软件定义边界(SDP)和零信任

cloud security alliance®

SDP 工作组官网地址：https://www.c-csa.cn/ruanjiandingyibianjieSDP.html
https://cloudsecurityalliance.org/software-defined-perimeter/

@2020 云安全联盟-保留所有权利。你可以在你的电脑上下载、储存、展示、查看、打印及，或者访问云安全联盟官网（https://cloudsecurityalliance.org）。须遵守以下: （a）本文只可作个人、信息获取、非商业用途；(b) 本文内容不得篡改; (c)本文不得转发; (d)该商标、版权或其他声明不得删除。 在遵循美国版权法相关条款情况下合理使用本文内容，使用时请注明引用于云安全联盟。

致谢

主要作者：

Juanita Koilpillai

Nya Alison Murray

贡献者：

Michael Roza

Matt Conran

Junaid Islam

Aditya Bhelke

Eitan Bremier

Tino Hirschmann

Steve Swift

Sam Heuchert

John Markh

Roupe Sahans

Oscar Monge Espana

Gerardo Di Giacomo

Vladimir Klasnya

J. Lam

Clara Andress

Dan Mountstephan

Manoj Sharma

CSA 分析师：

Shamun Mahmud

CSA 全球员工：

AnnMarie Ulskey (Design)

©2020 云安全联盟-版权所有

中文版翻译说明

由云安全联盟大中华区（CSA GCR）秘书处组织翻译《软件定义边界和零信任》(Software-Defined-Perimeter-and-Zero-Trust)，云安全联盟大中华区专家翻译并审校。

翻译审校工作专家：（按字母顺序排序）

组长：陈本峰（云深互联）、郑大义（万物安全）

组员：崔泷跃、高巍、靳明星（易安联）、杨正权（易安联）、姚凯、于乐、余晓光（华为）

在此感谢以上参与该文档的翻译审校工作的专家及工作人员。如译文有不妥当之处，敬请读者联系 CSA GCR 秘书处给与雅正！联系邮箱：info@c-csa.cn；云安全联盟 CSA 公众号：

©2020 云安全联盟-版权所有

序言

2010 年，原 Forrester 副总裁兼分析师，现 Palo Alto Network CTO 兼 CSA 大中华区顾问 John Kindervag 以“永不信任，始终验证”思想提出零信任模型 Zero Trust Model，零信任概念开始得到业界关注并被广泛认可。2013 年，云安全联盟 CSA 提出 SDP（Software Defined Perimeter）软件定义边界，成为零信任的第一个解决方案，由组长 Bob Flores（原美国 CIA 的 CTO）和包括 CSA 大中华区研究院专家在内的 CSA SDP 工作组制定编写并发布了 SDP Spec 1.0 等研究成果并提出零信任的 ABCDE 原则，在 RSA 安全大会上 CSA SDP 挑战赛从未被黑客攻破。2019 年，美国国家标准与技术研究院 NIST 主导，并由包括 CSA 大中华区研究院专家在内的业界众多安全专家参与，制定、编写并发布了 NIST SP 800-207 ZTA 零信任架构草案， 被全球业界一致认为是零信任架构的标准。NIST ZTA 属于参考架构，它明确提出企业实现零信任的解决方案包括软件定义边界 SDP，增强的身份治理 IAM，及微隔离 MSG。

本文中，CSA 全球 SDP 工作组和 CSA 大中华区 SDP 工作组的多位专家们对 SDP 如何实现零信任的战略、价值、实施等内容做了原创和翻译，相信对广大的安全专家、CIO、CISO 和公司业务高管在考虑企业的零信任落地时会有启示和帮助。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

©2020 云安全联盟-版权所有

目录

©2020 云安全联盟-版权所有

引言

软件定义边界（Software Defined Perimeter, SDP）是一个能够为 OSI 七层协议栈提供安全防护的网络安全架构。SDP 可实现资产隐藏，并在允许连接到隐藏资产之前使用单个数据包通过单独的控制和数据平面建立信任连接。使用 SDP 实现的零信任网络使组织能够防御旧攻击方法的新变种，这些新变种攻击方法不断出现在现有的以网络和基础设施边界为中心的网络模型中。企业实施 SDP 可以改善其所面临的攻击面日益复杂和扩大化的安全困境。

最初，零信任网络（ZTN）概念是由美国国防部（DoD）在 2000 年代初开发的，同时定义了全球信息网格（GIG）网络运营（NetOps）黑核（BlackCore）路由和寻址架构，这是国防部以网络为中心的服务策略的一部分。随着时间的流逝，此概念在 DoD 情报和安全社区内演变为当前的 ZTN / SDP 框架和测试实验 [1]。同时，市场咨询公司 Forrestrer 开始推广 ZTN，指出 ZTN 是企业安全团队值得考虑的技术。 如今，零信任在采用率和范围方面都得到了广泛的进步。

在题为“ Zero-Trust-eXtended-ZTX-Ecosystem”的报告中，Forrester 分析师观察到网络边界正在变化的规律，这导致了零信任架构很快从“跨位置和托管模型的网络安全隔离”思想中诞生。Forrester 断言，当前模型可应对挑战和消除当前安全策略中固有的信任假设的需求。它还指出应考虑使用各种新的基于自适应软件的方法。但是，它并没有为“扩展的生态系统框架”确定新的方向 [2]。

