5G 先锋

ZXUS vSTG 9000 虚拟穿越网关

ZTE中兴

ZXUS vSTG 9000 虚拟穿越网关

产品概述

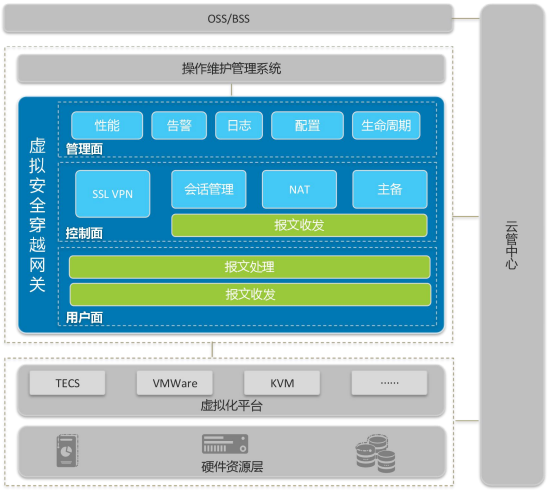
随着云计算/虚拟化技术的快速发展，数据中心和网络都发生了巨大的改变，不但传统安全威胁依然存在，还引入了新的安全问题和挑战。云环境下，不同租户的虚拟资源可以部署在相同的物理资源上，这引起了租户间的安全隔离和共享、资源的按需分配等问题，增加了恶意用户借助共享资源实施攻击的途径；移动办公、BYOD 等应用使得处于企业外网的终端需要访问企业内网资源，从而突破了内外网隔离的边界，同时数据中心内部的大量交互，导致网络边界更加模糊，这些因素使得攻击的途径和手段更加多样化；虚机迁移、虚机逃逸等问题需要新的安全策略进行应对。同时，新业务的飞速发展，使得安全与业务需要紧密结合，安全问题变得更为复杂，安全能力需要开放，安全也变成了一种服务，而不仅仅是防范工具。安全厂家需要提供更为开放、灵活的接口，为用户和应用提供定制化安全防护。

针对部署 NAT、防火墙以及 HTTP 代理的网络接入场景，虚拟安全穿越网关（vSTG，virtual Security Traversing Gateway）能够部署在云计算/虚拟化网络环境中，用于扩展 CM-IMS 业务的网络接入能力和安全通信能力，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。

基于传统的安全架构，ZXUS vSTG 9000 实现了安全穿越网关的资源抽象化和池化，可以自动部署和生命周期管理，支持与多种云平台集成，如 TECS、VMware 等。

ZTE中兴

系统架构



虚拟化平台

基于虚机方式的 vSTG 可运行于通用服务器上，为网络提供安全防护。vSTG 可以运行在 TECS、VMware、KVM 等多种虚拟化平台上，不依赖于专有硬件，实现了硬件和软件的解耦。

软件架构

为提高数据转发效率、增强系统可靠性和安全性，vSTG 采用管理面、控制面和用户面分离架构。管理面主要完成性能、告警、日志、配置、生命周期等管理；控制面主要负责协议相关处理和策略信息的动态生成；用户面根据静态配置，或动态生成的策略信息进行报文过滤、转换、处理、转发等流程。

这种隔离体现在如下方面：

网络平面隔离：内部网络分为控制面网络、管理面网络、用户面网络。

进程/线程间隔离：控制面、管理面和用户面的各个进程相互独立，且用户面线程进行了核绑定。

云管中心

云管中心中存在 vSTG 组件。在虚拟网络编排和运营过程中，针对不同的安全防护场景，vSTG 组件与云管中心其他网元协同为 vSTG 提供相应的管理，完成 vSTG 的生命周期管理。

操作维护管理系统

EMS 作为一个通用的操作维护管理系统，为虚拟安全设备提供操作维护功能，及告警、性能和日志的可视化呈现等功能。

ZTE中兴

产品特色

高性能/低时延

vSTG 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。

- SR-IOV

vSTG 采用 SR-IOV 技术将一个 PCI 设备在多个虚拟机中进行共享，因而提高了 I/O 设备的利用率，降低了网络延迟。SR-IOV 可以工作在 GE/10GE/40GE 接口上。

- DPDK

vSTG 采用 DPDK 技术来提升系统处理性能。DPDK 使用硬件多队列直接收发报文，有效地避免了软件分发线程造成的瓶颈，同时，采用用户态轮询模式来访问硬件资源，以提升网络的 I/O 吞吐能力，对硬件进行分类可以有效节省 CPU 资源。

