安全云服务作为一种特定的云服务，在其技术实现中最重要的也是资源能力的池化和虚拟化，只不过这种池化和虚拟化所针对的是网络安全这种特殊的计算资源和能力。为了满足用户的各种网络安全防范要求，安全云服务提供商在安全云服务的业务体系中一般包括防火墙访问控制、DDoS 攻击防护、入侵检测和防护、特定应用的安全检测和过滤（如 Email、Web 的内容过滤，木马、病毒等恶意代码的检测和过滤，特定 URL 流量过滤，垃圾邮件过滤等）、网络安全脆弱性扫描检测、Web 等特定应用的安全检测、安全事件的监控和分析、网络异常流量的检测、在线病毒和木马查杀、在线终端安全性检测等服务。这些安全云服务根据其业务提供的层次和形式分属于 SIaaS、SPaaS、SSaaS 的范畴，但不管这些业务的提供内容和形式如何，作为一种特定的云计算服务，均存在着资源池化和虚拟化的实现问题，所不同的是对于不同的安全云服务，其资源池化和虚拟化所采用的技术实现方案有所不同。

安全云服务资源池化指的是在多台安全设备中采用集群技术或者在安全处理软件中引入分布式计算技术，从而形成对用户透明的统一网络安全能力池的过程。安全云服务资源池化过程中要解决的主要问题是可扩展性、可管理性和可靠性。可扩展性指的是资源池的容量可以根据用户业务需求的增加进行弹性的扩充。可管理性指的是在资源池化之后系统具有对资源池的统一监控调度和分配的能力。可靠性指的是池化之后的资源池具有统一的一体化的协同处理和容错能力，不会因为特定物理安全设备单元的故障或失效影响到整个资源池的正常运作。

安全服务资源虚拟化指的是在实现资源池化的基础上根据用户需求在资源池中划分出逻辑独立的虚拟化安全能力提供给用户使用的过程。在用户看来，用户正在使用的是一个完全独立的安全设备和软件。安全服务资源虚拟化过程中要解决的主要问题是逻辑隔离、业务复用和智能感知。逻辑隔离指的是通过设备或用户管理实现用户之间资源和数据的隔离，保障用户独立资源使用的业务体验。业务复用指的是多个用户使用的虚拟安全能力资源在时间、带宽等方面实现在资源池中物理设备的复用，提高安全资源的利用率。智能感知指的是在安全服务资源虚拟化过程中可以智能感知资源池的业务状态和用户要求，实现设备资源和用户需求的契合。