可信网络白皮书

中国联合网络通信集团有限公司、中讯邮电咨询设计院有限公司、
中国信息通信研究院和华为技术有限公司联合发布

(2023)

中国联通 China unicom | 中讯设计 | CAICT 中国信通院 | HUAWEI

CONTENTS
目　录

CONTENTS
目　录

1 前 言

新兴科技的迅猛发展不仅造就了蓬勃发展的数字产业，也推动了各行各业的数字化转型浪潮。以云计算、5G 为代表的新型基础设施成为“数字新基建”的重要组成部分，大数据、智能技术加速实现数据驱动的业务转型，机器学习、物联网正在改变企业传统的生产运作方式，数字化技术已经成为企业的核心竞争要素。

随着企业数字化转型的发展，业务加速上云，安全边界的暴露面不断扩大，极大增加了安全防护的复杂度。企业应用的数字化改造，在提升用户体验并带来便利的同时，也面临着移动端数据泄露、账号密码泄露、特权账号共享、员工违规操作等众多内部引发的安全风险。令人防不胜防的外部攻击，日益加剧的内部威胁，不断加大的监管力度，使得传统的基于边界防御的安全架构不堪重负，迫切需要新一代的网络安全理念和架构来应对数字时代的多元复杂挑战。

运营商网络作为国家数字基础设施的“大动脉”，是支撑“数字中国”战略的关键，如何保障运营商网络安全可信和稳定可靠，是运营商的核心职责所在。中国联合网络通信集团有限公司、中讯邮电咨询设计院有限公司、中国信息通信研究院、华为技术有限公司联合发布“可信网络”白皮书，为运营商网络的安全建设提供指导和参考，最终达到为业务提供可预期的质量保障的目标。

本白皮书主要聚焦运营商 IP 网络的最新趋势、网络安全挑战，提出业界领先的网络安全新理念、新架构、关键能力以及行业实践，展现运营商网络基础设施领域部署可信网络架构的战略思考。

2 网络发展趋势与挑战

数字化转型加速网络基础设施的高速发展，业务上云改变了网络的流量模型，物理网络边界正在加速消失，引入新的网络安全问题，传统基于边界防护的安全体系逐步失效，需要新的网络安全防护思路和理念。与此同时，不断进化的外部攻击、令人眼花缭乱的欺诈手段、触目惊心的内部信息泄露，以及网络攻击引起的基础设施瘫痪，使得各单位安全风险不断扩大，造成的损失逐年剧增。因此，面对新形势下网络安全挑战，各国都将加强网络防护上升到国家战略。

2.1 网络发展对安全建设提出新的要求

随着企业数字化转型的发展，业务向云化、物联化、无线化的方向发展，业务边界、业务接入类型、接入终端类型、数据的流转等都发生了变化。网络也从以 IPv4 为基础的消费互联网向以 IPv6/IPv6+ 为基础的生产互联网升级，以满足多元化应用承载需求，释放产业新效能。网络的演进，也带来网络边界和连接模型的变化，这些变化主要体现在：

- **网络边界延伸：**基于云、网、边、端的新 IT 基础设施，重新定义了网络的边界。
- **接入多样化：**手机用户、PC 用户、企业用户多样化接入，物联终端、PC 终端、移动终端等设备多样化接入，无线、企业、互联网等业务多样化接入，有线、无线连接多样化。
- **数据无边界:** 数据在用户、设备、业务、平台之间持续流动，跨域企业园区、承载网、数据中心。
- **网络的开放性：**IPv6 协议本身具备开放性，通过可编程定义网络路径，使网络具备了一定的开放性能力。

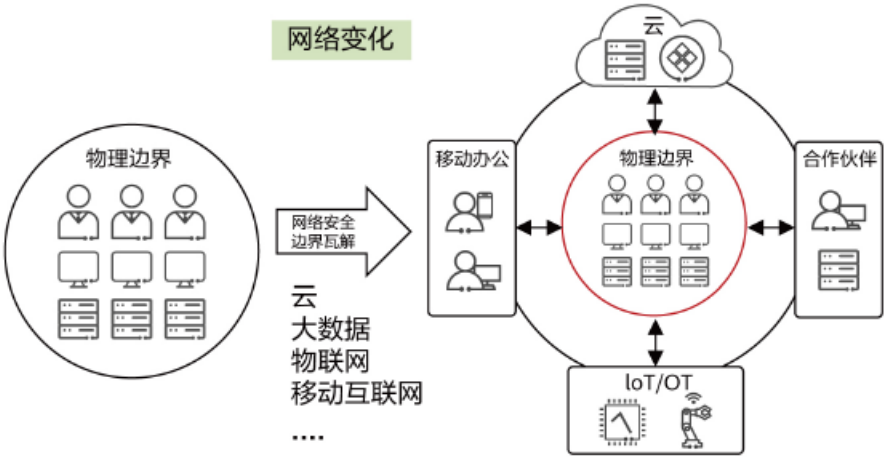

图1 网络安全边界发生变化

如图 1 所示，网络风险边界的扩大，增加了安全防护的复杂度，传统的安全防护思路已经不能满足业务及网络演进的诉求，已影响行业稳定生产。

- **传统网络防护思路**

  ✔ **设备是被信任的：**设备物理部署在运营商机房，集中管理，环境可控，嵌入式攻击难度大。

  ✔ **网络边界集中清晰：**网络有清晰的信任边界，内部网封闭专属可信，外网边界集中化安全管理。

  ✔ **防护策略易管理：**业务流量路径简单、变化小，策略易管理。

- **IP 网络安全新痛点**

  ✔ **设备不再 100% 可信:** 设备入驻企业、部署在云端，暴露面增加，网元易被近端攻击控制。

  ✔ **接入网不再是内部信任域：**toB 业务多样，网络边界分散到企业接入，原有的网络信任边界被打破。

  ✔ **人工运维攻击面大：**业务复杂、动态运维，原有的运维安全策略粒度粗，受攻击面大，并且缺乏设备安全态势可视能力。

  ✔ **协议风险逐步暴露：**随着网络规模变大，暴露面的增加，原有 IP 协议的路由安全问题更加凸显。

2.2 网络威胁事件频发危害网络基础设施

网络风险无处不在，近期网络安全事故频发，影响上千万用户的生活工作，造成严重的国际影响，已成为事关国家安全的重大战略问题。

- 2021年5月，美国最大成品油管道运营商Colonial Pipeline网络设备遭攻击，45%管道停运，政府宣布进入紧急状态。
- 2021 年 8 月，微软披露其网络遭遇一场 2.4Tbps DDoS 大流量瞬时攻击，造成欧洲某客户业务受损数十分钟。
- 2022 年 2 月 14 日乌克兰 70+ 银行、政府、军网遭 DDoS 攻击；2022 年 2 月 24-25 日，俄设备遭 DDoS 攻击，300 多个俄政府、媒体和银行网站瘫痪。
- 2022 年 3 月，乌克兰运营商 Triolan 表示，网络的关键节点被黑客入侵，关键网络设备恢复为出厂设置，路由器无法恢复，导致乌克兰用户互联网中断 12 小时。
- 2022 年 3 月，美国卫星通信提供商 Viasat 遭受恶意擦除软件攻击引发中欧和东欧的卫星服务中断，影响了位于乌克兰的数千名客户和欧洲各地的数万名客户。
- 2022 年 9 月，西北工业大学遭到境外非法入侵攻击，渗透控制网络服务器及关键网络设备，窃据核心技术数据，造成严重信息泄密。
- MANRS（Mutually Agreed Norms for Routing Security）路由安全报告，发生一起以上路由安全事故的网络数量达到 1236 个。包括：2022 年 7 月，俄罗斯 Rostelecom 劫持苹果服务流量达 12 小时，2022 年 8 月，黑客利用 BGP 劫持亚马逊窃取约 23 万美元加密货币。

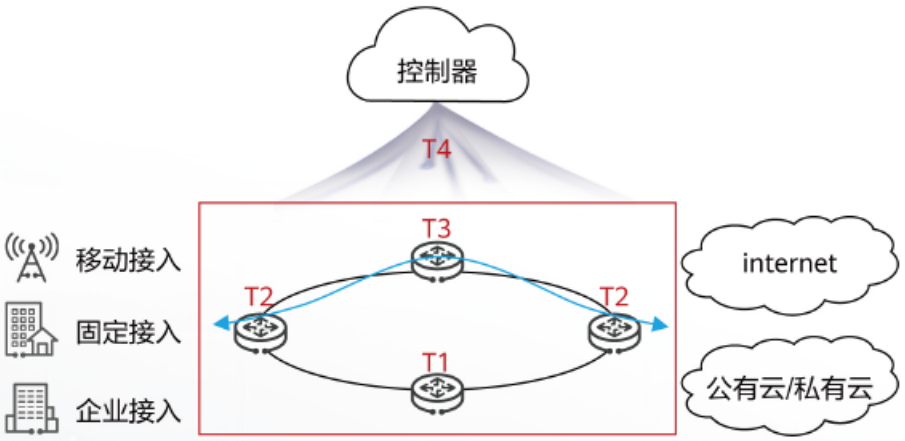

图2 网络潜在的攻击面

当前产业界以及学术界已经开始认识到基础设施网络安全的重要性和价值，并开展了积极有益的探索，但是目前关于基础设施网络安全的探索缺乏系统性的研究。

本白皮书就网络潜在的攻击面进行分析，包括基础设施设备、网络边界、网络通信、网络运维层面的攻击，如下表所示，汇总了基础设施网络面临的最重要的安全挑战。

攻击面	挑　战
基础设施设备	通过供应链或站点物理接触，更换设备或者单板进行仿冒 / 存储介质移除 / 篡改软件；或通过设备的安全漏洞突破到设备内部，做提权、横向移动攻击；设备的误配置和恶意配置导致网络存在安全薄弱点，容易被外部渗透或攻击。
网络边界	仿冒合法网络节点接入到运营商网络；通过网络边界发起 DDoS 的攻击，占用设备或网络带宽资源。
网络通讯	攻击者基于路由协议攻击、SRv6 的源路由攻击等；链路故障后路由协议收敛慢导致网络问题扩散；攻击者对网络中传输的业务数据进行窃取、仿冒、篡改。
网络运维管理	运维违规操作，无意或有意的隐藏恶意操作或下发高危命令等；利用管理用户弱口令、开放 3rd 对接接口等脆弱性，突破系统、获取权限，实现对网络的攻击；攻击的感知能力差，攻击溯源难。

