SOLUTION BRIEF

HIGH-PERFORMANCE VIRTUAL NETWORK FUNCTIONS FOR 5G MOBILE NETWORKS

INDUSTRY-LEADING NETWORK PERFORMANCE AND SECURITY THROUGHOUT THE 5G AND NFV MIGRATION

5G-enabled mobile network traffic and devices are projected to increase substantially in the next few years, propelled by commercial IoT devices and rich video applications with demanding latency requirements. Mobile network operators need a high-performance, scalable and manageable architecture that will reduce costs, strengthen service agility and scale up as needed. The network function virtualization (NFV) framework proposed by ETSI provides a flexible, scalable architecture that runs on standard hardware systems and provides the agility missing on proprietary hardware. 5G stand-alone networks require a virtualized core. Operators are moving to adopt the 5G and NFV models to virtualize core network functions as quickly as possible and to deploy automated service chaining, provisioning and other businesses processes to support those efforts and keep costs under control.

NFV EVOLUTION CHALLENGES

Security, performance, interoperability, and operations complexity are key challenges for operators, as traffic and competitive pressures relentlessly accelerate.

Mobile operators must still maintain a high-performance, always available network for subscribers as they transition the network to NFV. To accomplish this, they need a broad range of high-performance software-based virtual network functions that integrate easily into their existing and future networks.

CHALLENGE

Mobile network operators must quickly transform networks to virtualized 5G architectures to gain critical cost and service agility benefits. Security, performance, interoperability, and operations complexity remain key challenges as traffic and competitive pressures accelerate. Operators need proven software-based solutions.

SOLUTION

A10 Networks' high-performance virtual network functions (VNFs) are built for the unique security and performance requirements of evolving mobile networks. VNFs comply with the ETSI NFV framework, integrate with leading MANO systems and have been proven interoperable through multiple ETSI Plugtests and operator evaluations.

BENEFITS

- Speed NFV transition with fully interoperable, carrier-class VNFs
- Simplify operations through feature parity across physical, virtual, container and bare metal platforms
- Reduce operations risk through tested VNFs
- Meet the rising performance requirements of 5G applications

Security is a top concern for operators. The high volume of lightly protected devices, more distributed network nodes and the move away from proprietary hardware and protocols to more common protocols such as HTTP/2 provide new and easier opportunities for cybercriminals to target mobile networks and subscribers for a wide range of attacks.

Interoperability between physical and virtual functions as well as management systems is also a key requirement. High performance is mandatory, so in many cases, operators must deploy physical network functions instead of desired virtual functions to meet performance requirements. All software functions may not work well with the orchestration or MANO systems preferred by the operator and hardware-based functions must work with software-based elements.

Virtualized technology is still relatively immature, and operators need to deploy it carefully to ensure that the entire network is secured and operates seamlessly.

THE A10 NETWORKS 5G SECURITY SOLUTION PORTFOLIO -VIRTUALIZED NETWORK FUNCTIONS

A10 Networks' high-performance VNFs are built for the unique security, performance and feature requirements of mobile networks evolving to NFV and 5G. The high-performance VNFs include industry-leading DDoS protection, CGNAT, firewall, deep packet inspection, intelligent traffic steering and other functions.

Fully interoperable with leading MANO and orchestration systems, A10 vThunder® software solutions can rapidly deploy and scale on operators' virtualized infrastructures, protecting the mobile infrastructure and subscribers from multi-vector attacks and safeguarding always-on service availability. Operators can cost-effectively secure the entire network without sacrificing performance as they evolve their networks.

