零信任平台方案及关键技术

Zero Trust Architecture Platform Construction and Security Technology

严波/YAN Bo，王小伟/WANG Xiaowei
（深信服科技股份有限公司，中国 深圳 518055）
(Sangfor Technologies Inc, Shenzhen 518055, China)

DOI：10.12142/ZTETJ.202206005
网络出版地址：https://kns.cnki.net/kcms/detail//34.1228.TN.20221209.0854.001.html
网络出版日期：2022-12-09
收稿日期：2022-10-19

摘要：零信任平台由“中心+组件+服务”三大部分构成，以平台形式充分融合软件定义边界（SDP）、身份与访问管理（IAM）、微隔离（MSG）的技术方案优势，通过关键技术的创新，实现最佳可信访问控制和安全隔离，为用户在业务层、数据层、终端层的访问达到“从不信任，始终验证”的安全效果，提升整体安全水平的同时降低了安全复杂性和运营开销。

关键词：零信任平台；SDP；IAM；MSG

Abstract: The zero-trust platform is composed of three major parts: "center + component + service", which fully integrates the technical advantages of Software Defined Perimeter (SDP), Identity and Access Management (IAM), and Micro-Segmentation Gatekeeper (MSG) as a platform. Through key technological innovation, this platform achieves the best-trusted access control and security isolation, and achieves the effect of "never trust, always verify" for user access at the business layer, data layer, and terminal layer, improving the overall security level while reducing security complexity and operating expenses.

Keywords: zero-trust platform; SDP; IAM; MSG

随着数字化进程的深入演进，网络边界已逐渐模糊，基于“外网危险、内网安全”理念构建的安全防御体系已不再适用。在网络威胁不断变化和网络攻击日益猖獗的形势下，以“零信任”为代表的白环境分析手段也逐渐出现，从而逐渐替代基于威胁特征“一刀切”的黑名单机制。

2010 年，著名研究机构 Forrester 的首席分析师 J. KINDERVAG 首次提出零信任，核心思想是“从不信任，始终验证”。此后，零信任开始得到业界关注。零信任发展至今，主流三大技术方案分别是：软件定义边界（SDP）、身份和访问管理（IAM）和基于身份的微隔离（MSG）。不同技术方案各有特点，适用于不同的业务场景需求。SDP 重点在于按需定义业务访问边界，仅为合法请求提供业务资源的访问支持；IAM 重点在于用户的身份管理与权限分配，与业务深度结合；MSG 重点在于数据中心内部东西向流量的控制[1-4]。

对于跨国、跨地区的庞大业务规模、资源类别繁多的企业，仅依靠某一个技术路线而开发的单一产品，难以应对企业发展过程中面临的不同业务挑战，如远程办公、混合云环境、数据中心数据保护等安全问题。基于上述需求，融合各技术方案特色的零信任平台应运而生。从企业环境的关键业务需求出发，结合三大技术方案的防护思路与功能，统一规划、统一建设，可以打造安全与业务融合的零信任闭环[5]。

1 零信任平台方案

零信任平台（以下简称“ZTA 平台”）是以 SDP 为核心，融合其他零信任技术产品、功能组件的方案。在零信任平台方案中，各个产品和安全组件实现灵活解耦，在充分发挥各自功能特性的同时，还实现了“统一策略”“统一管理”的平台联动机制，达到“1+1>2”的效果。组件的解耦，可实现不同业务场景下的灵活组合：一是可解决单一产品覆盖场景不全的问题；二是可以在整体规划之下，按阶段选择需要的组件，实现安全防御强需求，并同步实现建设成本可控的要求，具体如图 1 所示。

