零触碰与零信任
Zero Touch and Zero Trust

李军 /LI Jun，胡效赫 /HU Xiaohe
（清华大学，中国 北京 100084）
(Tsinghua University, Beijing 100084, China)

DOI：10.12142/ZTETJ.202103010
网络出版地址：https://kns.cnki.net/kcms/detail/34.1228.TN.20210617.0922.004.html
网络出版日期：2021–06–17
收稿日期：2021–05–10

摘要：随着网络规模持续增加、应用日益复杂以及动态性不断增强，网络自动化的需求愈发迫切。网络转发呈现零触碰的趋势，以实现策略编排的自动化为目标。网络安全呈现零信任的趋势，以实现身份访问的自动化为目标。从基本理念、核心组成以及工业实践的角度对零触碰和零信任进行分析，阐述网络自动化的必要性与发展情形。

关键词：网络自动化；网络转发；零触碰；网络安全；零信任

Abstract: With the increasing scale of networks, complexity of applications, and dynamics of scenarios, there has been an urgent demand of network automation. Network forwarding is becoming zero touch, automating the policy orchestration. Network security is becoming zero trust, automating the identity and access management. Zero touch and zero trust networks are analyzed in three aspects, i.e., basic concept, core components, and industrial practice, and the necessity and development of network automation are described.

Keywords: network automation; network forwarding; zero touch; network security; zero trust

在学术研究中，研究者有时会把网络的转发与安全“正交化”，即把网络转发与网络安全“解耦”开来，以便简化问题、“分而治之”。按照这个原则设计出来的系统架构和解决方案，符合实际管理体系中的人员分工，自然也就比较容易落地应用。然而，网络的转发与安全事实上是高度相关、密不可分的。不发生网络转发的行为，就不存在网络安全的问题。而没有网络安全的保障，网络转发就容易受到攻击。网络转发协议、拓扑和流量的变化，必定会引发网络安全的机制设计、技术构成和实现方式的改变。而网络安全的完备性和有效性，又是与网络转发的私密性、完整性和可靠性交织在一起的。

通常所说的网络，主要是指交换和路由机制对网包的操作。伴随着网络规模和流速的指数增长，协议和应用的日趋纷繁，以及人类生活对网络依赖性的不断加剧，通过人工配置来管理网络的方法经常捉襟见肘、状况百出。网络管理人员难以应对“复杂大系统”。网络自动化成为日益迫切的需求。在这样的背景下，零触碰网络应运而生。

同时，随着网络虚拟化和动态化的不断增强，不但以工作环境为网络物理边界的安全防护早已无法满足移动办公和居家办公的普及要求，大量企业信息系统“云化”对逻辑边界的安全需求，以及企业核心资产面临的巨大数据安全挑战，也使得原有的“一次认证、一路畅通”的信任模式不再可靠。因此，我们需要建立零信任网络。或者说，对用户或终端的信任只能建立在持续的认证、鉴权、“健康体检”和行为监测控制的基础之上。

无论是零触碰还是零信任，本质上都是对网络自动化迫切需求的反映。

1 网络转发与零触碰

网络转发主要依靠路由器和交换机来完成，而这些物理资源并不是随时随地更换或增减的（至少变化频率不会很高）。此外，它们在运行软件时所遵从的协议，相对而言也是“静态”的，不会频繁切换或升级、卸载。网络转发设备或虚拟设备相互连接构成的网络拓扑及其承载的具体功能，主要是由策略（涵盖配置和规则等说法）编排决定的。

严格来说，这些策略也是程序的一部分，但不是在硬编码和预编译（机器语言，即二进制代码）之后才被绑定到物理设备或逻辑设备中的，而是在运行期间甚至运行时，依据网络设计目标和资源情形“动态”注入的。通常这些策略也会需要预编译，以紧

凑的数据结构来满足性能要求。

传统上，策略编排是由网络管理员来完成的。他们运用特定的网络连线和设备配置来完成网络设计目标。Google 研究报告显示，超过 7 成的网络故障发生在网络管理操作过程中[1]。在网络的规模、复杂性和动态性远超过人工能力范畴的情况下，策略编排需要新的范式来保障网络设计的效率和稳定性。

