SOLUTION BRIEF

Communications Service Providers
Network Security

Trend Micro™ Powers Cyber Security Using Intel® Technologies

Consumers' security concerns create service opportunities for MNOs. Trend Micro's URL filtering-based Virtual Network Function Suite provides consistently powerful cyber security protection features across PCs and mobile devices.

Introduction

Powerful smartphones, tablets, and other mobile devices are creating new challenges and opportunities for mobile network operators (MNOs). For example, parents worry that their kids are spending too much time on their mobile devices and that they will see objectionable content. And all consumers are increasingly worried about cyber-attacks aimed at their handsets. In fact, giving parents and consumers the tools to block access to unacceptable or malicious online content has been a growing business opportunity for MNOs for many years.

The Challenge

One key technology underlying these services is URL filtering—examining all URL requests, comparing them to a database of known problem sites, and blocking mobile access to any that are problematic.

As mobile data volumes grow, there is a need for more URL filtering. At the same time, MNOs are shifting to small cells, which increases the number of base stations in the network and the number of URL filtering servers needed to provide comprehensive services. Legacy, appliance-based security servers have been limited by proprietary hardware equipment that is expensive and can't easily scale. Along with most other network functions, MNOs are demanding the shift to virtualized security functions in order to lower costs and improve agility.

Trend Micro™ is working with Intel to power its Virtual Network Function Suite (VNFS), a software-based solution that delivers high-performance security solutions to MNOs, utilizing the Data Plane Development Kit (DPDK) for high-speed packet processing. By decoupling network functions from proprietary hardware, MNOs can scale their capabilities and enable faster delivery of services, all while reducing costs. The specific advantages of Trend Micro's VNFS over fixed legacy systems include:

- Security resources that can be dynamically allocated and configured for different services
- Native design for carrier-grade NFV with a pure software architecture that provides high-performance network security protection
- Inclusion of Trend Micro security features and market-tested threat intelligence
- Security services that can be dynamically scaled and allocated to meet demand when traffic increases

The Solution

Trend Micro VNFS is a fully virtualized set of network functions that sit in the MNO's Gi-LAN, between the packet gateway and the Internet, converting device- and user-level policies into effective URL blocking and deep packet inspection analysis critical to security and web monitoring services.

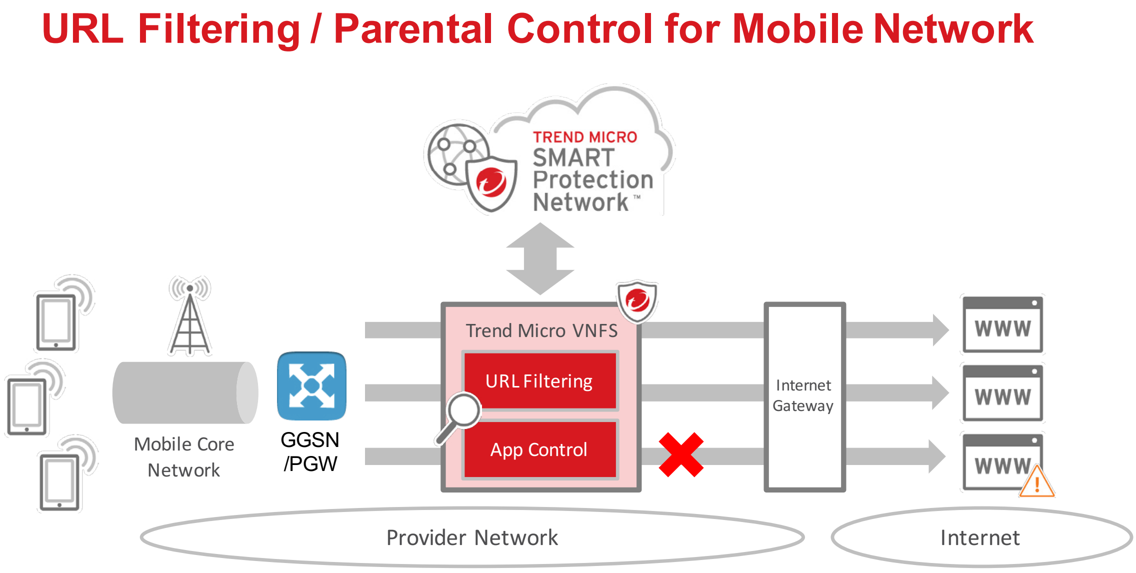


Figure 1. Trend Micro VNFS deployed in the Gi-LAN for a parental control service.[1]

Trend Micro VNFS leverages the Trend Micro™ Smart Protection Network™ (SPN) infrastructure, the company's global threat intelligence that rapidly and accurately collects and identifies new threats and delivers instant protection features for data wherever it resides. The SPN collects 15 terabytes worth of data for analysis, identifies 180,000 new threats, analyzes 1.5 billion new threat samples, and blocks 250 million threats every 24 hours.[2] It tracks the credibility of domains and assigns reputation scores based on the website's age and historical location changes. It also utilizes malware behavior analysis to uncover indications of suspicious activities. Through sandbox emulation modeling, multiple touchpoints, and smart feedback from real-world sensors, the SPN can accurately detect and block the latest malicious actors and inappropriate content.