▲图 1 零信任建设阶段

基金项目：深圳市云安全关键技术研究重点实验室项目（ZDSY20200811143600002）

ZTA平台分为3个部分：零信任中心、零信任组件、服务支撑，它们分别承担不同的功能职责，彼此联动，互相支撑。ZTA平台具体如图2所示。

零信任中心部分位于ZTA平台的控制平面，是ZTA平台的核心和关键所在。该部分包括两个子中心：分析中心和控制中心。分析中心基于多源数据对访问主体的信任等级进行持续分析、评估，并将评估结果发送至控制中心，用于访问策略的选择和应用。除此之外，分析中心还肩负实时风险展示、权限梳理、应用识别、办公安全行为可视等多种职责。控制中心是根据分析中心的评估结果，动态匹配访问控制策略，并将策略下发至数据平面的执行组件。

零信任组件部分位于ZTA平台的数据平面（或业务平面）。作为访问控制策略的执行点，该组件主要与控制平台联动，兼顾情报点、自身安全防护等职能。执行点主要负责访问策略的执行，即控制中心对具体的访问请求进行分析评估，并下发选定的执行策略，并负责执行[6]。在平台化中，执行类设备被称为网关，所有业务流量均由网关设备转发；情报点主要用于访问请求中的信息收集、分析和传输，包括认证登录、业务访问行为信息等。该类信任一方面用于优化使用体验，另一方面则为分析中心提供数据分析的来源[7]。

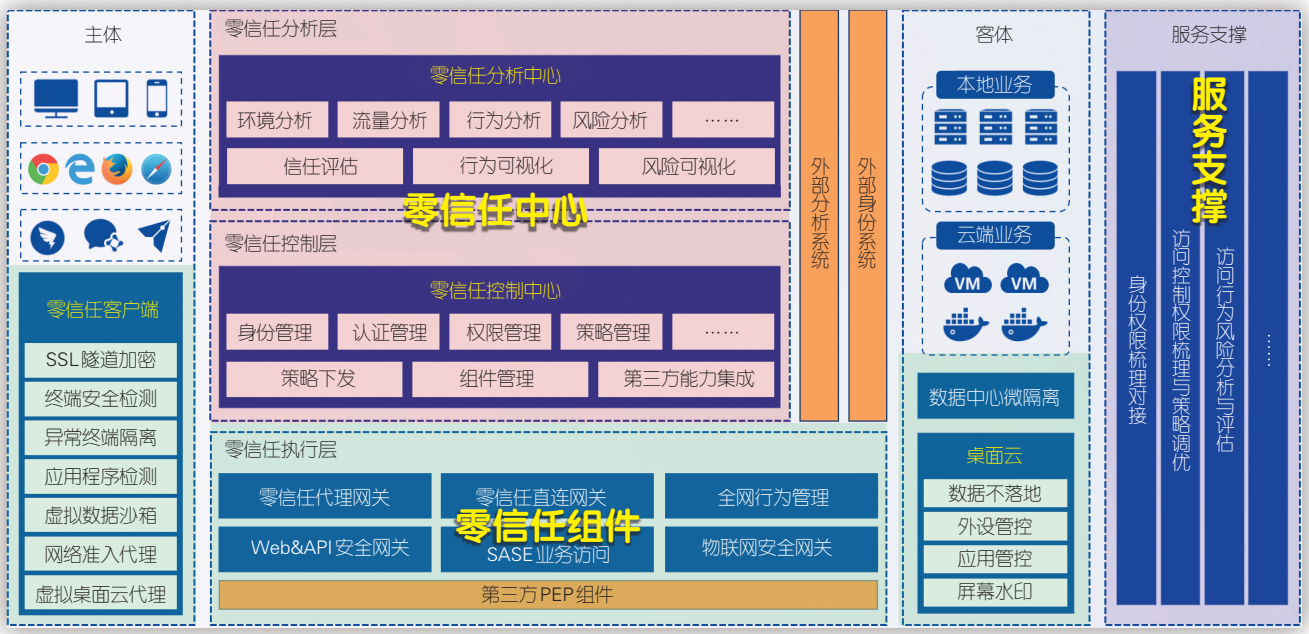
服务支撑部分是ZTA平台持续迭代、安全防御能力优化、业务保障的重要组成部分。通过交付阶段的业务梳理，服务支撑部分完成基础能力的建设，并进行动态策略调整，在业务运行平稳后，逐步扩大零信任的覆盖和使用范围，最终达成业务的全部迁移；在运营阶段，通过安全运营，持续完善业务白名单，建立、优化访问控制关系和策略调整，确保业务访问的合规化、合理化，达到安全自适应的闭环。

