SOLUTION BRIEF

# NFV-MANO INTEGRATION SUPPORT

## APPLICATION SECURITY VNF ORCHESTRATION AND AUTOMATION FOR MOBILE SERVICE PROVIDERS

With the rise of mobile and IoT devices, mobile service providers (SPs) are undergoing a rapid transition to 5G to improve service agility and generate new service revenue. There is already a wide range of network hardware devices to support mobile broadband services in today's 4G network. Adding more proprietary hardware from various vendors has been known to be inflexible, time-consuming and difficult to manage. SPs have turned to software-based implementation of network services on standard virtualization platforms to consolidate multiple network functions, shorten service delivery time and remain competitive. A10 Networks has collaborated with leading NFV-MANO vendors to introduce integrated NFV orchestration and automation solutions to rapidly deploy and scale A10 vThunder® software appliance on SPs' virtualized infrastructure, protecting mobile infrastructure and subscribers from multi-vector attacks and safeguarding always-on service availability.

## THE CHALLENGE

In response to the proliferating mobile, IoT and 5G service needs, mobile service providers (SPs) are adopting virtualized infrastructure, software defined networking (SDN) and network functions virtualization (NFV) solutions. SDN abstracts the network control and forwarding planes, enabling a programmable network, while NFV separates network functions from hardware, projecting to deliver as many virtualized network functions (VNFs) as possible. This new

## CHALLENGE

Mobile service providers need to apply network virtualization and automation to address the evolving business needs of digital transformation and increase service revenue from 5G and IoT services while protecting infrastructure resources and subscribers from malicious intrusions and security threats.

## SOLUTION

A10 vThunder software appliance, integrated with leading NFV-MANO solutions within the ETSI NFV framework, enables end-to-end, multi-vender network services delivery and provides a converged application and security solution with performance.

## BENEFITS

- Enable network service programmability and automation
- Simplify operation and lower the total cost of ownership
- Achieve higher business agility and reduce time to market
- Comply with the ETSI NFV framework and interoperability requirements

software strategy represents an opportunity to significantly reduce network services design complexity and accelerate end-to-end service delivery.

Achieving effectiveness of this new software strategy requires SPs to seek out new centralized NFV management and orchestration (NFV-MANO) solutions to foster a VNF ecosystem, facilitate network service design and delivery and fulfill SP operators' business objectives. NFV-MANO solutions also need to follow industry open standards in order to smoothly onboard VNFs from multiple vendors, orchestrate them in service chaining, interoperate with virtualized infrastructure managers (VIMs) and manage network services and VNFs through their instantiation-termination lifecycle with auto-scaling and auto-healing in between.

This new software strategy must also address the additional cybersecurity requirements to defend against internal and external multi-vector attacks. As SPs migrate to IP-based software strategy, mobile infrastructure resources and subscriber services become a wider landscape for bad actors to exploit—with billions of intelligent mobile devices and IoT devices on tap. SPs need to include more adaptable and programmable security solutions in their VNF portfolios and deploy them to protect the network service availability and enhance subscriber quality of experience.

## *NFV-MANO INTEGRATION SOLUTION*

A10 Networks supports SPs' software strategy and delivers A10 vThunder software appliance in a VNF Package based on ETSI NFV specifications. The vThunder software image is packaged along with a TOSCA-based VNFD (VNF Descriptor) and other configuration files to support full interoperability with NFV-MANO solutions.

