零信任架构在 5G 云网中应用防护的研究

何国锋

（中国电信股份有限公司研究院应用安全研究所，上海 200122）

摘　要：通过对 5G 云网融合时代的安全需求分析，研究零信任的基本原则，包括不依赖位置、不信任流量、动态访问控制等；研究零信任的基本架构，结合 5G 云网架构，提出了 3 种可行的应用防护方案，包括客户自建的 OTT 模式、利用现有 VPDN 改造模式、公共零信任架构模式，并进行了比较。分析了客户在 5G 云网中的应用场景，包括远程访问、安全上云、移动办公等，以及在这些场景中零信任架构可以给客户带来的价值，如实现应用隐藏、动态控制，确保应用的安全性。

关键词：网络安全；动态访问控制；应用隐藏；零信任；5G；应用防护

中图分类号：TP393

文献标识码：A

doi: 10.11959/j.issn.1000−0801.2020325

Application protection in 5G cloud network using zero trust architecture

HE Guofeng

Institute of Applied Security, Research Institute of China Telecom Co., Ltd., Shanghai 200122, China

Abstract: Based on the analysis of security requirements in the era of 5G cloud-network convergence, the basic principles of zero trust were studied, including not rely on location, untrusted traffic, and dynamic access control. The basic architecture of zero-trust was studied, combining with 5G cloud network architecture, the feasible application protection solutions include the customer-built OTT model, the use of the existing VPDN model, and the public zero-trust architecture model was proposed and compared. The application scenarios of customers in 5G cloud network were analyzed, including remote access, secure cloud, mobile office, etc. In these scenarios, the value that zero-trust architecture can bring to customers was proposed, such as application hiding and dynamic control, ensure the application safety.

Key words: network security, dynamic access control, application hiding, zero trust, 5G, application protection

1　引言

过去企业 IT 基础设备及用户办公都是在企业内网，企业 IT 架构是有边界的。在移动化和云化的大背景下，越来越多的企业用户开始使用云应用和移动设备进行移动办公，企业应用不再局限在办公室内，企业 IT 基础设施及用户办公的内外边界逐步模糊，传统安全边界瓦解，企业 IT 架构

收稿日期：2020−10−20；修回日期：2020−12−10

正在从“有边界”向“无边界”转变。

另一方面，APT 攻击者总是有办法进入企业网络，而企业内部的员工也越来越不可避免地、有意或无意地对信息安全造成损害。对处在企业内部的“人为风险”进行有效的管控。频发的信息安全事件显示，“堡垒最容易从内部攻破”，内网已不是安全的“自留地”。因此，考虑内网的安全，需要假设内网中的各节点（包括客户端、人员等）是不可信任的，需要针对性的安全防护。

传统的基于边界的网络安全架构假设内网的人和设备是值得信任的，认为安全就是构筑企业的数字护城河，通过防火墙、WAF、IPS 等边界安全产品及方案对企业网络边界进行重重防护就足够了。但是，安全是相对的，系统一定有未被发现的漏洞、一定有已发现但仍未修补的漏洞，系统已经可能被渗透、内部人员可能不可靠，这就需要全新的网络安全架构来应对信息化应用所面临的安全风险。

传统的网络安全是由下而上的防护，使用传输层隔离进行防护。这种方法在传统有内外之分的场景中还可以使用，但应用的设备、应用的程序在云环境中是无处不在的，同时移动设备随时随地接入，防护措施需要由传统的内部防护和外部防护，发展为无处不在的防护。传统的内网、外网是有物理区隔的，也由此产生了内网、外网安全等级的不同。而今，在移动互联时代，移动用户通过 Wi-Fi 接入、VPN 等工具随时随地进入内网获得访问权限，因此绝大多数内网的物理隔离已经不复存在，因此不能基于位置（IP 地址）信任来自内网的设备、接口和用户，所有的流量均不可信。

5G 时代大带宽、海量连接、低时延等特性，使得更多的业务联网进入快车道，并且虚拟化、切片等组网技术，使互联网、物联网、工业控制网深度融合和交叉，原来物理隔离的网络边界不复存在，攻击范围也已扩展到更广泛的领域。云网融合进一步加剧了网络和应用的融合，网络和应用共享计算资源，不同客户间的应用资源和网络资源在物理上完全融合，无法做到明确的物理边界，也无法实施传统意义上的边界防护。

