中兴通讯软件定义安全资源池

——助力中国移动互联网公司南北方基地扩容

一、 案例概述

1. 案例背景

随着虚拟化、云计算、SDN/NFV、大数据、物联网、人工智能等新技术的发展，传统的数据中心和网络都发生了巨大的变化，传统的安全设备难以在云平台上应用，例如传统的安全设备不具备虚拟化所需的自动部署、动态弹性等特性，同时也很难满足多租户的动态创建、按需分配的需求。

以建设软件安全资源池为核心和契机，围绕安全技术的研究和产品研发将有助于提升我国信息安全产业的整体技术水平，推动我国产业结构战略性调整，提升我国的网络信息安全水平，保障国家、企业和个人的数据安全，解决经济社会发展的一个重大瓶颈问题，保证社会稳定性及经济平稳发展，从而提高国民经济运行质量和效率，形成国民经济发展的新动力，实现经济社会的全面协调可持续发展。同时，网络安全也是应对经济全球化挑战、把握发展主动权、提高国际竞争力的必然选择，有利于提高我国在全球范围内竞争能力，提升我国政治和经济的国际地位。

2. 用户需求与痛点

随着新技术的发展，传统的数据中心和网络都发生了巨大的变化，同时带来了新的安全问题和挑战，导致了安全风险的叠加。

- 一方面，传统的安全问题仍然存在，原有风险一个不少，如病毒、

木马、勒索软件、DDOS 攻击、SQL 注入、僵尸网络、操作系统漏洞、应用程序漏洞、钓鱼软件等；

- 另一方面，新技术本身带来了新的安全问题，且传统的安全设备与安全策略又难以适应新的网络环境和安全需求，引起了大量新的风险，如虚拟机逃逸、数据残留、流量不可见、流量混杂、边界模糊、SDN 控制器安全、接口安全、转发面攻击等。

安全问题变得更加复杂，攻击的途径和手段更加多样化。因此，构建全新的软件定义安全资源池成为网络信息安全领域的热门方向，安全也变成了一种服务，而不仅仅是是防范工具。

3. 案例概述

在 SDN/NFV 的基础上，中兴通讯的安全资源池基于软件定义安全架构，对安全设备进行重构，实现了多种安全技术的动态联动、纵深防御，安全防护可以做到自动、动态、闭环处理。系统采用了通用、可编程、虚拟化的开放架构，可实现：

- 软件定义业务编排，支持安全业务链，安全服务按需定制、灵活编排、运维便捷；
- 借助软件定义边界技术，通过严格的身份认证、设备认证和业务权限认证等要素，形成动态业务防护网络；
- 基于业务和威胁进行策略动态调整，安全资源按需分配，弹性扩展。

二、 解决方案

1. 中移互联网公司南北方基地扩容项目解决方案概述

中移互联网公司开始发展云业务以来，快速增长，建设了融合通信平台、基础通信业务平台、互联网社交业务平台、杭研自研能力引入、智能网应用创新平台、企业应用创新平台、统一业务支撑平台，为满足这些平台的资源需求，中移联合中兴通讯对通用软硬件进行扩容。中国移动针对部署 NAT、防火墙以及 HTTP 代理的网络接入场景，扩展 CM-IMS 业务的网络接入能力和安全通信能力，引入中兴通讯软件定义安全资源池，增强用户随时随地接入的体验，保障用户数据的安全性，为 CM-IMS 业务提供端到端的私网穿越和安全加密能力。

中兴通讯提供了完整的 SDN/NFV 解决方案，完全兼容 Neutron 的 API 接口能力，支持对硬件安全设备及 vFW 等 NFV 资源的统一纳管，支持安全策略、Qos、IP/MAC 防欺骗等安全机制，形成统一的软件定义安全资源池，动态分配安全资源和策略，与控制器配合，按业务需求灵活编排网络，实现安全资源的快速部署和弹性伸缩，对安全资源统一管理、集中分析、闭环防护。软件定义安全资源池在传统的安全技术架构基础上，实现安全资源的抽象化、池化，提供弹性、按需和自动化部署能力。

