White Paper

Simplify NFV Deployment for Service Providers and Enterprises in the Data Center and Hybrid Cloud

Cisco, Intel, and Radware Collaborate to Accelerate the Adoption of High-Performance NFV

Contributors

Travis Volk, Technical VP of Sales Development, travis.volk@radware.com

Ilango Ganga, PE, Standards and Strategic Initiatives, Ilango.s.ganga@intel.com

Jalal Sadreameli, Market Development Manager, jalal.e.sadreameli@intel.com

Ken Hook, Technical Marketing Engineer, khook@cisco.com

Gunnar Anderson, Product Line Manager, guanders@cisco.com

Jim French, Distinguished Systems Engineer, jifrench@cisco.com

Contents

Barriers to Network Functions Virtualization Technology Adoption

For today's service providers and enterprises, bandwidth demands continue to increase and evolve. The introduction of Internet of Things (IoT) solutions, such as smart homes, smart cities, connected cars, and connected medical devices, is forcing organizations to change existing business models and to build more cost-effective networks.

In addition to reduced capital expenditures (CapEx) and operating expenses (OpEx) for basic connectivity services, service providers and enterprises are seeking unique technology values that will distinguish their offerings from those of competing service providers and over-the-top (OTT) solution vendors. Fast service introduction, agility, scalability, security, and low-latency access serve as the main differentiators of OTT content and the content offered by application providers.

Network functions virtualization (NFV) technologies are designed to meet this challenge and make better use of an organization's network investments. They can provide the tools to effectively grow complex network and server environments to meet business, application, and subscriber needs, while better matching revenue through smart utilization of the network.

NFV Benefits and Adoption Challenges

The goal of NFV technology is to alleviate some of the challenges of the modern network using the following means:

- NFV is designed to use x86 hardware, which allows more efficient use of capital than dedicated purpose-built hardware appliances. Significant cost reductions can be achieved through the following:
  - Hardware sharing and repurposing
  - Fast packet-processing algorithm for x86 servers based on the Intel® Data Plane Development Kit (DPDK)
  - Single-Root I/O Virtualization (SR-IOV) and pass-through technologies, which increase hardware performance
  - Hosting network functions, known as virtualized network functions (VNFs)
- Software-based NFV deployments alongside real-time software-defined networking (SDN) programming results in rapid service introduction and improved operation efficiency.
- As NFV enables the decoupling of network functions from their physical location, services can be placed at the most cost-effective locations. Also made possible are multi-site application availability, scalability, cloud bursting, and real-time deployment.
- Operation cost reductions can be achieved through end-to-end service lifecycle management, resulting from common automation and operating procedures.
- Open and standardized interfaces between virtualized network functions and the infrastructure enable service providers and enterprises to avoid vendor lock-in. Each service provider or enterprise can select its own best-in-class options and run in a multi-vendor environment.

Despite the many advantages of NFV, service providers and enterprises are still concerned that NFV technology is not mature enough to provide robust performance and service assurance.

