ZXUS vSeGW 9000 虚拟安全网关

ZTE中兴

ZXUS vSeGW 9000 虚拟安全网关

产品概述

在通信网络系统中，运营商或企业的网络或局点之间交互的 IP 报文常常会通过第三方网络进行传送。由于这些传输网络具有公开、透明的特点，且 IP 报文本身不具备任何安全特性，因此，报文在网络中进行明文传输时，攻击者为了获取非法的利益，采用诸如窃听、伪装等攻击方式来截获数据，从而窃取、篡改报文内容，使得个人用户、企业用户以及运营商遭受巨大损失。同时，恶意用户也可以借助第三方传输网络对运营商或企业自身的网络进行攻击，引起内部网络资源过度占用、关键信息泄密等安全问题。由此可见，传统 IP 层协议无法确保 IP 报文的传输安全，传输网络的不安全性容易导致数据泄露或篡改，内部网络亦可能遭受到恶意攻击，给用户和运营商均带来极大的安全隐患。例如，在用户通过基站接入核心网的情况下，运营商通常使用公共互联网或租用网络作为回程网络连接无线网和移动核心网，当明文传送的语音数据和媒体数据经过不授信的回程网络时，可能导致数据被恶意篡改、非法窃取，传输数据的私密性和完整性无法得到有效的安全保障，同时，运营商的移动核心网也面临着各种各样的网络攻击和安全威胁。

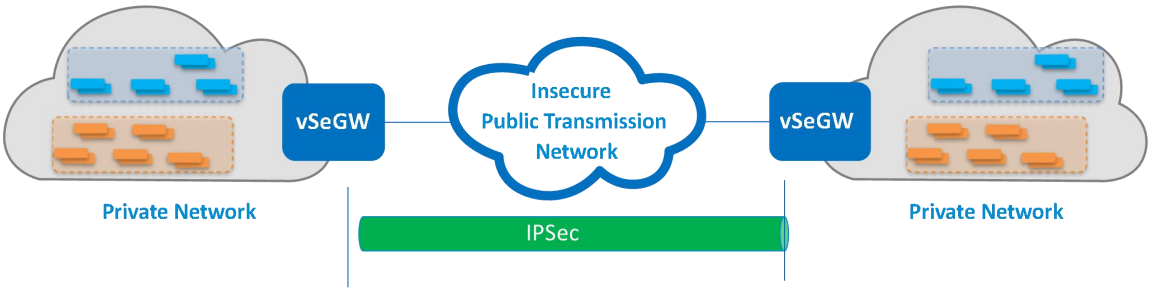
考虑上述提及的种种安全问题，在 IP 层上提供安全服务已成为通信网络系统中亟不可待的需求之一，IPSec 技术应运而生。IPSec 由 IETF 组织发布的系列协议组成，为 IP 及上层协议提供了数据完整性、数据源身份认证、抗重放攻击、数据内容的机密性等安全服务，是目前网络层实现 VPN 的标准 。IPSec 定义了一套系统来提供安全协议选择、安全算法、密钥确定等服务，在 IP 层提供安全保障。IPSec 由 AH 协议、ESP 协议、IKE 协议三部分组成。AH 能提供数据源的认证、完整性、及抗重放服务。ESP 提供了 AH 功能和数据保密性。

随着移动通信网络、物联网、5G 等技术的迅速发展和应用，网络业务数量、数据流量和用户规模不断增加，运营商对网络设备的扩展灵活性、业务快速部署、管理自动化、资源动态调整等需求愈发强烈，传统的通信网络系统无法适应、满足愈加灵活便捷的网络和业务部署，国内外传统通信网络正逐步向虚拟化网络发生转变，网络功能的软件化、虚拟化将成为必然。

中兴通讯安全网关的虚拟化形态也应运而生。ZXUS vSeGW 9000 采用 IPSec VPN 技术与对端网元进行信息交互，建立和管理 IPSec 隧道，为 IP 报文提供安全连接，经过该连接的数据将得以加密，即便数据被非法窃听、获取，也无法获悉信息的具体含义；同时，该安全隧道支持对数据的完整性保护，有效防止数据被破坏或篡改。此外，隧道通信双方网元将进行身份验证，尽可能避免攻击者伪装成合法用户去攻击用户设备或运营商基础设施等。ZXUS vSeGW 9000 解决了传统物理设备固定资源占用、运维成本高等缺陷，大幅提升了基础资源的利用率，为运营商提供按需分配资源、灵活部署业务、降低成本等优势，从而使其快速发展新业务，吸引并扩大用户群。