2 功能组成

2.1 零信任控制中心

零信任控制中心在ZTA平台中占具核心地位，与信任分析中心、零信任组件进行控制联动，提供的管理功能包括：身份管理、认证管理、权限管理、策略管理、策略下发、组件管理、第三方能力集成等。本文中，我们主要介绍身份认证管理、应用管理、策略管理三大内容。

身份认证管理主要通过与统一身份管理平台对接或由控制器自身提供认证服务，实现身份的认证和权限管理。身份认证的对象包括用户（人）、终端、设备、程序等。控制中心根据用户登录信息、终端环境信息等内容动态调整访问策略，例如，用户首次使用账户信息登录或在非常用地区登录时可能触发增强认证，即触发多因子认证，保障接入安全；在终端已被设置为授信终端或登录环境安全时，进行认证豁



API：应用程序编程接口　PEP：策略执行点　SASE：安全访问服务边缘　SSL：安全套接层

▲图2 零信任平台

免，免除二次认证过程或实现离线客户端一键上线，以提升用户的使用体验[8]。

应用管理部分主要围绕业务系统的访问需求，确定合适的安全发布机制和访问模式。例如，当用户的访问环境为内网时，应用管理触发直连网关（DGW）的访问模式；当用户的访问环境为互联网时，自动调整为SDP代理网关访问模式。

策略管理部分主要为不同环境下的访问需求，能够提供多类型的动态控制策略，常见的包括：安全策略、客户端接入策略等。动态策略选定主要来源于零信任分析中心，控制中心通过与分析中心联动，完成风险分析和持续信任评估，最终确定并生成动态的访问控制策略，下发给安全组件后完成执行。

为了更清晰地展现以上原理，我们以图3为例进行说明。由“客户端及用户”侧向“业务系统”发起业务访问，会经历以下几个阶段：首先客户端及用户需要与零信任控制中心完成身份验证，身份验证可以由控制器自身或统一身份管理平台来实现；认证成功后，控制中心检查与之相匹配的策略和该用户所具备的业务资源列表，判定满足访问条件后，下发放通或拒绝的策略到网关设备节点，网关设备来完成该策略执行。在以上过程中，控制中心还会持续接收来自分析中心的分析结果，辅助策略决策。

2.2 零信任分析中心

零信任分析中心主要为控制中心提供决策依据输入，并基于用户访问行为或访问环境等信息进行综合风险分析。例如，用户的客户端登录源IP地址在授信IP地址范围内时，在提供正确的身份信息后，即可访问业务系统；当源IP地址在非授信IP地址范围内时，即使提供了正确的身份信息，也可下发策略阻止本次访问。分析中心可以周期性检测客户端的源IP地址的变化情况，并将分析结果及时传递给控制器，以供决策参考。

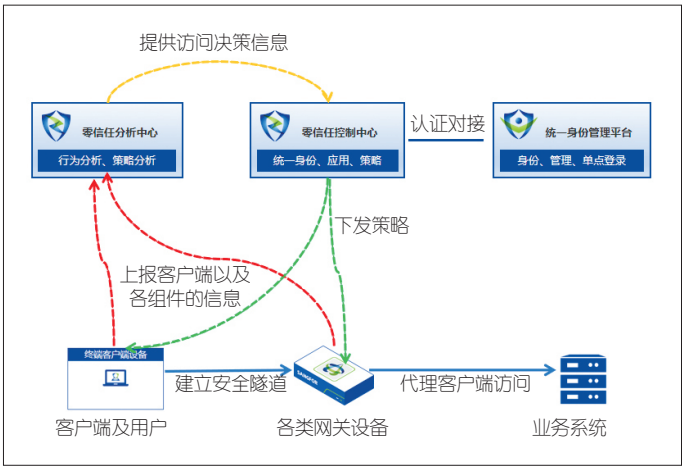
分析中心的情报数据采用的是多源并行的方式，不仅汇集客户端的数据信息，还可汇集其他安全组件或日志分析平台的数据，例如：终端安全环境检测的风险分析数据、用户认证和访问流量的风险分析数据，以及第三方策略信息点（PIP）分析中心分析数据。零信任分析中心对多源输入的情报信息进行统一聚合处理，控制中心将参考分析中心的具体分析结果做出访问决策，并匹配、下发具体的访问控制策略，如图4所示。