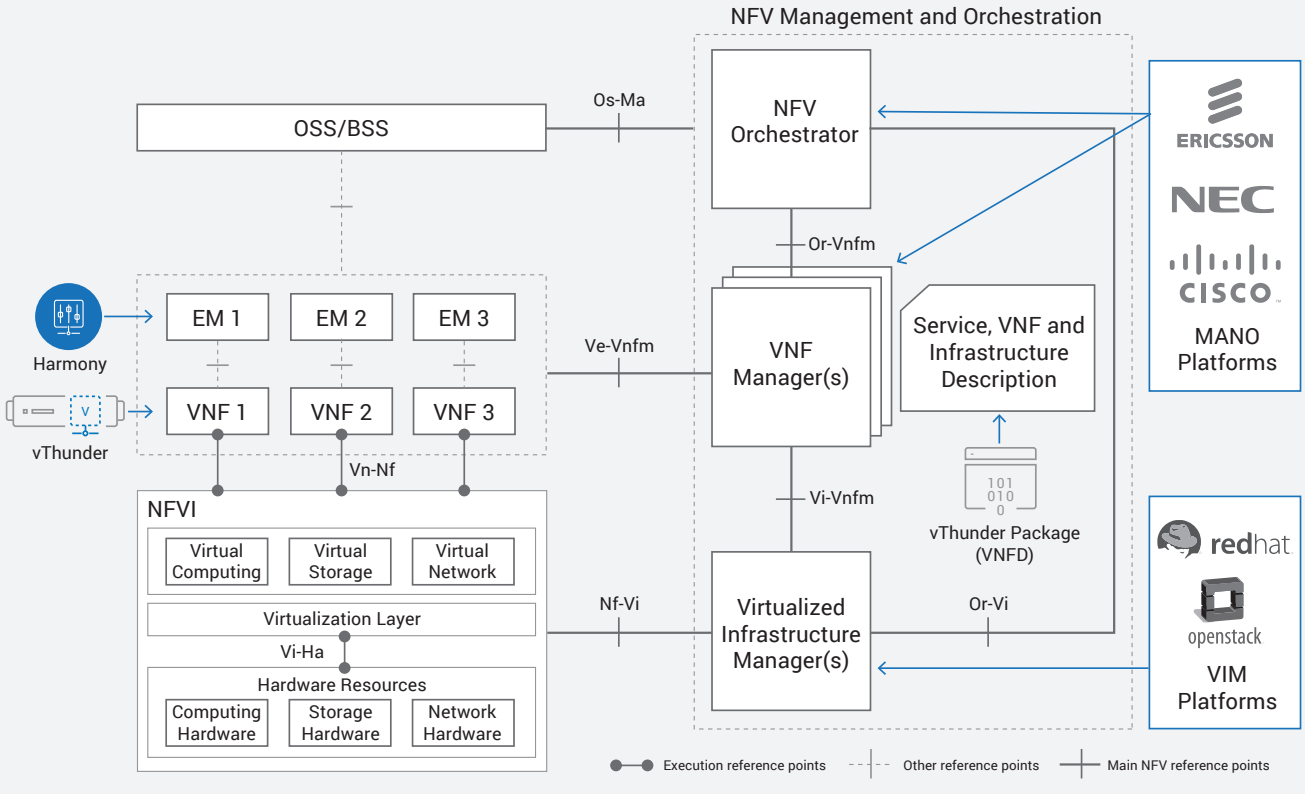


**Figure 1**: The A10 vThunder VNF solution and leading NFV-MANO solutions in an ETSI NFV-MANO architectural framework

## PROVEN VNF WITHIN AN ETSI NFV 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. The VNFD of vThunder also includes lifecycle management information required by NFV-MANO to perform VNF instance scaling, healing and termination functions beyond onboarding and instantiation.

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—for full interoperability within the ETSI NFV framework.

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 (see Figure 1).

## HIGH-PERFORMANCE ARCHITECTURE WITH SERVICE FUNCTION CONSOLIDATION

In second and third ETSI NFV Plugtests, A10 vThunder CFW was tested as ADC, CGNAT and partially Gi-Firewall for securing application delivery and enhancing service availability in multi-vendor network services. vThunder CFW is a converged application and security solution that consolidates ADC, CGNAT and L4-L7 firewall functions, leveraging A10's market-proven Advanced Core Operating System (ACOS®) that delivers high performance of up to a 100 Gbps bandwidth in virtual appliance form factor.