5G 时代，移动网络的商业环境、应用场景、技术形态、网络环境、监管要求等都发生了很大的改变，整个移动网络生态发生了重大变化。从商业环境上看，移动网络从单主体网络演进为一个多主体的网络，存在更多不同的信任关系，需要多方合作提供服务，共同建立多元化的 5G 商业生态；从应用场景看，从面向人的连接向面向机器的连接演变，承载了更多的业务，具有更高的商业和社会价值；从技术上看，引入基础设施云化、网络功能虚拟化、软件定义网络、网络切片、边缘计算、能力开放等使能技术，使网络的架构和层次复杂化、边界模糊化，业务开放，增加了攻击面，引入新的风险；从安全治理上看，《网络安全等级保护制度 2.0》的颁布和实施，对移动网络提出更高的安全要求；需要从被动防御到主动防御的转变。总体而言，移动网络从可信可控网络有向非可信网络发展，传统的基于位置的安全架构将无法满足移动网络发展的要求。

而目前移动网络安全架构（包括 5G 网络）还是按照安全域和安全层进行设计的，采用传统的基于位置和区域的安全设计方法和安全技术。因此，事实上，网络无边界和传统安全防护之间巨大的鸿沟会给网络、应用都带来极大的安全风险。5G 时代云网融合需要新的解决方案适应无边界无处不在的网络时代。

2 零信任架构

零信任又称为零信任安全、零信任网络、零信任网络接入、零信任模型。

零信任安全模型，是 2010 年由 Forrester 首席分析师 Kindervag J 提出的，他认为所有的流量都

不可信，不能以位置作为安全的依据，而需要为所有访问采取安全措施，采用最小授权策略和严格访问控制，所有流量都需要进行可视化和分析检查。这些理念也是网络安全领域存在已久的公认原则。

随着移动互联网发展，安全攻防态势不断演进，零信任越来越受到业界重视。2013 年，Google 开始向零信任架构转型，实施 Beyondcorp 方案。Google BeyondCorp 被业界认为是零信任的最佳实践者。从 2014 年开始实施，项目周期为 7 年，其核心理念就是完全不信任网络，着眼的是业务应用，将重点在于对人和设备的管理、认证、授权和访问控制；基于设备、用户、动态访问控制和行为感知策略，实现内、外网无差别的访问；持续对用户访问进行安全评估，应用被分为若干可信任级别，通过规则引擎验证和综合判定后确定可访问的内容。

2014 年，CSA 发布软件定义边界 SDP 规范。2014 年 4 月，云安全联盟（CSA）发布《SDP 规范 1.0（SDP Specification 1.0）》。软件定义边界（software defined perimeter，SDP）旨在为应用属主在不安全的网络上部署隔离的服务。其主要特点：控制和数据分离、策略集中管理、业务授权访问、使用单包授权（SPA）隐藏服务器。基于 SDP 模型方案可有效地减少攻击面，缓解或者彻底消除威胁、风险和漏洞。

2018 年，Gartner 将零信任（zero trust architecture）列为 Top 10 安全技术。Gartner 认为互联网成为不受信任的传输方式。零信任架构提供对资源的受控访问，从而减少了攻击暴露面。ZTA 通过隔离，无须将应用程序直接暴露给 Internet，提升连接安全性。

2019 年，NIST 发布零信任网络架构（zero trust network architecture）标准草案，认为零信任架构是一种端到端的网络安全体系，包含身份、凭据、访问管理、操作、终端、托管环境与关联基础设施。零信任架构提供了相关概念、思路和组件关系（体系结构）的集合，旨在消除在信息系统和服务中实施精准访问策略的不确定性。NIST 认为传统安全方案只关注边界防护，对授权用户开放了过多的访问权限。零信任架构的首要目标就是基于身份进行细粒度的访问控制，以便应对越来越严峻的越权横向移动风险。

2019 年，腾讯在 CCSA 立项《零信任安全技术安全框架》，中兴、奇安信等企业推出了相应的产品原型，可以看出产业界对零信任安全充满期待，说明了其技术的先进性以及市场前景。工业和信息化部在《关于促进网络安全产业发展的指导意见（征求意见稿）》的意见中，将零信任等网络安全新理念首次列入需要“着力突破的网络安全关键技术”。