2.3 零信任组件

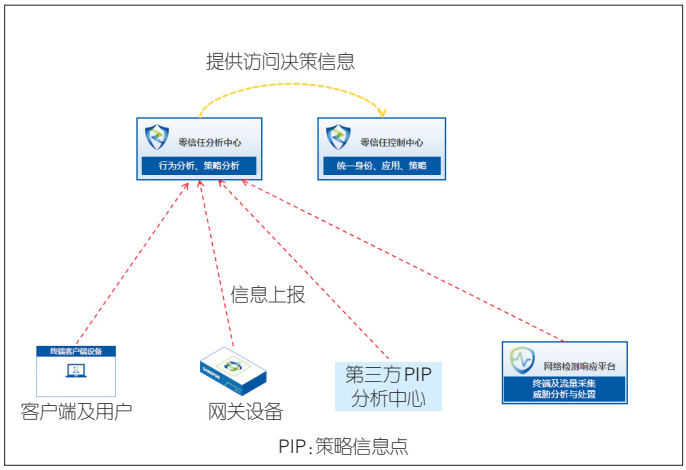
零信任组件主要指各类场景下负责策略执行处的安全管控组件，例如：SDP代理网关、DGW、安全访问服务边缘（SASE）类网关、物联网安全网关等。根据实际的业务场景和安全需求设置不同的安全组件，远程接入办公可选择SDP代理网关，内网办公场景可以选择DGW，物联网可选择物联网安全网关，互联网云上业务访问场景使用安全访问服务边缘–专用访问（SASE–PA）。

在ZTA平台中，常见的网关分为三大类：SDP代理网关、DGW、SASE–PA网关。

SDP代理网关适用于互联网接入和远程办公场景，如图5所示。SDP采用的是代理转发模式，即与终端建立连接，再与业务系统建立连接。SDP代理网关工作在“内外”网的逻辑边界处，业务系统隐藏在SDP代理网关之后。这样能够实现暴露面的收缩（仅剩余SDP代理网关本身对外暴露），而SDP代理网关的安全可通过其他的安全措施加以防护，例如单包授权（SPA）技术。



▲图3 零信任访问请求控制



▲图4 零信任分析中心

DGW适用于内网办公场景，因业务访问由内部网络承载，所以又被称为直连网关，如图6所示。DGW采用防火墙架构设计，用于放通/禁止内网客户端对于业务的访问。对于客户端发起的访问，DGW仍然会对客户端做应用级的校验，校验通过后才会放通本次访问请求。

SASE-PA网关适用于跨地区分支需要访问总部业务的办公场景，如图7所示。该模式是将网关组件以云化的方式部署在云端，通过终端客户端与SASE-PA网关建立加密隧道，实现业务数据引流。当客户端发起业务访问请求，流量会被“抓”取并放入隧道，通过云上SASE-PA网关实现代理访问。同时，客户端的非业务流量会自动过滤分流。相比于传统的SDWAN组网，SASE-PA网关模式极大地实现了企业跨地区灵活组网、高性价的安全业务访问需求。

以上3类网关各具特点。对于SDP代理网关模式，当网关出现故障时，通常需要通过修改域名或者映射配置来恢复业务访问；对于DGW模式，在网关故障发生时，可以通过透明模式部署来实现业务访问的快速逃生；相比于SDP代理网关与DGW，SASE-PA网关模式天生具备易部署、易扩展、访问健壮的特点，主要应用于云托管场景。

