华岳泰 OPNsense 防火墙技术服务-使用指南

【OPNsense 简介】：

防火墙是保护网络安全的重要屏障，有效监控网络间进出的各种数据包，能最大限度阻止黑客入侵被保护网络。本服务提供 OPNsense 防火墙免费镜像并在华为云上部署与运维。OPNsense 是一个开源、多功能、高可靠与易使用的企业级防火墙，具有 FW/NAT/路由/VPN/IPS 功能，提供商业防火墙中的大部分功能，具有状态检测防火墙、网络地址转换、路由、虚拟专用网络、入侵检测、报告与支持插件的特征。

【OPNsense 主要功能】：

1) **仪表盘**：能够监测防火墙的硬件信息，包括 CPU 利用率、内存利用率、SWAP 利用率、磁盘利用率，软件版本信息与状态表大小情况，能够监测服务状态、接口与网关信息等，支持部件管理与拖放；

2) **报告监测**：能够进行系统、网络包与流量的检查，能够进行流量分析，能够捕获与缓存网络流，并以 RRD 图形显示；

3) **防火墙**：OPNsense 是状态防火墙，跟踪网络连接的状态(TCP 流或 UDP 通信)，提供按类别分组的防火墙规则；

4) **NAT**：能够有效实现内网与外网的 IP 地址转换，避免内部网络被攻击；

5) **路由**：支持静态路由与策略路由；

6) **VPN**：包括 IPSec 与 OpenVPN，支持网关间与远程接入的 VPN 连接，OpenVPN 基于 OpenSSL(SSLv3/TLSv1)，具有简单易用的优点；

7) **IPS**：基于 Suricata 快速、深度检测网络数据包内容，Suricata 是一款开源高性能网络入侵检测和监控引擎，支持多线程，并利用 Netmap 提高性能与减低 CPU 使用。IPS 具有实时、主动拦截黑客攻击、木马、蠕虫、后门与网络病毒等功能，可以极大程度上减少网络威胁入侵，有效阻挡大多数网络安全攻击。最近几年，IPS 越来越受欢迎，目前大多数大型组织都全面部署了 IPS。

