**中神通UTMWALL-VM作为VNF与OpenStack 、SDN、NFV的关系说明**

* **本文链接: http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_as\_a\_VNF.docx**

●OpenStack是一个开源的云计算管理平台项目，由几个主要的组件组合起来完成具体工作。OpenStack支持几乎所有类型的云环境，项目目标是提供实施简单、可大规模扩展、丰富、标准统一的云计算管理平台。OpenStack通过各种互补的服务提供了基础设施即服务（IaaS）的解决方案，每个服务提供API以进行集成。Neutron模块提供云计算的网络虚拟化技术，为OpenStack其他服务提供网络连接服务。为用户提供接口，可以定义Network、Subnet、Router，配置DHCP、DNS、负载均衡、L3服务，网络支持GRE、VLAN。插件架构支持许多主流的网络厂家和技术，如OpenvSwitch。

●SDN，Software Defined Network，即软件定义的网络，是一种新型的网络体系结构，通过将网络控制与网络转发解耦合构建开放可编程的网络体系结构。狭义的SDN特指基于OpenFlow南向接口的网络，广义的SDN则是指具备这种理念的所有网络。

●NFV，Network Function Virtualization，即网络功能虚拟化，通过使用x86等通用性硬件以及虚拟化技术，来承载很多功能的软件处理，从而降低网络昂贵的设备成本。典型应用是一些CPU密集型功能，并且对网络吞吐量要求不高的情形。可以做网络功能虚拟化的设备有：WAN加速器，信令会话控制器，消息路由器，VPN，IDS，DPI，防火墙，CG-NAT，SGSN/GGSN，PE，BNG，RAN等。

●VNF，Virtualized Network Function，即虚拟化的网络功能，作为一个纯软件实现的网络功能，能够运行在NFVI之上，对应传统物理网络功能。从安装部署的角度来看，VNF是一个VM；从软件应用开发商的角度来看，VNF就是部署在一个或多个互联的VM中的软件实现。

●从ISO的协议栈来看，SDN针对的是下三层，而NFV就是针对之上的应用；NFV是针对网络中的功能点，SDN针对的是把功能点连接起来的通路；SDN针对数据传输，而NFV针对数据的处理。SDN和NFV是相辅相成的：只有实现了网络功能的极度虚拟化，才能保证SDN的水到渠成或者说让SDN轻装上阵，让网络功能在任何时间、任何地点、任何场景下都能被随心所欲地调度。

●中神通UTMWALL-VM虚拟云网关/虚拟化网络防火墙的产品形态是精简优化的硬件UTMWALL OS运行在虚拟机中进行网关、旁路或独立服务器式的连通和过滤 ，它作为VNF（Virtualized Network Function 虚拟化的网络功能）或vNSF（Virtualized Network Security Function 虚拟化的网络安全功能）为x86服务器的虚拟化铺路搭桥、保驾护航。它具备优化了的虚拟网卡等设备驱动，可以部署在OpenStatck、ESXi、Hyper-V、XenServer等专门的虚拟机云服务器系统中，为整个虚拟网络及每个租户提供全面而有区别的网络连接、安全防护及负载均衡服务。它的全部功能均有相应的WEB Services接口，方便第三方调用，实现SDN功能，它是您虚拟云网络中的第一台虚拟机，只需要2G硬盘、512M内存、1核CPU、不需要VLAN交换机支持就可以完美运行，而且网卡数量和南北东西向属性没有限制，支持多DMZ（micro-segmentation）及多租户架构，具备整机资源占用少、以APP方式进行功能扩展（Security as a Service/Software Define Security）、高安全性、高可靠性（HA集群）、低TCO、易管理的优良特性。