路由、流量、设备漏洞、人工运维攻击是基础设施网络面临的主要安全威胁，造成的后果包括：网络不可用、信息窃取，给企业和社会带来经济及声誉损失。

2.3 安全可信已经上升为国家战略

面对新形势下网络安全风险，各国都在通过立法、安全认证，及新的技术重新构建网络防御体系，将加强自身网络的安全能力上升到国家战略

- **欧盟：致力打造一个可信的和网络安全的欧洲**

✔ 2019 年 6 月 27 日，《关于欧洲网络与信息安全局信息和通信技术的网络安全》正式施行。指定欧盟网络和信息安全署（ENISA）为永久性的欧盟网络安全职能机构。为其确定了目标，即构

建一套欧洲网络安全认证系统，包括通用的网络安全认证框架、多种形式组合的认证方法、评定机构的资格认可标准等。

✔ 2020 年 7 月 17 日，ENISA《可信且网络安全的欧洲（A Trusted and Cyber Secure Europe）》战略文件发布，在整个欧盟的网络安全数字环境中，通过关键技术领域的可信认证计划，欧盟公民可以更加信任 ICT 产品、服务和流程的安全性，打造一个可信的和网络安全的欧洲。

✔ 通用标准互认协议（CCRA）是多个国家共同推进的安全评估 CC 体系，CC 作为网络设备认证的通用标准已经遍布全球，德国、法国、意大利等还在 CC 基础上针对本国进行了标准定制和扩展，对网络关键设备进行准入控制

- **美国：加强技术应用引导和统一部署，提高联邦网络安全整体能力**

✔ 2021 年 5 月 12 日，美国发布《改善国家网络安全行政令》。强化公私合作，加强威胁信息共享和健全网络安全审查机制。锚定关键软件，强化软件供应链安全管理，加强技术应用引导和统一部署，云计算、零信任架构、EDR、多因子加密认证等技术和应用均被纳入美国网安政策视野，以提高联邦网络安全整体能力。

✔ 2021 年 11 月 4 日，美国国防部发布“网络安全成熟度模型认证”（CMMC2.0），邀请第三方评估机构对承包商是否满足所要求的标准进行审计，只有符合要求后才能获得国防部的合同。

✔ 2022 年 1 月 26 日，美国联邦政府管理和预算办公室（OMB）正式发布《零信任战略》，要求在 2024 年财年前“实现具体的零信任安全目标”，这是业内首个国家级零信任架构。

- **我国：网络安全法律法规政策保障体系逐步健全和完善**

✔ 2016 年 11 月 7 日，《中华人民共和国网络安全法》经第十二届全国人民代表大会常务委员会第二十四次会议表决通过，自 2017 年 6 月 1 日起施行。网络安全法是我国第一部全面规范网络空间安全管理的基础性法律，是各种法规、标准的根本依据。

✔ 2021 年 4 月 27 日，《关键信息基础设施安全保护条例》经国务院第 133 次常务会议通过，自 2021 年 9 月 1 日起施行。关基保护条例是加强网络安全领域立法、完善网络安全保护法律法规体系的重要举措，是依法治理关键信息基础设施的纲领性文件之一，是化解关键信息基础设施安全风险的法律法规重器和重要里程碑。

✔ 2021 年 6 月 10 日，《中华人民共和国数据安全法》经十三届全国人大常委会第二十九次

会议表决通过，这是我国第一部有关数据安全的专门法律。

- 2021 年 8 月 20 日，《中华人民共和国个人信息保护法》经第十三届全国人民代表大会常务委员会第三十次会议表决通过，这是中国首部针对个人信息保护的专门性立法。

3 可信网络安全理念

3.1 信任边界延伸到网络基础设施内部

传统的网络安全防护思路是在网络边界构建防御体系，假设威胁持续存在，以“反向查”的思路，查漏洞、查病毒、查缺陷，试图通过安全测试、攻防演练等手段和方法发现所有漏洞。“反向查”的本质就是“黑名单”的思路，安全防护始终处于被动应对状态，不停的在网络的信任边界“打补丁”，这种防护思路不仅解决不了根本问题，还会把安全做得无比复杂，导致安全投资和建设就像“无底洞”，已经无法满足运营商网络对安全可信的新诉求。因此，需要引入新的网络信任理念和架构，重新定义网络的信任边界，将信任边界延伸到网络和设备内部，安全基因融入网络基础设施，构建纵深防御体系能力，从安全内生的视角解决安全问题，确保所有的设备、连接、流量都符合预期。

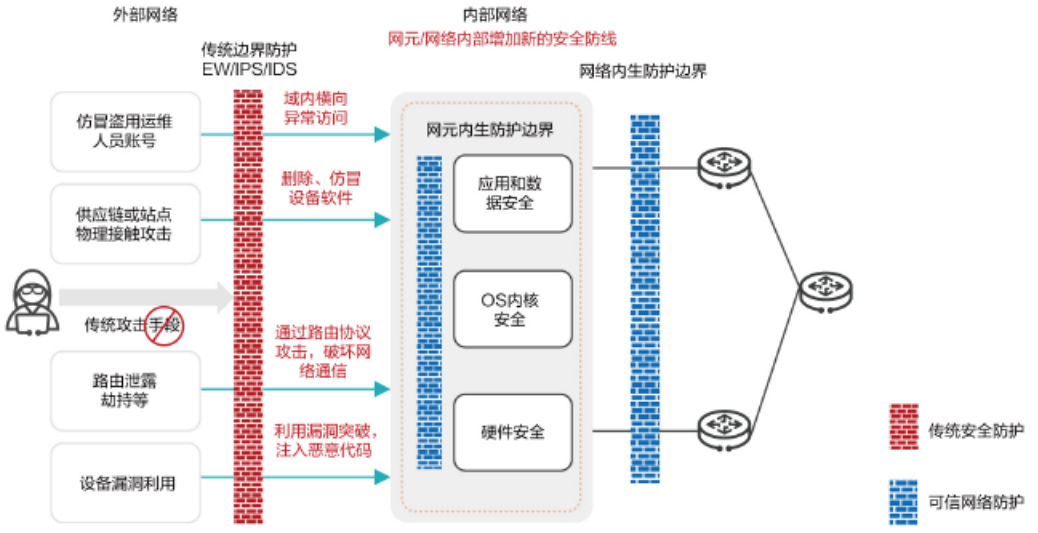

图3 可信网络防护

3.2 构建“正向建 + 反向查”的内生防御可信理念

为了有效应对国际国内复杂多变的网络安全形势，积极开展重大专项关键技术攻关，实现极限条件下基础电信网络可管可控提供支撑保障，我们在业界率先提出“可信网络”的概念。可信网络是指将安全可信技术融入到网络基础设施解决方案中，构筑网络的内生安全能力，实现数字实体信任关系的传递和验证，网络流量行为的持续监测和管控，业务访问异常的溯源和处置，从而实现结果可预期的网络。

为了实现以上可信网络目标，我们需要建立一个系统化的网络可信体系，其中可信的关键属性包括：1）安全性（Security）。网络具有良好的抗攻击能力，保护业务和数据的机密性、完整性、可用性；2）韧性（Resilience）。网络受攻击时保持原有定义的运行状态，以及遭遇攻击时快速恢复的能力。3）可靠性（Reliability）。网络能在生命周期内长期保障业务无故障运行，具备快速恢复和自我管理的能力，提供可预期的、一致的服务。

可信网络是在原有的传统安全防御体系基础上，延伸了信任边界，扩展了防御对象，形成良好的增强和互补。具体体现在：

- 信任边界从外部网络延伸到网络内部的链路、拓扑、路由、流量等和设备内部的硬件、操作系统、APP 应用等。
- 防御的攻击从原来的针对业务的病毒攻击、终端攻击、内容攻击等延伸到针对基础设施连接的路由攻击、流量攻击及设备攻击等。
- 安全管理能力从原来的全域安全管理延伸到设备和网络内部的安全管理，实现设备和网络内部的安全状态可视、可管，并做到全网统一协同防御。