By integrating with the SPN, Trend Micro VNFS includes the company's comprehensive URL reputation database that identifies and blocks malicious or inappropriate URLs for subscribers and filters over 80 URL categories across the following high risk domains: adult, business, communications, search, Internet security, lifestyle, and network bandwidth.

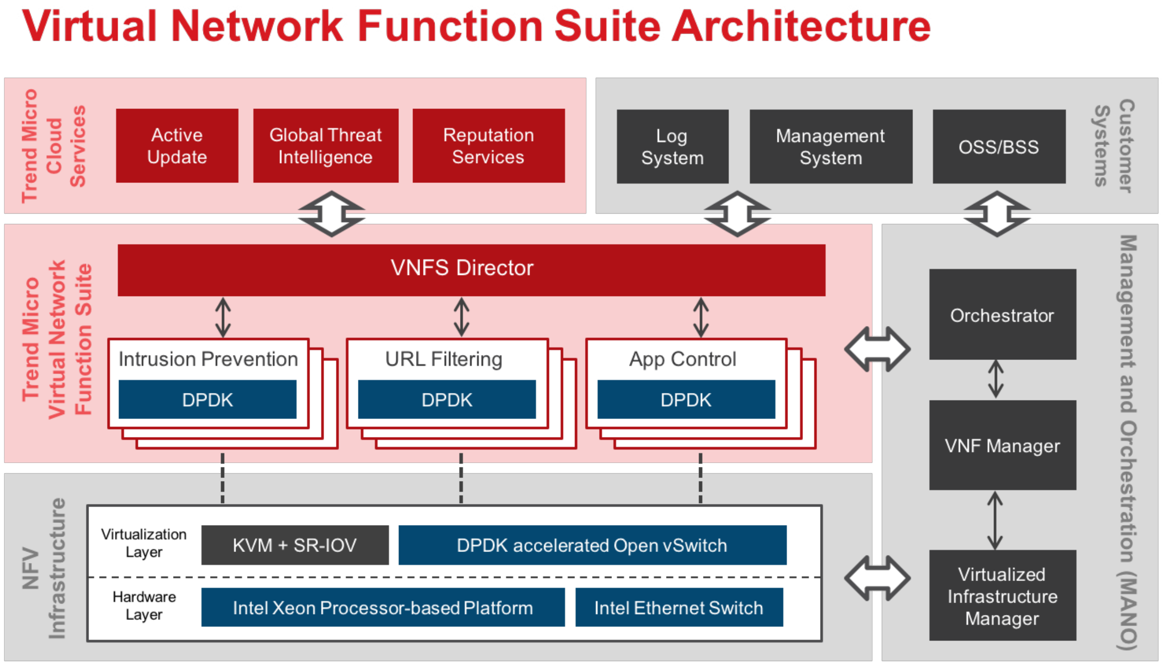

Virtual Network Function Suite Architecture
Trend Micro Cloud Services
Active Update
Global Threat Intelligence
Reputation Services
Log System
Management System
OSS/BSS
Customer Systems
Trend Micro Virtual Network Function Suite
VNFS Director
Intrusion Prevention
DPDK
URL Filtering
DPDK
App Control
DPDK
Management and Orchestration (MANO)
Orchestrator
VNF Manager
Virtualized Infrastructure Manager
NFV Infrastructure
Virtualization Layer
KVM + SR-IOV
DPDK accelerated Open vSwitch
Hardware Layer
Intel Xeon Processor-based Platform
Intel Ethernet Switch

Figure 2. VNFS block diagram

In addition to URL filtering, Trend Micro VNFS provides network security features, including intrusion prevention and application control, to enable MNOs to deliver a broader range of security services to the subscribers.

The Intel Difference: High Performance and High Reliability

Trend Micro VNFS leverages the Data Plane Development Kit (DPDK) for fast packet processing and excellent performance to manage the intensive computing required to deliver effective URL filtering and application control services. DPDK is an Intel-developed technology that is now an open source project run by the Linux Foundation.*

Running on servers powered by Intel® Xeon® processors E5-2600, with Intel® Ethernet Network Adapters, the VNFS obtains high levels of throughput and performance by running packet inspection, pattern matching, and metadata extraction in a heavily loaded core network environment. The high demands on the VNFS packet inspection process requires CPU performance that scales to demand.

Figure 3 shows VNFS's HTTP throughput and its scalability. The test was done on an Intel architecture-based platform with a single Intel Xeon processor E5-2680 v3 with 128 GB of DDR4 2133 MHz RAM, and two Intel® Ethernet Converged Network Adapters X710. The server also featured the Intel® C612 connectivity chipset for communications, storage, and embedded devices. The Intel C612 chipset provides multiple SATA Gen 3, USB PCI Express* Gen 2 ports along with an integrated Gigabit Ethernet controller.