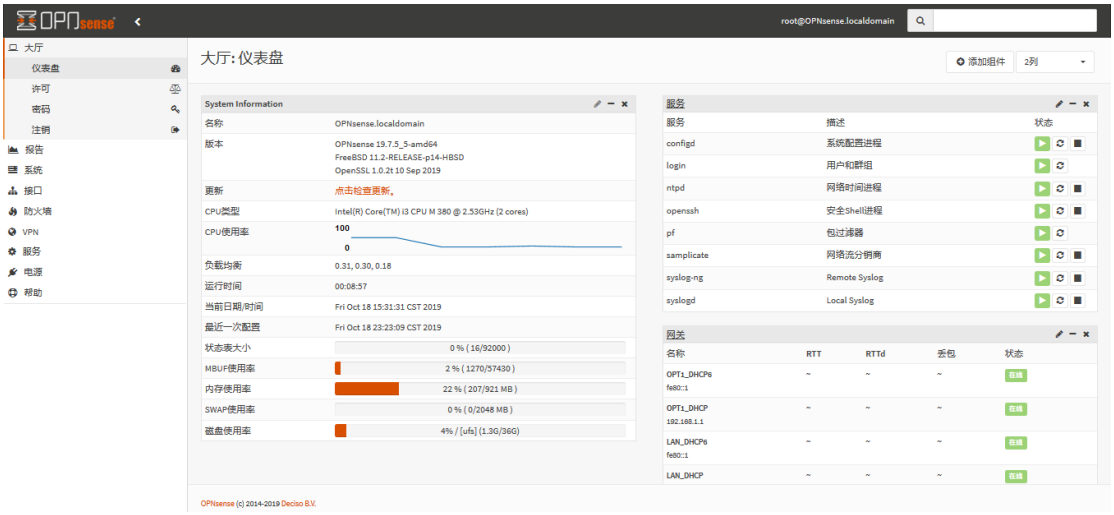
【OPNsense 使用方法】：

在华为云上购买云主机并部署 OPNsense 后，需要开放 443 端口，可以通过浏览器登录云主机。

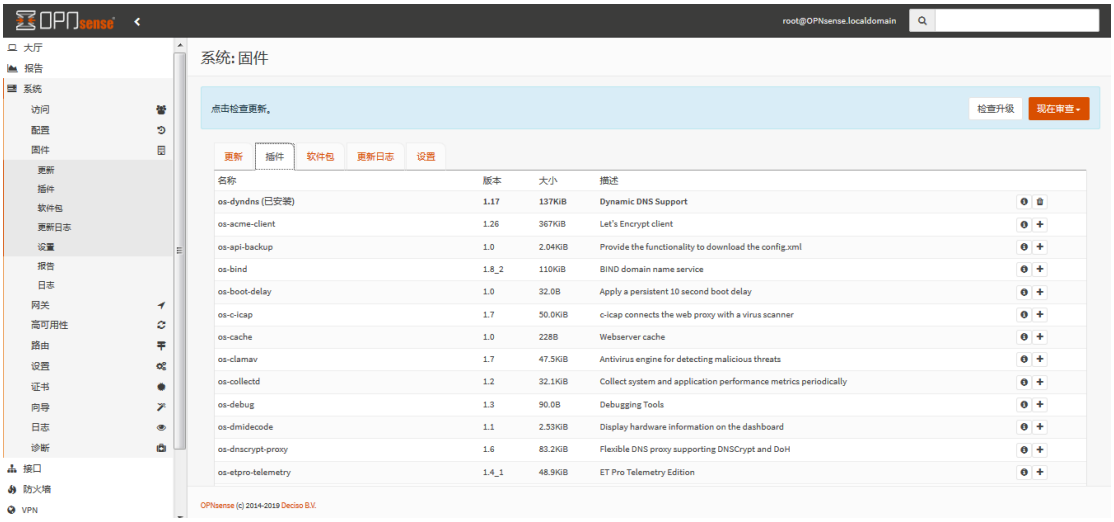
OPNsense 页面导航栏包括大厅、报告、系统、接口、防火墙、VPN、服务、电源与帮助。其中，大厅包括仪表盘、许可、密码与注销；报告包括健康检查、流量分析、网络流、设置与流量图表；系统包括访问、配置、固件、网关、可用性、路由、设置、证书、向导、日志与诊断；接口包括 LAN、WAN、分配、概况、设置与诊断等；防火墙包括规则、NAT、流控、组、虚拟 IP、设置、日志与诊断等；VPN 包括 IPSec、OpenVPN；服务主要包括各

服务进程的描述与状态。

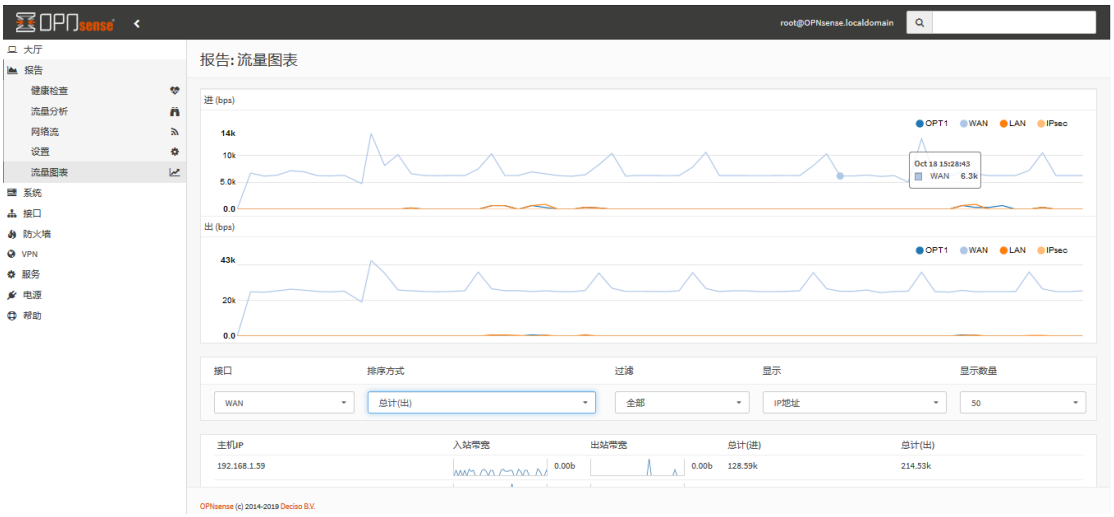
仪表盘页面使用： 在导航栏点击“大厅”->“仪表盘”，查看硬件信息，包括 CPU 利用率、内存利用率、SWAP 利用率、磁盘利用率；查看软件版本信息与状态表大小情况；查看服务状态、接口与网关信息；点击部件右上角笔形按钮进行部件元素编辑与拖放。如下图所示。



