 主机】可以启动连接（发起主机或 IH），也可以接受连接（接受主机或 AH）。 IH 和 AH 之间的连接是通过【SDP 控制器】与安全控制信道的交互来管理的。该结构使得控制层能够与数据层保持分离，以便实现完全可扩展的安全系统。此外，所有组件都可以是冗余的，用于扩容或提高稳定运行时间。通过遵循此处概述的工作流程，可以使用图 1 中概述的技术来保护这三个组件之间的连接。

工作原理

IH 上的**【SDP 客户端软件】**启动与 SDP 的连接。

包括笔记本电脑、平板电脑和智能手机在内的 IH 设备面向用户，也就是说 SDP 软件在设备自身上运行。网络可以是在部署 SDP 的企业的控制之外。

AH 设备接受来自 IH 的连接，并提供由 SDP 安全保护的一组服务。AH 通常驻留在企业控制下的网络（和/或直接的代表）。

SDP 网关 为授权用户和设备提供对受保护程序和服务的访问。网关还可以对这些连接进行监视、记录和报告。

IH 和 AH 设备连接到**【SDP 控制器】**，**【SDP 控制器】**可以是一种设备或程序，它确保用户是经过身份验证和授权、设备经过验证、通信是安全建立的、网络中的用户流量和管理流量是独立的，来确保对隔离服务的安全访问。

AH 和控制器使用单包授权（SPA）进行保护，这样让未授权的用户和设备无法感知或访问。第 21 页描述了单包授权（SPA）的参考实现。

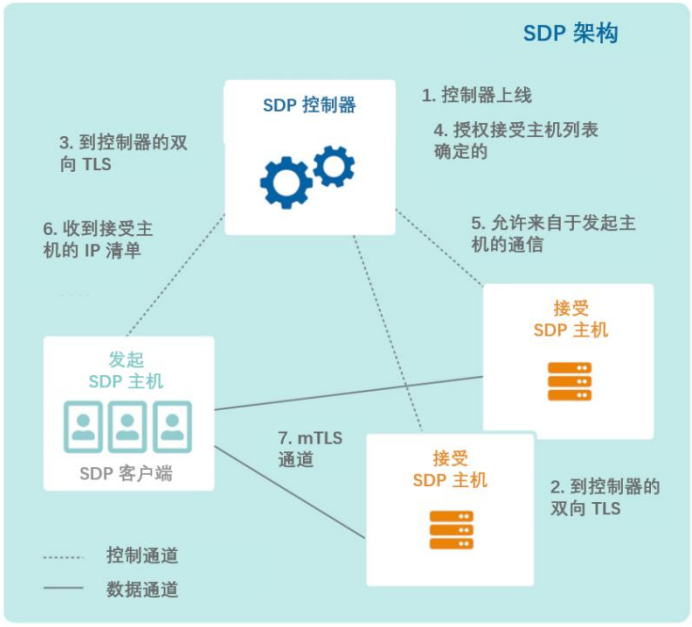


图 1：SDP 架构（已经在 《SDP 标准规范 1.0》 中发布）

SDP 的安全性遵循以下特定各步骤的工作流程：

1. 在 SDP 中添加并激活一个或多个【SDP 控制器】并连接到身份验证和授权服务，例如 AM、PKI 服务、设备验证、地理位置、SAML、OpenID、OAuth、LDAP、Kerberos、多因子身份验证、身份联盟和其他类似的服务。

2. 在 SDP 中添加并激活一个或多个 AH。它们以安全的方式连接控制器并进行验证。 AH 不响应来自任何其他主机的通信，也不会响应任何未许可的请求。

3. 每个 IH 会在 SDP 中添加和激活，并与【SDP 控制器】连接并进行身份验证。

4. IH 被验证之后，【SDP 控制器】确定 IH 被授权可以连接的 AH 列表。

5. 【SDP 控制器】指示 AH 接受来自 IH 的通信，并启动加密通信所需的任何可选策略。

6. 【SDP 控制器】为 IH 提供 AH 列表，以及加密通信所需的任何可选策略。

7. IH 向每个授权的 AH 发起 SPA。然后 IH 和这些 AH 创建双向加密连接（例如，双向验证 TLS 或 mTLS）。

8. IH 通过 AH 并使用双向加密的数据信道与目标系统通信。（注意：上一页的图 1 中未描述步骤 8）。

SDP 部署模型

CSA 的 **SDP 标准规范 1.0** 中定义了以下几种在组织机构中部署 SDP 的可能架构：

- 客户端-网关
- 服务器-服务器
- 客户端-网关-客户端
- 客户端-服务器
- 客户端-服务器-客户端
- 网关-网关

【客户端-网关】

当一个或多个服务器必须在网关后面受到保护时，无论底层网络拓扑如何，客户端/IH 和网关之间的连接都是安全的。网关既可以位于同一位置，也可以跨国的分布。

在这个部署模式下，客户端/IH 通过 mTLS 隧道直接连接到网关，并在网关终结 mTLS 隧道。如果要确保与服务器的连接是安全的，必须采取其他预防措施。【SDP 控制器】可以位于云中或受保护服务器附近，因此控制器和服务器使用相同的 SDP 网关。

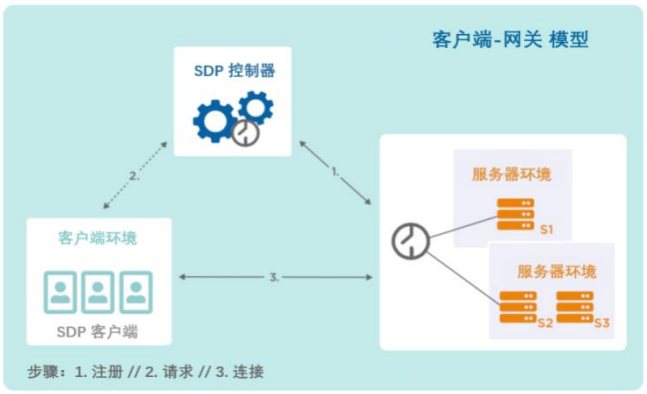


图 2：【客户端-网关】模型：一个或者多个服务器被网关保护

在图 2 中，（在一个或多个环境中的）服务器作为 AH 在 SDP 网关后受到保护。要确保穿过网关的服务器的连接安全性，服务器所处的环境应由运行 SDP 的组织控制。

网关和控制器被 SPA 和采用“缺省丢弃”（default-drop）策略防火墙所保护，除非通信来自于正常的客户端/IH，服务器是不可访问的。因此，服务器对于

非授权用户和潜在的攻击者而言，这些服务器是不可见且不可访问的。

受保护的服务器是无法访问的，除了来自正常的客户端/ IH，并且网关和控制器使用带有默认防火墙的 SPA 进行保护，因此它们是“黑暗的”并且对于未经授权的用户和潜在的攻击者是不可访问的。

受保护的服务器可以包含在 SDP 中，而无需对服务器进行任何更改。但是，它们所在的网络需要配置为仅允许从网关到受保护服务器的入站连接，这将防止未经授权的客户端绕过网关。

这种部署模式下，因为可以在 SDP 网关和受保护服务器之间部署安全组件，从而保留了组织机构使用其现有网络安全组件（如 IDS/IPS）的能力。从连接客户端到网关的流量从 mTLS 隧道中流出之后，可以进流量监控。

客户端/IH 既可以是终端设备，也可以是服务器。（参考第 16 页的【服务器-服务器】模型）

【客户端-网关】模型适用于将其应用程序迁移到云的组织。无论服务器环境位于何处（云、本地或附近），组织机构都希望必须确保网关和应用程序之间的数据安全。

此模型还适用于保护本地遗留应用程序，因为 IH 不需要进行任何更改。

【客户端-服务器】

当组织机构将应用程序移动到 IaaS 环境并提供程序端到端地保护连接时，此模型将服务器和网关组合在一个主机中。 客户端/IH 可以位于与服务器相同的位置，也可以是分布式的。在任何一种情况下，客户端/IH 和服务器之间的连接都是端到端的。

该模型为组织提供了极大的灵活性，因为“服务器-网关”组合可以根据需要在多个 IaaS 提供商之间移动。此模型也适用于保护无法升级的本地遗留应用程序。

在此模型中，客户端/IH 通过 mTLS 隧道直接连接到安全服务器，并终结于安全服务器。 SDP 控制器可以位于服务器上（因此控制器和服务器使用相同的网关）或者位于云中。

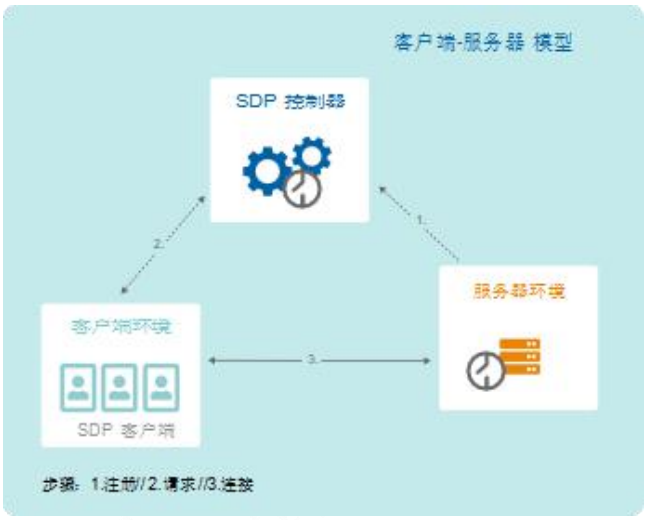


图 3：【客户端-服务器】模型：服务器上直接运行网关软件

服务器受 SDP 网关保护（作为 AH ）。通过网关连接到服务器（在服务器环境中）的安全连接可以在服务器上的应用程序/服务的所有者控制下，使所有者完全控制这些连接。