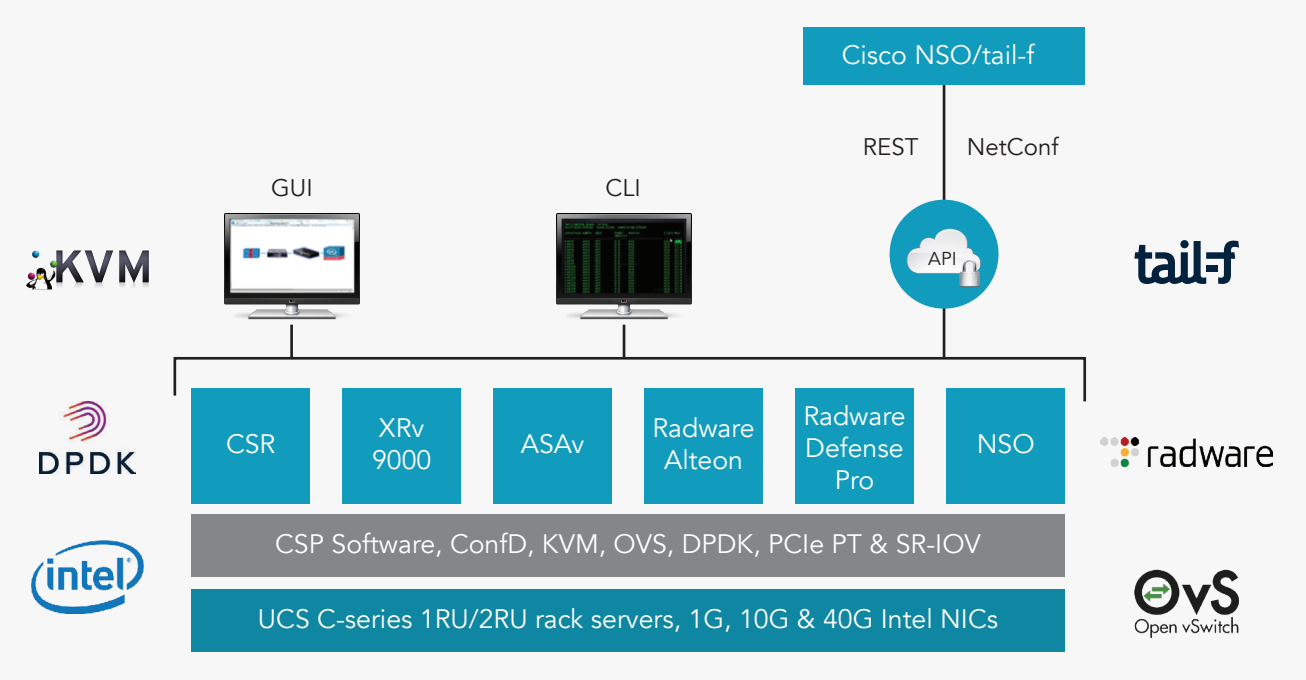
Furthermore, the distributed multi-site and multi-cloud application enablement that NFV offers introduces massive security challenges. Security policies should be enforced in an environment without a perimeter.

Cisco NFV Platform Software: Cisco Cloud Services Platform 2100

Cisco® Cloud Services Platform (CSP) 2100 (Figure 1) is a turn-key NFV and Open x86 Linux Kernel-based Virtual Machine (KVM) software platform for both service provider and enterprise environments. The CSP 2100 is a platform without all the complexities and overhead that come with Openstack deployments. You can start with ONLY one host, then add additional hosts as needed to scale-out.

The CSP 2100 bridges network, server, and security teams by offering several ways to manage and operate the platform. You can manage the platform using a GUI, command-line interface (CLI), representational state transfer (REST) API, and/or Network Configuration Protocol (NETCONF) using Cisco Network Services Orchestrator (NSO). The orchestrator has been used predominantly in service provider environments, but it is now increasingly being used in enterprise environments.

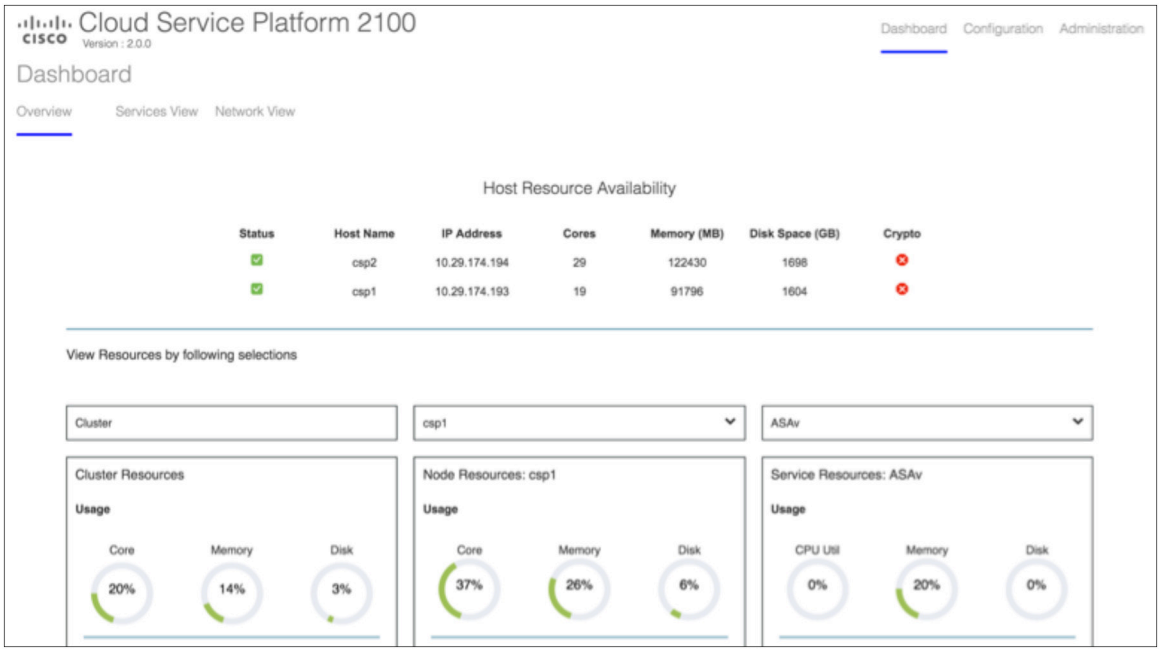
Figure 1. Cisco CSP 2100 High-Level Architecture