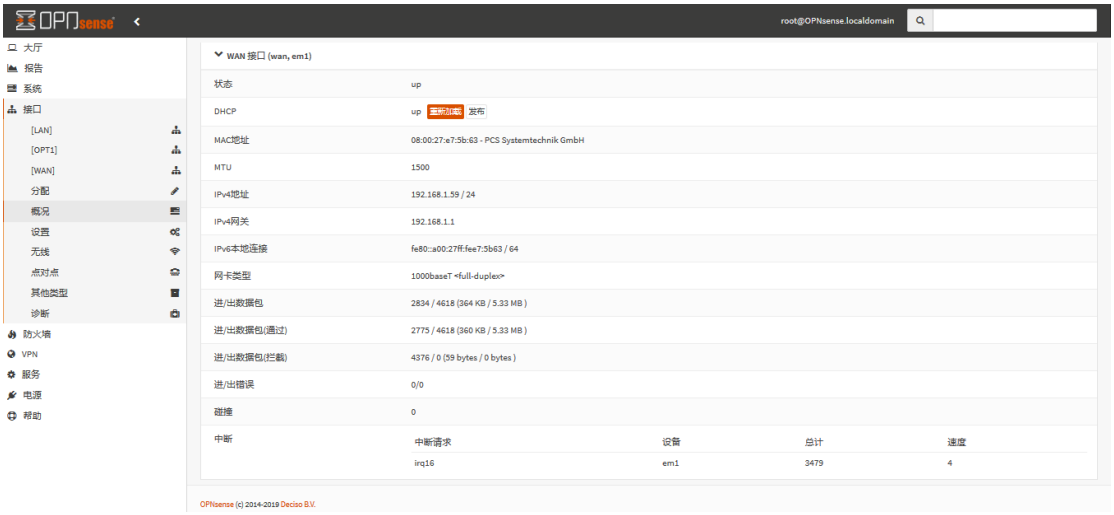
系统固件页面使用： 在导航栏点击“系统”->“固件”，查看更新、插件、软件包、更新日志与设置。如下图所示。



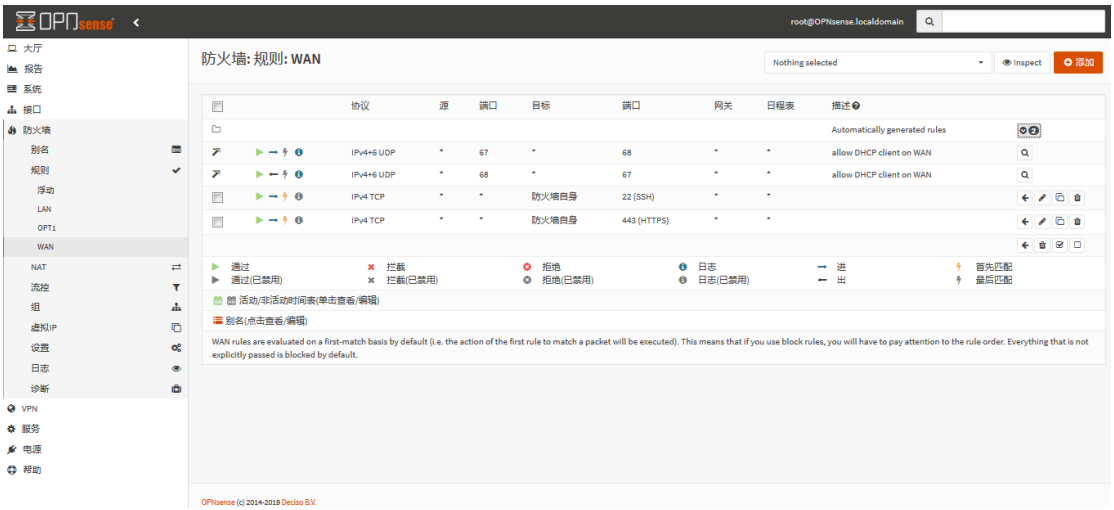
流量图表页面使用： 在导航栏点击“报告”->“流量图表”，查看每个主机与接口的流量大小，进行流量分析。如下图所示。



接口概况页面使用： 在导航栏点击“接口”->“概况”，查看接口状态、DHCP、MAC 地址、MTU、IPv4 地址、IPv4 网关、IPv6 本地连接、网卡类型、进/出数据包。如下图所示。



防火墙 WAN 规则页面使用： 在导航栏点击“防火墙”->“规则”->“WAN”，查看 WAN 的规则列表，列表信息包括协议、源 IP、源端口、目的 IP、目的端口、网关、日程表与描述信息。并进行添加、编辑、删除操作。如下图所示。



VPN 的 OpenVPN 服务器页面使用： 在导航栏点击“VPN”->“OpenVPN”->“服务

器”，查看与设置 OpenVPN 服务器，包括是否禁用、服务器模式、认证后端、强制本地组、协议、设备模式、接口、本地端口、加密设置、TLS 认证。如下图所示。