零触碰的宗旨是最小化网络管理生命周期中的人工介入，并最大化程序与工具在网络管理中的占比。其中的关键在于实现自动化的策略编排：管理员只需要关注网络设计的目标“是什么”，无须考虑连线与配置“怎么做”。零触碰网络的实现可以参照计算机程序编译和芯片设计的电子设计自动化（EDA）工具。网络自动化和程序设计都是把高级语义映射为机器代码的过程，而芯片设计面对的布局布线约束与网元资源及其连接的约束也有相似之处。

零触碰网络的提出不仅源自云计算和网络代际升级带来的管理挑战，还得益于软件定义网络（SDN）为网络开放创新打下的基础。在 SDN 的理念下，零触碰进一步融入闭环控制、软件验证、编程语言等多领域机制。这也充分说明计算机网络是信息科学中典型的交叉融合应用场景。

零触碰网络依托于一整套网络自动化系统和一系列策略编排核心技术。这主要体现在：（1）在系统设计方面，零触碰网络遵循抽象化原则，通过管理闭环来保障网络稳定性；（2）在管理员接口设计方面，零触碰网络遵循声明式编程范式，以提高系统易用性；（3）在模块实现方面，零触碰网络通过算法优化来应对规模增长带来的效率问题。

从网络自动化架构来看（如图 1 所示），零触碰分别体现在 3 个层面上。

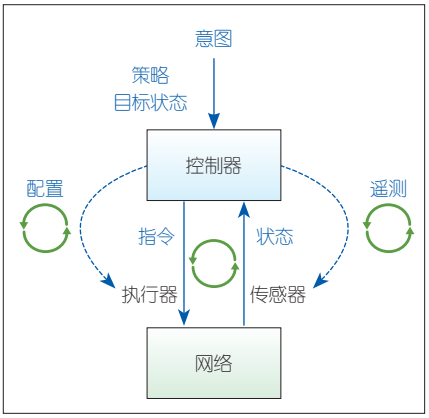
最上层是意图驱动网络（IBN）重点关注的，也是零触碰的关键。该层将管理平面用户或应用的意图，映射为逻辑集中的控制平面可以理解的策略。这使网络管理员从庞杂细碎的手工配置中抽出身来，以便他们把主要精力聚焦在网络设计目标的确定和达成上。这里涉及的主要是策略语言，它包括策略描述的定义和编译（也称综合）。网络策略通常被分为转发策略和其他网络服务策略，而服务策略主要包括安全策略。

中间层是 SDN 关注的核心，以控制器的能力来支撑零触碰。基于网络拓扑与协议，同时根据网络策略和状态，该层可求解策略部署方案，并验证策略的一致性。其中，策略和状态组成闭环控制的整体。零触碰根据特定的网络状态部署相应的策略以实现管理员意图。细化来看，策略部署的正确性也需要一个下发和校验的闭环来保障，状态获取的针对性也同样需要一个配置和监测的闭环来支撑。

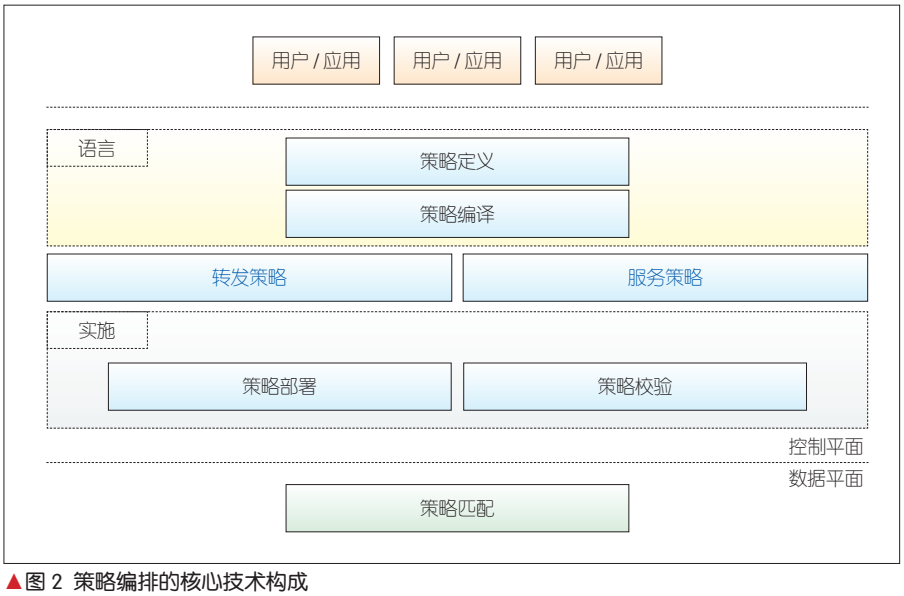
最下层是分布的数据平面。该层完成网络流量的策略匹配与状态监测，并执行相应的网络功能。

