

5G 先锋

**ZXUS vSSL 9000**

**ZTE中兴**



## ZXUS vSSL 9000

### 产品概述

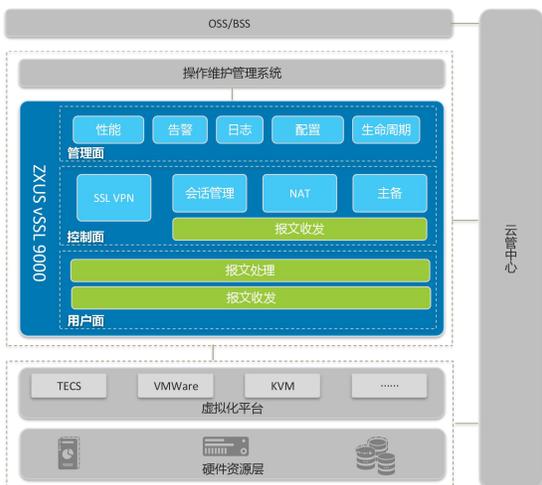
---

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；虚拟机迁移、虚拟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。

在大型企业的场景中，合作伙伴、客户、出差人员要求随时随地通过公共网络访问公司内网的资源。在这种场景下，SSL VPN 应运而生，提供了新型的远程接入方案，有效的解决了上述问题。基于传统的安全架构，ZXUS vSSL9000 实现了 SSL VPN 功能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。



## 系统架构



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。

这种分离架构体现在如下方面：

**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 vSSL 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，vSSL 组件与云管中心其他网元协同为 vSSL 提供相应的管理，完成 vSSL 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。

### 虚拟化平台

基于虚机方式的 vSSL 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，vSSL 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



## 产品特色

### 高性能/低时延

vSSL 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

vSSL 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

vSSL 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

vSSL 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

vSSL 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 vSSL 的单元（PP）不能正常启动或操作时，备用 vSSL 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。

### 运维简便

vSSL 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 vSSL 部署蓝图后，可以快速、灵活、自动地部署 vSSL，从而简化了运营商操作维护管理。

易集成：vSSL 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。

### 丰富的安全功能

vSSL 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。



## 性能参数

为满足各种资源需求，vSSL 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

vSSL 各规格性能参数如下表所示：

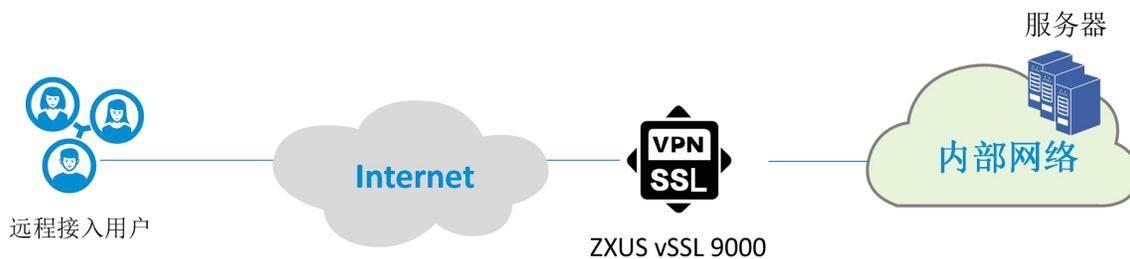
规格/类型	vCPU	内存(GB)	存储(GB)
C14	14	40	40
C8	8	32	40
C4	4	20	30



## 典型应用

远程接入用户采用标准的 SSL 协议对报文进行加密，与 ZXUS vSSL 9000 之间建立 TLS/DTLS 隧道，在隧道中传输加密后的报文。然后，ZXUS vSSL 9000 将远程接入用户的加密报文解密，再转发给指定的内部服务器，从而使得远程接入用户在通过验证后，可访问内网指定的服务器资源。

远程用户通过不同的路由，可以同时访问内部网络和公共网络。





5G 先锋



5G 先锋



深圳市科技南路 55 号中兴通讯大厦

邮编: 518057

Web: [www.zte.com](http://www.zte.com)

Tel: +86-755-26770000

Fax: +86-755-26771999

中兴通讯股份有限公司  
ZTE CORPORATION