2.1　零信任基本假定和原则

Gilman E 在《零信任网络》一书中将零信任架构建立在如下 5 个基本假定之上：

（1）网络无时无刻不处于危险的环境中；

（2）网络中自始至终存在外部或内部威胁；

（3）网络的位置不足以决定网络的可信程度；

（4）所有的设备、用户和网络流量都应当经过认证和授权；

（5）安全策略必须是动态的，并基于尽可能多的数据源计算而来。

基于以上假设，零信任模型被认为遵守以下 4 个基本原则。

（1）验证用户：基于位置、设备和行为来评估用户安全情况，确定用户是否是其声称的身份。采取恰当的措施（比如多因子身份验证）来确保用户的真实性。

（2）验证设备：无论是公司设备、BYOD 还是公共主机、笔记本计算机或移动设备，基于设备身份和安全情况实施访问控制策略。只允许受信终端访问公司的资源。

（3）限制访问与权限：如果用户和设备通过

了验证，对资源实施基于角色的访问控制模型，赋予其仅供完成当次工作的最小权限。

（4）自适应：各类源（比如用户、其设备、与之相关的所有活动）总在不断产生信息。利用机器学习来设置上下文相关访问策略，自动调整并适应策略。

2.2 零信任基本架构

零信任的核心目标是为不可信的网络区域的用户，通过认证、策略控制可以访问可信区域，如图 1 所示。

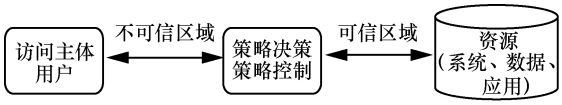

图 1 零信任访问模型

为降低访问过程的安全风险，需要一种持续动态安全访问控制技术，不基于访问主体的网络位置，而是在每一次访问客体被允许访问之前，基于安全和信任状态对访问主体进行安全授权；持续性地监测整个访问过程的安全、评估信任状态；动态调整访问权限，实施细粒度的安全访问控制。

为实现这种目标，还需要更多的网元支撑整个零信任架构。NIST 给出的 ZTA 架构如图 2 所示。

其中，身份管理（ID management）系统和企业公钥基础设施（PKI）主要用于对人员、设备的认证，这是基础。数据访问策略（data access policy）主要是提供资源访问策略，安全信息和事件管理系统（SIEM system）提供整个架构的安全信息和事件管理。同时要集成产业合规政策以及威胁检测等能力，更需要关注持续诊断和减灾（continuous diagnostics and mitigation，CDM）系统。

总体上，零信任架构是以身份为基础，为人和设备赋予数字身份，为访问主体设定最小权限；以业务安全为目标，实现业务隐藏、传输加密、精细控制；以持续信任评估为保障，包括用户信任评估、环境风险判定、异常行为发现等；以动态权限控制为手段，包括基于属性的访问控制基线，基于信任等级的分级访问，基于风险感知的动态权限等。

零信任架构聚焦身份、信任、访问控制、权限等维度的安全能力，而这些安全能力也是信息化业务系统不可或缺的组成部分，所以零信任天生就是一种“内生安全”。某种意义上说，是业务和安全的一次螺旋式升华，从最初的业务系统完成业务目标，安全设备实现安全保障的相互独立体系，融合成为安全和业务紧密关联，再次回到安全和应用的深度聚合。

2.3 零信任架构的关键能力

零信任架构的本质是在访问主体和客体之间构建以身份为基石的动态可信访问控制体系，通过以身份为基石、业务安全访问、持续信任评估和动态访问控制的关键能力，基于对网络所有参

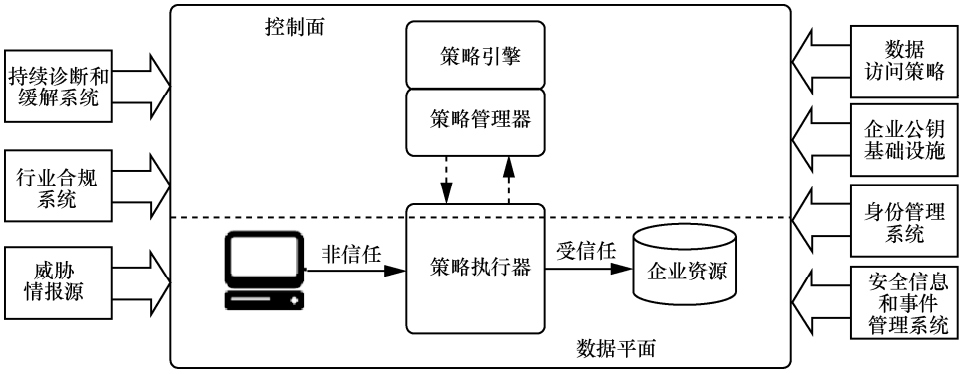

图 2 NIST ZTA 架构

与实体的数字身份，对默认不可信的所有访问请求进行加密、认证和强制授权，汇聚关联各种数据源进行持续信任评估，并根据信任的程度动态对权限进行调整，最终在访问主体和访问客体之间建立一种动态的信任关系，实现先认证后连接的安全模式。为实现这个目标，需要构建零信任架构的关键能力，如图 3 所示。

