Trend Micro

VIRTUAL NETWORK FUNCTION SUITE

Flexible, reliable, and high-performance network security solution for carrier-class NFV

Network Function Virtualization (NFV) has become an inevitable trend since European Telecommunication Standards Institute (ETSI) introduced it in 2012. It is a new network architecture concept that uses IT virtualization technologies to decouple network functions, such as router, firewall, network address transition (NAT), and domain name service (DNS), from proprietary hardware appliances so that they can run as software on standard servers, switches, and storages. NFV aims to help communication service providers (CSPs) to not only reduce costs but also to enable faster and more flexible service delivery. According to a survey[1], 94 percent of the CSP operators had NFV strategy plans in place.

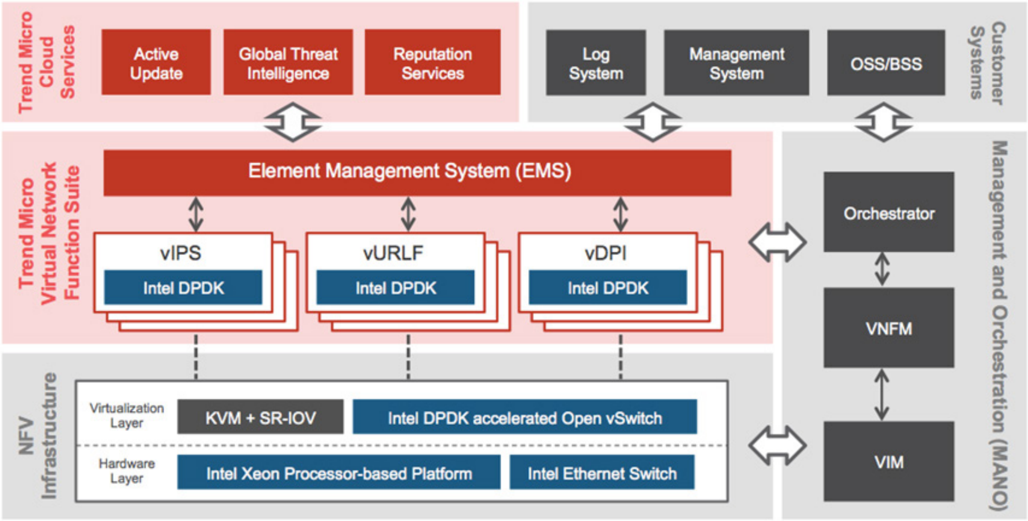
Trend Micro Virtual Network Function Suite is designed to offer flexible, reliable, and high-performance virtual network security functions for CSPs from premise, edge, to core network. The core of Virtual Network Function Suite is innovative deep packet inspection (DPI) technology, which provides various network security functions, including intrusion prevention, URL filtering, and application control, and has been widely adopted in a variety of network security products, from home routers to enterprise-facing next-generation firewalls and intrusion prevention systems.

By leveraging Intel® Data Plane Development Kit, Virtual Network Function Suite achieves tens of Gigabits per second in virtualization infrastructure, making it better fit for carrier-grade NFV environments. It can be deployed as virtual customer premise equipment (vCPE) or security protections for Gi-LAN.

ARCHITECTURE

Virtual Network Function Suite comprises two types of components: virtual network functions (VNFs) and element management system (EMS). The VNFs scan network traffic and performs desired inspection functions, such as intrusion detection and prevention, URL filtering, and application and device identifications. The EMS manages logs, updates, and policy configurations of multiple VNFs and integrates with the management and orchestration (MANO) systems to manage VNF life cycle.

Virtual Network Function Suite uses the global threat intelligence and reputation services from the Trend Micro™ Smart Protection Network™ infrastructure and provides immediate protections against the latest threats. Virtual Network Function Suite also provides friendly RESTful interfaces to easily integrate with third-party systems and provide complete end-to-end operation management to CSPs.