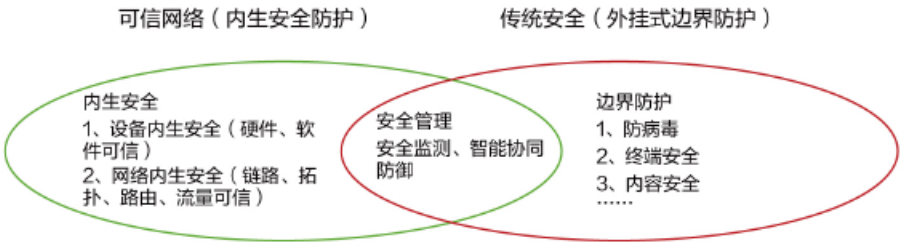

图4 可信网络范围与传统安全范围

可信网络通过**“正向建”与“反向查”相结合的安全理念**，持续消除网络不确定性，**构建信任可传递，行为可预期、结果可验证的网络基础设施，达到为业务提供可预期的质量保障的目标**。

- **正向建：**通过在规划、设计、开发、部署阶段构建设备和网络的内生安全能力，做到“设备出

生就是安全可信的”，确保“业务上线就具备网络韧性”，主动防御，消减风险点，建设确定性的信任链传递机制。如下图：

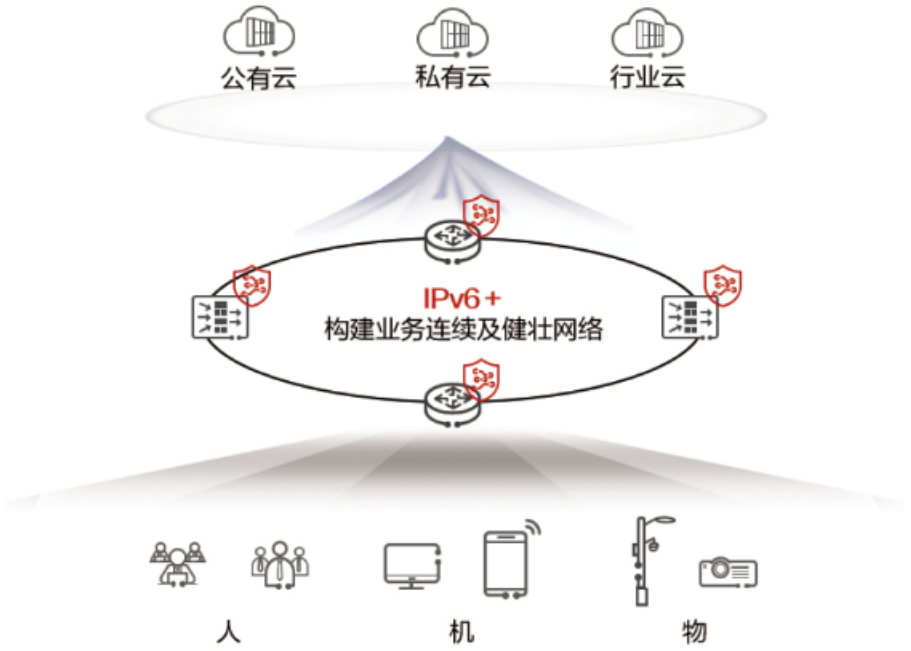

图5 正向建示意图

- **反向查：**在网络运行阶段，通过网络流量和日志监测技术，持续监控业务变化 / 行为异常，对网络的安全状态实时监控，及时遏制风险损失。在网络中分层部署安全大脑，负责全域安全监测，实现安全态势可视化，并且基于安全大脑进行威胁关联、网安协同智能协同防御。如下图：

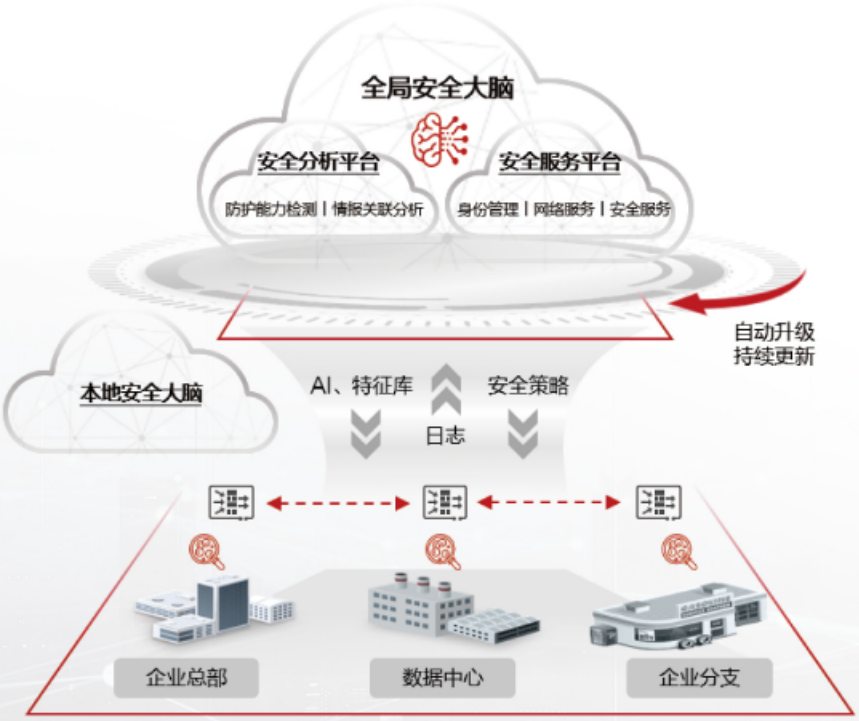

图6 反向查示意图

在网络的三大要素“实体”、“连接”、“业务与数据”中，“实体”具体化为 IP 网络中对应 OSI 相应层级的各种设备，“业务与数据”具体化为 IP 网络中对应 OSI 相应层级的业务应用和数据，“连接”负责将业务数据在各网络实体中传输。因此，可信网络也是围绕着这三个元素进行安全防护。

基于“正向建、反向查”的可信理念与网络防护三元素的相结合，提出设备可信、网络可信、管控可信的三级可信网络模型。围绕三级可信网络模型，构建网络内生安全架构，确保关键部件、基础协议、网络流量、系统架构安全可信，并满足网络端到端的安全需求。

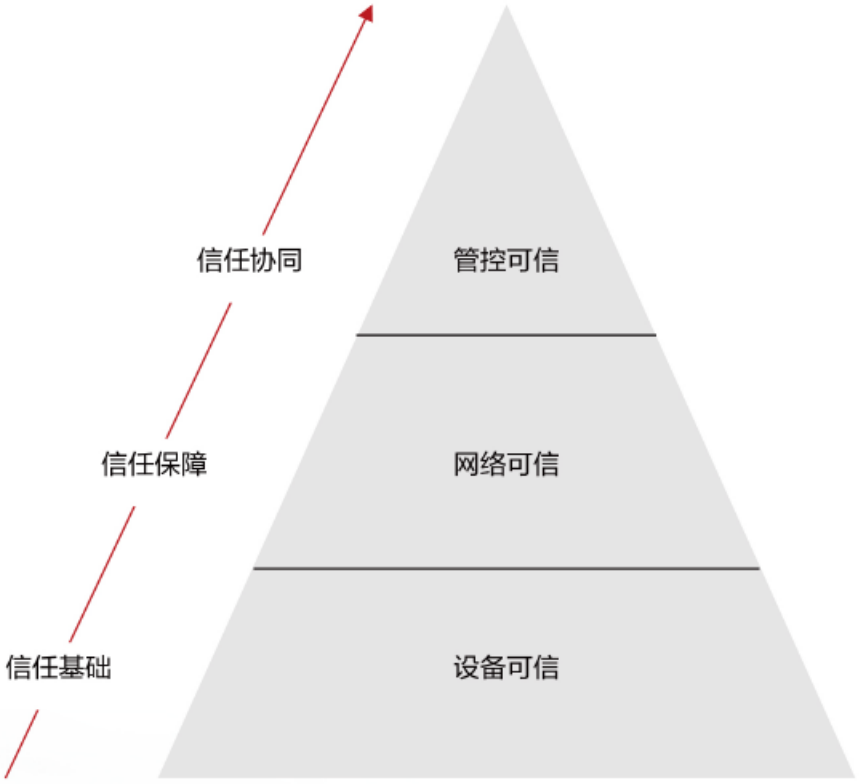

图7 可信网络模型

- **设备可信：**保护硬件安全、操作系统安全、中间件与应用的安全与韧性，防止设备被非法入侵，构建网络“可信基座”。设备可信是信任基础。
- **网络可信：**以设备可信为基础，保护协议控制安全、流量安全及接入访问控制的安全，保证业务流量转发路径的安全可信。网络可信是信任保障。
- **管控可信：**网络安全大脑，持续监测全域及设备的安全态势，一体化的安全防御，实现业务风险的实时感知，业务安全策略的自动化编排，提升安全防护有效性和安全运维效率。管控可信保证信任协同。

4 可信网络解决方案

4.1 可信网络设计目标和架构

传统网络存在诸多挑战，网络规模越来越大，网络配置越来越复杂，安全风险越来越不可控。并且，传统的安全产品与技术会产生大量不准确或者误报的告警，导致安全防护效果不佳，防护效率低下等问题。为了有效应对网络所面临的安全风险，我们认为，新型的安全保障体系应该是基于“正向建 + 反向查”的一体化安全体系，该体系具备以下特征：