零信任架构下，访问客体是核心保护的资源，针对被保护资源构建保护面，资源包括但不限于业务应用、服务接口、操作功能和数据等。访问主体包括人员、设备、应用和系统等身份化之后的数字实体，在一定的访问上下文过程中，这些实体还可以进行组合绑定，进一步对主体进行明确和限定。

其中，代理和网关是零信任架构的组成部分，是身份认证、控制策略、动态控制的执行点（policy enforcement point，PEP），但根据业务需要、场景差异，可以和访问主体或访问客体集成，形成整合体，加强访问主体或客体的安全性。在某些场景中，代理和网关亦可以合为一体，成为可信代理，并一般部署在访问客体侧，访问主体侧不需要改动。

实现基于身份而非网络位置来构建访问控制体系，首先需要为网络中的人和设备赋予数字身份，将身份化的人、设备和应用进行运行时组合构建访问主体，在用户进行连接前对主体进行身份认证。

零信任架构关注业务保护面的构建，通过业务保护面实现对资源的保护，在零信任架构中，应用、服务、接口、数据都可以视作业务资源。通过网关实现对暴露面的收缩，要求所有业务默认隐藏，根据授权结果进行最小程度的开放，所有的业务访问请求都应该进行全流量加密和强制授权，业务安全访问相关机制需要尽可能工作在应用协议层。

身份认证通过，不代表该主体就是安全可信的，需要建立信任关系。持续信任评估是零信任体系从零开始构建信任的关键手段，通过信任评估模型和算法，实现基于身份的信任评估能力，同时需要对访问的上下文环境进行风险判定，对访问请求进行异常行为识别，并对信任评估结果进行调整。认证是静态的，信任是动态的，基于主体的信任等级进行动态访问控制也是零信任的本质所在。评估的依据可以来自对终端的感知，也可以来自网络侧的感知，越多的数据源可以做越好的信任评估。

动态访问控制是零信任架构的安全闭环能力的重要体现。建议通过 RBAC 和 ABAC 的组合授权实现灵活的访问控制基线，基于信任等级实现分级的业务访问，同时，当访问上下文和环境存在风险时，需要对访问权限进行实时干预并评估是否对访问主体的信任进行降级。

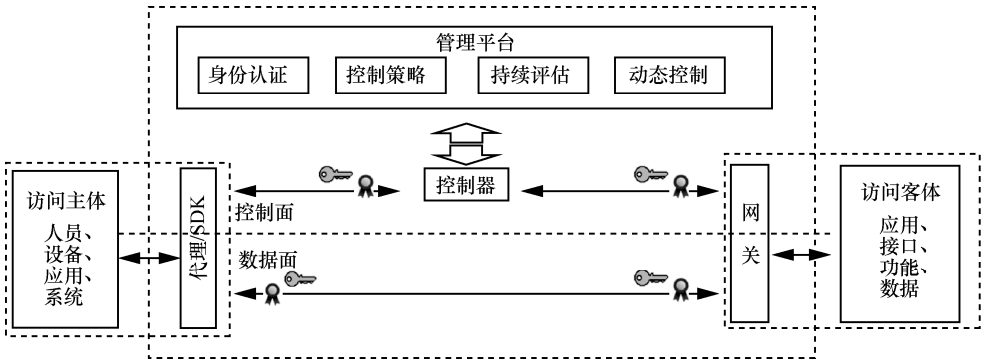

图 3　零信任架构关键能力

3 在 5G 云网中应用防护方案

在 5G 云网环境中，实现基于零信任架构的安全防护方案，主要有以下 3 种模式：客户自建模式、利用运营商虚拟专网建立应用子网的模式、利用运营商公共零信任架构的模式。

3.1 客户自建模式

客户基于零信任架构的应用防护自建模式如图 4 所示，在客户内网构建零信任控制器，在应用前部署 PEP，构建了基于运营商 5G 云网的 OTT 的零信任架构。这是目前 IT 领域最常见的模式，不依赖于运营商网络的可信度。建设成本相对较高、建设周期长，并需要专门的维护人员，对设备、人员的持续信任评估也只能依赖自有信息，对评估的准确性和及时性有极大的挑战。

3.2 利用运营商虚拟专网建立应用子网模式实现零信任模型

利用运营商 5G 网络中的 AAA 服务器、VPN 或微分段能力，建立基本满足零信任理念的解决方案，如图 5 所示。为更好地实现零信任架构，需要在用户 VPN 基础上建立应用子网的理念，即通过技术手段在该子网中仅能访问该应用，以便能实现权限最小化。