因为网关和控制器通过使用“默认丢弃”（default-drop）策略的防火墙以及 SPA 进行保护，因此除了来自被允许的客户端/IH 的请求之外，受保护的服务器是不可访问的。这意味着服务器对于内部、外部攻击者以及未经授权的用户是无法访问的，这可以提供对内部威胁的卓越保护。

使用此模型，受保护的服务器将需要配备网关。服务器所在的网络不需要配置为限制到受保护服务器的入站连接。这些服务器上的网关（执行点）使用 SPA 来防止未经授权的连接。

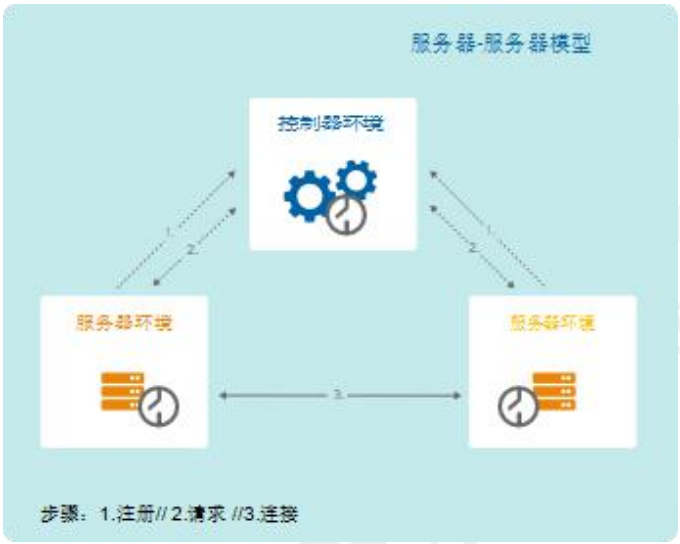
此模型可以更轻松地使用现有的网络安全组件，例如 IDS/IPS 或 SIEM。可以通过分析来自 SDP 网关/受保护服务器的丢弃数据包来监控流量，从而保留客户端/IH 与服务器之间的 mTLS 连接。（另请注意，客户端/IH 虽然描述为用户设备，但它本身可能是服务器。在这种情况下，请参阅下面的服务器到服务器模型。）

【客户端-服务器】模型非常适合将应用程序迁移到云的组织。无论服务器环境位于何处（云或本地），组织都可以完全控制与云中应用程序的连接。

【服务器-服务器】

此模型最适合物联网（IoT）和虚拟机（VM）环境，并确保服务器之间的所有连接都加密，无论底层网络或 IP 基础结构如何。服务器到服务器模型还确保组织的 SDP 白名单策略明确允许通信。跨不受信任的网络的服务器之间的通信是安全的，并且服务器使用轻量级 SPA 协议保持对所有未授权连接保持隐藏。

此模型类似于上一页中的客户端到服务器模型，除了 IH 本身是服务器，并且还可以充当 SDP AH。与【客户端-服务器】模型一样，【服务器-服务器】模型要求在每个服务器上安装 SDP 网关或类似的轻量级技术，并使得所有【服务器-服务器】的流量相对整个环境中其他元素而言不可见。基于网络的 IDS/IPS 需要配置从 SDP 网关而不是从外部获取数据包。此外，组织可能依赖基于主机的 IDS/IPS 。



图示 4：【服务器-服务器】模型：任何通信包括了 API 调用和系统服务

SDP 控制器可以位于服务器上，以便控制器和服务器使用相同的 SDP 网关。【SDP 控制器】也可以保留在云端。

服务器在作为 AH 的 SDP 网关后面而受到保护。通过网关的服务器（在服务器环境中）的安全连接默认由服务器上的应用程序/服务的所有者控制，这使得所有者可以完全控制这些连接。

受保护的服务器除了来自其他白名单服务器外是不可访问的，网关和控制器由 SPA 通过防火墙“默认丢弃”（default-drop）模式进行保护，因此服务器是不可见的（Dark），攻击者和未经授权的用户(内部和外部)无法访问这些服务器，从而提供了额外的保护免受内部威胁。

使用此模式，受保护的服务器将需要配备网关或轻量级 SPA 协议。受保护的服务器所在的网络不需要配置为限制 inbound(流量)连接。这些服务器上的网关(执行点)利用 SPA 协议防止内部和外部未经授权的连接。

该模式使应用 IDS/IPS 和 SIEMs 等网络安全组件变得更加容易。可以通过分析来自 SDP 网关/受保护服务器的所有丢弃包来监控流量，从而保持受保护服务器之间的 mTLS 连接。

该模式非常适合所有组织将物联网和 VM 环境迁移到云上的环境。无论服务器环境位于何处(云环境还是本地环境)，企业组织都可以完全控制到云环境的连接。

【客户端-服务器-客户端】

在某些情况下，点对点通信通过中介服务器，例如 IP 电话、聊天和视频会议服务。在这些情况下，SDP 连接客户端的 IP 地址，组件连接通过加密网络，并通过 SPA 保护服务器/AH 免受未经授权的网络连接。

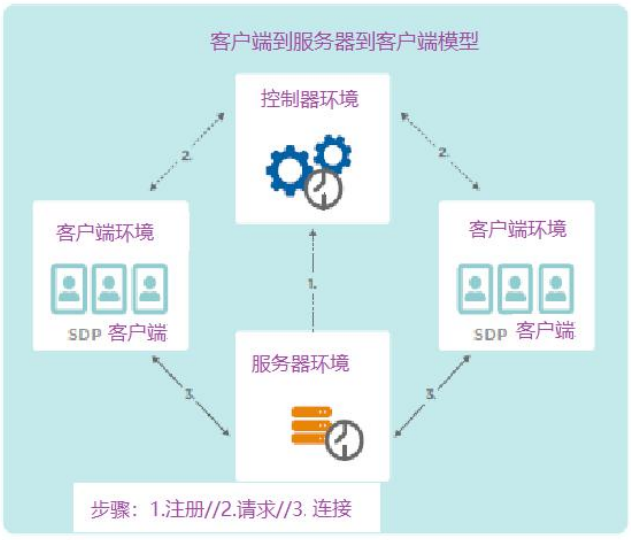


图 5:客户端到服务器到客户端模式:用于对等连接的模式，如 IP 电话或聊天。

SDP 控制器可能位于服务器上(因此控制器和服务器使用相同的 SDP 网关)或云中。如上所述，服务器在充当 AH 的 SDP 网关后面受到保护。默认情况下，通过网关到服务器的安全连接由服务器上的应用程序/服务的所有者控制。

受保护的服务器是不可访问的，除非来自其他被允许的客户端，而且网关和控制器由 SPA 通过防火墙“默认丢弃”（Default-drop）进行保护，因此服务器是不可见的，并攻击者和未经授权的用户(内部和外部)无法访问服务器，以提供额外的保护免受内部威胁。

使用此模式，受保护的服务器将需要配备网关或轻量级 SPA 协议。受保护服务器所在的网络不需要限制入向（inbound）连接。服务器上的网关(执行点)使用 SPA 来防止内部和外部未经授权的连接。

该模式使应用 IDS/IPS 和 SIEMs 等网络安全组件变得更加容易。可以通过分析来自 SDP 网关/受保护服务器的所有丢包来监控流量，从而保持客户端和受保护服务器之间的 mTLS 连接。

该模式非常适合于组织机构将其对等应用程序迁移到云中。无论服务器环境位于何处(云环境还是本地环境)，组织都可以完全控制到客户端的连接。

【客户端-网关-客户端】

此模式是上面客户机到服务器到客户机的变形。该模式支持对等网络协议，要求客户端在执行 SDP 访问策略时直接相互连接。

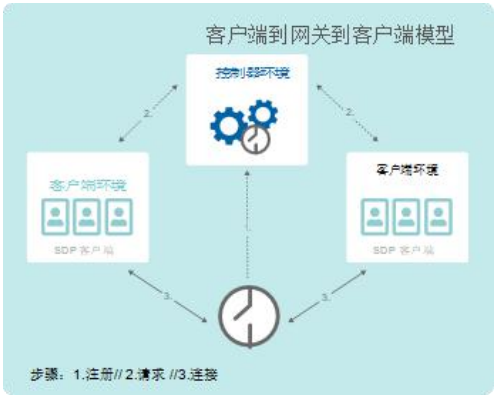


图 6:客户端到网关到客户端模型:用于保护客户端到客户端的通信。

这将导致客户机之间的逻辑连接(每个客户机都充当 IH、AH 或两者的角色，具体取决于应用程序协议)。注意，应用程序协议将决定客户端如何进行彼此连接，SDP 网关充当它们之间的防火墙。

未来将发布更多的关于这个模式的信息。

【网关到网关】

网关到网关模式没有包含在 SDP 规范 1.0 的初始发布中。该模式非常适合于某些物联网环境。在此场景中，一个或多个服务器位于 AH 后面，因此 AH 充当客户端和服务器之间的网关。与此同时，一个或多个客户端位于 IH 后面，因此 IH 也充当网关。

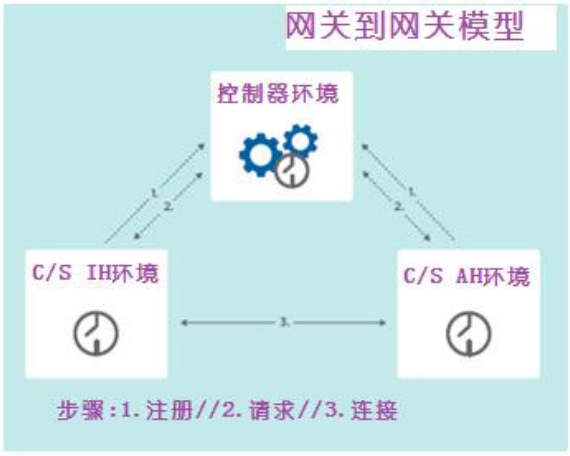


图 7:网关到网关模式:一个或多个服务器或客户端在网关后面受到保护

在这个模型中，客户端设备不运行 SDP 软件。这些设备可能包括那些不需要或不可能安装 SDP 客户机的设备，例如打印机、扫描仪、传感器和物联网设备。在这个模型中，网关作为防火墙，也可能作为路由器或代理，具体取决于实现部署方式。