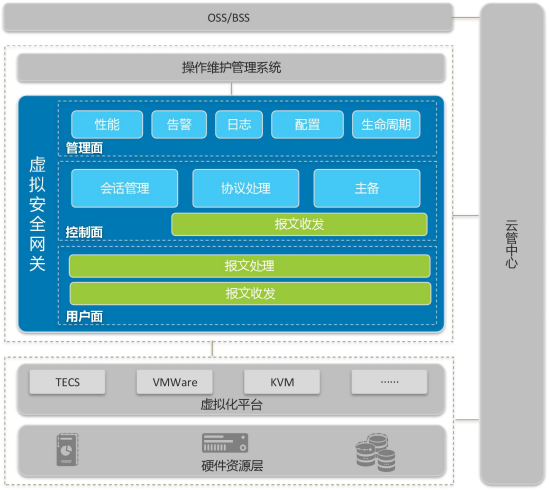
ZXUS vSeGW 9000 是电信级安全网关，通常部署在网络的边界，与对端节点协作实现安全相关的功能，从而为移动运营商提供安全的、可扩展的移动解决方案，包括无线接入、监听

网络、IGW 网络等安全解决方案，以确保网络与网络之间、局点与局点之间的通信数据在不授信网络中实现安全传递，为个人用户、企业用户和运营商提供信息隐私和网络资源保护。



系统架构

虚拟安全网关系统架构



虚拟化平台

基于虚机方式的 vSeGW 可运行于通用服务器上，为电信网络提供安全防护。vSeGW 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，vSeGW 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、会话管理、HA 管理等操作；用户面根据策略信息进行报文过滤、根据会话信息进行报文加解密等报文处理、报文转发流程。

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。

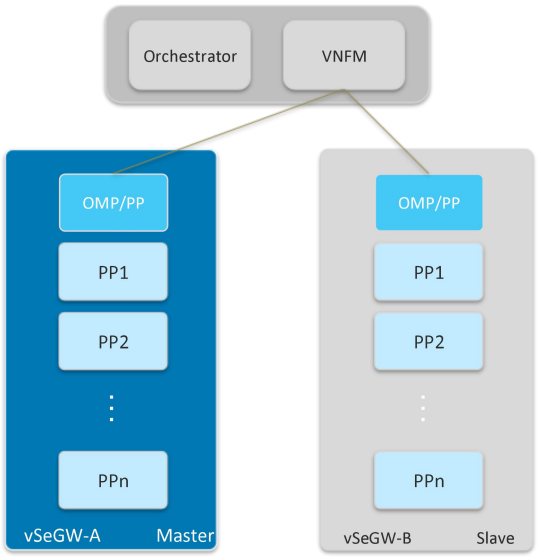
云管中心

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



ZTE中兴

vSeGW 是分布式系统，由一个 OMP 和多个 PP 组成。vSeGW 支持单虚机或多虚机部署，且支持双机热备模式。

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

PP 是 vSeGW 处理器单元（Peripheral Processor unit），执行报文检测、加解密、控制等处理。当 SA 数量或吞吐量变化时，PP 可以根据策略进行弹缩。

产品特色

完善的接入安全

vSeGW 支持多种认证方式和算法，满足不同场景下的加密、认证需求。

- 支持多种认证方式

为了实现高安全性能，vSeGW 支持对端网元认证机制。只有认证通过的合法设备才能建立 IPSec 隧道。vSeGW 提供了多种认证方式，包括源地址认证、证书认证、双重认证、基于 EAP-AKA 的认证、基于 PSK 的认证等。

- 支持多种安全算法

vSeGW 支持多种标准的加解密算法、完整性算法、伪随机函数和 DH Group，包括 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 和 DH Group 14 等。其中的一些高安全算法（如，DH Group 14 和 SHA2-512）在为用户提供更好的业务保护的同时，仍然具有良好的处理性能。