从本质上讲，零信任是一种网络安全概念，其核心思想是组织不应自动信任传统边界内外的任何事物，并旨在捍卫企业资产。实施零信任需要在授予访问权限之前验证所有尝试连接到资产的事物，并在整个连接期间对会话进行持续评估。如图 1 所示，美国国家标准与技术研究院（NIST）描述了使用“信任边界”。

1 https://www.secureworldexpo.com/industry-news/pentagon-zero-trust-security-framework
2 https://www.em360tech.com/wp-content/uploads/2019/04/The-Forres-er-Wave%E2%84%A2_-Zero-Trust-eXtended-ZTX-Ecosystem-Providers-Q4-2018-1-1.pdf

©2020 云安全联盟-版权所有

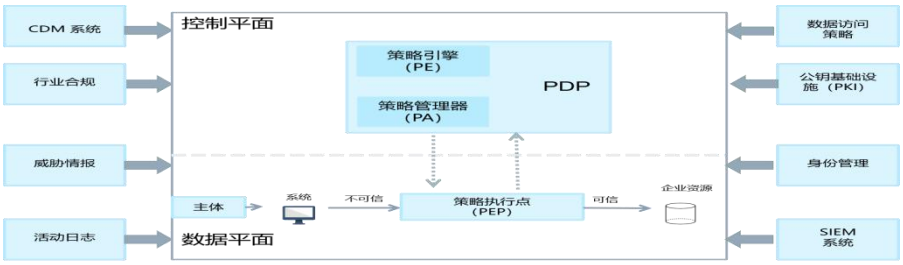

图 1：来源：NIST，800-207，零信任架构第二版草案 https://csrc.nist.gov/publications/detail/sp/800-207/draft

什么是零信任呢？根据 Forrester 的研究，零信任概念有三个要点：

- 向网络引入信任的概念，以确保资源永远可以被安全地访问，无论是谁创建流量或流量来自何处，无论在任何位置或者使用何种托管模型，无论是在云上、私有部署、或者混合部署的资源。
- 采用最小授权策略（LPS）来实施访问控制，以消除访问禁用资源的人性诱惑。
- 持续记录用户流量并分析检查是否存在可疑活动。

什么是 SDP？软件定义边界（SDP）是零信任策略的最高级实现方案。云安全联盟 CSA 已采用并倡导将以下结构应用于网络连接：

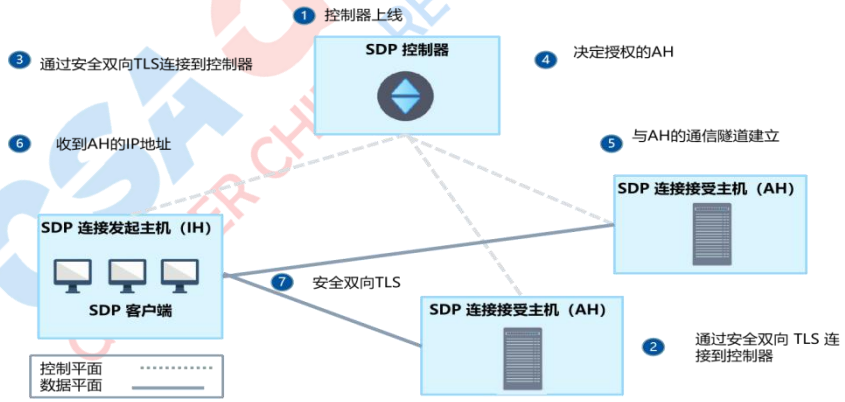

图 2：SDP 架构（来自 CSA SDP 规范 1.0）

- 将建立信任的控制平面与传输实际数据的数据平面分开。
- 使用动态全部拒绝（deny-all）防火墙（不是完全 deny-all，而是允许例外）来隐藏基础架构（例如，使服务器变“黑”，不可见）-丢弃所有未经授权的数据包并将它们用于记录和分析流量。
- 访问受保护的服务之前，通过单包授权（SPA）协议来认证和授权用户以及验证设备。-最小授权在此协议中是自带的。

©2020 云安全联盟-版权所有

由于 SDP 对于底层的基于 IP 的基础架构是透明的，并且基于该基础架构保证所有连接的安全，而且它可以部署在 OSI / TCP / IP 传输层协议之前的网络层并在会话层的应用之前，因此它是采用零信任策略的最佳架构。这一点很重要，因为传输层可以为应用程序提供主机到主机的通信服务，而会话层是终端应用程序进程之间打开、关闭和管理会话的机制。两者都有已知的和未发现的弱点，例如 TLS 漏洞和建立会话时的 TCP/IP SYN-ACK 攻击。下表将 ISO 开放系统互连（OSI）模型与 Internet 工程任务组（IETF）TCP / IP 协议相关联。

#	OSI 层	TCP/IP 层	协议数据封装	描述
7	应用层	应用层	数据	网络进程到应用
6	表示层		数据	数据表示和加密
5	会话层		数据	主机间通信
4	传输层	传输层	段	端到端连接和可靠性
3	网络层	网络层	包	路径确定寻址
2	数据链路层	数据访问层	帧	物理寻址
1	物理层		字段	媒介、信号和二进制传输

