Leading 5G Innovations

ZXUS vCube 9000

ZTE

ZXUS vCube 9000

Overview

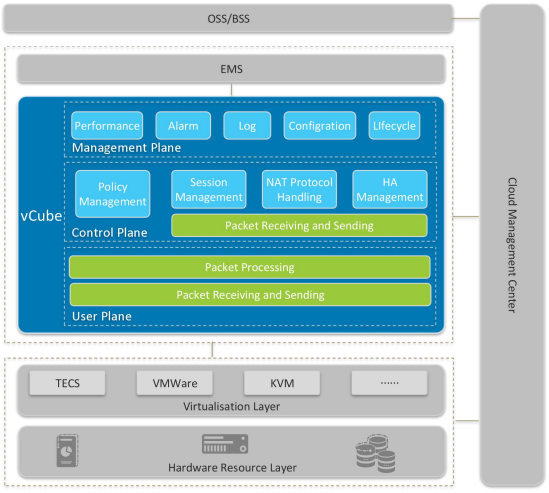
With the development of new technologies such as virtualization, cloud computing, SDN/NFV, big data, IoT, etc., traditional data centers and networks have undergone great changes. Traditional security devices are difficult to apply on the cloud platform. For example, traditional security devices do not have the features of automatic deployment and dynamic elasticity required for virtualization, and it is also difficult to meet the dynamic creation and on-demand allocation of multi-tenancy.

Security issues have become more complex, and the ways and means of attack have become more diverse. On the one hand, traditional security issues still exist, and the original risks are many, such as viruses, Trojans, ransomware, DDOS attacks, SQL injection, botnets, operating system vulnerabilities, application vulnerabilities, phishing software and so on.On the other hand, the new technology brings new security problems, and the traditional security devices and security policies are difficult to adapt to the new network environment and security requirements, causing a lot of new risks, such as virtual machine escaping, data residual, traffic invisible, traffic Hybrid, border blur, SDN controller security, interface security, forwarding surface attacks, etc. Therefore, in order to ensure network security, ZTE launched the virtual integrated security gateway ZXUS vCube 9000 to provide network security protection. ZXUS vCube 9000 can be deployed in a cloud computing or virtualized network environment to provide security protection for tenant and carrier network communication, and provide network security protection for various resources in the cloud computing or virtualized network.

Based on the traditional security architecture, ZXUS vCube 9000 enables integrated security gateway abstraction and the pooling technology. Featuring elastic expanding and automatic on-demand deployment, ZXUS vCube 9000 can be extensively used to protect core networks, medium and large private clouds, VDC，etc.

System Architecture

Overview



Virtual Platform

The VM-based vCube runs on universal servers to protect telecom networks. Adaptive to multiple virtual platforms including TECS, VMware, KVM and so on, it is not reliant on any private hardware, and allows decoupled hardware and software.

Software architecture

To perform efficient data forwarding and make the system more reliable and secure, the vCube is designed with a separate management plane, control plane and user plane. The management plane implements management of performance, alarms, logs, configurations and life cycle. The control plane takes responsibility for protocol processing and generation of policy information. The user plane performs packet filtering, packet conversion, packet processing and packet forwarding as per static configuration or dynamic policy information.

The isolation is performed in the following ways:

Isolation of network planes: The network is split into a control plane network, management plane network and user plane network.

Isolation of processes/threads: All the processes of the control plane, management plane and user plane are independent. The threads on the user plane are bound to vCPU cores.

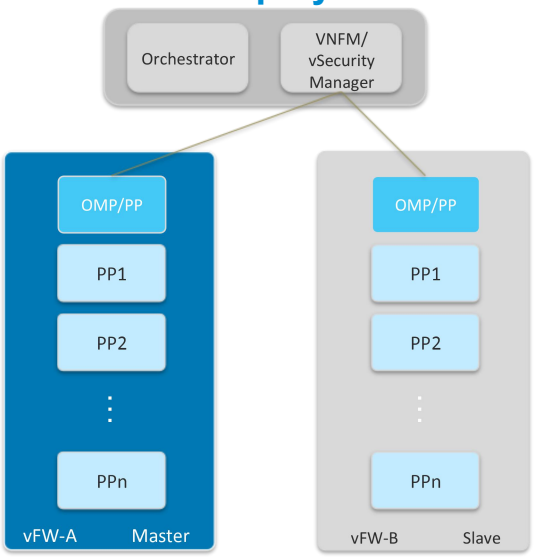
Cloud management center

vCube components locate at the cloud management center. During the virtual network orchestration and operation, the vCube components as per different security protection scenarios work together with other network element at the cloud management center to provide related management services and make vCube life cycle management proceed.

