5G 先锋

ZXSG SVFW-S 虚拟防火墙

ZTE中兴

ZXSG SVFW-S 虚拟防火墙

产品概述

随着云计算、虚拟化技术的快速发展，数据中心和网络都发生了巨大的改变，不但传统安全威胁依然存在，还引入了新的安全问题和挑战。云环境下，不同租户的虚拟资源可以部署在相同的物理资源上，引出了租户间的安全隔离和共享、资源的按需分配等问题，增加了恶意用户借助共享资源实施攻击的途径；移动办公、BYOD 等应用使得处于企业外网的终端需要访问企业内网资源，从而突破了内外网隔离的边界，同时数据中心内部的大量交互，导致网络边界更加模糊，这些因素使得攻击的途径和手段更加多样化；虚机迁移、虚机逃逸等问题需要新的安全策略进行应对。同时，新业务的飞速发展，使得安全与业务需要紧密结合，安全问题变得更为复杂，安全能力需要开放，安全也变成了一种服务，而不仅仅是防范工具。安全厂家需要提供更为开放、灵活的接口，为用户和应用提供定制化安全防护。

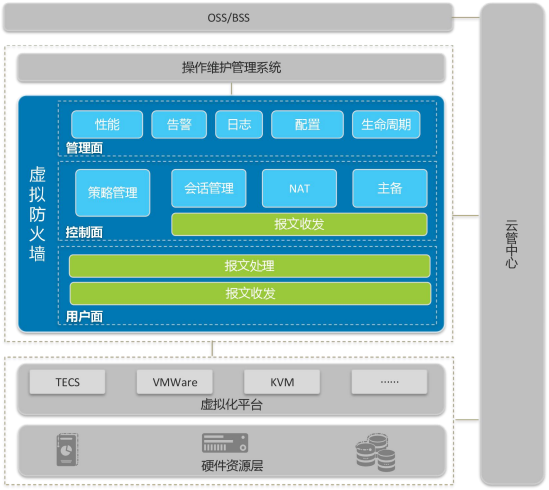
传统的安全设备不具备虚拟化所需的自动部署、动态弹性等特性，难以满足用户动态创建、按需分配等需求，也很难应对新业务所需要的新识别方式、新防护手段的挑战。所以传统的安全设备与安全策略难以适应新的网络环境和安全需求，很难在云平台上应用。因此，为保证云计算/虚拟化网络的安全，虚拟防火墙成为提供网络安全防护的重要安全设备。虚拟防火墙能够部署在云计算/虚拟化网络环境中，为租户和运营商的网络通信进行安全防护，为云计算/虚拟化网络中的各种资源提供网络安全防护功能。

基于传统的安全架构，ZXSG SVFW-S 实现了防火墙资源抽象化和池化技术，具有弹性扩展、按需自动部署等特点。ZXSG SVFW-S 虚拟防火墙（vFW，virtual Firewall）可以广泛应用于保障核心网、中大型私有云和 NBIoT 等场景网络的安全。

ZTE中兴

系统架构

虚拟防火墙系统架构



虚拟化平台

基于虚机方式的 vFW 可运行于通用服务器上，为电信网络提供安全防护。vFW 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。

防火墙软件架构

为提高数据转发效率、增强系统可靠性和安全性，vFW 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和策略信息的动态生成；用户面根据静态配置，或动态生成的策略信息进行报文过滤、转换、处理、转发等流程。

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。

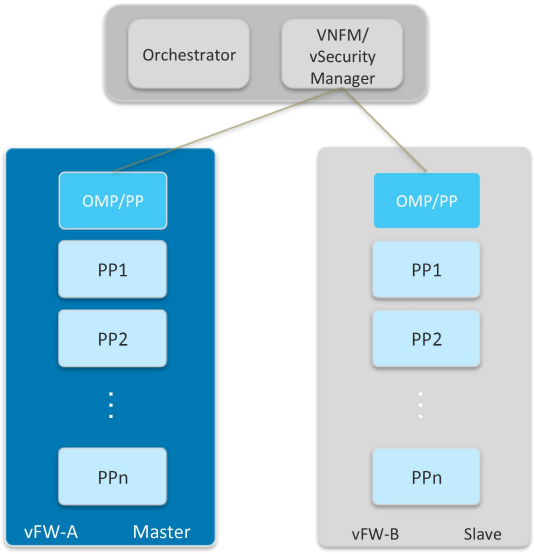
云管中心

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



vFW 是分布式系统，由一个 OMP 和多个 PP 组成，OMP 和 PP 可以部署在同一台虚机上，也可以部署在不同虚机上。

ZTE中兴

vFW 支持单虚机或多虚机部署，且支持双机热备模式。

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

PP 是 vFW 处理器单元（Peripheral Processor unit），执行报文检测、处理、控制和防护等。当用户数量或吞吐量变化时，PP 可以根据弹性策略进行弹缩。

