让黑客进不来；在局域网不同安全等级网络之间，设置安全网关、防火墙等技术手段进行逻辑隔离，保证网上不同密级信息相对独立、受控交互。

（2）全网布哨、追踪溯源

为及时发现和定位网络攻击，做到早感知、早告警、早处置，可运用“全网布哨、追踪溯源”安全策略。建立网络监测预警体系，确保多层覆盖、上下贯通；在各个网络节点和末端广布“监视器”、“摄像头”，对网络流量、传输信息、用户行为进行有效监控，提前发现安全威胁，及时响应攻击行为；关联分析各种网络安全事件，追踪定位攻击源头和传播路径，为后续处置提供依据。

（3）以攻助防、以攻验防

为提高网络安全水平，检验网络安全防护能力，可采取“以攻助防、以攻验防”战法。通过加强对攻击技术的研究和运用，逆向分析我国网络和系统存在的后门漏洞和薄弱环节，评估风险危害程度，为弥补不足、完善体系提供依据；国家安全专业人员应组织经常性网络攻防演练，建立互联网和局域网网络攻防和评估的专业队伍，以背靠背方式真攻真防实评，实际检验防护水平，促进整体安全防护能力不断提升。

3.2 应对攻击策略

主要体现有的放矢、针锋相对，阻止黑客发起各类网络攻击。

（1）隐真示假、诱敌深入

利用“蜜网”、“蜜罐”技术，在互联网或局域网的某些网络主机中预置虚假“重要信息”，误导黑客按我方意图进行攻击渗透，消耗其攻击资源；通过在网络中故意留下“破绽”，诱敌上钩，强化监控，从而发现攻击源头，捕获攻击数据，了解攻击技术和攻击企图，为反制行动提供“目标”，达到保护我目标网络和关键信息的目的。

（2）分流减压、疏散配置

拒绝服务攻击的目的是造成网上信息“淤积阻塞”，进而致瘫目标网络。应对拒绝服务攻击可采用“分流减压、疏散配置”战法。通过预设网络流量临界值，限制服务器能够接受的最大访问请求，保证服务器在异常情况下仍能正常工作；增加服务器数量，或采用分布式计算、云计算等技术，把原本集中的服务“打散”安装在多台机器上，实现访问流量负载均衡，减轻单点承受的压力，避免网络停转、服务中断。

（3）“热点”聚焦、筛查封控

网络意识形态渗透和舆情操控依赖信息传播，可采取“‘热点’聚焦、筛查封控”策略进行防范。针对互联网上有害信息传播渗透和热点舆情发展动向，通过关键字检测分析、上下文语义关联等方法对信息传输内容进行筛查监控；运用封锁网址、域名劫持等技术对境外反动网站实施封堵，必要时进行毁瘫攻击；强化局域网终端管理，“堵源头”与“控末端”结合，在用户终端上对非法信息、非法操作进行实时监控，严防各类有害信息的访问传播。

3.3 后续补救策略

主要体现为“牺牲局部、应急保底”，是网络与信息系统已遭攻击情况下的应对之策。

（1）断臂自救、要点优先

孙子曰：“必有损，损阴以益阳”。意为形势危急时，要作出某些局部的牺牲以保全大局。借鉴此思想，可在必要时采用“断臂自救、要点优先”安全策略。网络攻防对抗易攻难防，如果黑客已成功入侵我网络，出现局部病毒感染、系统运行效率降低情况时，要迅速果断地切断“病源”和全网的连接通路，避免危害进一步蔓延扩散；同时，集中人力资源和技术手段，把守交通、水利、电力等核心网络设施和信息系统，确保关键部位安全可控，待入侵影响得以清除后，再逐步恢复初始正常状态。

（2）储备“后手”、保住底线

充分考虑黑客成功破坏我交通、水利、电力等核心网络，瘫痪关键系统等后果，预先建立国家信息安全应急处理指挥协调制度，制定信息安全应急响应预案，明确保障重点、责任分工、操作流程和处置权限；建设国家分布式容灾备份系统，研发配备灾难恢复技术装备，采取多种手段保障通信联络，具备网络路由快速重组和关键数据备份能力，确保国家重要信息系统和核心数据安全。

4　结束语

网络空间安全没有捷径可走，也没有一劳永逸的办法，需要超越习惯思维定式和传统经验模式，瞄准黑客最高水平，着眼最复杂最困难局面谋篇布局，既要研究黑客采用的最新攻击技术和攻击策略，更要针对攻击策略研究安全防护策略，做到知彼知己，百战不殆。

参考文献：

[1]敖志刚.网络空间作战机理与筹划[M].电子工业出版社，2018.