图 3：来源：https://www.iso.org/ics/35.100/x/ ， https://tools.ietf.org/html/rfc1180

目标

本文将展示如何使用 SDP 来实现 ZTN，以及为什么将 SDP 应用于网络连接，以及为什么是最先进的 ZTN 实现。

读者

安全专家、CIO、CISO 和其他公司高管正在考虑将“零信任”技术作为有效防御大规模违规行为的防护措施，是本文的目标读者。

零信任网络和 SDP

安全行业承认现有的防御机制只能解决部分问题。SDP 可以在 TCP / IP 和 TLS 之前执行，从而减少了威胁参与者将易受攻击的协议作为攻击向量的可能性。符合 CSA SDP 第一版规范的软件定义边界实现了零信任，可以阻止常见的 DDoS、

©2020 云安全联盟-版权所有

凭证盗用以及 OWASP 发布的著名的十大威胁等攻击方法。SDP 是已被证明的零信任实践方案，它可以使资产是隐藏不可见的，直到与访问者关联的身份被成功验证并授权。

实际上，“零信任”是位于 SDP 架构背后的理念。 SDP 的基本原则是 ABCD：“A 不假设任何事（Assume nothing），B 不相信任何人（Believe nobody），C 检查所有内容（Check everything），D 阻止威胁（Defeat threats）。” 尽管 SDP 零信任被应用在 ISO OSI 模型的第 3 层网络层上，但鉴于常见的架构模式（例如访问混合云服务的应用程序），在将零信任网络部署在尽可能接近域边界的位置时必须小心，要确保最佳的性能并防止不必要的服务延迟。

为什么需要零信任

当今的网络安全实施类似于建筑物的墙和门，犯罪分子可能尝试开门撬锁。如今，组织依赖其安全“门锁”，并进行严密监控确保犯罪分子不会闯入。最好是围护数字资产，然后通过威胁阻止未经授权的用户。我们可能想看看谁在敲门，但为了防止恶意行为绝对不要让坏人有可以碰到锁的机会。这就是为什么迫切需要有效的零信任部署的本质所在。此外，众所周知，威胁参与者的主要目标是渗透进网络并横向移动，从而访问具有更高特权凭证的系统。零信任可以防止未经授权用户的隐藏活动，从而将访问限制在授权用户。

下列问题要求快速更改网络安全性的实现方式。

a）不断变化的边界

传统范式下，网络边界固定，受信任的内网受负载均衡和防火墙之类的网络设备保护，但这个范式已被虚拟网络取代并且过去的网络协议也被认为不是原生安全的。实际上，许多当前的网络协议（例如 IPSec 和 SSL VPN）都存在已知的漏洞 3。 此外，大量的移动和物联网设备对传统固定网络中边界网络的本质带来了挑战。

随着云的引入，环境已经发生了变化。除了云之外，BYOD 的要求、机器到

©2020 云安全联盟-版权所有

机器的连接、远程访问的增加和网络钓鱼攻击的增加都使得传统方法不断受到挑战。企业有许多内部设备，以及各种各样的用户。一个常见的用例是现场承包商必须访问内部和云中的网络资源。混合架构也正在发展，在这种架构中，企业工作站通过云赋能异地客户和合作伙伴处的员工可以共用站点设施。此外，在这些情况下，通过站点到站点的连接（包括与第三方的互连）重新定义了域边界。

b）IP 地址挑战

今天一切都依赖于对 OSI 网络堆栈 1-4 层上 IP 地址的信任，但这带来了一个问题：IP 地址缺乏任何类型的用户信息来验证设备请求的完整性。IP 地址根本无法拥有用户上下文信息。IP 地址仅提供连接性信息，但不对终端或用户的可信度提供指示。TCP 是 OSI 网络堆栈第 4 层上的双向通信协议，因此与外部不可信主机进行通信的内部可信主机可以接收到不可信消息。

IP 地址的任何更改都可能意味着复杂的配置，从而允许错误在网络安全组和网络访问控制列表中蔓延。被遗忘的内部主机可以通过默认响应过去的协议（如 ICMP 网络支持）为黑客提供入口。最后，IP 地址会动态分配，或者当用户从一个位置移至另一个位置时会发生变化，因此不应用作网络位置的基准。

c）实施集成控制的挑战

网络连接的可见性和透明性对于网络安全性和安全工具的实现存在问题。当前，对控制的集成是通过收集多个日志中的数据并转发给安全信息与事件管理（Security Information & Event Management, SIEM）或安全编排自动化响应（Security Orchestration Automation Response, SOAR）技术分析。

网络连接的单点信任很难实现。在允许通过防火墙访问之前集成身份管理是一项非常消耗资源的任务。 此外，对于大多数开发/运营/网络团队而言，使用安全编码规范、应用程序层防火墙和防 DDoS 保护非常重要。

3 https://crypto.stanford.edu/cs155old/cs155-spring11/lectures/08-tcp-dns.pdf

©2020 云安全联盟-版权所有

为单个应用程序提供控制安全态势的能力目前是一个巨大的挑战。改造应用程序和容器平台的安全性需要集成访问控制、身份管理、令牌管理、防火墙管理、代码、脚本、管道和图像扫描，以及对集成的整体编排。这对大多数团队非常困难。

