Leading 5G Innovations

ZXUS vSeGW 9000 virtual Security Gateway

ZTE

ZXUS vSeGW 9000 virtual Security Gateway

Overview

In communication network system, IP packets exchanged between different networks or different sites of an operator or an enterprise are often transmitted through a third-party network. Because these transmission networks have the characteristics of being open and transparent, and the IP packets do not have any security features, when the packets are transmitted in the plaintext on the network, attackers use interception methods such as eavesdropping and camouflage to stealing and tampering data in order to obtain illegal benefits. It will cause huge losses for individual users, business users, and operators. At the same time, malicious users can also attack the operator or the enterprise's network by the third-party transmission network, causing a lot of security problems such as excessive occupation of internal network resources, leakage of key information, etc. It can be seen that the traditional IP layer protocol cannot ensure the security of IP packet transmission. The insecure transmission network may easily lead to data leakage or tampering. The internal network may also be subjected to malicious attacks, which will bring great security risks to both users and operators. For example, when a user accesses a core network through a base station, the operator usually uses a public network or a leased network as the backhaul network to connect the wireless network and the core network. When plaintext transmitted voice data and media data through an untrusted backhaul network. The data may be maliciously falsified and illegally stolen, and the privacy and integrity of the transmitted data cannot be effectively secured. At the same time, the core network of the operator also faces various network attacks and security threats.

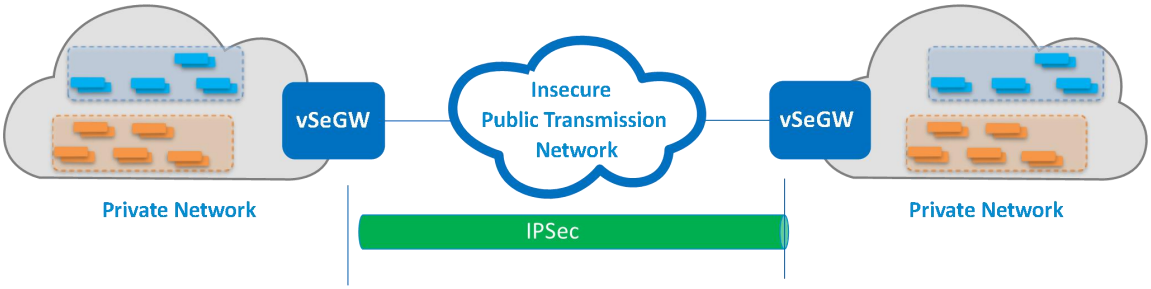
Considering the various security issues, providing security services at the IP layer has become one of the most demanding requirements in communication network systems. Then IPSec has emerged. IPSec provides security services such as data integrity, data source identity authentication, anti-replay attack, and confidentiality of data content for IP and upper layer protocols. It is the standard for implementing VPN at the network layer. IPSec defines a system to provide security protocol selection, security algorithms, key determination and other services to provide security at the IP layer. IPSec consists of three parts: AH protocol, ESP protocol, and IKE protocol. AH provides authentication, integrity, and anti-replay services for data sources. ESP provides AH and data privacy.

With the rapid development of mobile communication networks, IoT, 5G..., data traffic, and user scale are increasing. Operators have become more and more demanding for network equipment expansion flexibility, rapid deployment, management automation, and resource dynamic adjustment. Traditional communication network systems cannot adapt to increasingly flexible and convenient network and service deployment. Traditional

communication networks are gradually shifting to virtualized networks, software and virtualization of network functions will become inevitable.

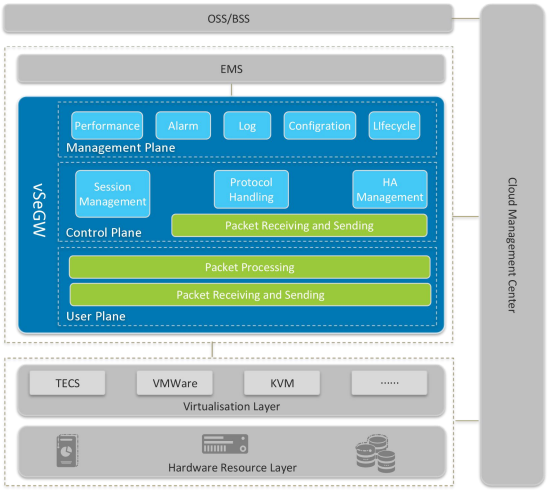
ZTE's ZXUS vSeGW 9000 uses the IPSec VPN technology to exchange information with the peer NEs to establish and manage an IPSec tunnel in order to provide secure connections for IP packets. The data is encrypted and transmitted in the secure tunnel. Even if the data is illegally eavesdropped and acquired, the information cannot be known. At the same time, the secure tunnel supports data integrity protection and effectively prevents data from being corrupted or tampered with. The network element of the tunnel communication will perform identity verification to prevent the attacker from pretending to be a legitimate user to attack the user equipment or the carrier infrastructure. The ZXUS vSeGW 9000 solves the problems of fixed resource occupation and high operation and maintenance costs of traditional physical devices, greatly improving the utilization of basic resources, allocating resources on demand, deploying services flexibly, and reducing operating costs, so that operator can rapidly develop new services, attract and expand the user group.