产品特色

高性能/低时延

vFW 采用多种技术来提升性能、降低时延，如 SR-IOV、DPDK、控制转发分离等。

- SR-IOV

vFW 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，降低了网络延迟。SR-IOV 可以工作在 GE/10GE/40GE 接口上。

- DPDK

vFW 采用 DPDK 技术来提升系统处理性能。DPDK 使用硬件多队列直接收发报文，有效地避免了软件分发线程造成的瓶颈，同时，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，对硬件进行分类可以有效节省 CPU 资源。

- 控制转发分离

vFW 通过采用不同的通道分离控制面功能（如协议处理、策略信息的动态生成）和用户面功能（如数据报文的过滤、转发、处理），以提升数据转发效率。

高可靠性

vFW 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 vFW 的单元（PP）不能正常启动或操作时，备用 vFW 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，vFW 通过多 HA 通道进行数据同步和备份。

快速部署

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

丰富的安全功能

vFW 可以检测、控制多种协议报文，并提供丰富的防御功能，如基于 ACL 包过滤、状态检测、ASPF、域间策略、DDoS、DPI、电信级安全防护等。

性能参数

为满足各种资源需求，vFW 支持多种规格部署。

- C4、C8 规格，满足运营商/政企用户一定资源约束条件下的网络安全保护
- C14 规格，满足运营商/政企用户高性能网络安全保护需要

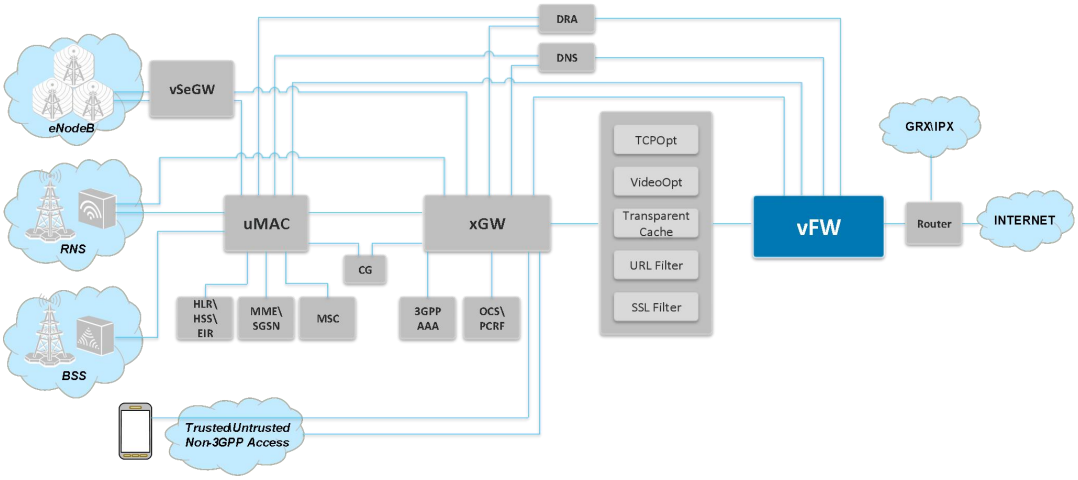
vFW 各规格性能参数如下表所示：

规格/类型	vCPU	内存(GB)	存储(GB)
C14	14	40	40
C8	8	32	40
C4	4	20	30

典型应用

核心网应用场景

vFW 位于 xGW 和 Internet 之间，保护 Gi 和 SGi 口安全——保障核心网 GGSN、PGW 等基础设施免受来自 Internet 的威胁。同时，vFW 也可以部署于 xGW 和 GRX/IPX 网络之间用以保护 Gp/S8 口安全——保障核心网免受漫游地威胁。Gi/SGi 口和 Gp/S8 口上下行数据报文均需经过 vFW 进行检测和控制。



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