零信任解决哪些问题

以下是当今网络架构中常见的固有弱点，因此需要一种全新方法设计网络安全:

a）**先连接再验证**——大多数网络装置都允许在验证身份之前进行访问。由于没有万无一失的守护者可以检验身份声明，因此访问控制机制可以被绕过。身份验证、授权和基于令牌的访问控制系统，不论是否经过加密，都可能存在多个缺陷。

今天用于连接的主要网络协议是传输控制协议（Transport Control Protocol, TCP）。当应用程序使用该协议连接时，将使用先连接再验证模型运行。当客户端要进行通信并访问某个应用程序时，需要首先建立连接，而后进行身份验证。客户端通过身份验证后，即可交换数据。

此模型允许客户端首先连接到网络，从而允许未经授权用户进入。然后验证客户端身份，但仅在允许连接之后验证。这意味着已连接但未经授权的用户现在处于网络中并且可以执行恶意活动。由于在身份验证前不知道谁是合法客户端，因此这些用户通常会在其身份声明未被质疑时绕过身份验证方法。

本质上讲，组织为设备提供连接到 Internet 的 IP 地址时做了三件事：

- 拒绝尝试连接的恶意行为者，这个群体主要依靠威胁情报来标识。
- 通过漏洞、补丁和配置管理功能加固机器，使其无懈可击。但事实证明这种做法不可行。
- 部署没有用户上下文的网络层防火墙设备。这些防火墙容易受到内部攻击，或使用过时的静态配置。 （注意：下一代防火墙（Next Generation Firewalls, NGFs）确实考虑了用户上下文，应用上下文和会话上下文，但仍是

©2020 云安全联盟-版权所有

基于 IP 的，会由于应用层漏洞而导致不确定的结果。详细信息请参阅 SDP 架构文档。）

SDP 观点：**这些技术都不能有效防止攻击。零信任的实现要求对网络、主机和应用平台基础架构上各层攻击免疫。**

b）**监视端点需要消耗大量计算、网络和人力资源**——使用 AI 进行端点监视尚无法正确检测出或防止未经授权的访问。虽然受保护资源有各种虚拟的隔离，但是随着时间的推移，（攻击者）可以通过捕获身份的详细信息了解授权机制以及伪造人员、角色和应用的身份验证凭证，从而进行破坏。

现如今人工智能模型是简单的行为模型，大多基于多重线性回归分析和/或专家系统，或经过训练可检测模式的神经网络。如果有足够的时间序列数据，则可以将 AI 安全检测模型扩展到基于时间的事件。这些模型用于非进化系统，主要是在事后检测入侵模式。AI 目前在快速发展，需要熟练的安全专业人员提供分析以检测和预防新的、不断发展的威胁。大量数据与训练有素的模型结合，可以检测到众所周知的攻击向量。但是要检测前所未见过的带有欺骗意图的全新入侵途径，则需要结合性能监视、交易数据模式分析和安全专家提供的分析。仅依靠端点监视仍然会使企业容易受到不可检测的攻击。

SDP 观点：**对高度机密的数据，保证安全性最好的方法是在攻击发生之前进行防范。SDP 零信任部署可以基于逐个数据包分析，揭示非法的身份标识，从而拒绝存在风险的数据交换。**

c）**缺乏用户上下文的数据包检查**——网络数据包检查有其局限性，即数据包“分析”发生在应用层，因此入侵可能在检测前已经发生。

通过对网络中单个数据包的检查以识别连接的做法在一定范围内是创新的且成功的。这些方法仅与 TCP / IP 和 TLS 协议以及应用程序代码一样安全。

传统上，数据包检查是在防火墙上或防火墙附近使用入侵检测系统（IDS）和/或在重要的战略监视区域进行的。传统的防火墙通常基于源 IP 地址控制对网

©2020 云安全联盟-版权所有

络资源的访问。检查数据包的根本挑战是从源 IP 识别用户。工具是基于 IP 地址检查的。尽管可以使用现有技术检测某些攻击（例如 DDoS 和恶意软件），但是绝大多数攻击（例如代码注入和凭证盗用）这些攻击在应用层执行，因此需要上下文才能检测。

SDP 观点：**与之相反，SDP 不但有数据包检查而且还有用户上下文。通过 SDP 零信任部署，可以把在 SDP 网关收集被丢弃的数据包进一步转发，进行额外检查和分析。 结合网络数据，可以在入侵发生前检测到风险概况。**

实施零信任战略

零信任是设计实现网络安全架构一种的理念，在这种架构下，服务只有在用户、设备甚至每一个网络数据包都被充分地检查、认证和授权后才能被访问。即便如此，访问授权也应授予其最小权限。实现零信任架构需要如下几个部分。

a） 访问前身份验证

使用 VPN 和防火墙建立的零信任体系供用户访问服务（例如：邮件服务）。防火墙可以设置 IP 黑名单并且服务也可以设置哪些 IP 地址可以访问。VPN 可以设置为网络上只有通过认证的 VPN 客户端和拥有适当的密钥的用户可以连接来实现零信任。然而，如果一个未授权的用户复制了 VPN 客户端并且偷到了密钥，那么他也可以访问邮件服务，并且他还可以猜解其他用户的用户名和密码，或者执行诸如 DDoS、凭证盗窃等恶意行为。 VPN 允许用户登录网络并拒绝对不在邮件服务器网段上的其他服务的访问（例如：SharePoint）。如果一个未授权用户已经连入了网络，那么一般来说他会横向访问到 SharePoint 服务。身份认证前允许用户可访问的内容总是会比访问权限控制后要多。