The server's data plane was based on DPDK v16.11. As Figure 3 shows, VNFS is capable of processing 17.2 Gbps of HTTP traffic by using only one virtual CPU core, with the performance number potentially exceeding 40 Gbps when using four virtual CPU cores.[2]

The VNFS may be capable of higher throughput levels, but its true maximum throughput was not determined as the test equipment used could generate only up to 40 Gbps of HTTP traffic. The testing results below are for 21K and 44K HTTP response sizes and show that the Trend Micro VNFS is ideal for heavy traffic applications because of its high efficiency and linear scalability.

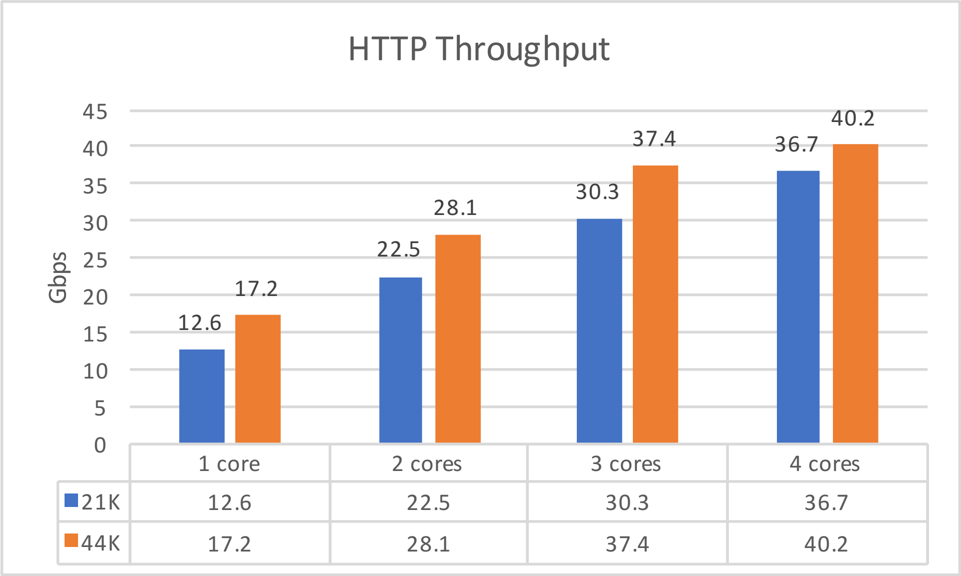
Leveraging DPDK and Intel architecture hardware technologies, VNFS deployments can be flexible and agile as VNFS consumes only a few CPU cores, leaving compute capacity for other applications.

Conclusion

Trend Micro VNFS provides a high-performance foundation to help MNOs keep customers cyber safe and prevent unwanted exposure to objectionable content. Moving beyond expensive and fixed legacy systems with virtualized security solutions means MNOs can transition their security services along with other network functions into flexible and scalable systems. The virtualization of security functions with the Trend Micro™ Virtual Network Function Suite delivers services that:

- leverage Trend Micro's extensive global threat identification and prevention services
- block access to malicious and inappropriate websites in a database that is cataloged and updated daily
- utilize heuristics and predictive analytics to react quickly to the emergence of bad actors

Trend Micro VNFS requires superior processing power to accomplish intensive deep packet processing across its extensive breadth of security management services. The company has worked with Intel® Xeon® CPU E5-2600 series to achieve excellent processing performance and scale to the demands of MNOs in a rapidly growing and changing environment.



	1 core	2 cores	3 cores	4 cores
🟦21K	12.6	22.5	30.3	36.7
🟧44K	17.2	28.1	37.4	40.2

Figure 3. VNFS HTTP throughput and scalability[3]

About Trend Micro

Trend Micro Incorporated, a global provider 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.

About Intel® Network Builders

Intel® Network Builders is an ecosystem of independent software vendors (ISVs), operating system vendors (OSVs), original equipment manufacturers (OEMs), telecom equipment manufacturers (TEMs), system integrators (SIs), enterprises, and service providers coming together to accelerate the adoption of network functions virtualization (NFV)-based and software-defined networking (SDN)-based solutions in telecom networks and in public, private, and hybrid clouds. The Intel Network Builders program connects service providers and enterprises with the infrastructure, software, and technology vendors that are driving new solutions to the market. Learn more at http://networkbuilders.intel.com.

[1] Figures provided courtesy of Trend Micro.

[2] To learn more about the Trend Micro Smart Protection Network, visit http://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html

[3] Test conducted by Trend Micro. Configurations: Single Intel Xeon processor E5-2680 v3, two Intel® Ethernet Converged Network Adapters X710, Intel® C612 chipset, and 128 GB of DDR4 2133 MHz RAM.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. **No computer system can be absolutely secure.** Check with your system manufacturer or retailer or learn more at intel.com.

Cost reduction scenarios described are intended as examples of how a given Intel-based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors.

Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit www.intel.com/benchmarks.

Trend Micro, the t-ball logo, and Smart Protection Network are trademarks or registered trademarks of Trend Micro Incorporated.

© Intel Corporation. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

0817/DO/H09/PDF ♲ Please Recycle 336334-001US