SDP 部署模式和相应的场景

下表显示了哪些部署模式可以对应到哪些 SDP 场景。每种类型的部署都需要保护不同的连接。

网络场景	客户端到网关	客户端到服务器	服务器到服务器	客户端到服务器到客户端	客户端到网关到客户端	网关到网关
基于身份的网络访问控制	Y	Y*	Y	Y	Y	Y**
所有的 SDP 模式都支持身份驱动的网络访问控制。 *此模式提供到网络和服务的安全连接。 ** 此模式为，SDP 识别设备的程度取决于特定的 SDP 实现执行设备识别和验证的方式。例如，MAC 地址提供的身份验证比 802.1x 更弱。						
网络微隔离	Y*	Y**	Y***	Y	Y	Y
所有的 SDP 模式都通过保护单个连接来提供网络微隔离。 *此模式通过保护客户端和网关之间的连接来提供微隔离，但不提供到网关后面服务器的微分隔连接。 **该模式通过保护到服务器的所有连接来提供网络微隔离。此外，承载网关的服务器是隐藏的。 ***该模式通过保护到指定服务器的所有连接来提供网络微隔离。此外，承载网关的服务器是隐藏的。						
安全远程访问（VPN 替代）	Y	Y	Y	Y	Y	Y
SDP 是传统 VPN 的替代品。在所有情况下，控制器和网关/AH 必须能够被远程设备访问 他们可以使用 SPA 启动连接。						
第三方用户访问	Y	Y	Y*	Y	Y	Y
根据需要保护的连接，SDP 支持对所有场景的第三方访问。第三方可能是 远程或现场，也可以有一个独立的身份提供程序对其进行身份验证。 * SDP 模式为，提供保护连接从第三方应用对内部应用程序的访问，第三方应用程序作为客户端。						
特权用户访问安全	Y	Y	N	Y	Y	N
SDP 保护来自客户端特权用户的访问连接。通常，特权用户访问指的是访问服务器的客户机（身份或权限），但可以应用于所有模式，具体取决于所涉及的应用程序。						
高价值应用的安全访问	Y	Y	Y	Y	Y	N
除了网关到网关模式以外，所有保护模式都提供特定的方式来进行高价值应用程序的访问保护。						
托管服务器的访问安全	Y	Y*	Y	Y	N	Y

此场景用于服务提供者访问托管服务器。服务器可以完全由网关隐藏，或者在托管服务环境中，只有管理界面由网关隐藏。 *在该模型中，SDP 网关软件部署在服务器上。服务器被隐藏，MSSP/托管服务被检测和控制服务进行连接。						
简化网络集成	Y	Y*	Y*	Y	Y	Y
所有 SDP 部署模式都支持此场景，不同模式有不同的安全连接。 *对于这些模式，另一个优点是服务器上的服务可以通过网关隐藏。						
安全迁移到 IaaS 云环境	Y	Y	Y	Y	Y	Y
这个场景涉及到将服务从本地迁移到云。						
强化身份验证方案	Y	Y	Y*	Y	Y	Y
所有 SDP 模式都提供增强身份验证的能力，通常通过多因素/逐步验证。 *此模式下没有用户，无法提示输入一次性密码。但是，它可以支持多因素身份验证，比如使用 PKI 或基于服务器的 HSM。身份管理系统可以(也应该)用于系统或设备，而不仅仅是用户。						
简化企业合规性控制和报告	Y	Y	Y	Y	Y	Y
所有 SDP 模式都通过集成控制方式帮助企业简化合规性。						
防御 DDoS 攻击	Y	Y	Y	Y	Y	Y
因为所有的 SDP 模型都在网关中使用 SPA，它们提高了组织对 DDoS 攻击的弹性。在这种情况下,我们不使用拒绝网关服务，与内部托管服务相比，面向互联网的服务更频繁的受到 DDoS 攻击。						

SDP 连接安全

SDP 架构提供的协议在网络栈所有层都对连接提供保护。图 8 描述了被各种 SDP 部署模式保护的连接。通过在关键位置部署网关和控制器，实施人员能够专注于保护对组织最关键的连接，并保护这些连接免受网络攻击和跨域攻击。

单包授权

SDP 技术最关键的组成部分之一是要求并强制实施“先认证后连接”模型，该模型弥补了 TCP/IP 开放且不安全性质的不足。SDP 通过单包授权（SPA）实现这一点。SPA 是一种轻量级安全协议，在允许访问控制器或网关等相关系统组件所在的网络之前先检查设备或用户身份。

包括请求方的 IP 地址等在内的连接请求的信息，在单一的网络消息中被加密和认证。SPA 的目的是允许服务被防火墙隐藏起来并被默认丢弃。该防火墙系统应该丢弃所有 TCP 和 UDP 数据包，不回复那些连接尝试，从而不为潜在的攻击者提供任何关于该端口是否正被监听的信息。在认证和授权后，用户被允许访问该服务。SPA 对于 SDP 不可或缺，用于在客户端和控制器、网关和控制器、客户端和网关等之间的连接中通信。

尽管各种 SPA 的实现可能有轻微差别，这些实现都应该能满足以下原则：

1. 数据包必须被加密和认证
2. 数据包必须自行包含所有必要的信息；单独的数据包头不被信任
3. 生成和发送数据包必须不依赖于管理员或底层访问权限；不允许篡改原始数据包
4. 服务器必须尽可能无声地接收和处理数据包；不发送回应或确认

SPA 的好处

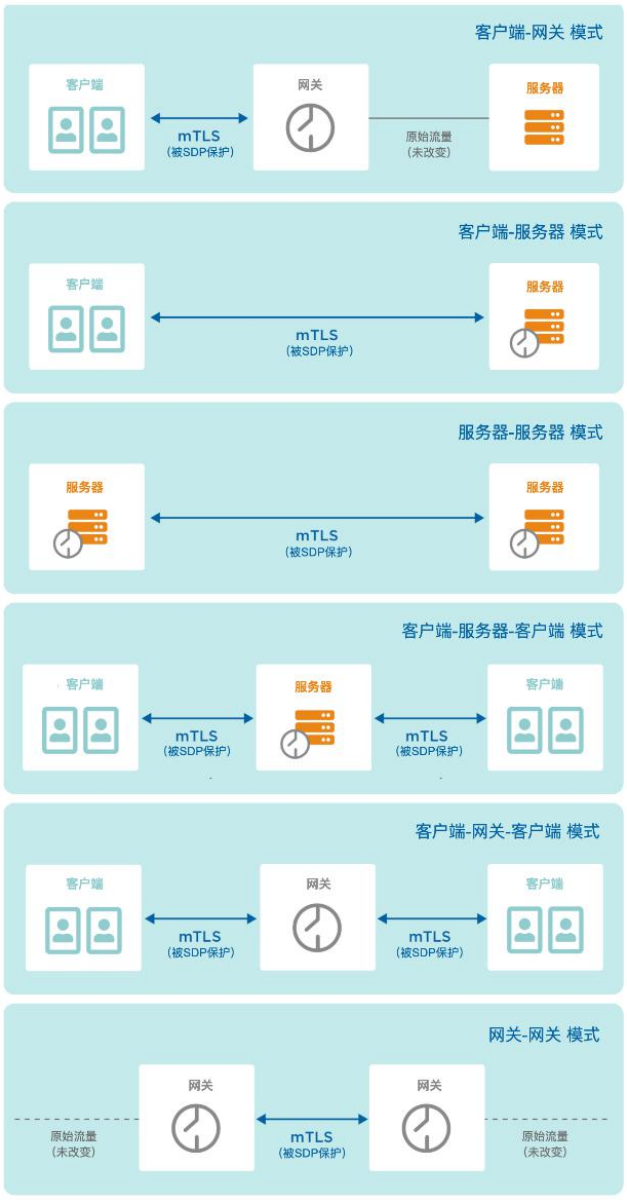


图 8：被各种 SDP 部署模式保护的连接

SPA 在 SDP 中起很大作用。SDP 的目标之一是克服 TCP/IP 开放和不安全的基本特性。TCP/IP 的这个特性允许“先连接后认证”。鉴于今天的网络安全威胁形势，允许恶意行为人员扫描并连接到我们的企业系统是不可被接受的。与 SDP 组合的 SPA 通过两种方式应对这个弱点。使用 SDP 架构的应用被隐藏在 SDP 网关/AH 后面，从而只有被授权的用户才能访问。另外，SDP 组件自身，如控制器和网关也被 SPA 保护。这允许它们被安全地面向互联网部署，确保合法用户可以高效可靠地访问，而未授权用户则看不到这些服务。**SPA 提供的关键好处是服务隐藏。**防火墙的 Default-drop（默认丢弃）规则缓解了端口扫描和相关侦查技

术带来的威胁。这种防火墙使得 SPA 组件对未授权用户不可见，显著减小了整个 SDP 的攻击面。相比与 VPN 的开放端口以及在很多实现中都存在的已知弱点，SPA 更安全。

SPA 相对于其他类似技术的另一个优势是**零日(Zero-day)保护**。当一个漏洞被发现时，如果只有被认证的用户才能够访问受影响的服务，使该漏洞的破坏性显著减小。