2.4 ZTA平台落地与服务支撑

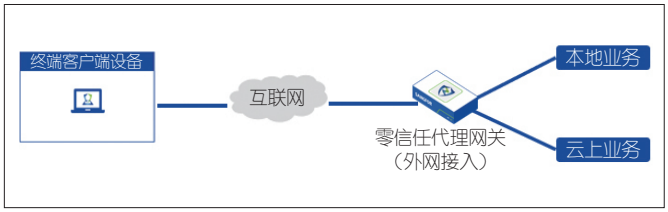
传统的网络安全防御体系与被保护的业务系统属于分割、松耦合关系，在计算环境、网络边界、传输网络中以设定“黑名单”为主的安全策略。ZTA平台作为一种全新的安全架构，与业务需求、安全能力动态持续融合，增强“白环境”检测逻辑，以场景化、阶段化的方式，逐步构建完整的业务安全防御体系，所以ZTA平台方案落地可分为三大阶段，分步实施。

第1阶段，优先实现通过互联网或广域网（类似政务外网等专网）进行远程接入访问的业务场景部分，通过零信任架构，收缩业务对外的暴露面。

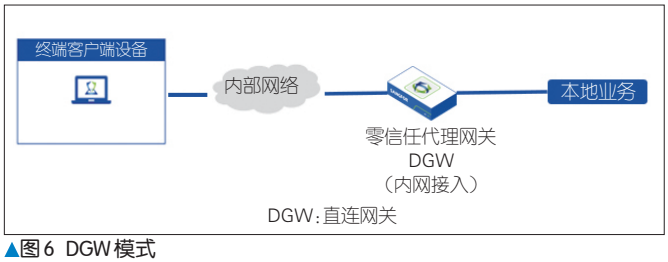
第2阶段，优先考虑内网访问和分支机构接入访问的业务场景部分，可将传统网络安全升级为零信任架构体系，实现内外网统一、无差别的安全访问办公体验。

第3阶段，深入组织数据中心内部访问场景，主要解决数据中心主机、虚拟机、容器、服务之间相互访问调用的安全访问控制逻辑。

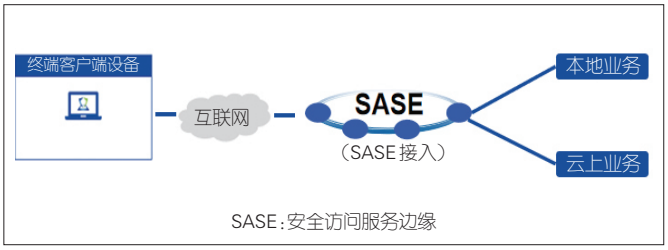
在平台的运营阶段，还需专业团队以安全运营服务的方式，持续提升企业的“白”化能力。通过可视化报表和自动化技术的辅助，主动挖掘和发现未知风险，实现动态、自进化式的安全策略调整。



▲图5 软件定义边界代理网关模式



▲图6 DGW模式



▲图7 SASE-PA网关模式

3 关键技术

ZTA平台是通过在多个层面，以多种安全控制技术，实现以下的一些安全目标：正确的人利用可信的终端，通过安全的通道，使用适当的权限，访问重要的业务，从而保护敏感的数据。

3.1 第3代SPA技术

零信任核心能力之一是实现基于身份的安全访问控制。这需要两个必要条件：一是实现流量身份化；二是在通过身份认证之前，要充分缩小业务的暴露面，做到先认证后访问。

在传统的远程办公场景中，客户端需要先与业务系统建立连接，再进行用户身份认证，认证通过后即可获取相应的业务资源列表。先连接的前提条件是业务端口保持开放，但这种开放先天就存在被攻击的风险，例如：端口扫描、分布式拒绝服务攻击（DDOS）等。

