ZXUS vSSL 9000

ZTE

ZXUS vSSL 9000

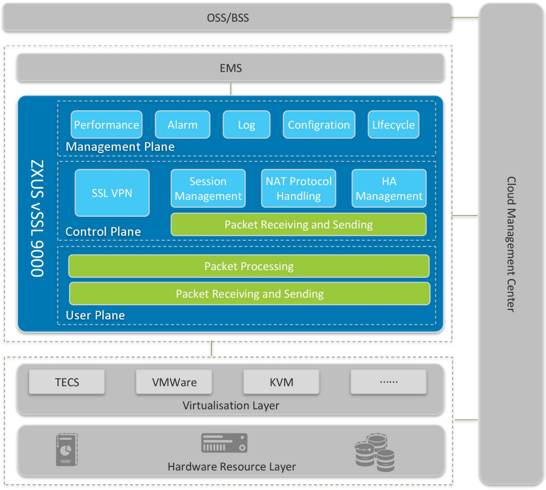
Overview

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.

In a large enterprise scenario, partners, customers and business travelers require access to corporate intranet resources through the public network anywhere and anytime. In this scenario, SSL VPN emerges as the times require and provides a new remote access solution that effectively solves the above-mentioned problems.

Based on traditional security architecture, ZXUS vSSL 9000 enables security traversing gateway abstraction and the pooling technology. ZXUS vSSL 9000 can be automatically deployed and lifecycle management, and supports integration with multiple cloud platforms, such as TECS, VMware, etc.

System Architecture



Virtual Platform

The VM-based vSSL 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 vSSL 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

vSSL components locate at the cloud management center. During the virtual network orchestration and operation, the vSSL 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 vSSL 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.

Features

High Performance/Low Latency

The vSSL 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 vSSL 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 vSSL 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 vSSL 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 vSSL 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 vSSL unit (PP) breaks down, the standby vSSL unit will take over its work automatically. As the HA path is an independent neutron network, it does not affect service networks.

Easy operation and maintenance

Automatic Deployment: The vSSL can be deployed on a universal server automatically. When maintenance engineers finish making the vSSL deployment blueprint, the entire deployment can be done rapidly, flexibly and automatically, which obviously makes the O&M much easier.

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

Rich Security Services

A rich defense functions, for instance, the ACL-based packet filtering, status inspection, ASPF, inter-zone policies, DDoS, DPI and carrier-grade security protection.

The vSSL can detect and control multiple protocol packets, support SSL VPN, and provide rich defense functions such as ACL packet filtering, state detection, ASPF, inter-domain policies and so on.

Specifications

To satisfy the requirements of diversified resources, the vSSL 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.

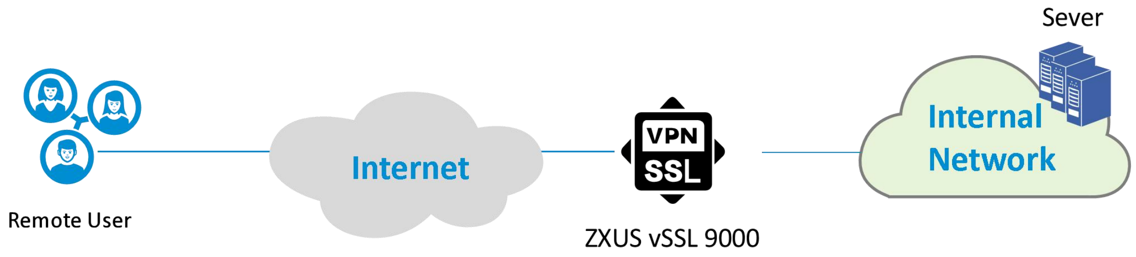
The performance of the vFWs in different specs are as shown in the following table.

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

Application Scenarios

The remote user encrypts the packet using the standard SSL protocol, establishes the TLS/DTLS tunnel with ZXUS vSSL 9000, and transmits the encrypted packet in the tunnel. Then, ZXUS vSSL 9000 decrypts the encrypted messages and forwards them to the specified internal server, so that the remote access user can access the specified server resources after passing the authentication.

Remote users can access both internal and public networks through different routes.



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