图 2 展示了策略编排在网络自动化系统架构中对应的核心技术构成。

策略语言中定义和编译环节的关键在于意图基元的设计。这种设计背后反映的是对网络流量、协议和拓扑的描述，以及对生成、修复等不同管理操作的构建。在策略实施中，策略部署的关键在于求解给定网络约束下策略分配和部署网元（或节点）选取的优化问题，策略校验的关键在于对拓扑和网元的建模以及适应性算法的设计。策略匹配的关键在于软件算法优化和硬件平台加速。整体来看，当前的策略编排技术能够针对具体的网元和拓扑需求抽象出特定模型，并能应用特定算法。但从系统性的角度看，实现零触碰的统一化和插件化还有很多工作要做。



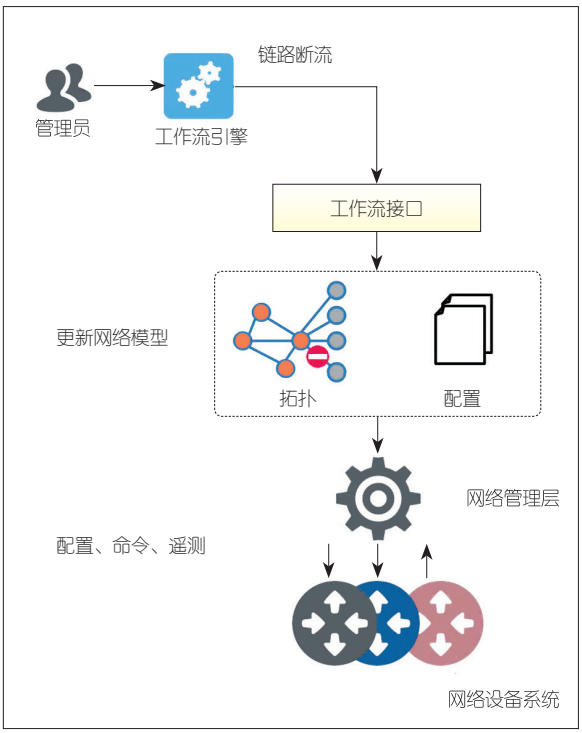
▲图 1 网络自动化系统的逻辑架构



▲图 2 策略编排的核心技术构成

零触碰网络的理念来源于 Google 在 2016 年发表的学术论文[1]。欧洲电信标准化协会（ETSI）后续成立了面向 5G 的零触碰网络与服务管理工作组。与零触碰相类似的理念包括 2016 年 Juniper 公司提出的自动驾驶网络（SelfDN）和 2017 年 Gartner 公司提出的 IBN。这些理念的共性都是要实现自动化的策略编排，减少网络基础设施的交付时间，并降低网络故障的发生频次。

在零触碰方面上，走在业界前沿的是 Google、Microsoft、阿里云等大型云计算厂商。零触碰网络的业界实践可参考 Google 的设计方案（如图 3 所示）。该方案在系统架构上与图 1 所描述的网络自动化架构相似。阿里云在 2019 年发表了针对骨干网接入控制的策略编排，定义并实现了特定领域的意图。拥有面向云数据中心和混合云场景的网络自动化方案的代表性厂商有 Apstra、Intentionet 等。在零触碰产品的市场认可和推广方面，向下需要扩充对底层网元功能和协议类型的适配广度，向上需要丰富典型业务场景的操作意图参考设计，以满足网络连通到网络安全等多样需求，实现系统的“能观”与“能控”。



▲图 3 Google 的零触碰网络架构[1]

2 网络安全与零信任

信任是人际交往和交易中影响效率的重要因素，因此网络访问或网络交互也必然依赖于信任的建立。关于零信任，业界流传着这样一句话：“永远不要信任，始终进行验证，实施最小权限。”其实，不是“永远不要信任”，而是“不要永远信任”。也就是说，应将传统的一次性认证改为经常性查验，而且不是严格意义上的不间断地“始终进行验证”。通常，人们还是采用定期采样或事件触发的验证，并给予一定期限和条件的授权。