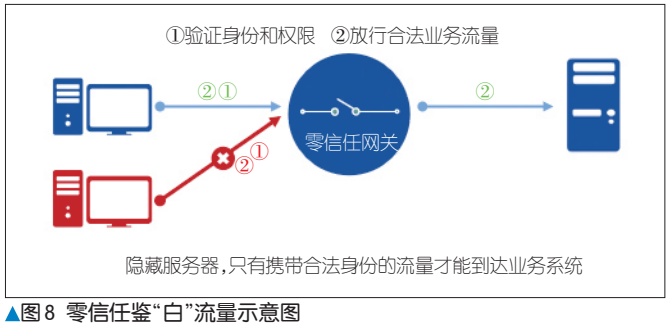
在ZTA平台中，客户端在正式发起连接前，需要完成身份验证，验证通过后才能进行正式连接，同时实现对设备自身的安全防护。未通过身份验证的客户端，无法得知业务端口，更无法与之建立连接。整个过程包括两个阶段：第1个阶段，通过控制平面的身份校验后，控制平台通过策略配置，打开业务连接端口；第2个阶段，客户端与打开的端

口，在数据平面建立业务连接，实现业务访问。零信任鉴“白”流量示意如图8所示。

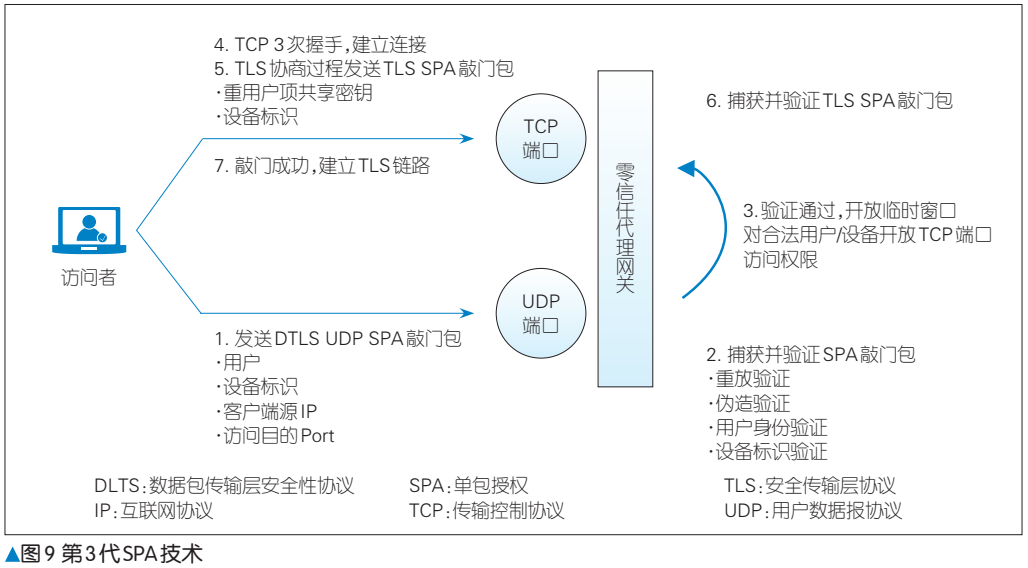
在互联网访问的具体场景中，SDP代理网关通过第3代SPA技术和隧道技术，实现暴露面隐藏和流量身份化。由于安全网关采用代理的方式替代了客户端进行业务访问，所以在隧道头部中以插入字段的方式，传递身份验证所需内容。

零信任系统默认隐藏所有服务端口，仅开放所需的用户数据报协议（UDP）端口。在正常用户访问前，客户端发送含有身份凭证的UDP SPA“敲门”包，验证通过后会临时打开一个时间窗口，且仅允许指定源IP地方访问的443端口（即TCP SPA敲门端口）。后续的传输控制协议（TCP）连接过程遵循第2代TCP SPA流程，在安全传输层协议（TLS）协商过程中完成TCP敲门，具体如图9所示。