SPA 也可以抵御分布式拒绝服务（DDoS）攻击。如果一个 HTTPS 服务暴露在公共互联网而能被攻击，很少的流量就可能使其宕机。SPA 使服务只对认证的用户可见，因而所有 DDoS 攻击都默认由防火墙丢弃而不是由被保护的服务自己处理。

SPA 的局限

SPA 只是 SDP 多层次安全的一部分，仅其自身并不完整。虽然 SPA 实现应该设计成能够抵御重放攻击，但是 SPA 仍然可能遭受中间人（MITM）攻击。具体而言，如果一个 MITM 敌方能够捕获并修改 SPA 数据包，虽然该敌方不能建立到被授权客户端的连接，但是可能有能力建立到控制器/AH 的连接。但该敌方将不能在没有客户端证书的情况下完成 mTLS 连接。因此控制器/AH 应该拒绝这个连接尝试并关闭 TCP 连接。即使是在 MITM 场景下，SPA 也远比标准 TCP 安全。

不同供应商的 SPA 实现可能有轻微差异。Fwknop（FireWall KNock Operator）项目[14]提供了一个开源的 SPA 参考实现，请参考第 38 页附录 2。另一个很好的参考是 Evan Gilman 和 Doug Barth《零信任网络》(O'Reilly Media, Inc., 2017)一书的《信任其流量》一章。

SDP 和访问控制

SDP 作为一个新兴架构的价值在于加强了访问控制管理，并为实施用户访问管理、网络访问管理和系统认证控制等设定了标准。SDP 有能力通过阻止来自于未授权用户和/或使用未批准设备的网络层访问的方式实施访问控制。因为 SDP 部署了“全部拒绝”（Deny-all）的防火墙，可以阻止、允许或防止网络数据包在 IH 和 AH 间流动。至少，SDP 使组织机构能够定义和控制自己的访问策略，决定哪些个体能够从哪些被批准的设备访问哪些网络服务。

SDP 并不尝试去替代已有的身份和访问管理方案，但对用户认证的访问控制进行了加强。SDP 通过将用户认证和授权与其它安全组件集成（见第 8 页的“SDP 的主要功能”）显著减小了潜在攻击面。例如，用户 Jane 可能没有登录公司生产财务管理服务器的密码，但该服务器即使只是简单地在网络上对 Jane 的设备可见，就仍然存在风险。如果 Jane 的公司部署了 SDP 架构，财务管理服务器就对 Jane 的设备隐藏了。所以，即使攻击者已经在 Jane 的设备上立足，SDP 将阻止从该设备连接到财务管理服务器。即使 Jane 确实有允许访问财务管理服务器的密码，在她的设备上安装 SDP 客户端也提供了额外的保护。攻击者仍然将被多因子身份认证加上强力的设备验证拒之门外。

[1]https://www.cipherdyne.org/fwknop/

补充架构

零信任和 BeyondCorp

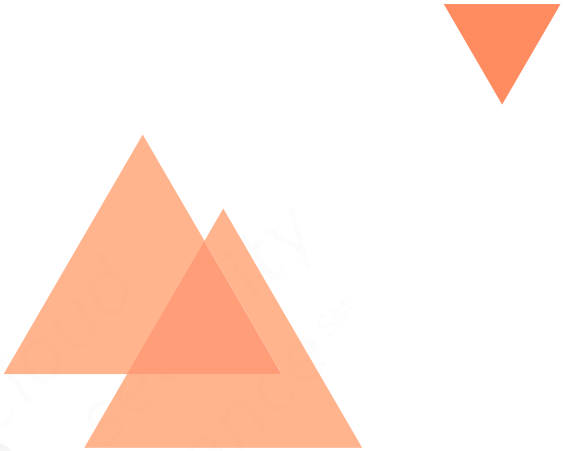
在当今的安全蓝图中，除了软件定义边界之外还有另外两个新思路：由行业分析公司 Forrester 最早推动的“零信任”概念和 Google 内部的 BeyondCorp 举措。

Forrester 的零信任模型

Forrester 的零信任模型[2]在过去的几年中扩大了其范围，零信任模型建立在三个原则之上：

- 不管用户和资源所处位置，确保所有资源访问都是安全的
- 记录和检查所有流量
- 执行最小权限原则

这些原则与 SDP 所提供的一致。SDP 架构可能是实施这些零信任原则的最佳方法。SDP 对用户和设备进行强认证，并对网络连接进行加密，从而保证不管用户所在位置，所有资源都被安全地访问。SDP 通常作为覆盖层部署在现有网络上，因此也确保无论资源是部署在内部、云上或其他位置，都可以被安全地访问。在 SDP 实现中，网络连接也受控制，提供了一个中心位置记录哪些个体（人或机器）正在访问哪些资产。如果需要对数据包进行深度检测，SDP 能够很容易地与网络流量探测系统集成。最后，也许是最重要的，SDP 天然地且强力地执行最小特权原则。



SDP 从一个默认的、拒绝所有的网关开始，并严格按照白名单访问模型访问，个体只有在明确被 SDP 控制器允许时才能访问 SDP 自身和联网的应用。这是最小特权原则的本质。

Google 的 BeyondCorp 模型

BeyondCorp 是 Google 内部网络的安全访问平台，用于帮助其员工访问内部资源。BeyondCorp 强调通过设备许可管理企业提供的 Chromebook 。这个系统已经被充分研究和记录[3]，并且已经成为 Google 在过去五年中的一个成功的内部项目。

与 SDP 模型有所区别的是，BeyondCorp 是一个基于 Web 代理的方案，支持 HTTP、HTTPS 和 SSH 协议。SDP 实现通常支持更多 IP 协议，在某些实现中甚至支持所有 IP 协议。SDP 也比 BeyondCorp 支持更细颗粒度的访问控制。在 Google 的系统中，应用都被

[15]https://www.forrester.com/report/The+Forrester+Wave+Zero+Trust+eXtended+ZTX+Eco- system+Providers+Q4+2018/-/E-RES141666 and https://go.forrester.com/blogs/next-genera- tion-access-and-zero-trust/

[16]https://cloud.google.com/beyondcorp/#researchPapers

[17]https://cloud.google.com/istio/

分配成若干“可信级别”。通过用户和设备上下文信息，SDP 支持更细颗粒度和独立的访问控制。

尽管 Google 的 BeyondCorp 不能在市场中买到，但 Google 已经在其用于保护微服务的开源平台 Istio[4] 中包括了 BeyondCorp 平台的一些组件。Google 也发布了一个称为身份感知代理(Identity- Aware Proxy，IAP)的免费组件[5]，控制对 Google 云平台（Google Cloud Platform，GCP）中资源的访问。IAP 不是 SDP，也不具有 BeyondCorp 的全部能力。据 Google 称，“云 IAP 是 BeyondCorp 的一个构成模块”。

如果你的企业在考虑构建建一个零信任安全环境，或者你的团队喜欢 BeyondCorp 方法，你可能也不妨评估一下 SDP，因为它提供了类似的好处且有多个可在市场中购买到的产品。

总之，SDP 架构能够保证零信任原则的成功实现。BeyondCorp 实现为读者提供了将 SDP 架构结合到 BYOD 战略中的成功参考。

[18]https://cloud.google.com/iap/

软件定义边界 SDP 与您的企业

因为组织机构中的许多利益相关者都存在安全风险和顾虑，企业信息安全架构很复杂。无论底层 IP 基础设施如何，软件定义边界 SDP 都能确保安全连接。软件定义边界 SDP 因为包含以下关键概念，所以可以作为企业安全架构的基础：

1.在允许连接之前授权用户并验证设备

2.双向加密通信

3.拒绝一切（Deny-all）的防火墙动态规则和服务器隐身功能

4.集成应用上下文和细颗粒度的访问控制

在本节中，我们提出了架构师们在其企业中规划部署软件定义边界 SDP 时应考虑的一些问题。这些问题将帮助架构师们考虑安全性的各个方面，这些方面包括用户群、网络、服务器环境以及安全性和合规性要求。

SDP 的部署如何适应现有的网络技术？

架构师们必须决定使用哪个软件定义边界 SDP 部署模型，同时必须理解某些模型中网关可能代表一个额外的在线网络组件。这可能会影响到他们组织的网络，例如需要对防火墙或路由进行一些更改，确保受保护的服务器是不可见的，并且只能通过 SDP 网关访问。

SDP 如何影响监控和日志系统？

由于软件定义边界在 SDP 连接发起方 IH 和 SDP 连接接受方 AH 之间使用 mTLS 协议，因此网络流量对于可能用于安全、性能或可靠性监控目的的中介服务不透明。架构师们必须了解哪些系统正在运行，以及软件定义边界对网络流量的相关更改如何影响这些系统。由于软件定义边界通常为用户访问提供更丰富的、以身份为中心的日志记录，因此它们还可以用于补充和增强现有的监控系统。此外，所有软件定义边界网关和控制器丢弃的数据包都可被记录到安全信息和事件平台中进行进一步分析。每个连接的“谁、何时、何地”信息变得更容易收集。

软件定义边界如何影响应用程序发布/DevOps 流程和工具集，以及 API 集成？

许多组织机构都采用了 DevOps 或 CI/CD(持续集成/持续交付)[19] 等快速应用程序发布流程。这些流程及其支持的自动化框架与安全系统的集成需要经过深思熟虑，SDP 也不例外。SDP 可以有效地保护授权用户在 DevOps 时可与开发环境连接。SDP 还可以在操作期间保护连接，即使是合法用户到受特殊保护的服务器和应用程序间的连接也得以保护。

安全架构师们必须理解他们的 SDP 部署模型，以及他们组织的 DevOps 机制将如何与之集成。因为 API 集成通常是 DevOps 工具集集成的需求，安全团队应该查看他们的 SDP 实现所支持的一组 API。