为了确保在访问前进行认证，有一个隐含的要求：即将用户身份认证的控制平面和数据平面分离。为了确保响应时间在可接受范围内，还需要一种即时的身份认证机制。

©2020 云安全联盟-版权所有

b） 限制网络连接和暴露面的能力

公有云/私有云划定了网络安全边界。它提供了一种分层的安全方法，将日志导入监控工具，并且提供了分析和混合服务来控制策略。然而，这些特性并没有解决在访问之前身份验证的问题。

原生云平台和应用服务的强大功能支持包括入站/出站安全配置和企业网络策略配置。强身份认证和授权的行业标准是双向 TLS（双向 ssl）证书认证。一种更好的方法是在数据包访问之前进行身份验证，将 SDN 控制器与 SDP 零信任平台连接，并在 SDN 控制器提供的流量管理控制下在网络层丢弃或放行数据包。通过这种结构，SDN 控制器可以在用户身份验证失败后断开网络连接。

c）信任认证机制的粒度

网络层 VPN 和防火墙以及应用层防火墙和 SSL VPN 没有办法实现细粒度的访问控制。零信任体系不仅天生的具有基于策略的授权能力，而且还要求其在细粒度的网络上下文以及分布式服务连接和私有云/公有云的多云互联方案中进行身份认证。

使用网络层防火墙时需认真斟酌下。由于它是静态的，因此用户组是它所能提供的信任颗粒度。来自不同部门、不同角色的一组用户需要访问具有相同 IP 地址的同一服务情况是很常见的。防火墙规则是静态的，其策略只依赖于网络信息。它们不会根据上下文（即网络中设备所需的信任级别）动态更改。一个常见的例子是用户在风险更高的网络例如网吧中请求访问。如果本地防火墙或防病毒软件因恶意软件或某种意外而关闭，传统防火墙将不会检测到这一点。另一个例子是 IPSec VPN，它在允许访问前不会进行身份属性的认证。相反，IPSec VPN 依赖令牌（token）和凭证，而这可能被截获。而 SSL VPN 又有已知的漏洞。

相比以上这些限制，基于网络边界零信任方案通过细粒度信任认证机制和基于策略的授权达到了更安全的效果。

©2020 云安全联盟-版权所有

d） 监测可疑行为

让我们再考虑下基于身份属性的认证何时失败。将基于包检查的可疑行为导入日志和检测服务的能力为安全编排、自动化及响应(SOAR)提供的真正有用的数据，该技术使组织能够从各种来源获取输入（主要来自安全信息和事件管理（SIEM）系统，有关详细信息，请参阅 SDP 体系结构指南）。自动化是指为收集数据、进行集成和编排、提供操作智能和可视化图形和仪表板而启动的工作流过程。零信任实现可以为输入提供有用的情报，以提高 SOAR 人工智能模型和适当监测可疑活动的能力。

零信任解决方案的优势和价值

如同 CSA 在 SDP 架构介绍中描绘的那样，SDP 零信任解决方案具有如下安全优势和商业价值。

安全价值

价值	描述
减少攻击面	控制平面和数据平面分离，从而隐藏应用，避免潜在的网络攻击，保护关键资产和基础设施
保护关键资产和基础设施	通过隐藏来增强对云应用的保护： •给管理员更集中的管控 •对所有的应用访问可视化管理 •支持即时监控
应用隐藏	在用户/设备经过身份验证和授权访问资产之前默认关闭端口，拒绝访问
降低管理成本	降低端点威胁预防/检测的成本 降低事故响应成本 降低集成管理的复杂性
基于连接的安全架构	提供基于连接的安全架构。随着互联网和云应用的爆发式发展，传统的基于 IP 和边界的网络防护已经变得薄弱
可集成的安全架	提供了一个可集成的安全体系架构，可以方便的和现有安

©2020 云安全联盟-版权所有

构	全产品（如 NAC 或反恶意软件）实现集成 SDP 把以下分散的安全元素集成到了一起： •用户感知应用 •客户端感知设备 •防火墙/网关等网络感知元素
单包授权	使用单包授权机制确定连接，并启用身份验证和授权的控制
连接预审查	用基于用户、设备、应用、环境等因素制定预审查机制，去控制所有的连接
在允许访问资源之前进行身份验证	控制层面和数据层面分开，在TLS/TCP握手之前进行身份验证并提供细粒度的访问控制，进行双向加密的通信
开放规范	针对审查机制建立社区，让更多参与者反馈规则问题、不断优化规则