零信任的实现，不仅需要引入新技术或新设备，还需要借助微隔离（MSG）以及细粒度的边界策略。在虚拟网络特别是云场景中，相对于传统模式来说，规模和复杂性增加很多，因而工程实现的难度也将增加。在解决新问题、引进新能力的同时，零信任的实施也牵涉更多的人力和物力资源。适度的信任和自动化，是在特定安全等级下降低成本、提升效率的良好途径。

当然，面对自带设备（BYOD）和 5G 带来的接入多样化，应用与系统的日趋云化，以及社会组织、网络安全的态势改变，信任和风险总是相互关联的。

零信任的前提是实施最小特权，而零信任的基础是实践动态认证。不同应用场景下的零信任系统，会因地制宜地选择和融合多种网络安全和数据安全技术。但身份认证和边界控制是所有零信任实践的核心。

最小特权也称最小授权，是信息安全的基本模型之一。最小特权的概念最早源于容错理论。它涉及特权分离和完全仲裁等一系列原则。在网络安全实战中，它可以减少应用的公共可见性，从而显著减小攻击面。一般情况下，传统网络物理边界的失效，并不意味着“无边界”。网络不同安全区域之间的逻辑边界是实施安全分级（等级保护）治理的前提条件。普通用户对网络边界无感并不意味着完全没有边界。零信任恰恰是在软件定义边界（SDP）和云访问安全代理（CASB）等技术体系的基础上整合出来的解决方案。当然，边界的极致就是终端。零信任也可以在终端侧部署，以解决传统边界防护在端到端远程访问场景下的诸多问题。

动态认证则是身份权限管理（IAM）中身份验证和鉴权的延伸。从最简单的“五元组”接入控制表（ACL），到基于角色的接入控制（RBAC），再到基于属性的接入控制（ABAC），都是网络安全中身份认证不断精细化的体现。然而，除了简单的定期复检（超时）外，它们大多不会“与时俱进”，反映即时的变化。而对用户、设备、网络“身份”的识别和认证，以及对网络安全相关状态、流量、行为甚至“全息”数据的掌控，则是安全身份判定逐步动态化的体现。实际上，这和大数据技术中常用的“用户画像”概念十分类似，它们都通过精准定位来服务对象，以达到提供精准服务的目的。零信任正是通过精细化、动态化的风险评估，才实现了相应的接入或准入控制，在空间和时间上为网络提供最大程度的防御。

目前，业界参考的零信任理念大

多基于美国国家标准研究院（NIST）于2020年发布的《零信任架构（ZTA）》（2019年以建议为名发布第一版草案）。其中，零信任的核心技术被归纳为“SIM”。这里，“S”是SDP，“I”是IAM，“M”是MSG。市场上已经推出的零信任产品则是在厂家原有技术基础上扩充而来的。这些产品或是基于云安全联盟（CSA）的SDP规范（如图4所示），或是参考Google的BeyondCorp（如图5所示）。

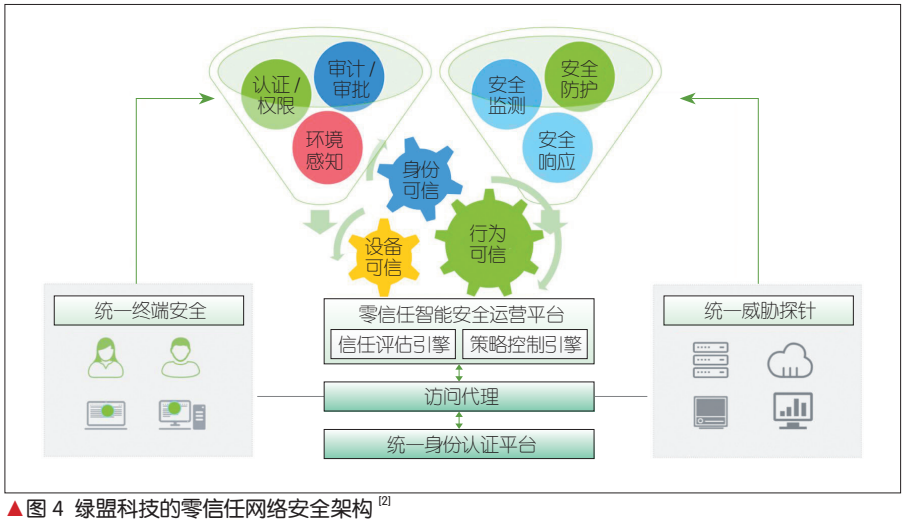
其实，还有一个技术框架可以被整合、升级，并作为零信任技术的基础，那就是TNC（可信网络连接）。TNC经历过Cisco和Microsoft两大阵营的多年竞合，有IETF系列协议层面的标准RFC支撑，在身份和安全状态、情报等数据交换格式上具备扎实的基础，利于推进开放兼容，避免形成厂商锁定。