[2]蒋天发，苏永红.网络空间信息安全[M].电子工业出版社，2017.

[3]杨林，于全.动态赋能网络空间防御[M].人民邮电出版社，2016.

基于 UEBA 的网络安全态势感知技术现状及发展分析

◆徐飞

（公安部户政管理研究中心　北京　100070）

摘要：近年来，随着信息技术的快速发展和信息资源重要性的日益凸显，网络安全事件的数量与频率大幅提升，攻击者组织化、目标定向化、技术多样化的攻击行为成为新的趋势。偏重于外部攻击全局预警的态势感知和侧重于内部威胁检测的用户实体行为分析（User and Entity Behavior Analytics，UEBA）衔接，可以高效解决以人、资产、应用为维度的账号安全和数据安全问题。本文总结了基于 UEBA 的网络安全态势感知技术现状，并从大规模异构平台安全管理角度，对未来的发展方向进行了分析。

关键词：网络安全态势感知；UEBA；规则匹配；特征分析；机器学习

党的十八大以来，习近平总书记站在党和国家的全局高度，就网络安全和信息化工作提出了一系列新理念新思想新战略，科学分析了信息化变革给我们带来的机遇和挑战，系统阐述了事关网信事业发展的重大理论和实践问题，明确做出了关于建设网络强国的战略部署。近年来，我国网络安全顶层设计不断完善，《中华人民共和国网络安全法》、《中华人民共和国密码法》、《信息安全技术 网络安全等级保护基本要求》等多项法律法规、配套制度及有关标准陆续发布，政府、金融、公安、电信等行业均以“合规性”为目标，正在大力推进网络安全建设。

随着区块链、人工智能、5G、IPv6 等新技术快速发展、逐步应用，以高级持续性威胁（Advanced Persistent Threat，APT）、高危零日漏洞利用（0-day）等为代表的新一代攻击渗透技术日新月异；同

时，攻击者除了通过技术手段进行“正面”突破外，还会着重搜集人员和管理上的漏洞，从社会工程学角度尝试“绕行”。故此，基于规则匹配和特征分析等被动防御技术构建的传统安全防护体系（如防火墙、入侵检测系统、反病毒软件等）已明显存在不足，亟需提升风险排查、威胁预警、溯源取证、应急处置等主动防御能力。

1　网络安全态势感知

网络态势是指由各种网络设备的运行状况、网络行为以及用户行为等因素所构成的整个网络的当前状态和变化趋势[1]。网络安全态势感知是指在大规模网络环境中，对能够引起网络态势变化的安全要素进行获取、理解、显示以及未来趋势预测[2]。态势感知最初用于安全态势可衡量、安全指标 KPI（Key Performance Indicator）考核，通过安全评估、漏洞等级、安全基线、资产赋值等关键点进行评分，根据地域、资产、风险、业务系统等不同维度进行安全态势展示。

2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上明确指出“全天候全方位感知网络安全态势”。这个要求恰恰对态势感知的建设目标做出了准确描述：“全天候”是时间纬度，贯穿过去、现在和未来；“全方位”是内容维度，要求检测分析分析的对象覆盖面广（至少包括网络流量、终端行为、内容载荷三个方面）、有深度。通过多源异构网络安全数据和事件的获取、理解、分析和评判，客观反映网络中发生的攻防行为，从时间和空间两个维度，从 OSI（开放式系统互联通信参考模型）1~7 层整体角度从更高层次直观、动态、全面、准确、细粒度地感知各类网络攻击行为，进而提升主动防御能力，这正是态势感知的意义所在[3]。

目前，国内主流的态势感知产品或解决方案从技术实现上看可大体分为基于流量的态势感知、基于 SIEM（Security Information Event Management，安全日志事件管理）的态势感知、基于产品集成的态势感知等 3 种类型。