服务资源通过专线接入应用子网，客户在通过运营商的 VPDN 模式，即 AAA 服务器认证后，通过 LNS 进入 VPN，需要对 LNS 进行技术升级，支持根据用户属性，分配到特定子网，实现访问授权应用。运营商 AAA 服务器也可以进行进一步优化，充分利用网络感知优势，对客户或设备等访问主体进行信任动态评估，更精确地防范非法接入者。客户可以建立 FW，进行更细力度的控制，但无法和用户身份、动态信任等进行联动。

此方案中，LNS 相当于 PEP，AAA 服务器相当于控制器，但为更好地达到零信任的基本原则，需要对网元进行技术升级，包括支持子网划分、动态信任、动态控制等。

3.3 利用公共零信任架构模式

运营商在 5G 云网中，建设公共零信任控制器、PEP，如图 6 所示。PEP 和客户服务资源建立安全连接，不对公网暴露。客户通过零信任控制器自主服务注册授权用户信息和服务资源信息。客户在访问特定服务资源时，运营商会激活客户认证，认证可以借助运营商 AAA 系统，并可以利用态势感知等系统，对客户动态评估其可信度，

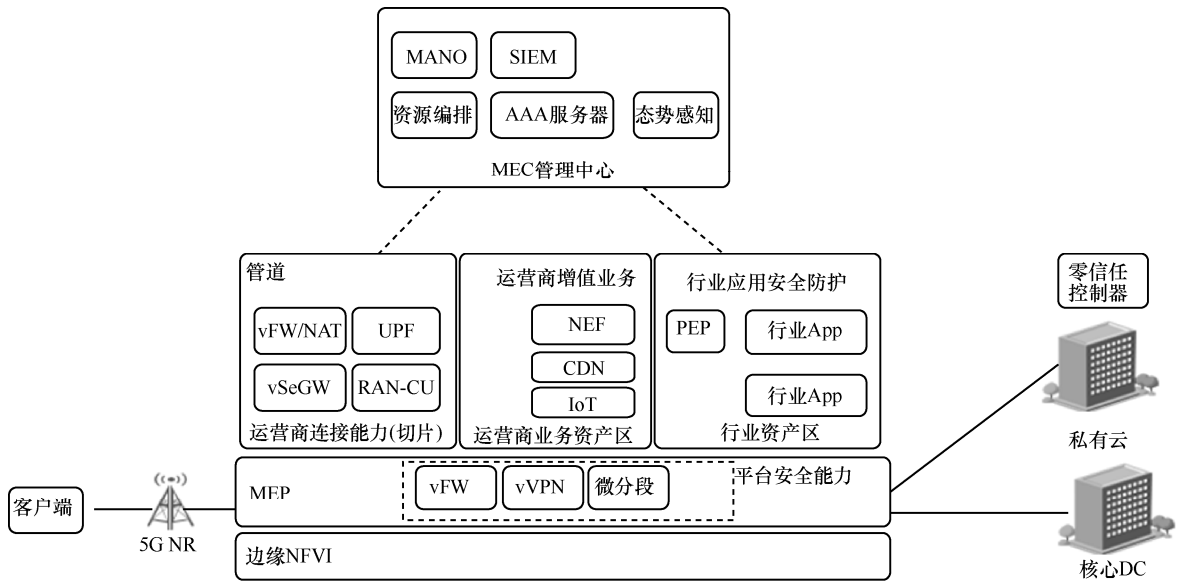

图 4 基于零信任架构的应用防护自建模式

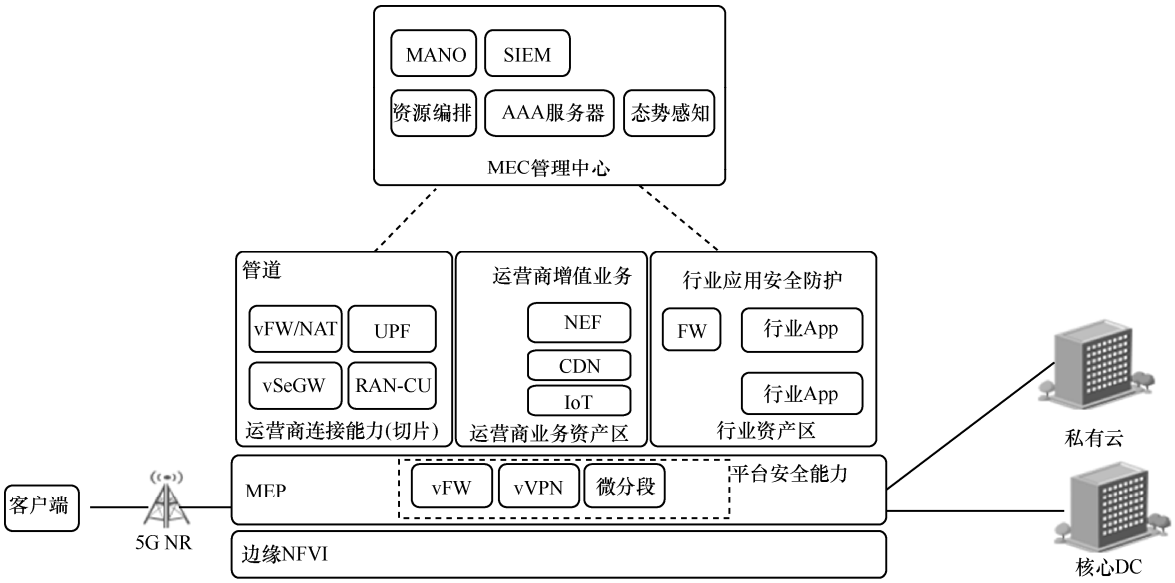

图 5　基于零信任架构的应用防护虚拟专网模式

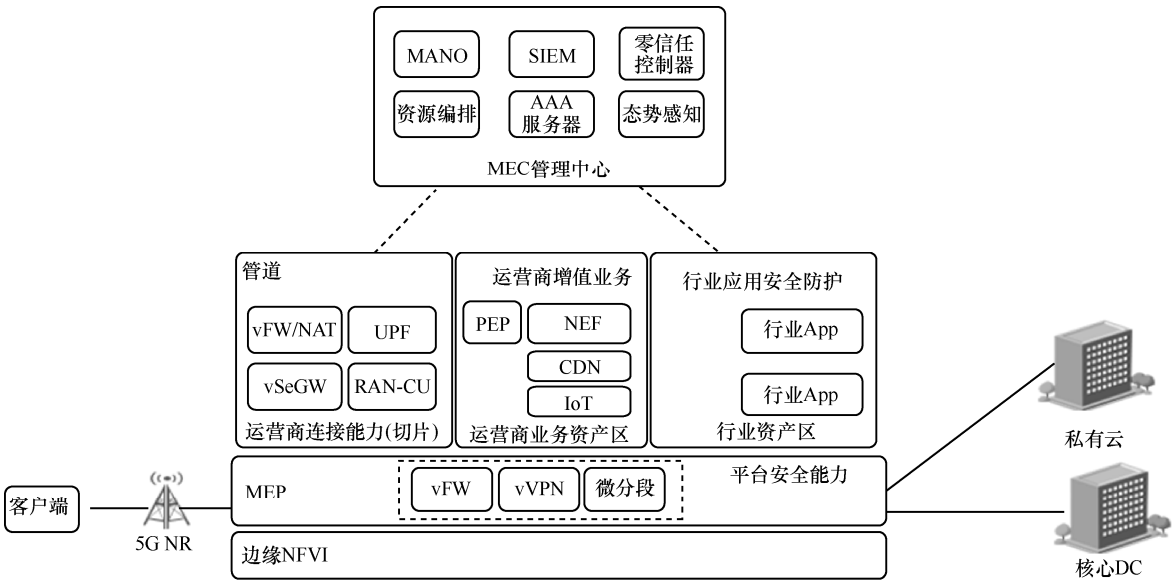

