
# ZXUS vCube 9000 虚拟综合安全网关

ZTE中兴

# ZXUS vCube 9000 虚拟综合安全网关

## 产品概述

随着虚拟化、云计算、SDN/NFV、大数据、物联网等新技术的发展，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。

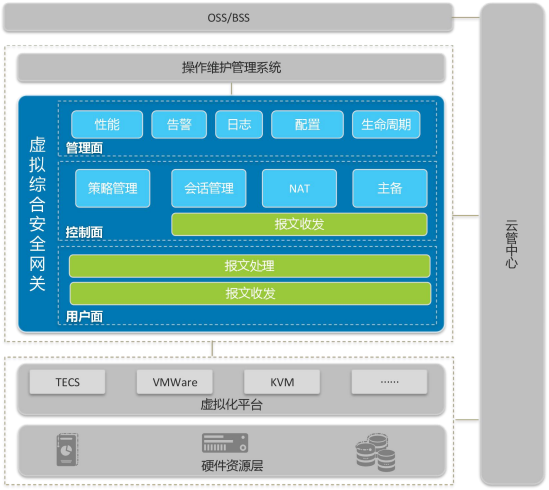
安全问题变得更加复杂，攻击的途径和手段更加多样化。一方面，传统的安全问题仍然存在，原有风险一个不少，如病毒、木马、勒索软件、DDOS 攻击、SQL 注入、僵尸网络、操作系统漏洞、应用程序漏洞、钓鱼软件等；另一方面，新技术本身带来了新的安全问题，且传统的安全设备与安全策略又难以适应新的网络环境和安全需求，引起了大量新的风险，如虚拟机逃逸、数据残留、流量不可见、流量混杂、边界模糊、SDN 控制器安全、接口安全、转发面攻击等。因此，为保证网络安全，中兴通讯推出虚拟综合安全网关 ZXUS vCube 9000，提供网络安全防护。虚拟综合安全网关能够部署在云计算/虚拟化网络环境中，为租户和运营商的网络通信进行安全防护，为云计算/虚拟化网络中的各种资源提供网络安全防护功能。

基于传统的安全架构，ZXUS vCube 9000 实现了综合安全网关的资源抽象化和池化技术，具有弹性扩展、按需自动部署等特点。ZXUS vCube 9000 虚拟综合安全网关可以广泛应用于保障核心网、企业网、VDC 等场景网络的安全。

ZTE中兴

# 系统架构

## 虚拟综合安全网关系统架构




### 虚拟化平台

基于虚机方式的 vCube 可运行于通用服务器上，为电信网络提供安全防护。vFW 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，vCube 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。

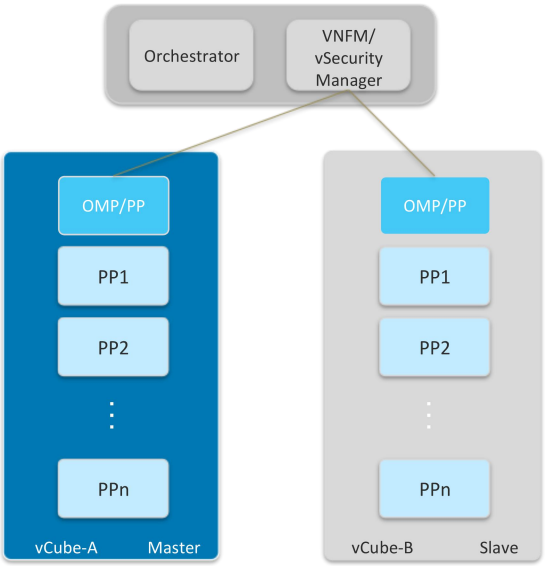
### 云管中心

云管中心中存在 vCube 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，vCube 组件与云管中心其他网元协同为 vCube 提供相应的管理，完成 vCube 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。

## 分布式系统部署




vCube 是分布式系统，由一个 OMP 和多个 PP 组成，OMP 和 PP 可以部署在同一台虚机上，也可以部署在不同虚机上。

ZTE中兴

vCube 支持单虚机或多虚机部署，且支持双机热备模式。

OMP 是 vCube 的主处理器（Operating Main Processor），即管理单元，可以管理所有的 PP 单元。当 vCube 进行弹缩时，OMP 不受影响。

PP 是 vCube 处理器单元（Peripheral Processor unit），执行报文检测、处理、控制和防护等。当用户数量或吞吐量变化时，PP 可以根据弹性策略进行弹缩。

# 产品特色

## 高性能/低时延

vCube 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

vCube 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

vCube 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

vCube 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

vCube 采用改进的 VRRP 协议实现热备份功能。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 vCube 的单元（PP）不能正常启动或操作时，备用 vCube 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。

为了保证系统的可靠性，避免数据阻塞，vCube 通过多 HA 通道进行数据同步和备份。

## 运维简便

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

弹性伸缩：为了简化部署和管理，提升资源利用率，vCube 实现了用户自定义 Scale In/Out 弹性策略，以虚机为粒度进行伸缩。

易集成：vCube 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。

ZTE中兴

## 丰富的安全功能

vCube 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。

支持多种 VPN 功能，包括 IPsec VPN 和 SSL VPN。

# 性能参数

为满足各种资源需求，vCube 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

vCube 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 |

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