表 1 国内主流态势感知产品或解决方案对比

类型	基于流量	基于 SIEM	基于产品集成
说明	利用传统的基于特征安全检测技术，融合威胁情报，提高安全检测的深度，通过告警合并、攻击链分析等技术优化安全告警后进行可视化展示	通过日志解析、处理与分析展示安全威胁与事件，利用关联分析、机器学习算法降低安全告警数量与误报，融合资产、漏洞等上下文信息对网络安全整体态势进行可视化展示	将某几款产品（如防火墙、Web 应用防护系统等）作为探针，将相关告警集中到态势感知平台进行大屏展示，属于整体的解决方案
优势	部署非常方便，可以高效利用检测与威胁情报能力	展示要素比较丰富，资产、漏洞、威胁、告警只要接入数据均可展示，作为日常安全监控平台，方便安全事件追踪溯源	安全探针与态势感知平台整合比较好，在威胁检测、安全分析与可视化展示方面已经进行了优化，且态势感知平台可与探针设备进行联动
劣势	此类产品实质上属于检测设备，在资产、日志、漏洞的接入与关联分析等方面能力较弱，对安全事件进行追踪溯源不便	本身并不具备安全检测能力，需接入其它安全设备的告警日志来进行二次加工与分析，故实施复杂度、成本比较高，对其它安全设备有依赖	对于第三方设备的兼容性存在缺陷，如果现网已存在或拟新增其它品牌安全设备，定制化成本很高

与忽视采集分析安全监测数据且不主动掌握安全状况的早期网络安全运营模式相比较，通过建设与态势感知相关的系统平台，加强对安全数据的统计汇总和对安全状况信息的主动展示，确实具有较大的积极意义，并且也确实能够揭示一些中长期存在的安全问题，并推动展开优化调整安全策略等解决措施。但这种依赖“监测事件汇聚+大屏展示”的建设导向，即展现宏观的整体安全状态并罗列微观的安全事件信息，缺乏在中观层面对安全信息进行结构化组织与聚合呈现的能力，通常存在“有态无势”“感而不知”“感而不为”等问题[4]。针对复杂多变的敌情，网络安全态势感知亟需由面向掌握宏观态势和安全策略调整的“监测型”向注重高水平威胁对抗和响应行动的“战术型”转变。

2　基于 UEBA 的网络安全态势感知技术现状

UEBA 前身是 UBA（User Behavior Analytics，用户行为分析），最早用于购物网站上，通过收集用户搜索关键字，实现用户标签画像，并预测用户购买习惯，推送用户感兴趣的商品。这项技术很快就被应用到网络安全领域，通过建立用户行为基线、进行状态跟踪，在此基础上增加对设备和应用的纳管，监测用户的同时，将与用户互动的资源放到同样重要的位置。

UEBA 相较于传统的 SOC/SIEM（Security Operations Center/Security Information Event Management，安全运营中心/安全日志事件管理），不关心各种海量告警、不聚焦某条高级事件，而是对“异常用户”（即特权账号被盗用）和“用户异常”（即合法的人做不合法的事）行为具备高命中率，使异常事件的告警更符合业务场景。以设备重启为例，SOC/SIEM 会认定为高等级的安全事件并告警，而在 UEBA 的理解中，先判断重启的用户是谁？此用户在过去的一年内每月固定时间是否都有类似的行为？如果都有，即可不发送告警，仅作记录，误报率大幅降低。安全运营人员有更多的精力去关心真正的安全事件，内部威胁特别是数据泄密在实践中被有效发现。

UEBA 侧重于内部威胁检测，态势感知强调的是全局预警，两者有效衔接，可以解决以人、资产、应用为维度的账号安全和数据安全问题。除了考虑网络侧的安全问题，尤其要重视业务侧面临安全威胁的特点，即用户行为是符合访问控制规则的，相关操作都不带有如 SQL 注入、跨站脚本攻击（XSS）等明显的攻击特征，且存在“低频长周期”的情况，这对基于 UEBA 的网络安全态势感知关键技术提出了更高的要求。从数据收集到最终决策，基于 UEBA 的网络安全态势感知包括数据采集、用户画像、判别规则生成和多规则的联合决策等主要功能。

2.1 多源异构数据采集

多源数据异构性是指生成数据的设备和系统之间以及数据类型本身之间的差异[5]。传统 SOC/SIEM 的数据采集，需要各种日志规格化入库，即每接入不同类型的设备日志时定制 syslog 的格式，故难以快速实施。以事件等级字段为例，有的安全设备使用标准 syslog 且定义清晰（0-7），而有的采用私有 syslog，定义并不清晰，读懂高等级的日志可能需要厂商的配合。“易采集”的基本要求在于能够快速采集到结构化、非结构化日志，使用全文分布式索引，支持数据格式