- **内建而非外挂：**所有安全能力以内建的方式为产品和解决方案提供各种安全机制，并且从内向外构建立体化的防御体系，不是外挂“打补丁”式的。
- **主动而非被动：**安全体系中通过动态持续检测各种入侵行为和安全风险，主动阻断外部攻击，将攻击阻断在系统之外，而非被动的事后处置。
- **融合而非孤立：**安全体系中各模块就像人体的免疫系统一样，各司其职又协同免疫，缺一不可。当攻击或不符合预期的异常发生时，整体系统各部件统一协同，并通过相应的手段进行阻断，彻底消除威胁。

基于上述可信网络体系的特征，可信网络解决方案应有如下设计目标。

- **内生安全：**安全能力以内建的方式构建在路由器、交换机等网络基础设施上，为产品和网络提供各种安全机制，并提供主动防御手段。
- **纵深防御：**在外部威胁和内部关键资产之间，构建多层次的安全措施，不同的层次采用不同的安全技术，避免出现突破一点即突破全局。

- **安全可视化：**安全风险可视，安全态势及时感知，实时查看基础设施网络的安全状态，只有可视才能可管。
- **安全协同：**基于云网安联动的安全策略，结合 AI 的威胁关联检测，提升威胁的检测、处置效率，并适应不断变化的安全威胁，实现安全损失最小化，提升安全防护效果，保障业务可信。
- **安全自适应：**基于 IPDRR(识别、保护、检测、响应、恢复) 原则，对于安全措施动态、持续优化，自动闭环，构建网络的韧性恢复能力。
- **可靠性：**在网络故障场景下，网络具备自愈能力，能及时恢复业务连接，提升网络的抗毁性和业务的生存性。
- **分级演进：**可信网络分级演进，定义等级能力要求，能力等级可评估、可测量，识别差距，为网络安全等级演进提供技术路线。

基于上述设计目标，结合前述章节关于威胁和挑战的分析，我们定义了可信网络解决方案架构，如图所示：

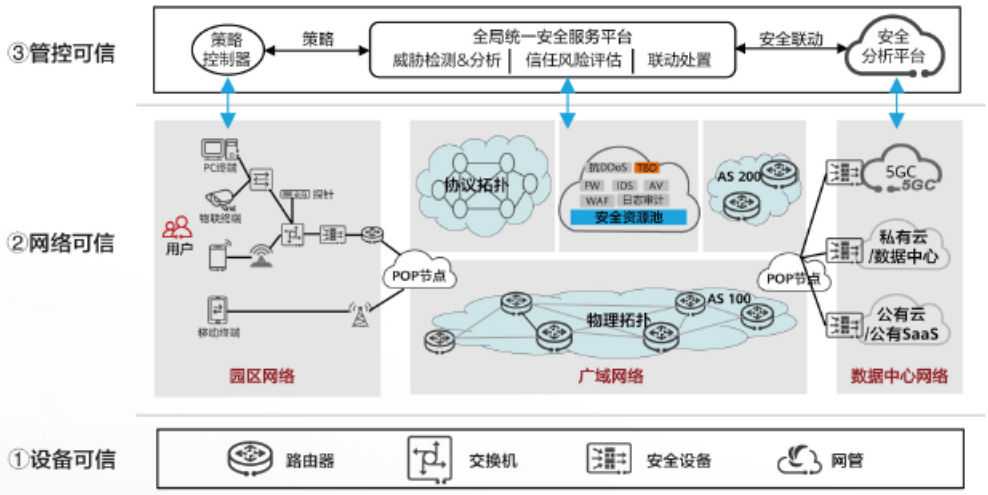

图8 可信网络解决方案架构

可信网络解决方案总体架构主要由三大部分组成：

- **设备可信：**可信网络基础设施，组成网络的关键设备（路由器、交换机、防火墙等）和网管系统应满足安全可信的要求，并基于安全启动、数据机密性、韧性恢复、单域安全等技术手段，实现设备防篡改和入侵防御等安全能力。

- **网络可信：** 可预期网络，网络里的所有流量路径和行为都具有可预期性，避免不符合预期的流量，确保“网络可信”。采用路由安全、流量加密、网络保护、恢复等技术，确保流量路径可预期，行为可溯源，避免发生不符合预期的横向扩散和违规访问行为。
- **管控可信：**云网安一体管控，通过采集全网的流量、安全日志、告警、文件、资产等安全数据，并对这些数据进行全域安全分析，及时发现异常或违规行为，快速处置和闭环威胁事件，避免风险扩散。基于自动化的安全策略处置，可以将威胁闭环的时间从 24 小时降低到分钟级，实现安全损失最小化，实现网安一体化的智能安全防御。

4.2 设备可信

4.2.1 设计目标

网络设备是网络的基础单元，承载网络的基本业务能力，当其受到攻击后会导致：

- 网络不可用，失去提供业务承载的基本能力。
- 攻击者获得设备控制权，并将其作为网络攻击的跳板。
- 攻击者获得设备的关键数据信息，信息泄露。

因此，设备可信是保证网络基础设施安全可信的基础。通过构建设备内生安全能力，在保证业务功能的同时，防止设备被非法入侵，针对异常行为及时进行检测和响应。设备可信主要目标如下：

- **纵深防御：**基于硬件可信根构建信任可传递的纵深防御内生安全能力，保证设备的机密性、完整性和可用性。
- **漏洞难利用：**防止恶意人员暴力破解、数据窃取、控制设备等攻击行为，提升攻击难度。
- **攻击发现快：**通过及时检测发现入侵者对系统的探测、入侵、窃取、篡改等攻击行为，提供证据留存、追踪溯源能力。
- **响应恢复快：**在遭受攻击后设备可以快速响应自愈，保证业务功能持续安全、可用。
- **高可靠可用：**实现芯片 / 单板 / 硬件系统 / 软件 4 级高可靠性保证，达到设备整体 5 个 9 的可用性目标。

4.2.2 能力要求

为实现设备可信目标，必须围绕设备在全生命周期内形成纵深防御内生安全能力，构建软件完整性保护、敏感数据机密性、认证与鉴权机制、攻击检测及韧性恢复等安全能力。

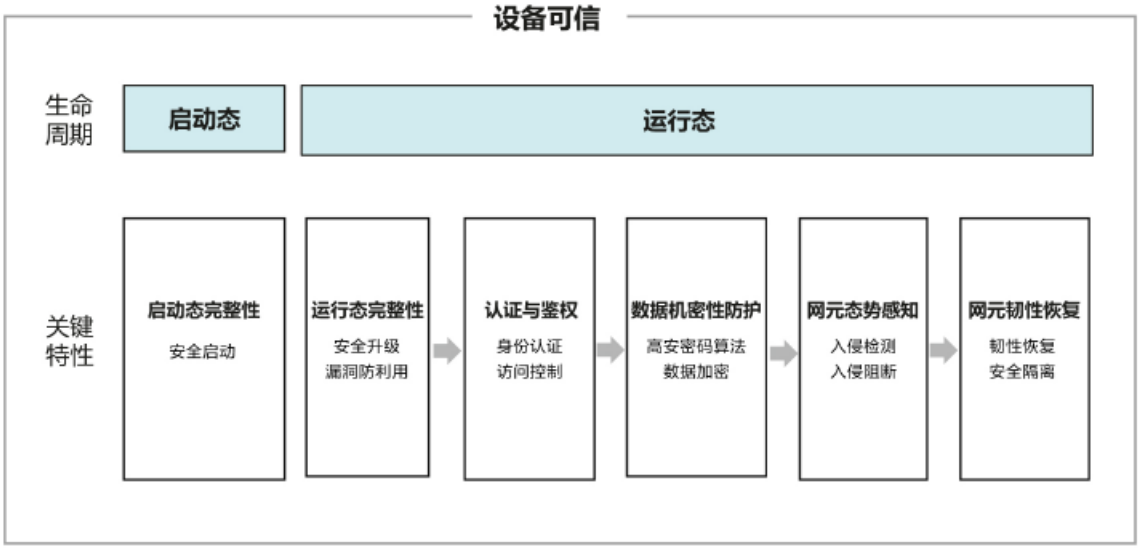

图9 设备可信架构

- **软件完整性保护：**软件完整性是启动安全和运行安全的重要保障，是提升产品和服务安全性的基础。构建从硬件到软件基于信任链的全生命周期软件完整性保护，能有效防止软件发布、启动、运行和升级阶段被篡改。关键安全能力包含软件签名、安全启动、操作系统漏洞防利用，安全升级等。
- **认证与鉴权：**对接入系统的主体身份进行验证、授权，防止非法接入。关键安全能力包含身份账号管理、访问控制、权限最小化、默认安全、口令安全等。
- **数据机密性保护：**对关键数据（如认证凭据 / 证书 / 日志 / 配置等）进行安全保护，防止数据被篡改和窃取。关键安全能力包含安全密码算法应用、认证凭据保护、安全日志保护、传输数据保护等。
- **网元级动态感知：**