- 控制转发分离

vSTG 通过采用不同的通道分离控制面功能（如协议处理、策略信息的动态生成）和用户面功能（如数据报文的过滤、转发、处理），以提升数据转发效率。

高可靠性

vSTG 采用改进的 VRRP 协议实现虚拟安全穿越网关热备份功能。改进的 VRRP 运行在主备 OMP 之间的 HA 通道上。系统运行期间，主备 OMP 之间通过接收到的 VRRP 报文协商主备工作状态。当任何一个主用 vSTG 的单元（PP）不能正常启动或操作时，备用 vSTG 上的单元将自动接管它。

由于 HA 通道是独立的 neutron 网络，因此不影响服务网络。

快速部署

vSTG 可以自动部署在通用服务器上，维护人员根据部署模板制作 vSTG 部署蓝图后，可以快速、灵活、自动地部署 vSTG，从而简化了运营商操作维护管理。

易集成

易集成：vSTG 可以快速、简便地集成在不同的安全防护场景中，由相应的云管中心进行编排和管理。

SDK 客户端集成：SDK 客户端支持多种操作系统，包括 Android、IOS、Windows、Mac。

丰富的安全功能

vSTG 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、域间策略等。

ZTE中兴

性能参数

为满足各种资源需求，vSTG 支持多种规格部署。

- C4、C8 规格，满足运营商/政企用户一定资源约束条件下的网络安全保护
- C14 规格，满足运营商/政企用户高性能网络安全保护需要

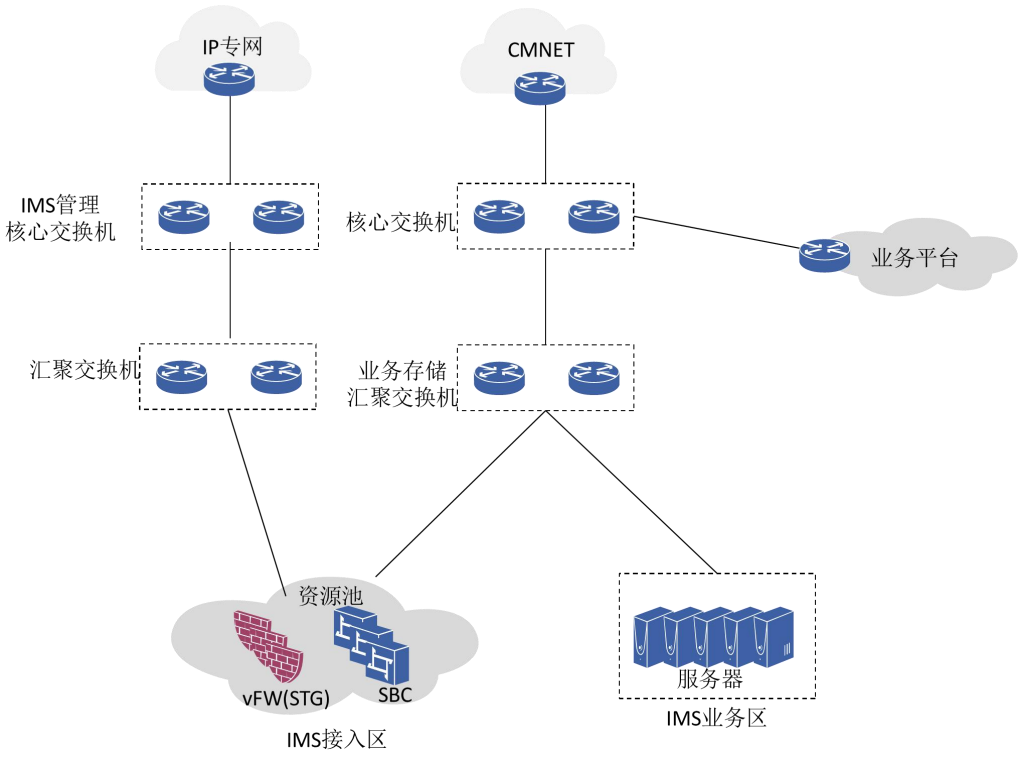
vSTG 各规格性能参数如下表所示：

规格/类型	vCPU	内存(GB)	存储(GB)
C14	14	40	40
C8	8	32	40
C4	4	20	30

典型应用

在 CM-IMS 网络中部署 vSTG，企业网中可部署 HTTP 代理等设备连接 vSTG，将 vSTG 作为 CM-IMS 的入口点。vSTG 作为 VPN 隧道的服务器端，负责维护 vSTG 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。

终端将 CM-IMS 数据封装后通过隧道传送给 vSTG，vSTG 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 vSTG，vSTG 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。vSTG 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。



5G 先锋

中兴通讯股份有限公司
ZTE CORPORATION
深圳市科技南路 55 号中兴通讯大厦
邮编: 518057
Web: www.zte.com
Tel: +86-755-26770000
Fax: +86-755-26771999

ZTE中兴