园区网

1 方案介绍

随着 IT 基础架构、移动互联网等技术的发展和变化，传统园区网络的安全防护手段和思路面临着诸多挑战。首先，传统园区网往往会为每个业务建设一张独立的物理网络，但是在新一代园区网中业务种类越来越多，传统的建设模式会使得网络运维管理非常复杂，也不利于网络资源的有效利用。然后，传统园区网中的安全设备都是零散分布在区域边界，性能瓶颈、单点故障、信息孤岛等问题也困扰着网络运维人员。最后，新一代园区网络中移动终端种类和数量越来越多，任何一个终端设备都有可能成为入侵整个园区网络的跳板。

传统园区网的诸多挑战对新的安全解决方案提出了迫切需求。H3C 新一代园区网安全解决方案应运而生，为用户带来立体化、智能化的安全解决方案。

2 方案优势

2.1 虚拟化园区网络架构

通过 H3C 独创的 IRF2 技术将园区网络的接入层，汇聚层与核心层设备各自进行横向虚拟化，将多台冗余设备虚拟化为单台逻辑设备，形成一个网络管理与转发节点。横向虚拟化完成以后通过链路捆绑技术完成上下行链路的连接，无需再运行复杂的生成树协议。所以新一代园区网络的网络结构是简单的、路由表是简单的、管理是简单的。

另外新一代园区网络往往会为多个不同单位或业务提供网络需求，所以在整个园区网络中存在彼此完全隔离的网络、部分需要互访的网络以及能够公共访问的网络。华三通信使用 MPLS VPN 的多通道特性来满足这一需求，核心层设备作为 P 节点完成 MPLS VPN 数据转发，汇聚层设备作为 PE 节点完成对接入用户的网络隔离，接入层设备作为 CE 节点使用 EAD 技术对用户进行认证，将用户下发到相应的 VLAN 并对应到汇聚层设备的 VRF 中，通过 MPLS VPN 的路由控制满足各类访问需求。

2.2 终端安全准入和管控

针对新一代园区网络中终端设备呈现出的类型多样化和接入无界化的发展趋势，华三通信提出了“BYOD 终端移动化解决方案”。该方案支持 802.1X、Web Portal、MAC 和 VPN 等多种认证方式；支持完善的身份生命周期管理能力、独特的访客接入模式和基于角色的资源访问控制能力；支持对终端设备进行外设控制、黑白软件管理、防病毒管理、客户端 ACL 等安全

控制策略；支持细致的网络访问行为审计能力，通过详细的报表可以轻松掌握智用户网络访问轨迹。

2.3 关键路径的纵深防御

新一代园区网络要以“流量路径”为核心构筑层层递进的纵深安全防御体系。首先通过合理划分安全区域确定安全防御边界，包括互联网接入区、广域网接入区、用户接入区、服务器接入区等安全区域，然后根据流量路径上的每一道区域边界进行安全防护部署。依据“纵深防御“原则，流量路径的边界防护应具备网络层、应用层等多层次的防御能力，在流量路径上通过防火墙、入侵防御、Web 应用防火墙等产品的策略组合形成有力的防御体系。

在园区网中，互联网接入区作为连接园区内网和外部互联网的桥梁，一方面为园区网用户提供了访问互联网资源的能力，另一方面互联网带来的蠕虫、木马、钓鱼网站等各种攻击方式对园区网络的安全产生了严重威胁。因此互联网接入区是整个园区网络中最为重要的安全防护部分。在互联网接入区，不仅要部署防火墙、入侵防御、Web 应用防火墙等安全防护设备，同时也需要部署应用控制网关提供互联网应用访问分析和流量分析，部署负载均衡设备提供多出口链路的高可靠性。

2.4 安全态势监测与分析

在传统园区网络中，由于安全业务设备的种类不同、厂商不同和地理位置分散等问题导致安全业务运维非常复杂。另外由于各类安全业务设备的日志信息难以做到集中统一关联和分析，导致了园区网络“安全孤岛”的产生，很难从杂乱无章的安全日志中分析安全态势和追溯安全事件。H3C 新一代园区网安全解决方案针对这个问题，提出了“统一智能运维管理方案”。该方案将网络中的终端、网络安全设备、应用服务器等 IT 资源全部纳入安全监测范畴内，在统一的平台上进行日志信息、安全事件的统一收集、归类处理、智能关联和分析，可以实时动态分析园区网安全态势、回溯安全事件和安全预警，便于安全运维人员掌握安全状态。