的动态解析、实时流式分析，实现百度式快速检索，提供通用的 API 接口等。同时，数据源除了网络流量、安全设备告警、应用系统日志和威胁情报之外，还更关注用户视角，接入门禁刷脸日志（第二代居民身份证识别记录）、VPN 日志、HR 日志（入职、离职、岗位变动等信息）、OA 日志、工单日志等场景数据。

2.2 上下文感知与用户画像

上下文感知就是系统通过自动收集和分析用户的信息，利用上下文信息智能判断用户行为并提供高效率的信息交互，从而实现对用户服务的人性化。上下文感知集中体现了普适计算中以人为服务中心的理念[6]。举例来说，当智能手机的传感器收集到足够的信息（日历、位置、邮件、提醒等），处理器通过对信息融合、建模、推理等方法，判断使用者正在会议室开会，自动设置为震动模式，非重要的电话可选择自动语音留言或拒绝接听。

当上下感知应用在基于 UEBA 的网络安全态势感知时，通过分析用户是否在常用地点（IP 地址）、常用时间（工作时间、非工作时间）登录，从而智能判断是否触发相关告警，这区别于传统的防护策略，即常用地址、常用时间都是基于历史基线建模分析得出，而非配置的。

用户画像，即用户信息的标签化，是通过收集与分析消费者社会属性、行为习惯等主要信息后，抽取用户信息并进行标签化和结构化处理，完美地抽象出一个用户的全貌。用户画像是一个或一类真实用户的虚拟抽象，是基于一系列实际数据的虚拟用户模型[7]。用户画像技术的关键是标签系统的设计与构建，标签分为两类，一是基础数据（包括年龄、地区、性别、职业等信息），二是通过基础数据分析而来的高度提炼的特征标识。

在基于 UEBA 的网络安全态势感知中，使用同类用户横比和历史基线环比的方法来发现异常、定义标签并对权重进行赋值，根据分值来展现高风险前几类人群供安全运营人员来决策。

表 2 用户画像标签示例

标签	权重分值	说明
非常用时间访问	1	
非常用地点访问	1	源 IP 为普通 IP
	5	源 IP 属于 IP 信誉库
疑似账号盗用	3	业务账号
	6	管理员账号
疑似绕行访问	2	有日志
	5	无日志
疑似越权操作	1	一般业务
	5	核心业务
疑似盗取资料	4	一般资料
	8	保密资料

2.3 规则匹配融合机器学习

传统的基于规则匹配的分析技术从多个数据源收集日志，采用由安全专家预先创建的关联规则来实时执行，其能力局限于与系统或应用程序相关的网络信息的联系，如基于源 IP 和目的 IP 关系的分析。

随着内部威胁的增加，尤其是人的行为在动态变化时，由安全专家手动定义的规则不再具有适用性，使用传统的方法检测恶意用户行为变得非常困难。例如分析特定账户传输的数据量时，规则通常定义“阈值”大小以确定可疑活动，但在实际场景中阈值取决于不同的用户类型（某业务确需传输大量数据）、传输的时间和频率（单次大量数据传输或多次长周期少量数据传输），静态规则无法解决这种复杂情况。

基于自学习的关联分析被称为机器学习，通过学习用户和资产行为，从个例数据中进行抽象、发现个例背后的规律，对重大偏差产生告警，对规则进行修正，从而对安全事件的发现和预测起指导作用。机器学习包括以下几个方面的功能：

（1）形成统计模型：根据模型设定，统计每个指标的历史情况，根据时间维度、资产维度等生成统计模型；

（2）检测异常点：基于统计模型，在学习过程中实时检测数据和模型匹配情况，识别出异常数据；

（3）预测行为趋势：根据已有模型以及一定算法，预测未来一段时间内统计对象的发展趋势，以对未来的运营做出分析和提出指导意见。

表 3 基于规则匹配和机器学习的分析方法对比

分析方法	基于规则匹配	基于机器学习
示例	如果 20+次失败的登录尝试跟随 1 次成功登录，则告警； 如果工程师访问 HR 或财务文件共享，则告警	如果用户有异常的登录尝试失败，即尝试登录到以前从未登录过的系统，则告警； 如果任何部门的任何用户非正常访问文件共享，则告警
优势	1、安全运营人员确切知道何种行为能够触发告警，相应的也清楚如何处理告警； 2、可精确定位到异常行为的确凿证据	1、系统只被告知什么行为属于要学习，而无需穷举每一个好/坏组合； 2、可检测未知的行为； 3、自动调整模型，特别是当攻击类型或业务逻辑有变化的时候
劣势	1、必须知道每一个可能的攻击场景，并为之定义每一个可能的规则； 2、如果攻击模型变化，规则也必须随之更新	1、检测到的“异类”结果可能多种多样； 2、安全运营人员必须分析每种异常行为的根源，然后调整相应流程来处置告警

