## 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

ZOPOsense <						root@OPNsense.l	ocaldomain	۹		
2 大厅		十日・心主舟								
仪表盘	B							0 78	和加强1年 2月	
许可	<u>4</u> 2				an da					
密码	٩	System Information		/ - ×	設定				404	/-
注销	۲	谷标	OPNsense.localdomain		88,95	伸达			大法	2
报告		版本	OPNsense 19.7.5_5-amd64 FreeBSD 11.2-RELEASE-p14-HBSD		configd	363708	は白田程			0
系统			OpenSSL 1.0.2t 10 Sep 2019		login	用户和	口群组			0
接口		更新	点击检查更新。		ntpd	网络时	时间进程			€ ∎
防火墙		CPU类型	Intel(R) Core(TM) I3 CPU M 380 @ 2.53GHz (2 cores)		openssh	安全s	ihell进程			0
VPN		CPU使用率	100		pf	包过滤	<b>\$</b> 8			0
服务			0		samplicate	网络派	充分销商			0
电源		负载均衡	0.31, 0.30, 0.18		syslog-ng	Remo	te Syslog			
帮助		运行时间	00:08:57							
		当前日期/时间	Fri Oct 18 15:31:31 CST 2019		systoga	Local	Systog			
		最近一次配置	Fri Oct 18 23:23:09 CST 2019		网关					1-
		状态表大小	0 % (16/92000)		名称	RTT	RTTd	丢包	状态	
		MBUF使用率	2 % (1270/57430)		OPT1_DHCP6	~	~	~	在线	
		内存使用率	22 % ( 207/921 MB )		fe80::1				_	
		SWAP使用率	0 % ( 0/2048 MB )		OPT1_DHCP	~	~	~	在战	
		磁盘使用率	4% / [ufs] (1.3G/36G)		192.168.1.1					
					LAN_DHCP6 fe80::1	~	~	~	在线	
					LAN_DHCP	~	~	~	在线	

**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。

	<									root@OPNsense.localdomain			
旦 大厅		<u> </u>	之际 田	<i>II</i> +									
▶ 报告		-	秋切: <u></u> 四1十										
■ 系统													
访问	쓭		点击检查更新,										
配置	9												
固件			更新	插件	软件包	更新日志	设置						
更新			名称					版本	±/h	描述			
括件			as durida	(日安準)				1.17	127Kip	Dynamic DNS Support			
软件包			US-Gynan	a (Luscae)				1.00	2071/00	Let's France beta Support			
更新日志			os-acme-o	cuent .				1.20	307610	Let's Encrypt client	0 +		
役置		E	os-api-bao	ckup				1.0	2.04KiB	Provide the functionality to download the config.xml	0 +		
秋告 ロー			os-bind					1.8_2	110KiB	BIND domain name service	0 +		
			os-boot-d	lelay				1.0	32.0B	Apply a persistent 10 second boot delay	0 +		
网天	1		os-c-icap					1.7	50.0KIB	c-icap connects the web proxy with a virus scanner	0 +		
同り用性	-		os-cache					1.0	2288	Webserver cache	0 +		
治量	*		os-clamav	v				1.7	47.5KiB	Antivirus engine for detecting malicious threats	0 +		
证书			os-collect	d				1.2	32.1KiB	Collect system and application performance metrics periodically	0 +		
向导	7		os-debug					1.3	90.0B	Debugging Tools	0 +		
日志	۲		os-dmide	code				1.1	2.53KiB	Display hardware information on the dashboard	0 +		
诊断	ß		os-dnscry	pt-proxy				1.6	83.2KiB	Flexible DNS proxy supporting DNSCrypt and DoH	0 +		
▲ 接口			os-etpro-t	telemetry				1.4_1	48.9KiB	ET Pro Telemetry Edition	0 +		
<b>約</b> 防火墙													
Ø VPN			OPNsense (c) 201	14-2019 Deci	so B.V.								