The platform enables users to quickly deploy any Cisco or third-party network VNF that supports the KVM hypervisor. The CSP 2100 NFV platform is shipping today with the CSP software running on Cisco UCS® C-Series Rack Servers for 1 and 2 rack units (1RU and 2RU).

The CSP 2100 is designed for a variety of use cases in the cloud, data center, point-of-presence (POP), central office (CO), co-location (COLO), carrier-neutral facility (CNF), WAN aggregation, DMZ and extranet, core network, and server farm environments. Figure 2 shows the Dashboard within the GUI. A simple 2-node cluster is displayed with one VNF running on "csp1".

Figure 2. Cisco CSP 2100 GUI Showing a Simple 2-Node Cluster



Intel Architecture, Software, and Hardware

The Intel® Xeon® E5-2600 v3 product family offers the following innovative features in the 22-nanometer (nm) Intel process technology node:

- Accelerated boot and runtime security with little overhead and faster encryption
- Technologies targeting virtual machine integrity improvement during migration and runtime
- Asynchronous dynamic random access memory (DRAM) refresh for memory data protection
- Comprehensive reliability, availability, and serviceability (RAS) features optimized for demanding communications infrastructure needs

The Intel Ethernet Controller XL710 delivers a variety of features, including:

- Software-configurable Ethernet port speed for up to two 40 Gigabit Ethernet or up to four 10 Gigabit Ethernet connectivity
- Network virtualization overlay stateless offloads for Generic Network Virtualization Encapsulation (Geneve), Virtual Extensible LAN (VXLAN), and Network Virtualization Using Generic Routing Encapsulation (NVGRE) protocols
- Intelligent load balancing for high-performance traffic flows of virtual machines
- Intel DPDK optimized for efficient packet processing to support NFV

Intel DPDK offers the following features:

- A set of optimized software libraries and drivers that can be used to accelerate packet processing on Intel architecture
- Support for buffer management, queue and ring functions, flow classifications, network interface cards (NICs), poll mode drivers (PMDs), and an environmental abstraction layer (EAL)

Radware VNF Fueled by Cisco and Intel

Radware offers NFV and attack-mitigation solutions fueled by Cisco and Intel technologies.

Radware Network Functions Virtualization

The Radware Alteon and DefensePro virtual appliances decouple network functions from dedicated underlying hardware, allowing next-generation services on the CSP 2100 (Figure 3). Delivering a scalable, ultra-high capacity of up to 225 Gbps per instance (Layer 4) and up to 1 Tbps per cluster, the Alteon virtual appliance for NFV:

- Reduces total cost of ownership (TCO)
- Simplifies network services deployment
- Enables capacity elasticity through a simple license upgrade
- Automates service lifecycle management

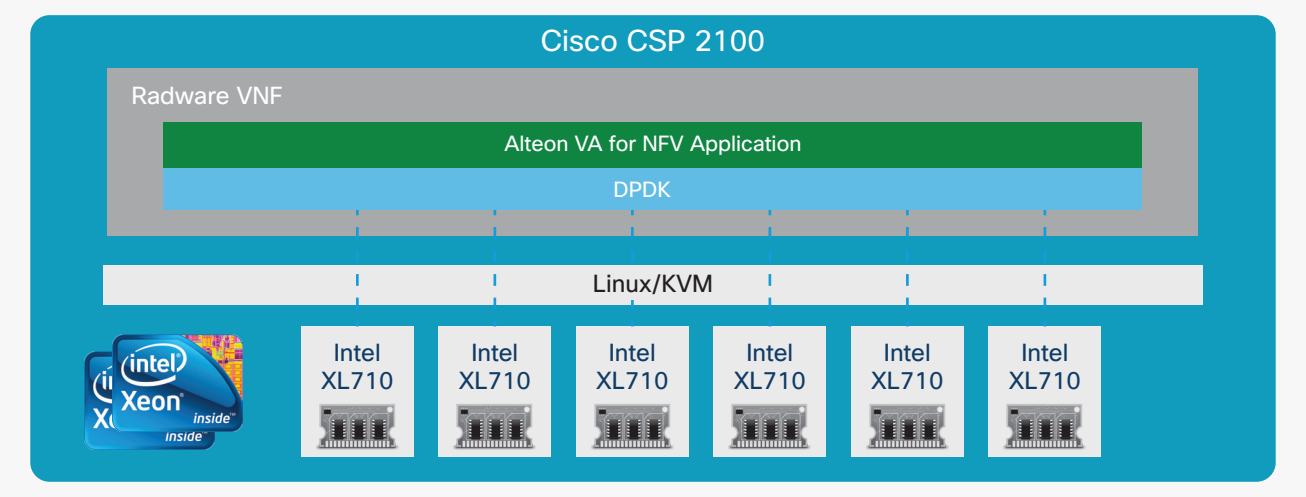
A total of 225 Gbps was achieved on a CSP 2100 2RU form-factor solution, which included the following:

- CSP 2100 Software running on a 2RU Cisco UCS C240 M4 Rack Server
- Intel Xeon processor E5-2699 v3 2.30-GHz 145W CPU with 18-core 45-MB cache and DDR4 at 2133 MHz and Intel Xeon processor E3-2600 v3 CPU (two processors)

Note: Intel Broadwell processors were not available when testing started, but they will be available in Q3CY16 on the CSP 2100.

- Dual-port 40-Gbps Quad Enhanced Small Form-Factor Pluggable (QSFP+) Intel Ethernet Controller XL710 NICs (six cards total)
- Radware Alteon virtual appliance for NFV

Figure 3. Radware VNF Fueled by Cisco and Intel



The Alteon and DefensePro VNFs provide highly efficient resource utilization on open-source hypervisors by redesigning the virtualization approach to incorporate new technologies that increase overall performance:

- They bypass the hypervisor's virtual switch, providing direct and the fast access to the physical NICs of the server based on the Intel PCIe pass-through which is available on the Intel Niantic (Intel 82599 10-Gbps Ethernet controller) and Fortville (Intel Ethernet Controller XL710) NICs.
- They use a fast-packet-processing algorithm for x86 server-based platforms such as the CSP 2100, which is based on the Intel DPDK code.
- They use the non-uniform memory access (NUMA) topology of the host server, which enables the VNF to optimize its performance to the underlying server configuration.

These capabilities enable the Alteon virtual appliance for NFV to reach the industry's best performance of up to 225 Gbps on the CSP 2100.

Radware Attack-Mitigation Solution

The Radware Attack Mitigation Solution (AMS) is a multi-layered security architecture that is well suited for service providers, including carriers and cloud providers. It is based on these main pillars: robust data collection, anomaly detection, attack mitigation, service automation, and attack lifecycle management.

AMS is a hybrid solution offering multi-vector attack detection and mitigation. It combines always-on, on-demand, and cloud peak protection service layers to help guarantee availability in an evolving threat landscape.

AMS provides zero-day network-to-application protection, malware propagation protection, and intrusion defense with the most complete distributed denial-of-service (DDoS) solution on the market. Radware offers unique behavioral capabilities for detecting and generating adaptive real-time signatures with encrypted attack support. A web application firewall is integrated through signaling, combining expression protection with the performance of volumetric mitigation. End-to-end visibility and reporting allows service providers to monetize tailored service through a multitenant managed services service provider (MSSP) portal.

Radware partners with service providers to help guarantee mitigation support with an emergency response team (ERT) dedicated to defending customers from attack.

Radware NFV Solution Use Cases

Radware NFV solutions are compatible with cloud, carrier, and enterprise application and service delivery environments.

Table 1 lists well-defined use cases for integrating a Radware VNF solution with CSP 2100 running on Intel processors and NICs.

Table 1. Radware NFV Use Cases

VNF Use Case	LB	Acceleration H2GW, TCPO	SSL Inspect IP Reputation URL Filtering	Defense SSL	vDP Detector	vDP Mitigation	WAF
vCPE	✓	✓	✓	✓	✓	✓	✓
Mobile DC: DNS, IMP, Billing, VAS, Portals	✓	✓		✓	✓	✓	✓
SDDC	✓	✓	✓	✓	✓	✓	✓

Use Case 1: Virtual Customer Premises Equipment

Virtual customer premises equipment (vCPE) is designed to help service providers save expenses incurred while operating and managing network functions such as routing, firewall, application delivery controller (ADC), DDoS protection, intrusion prevention system (IPS), WAN optimization, access control, and web application firewall (WAF) services. The cost savings are achieved by deploying existing CPE functions in POPs running on software and hardware platforms such as the CSP 2100, which elastically manages capacity based on subscription.