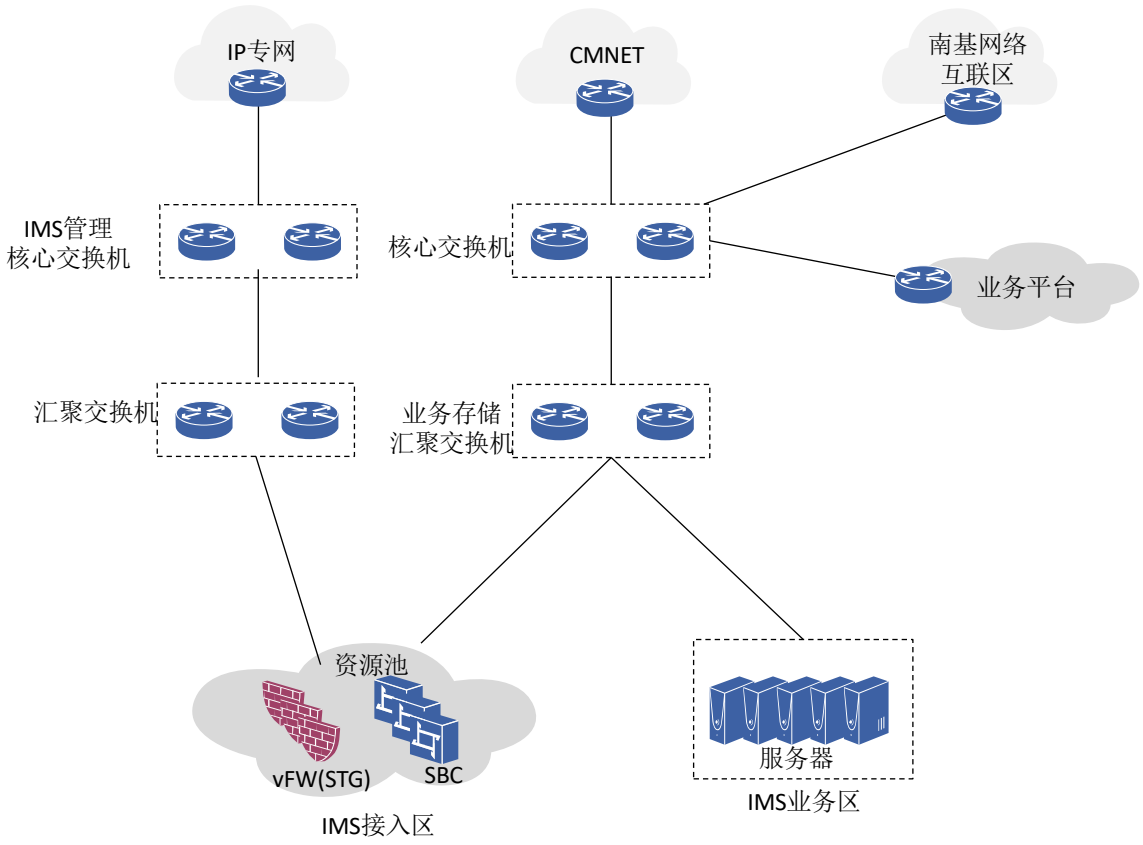

图 1 中移项目组网示意图-南

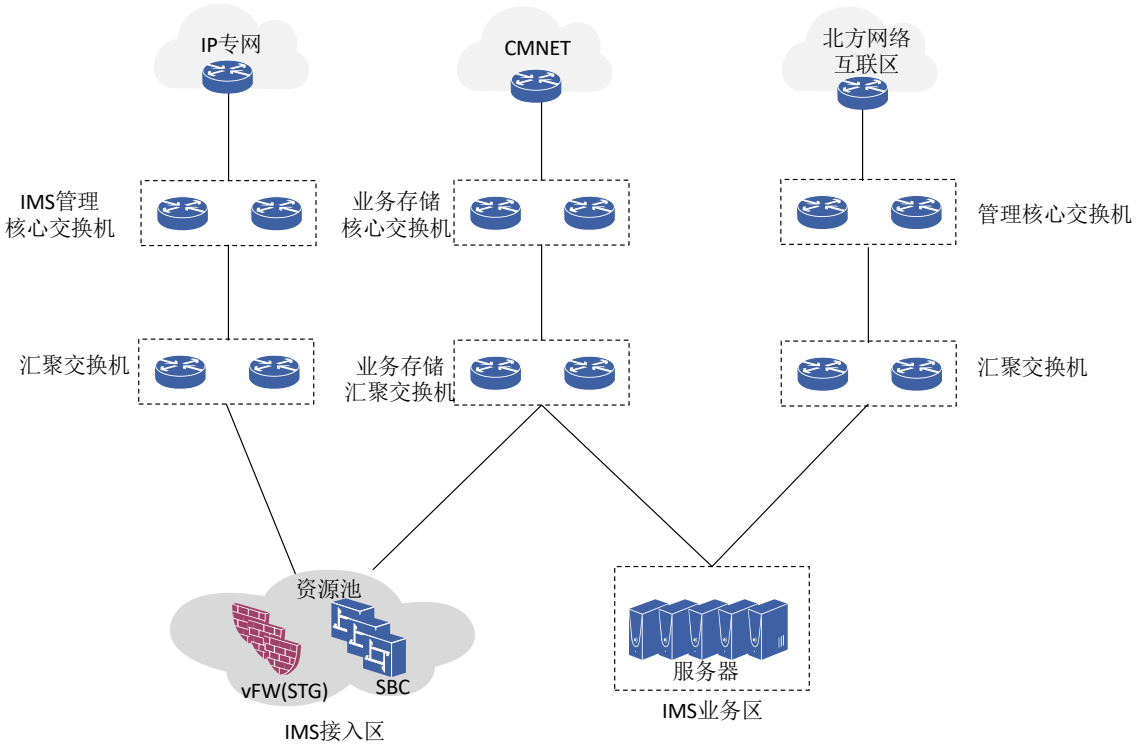

图 2 中移项目组网示意图-北

中移在 CM-IMS 网络中部署软件定义资源池，使用 vFW 安全服务，其包含 STG（Security Traversing Gateway 安全穿越网关）功能，企业网中可部署 HTTP 代理等设备连接 vFW，将 vFW 作为 CM-IMS 的入口点。