图 6　基于零信任架构的应用防护公共架构模式

在通过认证后，根据控制策略，借助 LNS 和 PEP 联动，控制主体访问客户应用。这种模式客户只需订购服务，成本低，无须专业人员，基于业务场景的人、设备、流程、访问、环境等多维的因素，对访问主体的风险和信任度进行持续度量和评估，并通过信任等级对权限进行动态调整，很好地保护客户服务资源的安全。

在此模式下，零信任架构需要支持多企业模式，并应提供自服务功能，降低运维复杂度。

3.4　方案比较

从满足零信任基本原则和性价比几个方面对上述几个方案进行比较，具体见表 1。

显然，利用运营商公共零信任设施，具有较高性价比。

4　零信任架构在 5G 云网防护常见应用场景

目前，产业界基于对零信任安全框架的理解开展了技术探索和应用研究，尤其是 IT 领域，充

表 1　几个方案的比较

比较项	自建模式	VPDN 应用子网	公共零信任架构
先认证后连接	是	是	是
公网隐藏服务	是	是	是
身份认证设施	自行建立	运营商	运营商
持续评估	仅客户自有信息，评估依据较少	可利用运营商大网信息	可充分利用运营商大网信息
动态访问控制	可细粒度控制	通过子网模式隔离，细粒度控制、动态控制能力较弱	可细粒度控制
客户端复杂度	需要集成代理	无须客户端改造，利用现有 VPDN 技术	无须客户端改造，利用现有 VPDN 技术
维护复杂度	一般	较高	一般
技术成熟度	新技术	依赖已有技术	新技术
总体成本	高	低	低