SDP 如何影响用户，特别是业务用户？

安全团队经常努力使其解决方案对用户尽可能透明，SDP 支持这种方法。如果实现了最小权限原则，用户将可以完全访问他们需要的一切，而且不会注意到不必要的访问被拒绝。根据 SDP 部署模型，用户将在其设备上运行 SDP 客户端软件。安全架构师应该与 IT 部门协作，对用户体验、客户端软件分发和设备安装过程进行规划。

19 https://en.wikipedia.org/wiki/DevOps and https://en.wikipedia.org/wiki/CI/CD

企业信息安全的元素

图 9 表明了企业安全架构的主要元素。该图是混合企业的简化视图，描述了安全基础设施原型的主要元素以及这些元素之间的关系。

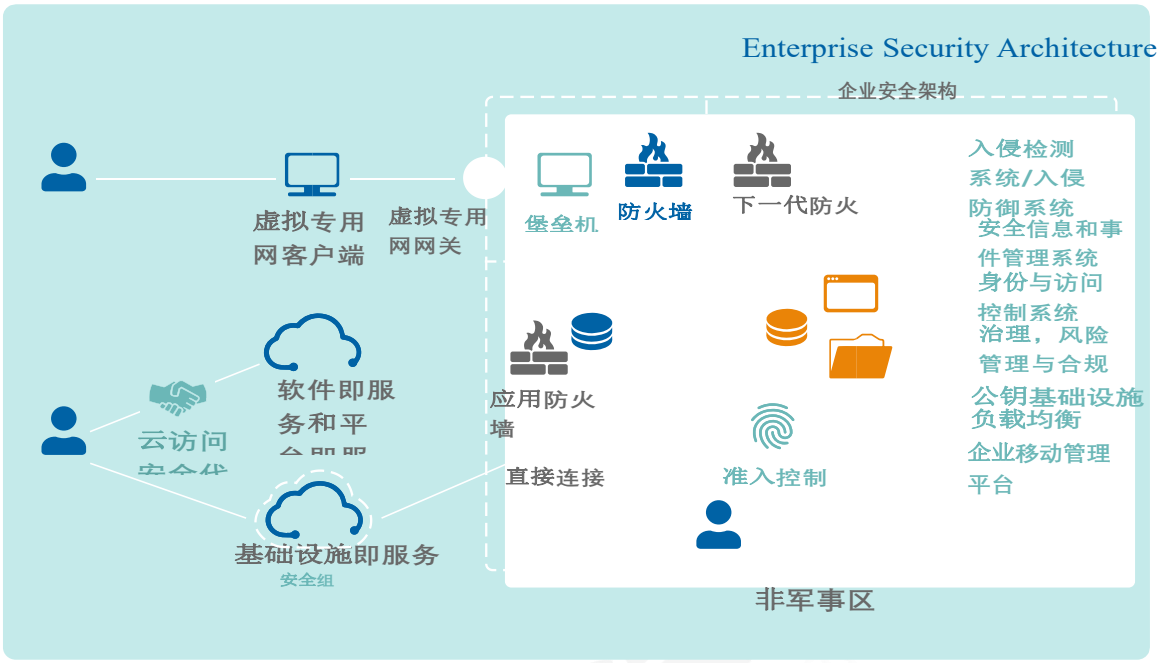
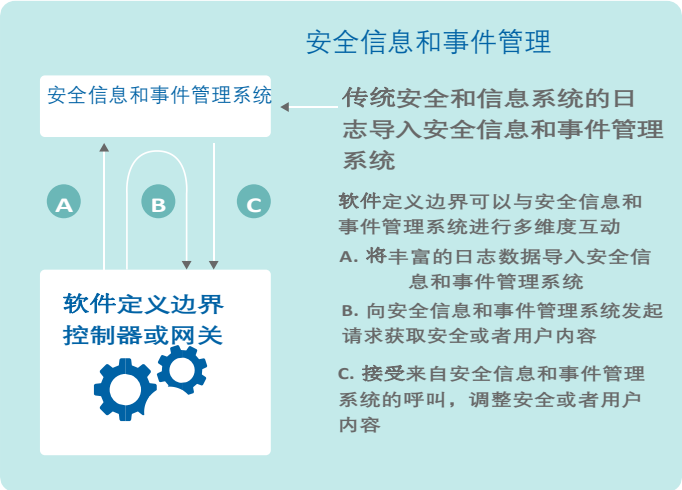


图 9：安全基础设施原型的主要元素

此企业安全体系结构示例由内部部署和基于云的资源（IaaS 和 SaaS / PaaS）组成，其中包含一组标准的安全、IT 和合规性组件。以下几页将详细地探讨这些标准组件如何与 SDP 集成。

安全信息和事件管理（SIEM）

SIEM 系统[14]提供对应用程序和网络组件生成的日志信息和安全警报进行分析的功能。SIEM 系统集中存储并解析日志，支持近乎实时地分析，这使得安全人员能够快速采取防御措施。SIEM 系统还提供了基于法律合规通常所需的自动化集中报告。



图表 10：安全信息和事件管理 SIEM 和软件定义边界 SDP

安全信息和事件管理系统无论是部署在内网还是在托管在云中，都是 IT 和安全管理系统中一个成熟的主流部分。虽然商业化的 SDP 解决方案通常提供内部日志记录功能，但当 SDP 日志被定向到从多个来源聚合信息的 SIEM 系统时，它们的价值会被放大。企业系统可能直接从分布式 SDP 组件接收反馈，也可能以分层方式部署多个收集代理。SIEM 系统通过将预定义和定制的事件转发到集中管理控制台或通过以电子邮件向指定的个人发送警报的形式执行检查并标记异常

因为 SDP 以审查身份和设备的方式控制访问，所以为 SIEM 系统提供比典型的网络和应用程序监视工具更为丰富的信息。SDP 实时提供有关每个连接的“谁、什么、在哪里”信息，从而增加了 SIEM 系统的价值。就这一点与 SIEM 系统当前用于日志记录的方式进行比较：安全分析人员必须将多个日志中的信息拼凑在一起识别未经授权的用户（“谁”），在识别从“什么”到“哪里”的未授权连接时非常具挑战性。但是，如果 SDP 客户端安装在用户的设备上，就可以从设备收集特定信息。所有从 SDP 网关丢弃的数据包都可以存储起来，以便进一步分析潜在的黑客企图或评估消耗。

这种级别的记录优于传统防火墙生成的 IP 地址和端口列表。SDP 还增强了 SIEM 系统关联跨多个设备发生的用户活动的能力。如果没有 SDP，以这种方式关联用户活动通常很难实现，特别是随着自带设备办公和移动设备（BYOD）的出现时更为困难。

将 SIEM 系统与 SDP 部署集成有助于实现将安全操作从被动操作转移到主动操作的目标。为了控制风险，现有的 SIEM 除了作为 SDP 日志信息的接收器之外，还应被视为重要的信息源。SIEM 系统可以通过断开用户连接、禁止来自未验证设备或某些主机的连接以及删除可疑连接帮助控制风险。例如，如果 SIEM 系统指示高于正常风险级别，指示未经授权的用户活动，则 SDP 将断开用户的所有连接，直到可以执行进一步的分析。SDP 通过在几秒钟内寻址和控制连接补充了 SIEM 系统的功能。

与所有生成日志信息的系统一样，SDP 日志产生了企业潜在的数据隐私问题。由于网络连接（及其元数据）可能与日志中的特定用户关联，因此组织需要在部署 SDP 期间采取预防措施解决此问题。

SDP 增强并提高了 SIEM 系统预防、检测和响应不同类型攻击的能力。下一页显示了可以减轻攻击类型的一些示例。（通过将 SDP 与 SIEM 集成可以预防的攻击的更详细列表将在未来的 CSA 出版物中给出。）

安全攻击类型	缓解措施	如何将 SDP 和 SIEM 集成
端口扫描/ 网络侦察	封锁并通知	SDP 阻止所有未经授权的网络活动，并可以记录所有连接请求以供 SIEM 系统使用。
拒绝服务 DDoS 攻击	封锁并通知	由于 SDP 受单包授权（SPA）保护，拒绝服务 DDoS 攻击在很大程度上无效。单包授权会丢弃坏数据包，这些数据包可以被记录到 SIEM 系统
恶意使用授权资源	检测和定位	SDP 允许授权用户访问授权资源，但 SIEM 系统可以分析用户活动是否存在异常行为，然后 SDP 可以禁止授权用户访问，直到可以执行进一步的分析。
使用被盗凭证	封锁并通知	SDP 在连接之前需要进行多因素验证，使得被盗密码不足以让攻击者获得访问权限。

传统防火墙

传统防火墙基于七层开放系统互连（OSI）模型，按照一组规则监控网络流量，其中 OSI 的第 2、3、4 层分别为：数据链路层（2）、网络层（3）、传输层（4）。它们遵循 5-元组 [14] 方法，该方法基于源和目标 IP 和端口过滤网络包数据，并定义流经连接的网络协议。防火墙还可以支持其他功能，例如网络地址转换（NAT）和端口地址转换（PAT）。

几十年来，防火墙一直是企业网络安全的支柱。但是，因为它们只是安全基础设施的一部分，并且只在 5 元组的有限世界中运行，确实存在诸多限制。通常，传统防火墙只能表示静态规则集，不能基于身份信息来表示或执行规则。

软件定义边界 SDP 使用防火墙或实现类似的网络流量强制功能，显著改善企业当前使用防火墙的方式。SDP 可以实现许多企业组织试图通过防火墙控制的网络访问控制。企业可以通过 SDP 大大减少防火墙规则集。SDP 可以抛开 5 元组的约束，对以身份为中心的访问控制进行建模，允许对访问控制进行更准确的表示和执行。除了减少在复杂环境中编写、测试、调试和部署防火墙规则所需的工作量，SDP 还支持更丰富和更精确的访问控制机制。