Operation maintenance and management System

As a universal operation maintenance and management system, the EMS enables the virtual security device to provide operation maintenance services and visualized display of alarms, performance and logs.

Distributed Deployment



Designed with a distributed system, the vCube is composed by one Operating Main Processor (OMP) and multiple Peripheral Processor units (PP). The OMP and PP can be deployed on the same VM or the different VMs. The vCube supports either single-VM or multi-VM deployment and dual-host hot redundancy mode.

As the main processor of the vCube, the OMP manages all the PP units. vCube scale-in/out does not impact the OMP a little.

The PP of the vCube is responsible for the inspection, processing, control and protection of the messages. When the user quantity or throughput changes, the PP can scale out or scale in according to the elastic policies.

Features

High Performance/Low Latency

The vCube employs many technologies including SR-IOV, DPDK and separated control and forwarding to improve performance and reduce latency.

- SR-IOV

By using the SR-IOV technology to share one PCI device with multiple VMs, the vCube enhances the utilization rate of I/O devices and shortens the network latency. The SR-IOV can work on GE/10GE/40GE interfaces.

- DPDK

The vCube employs the DPDK technology to enable more powerful system processing. Using multi-alignment hardware directly, the DPDK accesses the hardware resources via polling in user mode, which improves the network I/O throughput capability. Sorting hardware into different classifications effectively saves CPU resources. Using Hardware queues for processing messages can prevent obstacles caused by software distribution threads.

- Separated control and forwarding

The vCube uses different paths to separate control plane services (for example, protocol processing and dynamic generation of policy information) and user plane services (for instance data packet filtering, forwarding and processing), making data forwarding more efficient.

High Reliability

The vCube employs the enhanced VRRP protocol running on the HA path between the active and standby OMPs to ensure the virtual integrated security gateway capable of working in the hot redundant mode. When the system is running, the active and standby OMPs negotiate their working mode according to the received VRRP messages. When any of the active vCube unit (PP) breaks down, the standby vCube unit will take over its work automatically.As the HA path is an independent neutron network, it does not affect service networks.

To keep the system reliable and away from data blocking, the vCube implements data synchronization and backup via multiple HA paths.

Easy operation and maintenance

Automatic Deployment: The vCube can be deployed on a universal server automatically. When maintenance engineers finish making the vCube deployment blueprint, the entire

deployment can be done rapidly, flexibly and automatically, which obviously makes the O&M much easier.

Elastic Scale-In/Out: To enable simplified deployment and management, as well as more efficient resource utilization, the vCube enables user-defined Scale-In/Out policies.

Easy to Integrate: The vCube can be easily integrated to different security protection scenarios. Related cloud management centers are responsible for the orchestration and management.

Rich Security Services

In addition to detect and control multiple sorts of protocol messages, the vCube can also provide rich precaution services, for instance, the ACL-based packet filtering, status inspection, ASPF, inter-zone policies, DDoS, DPI and carrier-grade security protection.

Support a variety of VPN features, including IPsec VPN and SSL VPN.

Specifications

To satisfy the requirements of diversified resources, the vCube can be deployed with varying specs.

- C4 and C8: Keep the network safe while satisfying operators/enterprise users' some resource restrictions.
- C14: Keep the network safe while satisfying operators/enterprise users' high-performance requirements.

The performance of the vCubes in different specs are as shown in the following table.

Specs/Types	vCPU	Memory(GB)	Storage (GB)
C14	14	40	40
C8	8	32	40
C4	4	20	30

Leading 5G Innovations

NO. 55, Hi-tech Road South, ShenZhen, P. R. China

Postcode: 518057

Web: www.zte.com.cn

Tel: +86-755-26770000

Fax: +86-755-26771999

ZTE CORPORATION