高性能/低时延

vSeGW 采用 SR-IOV、DPDK、控制转发分离、AES NI、QAT 加解密子卡等技术来提升处理性能、降低报文处理和传输延迟。

- SR-IOV

vSeGW 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，减少了网络延迟。SR-IOV 可以工作在 GE/10GE/40GE 接口上。

- DPDK

vSeGW 采用 DPDK 技术来提升系统处理性能。DPDK 直接使用硬件多队列，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，对硬件进行分类有效节省 CPU 资源，使用硬件队列直接收发报文可以避免软件分发线程造成的瓶颈。

- 控制转发分离

vSeGW 通过采用不同的通道分离控制面功能（如，协议处理、HA 管理等）和用户面功能（如，数据报文的加解密、过滤、转发等），提升数据转发效率。

- AES NI

vSeGW 支持 AES NI 技术。该技术是 Intel 在 2008 年 3 月推出的 x86 处理器上的指令集扩展，包含了 7 个新的指令。AES NI 在执行复杂的计算密集型 AES 算法时能较好地利用底层硬件，以便减少 CPU 周期、提高 AES 加密和解密性能。

高可靠性

vSeGW 采用改进的 VRRP 协议实现防火墙热备份功能。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 vSeGW 的单元（PP）不能正常启动或操作时，备用 vSeGW 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，vSeGW 通过多 HA 通道进行数据同步和备份。

快速部署

自动部署：vSeGW 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 vSeGW 部署蓝图后，可以快速、灵活、自动地部署 vSeGW，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，vSeGW 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：vSeGW 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。

性能参数

为满足各种资源需求，vSeGW 支持多种规格部署。

- C4 规格，满足小流量的 IPSec 需求
- C8 规格，满足运营商/企业用户一定资源约束条件下的网络安全需求
- C14 规格，满足运营商/企业用户高性能网络安全需求