商业价值

价值	描述
节省成本和人力	SDP可取代部分传统的网络安全组件，减少了其许可和支持成本，可以最小化或取代MPLS、提高线路利用率，减少或取代专网，降低企业成本。同时SDP安全策略可以降低操作的复杂性和对传统安全工具的依赖，简化网络安全管理，提升工作效率，最终有助于减少人力需求。
敏捷IT运营	IT流程如果响应不及时会影响业务流程并进一步影响企业效率，而SDP的机制实现了IT或IAM事件的自动驱动，保证IT流程的即时响应，从而满足业务和安全需求。
利于 GRC（治理、风险与合规）	与传统的网络安全方法相比，SDP降低了风险并减少攻击面，防止基于网络的攻击和应用程序漏洞的利用。SDP可以和GRC（Governance, Risk & Compliance，治理、风险与合规）系统集成对接，比如与SIEM（安全信息和事件管理）集成，以实现系统和应用的适配。
更好的数据审核分析	SDP对用户、设备、访问的应用集中管理，可以更方便的进行数据收集、生成报表，和数据审核分析，同时可以为在线业务提供额外的连接性溯源跟踪。SDP的网络微隔离技术经常被用来缩小管理的单元范围，这对于报表的生成和分析十分有利。

©2020 云安全联盟-版权所有

更适合云安全迁移	SDP降低了应用上云所需的安全成本和复杂度，支持公共云、私有云、数据中心和混合部署，可以帮助企业快速、清晰、安全的完成业务上云迁移。与其他方式相比，SDP可以让业务云迁移更快、更好、更安全。
敏捷业务便捷创新	使能企业快速、安全地解决其当务之急。 比如： •使能把集中部署的呼叫中心转型为远程/居家坐席模式 •使能将非核心业务功能外包给第三方 •使能在远程第三方设备上实现面向客户的信息呈现 •使能将公司资产部署到客户侧，与客户建立更强的集成，并产生新的收益
加速业务转型	通过微隔离和权限控制实现物联网安全，可以连接到迁移工程师而不影响现有业务，结合物联网和私有区块链打造下一代安全系统。

SDP 零信任战略实施方针和 POC 概念验证

鉴于近年来大规模的数据泄露事故，企业应采取一些重要的措施，例如将基础服务涉及到的敏感信息资源分离到高安全等级网络中，以保护数据隐私。最近 CSA 在《2019 年云安全威胁报告》中的分析表明，人类高风险行为仍然是造成数据泄露、云恶意软件注入和 DDOS 事件的重要原因。

云安全联盟（CSA）于 2013 年发布了一种新的网络架构范式，即软件定义边界（SDP）协议。它用于创建一个在访问敏感数据前就主动从单个数据包检查中识别出合法网络连接的架构。该架构强调建立信任的控制平面与实际数据传输的数据平面的分离。这解决了 TCP 和 TLS 卸载后固有的漏洞问题，以及网络防火墙上千变万化的 IP 地址转换问题。

SDP 提供了一种简单的方式，防止有人在云上绕过企业和法律安全控制而导致的不良后果。 采用 SDP 的实施方式，强制信任建立与数据传输的分离。网络隔离和建立微型网络对多云部署非常重要，它也能从采用软件定义边界的零信任架构中受益。

©2020 云安全联盟-版权所有

将 SDP 软件定义边界、多因子认证和改进的访问控制/授权机制相结合，使组织走上了解决安全漏洞和大规模入侵的战略路径。软件定义边界除了运行时检测和响应外，还在配置和部署时强制执行安全策略。

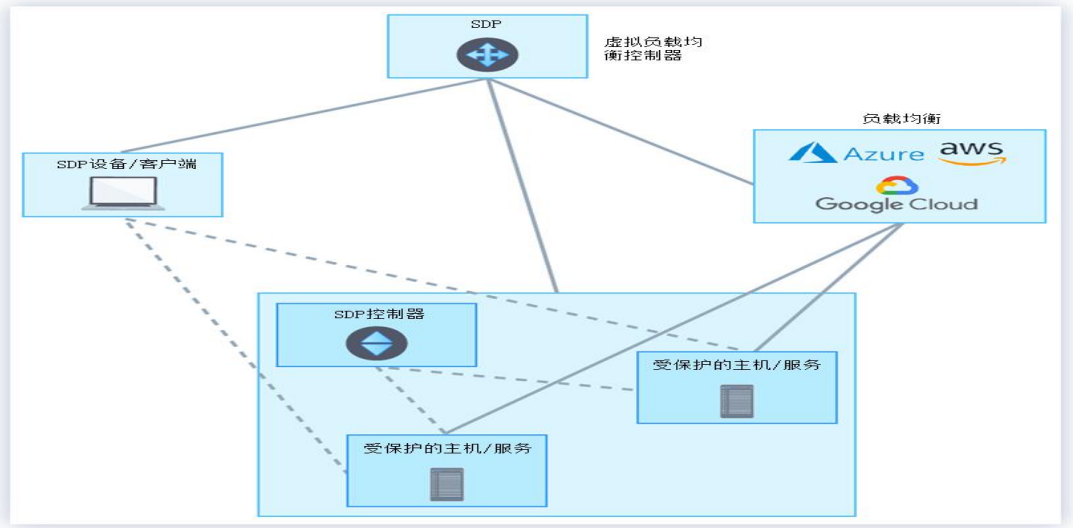

图 4：混合云环境

SDP 架构的概念验证(POC)可以展示 SDP 如何应对混合多云环境中应用交付的挑战。具体来说，POC 可以证明以下几点：

- 使用 SDP 方法，确保被分类为高度敏感的通信可以运行在任何类型的网络上（甚至是公共互联网），可以从一个安全环境进入到另一个安全环境，而无需经历网络层到应用层的不安全因素的考验。
- SDN（软件定义网络）通过提供独立的控制平面和数据平面的支持，以及拒绝所有（deny-all）/允许(allow)防火墙的实施，来进化成 SDP 软件定义边界；以及
- 在混合多云部署中的网络转发的 SDP 方法完全契合基于单一数据包检测的零信任网络原则。