由于非代理模式下不能修改数据包内容，所以DGW访问场景无法直接使用SDP来实现业务端口隐藏。该场景以使用前置验证包的方式来实现应用级鉴权。客户端在每一次发起会话连接时，需要先通过一个前置验证包来完成验证，验证通过后才能建立会话；验证失败，则会拒绝建立会话。



▲图8 零信任鉴“白”流量示意图



▲图9 第3代SPA技术

3.2 新一代沙箱技术

在零信任方案中，数据安全也需要重点考虑。实现数据安全保护的技术主要包括：桌面云（VDI）、虚拟浏览器（SBC）、沙箱（SandBox）。桌面云和虚拟浏览器技术能实现数据云端存储，可见、可用，但不可得；沙箱技术能实现数据落地，但不泄密。

沙箱技术是通过在终端上创建与当前终端环境逻辑隔离的安全工作空间，来实现数据隔离保护。该技术通常是以插件的形态来实现轻量化、简洁化的应用。沙箱技术使用驱动层的文件透明加解密技术，在文件系统添加一个加解密过滤层。所有软件的磁盘写入操作最终都会经过这个加解密模块，再进入磁盘。加解密模块会对写入操作的进程进行判断，属于工作空间的进程则写加密、读解密，属于终端空间的进程读写均不做额外操作。沙箱技术在应对勒索病毒方面也具有一定优势。勒索病毒主要是通过磁盘文件遍历的方式来获取对应格式的文件并实行加密。写入沙箱文件系统的文件被隔离保护，在个人桌面无法搜索找到对应文件，也就无法实现对其加密勒索。与此同时，沙箱技术还可以实现对数据导入和传出的控制，避免数据失控、外泄。

3.3 动态访问控制列表（ACL）技术

传统网络安全的ACL策略是静态制定、规则匹配的模式，无法实现动态、细粒度、差异化管控，无法实现主动防御和响应。ZTA平台中以动态ACL技术来评估终端接入的风险，从而实现动态策略控制。

零信任的策略引擎主流模式有两种：一种是信任评分机制，一种是规则机制。

信任评分机制又分为配置评分和智能评分两种模式。配置评分模式是管理员为不同安全缺陷情况预设分值，并对整体评估结果设定一个“及格线”分值；智能评分则是通过平台引擎进行统计、学习从而完成判断和赋值，整个过程无须人员参与，所以智能评分机制的弊端是如何设定合理的“及格线”。

规则机制是通过在不同的板面上分别设定安全策略基线，以“短板”效应的方式，达到设定目标。相比于

信任评分机制，规则机制更有利于保障安全的底线和原则，不会单方面通过得分情况做出策略判断。

在ZTA平台方案中，我们采用规则+评分的混合模式，以规则机制为主，评分机制为辅，共同完成安全分析判定。ZTA平台的理念是："安全有原则，管理有灰度，信任有智慧"。"安全有原则"是指策略引擎以规则为主；"管理有灰度"是指在动态ACL规则方面可配置二次认证或告警，或提供过渡期整改再处置，以保证业务优先，而非"一刀切"的统一策略；"信任有智慧"是指在规则基础上引入智能评分机制，辅助决策。

ZTA平台中的动态ACL涵盖时间、位置、可信应用程序等多种维度，可根据实际场景需求进行细粒度设置。在智能评分模式下，零信任中心联动终端安全设备，实现客户端的环境评估赋值，辅助决策；在规则模式下，通过对发起访问请求的终端程序进程的使用情况、签名信息等内容进行安全评估，与预置的可信进程和不可信进程标签进行动态匹配，以支撑不同策略的差异化选择。

3.4 三层转四层隧道技术

隧道技术是在传输层面实现安全控制，主要包括3个关键内容：引流、传输和代理。引流是精准"抓"取业务访问流量，传输是指以加密后传输给隧道代理网关，代理是由网关代理客户端完成业务访问。