就现阶段技术趋势来看，基于机器学习的高级分析方法和基于规则匹配的传统分析技术正在融合，越来越多的基于大数据的安全厂商正在引入 UEBA 高级分析模块，而基于 UEBA 的厂商也正在丰富自己的大数据分析平台的建设能力。

2.4 多维度行为分析决策

长期以来，安全设备内置的威胁检测技术如数据防泄露（Data leakage prevention，DLP）、端点保护平台（Endpoint Protection Platform，EPP）、上网行为管理等多是以特征匹配为手段，即使后来出现的沙箱检测技术，也主要是依赖于专家经验提取已知病毒与攻击的行为特征进行分析，不能适应新类型的威胁或系统行为，对一些高级的未知威胁检测效果更是有限。例如 DLP 以关键字或模式匹配来识别敏感数据的流向、上网行为管理以是否访问招聘网站或者竞争对手网站来判断员工是否具有离职倾向，但其只关注数据内容、缺乏情景分析，由于观察维度单一导致误报太多，很难真正意义上作为安全分析的决策依据。

基于 UEBA 的网络安全态势感知则增加了对人员或实体多维度行为的关联分析，从而更准确地定位异常。以病毒检测场景为例，EPP 基于已知病毒文件的特征值匹配来查找病毒感染文件，但只要出

现任何形式的病毒变种，哪怕是同一个病毒家族的变种，静态的特征值匹配的技术会失效；而终端检测和响应技术（Endpoint Detection & Response，EDR）作为补充和升级，通过对终端上的文件执行和修改、注册表更改、网络连接、可执行程序的运行等行为的实时监控，查找异常或进一步的取证分析，即使遇到病毒变种的情况，因为其相似的行为，也能最终检测出变种，基于终端行为的威胁检测范围更大，覆盖效果更加明显。

3　基于 UEBA 的网络安全态势感知技术发展分析

回顾近年来网络安全态势感知的发展，无论是传统安全厂商还是新兴创业公司，先期的注意力主要是集中在对未知威胁的检测领域，借助相关产品和技术，用户获得了更低的 MTTI（平均检测时间），更快、更准确地检测出攻击和入侵，但这些产品和技术大都没有帮助用户降低 MTTR（平均响应时间）。

以笔者参与建设、运维的支撑平台为例，服务器、网络和安全等各类设备近 500 台（套），承载的应用系统 50 余个且类型多样（包括信息查询类的页面和接口、视频结构化、人像比对、数据抽取同步等）、部署架构不一（包括物理机、虚拟机、云平台、大数据平台等），受攻击面大、薄弱环节多。同时，参与项目建设、运维的外部人员（包括应用研发单位、系统集成单位、厂商等）较多，安全技术、意识不高，存在一定的失泄密风险。面对如此大规模的异构平台安全管理工作，检测出问题仅是第一步，对问题进行响应则更加重要，即考虑全网整体安全运维，需要将分散的检测能力与响应机制整合起来。

3.1 基于搜索的可视化溯源

网络安全态势可视化的目的是生成网络安全综合态势图，使网络安全态势感知系统的分析处理数据可视化、态势可视化。网络安全态势可视化是一个层层递进的过程，包括数据转化、图像映射、视图变换 3 个部分。数据转化是把分析处理后的数据映射为数据表，将数据的相关性以关系表的形式存储；图像映射是把数据表转换为对应图像的结构和图像属性；视图变换是通过坐标位置、缩放比例、图形着色等方面来创建视图，并可通过调控参数，完成对视图变换的控制[8]。目前，绝大多数安全厂商的相关产品界面已非常绚丽，可以将原本碎片化的威胁告警、异常行为告警、资产管理信息等数据结构化，形成 3D 图表、雷达图、拓扑图、热度图等多种样式。