网络设备面临着各种全天候的攻击。需要具备实时高效的检测和闭环响应能力。传统安全分析检测技术比较单一，人工处理为主，效率低下。

网元级安全态势感知旨在对网元进行定期的“体检”，针对面向设备的攻击行为进行快速的入侵检测，并与管控面合作，实现威胁关联、分析，自动防护、快速处置，达到“分钟级”的快速感知和闭环响应。降低运营商客户的安全运维技术门槛和人员成本，提高效率。主要的能力包括安全审计、入侵检测、安全处置等。

- **韧性恢复能力：**

系统韧性指系统受攻击时承受并保持在有定义的运行状态（包括降级）、恢复并适应攻击以保障业务目标的达成能力。

韧性的系统在不利的条件下具备隔离、承受、恢复的能力。

✔ **隔离：** 网络设备要能在系统受到持续的攻击时，支持多层次的系统隔离，防止单点攻击、全局突破。

✔ **承受：** 系统在被恶意入侵后还具备完成关键业务功能的基本能力，同时在一定程度上为系统的恢复和适应争取了缓冲的时间。协议要具备在过载时能继续提供业务的能力。

✔ **恢复：** 通过在系统受到攻击后导致任务和业务功能受损时，具备韧性能力，确保在攻击后重新恢复系统正常运行，持续提供核心业务的能力。具体关键能力包括关键业务协议所在进程可以自动重启恢复业务，提供最小业务系统。

- **高可靠性：** 可信网络要求设备的可靠性要能达到 5 个 9，设备要能从芯片、单板、硬件系统、软件不同维度具备相关的高可靠性能力，主要包括冗余设计、故障检测、恢复、隔离等可靠性措施。设备具备按需扩容、多代兼容的能力。

4.3 网络可信

4.3.1 设计目标

网络可信是信任保障，以设备可信为基础，构建多层连接可信，屏蔽异常访问，保护协议安全、路由安全、接入访问控制安全及网络流量安全，构筑业务安全的可信保障。网络可信针对协议、路由、流量、接入控制、业务保障五方面进行分析，构建网络层安全能力。实现网络自身连通安全和传输信息的安全，确保设备间网络通讯的机密性、完整性、可用性。

- **协议安全目标：** 协议邻居可信，防止邻居仿冒，防止协议畸形报文攻击和协议报文泛洪攻击，保证网络可用性；保证隧道安全性，防止拓扑信息泄露、仿冒接入及隧道篡改。
- **路由安全目标：** 基于路由合法性验证，实现 BGP 路由防劫持、防泄露。
- **接入控制安全目标：** 实现终端可信接入及用户可信接入。
- **流量安全目标：** 防止流量被窃取、被篡改；实现 DDoS 快速防御能力；实现流量按需动态引入安全防护资源；实现异常及恶意流量安全威胁快速溯源、精准阻断。
- **业务差异化体验保障：** 网络具备确保不同服务等级业务的差异化体验保障能力，能够满足不同用户对网络的 SLA 诉求。
- **可靠性目标：** 协议、隧道具备快速收敛能力，能够确保故障后业务快速恢复；协议具备过载抗攻击能力。

4.3.2 能力要求

网络作为数据传输的管道，存在设备物理接口、通信协议报文接口等暴露面，种类比较多样，个体数量也比较多。如果网络配置不当，或者某一保护环节缺失，攻击者通过相关暴露面，对网络发起攻击，就可能产生仿冒接入网络、窃取通信数据、破坏网络管道等威胁。为了抵御这些攻击，必须根据网络层次结构的特点，以设备可信为基础，保护协议控制安全、路由安全、流量安全及接入访问控制的安全，永久保证业务转发路径安全可信。按照网络自下而上，分别对链路连接、拓扑连接、隧道连接、路由连接、准入连接、网络流量及业务保障等网络各层次进行安全加固，形成立体防护的网络防护能力，构筑完整可信网络体系。

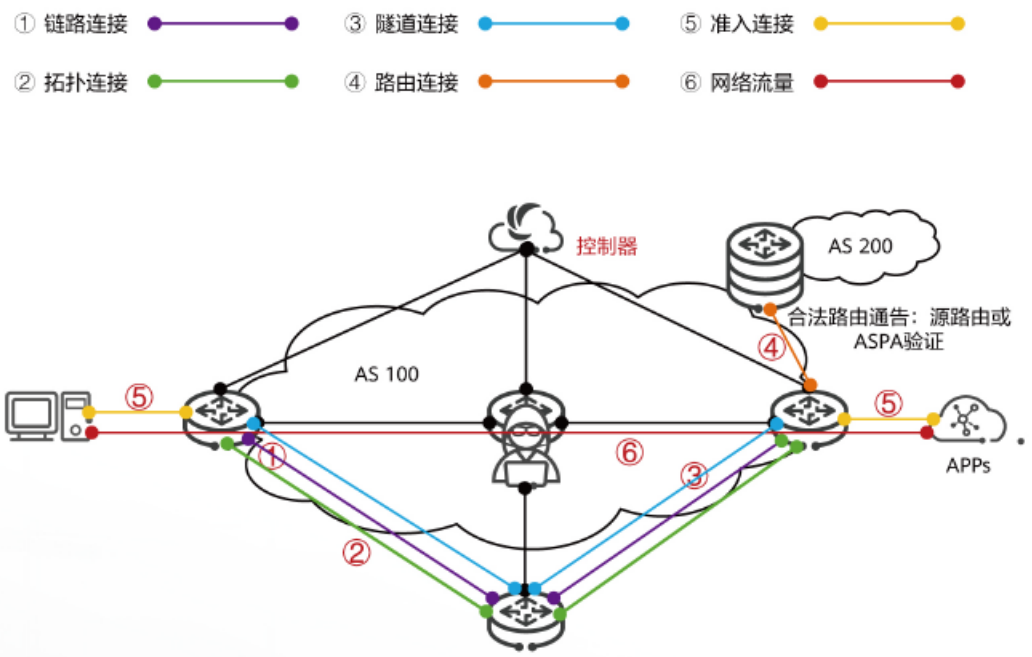

图10 网络可信架构

- **链路连接可信**

链路连接应以设备自身可信为基础，链路的连接需要具备确保所承载业务质量的能力，能够按照业务所需的质量要求提供服务。链路连接可信主要关键能力是，为设备签发身份证书，在设备接入网络或建立通信关系时，网络需要验证接入网元身份合法性，确保网络设备接入可信；业务发放时，需要把接口的 CRC、FEC 误码率等能够真实反映链路质量的因素作为约束条件，并在业务运行时能够实时感知链路质量。

- **拓扑连接可信**

基于可信的物理连接，构筑网络拓扑，保证网络连接可信。网络拓扑是网络可通信的基础，路由协议对网络中节点、链路进行计算，形成网络拓扑。攻击者对路由协议的攻击，可能导致业务访问失败或用户数据丢失等后果。

因此，网络拓扑对保护业务至关重要，需要对路由协议、网络拓扑连接进行防仿冒、防篡改等保护，保证网络拓扑是安全可信的。同时，确保故障后业务快速恢复、过载时具备优雅降级能力。拓扑连接可信关键能力包括：对 BGP/ISIS/OSPF/MPLS LDP 等协议对等体进行认证，防止非法邻居仿冒；通过对畸形的协议报文进行识别和丢弃，对泛洪的协议报文进行限速，防止报文攻击导致的系统过载或异常。

- **隧道连接可信**

在使用 MPLS/SRv6 等业务隧道进行端到端数据传输时，需要确保隧道是安全可信的，按照客户预期部署，防范恶意仿冒接入、信息泄露及隧道篡改等攻击行为，保护业务转发数据和管理数据。隧道连接可信能力包括：对 SRv6 配置安全域隔离功能，通过边界过滤实现防仿冒，使用内部信息隐藏实现网络信息防泄露，通过建立安全隧道保证数据防窃取、防篡改。

- **路由连接可信**

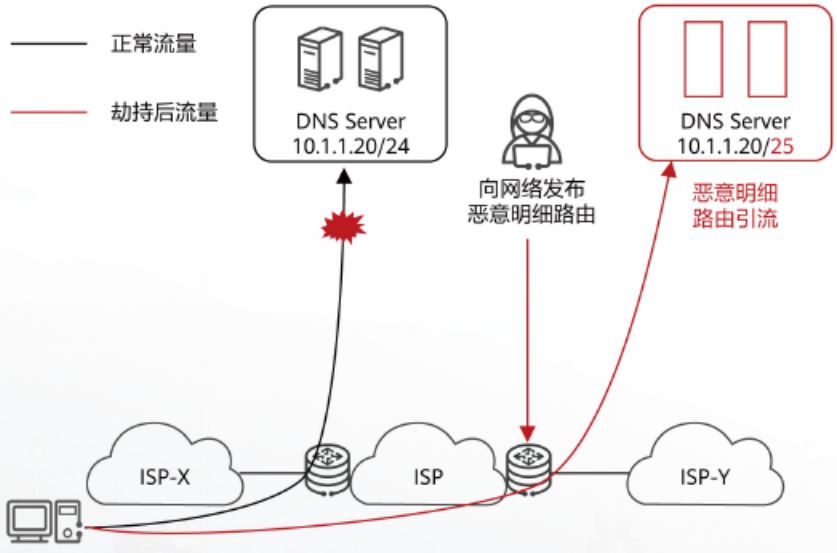

图11 BGP路由安全威胁场景

对于来自互联网或域间邻居的 BGP 路由，可能会产生如下威胁：如果某个 AS 向邻居 AS 传播违背路由出站策略的路由通告，则发生路由泄露；如果攻击者非法伪造或篡改 BGP 路由，发布给 BGP 邻居，则发生路由劫持。

