Leading 5G Innovations

ZXSG SVFW-Z virtual FireWall

ZTE

ZXSG SVFW-Z virtual FireWall

Overview

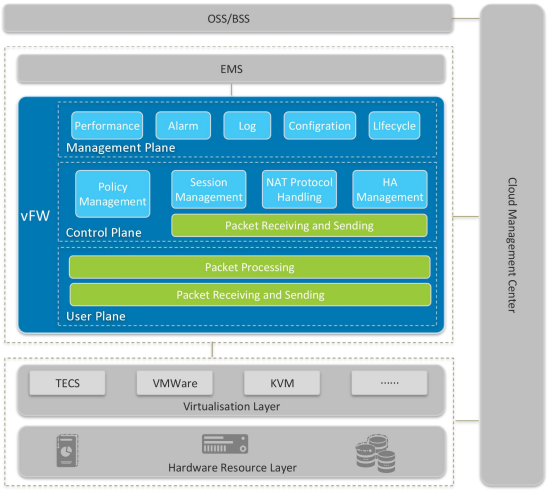
Rapid development of cloud computing and virtualization technologies tremendously change both data centers and networks. So besides old safety threats, customers today have to face lots of new security issues and challenges. In a cloud environment, different tenants ' virtual resources can be deployed on the same physical asset, which makes malicious users easy to attack the network via shared resources. Applications like mobile business and BYOD make it possible for terminals at internet to access the resources of the enterprise intranet. The blurring boundary between intranet and internet not only brings customers conveniences to process regular business, but also leaves more opportunities for attacks. Problems such as virtual migration and virtual escape urge for new security policies. At the same time, as today ' s booming new services are more strongly tied up with safety requirements, security issues become more vital and more complicated. Instead of being a simple precaution, the security capability shall be treated as an important service. Security service suppliers need to provide users and applications with opener and more flexible interfaces,as well as individualized security protection.

Traditional security devices incapable of performing automatic deployment and dynamic scale-in/out required by virtualization can hardly comply with massive requirements generated by new services, for instance, dynamic user creation, on-demand distribution, new identification methods for new services and new protection ways. Therefore, to process safe cloud computing and build reliable virtual networks, virtual firewalls (vFW) deployed on a cloud computing/virtual network for safe network communications now becomes a crucial security measure making the network and all sorts of resources safe and reliable.

Based on traditional security architecture, ZXSG SVFW-S enables firewall abstraction and the pooling technology. Featuring elastic expanding and automatic on-demand deployment, ZXSG SVFW-S (vFW) can be extensively used to protect core networks, medium and large private clouds, and NBIoT networks.

System Architecture

Overview



Virtual Platform

The VM-based vFW 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 vFW 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.

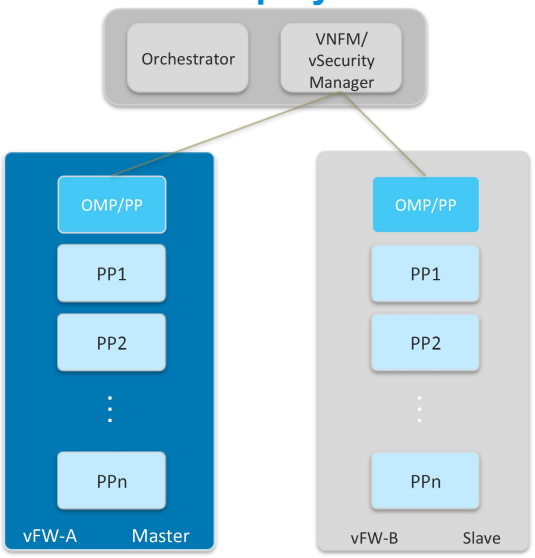
Cloud management center

vFW components locate at the cloud management center. During the virtual network orchestration and operation, the vFW 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 vFW 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 vFW 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 vFW supports either single-VM or multi-VM deployment and dual-host hot redundancy mode.

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

The PP of the vFW 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 vFW 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 vFW 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 vFW 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 vFW 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 vFW employs the enhanced VRRP protocol running on the HA path between the active and standby OMPs to ensure the firewall 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 vFW unit (PP) breaks down, the standby vFW 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 vFW implements data synchronization and backup via multiple HA paths.

Easy operation and maintenance

Automatic Deployment: The vFW can be deployed on a universal server automatically. When maintenance engineers finish making the vFW 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 vFW enables user-defined Scale-In/Out policies.

Easy to Integrate: The vFW 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 vFW 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.

Specifications

To satisfy the requirements of diversified resources, the vFW 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.

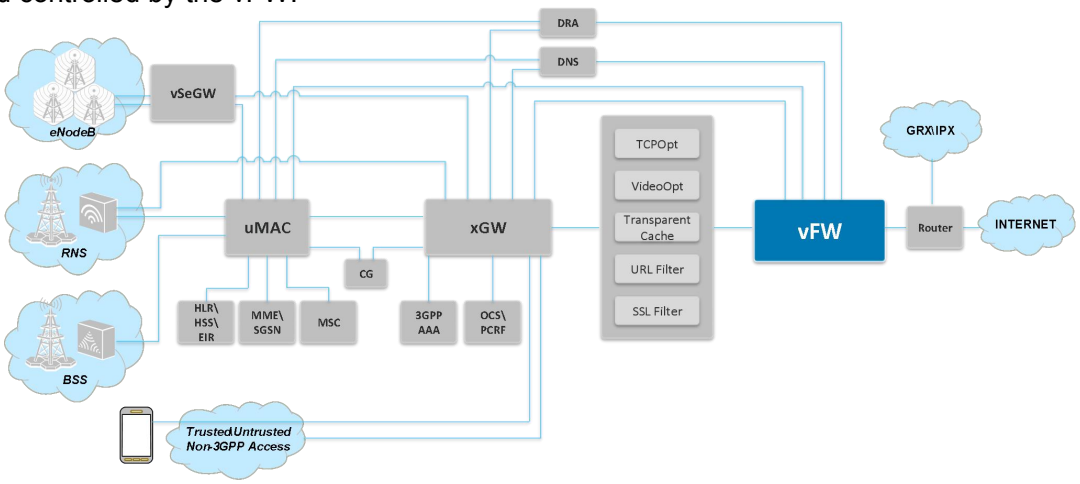
The performance of the vFWs in different specs are as shown in the following table.

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

Application Scenarios

Core Networks

Locating between the xGW and Internet, the vFW protects the Gi and SGi interfaces, which prevents core network GGSN and PGW from Internet attacks. At the same time, the vFW can also be deployed between the xGW and GRX/IPX networks to make the Gp/S8 safe. Under this circumstance, it helps the core network stay away from roaming threats. All the upstream and downstream messages of the Gi/SGi and Gp/S8 ports shall be inspected and controlled by the vFW.



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