Radware introduces best-in-class vCPE cybersecurity, traffic acceleration, and content delivery functions, exceeding customer requirements while accelerating service agility. Always-on multitenant network and application DDoS services offer any combination of:

- Encrypted attack protection
- Multitiered web application firewall services
- Web acceleration, HTTP 2.0 Gateway (H2GW), SSL inspection, URL filtering, etc.
- End-to-end health monitoring that helps ensure service continuity and origin-based high availability
- MSSP portal available for white labeling to promote downstream channels

Use Case 2: Mobile Data Center

Voice over long-term evolution (VoLTE) service, based on virtual IP multimedia subsystem (vIMS) infrastructure, offers operators huge cost savings and operational benefits. It eliminates the need to have voice and data on separate networks, and it can unlock new revenue potential with rich communication services (RCS) multimedia services such as VoLTE. As VoLTE becomes more attractive, service providers are looking for advanced scalability solutions. Along with its benefits, VoLTE does introduce many security risks because it is based on IMS technology.

vIMS introduces the potential for application DDoS attacks targeting control-plane elements, such as Session Initiation Protocol (SIP) application servers (IMS infrastructure), and data-plane elements, such as session border controllers (SBC) and IMS proxies (P-CSCF).

The Radware vIMS solution is equipped to provide scalability plus protection against SIP scans, SIP application DDoS attacks, brute-force and pre-attack activities, and SIP anomalies.

Control-plane network components are considered mission critical. Radware control-plane solutions provide high availability, scalability, resiliency, and application protection for control-plane protocols, including Domain Name Service (DNS), RADIUS, DIAMETER, Dynamic Host Configuration Protocol (DHCP), and syslog. Radware also provides the best response time in the industry because the company understands that delays in control-plane traffic have a direct, negative impact on users' quality of experience (QoE).

Transparent traffic handling within SGi-LAN zones include header enrichment, packet normalization, real-time policy updates, and advanced TCP acceleration for effective spectral efficiency. Radware offers elasticity and high availability for value-added proxies, gateways, and other high-speed session brokers to increase the resilience and utilization of highly distributed resources. The capability to combine application delivery, performance acceleration, and security across a broad range of elements in a consistent manner offers element consolidation and efficiency.

Use Case 3: Software-Defined Networking

Enterprises and cloud providers are gradually shifting to SDN. Radware provides compelling solutions that transparently integrate its ADC and cybersecurity product portfolio into such environments, allowing customers to capitalize on their investments. Radware's SDN and NFV-based solutions allow customers complete elasticity in deploying their ADC and security services throughout the network on the Cisco CSP 2100. Customers can now deploy and redeploy ADC and security services across their entire network in hours, regardless of the desired location of those solutions. With Radware's Alteon NFV and virtual DefensePro (vDP) solutions, network operators can now quickly deploy high-throughput services wherever required across their network.

The joint venture among Cisco, Intel, and Radware frees expensive IT resources for innovation. Radware's SDN-integrated solutions are focused on simplifying and abstracting the deployment, management, and monitoring of ADC and security solutions, thus requiring less of IT and networking personnel. ADC and security professionals are now able to explore and experiment.

At the same time, simplified implementation of network services, including complex, multi-appliance services, reduces the cost of implementation.

Conclusion

Radware's SDN and NFV solutions broaden an organization's ability to introduce new network services that previously had been either too costly to deploy or impossible to implement. High-scale network services use NFV-compliant ADC and security components, which can perform and scale to match the performance of a high-end hardware device.

Intel products offer open architecture in a secure, low-latency, virtualized, and scalable environment to optimize Cisco and Radware software.

The Cisco CSP 2100 NFV platform software for the Cisco Unified Computing System™ (Cisco UCS) provides both service providers and enterprises a turn-key solution that they can use to begin benefiting from NFV starting today.

For More Information

For additional information, see:

- http://www.cisco.com/go/csp
- https://dcloud-cms.cisco.com/?p=23376
- https://networkbuilders.intel.com/
- http://www.radware.com/Products/Alteon-VA-NFV-Resources/

For questions and comments, contact CSP-2100@cisco.com.

C11-737457-00 06/16