推论是，在网络层实施 SDP 的部署可以通过 SDN 控制器接口，将连接从发起主机路由到 SDP 控制器来实现。配置这种路由的优选方式是一个能够实现自助配置的 REST 接口。

提供这个网络层 SDP 演示的理由是为了解决终止 TLS 后在应用层采用"零信任"产生的问题。现有的"零信任"安全措施大多是在 TLS 证书卸载后，根据策略应用认证和"有时"授权。证书验证是一个复杂的验证和确认过程，已知 TLS 1.2、TLS

©2020 云安全联盟-版权所有

1.3 和双向 TLS 都可能存在漏洞。

各大云服务提供商都有一些针对内容交付的零信任方法的举措。到目前为止，还没有零信任应用仅仅在网络层，特别是涉及混合多云部署的应用。在本例中，"混合云 "指的是从私有云到企业到数据中心的连接，而"多云"指的是跨不同公有云和私有云的网络连接。业内人士表示，目前大多数企业已经或打算采用混合多云战略。

POC 概念验证利用了网络虚拟化使得在 SDP 实现的控制平面上执行与安全相关的操作成为可能。从这个角度来看，软件定义网络(SDN)的广泛采用和演进使服务提供商能够简化网络管理。然而，SDN 的广泛应用给如何为 API 驱动的网络路由协调提供适当的认证、访问控制、数据隐私和数据完整性等方面带来了真正的挑战。虽然 SDN 允许按需提供虚拟网络，以实现高效的数据传输和精细的控制服务，但当前的安全实践并没有被设计成与这些软件定义基础架构的集成所带来的复杂性和挑战相匹配。然而，软件定义网络模式允许 SDN 控制器调用软件定义边界服务，该服务可以协调连接，并根据请求的 SDP 身份和设备验证对网络连接执行允许/拒绝操作。然后 SDP 控制器指示 SDN 将连接路由到接受的主机，或者当数据包识别属性没有通过所需检查时，放弃连接。

OSI 模型	云模型		概念验证(PoC)组件
应用层	应用	终端用户层–提供应用与业务价值	应用，用户界面
			SDP 客户端(SPA)
表示层	服务	中间件–应用不同层级中使用的功能组件	SDP 控制器，用户令牌，设备验证
会话层	镜像	操作系统–正确管理底层虚拟化	SDP 网关–防火墙规则，负载均衡
传输层	软件定义数据中心	云 API–启用创建绑定到资源池/用户的虚拟化资产	SDP–传输控制，数据包分析

©2020 云安全联盟-版权所有

网络层	虚拟机管理应用	虚拟化-提供计算，存储和监控的虚拟化	
数据链路层 物理层	基础架构	硬件-数据中心的硬件设备	

图 5：概念验证(PoC)组件

技术组件及架构

通过下述相关功能服务来展示部署 SDP 后可以解决企业信息技术漏洞的能力。这一展示构建在现有的、开源 SDP 方案之上。这个展示将会提供给公众使用，如果无法提供对应开源代码的话，技术供应商需要提供关于配置和组件部署的详细指导手册。

SDP 的控制平面和数据平面技术组件包括如下：

1. SDP 代理部署在一个 SDP 的客户端上
2. SDP 控制器部署在可以访问到 SDN 虚拟负载均衡（VLB）设备之上
3. SDP 主机需要基于零信任的允许/拒绝的安全态势感知（为了可以验证这个概念，这些服务器以虚拟机方式部署在可以通过外部云负载均衡访问的公有云之上）
4. 网络连通性源于公共互联网

网络负载均衡控制器及公有云技术组件

1. SDN 虚拟负载均衡能够将 SDP 请求路由到身份访问控制微服务之上，并确定允许/拒绝来响应该请求
2. 服务于 VLB 的公共云外部负载平衡，将请求转发给部署在公共云服务之上的 SDP 接受主机/服务

©2020 云安全联盟-版权所有

技术风险及问题

当配合软件定义网络（SDN）和虚拟负载平衡器（VLB）一起在网络层部署SDP/零信任方案时，会存在一定风险。因为针对网络连通性而言，SDP 是一个允许/拒绝的二选一模式，很明显，业务实现时会存在单点故障风险。因此，在数据平面的集成访问控制机制具备一定深度安全性是至关重要的。这确保了用于身份标识的属性被安全地规划、构建和运行。