分证明了技术的先进性以及市场前景，在网络领域或运营商尚未有很多的应用。但随着技术成熟，5G 网络发展，移动应用不断丰富，必然会出现越来越多的应用场景。

对于 5G 而言，利用零信任架构，可以提升 5G 网络自身的安全性，尤其是网络管理平面和 5G 核心网。5G 网络中，虚拟化技术、切片技术、边缘节点等形态对安全提出较高的挑战，可以通过零信任安全技术提高 5G 网络的安全性，满足 5G 网络安全运营的需要。

如在 5GC SBA 架构具备零信任安全的基本要素：基于证书体系的 NFS 认证、基于 NFS ID 的业务访问授权、采用 TLS 保证传输安全。可以考虑通过细化访问策略，最小权限访问，网络层动态白名单，SPA（单包认证）隐藏服务入口，流量检测、可视化地提供持续的安全评估、安全评级、全生命周期的安全管理，通过微分段隔离，强化网络层防护等。

在 SEPP 之间进行设备认证，使用加密传输，可进一步考虑对接口进行流量检测，实现可视化，在 N32-c 通道传递安全相关运行信息，作为对端进行安全评估的参考，根据对端的安全状态进行业务访问控制，专门设置 SEPP 的控制点实现发现和策略控制等。

当然，对于运营商来说，更具有战略意义的是在 5G 行业应用方面，在边缘计算、政企网络中应用，通过零信任技术满足行业用户的安全需求。如在 MEC 复杂环境中，实现不同主体之间的安全接入控制；作为 MEC 的安全组件，对行业应用提供安全防护；安全策略集中管控，满足等保要求等。

典型的行业应用场景有 3 种：远程访问、企业上云以及移动办公。

4.1　远程访问（企业合作伙伴/分公司访问业务系统）

随着网络普及，协作企业互相访问，多地分支机构或分布式办公情况越来越多，采用零信任架构的应用防护很好地满足客户或分支机构访问企业内部应用系统的需求。通过零信任机制，只有身份、设备均验证合法的合作伙伴才能访问业务系统。实现了基于身份的“按需授权”安全策略，合作伙伴只能访问完成工作授权的应用，不暴露其他内网资源。基于零信任架构的应用防护——远程访问场景如图 7 所示。

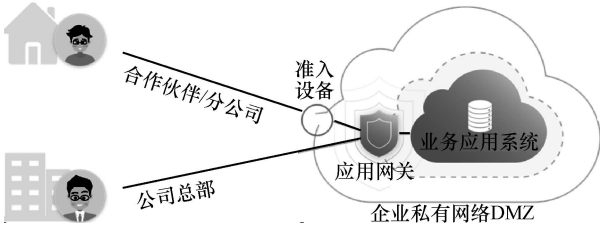

图 7　基于零信任架构的应用防护——远程访问场景

4.2　企业上云

信息化的推进，云计算的普及，越来越多的应用系统从企业自建机房迁移到公共云平台，内部的应用系统也随之迁移到云上，基于零信任的应用防护很好地满足了安全访问云上内部应用系统的需求。

零信任机制屏蔽了基于网络向业务应用系统发起的攻击，网关的“网络隐身”效果有效减小了攻击面。只有身份、设备验证合法的授权用户才能正常访问业务系统。企业既享受了上云的好处，又降低了上云带来的安全风险。基于零信任架构的应用防护——企业安全上云如图 8 所示。

4.3　移动办公

移动互联网发展，效率的提升，要求员工或领导能及时对工作事件进行响应，移动办公、远程办公、居家办公成为趋势，尤其是今年疫情防护期间，大部分员工居家办公。利用零信任机制，无论在政府机关/公司、咖啡厅，还是在分公司/门店，用户无须配置即可访问内网应用，使用更便捷。内外网统一验证用户、验证设备、限制授权，帮助企业实现了“零信任”网络安全理念。基于零信任架构的应用防护——移动办公如图 9 所示。