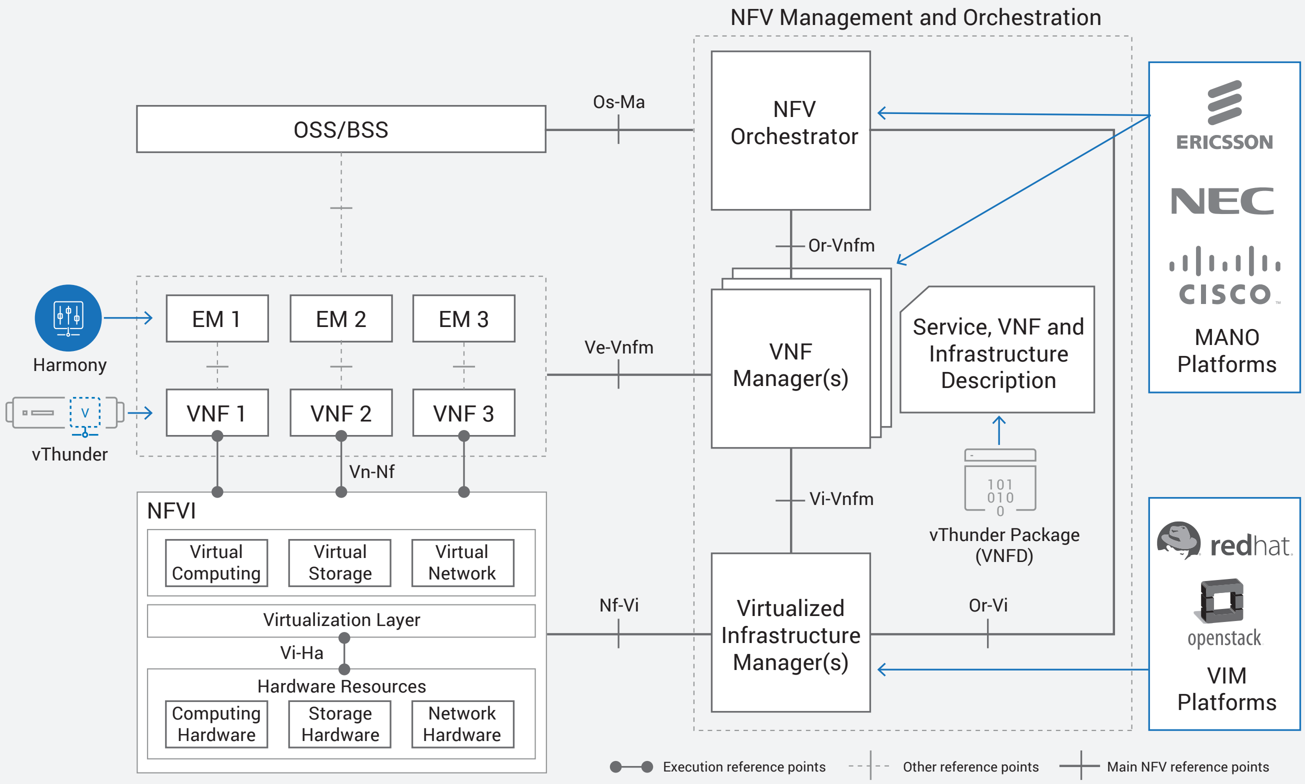


Figure 1: The A10 vThunder VNF solution and leading NFV-MANO solutions in an ETSI NFV-MANO architectural framework

FEATURES AND BENEFITS

PROVEN VNFS WITHIN THE ETSI FRAMEWORK

By following ETSI NFV specifications, the NFV-MANO solution can accept and automatically onboard the A10 vThunder VNF package onto its VNF catalog. NFV-MANO can then dynamically orchestrate and deploy vThunder as an application and security VNF instance(s) in multi-vendor or single-use network services.

vThunder also includes lifecycle management information required by NFV-MANO to perform VNF instance scaling, healing and termination functions beyond onboarding and instantiation.

A10 Networks participated in the ETSI NFV Plugtests events to test its end-to-end VNF lifecycle operation capabilities, allowing network programmability and cloud service orchestration. In addition, the vThunder VNFs have already been tested by tier-one mobile network operators and deployed in 5G launches.

NFV-MANO INTEGRATION AND HYPERVISOR SUPPORT

The A10 vThunder VNF package has been integrated and validated with leading NFV-MANO solutions, including Ericsson Cloud Manager, NEC Netcracker HOM, Cisco NSO, Red Hat OpenStack and more.

Customers can gain on-demand deployment flexibility of vThunder software instances on leading hypervisors, such as VMware ESXi, Microsoft Hyper-V and KVM. They can achieve strong isolation with completely independent vThunder instances (with no shared components). Factors such as planned maintenance reboots on one vThunder instance do not affect other virtual machines. Virtual software is portable to another compatible host, as needed.