Trend Micro Cloud Services
Active Update
Global Threat Intelligence
Reputation Services
Log System
Management System
OSS/BSS
Customer Systems
Trend Micro Virtual Network Function Suite
Element Management System (EMS)
vIPS
Intel DPDK
vURLF
Intel DPDK
vDPI
Intel DPDK
Orchestrator
VNFM
VIM
Management and Orchestration (MANO)
NFV Infrastructure
Virtualization Layer
KVM + SR-IOV
Intel DPDK accelerated Open vSwitch
Hardware Layer
Intel Xeon Processor-based Platform
Intel Ethernet Switch

[1] - https://www.opnfv.org/news-faq/press-release/2016/06/survey-reveals-93-percent-network-operators-view-opnfv-important

COMPONENTS

Virtual Intrusion Prevention System (vIPS)

The vIPS is a VNF that scans incoming and outgoing packets in order to discover malicious exploit attacks in real time. The scanning checks only necessary parts of a network connection according to the signature rules to maximize packet-processing throughput, allowing for the examination of a large set of known exploits and malicious attacks in the shortest possible time. The core engine of vIPS is capable of normalizing packets from L3 to L7 to detect evasion techniques, such as HTML obfuscation and RPC fragmentation. The built-in zero-copy normalization technology enables high-speed packet normalization.

Virtual URL Filter (vURLF)

The vURLF is a VNF that identifies and blocks malicious or unwanted content from the Internet by using global threat intelligence from the Smart Protection Network. Every day it analyzes more than 15 terabytes of web data to discover potential threat content and classify web sites into more than 80 categories. The vURLF also accepts user-defined URL lists or third-party URL databases as detection sources to fulfill region or business-specific requirements, such as local government regulations.

Virtual Deep Packet Inspector (vDPI)

The vDPI is a VNF that identifies over 2,100 network applications, including instant messaging, peer-to-peer, games, media streaming, and VPN software, and more than 3,800 device types, such as PCs, smart phones, tablets, and smart home devices, by examining packet signatures. The built-in advanced heuristic analysis engine scans only the first few packets of a connection to minimize latency impact, and analyzes the states of encrypted packets to correctly identify a wide variety of applications using encrypted communications. Separate controls can be made not only on the network applications but also the individual capabilities, including login, chat, file transfer, live audio, and live video.

Element Management System (EMS)

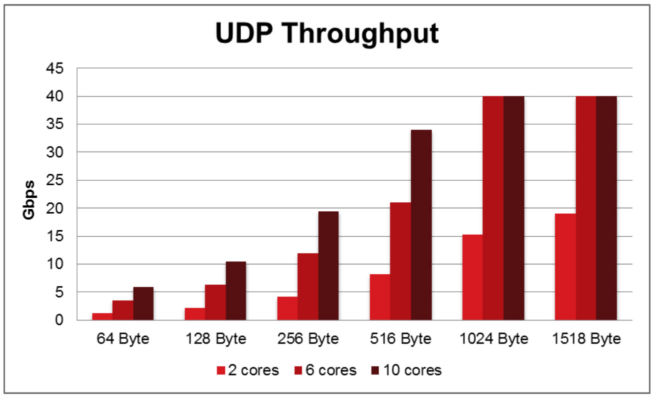
The EMS serves as the central manager in the Trend Micro Virtual Network Function Suite and manages logs, updates, configurations, and life cycle of one or more VNF instances. The EMS collaborates with MANO to exchange system information, such as VNF health status or workload, and scale out or scale in the system if necessary. When a new VNF instance is provisioned, the EMS deploys necessary policy configurations and updates to the VNF instance, and monitors its status. The EMS provides RESTful APIs to integrate with third-party systems and supports forwarding systems or inspection logs to syslog servers for further analysis, reporting, or auditing.

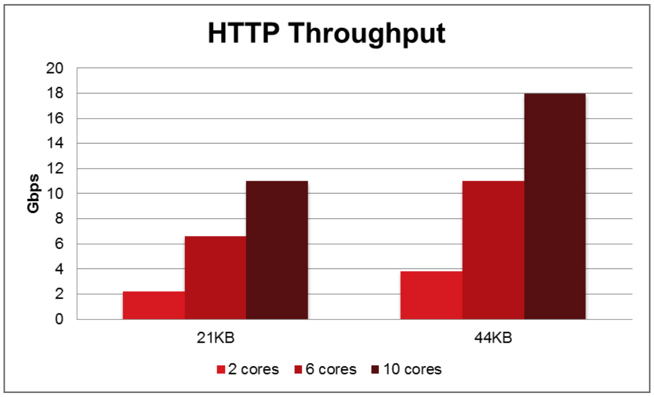
ADVANTAGES

High Performance

Trend Micro Virtual Network Function Suite's unified DPI engine checks network packets and performs select functions, such as intrusion prevention, application controls, or URL filtering, in one single scan, eliminating the performance impact introduced by checking the same network packets in repetitive cycles with multiple engines. In addition, it leverages Intel® DPDK, a program library designed specifically for packet processing, to achieve maximum throughput.