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。

ZOPO <mark>sense'</mark> <				roc	ot@OPNsense.localdomain						
旦 大厅		❤ WAN 接□ (wan, em1)									
■ 180 ■ 系统		状态	up								
▲ 接□		DHCP	up <mark>重疏加或</mark> 发布								
[LAN]	# #	MAC地址	08:00:27:e7:5b:63 - PCS Systemtechnik GmbH								
[WAN]	 #	мти	1500								
分配	/	IPv4地址	192.168.1.59 / 24								
概况	E	IPv4网关	192.168.1.1								
无线	Ŷ	IPv6本地连接	fe80:::a00:27ff;fee7:5b63 / 64								
点对点	۲	网卡类型	1000baseT «full-duplex»								
其他类型	8	进/出数据包	2834 / 4618 (364 KB / 5.33 MB )								
分 防火墙		进/出数据包(通过)	2775 / 4618 (360 KB / 5.33 MB )								
VPN		进/出数据包(拦截)	4376 / 0 (59 bytes / 0 bytes )								
✿ 服务		进/出错误	0/0								
♥ 帮助		碰撞	0								
		中断	中斷请求	设备	总计	速度					
			irq16	emi	3479	4					

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。

₩ OPN <mark>sense'</mark> <											root@	OPNsense.localdomain	۹				
旦 大厅	RÈ		±000.000														_
▶ 报告	P/_	」人间:	⊼光火J: ₩F	AIN							Nothing se	elected		•	Inspec	4	> 添加
■ 系统																	
▲ 接口					协议	源	端口	目标	茜口	网关	日程表	描述☺					
<b>幼</b> 防火墙	1	6										Automatically generated	d rules		00		
别名 🚍	•	7	► → ½ 0		IPv4+6 UDP	•	67		68	•	•	allow DHCP client on W	AN		Q		
規則 🗸	· .	7	► + 4 0		IPv4+6 UDP	•	68	•	67	•	•	allow DHCP client on W	AN		Q		
浮动			► → † 0		IPv4 TCP	•	•	防火墙自身	22 (SSH)	•	•				4	/ 6	1
LAN			► → † 0		IPv4 TCP		•	防火墙自身	443 (HTTPS)	•	•				4	/ 6	1
WAN															4	• •	
NAT ≓		▶ <u>通</u> 过			× 拦截			拒绝	0	日志		→ 进		首先	582		
流控して	- 1	▶ 通过(i	巳禁用)		× 拦截(已禁)	用)		拒绝(已禁用)	0	日志(已禁用)		<b>+</b> ±	5	最后日	582		
组 晶		🗎 🏥 活动	加非活动时间	表(单击查和	香/编辑)												
虚拟IP D	5	■ 别名(点	(击查看/编辑)	)													
设置 😪	e 1	WAN rules a	are evaluated	on a first-m	atch basis by default	(i.e. the ac	tion of the fi	st rule to match a packet	t will be executed). Th	his means that if yo	u use block ru	lles, you will have to pay atter	ntion to th	e rule ord	er. Everythi	ng that i	is not
日志 💿	•	explicitly pa	assed is block	ed by derau	at.												
诊断 🖸	5																
VPN																	
✿ 服务																	
🖋 电源																	
● 帮助																	
	OPI	Nsense (c) 20	14-2019 Deciso E	B.V.													

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。

ZOPO <mark>sense</mark> <					root@OPNsense.localdomain Q	
旦 大厅		VPN: OpenVPN: 服务器				
▲ 报告						
■ 系统		常规信息.				完整帮助①
よ接口		6 葉用				
<b>约</b> 防火墙		● 描述				
O VPN						
OpenVPN	-	● 服务器模式	远程接入(用户认证)	•		
服务器 客户端		●认证后端	本地数据库	•		
客户编特定覆盖 客户编号出		●强制本地组	admins	•		
连接状态 日志		● 协议	UDP	•		
✿ 服务		0 设备模式	tun	•		
<ul> <li>帮助</li> </ul>		●接口	wan	*		
		❷ 本地講口	1194			
		加密设置				
		❸ TLS 认证	☑ 启用TLS 认证.			
		OPhicano (e) 2014 2010 Decise P.V				