PORTFOLIO OF HIGH PERFORMANCE VNFS

A10 Networks 5G security solution portfolio includes the following high-performance VNFs:

VIRTUAL NETWORK FUNCTION (VNF)	DESCRIPTION
vThunder CFW	vThunder CFW is a converged application and security solution that consolidates ADC, CGN, DPI and firewall functions for mobile infrastructure.
vThunder CGN (Virtual carrier-grade Networking)	Deliver advanced carrier-grade networking with vThunder CGN as a VNF for CGNAT and IPv4-to-IPv6 migration. Automate on-demand provisioning of IPv4 and other tenant services quickly and efficiently to avoid business disruptions due to IPv4/IPv6 compatibility issues.
Gi/SGi FW	The vThunder CFW with Gi/SGi firewall allows mobile carriers to block network attacks and unauthorized access. It incorporates a stateful firewall with a rich set of features to protect subscribers and shields the LTE data and control plane services from a wide array of threats.
vThunder SeGW	vThunder security gateway protects the mobile network backhaul at the S1 interface between the radio access network (RAN) and core network with IPsec tunnels. The SeGW allows authentication of eNodeB base stations for accessing the evolved packet core (EPC). Once authentication is established, secure backhaul is established between the eNodeB base station and the gateway, from one side, and the gateway to the EPC on another.
vThunder TPS	Detect and mitigate multi-vector DDoS attacks with vThunder TPS as a VNF. Protect network assets from volumetric, protocol and resource attacks, application-level attacks and IoT-based attacks at the network edge or on a per-application/tenant basis.
vThunder ADC	vThunder ADC provides virtualized L4-L7 server load balancing to optimize, accelerate and secure applications. It scales web and infrastructure servers seamlessly to ensure business continuity, accelerates applications and protects infrastructure for uninterrupted, efficient operations.
GTP FW	A GTP firewall provides security and scalability, while protecting the mobile core against GTP-based threats such as information leaks, malicious packet attacks, and DDoS attacks through GTP interfaces in the access networks and GRX/IPX interconnect to support uninterrupted operations.
Integrated DDoS	A10 vThunder CGN is augmented with integrated DDoS mitigation capabilities for improved attack detection, reporting, and mitigation. Includes IP protocol anomaly filters and connection rate limiting.
Deep Packet Inspection (DPI)	Deep packet inspection-based application visibility classifies more than 3,000 applications in over 40 categories to provide granular insights into network traffic.

HIGH PERFORMANCE WITH SERVICE FUNCTION CONSOLIDATION

The vThunder CFW is a converged application and security solution that consolidates ADC, CGN features, DPI and firewall functions, leverages the company's proven Advanced Core Operating System (ACOS®) and delivers high performance in a virtual appliance form factor.

SIMPLIFIED OPERATIONS

MANAGEMENT INTEGRATION

To further simplify and automate operation tasks, A10 Networks' full-featured RESTful API offers rapid integration with third-party management consoles to efficiently operate one or more vThunder appliances.