传统的三层引流技术主要是通过虚拟网卡和路由完成引流，兼容性较好。其原理是通过在终端本地安装虚拟网卡，并下发路由的方式，实现引流进入隧道，同时通过虚拟域名系统（DNS）配合，实现域名资源的访问。由于工作在三层，也被称为是三层隧道。当客户端存在多个客户端/服务端模式（C/S）的应用程序时，会通过一条传输控制协议（TCP）长连接与代理网关实现数据交互。长连接的传输受网络波动、切换的影响较大，用户感知明显。

三层转四层技术是在三层虚拟网卡处，通过IP路由表引流获取到终端的请求流量，之后以轻量级IP协议栈转换成四层数据包，再将数据包通过客户端私有隧道代理的方式发送至网关。这种模式使用TCP的短连接，客户端与代理网关之间会为每个隧道均建立一个TCP短连接。当数据传输完成后，立即释放该短连接资源。由于短连接对应用层（四层以上）流量不做改写，在数据包被加密封装的payload部分长度要比长连接更短，因此在大文件传输和下载场景中，传输效率高于长连接方式。

4 结束语

零信任是内生安全模型的代表之一，以强调业务"白"化能力的方式，与被保护的业务深度融合。依托零信任平台方案和可行技术的应用，零信任构建了安全与生产力的平衡发展态势，优先保障业务可用性，并以系统化思维全面提升业务自身的安全免疫力，为数字化、智能化社会的安全建设指明了方向，奠定了的"可信"基石。零信任架构旨在加强安全性以保护企业资产的系统和操作设计指南，它本身并不是一个单一的架构。零信任平台通过融合软件定义边界、身份与访问管理、微隔离的技术优势，为企业提供业务与安全同行的网络环境，是保障企业数字化良好发展的重要路径。

致谢

本文的撰写得到深信服科技股份有限公司游建舟、王琦然的帮助，在此表示感谢。

参考文献

[1] 潘吴斌, 任国强. 软件定义边界SDP: 概念、技术及应用研究综述 [J]. 数字通信世界, 2021, (3): 192-195. DOI: 10.3969/J.ISSN.1672-7274.2021.03.084
[2] 田由辉. 基于零信任架构的网络安全防护思路 [J]. 信息技术与信息化, 2020(5): 154-157. DOI: 10.3969/j.issn.1672-9528.2020.05.048
[3] 魏小强. 基于零信任的远程办公系统安全模型研究与实现 [J]. 信息安全研究, 2020, 6(4): 289-295. DOI: 10.3969/j.issn.2096-1057.2020.04.002
[4] 朱良海, 张义超, 袁震. 构建基于SDP技术的网络安全体系 [J]. 网络安全和信息化, 2019, (12): 109-112
[5] 王刚, 张英涛, 杨正权. 基于零信任打造封闭访问空间 [J]. 信息安全与通信保密, 2020, 18(8): 78-86
[6] 江伟玉,刘冰洋, 王闯. 内生安全网络架构 [J].电信科学, 2019(9). 20-28
[7] 訾然, 刘嘉. 基于精益信任的风险信任体系构建研究 [J]. 信息网络安全, 2019, (10): 32-41. DOI: 10.3969/j.issn.1671-1122.2019.10.005
[8] 王琦然, 王金红, 卢艺, 等. 零信任助力数字化办公安全高效: 深信服零信任安全解决方案 [C]//2021年国家网络安全宣传周"网络安全产业发展论坛"论文集. 西安, 2021: 189-192

作 者 简 介

严波，深信服科技股份有限公司产业教育中心教学教研部主任、安全服务认证专家、网络安全等级保护体系专家、网络安全高级咨询顾问；长期从事零信任、云安全、数据安全方向的技术研究工作；曾参与多项国家标准的研究和编写工作。

王小伟，深信服科技股份有限公司产业教育中心教学教研部资深讲师、深信服安全技术认证专家；长期从事零信任、云安全方向的技术研究工作；曾多次主导及参与媒体、能源、金融等行业数据中心网络安全实战项目的规划、交付和研究工作。