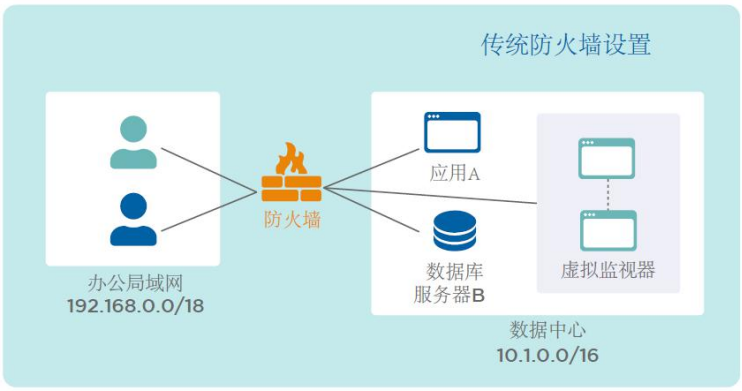


图 11: 传统防火墙设置

图 11 描述了在传统办公局域网环境下，通过单独的防火墙控制从用户子网（192.168.100.0/18）到当地的数据中心子网的连接，试图安全访问的困难性。

因为办公网上的各个用户仅仅通过 IP 地址标识，防火墙并不能区别他们。此外，很多用户定期地连接或断开其笔记本电脑，所有用户的 IP 地址会频繁变化。

一个典型的数据中心承载着包括测试和生产系统在内的大量负载。虽然一些应用是长期存活的并使用静态 IP 地址，但是另外的应用则部署在虚拟机之上，这些应用经常会被创建和销毁，因此 IP 地址不可预测。虽然没有一个用户需要访问数据中心中所有的服务器，甚至是这些服务器之上的所有端口，但实际上在这个环境中，防火墙有一个规则集会强制放行在办公局域网内的所有 IP 地址都可以访问在数据中心网络中的所有 IP 地址。相比于传统防火墙设置，图 12 中描述了一个简化的客户端到网关的 SDP 模型。为了清晰起见，忽略了控制器。另外需要说明，其他 SDP 模型部署也是类似的。

在这个例子中，网络防火墙已经被扮演相似功能的 SDP 网络代替 [15]。因为 SDP 基于明确的用户身份和他们使用的设备信息，所以 SDP 网关可以实现对数据中心访问的细颗粒度控制。这个开放的、扁平化的网络表示一个巨大的攻击面已经变得最小化了。注意，通过在数据中心服务器附近或者在其上增加更多的 SDP 网关可以实现对特定服务的更加细颗粒度的访问。（请查看第 15 页客户端到服务器的介绍）

在实际的部署中，防火墙仍在相应的位置之上，但是只设定最小权限规则集，例如：只能允许办公局域网的流量到 SDP 网关之上，然后 SDP 网关强制用户使用特定的设备连接特定的服务。

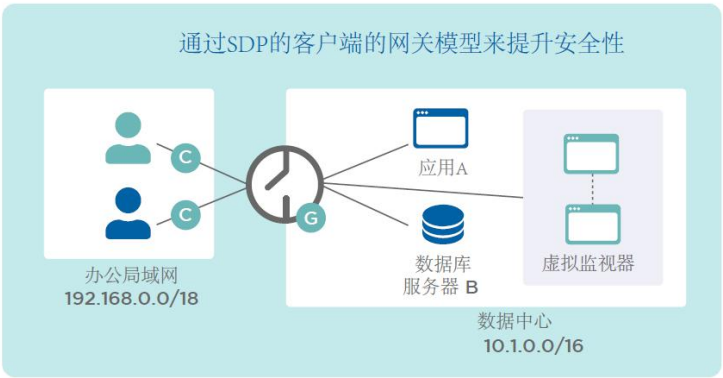


图12: 通过SDP的客户端的网关模型来提升安全性

入侵检测和入侵防御系统（IDS/IPS）

入侵检测和入侵防御系统（IDS/IPS）在这里被看成是同义词，是用作检测网络或系统恶意行为及策略违规的安全组件。它们是基于网络的（检查流量）或者基于主机的（检查活动和潜在的网络流量）。尽管需要更改基于 IDS 的网络，SDP 可以支持 IDS/IPS 系统的部署。在单网络远程办公室等小型运营环境中，部署 SDP 可以不需要部署 IDS/IPS，从而降低成本。

另外，因为 SDP 采用 mTLS 技术加密客户端和网关间的通信，所以对于 IDS 系统而言，网络流量变得不透明了。IDS 可以采用引入证书的方式代理 TLS 数据流，但这会带来增加攻击面的副作用[17]。通常，因为 SDP 是基于 mTLS（通常基于临时证书）通信的并且它可以反弹 IDS 扮演的中间人攻击（MITM），所以一般不会增加攻击面。

因为这些逻辑连接通过 SDP 证书进行加密处理，这些连接的 mTLS 分段（图中蓝色标识）对于任意的外部系统是不透明的。同时，在设计上，尝试做流量分析的系统也不能访问这些连接。这个变化对于中间安全和网络监控系统有一定影响，特定使用场景不再适用，这个情况和从 TLS1.2 升级到 1.3 类似。[18]（对于每种 SDP 部署模型的图形化展示请参考第 21 页“SDP 连接安全”一节）

此外，SDP 支持把未加密的网络数据流（例如：被丢弃的数据包）推送到远端 IDS 设备。另外，基于本地部署的 IDS 要比基于网络部署的 IDS/IPS 更能增强安全操作。当然，SDP 并非是影响基于网络的 IDS 的唯一趋势。应用向云端迁移也提升了基于云部署的 IDS 的有效性和使用。

虽然部署 SDP 系统可能会需要对 IDS 系统带来一定的变更，但通过阻止未认证的网络流量的方式有助于降低系统噪声。这种改变使得 IDS 及其操作团队更关注已授权应用的网络流量，同时把资源有效倾斜到内部威胁检测方面。

SDP 同样也可以简化和增强“蜜罐”系统的创建和有效性。因为所有的被保护系统针对攻击者而言都是不可见的，而 SDP 就增加了恶意攻击者发现和攻击蜜罐的可能性。一个基于 SDP 的“蜜罐”系统可以更快定位网络上的恶意软件行为。

虚拟专用网（VPNs）

VPN 用于跨越非可信的公用网络构建一个安全的访问连接。VPN 通过被用作远程访问（例如：外出的员工访问公司站点），安全的内部通讯，甚至是在不同公司之间通信（点到点的外部网）。VPN 通常使用 TLS 或者 IPSec 方式。[19]

虽然可以使用 VPN 封装和加密网络流量，但使用 VPN 会遇到一些限制，而 SDP 可以更好的解决这些问题。虽然 VPN 的授权成本可能很低，但是其运维需要投入大量的人力。VPN 通常提供广泛的、过于宽松的网络访问能力。VPN 的典型使用方式是只提供基于子网范围等方式的基本访问控制能力。在很多组织机构这些限制代表了安全和合规性方面的风险。在分布式的网络环境中，VPN 可能会将用户的大量不必要的流量都导到企业的数据中心，加重企业的带宽成本以及网络延迟。VPN 服务器作为一个服务是暴露在公共互联网上，其可见性将导致容易被攻击者攻入。

此外，VPN 给用户带来了相当大的负担和较差的用户体验。用户被要求记忆哪些应用需要使用 VPN 访问，哪些不需要，同时，他们也被要求手动连接或者断开 VPN。对于那些有多个远程地点需要登录的用户来说，VPN 无法支持同时连接，而是要求在不同环境之间进行切换。只要涉及云业务迁移，VPN 的管理就爆炸式地变得复杂，使得 IT 管理员需要在不同的物理节点之间配置和同步 VPN 和防火墙访问策略。这种操作的复杂度使得消除过期的访问权限更为困难。

替代 VPN 是 SDP 最基本的目标。和 VPN 类似，SDP 同样要在客户端设备上部署一个客户端。通过使用 SDP 代替 VPN，组织机构可以对远程用户、内部用户、移动设备用户等提供同一套访问控制平台。也正是因为 SDP，尤其是那些部署在互联网上的 SDP 设备，通过 SPA（单包认证）技术和动态防火墙技术，可以比传统的 VPN 服务器抵御更多的攻击。

下一代防火墙（NGFW）

一般而言，NGFW[20] 具备传统防火墙的能力，同时添加了额外的属性使得他们成为了“下一代”。NGFW 基于预定义的规则策略监视访问并检测网络数据包，并且用 OSI 模型 2 到 4 层的数据信息过滤数据包。NGFW 同样也使用 5 到 7 层（会话层、表示层、应用层）增加额外的功能。

NGFW 提供如下的能力，不同的供应商会有所差异：

- **应用识别：**根据应用决定进行何种攻击扫描
- **入侵检测（IDS）：**监视网络的安全状态
- **入侵防护（IPS）：**为了阻止安全漏洞而拒绝通信
- **身份识别（用户和组控制）：**管理用户可以访问的资源
- **虚拟专用网（VPN）：**NGFW 可以提供在不信任网络上的远程用户的访问能力

虽然 NGFW 相比传统防火墙有很大提升，但与 SDP 相比仍然存在一些限制：

- 时延：和任何的 IDS/IPS 一样，会对网络流量造成额外时延，在执行文件审查时尤其如此。
- 可扩展性：需要很多硬件资源进行弹性扩展
- 规则复杂度：一些 NGFW 厂家提供了用户和分组属性等相关的身份识别能力，但是这些能力的配置很复杂。