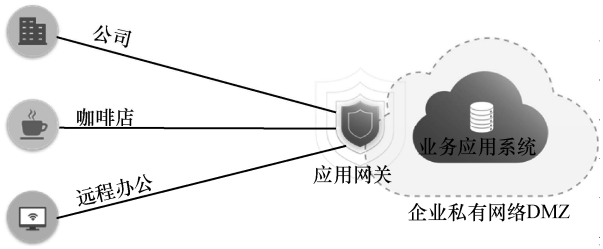

图 9　基于零信任架构的应用防护——移动办公

5　结束语

零信任安全架构对传统的边界安全架构思想重新进行了评估和审视，并对安全架构给出了新的思路，不信任网络内部和外部的任何人、设备、系统和应用，而是应该基于认证、授权和加密技术重构访问控制的信任基础，并且这种授权和信任不是静态的，它需要基于对访问主体的风险度量进行动态调整。

零信任架构很好地满足了 5G 云网融合时代的需求，远程办公、移动办公、无处不在的信息化，需要用新的技术在提供便利的同时保障安全。无论对于运营商自身网络安全的提升，还是对于

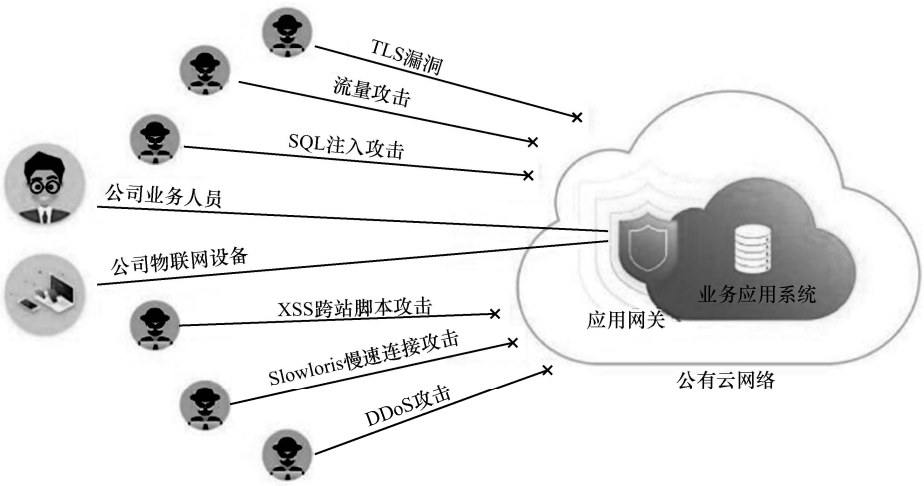

图 8　基于零信任架构的应用防护——企业安全上云

其客户安全能力的提升都具有重要意义。

参考文献：

[1] OSBORN B, MCWILLIAMS J, BEYER B, et al. BeyondCorp: design to deployment at Google[Z]. 2016.

[2] SCA. SDP specification 1.0[S]. 1994.

[3] 网络安全架构：零信任架构正在标准化[EB]. 2019.
Network security architecture: zero trust architecture is being standardized[EB]. 2019.

[4] 埃文·吉尔曼，道格·巴斯. 零信任网络在不可信网络中构建安全系统[M]. 奇安信身份安全实验室，译. 北京：人民邮电出版社, 2019.
GILMAN E, BARTH G. Zero trust networks[M]. Translated by Qi-Anxin Technology Group Inc.Beijing: Posts & Telecom Press, 2019.

[5] 吴伟，张文强，杨广铭，等. 5G 承载网的“SRv6+EVPN”技术研究与规模部署[J]. 电信科学, 2020, 36(8): 43-52.
WU W, ZHANG W Q, YANG G M, et al. SRv6 +EVPN technology research and scale deployment of 5G bearer network [J]. Telecommunications Science, 2020, 36(8): 43-52.

[6] 马培勇，吴伟，张文强，等. 5G 承载网关键技术及发展[J]. 电信科学, 2020, 36(9): 122-130.
MA P Y, WU W, ZHANG W Q, et al. Key technologies and development of 5G bearer network [J]. Telecommunications Science, 2020, 36(9): 122-130.

[7] 何晓明，岳萍，卢泉，等. 面向 5G 承载的 IP RAN 演进及关键技术[J]. 电信科学, 2020, 36(3): 125-135.
HE X M, YUE P, LU Q, et al. Evolution and key technologies of 5G-oriented IP RAN[J]. Telecommunications Science, 2020, 36(3): 125-135.

[作者简介]

何国锋（1976–），男，博士，中国电信股份有限公司研究院应用安全研究所所长、教授级高级工程师，主要研究方向为移动应用安全、Web 应用安全、代码安全、PKI 体系等。