CAPACITY-BASED PRICING – NO FEATURE LICENSES

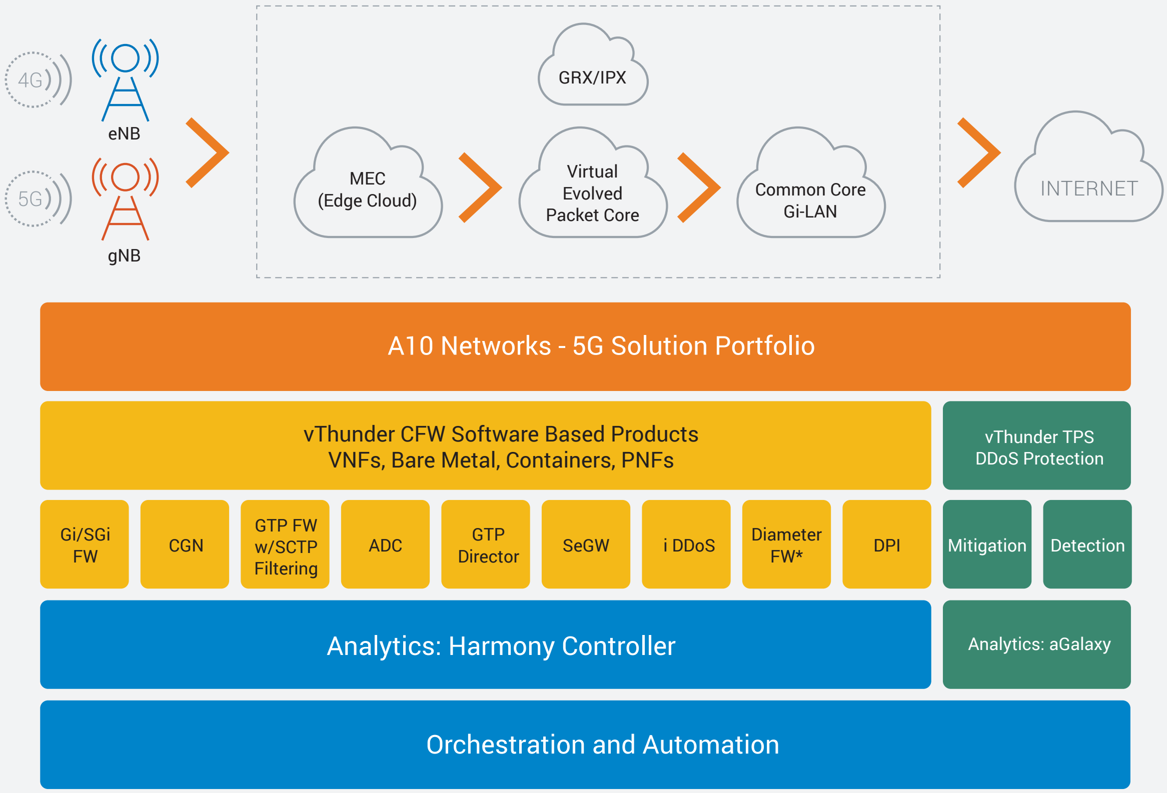
The A10 FlexPool® license, a software subscription-based capacity pooling model, provides great flexibility to allow operators to allocate and distribute multiple vThunder instances whenever and wherever they need. A10 networks' all-inclusive licensing model, along with the FlexPool, can drastically reduce the complexity of operations and licensing management in the software-based network, and provide predictable CAPEX and OPEX.

FEATURE PARITY ACROSS PHYSICAL NETWORK FUNCTIONS, VIRTUAL NETWORK FUNCTIONS, CONTAINERS, BARE METAL

vThunder software appliances leverage the same high-performance architecture, advanced features and familiar GUI/CLI options that power A10 Thunder hardware appliances, delivering feature parity between hardware and software.

API-DRIVEN ARCHITECTURE

vThunder software integrates with hypervisor management tools and automates management tasks with easy-to-use industry-standard CLI, a web-user interface and a RESTful API (aXAPI®) and integrates with custom or third-party management consoles. Full RESTful API control enables DevOps and SecOps efficiency.


4G
eNB
5G
gNB
GRX/IPX
MEC (Edge Cloud)
Virtual Evolved Packet Core
Common Core Gi-LAN
INTERNET
A10 Networks - 5G Solution Portfolio
vThunder CFW Software Based Products
VNFs, Bare Metal, Containers, PNFs
vThunder TPS DDoS Protection
Gi/SGi FW
CGN
GTP FW w/SCTP Filtering
ADC
GTP Director
SeGW
i DDoS
Diameter FW*
DPI
Mitigation
Detection
Analytics: Harmony Controller
Analytics: aGalaxy
Orchestration and Automation

*Roadmap

Figure 2: A10 Networks 5G solution portfolio includes a broad range of virtual network functions

HIGH-PERFORMANCE, FLEXIBLE VNFS FOR RAPID AND SIMPLIFIED NETWORK EVOLUTION

A10 Networks provides highly scalable security solutions for 5G network scenarios. Its robust security portfolio can be deployed in physical, virtual, bare metal, and container form factors to suit individual network topologies, including 4G, 5G-NSA, 5G-SA, MEC and NFV.

The A10 Thunder and vThunder CFW provides exceptionally high connection rates, throughput and concurrent sessions for the most demanding 5G use cases.

The A10 Thunder and vThunder TPS is an automated multi-vector DDoS protection solution that ensures availability of business services at any scale or type of network.

The A10 Networks 5G security portfolio provides the highest flexibility, scalability and protection for mobile networks.

NEXT STEPS

For more information, please visit www.a10networks.com/solutions/service-provider/.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™, with a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices in more than 80 countries worldwide. For more information, visit: www.a10networks.com and @A10Networks.

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19203-EN-01 OCT 2019