SDP 是已经部署的 NGFW 的天然补充。企业可以使用 SDP 确保用户访问策略，同时使用 NGFW 进行核心防火墙保护，使用 IDS/IPS 进行流量监测。SDP 和 NGFW 进行集成后带来的好处包括：强制实现不可见，并使得 NGFW 更加动态（后续章节会有详细描述）。虽然将 NGFW 和 IAM 或 AD 集成同样可以强化用户访问策略，但是使用 SDP 可以提供可控的、真正安全的连接。

在某些情况下，NGFW 的架构和 SDP 存在竞争和重叠。在过去一段时间里，NGFW 厂商已经成功地、创新式的解决了 SDP 范围内的一些问题。通过组合使用 NGFW 和 VPN 并配以用户和应用识别，企业可以在一定程度上实现 SDP 的许多目标。但是，在架构设计实现方面，这种方案和 SDP 的实现不同。NGFW 是基于 IP 地址的，而 SDP 是基于连接的。NGFW 可以提供有限的身份认证和以应用为中心的功能。NGFW 的访问模型是典型的粗颗粒度方式，提供给用户比他们严格需要更广泛的访问能力。相比 SDP，NGFW 提供了较少的针对外部系统的访问决策动态管理能力。比如说：SDP 系统可以只允许开发人员在经过批准的变更管理窗口期访问开发用服务器。SDP 有能力强化逐步认证，但通常 NGFW 不支持这一点。

NGFW 仍然还是防火墙，所以还是工作在传统的以边界为中心的体系架构下站点到站点连接的场景中。SDP 部署通常支持更加分散和灵活的网络，从而具备灵活地网络分段能力。SDP 是基于 Need-to-know“需知”（白名单）的安全方式设计的，这样就可以屏蔽未授权的用户和未授权的设备的未授权访问服务。SDP 使用 SPA 和动态防火墙技术保护和隐藏认证的连接。NGFW 则在一个高度暴露的环境中进行相关操作。

身份及访问管理 (IAM)

IAM 系统为用户和设备提供了验证其身份(通过身份验证)的机制，并存储关于这些身份的管理属性和组成员关系。SDP 体系结构旨在与现有的企业 IAM 提供者集成，例如 LDAP、活动目录（Active Directory）和安全断言标记语言（SAML）等。

SDP 的控制访问通常基于 IAM 属性和组成员关系以及用于连接的设备的属性等因素。用户和设备授权的组合有助于建立更细颗粒度的访问规则，进行授权或予以限制，确保只有授权设备上的授权用户才能对授权应用程序进行访问。

SDP 与 IAM 的集成不仅用于初始用户身份验证，还用于加强身份验证，例如提示使用动态口令（OTP）

访问敏感系统，或者在某些情况下(例如远程访问与本地访问)加强验证。IAM 系统还可以通过应用程序编程接口（API）调用 SDP 进行通信，响应身份的生命周期行为，例如禁用帐户、更改组成员、删除用户连接或更改用户角色。

在 SDP 中使用 IAM 对用户进行身份验证，为 SDP 提供用于做出授权决策的信息，并对用户从注册设备发出的所有授权访问提供丰富的审计日志。将应用程序访问(不是网络访问)与用户(而非 IP 地址)绑定在一起，可以为日志记录提供有用的连接信息，并在出于安全或合规性原因需要审计历史访问记录时显著降低 IT 开销。

IAM 工具通常关注维护身份生命周期的业务流程，并对如何使用身份信息控制对资源的访问进行标准化。例如，授予用户访问的机制通常是手动和自动流程的组合。因此这些流程依赖于由 IAM 工具管理的身份属性和组成员关系，所以 SDP 支持这些流程。当用户属性或组成员关系发生更改时，SDP 会自动检测这些更改，并在不更改 IAM 流程的情况下更改用户访问权限。

SDP 与 SAML 可以集成 [21]。在 SDP 的部署中，IAM 提供者可以充当用户属性的身份提供者和/或身份验证提供者(例如多因子认证)。除了 **SAML 之外**，还有许多开放身份验证协议，如 OAuth[22]、OpenID Connect[23]、W3C Web 身份验证 (WebAuthn)[24]、和 FIDO Alliance Clientto-Authenticator 协议(CTAP)。[25](这些协议将在未来与 SDP 相关的研究中进行探索。)

21 https://en.wikipedia.org/wiki/Security_Assertion_Markup_Language
22 https://en.wikipedia.org/wiki/OAuth and https://oauth.net/
23 https://en.wikipedia.org/wiki/OpenID_Connect
24 https://www.w3.org/TR/webauthn/
25 https://fidoalliance.org/specs/fido-v2.0-id-20180227/fido-client-to-authenticator-proto- col-v2.0-id-20180227.html and https://fidoalliance.org/fido2/
26 https://en.wikipedia.org/wiki/Network_Access_Control

网络准入控制(NAC)解决方案

NAC 解决方案通常控制哪些设备可以连接到网络，以及哪些网络主体可被访问。这些解决方案通常使用基于标准的硬件(802.1X)和软件来验证设备，然后授予设备访问网络的权限，这些操作运行在 OSI 模型的第 2 层。

当设备首次出现在网络上时，NAC 执行设备验证，然后将设备分配给网络段(VLAN)。在实际中，NAC 将设备粗略地分配给少量网络。大多数组织只有几个网络，比如“访客”、“员工”和“生产”。由于 NAC 运行在网络的第 2 层，它们通常需要特定的网络设备，不能运行在云环境中，也不能远程使用。

SDP 是一个集成了用户和设备访问的 NAC 的现代化解决方案。然而，在某些环境中使用 NAC 是有意义的——例如，像打印机、复印机、固定电话和安全摄像头这样的硬件设备。这些设备通常内置 802.1X 支持，不支持安装 SDP 客户端。通过 SDP 网关到网关模型来保护这些设备并控制用户对它们访问是一个更好的选择，也是未来 SDP 研究的一个主题。

终端管理(EMM/MDM/UEM)

许多企业使用终端管理系统，通常分为企业移动化管理(EMM)、移动设备管理(MDM)或统一端点管理(UEM)。这些是企业 IT 和安全的重要元素，它们的价值和重要性通过 SDP 部署得到增强。

终端管理系统可用于跨用户设备自动化分发和安装 SDP 客户端。由于这些系统通常使用与 SDP 相同的身份及访问管理系统，因此可以紧密协调部署以简化用户体验。这些系统通常还提供了功能丰富的设备自检和配置评估功能。SDP 可以对设备管理平台进行 API 调用，获取特定设备的信息，然后根据这些信息做出动态访问决策。

或者，没有部署终端管理系统的企业组织可以直接利用软件定义边界 SDP 来管理和控制设备。

Web 应用防火墙(WAF)

Web 应用程序防火墙(WAFs)用于过滤、监视和阻止 Web 应用程序进出的 HTTP(S) Web 流量。Web 应用程序防火墙检查应用程序协议的流量，阻止源于应用程序安全漏洞的攻击，如 SQL 注入、跨站点脚本(XSS)和文件包含 [27]。Web 应用程序防火墙尽管通常在用户和应用程序之间以类似于入侵检测（IDS）/入侵防御（IPS）的方式联机运行，但却不是网络访问控制或网络安全解决方案。Web 应用程序防火墙主要检查 HTTP(S)协议流量，检测并阻止恶意内容。

Web 应用程序防火墙是 SDP 的补充。例如，在客户端到网关模型中，Web 应用程序防火墙部署在 SDP 网关之后，在从 SDP 的 mTLS 隧道中提取本地 Web 应用程序流量之后，对流量进行操作。在客户机到服务器和服务器到服务器模型中，Web 应用程序防火墙与服务器上的 SDP 网关集成，以便对检查的 HTTP 流量进行进一步分布式控制。

负载均衡

负载均衡是许多网络和应用程序架构的一部分。负载均衡包括基于 DNS 和基于网络的解决方案，架构师需要在规划 SDP 部署时了解企业组织如何使用它们。

例如，基于网络的负载均衡通常联机部署在网络上，类似于上面讨论的 WAF 一样位于客户机和服务器之间，可能无法检查 SDP 组件之间的 mTLS 连接。SDP 部署和负载均衡方法的细节需要仔细分析，确保可以最大限度地部署 SDP。

云访问安全代理 (CASB)

CASB 位于云服务用户和云应用程序之间，监视与安全策略的执行相关的所有活动。它们提供各种各样的服务，包括监视用户活动、警告管理员潜在的危险行为、强化安全策略合规性和自动防止恶意软件。CASB 既能位于用户和云服务之间，也能使用 SaaS API 的方式部署于 SaaS 系统内部，这取决于供应商和 SaaS 平台对 API 的支持水平。

CASB 功能通常不与 SDP 功能重叠，因为 CASB 通常在第 7 层(应用层)操作，检查应用程序流量。CASB 通常不提供网络安全或访问控制。但是，还是可以通过 SDP 进行数据保护和用户行为分析，从而简化其运维。

基础设施即服务 (IaaS)

IaaS 平台的安全性是围绕行业标准的“共享责任”模型构建的 [29]，其中云提供商承担一定的责任(云自身的安全性)，而客户负责保护其应用程序(云上的安全性)。IaaS 中客户使用云网络安全组 [30] 控制对其云资源的访问。这些网络安全组作为简单的防火墙配置和使用。这些安全措施可以与软件定义边界 SDP 集成，创建一个更加健壮的安全环境。

软件即服务 (SaaS)

Salesforce.com 和 Office 365 等 SaaS 应用程序是多租户的，并可以在公共互联网上公开访问。目前，防止未经授权的用户进行网络级访问并不是这些系统的目标。组织机构可能希望在采用 SaaS 应用程序时加强安全性，原因如下:

- 确保只有授权设备上的授权用户才能访问该特定组织租用的 SaaS
- 确保 SaaS 应用程序使用管理的企业 IAM 身份凭证进行身份验证
- 确保用户访问 SaaS 应用程序时强制进行多因子身份验证
- 确保对 SaaS 应用程序访问的所有行为都被识别并记录