3 客户价值

（1） 实现了多租户环境下的网络隔离和灵活访问需求

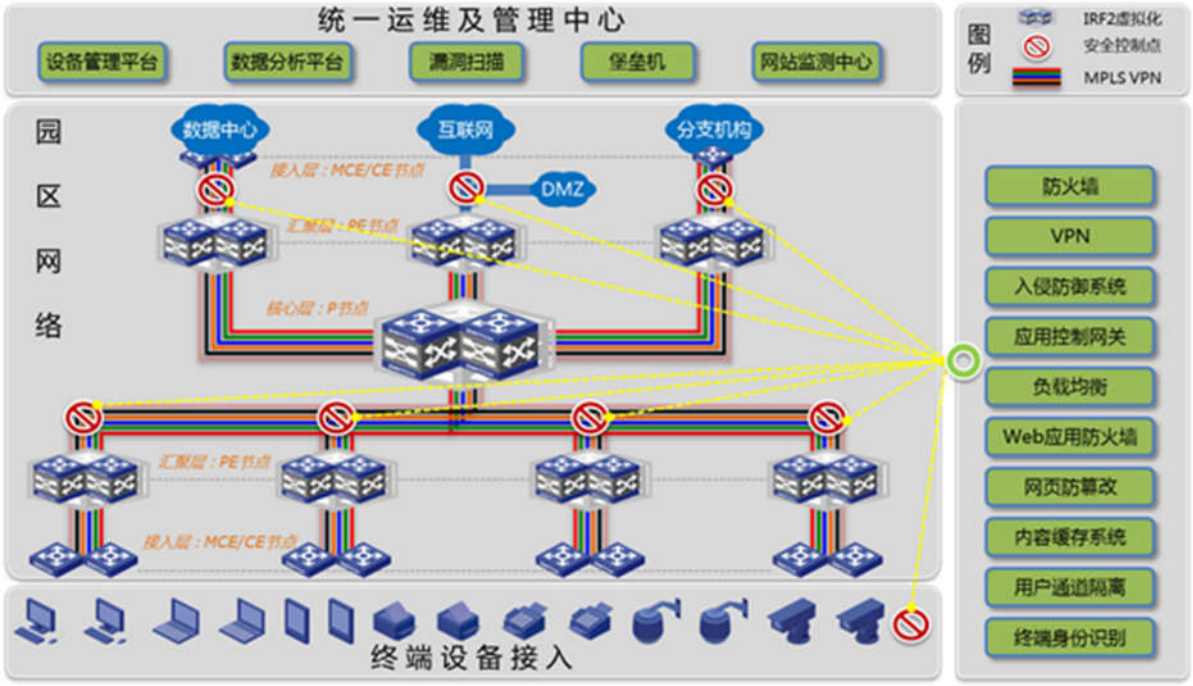
（2） 实现了对各类移动终端、物联网终端的安全接入和管控

（3） 实现了全网安全事件分析、态势监测、安全预警和及时响应

（4） 实现了简化网络结构、简化转发路径以及简化运维管理

（5） 实现了高可靠性的基础网络架构

4 典型组网



5 核心安全产品

管理平台： 天机/SSM

安全产品： H3C SecPath M9000 综合多业务网关、H3C SecPath F50X0 超万兆下一代防火墙产品系列、H3C SecPath T1000 系列入侵防御系统产品系列、H3C SecPath L5000/L1000 应用交付产品系列、H3C SecPath ACG1000 应用控制网关产品系列、H3C SecPath W1000/W2000 WEB 应用防火墙产品系列、H3C A2000 运维审计产品产品系列、H3C 云安全监测中心产品、H3C X-Scan 漏洞扫描产品系列、H3C 网页防篡改产品系列。

6 典型客户

7 未来展望

在 SDN、Overlay 等新技术的推动下，未来的园区网络将会发生巨大的改变。利用 Overlay 技术的虚拟网络特性能够天然地实现业务网络的隔离，满足园区网多租户的业务建设要求。Overlay 技术的另一个作为就是构建“大二层网络”，使得移动终端可以在园区网中任意迁移而访问策略不变。再结合上 SDN 转发与控制相分离的技术可以将整个 Overlay 网络的控制

层面进行集中和统一，可以实现对 Overlay 网络流量转发的灵活管理。在这些新技术背景下的未来园区网安全问题将会是一个崭新的命题：未来园区网的安全能力要和网络转发能力一样融入 Overlay 网络，并且能够被 SDN 控制器集中管理和控制，实现安全防护能力的同时做到按需灵活调度。