3 结束语

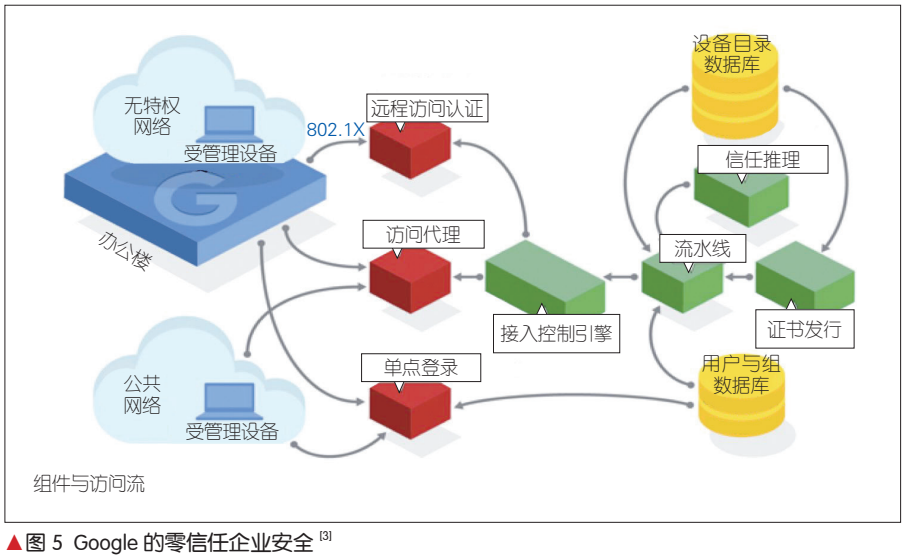
近年来，网络领域最主要的变革都源于网络虚拟化和SDN。无论是意图驱动网络，还是自动驾驶网络，它们都指向网络自动化，即零触碰。而这一切在网络安全方面的反映，就是零信任。

无论是零触碰还是零信任，它们的关键都是实现闭环。从业务的视角看，它们实质上是基于反馈控制的网络编排和信任管控自动化。有趣的是，SDN和零信任都是Google率先验证和推出的。SDN将控制平面与数据平面分离，并将分布、自治的网络升级为集中与分布式结合的控制系统。作为经典实践，Google的B4显著提升了网络带宽的有效利用率。较为完整的零信任概念由市场分析和咨询公司Forrester于2010年提出。之后，Google经过7年时间，成功地将零信任全面上线部署。

总之，以零触碰和零信任为目标的网络自动化，已经成为大势所趋。它正在不断推进技术创新、产品研发和服务落地。



▲图4 绿盟科技的零信任网络安全架构[2]



▲图5 Google的零信任企业安全[3]

参考文献

[1] KOLEY B. The zero touch network [EB/OL]. [2021-03-18]. http://www.cnsm-conf.org/2016/presentations/CNSM2016-Keynote1-Koley.pdf

[2] 绿盟科技. 零信任安全解决方案[EB/OL]. [2021-03-18]. https://www.nsfocus.com.cn/html/2020/210_0608/129.html

[3] BeyondCorp. Run zero trust security like Google [EB/OL]. [2021-03-18]. https://beyondcorp.com

作 者 简 介

李军，清华大学自动化系研究员、博士生导师，中国电子学会计算机工程与应用分会副主任委员；主要从事网络与网络安全等领域的教学和研究工作；主持了多个“863”、国家重点研发计划和自然科学基金等项目；作为第一完成人荣获2014年中国电子学会科学技术奖二等奖；著译中外教材3部，发表学术论文100余篇，获得美国专利2项、中国发明专利20余项，且多数成果已商用。

胡效赫，清华大学计算机系博士后；主要从事软件定义网络、高性能网络处理、安全隐私等方向的研究工作；先后参与国家重点研发计划和自然科学基金等项目；发表论文10余篇，获美国专利1项、中国发明专利2项。