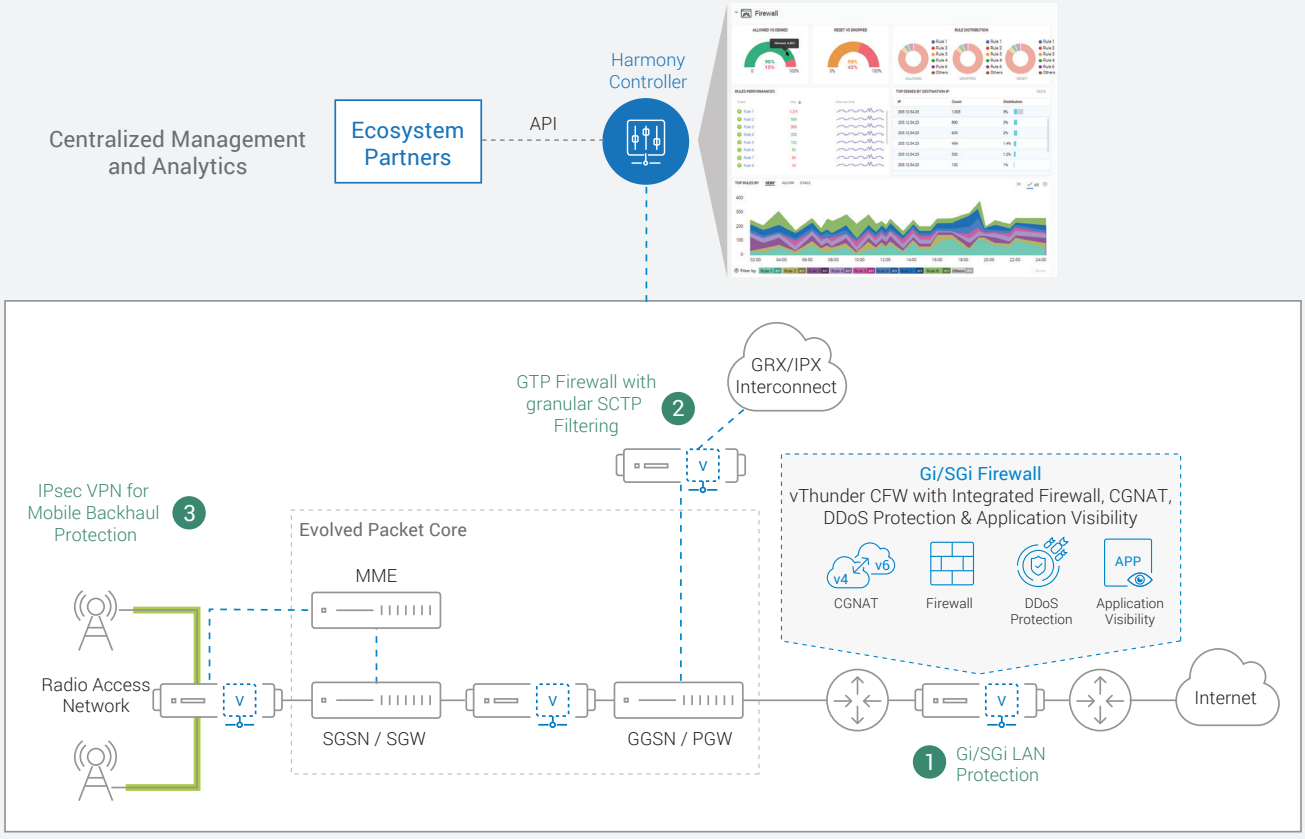


**Figure 2**: A10 vThunder deployment scenarios for securing a mobile infrastructure

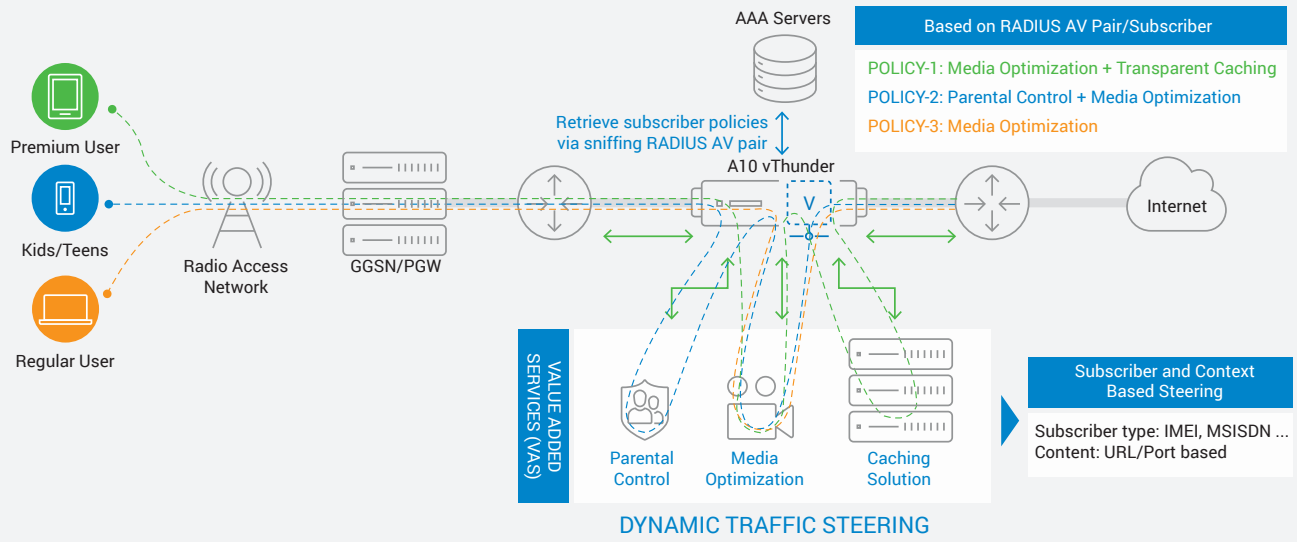


**Figure 3**: A10 vThunder deployment scenario for per-subscriber traffic steering

A10 vThunder CFW offers the performance and versatility needed to scale and protect mobile infrastructure and subscribers from various attacks and service disruption. It can be deployed as a Gi/SGi firewall to provide consolidated CGNAT, stateful firewall, integrated DDoS protection, DPI and L4-L7 services on the Gi-LAN between the mobile infrastructure and the Internet. It can also be deployed as a GTP firewall with granular SCTP filtering to protect the mobile infrastructure against attacks from access network and roaming partners. On the radio access network, vThunder can be deployed to protect untrusted backhaul traffic over control and data planes and deliver exceptional IPsec VPN performance with scale (see Figure 2).

A10 vThunder also enables SPs to offer value-added services and drive new service revenues. For instance, when deployed as the Gi/SGi firewall, SPs can apply dynamic traffic steering policies based on the subscriber type or the traffic context toward value-added services (VAS) for better traffic management and differentiated subscriber experience (see Figure 3).

## SIMPLIFIED OPERATION AND MANAGEMENT WITH VISIBILITY

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

A10's FlexPool™ license, a software subscription-based capacity pooling model, provides great flexibility that allows operators to allocate and distribute multiple vThunders whenever and wherever they need. A10's all-inclusive licensing model, along with the FlexPool, drastically reduce the complexity of operation and licensing management in the software-based network.