越来越多的 SaaS 供应商认识到他们的企业客户想要“限制源 IP 地址和设备”功能。这些特性在软件定义边界 SDP 和传统 VPN 上同样有效，并使 SaaS 客户能够限制用户通过特定的 IP 地址访问(登录和使用)他们的域(租用的服务)。对于软件定义边界而言，源 IP 是系统(网关)的一个元素，用户流量通过它进行路由、被授权或被拒绝。

平台即服务 (PaaS)

与标准硬件或基于 IaaS 的系统相比，PaaS 产品允许企业以更小成本构建和部署定制应用程序。与 IaaS 和 SaaS 不同，对 PaaS 系统的网络访问控制(以及 SDP 的相关程度)取决于 PaaS 提供者提供的功能以及启用外部访问控制的方式。

然而，主要的 PaaS 提供者的 PaaS 和 IaaS 平台支持相同的网络安全模型。例如，微软 Azure PaaS 安全模型通过 Azure 网络安全组支持源 IP 地址限制。谷歌云平台 App Engine 和亚马逊 Elastic Beanstalk 也可以

- 部署不同的 SDP 模型，这取决于 PaaS 应用程序是什么以及需要保护哪些连接。

治理、风险管理及合规(GRC)

治理、风险管理和合规（GRC）[36]通常是企业整体安全框架的一部分，帮助确保组织实现安全目标并行事正直。GRC 系统通常通过购买的治理、风险管理及合规软件 [37] 实现，通过标准和指南(如 SOX、PCI 等)定义并强化对包括 IT 在内的许多组织系统的控制。

SDP 可以通过强制执行和记录 GRC 系统所需的访问控制的方式与 GRC 系统交互并支持 GRC 系统。例如，GRC 系统可能要求生产系统与非生产系统隔离，并记录所有用户对生产系统的访问。软件定义边界可以执行这种网络分割，并且可以为 GRC 系统提供审核日志进行验证。

公钥基础设施(PKI)

公钥基础设施(PKI)是“创建、管理、分发、使用、存储和吊销数字证书，以及管理用于加密、解密、散列和签名的私有和公共密钥所需的一组角色、策略和过程”。 SDP 可以使用 PKI 生成 TLS 证书和安全连接。即使不存在公钥基础设施，SDP 也可以提供 TLS 证书保护连接 [39]。现有的 PKI 是 SDP 的一个自然集成点，因为它们可被 SDP 用于生成证书以及验证用户身份。

软件定义网络(SDN)

软件定义网络是通过 API 驱动 IT 网络基础设施，用于协调 IT 网络内的网络导流。SDN 支持高效的网络配置，提高性能和监测能力。软件定义网络的重点是流量效率，而不是安全性和授权。运行良好的 SDN 系统为企业提供可靠、高效和自适应的网络带宽。

无论底层网络基础设施如何，SDP 协调网络上对象之间的连接。SDP 可以与 SDN 集成在一起从而获得部署 SDN 带来的益处，但这种集成不是必须的。例如可以把 SDP 和 SDN 的控制器集成在一起。SDN 还可以为加密的、非透明的 mTLS 连接提供 QoS。

无服务器计算模型

随着计算模型的发展，安全工具和体系结构也必须随之发展。一个例子是“无服务器”计算模型 [41] 的增长，云提供商提供了在“函数即服务”模型中运行自定义代码或在“无服务器数据库”中预构建代码集的能力。

“函数即服务”模型可以向整个互联网公开通用公共节点，并使用 API 密钥控制身份验证和授权。在这种情况下，因为这些接口被设计为公共的，SDP 模型将不适用。然而，其他服务(或其它云提供商)可能选择遵循不同的安全模型，其中每个客户都有自己的专用接入点实现“作为服务”功能。在这样的模型中，可以使用 SDP 网关保护私有接入点的安全。

架构关注点

虽然 SDP 所涉很广，可以涵盖大量的网络访问场景，但它并不能解决所有的安全问题。这些领域不在关注的范围之内：

- 保护或控制对公共网络服务(例如不需要身份验证的网站)的访问——SDP 更适合会员制的服务（针对特定人群）
- 终端防护
- 某些计算模型，如无服务器计算
- 特别的网络连接拓扑，如点对点，取决于 SDP 部署模型(参见第 19 页的“SDP 部署模型和相应场景”)

29 https://aws.amazon.com/compliance/shared-responsibility-model/ and https://blogs.msdn.microsoft.com/azuresecurity/2016/04/18/what-does-shared-responsibility-in-the- cloud-mean/
30 https://docs.aws.amazon.com/vpc/latest/userguide/VPC_SecurityGroups.html and https://docs.microsoft.com/en-us/azure/virtual-network/security-overview
31 https://downloads.cloudsecurityalliance.org/assets/research/sdp/sdp_for_iaas.pdf
32 https://en.wikipedia.org/wiki/Platform_as_a_service
33 https://docs.microsoft.com/en-us/azure/security/security-paas-deployments
34 https://cloud.google.com/vpc/docs/firewalls
35 https://aws.amazon.com/premiumsupport/knowledge-center/security-group-elastic-beanstalk/ and https://docs.aws.amazon.com/elasticbeanstalk/latest/dg/using-features.managing.ec2.html
36 https://en.wikipedia.org/wiki/Governance,_risk_management,_and_compliance
37 https://searchcio.techtarget.com/definition/GRC-governance-risk-management-and-compliance-software
38https://en.wikipedia.org/wiki/Public_key_infrastructure
39https://cloudsecurityalliance.org/download/software-defined-perimeter-glossary/
40https://en.wikipedia.org/wiki/Software-defined_networking
41https://en.wikipedia.org/wiki/Serverless_computing

结论

当今，企业和政府机构都面临着信息安全的严峻挑战，必须采取更有效的方法保护数据资产。SDP 为组织机构的安全专业人员提供他们寻求的工具，为稳健的企业开发、操作、安全提供健壮的、可适应的、可管理的基础架构。我们希望本文能帮助安全人员更好地理解 SDP 体系结构是如何工作的，以及如何将其部署到他们独特的环境中。

当然，我们的工作并不止于此。未来我们将涉及更多的主题研究，包括上文提到的离散 SDP 部署模型以及集成的文章，以及 SDP 对各种业务的收益的详细解读，基于 SDP 部署的合规控制映射工具，以及更多的出版物。

最重要的是我们认识到我们没有所有的答案，我们诚挚邀请您加入我们的 SDP 工作组参与讨论，并做出贡献。作为支持安全、开放和可用的互联网的安全人员，为道德所激励的人，我们努力工作确保一个更美好的未来。我们希望你能加入我们的旅程。更多参与信息请关注。

国际云安全联盟 SDP 工作组：
https://cloudsecurityalliance.org/working-groups/softwaredefined-perimeter/.

中国云安全联盟 SDP 工作组：
https://www.c-csa.cn/ruanjiandingyibianjieSDP.html

附录 1：
参考文献

Software-Defined Perimeter Working Group: SDP Specification 1.0.Brent Bilger, Alan Boehme, Bob Flores, Zvi Guterman, Mark Hoover, Michaela Iorga, Junaid Islam, Marc Kolenko, Juanita Koilpilla, Gabor Lengyel, Gram Ludlow, Ted Schroeder, and Jeff Schweitzer (CSA, 2014 年 4 月)

《SDP 标准规范 1.0》
Software-Defined Perimeter for Infrastructure as a Serviceby Jason Garbis and Puneet Thapliyal (CSA, 2016)

《SDP 在 IaaS 中的应用》
Software-Defined Perimeter Working Group Glossary," Cloud Security Alliance (CSA, 2018)

《SDP 工作组术语》
Zero Trust Networks: Building Secure Systems in Untrusted Networks," Evan Gilman and Doug Barth (2017 年 6 月)

《零信任网络：在非受信网络中构建安全体系》
http://shop.oreilly.com/product/0636920052265.do

"fwknop: Single Packet Authorization > Port Knocking," Michael Rash
fwknop:单包授权>端口碰撞

http://www.cipherdyne.org/fwknop/
Open Source Software-Defined Perimeter," Waverley Labs

开源 SDP
http://www.waverleylabs.com/open-source-sdp/

附录 2：

SDP 详解

下面是 SDP 1.0 标准规范中定义的 SPA 包格式。

密文	Nonce 临时随机数	防止接受过期的 SPA 包
	Timestamp 时间戳	最常见的:服务访问请求
	Message Type 消息类型	可能弃用：访问请求，NAT 访问请求，网关命令消息
	Message String 消息串	被允许的源 IP 地址，打开的目标服务 ID(s)
	Optional Fields 可选字段	注意：网关知道打开哪个端口，是否和向哪里转发连接
	Digest 摘要	注意：可能用于请求服务流量隧道
明文	HMAC	在加密之前，这个 SHA256 哈希是在消息的密文部分上计算的，然后由服务器在成功解密消息后用于验证消息完整性。

对于该规范的一个改进意见是增加一个明文客户端 ID，以便更高效处理进入的数据包。目前二进制 SPA 格式正在被设计中，而且描述该格式的 RFC 文档也会被创建。

SPA 作为单个 UDP 数据包发送是最有效的。但在某些场景中是不可行的，因为（某些）网络环境可能会阻止一些或所有传出的 UDP 数据包。在这种情况下，可以通过 TCP 连接发送 SPA 包。这在技术上违反了 SPA 的“单包”特性，但有时从实际出发考虑是必要的。

SPA 包也可以通过连接机器或其他设备发送。这种做法的一个例子就是移动设备被用于代表台式计算机发送 SPA 包。在某些场景中，尤其在阻止 UDP 包的网络环境中这也是一个合理的变通方案。