The ZXUS vSeGW 9000 is a carrier-class security gateway. It is usually deployed at the boundary of the network and cooperates with the peer node to implement security functions. It can provide mobile operators with secure and scalable mobile solutions, including wireless access, monitoring networks, IGW networks and other security solutions to ensure data security between the network and the network, between the office and the office. Provide information privacy and network resource protection for individual users, enterprise users and operators.



System Architecture

Overview



Virtual Platform

The VM-based vSeGW 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 vSeGW 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.

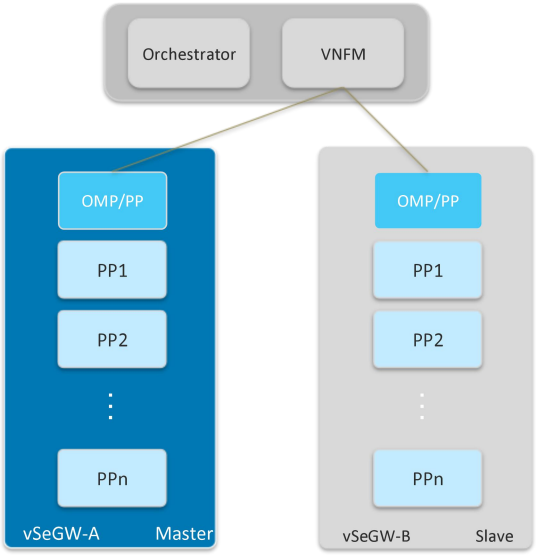
Cloud management center

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

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

The PP of the vSeGW is responsible for message detection, encryption and decryption, control, etc. When the number of SAs or throughput changes, the PP can scale out or scale in according to the elastic policies.

Features

Perfect access security

The vSeGW supports multiple authentication modes and algorithms to meet the encryption and authentication requirements in different scenarios.

- Support multiple authentication methods

To achieve high security, the vSeGW supports the peer NE authentication mechanism. An IPSec tunnel can be established only for legitimate devices that pass the authentication. vSeGW provides multiple authentication methods, including source address authentication, certificate authentication, dual authentication, EAP-AKA authentication, and PSK-based authentication.

- Support multi-standard cryptographic algorithms

Support multi-standard encryption/decryption algorithms, integrity algorithms, pseudo-random functions and DH Groups, including DES, Triple-DES, AES-CBC, HMAC-SHA-1, HMAC-MD5, HMAC-SHA-2, AES-XCBC-PRF, DH Group 1, DH Group 2, DH Group 5 and DH Group 14, etc. The high-security algorithms, such as DH Group 14 and SHA2-512, provide the better processing performance while providing the better service protection.

High Performance/Low Latency

The vSeGW employs many technologies including SR-IOV, DPDK, separated control and forwarding, AES NI and QAT sub-card to improve performance and reduce latency.

- SR-IOV

By using the SR-IOV technology to share one PCI device with multiple VMs, the vSeGW 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.

- AES NI

Employs the AES NI technology to use the underlying hardware in order to reduce CPU cycles and improve AES encryption/decryption performance.

AES NI is an instruction set extension on Intel's x86 processor introduced in March 2008, which includes seven new instructions. AES NI can utilize the underlying hardware when performing complex compute-intensive AES algorithms to reduce CPU cycles and improve AES encryption and decryption performance.

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.

Specifications

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

- C4: Keep the network safe while satisfying the IPSec requirements of small traffic.
- 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.

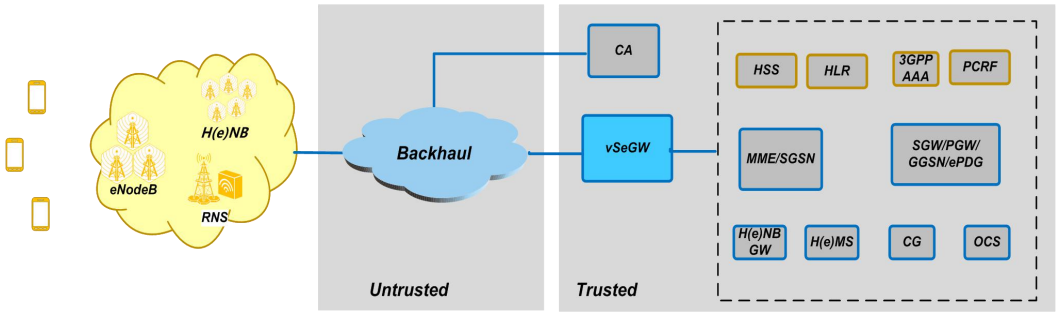
The performance of the vSeGWs in different specs are as shown in the following table.