The A10 Harmony® Controller is the centralized management system for A10 vThunder® appliances. Harmony Controller provides the capabilities to distribute application security policies, backup and restore configurations and access service visibility and analytics in real-time across vThunder appliances in the service provider network.

## SUMMARY

The ETSI NFV compliant A10 vThunder VNF appliance, which is fully integrated with leading NFV-MANO solutions, enables rapid network service innovation, dynamic application security delivery and new service revenue to mobile service providers with centralized orchestration and automation. vThunder VNF offers ADC, CGNAT and L4-L7 firewall functions in one consolidated virtual appliance, enabling further cost reduction at both CAPEX and OPEX to SPs. This NFV-MANO interoperability by A10 vThunder supports SPs' pursuit of 5G software strategy and business agility.

## NEXT STEPS

For more information, please visit www.a10networks.com/solutions/5g-mobile-network-security and www.etsi.org/index.php/news-events/events/1278-3rd-nfv-plugtests.

## ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) provides Reliable Security Always™ through a range of high-performance solutions that enable intelligent automation with deep machine learning to ensure business critical applications are protected, reliable and always available. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

## LEARN MORE

ABOUT A10 NETWORKS

### CONTACT US

a10networks.com/contact



Part Number: A10-SB-19198-EN-01 JAN 2019