(For UDP test, the test rig generates up to 40 Gbps UDP traffic.)





Scalability and Availability

The ability to scale on demand is one of the most important capabilities that NFV offers. When traffic volume becomes larger and causes high resource utilization, such as high CPU usage or large number of network sessions, Trend Micro Virtual Network Function Suite collaborates with MANO and provides new VNF instances to provide larger processing capability. When the workload becomes smaller, some working VNF instances can be terminated to release infrastructure resources to other functions. When any VNF instance become abnormal, Virtual Network Function Suite's scalable capability can also be applied and create new VNF instances to substitute the abnormal ones, and keep service availability and continuity.

Friendly RESTful APIs

Trend Micro Virtual Network Function Suite provides friendly and comprehensive RESTful APIs, such as policy configuration management, log queries, VNF health status, and account management, making it easily integrated with MANO or other third-party systems.

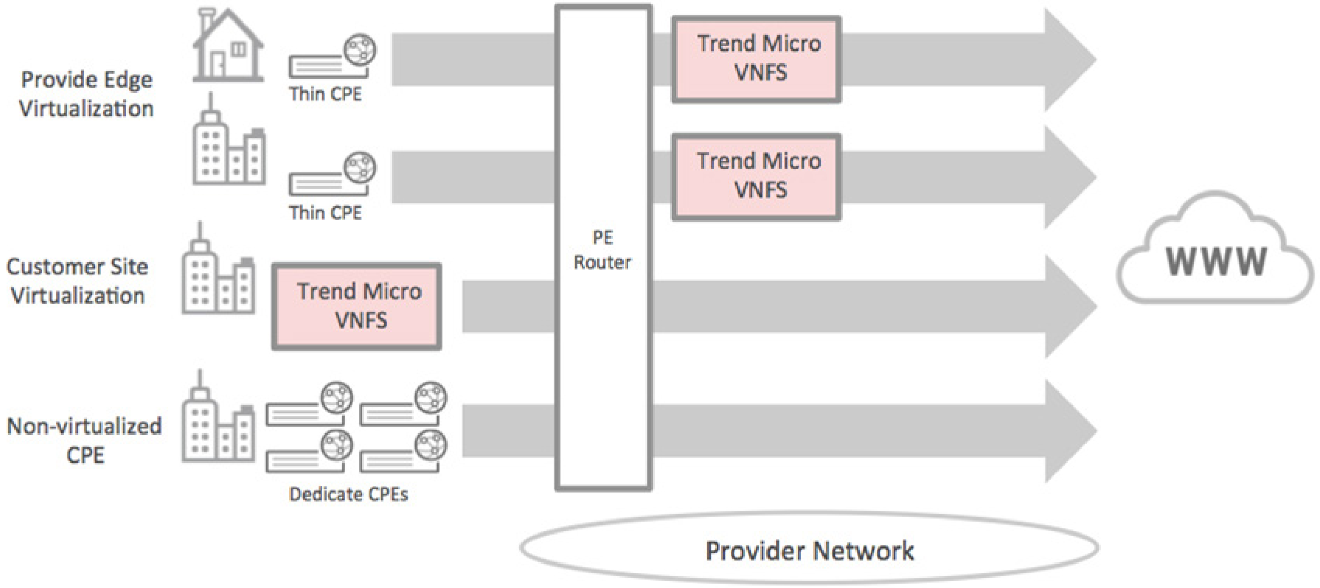
Support of Multiple CPU Architectures

Trend Micro Virtual Network Function Suite can run on both Intel x86 and ARM-based CPU architectures. CSP may decide which CPU architecture to adopt according to use case or cost consideration.