vFW 支持 STG 功能，作为 VPN 隧道的服务器端，负责维护 vFW 和 CM-IMS 客户端中集成的 CM-IMS 终端之间建立的 VPN 隧道，对 CM-IMS 业务数据进行封装和解封装。可选的 VPN 隧道类型包括 TLS 隧道、DTLS 隧道，可选择性的扩展到 HTTP 隧道（要求 CM-IMS 终端与 vFW 建立和维持 HTTP 长连接，确保 vFW 网元主动推送信息给 CM-IMS 终端）。

终端将 CM-IMS 数据封装后通过隧道传送给 vFW，vFW 将报文解封装后转发给 SBC，再对 CM-IMS 业务数据进行处理。CM-IMS 业务数据从核心网发往以安全隧道方式接入的终端时，由 SBC 将数据发给 vFW，vFW 对业务数据进行封装和加密，通过安全隧道转发给 CM-IMS 终端。vFW 具备对在线用户会话管理以及为 CM-IMS 终端分配虚拟 IP 地址的功能。

vFW 网元提供配置管理接口和业务接口（含与 CM-IMS 终端的业务数据接口、与 CM-IMS 核心网网元的业务数据接口）。其中配置管理接口负责接收管理员或者管理软件下发的配置请求，返回配置执行结果，业务接口负责 vFW 和业务网元间的业务交互。

中移部署软件定义安全资源池时，在租户内部，用户通过 dashboard 创建防火墙服务(FWaaS)，防火墙插件会将消息解析为对应

的虚机创建命令，交由 VNFM(MANO)来创建管理对应的 vFW 虚机；虚机创建完成后，采用 SDN 控制器引流方式，VNFM 调用控制器提供的引流接口，将对应的 vrouter 流量引入到 vFW 虚机内，vFW 处理后再返回给 vrouter。在实际工作中，vFW 处于交换透明模式，不影响现有组网；在虚拟环境中，提供安全服务的全部虚机集中管理在一个租户内，对普通用户不可见。

vFW 还可以检测、控制多种协议报文，并提供丰富的防御功能，如基于 ACL 包过滤、状态检测、ASPF、域间策略、DDoS、DPI、电信级安全防护等，提供云数据中心业务主机（包括虚拟主机）间东西向流量的安全隔离管控能力，提供数据中心对外访问安全防御能力，依据 X86 机架服务器的数量和性能平滑扩展。用户可通过自服务门户配置防火墙安全策略的配置，添加成功后，即时生效，能够有效保障用户业务安全。

软件定义安全资源池支持弹性伸缩，根据弹性策略，动态弹缩。以虚机为粒度进行弹性扩展，当吞吐量或者会话数增大，达到阙值上限时，开始弹出新的虚机，分担原有虚机的流量；当吞吐量或者会话数降低，达到阙值下限时，开始缩回虚机，减少虚机数量，节约资源。

采用多种技术来提升性能、降低时延，如 SR-IOV、DPDK、控制转发分离等。

支持高可用，包括设备级主备和单板级主备，主备 VNF 之间会话实时同步，主备 VNF 业务无缝切换，不存在单点故障造成业务中断，对于分布式虚拟防火墙，结点故障不能影响其它结点业务，时延低于

1.5 秒，领先业界水平。

2. 技术优势和方案亮点

- 安全资源池化

软件定义安全资源池通过软件定义的方式，将安全策略控制和防护转发分离，将硬件安全设备虚拟化、云原生，不但解决了数据中心内部安全防护需求，同时也为 SDN/NFV 方案提供了灵活按需的安全服务。

- 弹性伸缩

支持弹性伸缩，按租户动态分配安全资源和策略，与控制器配合按业务需求灵活编排网络，提升了资源利用率。

- 降低成本

通过虚拟化技术，重构电信级的安全功能，减少了硬件设备的采购，极大降低了设备投资成本。

软件定义安全资源池将安全服务统一部署和按需编排，实现对安全资源的全生命周期管理，以及安全策略自动化配置，具备智能的安全运维能力，同时也降低了安全运维成本。

3. 商业价值

中移互联网公司融合通信扩容建设的新增资源已正式上线，分别部署在北方呼和浩特节点和南方广州节点，包括弹性计算、弹性存储、云网络、云安全、云运维 5 大类基础云服务，以及 SaaS 平台服务，相较于现网硬件设备改造扩容，资源池降低了 50%以上的硬件投入成本，实现了对 IT 基础设施与虚拟化资源的集中监控、性能告警、统计

分析，管理容量、配置信息与资产信息、资源管理、资源模板管理以及系统管理、运营报表查看等。中兴通讯软件定义安全资源池方案已在陕西移动等地规模商用。