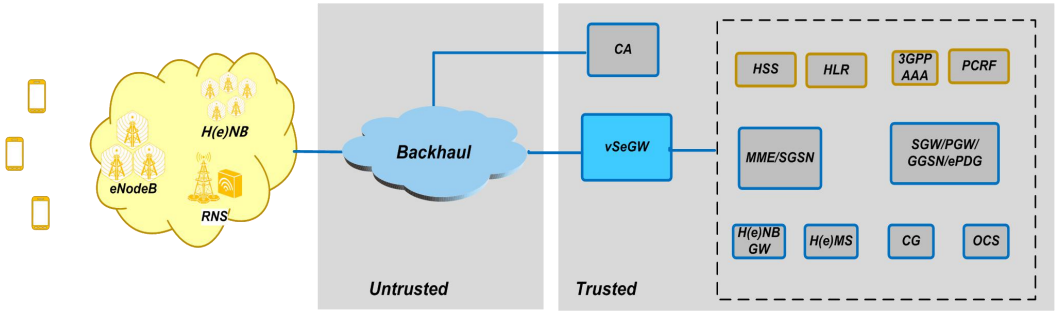
vSeGW 各规格性能参数如下表所示：

规格/类型	vCPU	内存(GB)	存储(GB)
C14	14	20	40
C8	8	16	30
C4	4	10	30

典型应用

移动核心网应用

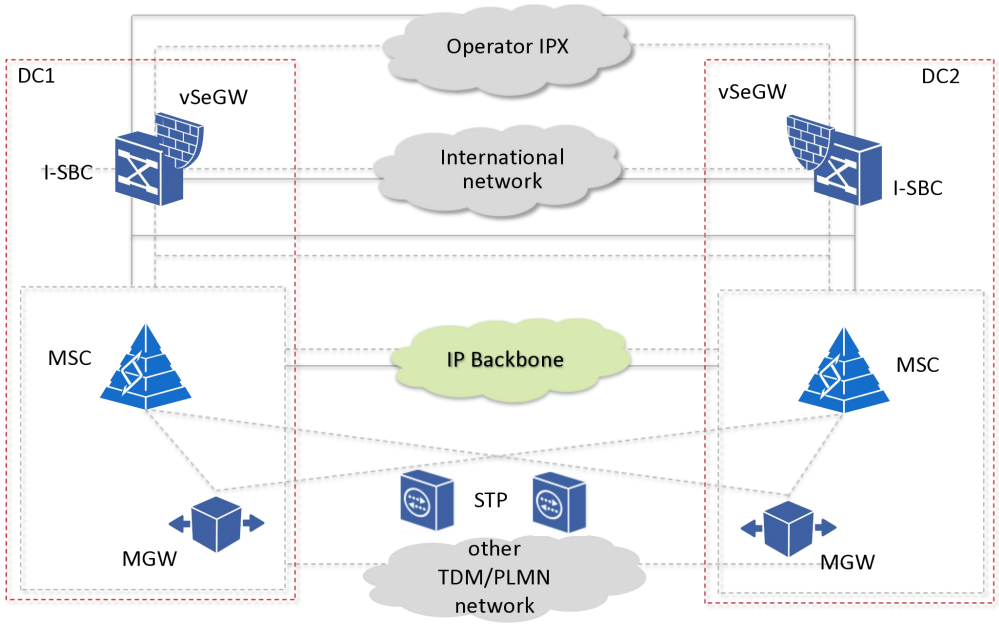
在移动核心网的应用场景中，vSeGW 部署在运营商核心网络边界，与基站之间通过双向认证后建立并管理 IPSec 隧道。通过该安全隧道，为无线侧与核心网之间控制面信令、用户面数据的传输提供安全保障，从而保证基站到核心网的安全接入，为不同安全域之间提供 IPSec 隧道管理功能，实现经过非授信回程网络数据的加密和完整性保护。



IGW 应用

在 IGW 应用场景中，vSeGW 位于数据中心边缘，进行彼此认证、密钥协商、会话建立等，对 I-SBC 之间交互的 SIP 信令流量进行 IPSec 隧道加密保护，在不授信传输网络中提供安全保障。

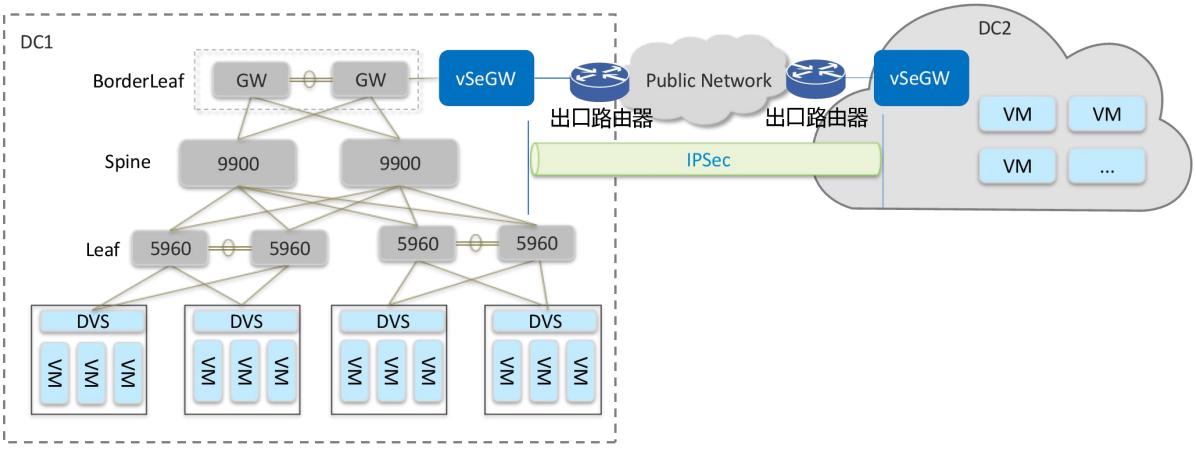
ZTE中兴



VDC 应用场景

VDC（Virtual Data Center，虚拟数据中心）是将云计算概念运用于数据中心的一种新型的数据中心形态，通过虚拟化技术将物理资源抽象整合，进行动态的资源分配和调度，实现数据中心的自动化部署，大大降低了数据中心的运营成本。VDC 将所有硬件（包括服务器、存储器和网络）整合成逻辑资源，从而提高资源的使用率和灵活性，以及提升应用软件的可用性和可测量。

vSeGW 部署于 VDC 边缘，提供安全隧道建立和管理、非法接入防护，使 VDC 之间传输的流量在经过公网时免受泄露和非法截获，实现企业数据的安全传送、员工/合作伙伴的 VPN 安全接入。



ZTE中兴

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