USE CASES

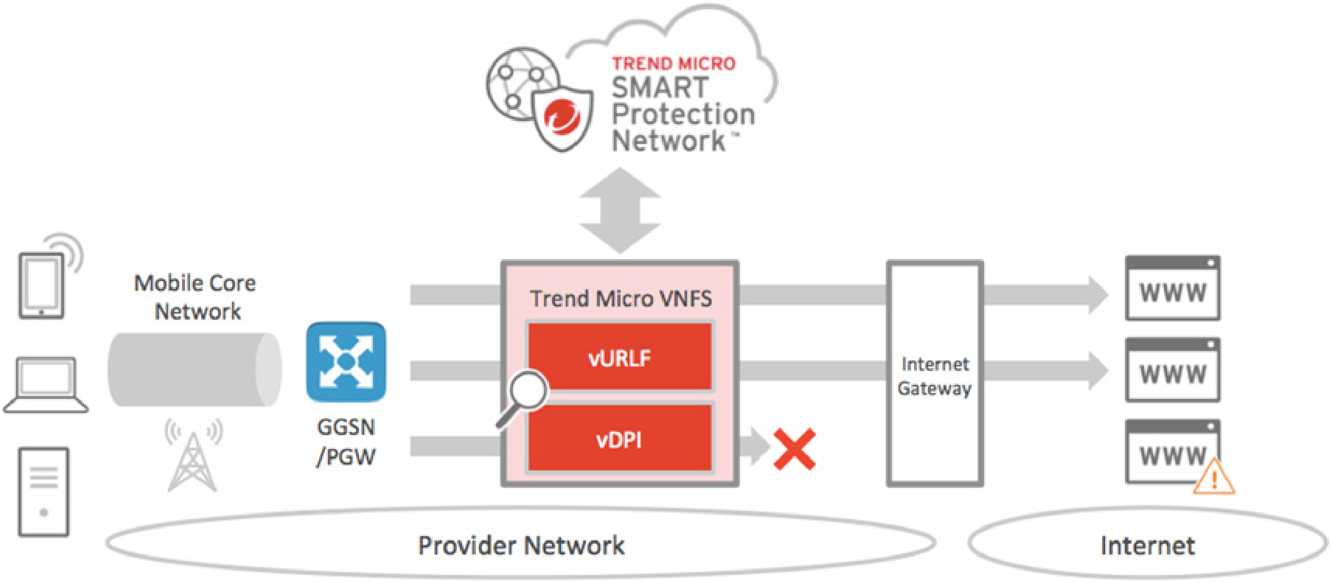
Virtual Customer Premise Equipment (vCPE)

vCPE leverages NFV infrastructure and allows service providers to provide flexible network services to home and enterprise users. By replacing existing complex customer-side appliance with NFV compliant virtualized solutions, vCPE helps to reduce labor cost in CPE maintenance and, more importantly, enables faster and more flexible service updates and installation. With rich experiences in home and enterprise networks, Trend Micro Virtual Network Function Suite can help CSP to provide reliable and flexible network security services to home and enterprise users. For enterprise users, the solution can also be deployed at the enterprise cloud.



Parental Control

By leveraging URL filtering and application control functions, Trend Micro Virtual Network Function Suite can prevent children from visiting inappropriate web pages, or using certain network applications, such as instant messaging, peer-to-peer, games, or social networks.



SYSTEM REQUIREMENTS (FOR EVALUATION)

The following table shows Virtual Network Function Suite's minimum system requirements for general evaluation purposes. The recommended system requirements may vary due to the number and characteristics of evaluated functions or specific NFV environments to integrate. Consult Trend Micro for more details.

Component	vIPS, vURLF, or vDPI (Minimum)	vIPS, vURLF, or vDPI (Recommended)	EMS (Minimum)	EMS (Recommended)
vCPU Core Number	2	2 or more	1	2
Memory	6 GB	8 GB	4 GB	8 GB
Storage	2 GB	2 GB	20 GB	20 GB
NFV Infrastructure and MANO	• OPNFV Brahmaputra 3.0 • OpenStack Liberty • Open vSwitch 2.3.90 • Tacker 0.0.1			

ABOUT TREND MICRO

Trend Micro Incorporated, a global leader in cyber security solutions, helps to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses, and governments provide layered security for data centers, cloud environments, networks, and endpoints. With over 5,000 employees in over 50 countries and the world's most advanced global threat intelligence, Trend Micro enables organizations to secure their journey to the cloud.

For more information, visit **www.trendmicro.com**

Securing Your Journey to the Cloud