●中神通UTMWALL-VM作为VNF与OpenStack 、SDN、NFV的关系如图1所示：



图1 中神通UTMWALL-VM作为VNF与OpenStack 、SDN、NFV的关系示意图

●中神通UTMWALL的功能及流程（Service Function Chaining）图如图2所示：



图2中神通UTMWALL功能及流程（Service Function Chaining）图

●中神通UTMWALL-VM与OpenStack网络功能的对比详见表1所示：

|  |  |  |  |
| --- | --- | --- | --- |
| **项目** | **OpenStack 网络功能项** | **中神通UTMWALL v1.8功能项** | **页码** |
| **1** | **网络/虚拟交换机** | 3.1 nic网卡设置 | 67 |
| **2** | **网桥** | 3.4 bridge网桥设置 | 74 |
| **3** | **VLAN** | 3.3 vlanVLAN | 72 |
| **4** | **静态路由** | 3.6 route路由设置 | 78 |
| **5** | **DHCP服务** | 4.3 dhcpDHCP服务 | 86 |
| **6** | **IP&MAC地址绑定** | 4.1 ipmacARP服务 | 82 |
| **7** | **虚拟路由器之SNAT** | 5.6 natSNAT策略 | 103 |
| **8** | **虚拟路由器之浮动IP** | 5.6 natDNAT策略 | 103 |
| **9** | **安全组** | 5.7 firewall总控策略  | 105 |
| **10** | **QoS带宽控制** | 5.5 qos_objQoS对象 | 101 |
| **11** | **FWaaS 防火墙** | 5.7 firewall总控策略  | 105 |
| **12** | **LBaaS 负载均衡** | 5.6 natDNAT策略 + 健康检测 | 103 |
| **13** | **VPNaaS 虚拟局域网** | 10 IPSEC VPN9.1 pptp_vpnPPTP总体设置11.2 sslvpnSSLVPN总体设置 | 199191210 |
| **14** | **HA 双机热备** | 3.5 failover双机热备 | 76 |
| **15** | **CPU/内存/存储趋势图** | 1.3 system_status系统状态 | 21 |
| **16** | **吞吐量/会话数趋势图** | 1.4 network_status网络状态 | 23 |
| **17** | **网卡状态** | 1.5 nic网卡状态 | 25 |
| **18** | **流量统计** | 1.8 traffic_stat流量统计 | 31 |
| **19** | **ARP缓存状态** | 1.7 arp_statusARP状态 | 29 |
| **20** | **ping/traceroute/telnet调试** | 1.13 nettool测试工具 | 41 |
| **21** | **tcpdump抓包** | 1.12 realtime_monitor实时监控 | 39 |
| **22** | **NTP服务** | 2.5 systime本地时间 NTP服务 | 56 |
| **23** | **DNS代理服务** | 6.5 dnsfilterDNS代理过滤 | 117 |
| **24** | **DDNS服务** | 4.4 ddnsDDNS服务 | 88 |
| **25** | **Netflow探针** | 4.5 netflowNetflow探针 | 89 |
| **26** | **RIP/BGP/OSPF/MRoute** | 3.6 route路由设置 | 78 |
| **27** | **日志浏览/查询/统计/留存** | 1.14 log日志操作1.15 log_stat日志统计 | 4345 |
| **28** | **用户认证/用户门户** | 8.2 user用户8.3 usergroup用户组 | 181183 |
| **29** |  | 1.10 active_host在线主机 | 35 |
| **30** |  | 1.11 session_status会话状态 | 37 |
| **31** |  | 3.2 bonding链路聚合 | 70 |
| **32** |  | 3.5 failover双机热备 | 76 |
| **33** |  | 5.2 shedule_obj时间对象 | 95 |
| **34** |  | 5.3 traffic_obj流量对象 | 97 |
| **35** |  | 5.4 session_obj会话对象 | 99 |
| **36** |  | 6.1 specapp_basic特殊应用 | 109 |
| **37** |  | 6.3 netaudit网络审计 | 113 |
| **38** |  | 6.4 wafWEB审计过滤 WAF | 115 |
| **39** |  | 6.6 dns_url_dbDNS&URL库 | 119 |
| **40** |  | 6.7 domain_rules自定义域名规则 | 122 |
| **41** |  | 6.8 webproxyWEB代理过滤 | 124 |
| **42** |  | 6.10 webfilterWEB内容过滤 | 128 |
| **43** |  | 6.15 ftpfilterFTP代理过滤 | 138 |
| **44** |  | 6.16 telnetproxyTELNET代理 | 140 |
| **45** |  | 6.17 pop3filterPOP3代理过滤 | 142 |
| **46** |  | 6.18 smtpfilterSMTP代理过滤 | 144 |
| **47** |  | 6.19 qqQQ审计过滤 | 146 |
| **48** |  | 6.20 h323proxyVOIP | 147 |
| **49** |  | 6.24 antivirus防病毒引擎 | 155 |
| **50** |  | 6.26 antispam防垃圾邮件引擎 | 159 |
| **51** |  | 7.5 idp_rulesIDS/IPS特征值规则 | 170 |
| **52** |  | 7.8 honeypot蜜罐检测 | 176 |
| **53** |  | 11.1 sslSSL接入 | 208 |

表1中神通UTMWALL-VM与OpenStack网络功能的对比表

**结论**

在网络吞吐量可控、安全防护及合规审计要求高、原生功能又不能满足要求的NFV（Network Function Virtualization网络功能虚拟化）项目中——典型应用是租户网络、VPC（Virtual Private Cloud 虚拟私有云）、桌面云的边界接入网关，中神通UTMWALL-VM可以代替OpenStack内置的安全组、vRouter、FWaaS、VPNaaS、LBaaS、DNSaaS以及物理网络里的硬件防火墙、安全网关、负载均衡器（SLB）、应用交付器（ADC），并提供全面、安全、便捷、灵活的管理和服务。

**参考文件：**

1. OpenStack云计算平台管理员手册（2015年9月26日）

http://docs.ocselected.org/openstack-manuals/kilo/admin-guide-cloud/admin-guide-cloud.pdf

2. 中神通UTMWALL网关管理员手册
http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_v1.9\_Manual\_CN\_20150331.pdf

3. 中神通UTMWALL-VM在OpenStack环境里的安装手册

http://www.trustcomputing.com.cn/utmwall-rom/UTMWALL\_in\_OpenStack.docx

4. Network Functions Virtualization（NFV，网络功能虚拟化）介绍

http://t.51gocloud.com/?p=323

5. 切勿混淆 解读网络虚拟化、NFV与SDN

http://www.techweb.com.cn/network/virtual/2015-11-20/2229252.shtml