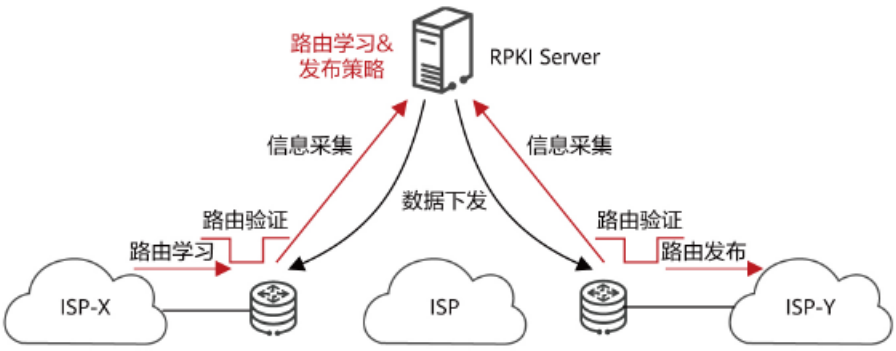

图12 BGP路由安全方案

对于这些威胁，需要保证路由发布的来源是可信的，并且路由经过的 AS 路径也是合法可信的，这样才能确保路由器收到的路由是可信的，路由连接是安全的。路由连接可信相关的能力包括：基于路由可信源部署对 BGP 路由进行认证，实现 BGP 路由防劫持、防泄漏，如上图所示；系统具备网络路由状态采集及可视化能力，能够对路由变化进行存储及分析，为评估网络路由的健康状态提供有力支撑。

- **准入连接可信**

对应接入网络的设备或者用户，需要进行准入接入认证，防止不可信接入源对网络和业务的攻击。准入连接可信的能力有：使用端口认证机制对接入端口或终端进行身份认证，确保接入合法；对接入业务用户使用认证协议进行身份验证，保证合法才能接入网络；对接入侧连接进行防攻击保护，确保不受非信任域的仿冒、窃取、DoS 等攻击。

- **网络流量防护**

为了确保用户流量的安全，需要支持对网络流量进行加密、认证，同时需要防止网络流量的 DDoS 攻击。对于异常及恶意流量安全威胁可以实现快速溯源、自动阻断。实现流量按需动态引入安全防护资源（FW、IPS、AV 等）。网络流量防护的相关能力包括：建立端到端 IPSEC 的业务流隧道，保证转发流量安全性; 具备流量路径控制能力，通过流量控制等手段动态控制和消减攻击流，保证防御 DDoS 攻击的实时性；异常及恶意流量安全威胁快速溯源、自动阻断；安全业务按需动态编排和协同处置。

- **网络可靠性**

网络承载用户业务需要确保故障后业务快速恢复。在配置错误或协议报文过载攻击时，保障关键业务正常运行。可靠性关键能力包括：OSPF/ISIS/BGP 等协议具备快速收敛能力，能够确保故障后业务快速恢复；MPLS LDP/MPLS TE/L3VPN/L2VPN/EVPN /SRv6 隧道具备快速收

敛能力，能够确保故障后业务快速恢复；负载分担精度应满足业务要求，链路调整后具备快速收敛能力，缩短连接建立时间，确保网络可靠; 协议应具备优雅降级能力，在系统过载时进行策略性操作，保障 IGP/BGP 等关键业务正常运行。

承载安全域组网安全设计防护要求，主要面向故障场景（包括设备故障、链路故障、网络故障场景），承载网继续提供安全可靠的传输路径，提供主备冗余逃生平面或者规划关键节点的角色分裂设置，防止不同业务类型同时发生故障。

- **差异化体验保障**

从不同用户的需求及各行各业的数字化转型看，网络提供业务体验的差异化已成为普遍诉求。差异化体验保障的关键能力包括：具备构筑差异化平面的能力，针对不同业务提供服务体验，例如低时延、高可靠及安全隔离等，作为用户体验保障的基础；具备精确测量业务质量的能力，能够提供业务级 SLA 的实时感知以及连接的可视化服务，作为用户体验保障的支撑；具备快速调优能力，能够结合业务质量的实时测量结果实现网络快速优化，确保用户的端到端服务体验。

4.4 管控可信

4.4.1 设计目标

管控可信是设备及网络安全大脑，持续监测全域及设备的安全态势，实现可信行为可预期，一体化的安全防御，打造网络安全可信能力。当受到外部攻击时，整个系统可以对单域和全域两个层次的威胁关联分析和闭环阻断，实现可信结果可验证。

- **单域闭环：**当设备受到攻击时上报控制器，控制器负责威胁关联分析，并下发安全响应策略到网元层。支持单域内安全事件自闭环。
- **全域闭环：**全域安全大脑负责端到端收集网络安全风险信息，进行全域的风险关联分析，并在网络内部实现威胁近源阻断，自闭环。

管控可信如下图所示，有三个设计目标需要达成。

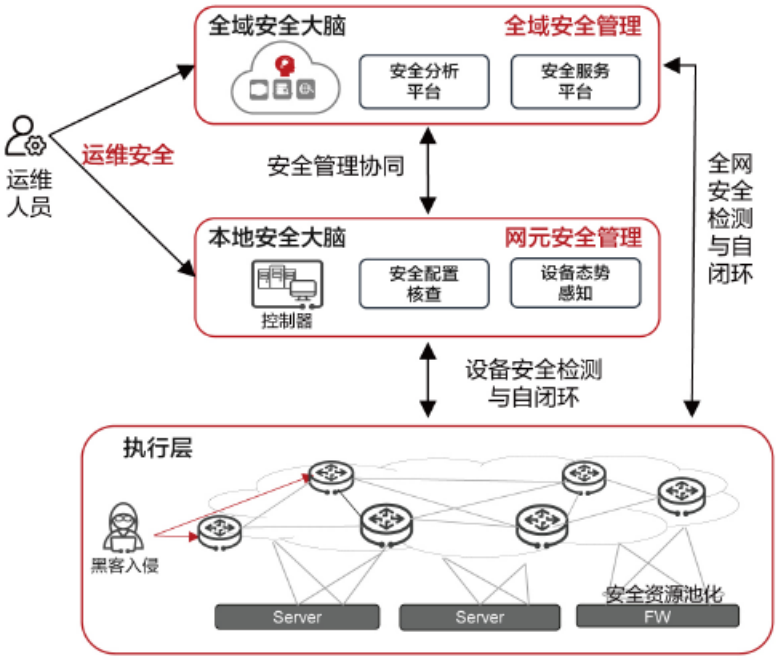

图13 管控可信架构

- **云网安一体协同：**

通过全面收集终端、网络、边界、云的资产、网络流量、安全日志、漏洞扫描日志、主机安全等尽可能全的安全威胁事件信息，进行统一综合分析和研判，提升安全分析精准率，安全态势可全域统一呈现，同时实现精准溯源和安全事件快速闭环处置，可对违规的主体立即就近阻断，实现云网安一体防护和一体运营。

- **网元设备态势感知：**

网络控制器在提供网络运维能力的同时，通过单域态势感知提供安全运维能力，可以针对网元、网管自身遇到的攻击入侵、软件篡改、恶意操作等安全事件，构建安全检测和响应、安全策略编排的能力，实现“分钟级”的快速感知和处置能力，降低用户的安全运维技术门槛、人员成本。

- **管理运维零信任：**

零信任代表了新一代的网络安全防护理念，提倡以身份为边界作为权限管控的基础。零信任认为企业不应该自动信任内部或外部的任何人 / 事 / 物，应在授权前通过动态和持续的身份认证和信任评估，对访问过程中的人和设备等访问主体的危险等级进行科学准确判定，采用最小权限访问策略，严格执行访问控制，提升所有网络实体连接之间的可信关系，增加企业安全保障，实现管理用户的防黑、防呆、防内鬼。

4.4.2 能力要求

实现管控可信的云网安一体协同、网元设备态势感知、管理运维零信任的设计目标，需要具备如下的技术能力。

- **云网安一体协同的关键能力：**

云网安一体协同主要分为四个能力，统一安全分析，精准溯源、近源处置和网络安全服务。通过持续收集全网全量的流量信息，以及终端的安全、漏洞等安全事件信息，进行统一的安全关联分析，提升安全分析准确率，减少重复或者无效的告警，并对于威胁源进行精准溯源，溯源到攻击者的身份和位置，根据溯源后的位置进行近源快速阻断，防止威胁横向扩散。

① **威胁的全面收集，统一安全分析：**

为了提升安全事件分析的准确性，需要收集尽可能多的信息，特别是终端（含服务器）信息、流量信息、安全日志信息等。这些信息散落在不同的网络位置，必须要把端、网、云、安进行统一纳管并收集，通过统一的安全大脑，以获得更精准的分析结果。在信息收集的时候，在所有可能的攻击路径上部署探针采集流量信息，采集各级安全设备的事件、告警信息、与云安全分析平台对接获取云内威胁事件，与终端安全服务器对接采集终端安全日志及合规信息。在信息收集之后，基于采集的多维度数据，通过诱捕、沙箱、大数据关联分析、智能检测算法分析，发现全网已知或未知威胁，实现云内、云外威胁统一呈现。