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

Application Scenarios

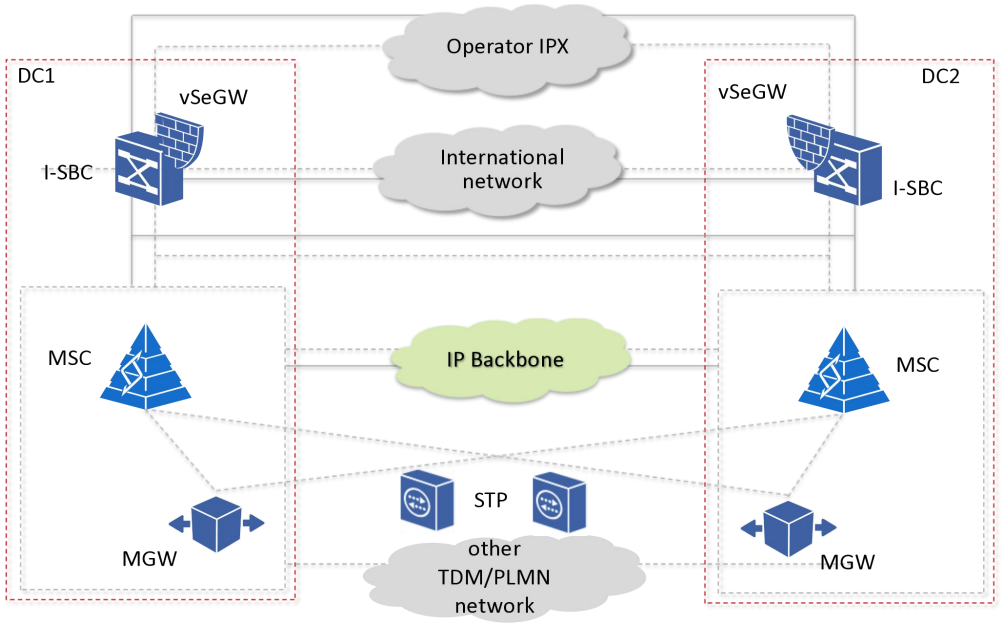
Core Networks Application Scenario

In the scenario of core network, vSeGW is deployed on the carrier's core network boundary, and the IPSec tunnel is established and managed through mutual authentication with the base station. The security tunnel provides security for control plane signaling and user plane data transmission between the wireless side and the core network, thereby ensuring secure access from the base station to the core network, providing IPSec tunnel management functions between different security domains, and implementing encryption and integrity protection for untrusted backhaul network data.



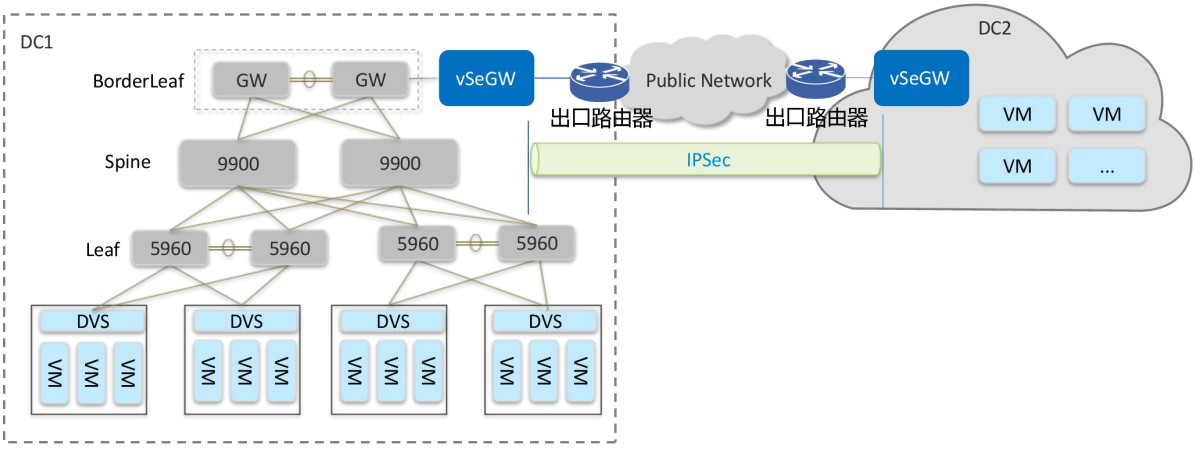
IGW Application Scenario

In the IGW scenario, vSeGW is deployed at the edge of the data center to perform mutual authentication, key agreement, session establishment, etc. It performs IPSec tunnel encryption protection on the SIP signaling traffic exchanged between the I-SBCs, and provides data security in the untrusted transmission network.



VDC Application Scenario

As a brand-new data center melting cloud computing theories into traditional data centers, virtual Data Center (vDC) employs virtualization technologies to abstract physical resources. Via dynamic resource distribution and scheduling, it enables automatic deployment of the data center and greatly reduces the CAPEX. By converting all the hardware (including servers, storage and networks) into logical resources, the vDC not only improves resource utilization rate and flexibility, but also uplifts the availability and measurability of the application software.



The vSeGW is deployed on the edge of the VDC to provide secure tunnel establishment and management, and illegal access protection to protect the traffic transmitted between VDCs from leakage and illegal interception when passing through the public network. It

implements secure transmission of enterprise data and secure VPN access for employees/partners.

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