假定

1. 一个现有的开源 SDP 部署方案作为概念验证演示的基础。
2. 选定一个虚拟负载均衡 VLB 设备。它可以调用微服务并把请求转发给公有云或私有云的负载均衡设备。
3. 负责 POC 概念验证的技术供应商应该公开访问并且提供详细的实现细节，其中不应该包含专有或者私有能力。
4. 针对本次 PoC 验证的意图，需要支持虚拟私有云的微部署方式。
5. 需要提供基于物理设备或者虚拟机的请求发起主机/服务器
6. 测试环境需要覆盖“合格”和“不合格”连接的测试用例。也就是说，在请求报文头中需要有身份标识来匹配对应服务（连接允许）或不匹配（连接断开）。

技术分析

部署真正的网络层零信任“允许/拒绝”连接状态所需的技术组件，需要在接受主机上应用网络协议之前访问新连接。

概念验证（POC）需要在流量管理期间、路由期间以及 TLS 证书终止之前部署组件，并且在最终 TCP/IP 端点目标确认之前不公开实际接受主机。这有一个明显的优势，即防止通过证书弱点进行入侵，也防止对目标主机的 DDoS 攻击。所需的技术是部署一个包检查服务，直接从虚拟负载均衡器访问身份标识属性。

©2020 云安全联盟-版权所有

可以通过 SDP 控制器服务路由访问连接，SDP 控制器服务根据身份属性服务决定断开连接或允许转发到接受主机服务器。

为了方便当前的网络环境，这些环境可能是连接了单个或多个服务，需要与 SDP 部署接口的技术是一个虚拟负载均衡器（VLB），该虚拟负载均衡器能够与云服务提供商和企业负载均衡器进行接口。

此技术还必须能够连接到部署 SDP 控制器的虚拟机，以及从初始化的客户机/服务器设备或虚拟机截获与 SDP 相关的请求。

所需资源

SDP 零信任概念验证演示所需的组件如下：

1.初始化网络连接的客户端/服务器。

2.互联网网络连接

3.基于数据包检查，在转发前能够调用 REST 服务的虚拟负载均衡器

4.SDP 控制器部署微服务

5.接受网络连接的客户机/服务器

6.CSP/企业外部负载均衡器将请求转发到接受客户端/服务器

注意：客户端/服务器是一个通用术语，不包含特定的入站/出站方向。

需求	组件
连接需要在访问前进行身份验证	部署在 SDP 控制器上的身份属性验证服务
审查连接和上报的能力	虚拟负载均衡器控制器丢弃未经 SDP 控制器检查的连接
细粒度身份和访问管理控制	对部署在 SDP 控制器上的虚拟负载均衡器控制器转发的每个连接进行单包检查，以在运行时对每个连接认证
向监控系统转发可疑活动	拟负载均衡控制器将可疑连接的信息转发到端点监视 SIEM 服务

©2020 云安全联盟-版权所有

关键产业发展

SDN 的进步，特别是配置为 REST 服务 API 形式的的虚拟负载均衡器控制器，以及路由网络连接的能力，使得零信任 PoC 是可行的。因此，虚拟负载均衡器控制平面的服务能够基于网络数据包做出智能决策。这意味着，现在可以通过 REST 方式调用边界保护服务来实现身份的网络验证，该服务可以验证数据包身份属性。

交付实施

交付实施 SDP 零信任，包括以下几个活动：

1.建设虚拟是私有云网络和虚拟主机

2.在端点间建立互联网连接

3.建立身份认证微服务

4.建设 VLB 虚拟负载均衡，并与 CSP（内容安全策略）的对外负载均衡器的公网 IP 建立路由

5.通过数据包检测确定 SDP 连接

6.通过单包检测提取身份属性信息

7.基于 REST 服务的身份认证微服务

8.在 VLB 与 SDP 控制器间建立网络连接路由

现状分析

目前，许多供应商都声称其产品和服务具有“零信任”能力。在授权访问网络端点之前进行身份验证，是建立零信任网络的基础。下列的能力和活动作为零信任的主要能力：

- 配置网络安全边界
- 将日志流传输到解析监控工具
- 配置混合服务控制策略
- 配置防火墙双向数据流安全规则
- 联动配置网络策略

©2020 云安全联盟-版权所有

- 基于双向 TLS 证书授权
- 基于 SPA（单包数据）授权

大多数情况下，在 TCP/IP 协议确立链接和 TLS 证书认证确认后开始进行授权。

相关说明

有兴趣参加 SDP 零信任演示的技术组件供应商，请通过电子邮件联系云安全联盟 SDP 工作组 info@c-csa.cn。

引用

云安全联盟相关著作：

- SDO 架构指南/ SDP Architecture Guide（2019.3）

https://cloudsecurityalliance.org/artifacts/sdp-architecture-guide-v2/

- SDP 在 DDOS 防御中的运用/ SDP as a DDoS Defense Mechanism（2019.10）
- https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-as-a-ddosprevention-mechanism/
- SDP 技术规范 2.0（2020.1，目前还在更新）

市场调研报告摘取：

- 云安全联盟，SDP 现状综述

开源参考实现（DHS）：

- http://sdpcenter.com/test-sdp/

面向 OMG（对象管理组）的零信任演示：

- https://cloudsecurityalliance.org/artifacts/sdp-the-most-advanced-zero-trust-architecture/

美国国防部网络中心服务战略：

- https://dodcio.defense.gov/Portals/0/documents/DoD_NetCentricServicesStrategy.pdf

©2020 云安全联盟-版权所有