✔ **采集全网流量信息：**在网络中分级部署内置探针或流量探针，在所有可能的攻击路径上采集流量信息。

✔ **获取云内的威胁信息：**安全态势感知平台和云安全分析平台对接，从云安全分析平台获取租户安全信息、威胁事件、资产信息等。

✔ **收集终端安全信息：**在园区的智能终端上部署终端安全软件进行安全合规检测，终端安全服务器收集终端安全信息，并将信息传递给安全态势感知平台。

✔ **收集资产数据和漏洞信息：**安全态势感知平台通过内置探针、漏扫等收集全网的资产数据和漏洞信息。

✔ **收集全网的事件、日志数据：**安全态势感知平台和云安全分析平台对接，收集全网的网络、安全设备，如防火墙的安全事件、告警、日志等数据。

② 精准溯源

安全态势感知平台发现威胁后，需要找到真正的攻击源。通过云网安协同联动可确定攻击路径，可自动精准溯源到威胁接入位置，识别威胁发生的接入对象名称，威胁发生位置可视，为威胁处置提供精准的数据。

③ 近源处置

安全态势感知平台发现威胁后，需快速处置威胁，缩短威胁平均遏制时间，通过自动化的手段提升威胁事件的处置效率，避免威胁扩散。当识别到严重威胁时，需要立即自动或者手动确认后对威胁进行遏制，以避免威胁进一步扩散到其他位置。进行遏制的位置会有多种选择，如果位置选择过高，威胁会继续扩散同区域内的其他资产，因此必须选择尽可能接近攻击源且在可控制范围内的设备。如果通过手工对接入位置进行排查，一般需要查找多台网络 / 安全设备的日志 / 表项才能够找到，还有可能涉及跨部门的协同，往往需要天级或者小时级，效率低下。所以，可通过在全域安全大脑进行全网信息协同实现威胁自动识别，达到分钟级地查找和近源阻断。

④ 网络安全服务

构建安全资源池，安全管理平台对安全资源池内组件进行统一的策略下发和流量编排实现安全服务能力动态调配。安全资源池支持各种安全服务组件（AntiDDoS、防火墙、IPS 等），网络支持基于 SRv6 业务链实现引流策略、防护策略的下发，实现安全服务的灵活调度及编排，提供按需、弹性的安全服务。

- **网元设备态势感知关键能力：**

✓ **安全配置检查：**为了降低用户配置带来的安全风险，解决人工核查的繁琐过程，需要针对不安全配置提供自动核查能力。同时，提供对不安全配置的自动审核、闭环修复能力。安全配置是减小暴露面的有效手段，发现设备配置缺陷，可以防止配置不当触发的网络入侵。持续感知网元风险态势，缩短风险暴露期。

✓ **网元入侵检测：**通过检测黑客多路径的系统入侵行为（例如事前扫描、暴力破解，事中提权、安装恶意进程，事后安装后门、数据外发、软件篡改等），或用户行为异常操作检测（例如新增账号、更改口令、删改日志等），分钟级感知网元 / 网管入侵事件。

✓ **安全可视化：**为网元及网管提供安全可视化管理能力。

✓ **安全响应：**支持闭环脚本，动态按需编排实现及时响应威胁事件，并快速闭环处置。如果

是单域内的基础安全事件，在单域内实现分钟级快速闭环。如果是高级安全事件，接受上层整网安全运营平台的统一调度，接受并执行响应策略。

- **管理运维零信任的关键能力：**

管理运维网络主要承载运维用户对企业 IT 资产和具体业务的日常运维工作。通过网管集成运维动态安全分析能力，实现异常操作及时发现。管理运维零信任主要包含如下几方面内容：

✔ **运维人员动态精准识别：**网络管理系统协同 4A 构建 PDP 能力，对用户进行持续信任评估监控，判断用户“是敌是友”。

✔ **异常行为实时感知：**管控单元侧构建动态信任评估引擎，对异常行为评估风险等级，触发安全事件上报，支持上层 PDP 对于历史行为主动审计。

✔ **恶意行为事中实时响应：**管控单元对用户进行持续信任评估监控，结合避免恶意删除的规则，发现该用户在非正常时间范围执行高危命令，与正常行为存在偏差，马上上报告警并阻止用户执行。

5 可信网络实践案例

5.1 网络可信 – 路由连接可信能力实践

5.1.1 实践背景

数字化时代，互联网业务高速发展，对承载业务的 IP 网络也提出了更高稳定性、可靠性的要求，IP 网络控制平面稳定又是 IP 网络稳定的基石，一旦控制平面发生故障，对业务影响面大。传统的 IP 网络控制平面运维面临诸多挑战：

- **缺乏有效预警和故障定位手段：**路由查询基本靠手工，运维人员要花很长时间才能在全网设备中定位故障源；
- **控制平面的瞬时故障定位难：**运维人员定位时无法重现，也无历史信息可查。

5.1.2 部署方案

中国联通北京分公司联合华为在北京核心路由器上成功部署了路由安全解决方案。通过在核心路由器与服务器建立 BMP 连接，监控 BGP 邻居及 169 骨干网的入方向和出方向路由，实现全网路由实时监控及重点客户的业务保障。

该解决方案凭借实时感知域内 / 跨域节点千万级路由信息的多维统一管理和分析、历史路由变化一键回溯等核心能力，及时发现路由波动、路由异常等问题，有效解决 IP 运维难题，提升运维效率，助力北京联通重塑安全的智能 IP 网络边界。

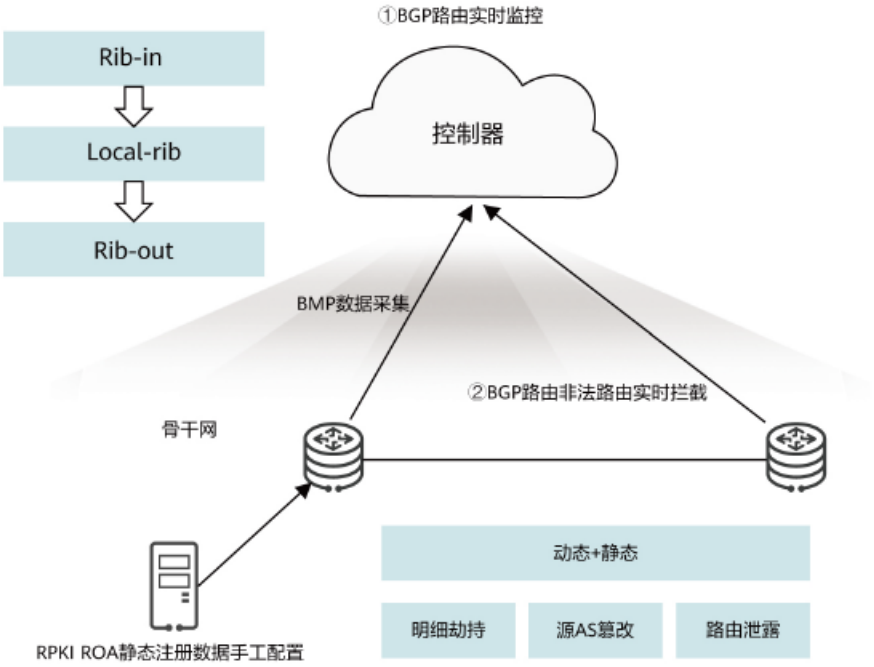

图14 路由连接可信部署方案

5.1.3 实践价值

- **路由实时采集，多维可视**

传统方案单纯采集分析 IPv4 单播路由，无法获得设备上 BGP 全量路由信息，呈现信息有限。路由安全解决方案，通过 BMP 协议机制拓展了 BGP 路由监控的能力，支持 BGP 路由信息在线收集，通过多种可视化手段（如物理拓扑视图、协议视图等）让运维人员直观地观察和了解 IP 网络的动态变化，并且具备千万级的路由处理能力，充分满足大型网络的应用场景。