但安全威胁特别是数据泄漏类安全事件的最终确认、全方位的风险评估以及溯源分析还是要透过对原始日志、事件的分析判定，因此对海量日志、事件的搜索能力以及将搜索的结果转化成图表/仪表盘的能力非常关键。

通过强大的图形分析、内置的基于时间轴的异常人员或实体的行为图谱、异常行为的可视化标示，对安全事件全过程还原，呈现出完整的攻击链条，覆盖攻击的源头、手段、目标、范围等相关信息。对安全运营人员来说，这将极大简化工作量，提高应对各类威胁的技术门槛，丰富有效面对新增威胁的技术手段。

3.2 基于 SOAR 的联动处置

2017 年，Gartner 提出了安全编排自动化响应（Security Orchestration Automation and Response，SOAR）概念，其定义为“帮助企业和组织收集安全运维团队监控到的各种信息（包括各种安全系统产生的告警），并对这些信息进行事件分析和告警分诊。然后，在标准工作流程的指引下，利用人机结合的方式帮助安全运维人员定义、排序和驱动标准化的事件响应活动”。

为了提高平均响应时间，基于 UEBA 的网络安全态势感知还需要利用 SOAR 思想进行联动安全防护。发现疑似安全事件时，实现强制切断连接、病毒消杀、安装漏洞补丁等处置措施，其技术难点在于对不同厂商安全防护设备的兼容。以最有效、最常见安全防护设备防火墙为例，主流厂商包括华为、新华三、深信服、网御星云、Cisco、Juniper 等，远程管理接口类型不同（Telnet、SSH、SNMP、HTTP/HTTPS 等），ACL（访问控制列表）的命令集也都不一样，需要定制开发才能下发策略。

因此，基于 SOAR 的联动处置应包括以下几个步骤：

（1）编排策略的预设条件：针对不同资产、事件级别、事件类型来选择联动范围；

（2）设置编排策略的响应手段：针对不同场景、事件级别的安全事件，选择不同的响应手段，一旦事件被触发，则自动执行相应的编排策略；

（3）设置编排策略的执行对象：针对不同响应手段，选择不同的联动设备，同时还可以选择策略生效时间段。

4　结束语

时至今日，通过不断夯实网络安全防护堡垒，加强业务系统健壮性，力求抵御黑客一波又一波的攻击，基于 UEBA 的网络安全态势感知因其具备多种关键技术能力成为了高效的主动防御手段，实现了对网络安全事件的事后、事中、事前管控。从实际出发，技术最终是被人使用，因此还需要通过加强安全意识培训、组建安全运营团队、完善安全管理制度、构建安全闭环流程等方式方法，才能有效降低网络安全风险。

参考文献：

[1]韩伟红，隋品波，贾焰.大规模网络安全态势分析与预测系统 YHSAS[J]. 信息网络安全，2012（8）：11-14.

[2]管磊，胡光俊，王专.基于大数据的网络安全态势感知技术研究 [J]. 信息网络安全，2016（9）：46-50.

[3]杜嘉薇，周颖，郭荣华，索国伟.网络安全态势感知：提取、理解和预测 [M].北京：机械工业出版社，2018.

[4]Alexander Kott，等.网络空间安全防御与态势感知 [M].黄晟等译.北京：机械工业出版社，2018.

[5]苏小玉，徐奎奎.网络安全态势感知中数据融合算法应用描述[J]. 河北省科学院学报，2020（6）：37-44.

[6]张乐媛.基于上下文感知的网络用户行为分析[D].[硕士学位论文].北京：北京邮电大学，2010.

[7]赵刚，姚兴仁.基于用户画像的异常行为检测模型[J].信息网络安全，2017（7）：18-24.

[8]陶源，黄涛，张墨涵，等.网络安全态势感知关键技术研究及发展趋势分析[J].信息网络安全，2018（8）：79-85.

SDN/NFV 技术对电信网络架构意义及有关技术探讨

◆房栋斅　吕辉

（中国移动通信集团设计院有限公司北京分公司　北京　100089）

摘要：随着电信网络虚拟化建设愈发深入，电信运营者迎来良好的发展机遇，同时也面临一系列挑战难题，怎样推动 SDN/NFV 新型网络快速转型，成为电信运营者首要思考的课题之一。为了促进网络运维水平的提升，控制网络运维的经济成本，增强电气运营者的