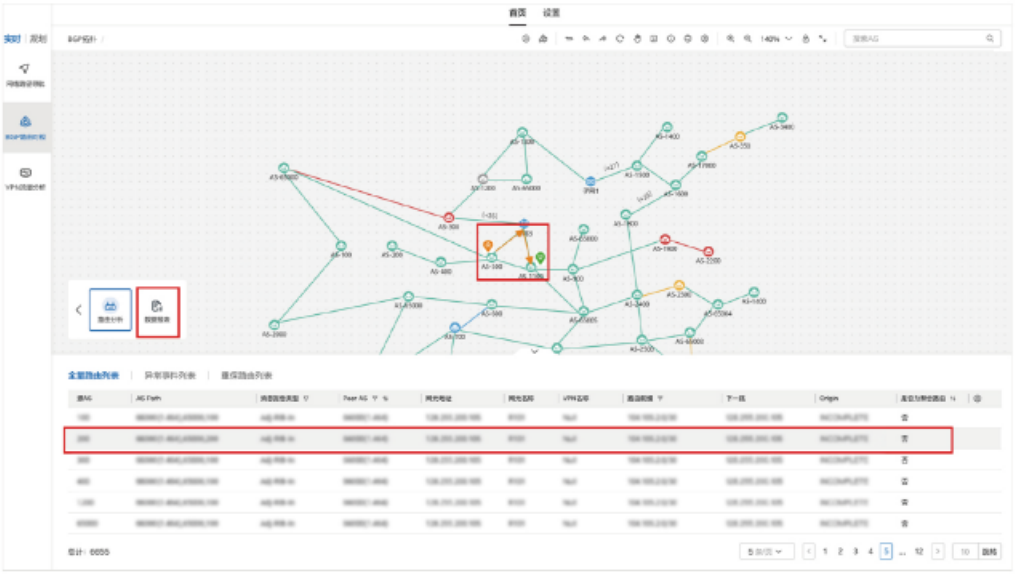

图15 路由拓扑可视化呈现

- **多维历史回溯，一键查询**

在城域网络出口，路由量大，变化频繁，而且许多异常是短暂的，由此引发的业务质量问题都难于回溯和定位。路由安全解决方案可根据 BGP 路由属性、路由前缀特征等多维信息组合查询，长期采集并保存控制平面的路由消息，可视化呈现网络历史的拓扑，可按照事件发生的时间先后回溯网络在选定时间段内的变化过程，轻松发现瞬时出现的故障。

- **主动防御及路由劫持抵御能力**

支持基于 ROA（Route Origin Authentication）校验路由前缀与 AS 号的合法性，在转发层面也具备主动防御路由劫持的能力，从而实现控制层面与转发层面的双重防护。

5.2 网络可信 – 流量安全可信能力实践

5.2.1 实践背景

当前市面上的网站安全防火墙产品基本都是通过 DNS 域名重定向方式提供服务，具有以下问题：

- 无法针对没有域名的网站及系统提供应用层防护且攻击者直接采用 IP 访问时，会绕过高防，不能进行有效防护；
- 高防 IP 变化时，需同步 DNS 修改，更新不及时；
- 部署在云端，虚拟化形态，性能较弱。

5.2.2 部署方案

中国联通联合华为在现网成功部署了新型高防智能协防架构，提供网络大流量攻击全栈清洗及网站攻击防护服务 。利用 SRv6 业务链技术实现基于 IP 地址的广域双向流量牵引，构建骨干网分布式高防中心，借助 SRv6 业务链与已有 DDoS 流量清洗中心形成协同防护的一体化智能防护架构，打造新型高防产品。

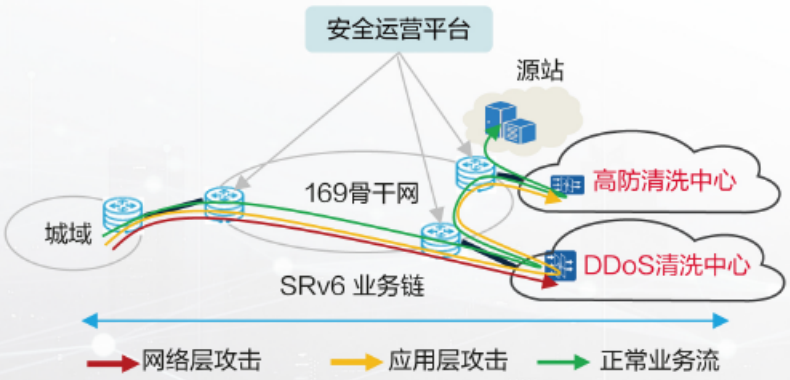

图16 流量安全可信部署方案

安全运营平台收到攻击流告警后，下发引流任务，从而实现攻击流量近目的和近源清洗。在提供清洗网络层 DDoS 攻击服务的基础上，进一步提升了对应用层攻击处置的能力，建立了可针对域名的网站及系统提供应用层防护，构建了新型高防产品的智能协防架构，得以实现高防中心、清洗中心等不同资源间灵活配置、协防部署，形成了网络攻击全栈清洗及防护标准化产品。

该解决方案成功突破传统安全防护能力的局限性，采用业务链 SFC、SRv6、BFS 等 IPv6+ 技术，通过部署安全资源池，为互联网专线、家宽等业务访问目标源站提供安全增值服务。

5.2.3 实践价值

提供运营商独有的大网能力，从中国联通全网视角进行攻击流量的监测、分析、溯源及定位，达到用户业务所需的 3-7 层全方位的精准防护，并且可在用户网络上游缓解宽带资源拥塞，从源头有效防御流量攻击。

透明化防护通道保证用户无需设备维护，无需网络配置，无需更改业务流量路径，即时开通防护，实现流量安全防护。

6 总结与展望

数字化转型是国家十四五阶段的关键任务之一，各地积极贯彻落实党中央国务院关于数字化发展的战略部署，纷纷出台数字化转型的发展总体规划、行动计划、实施方案等落地举措，抢抓数字化新机遇，布局数字化先手棋。站在新起点，数字化发展呈现“引领”、“改革”、“创新”新特征，愈益成为引领高质量发展的主要引擎、深化供给侧结构性改革的主要抓手、增强经济发展韧性的主要动力。

数字化浪潮既为企业开启了商业模式再造和产业转型升级的大门，又为企业带来了多方面严峻的安全挑战。新冠疫情带来的居家办公和移动办公，改变了企业传统的运作方式，同时数字化服务价值使得企业更加重视数字化业务的投入，促使企业以更加审慎的目光聚焦现有的安全机制，并迫切需要新一代的网络安全防护体系来为企业的数字化进程保驾护航。

可信网络安全模型作为一种全新的安全防护模型，经过多年的实践已经从理念走向了实践。作为全新的安全模型，其所带来的不仅是技术的改变、安全架构的重构，更是要求企业信息安全管理思维模式的转变，并深入影响到企业文化、运营流程以及管理规范。可信网络建设不可能一蹴而就，在这个过程中，企业在理解可信网络理念、规划可信网络路径、评估可信网络方案以及部署可信网络体系方面，仍不可避免地面临一些问题。因此，我们提出，正在推进数字化转型以及发展数字化服务的政府、各行业企业与组织机构，首先需要将可信网络的理念融入企业的发展战略，并通过渐进和务实的整体规划，从当前的核心场景出发，制订可信网络建设路径，并借助合作伙伴的产品和技术、生态系统覆盖以及相关行业实践的经验，构建面向未来业务发展的新一代可信网络安全防护

体系，通过增加自适应性以应对未来不确定性所带来的挑战。具体建议包括：

- **建生态：**借助合作伙伴生态，邀请业内企业、行业组织的专家，通过开放论坛成立可信网络联盟，打造网络安全生态体系，构筑可信网络产业链生态。首先，企业与组织机构必须具备开放心态，积极拥抱可信网络理念，选择能够进行自主知识产权创新的可信网络解决方案。其次，所选择的可信网络解决方案必须能有效解决在构建安全防护体系的多层面问题，形成一体化的解决方案，并具备定制化开发等服务能力，以及针对现有安全组件的集成能力。最后，需要充分整合合作伙伴的力量，共同构筑可信网络的产业链，为企业的数字化之旅奠定坚实的安全基础。
- **立标准：**网络安全已经成为国家的战略，并通过立法、标准、规范来推动网络安全的建设，但面临 CT 关基领域的标准缺失。因此在 CT 关基领域建立国家级产业统一标准规范已经迫在眉睫。首先，对准国家网络安全法，定义可信网络总体安全目标、能力要求及措施，作为可信网络的总体指导。其次，定义可信网络技术要求及网络分级指南，明确网络安全能力分级指导原则、方法及分级的技术能力要求。最后，定义可信网络测评要求，明确等级评测的具体测评方法、对象及对测评结果进行判定的基本规则。
- **推创新：**面向未来业务发展及网络风险的不确定性，一方面需要整体规划可信网络战略路径、解决方案，从体系上进行安全防护。另一方面，结合业务风险，不断地联合探索技术创新方向，将技术创新作为推动网络安全防护的重点方向，通过新技术屏蔽未来网络安全的越来越多的不确定性。最终打造三层可信架构的坚强网络，全面填补可信技术与体系空白。

最终，构建开放的创新体系，打造全网可信评估体系，规范推进产业高质量发展。

7 术语&缩略语

缩略语	英文全称	中文全称
4A	Account Authentication Authorization Audit	账号认证授权审计
APN	Application-Aware Networking	业务感知网络
BGP	Border Gateway Protocol	边界网关协议
BGP FlowSpec	BGP Flow Specification	边界网关协议流规则
BMP	BGP Monitoring Protocol	BGP 监控协议
CCRA	Common Criteria Recognition Arrangement	通用标准互认协议
CRC	Cyclic Redundancy Check	循环冗余校验计算
DDoS	Distributed Denial of Service	分布式拒绝服务
DNS	Domain Name System	域名系统

EDR	Endpoint Detection and Response	端点检测与响应
ENISA	European Union Agency for Cybersecurity	欧盟网络安全局
FEC	Forward Error Correction	前向纠错
IPv6	Internet Protocol Version 6	互联网协议第 6 版
MANRS	Mutually Agreed Norms for Routing Security	互联网路由安全规范
PDP	Policy Decision Point	策略决策点
RPKI	Resource Public Key Infrastructure	资源公钥基础设施
SRv6	Segment Routing over IPv6	基于 IPv6 的段路由