SOLUTION BRIEF

Network Virtualization: VMware NSX* with Intel® Technology

Software-Defined Data Center / Software-Defined Infrastructure
Intel® Xeon® Processor E5 Product Family
Intel® Ethernet 10Gb/40Gb Converged Network Adapters
Intel® Security Product Family

Virtualization has been a critical approach for IT to deliver new efficiencies in recent years. Consolidating compute resources onto virtualized hosts has helped reduce CAPEX by lowering equipment requirements in the data center, as well as cutting OPEX through simplification of the environment.

Extending that value further, VMware NSX virtualizes network resources, which is analogous to hypervisor-based virtualization of compute resources using virtual machines (VMs). Network virtualization helps increase agility and IT's ability to respond to evolving business requirements. Networks can be provisioned in seconds, using NSX building blocks such as logical switches, routers, firewalls, load balancers, and VPNs. All NSX elements and services are integrated with VMware vSphere*, designed to be complemented by Intel® security technologies, and highly optimized for Intel® architecture. These elements and services are built to be spun up and down as needed and to be programmatically assembled in any combination to create custom networks on demand. In addition, the NSX distributed service framework enables the dynamic insertion and orchestration of security services offered by partners.

IT Transformation

The integrated NSX network virtualization platform deployed with Intel® technology enables IT innovation by playing a key role in building the software-defined data centers (SDDC) and software-defined infrastructures (SDI), illustrated in Figure 1. In this model, all infrastructure is virtualized on Intel architecture and delivered as a service, created in and controlled by software. The environment can be automated to rapidly create, maintain, and de-provision infrastructure as needed, without human intervention.

SDDC and SDI transform IT as a whole, delivering the following capabilities and benefits:

- **Resource usage is optimized**. Because compute, network, storage, and security are virtualized and delivered as a service, they abstract the physical network, and general-purpose Intel architecture takes the place of special-purpose equipment, serving all functions on an as-needed basis and saving on costs.
- **Operations are accelerated, with enhanced agility**. Infrastructure automatically responds to changing needs, without human involvement. This approach allows new services and applications to be deployed more rapidly than with conventional infrastructure, giving IT greater control.
- **Security and services are unified across the environment**. Security is orchestrated by policy and applied automatically to all resources as appropriate, including to networks that are logically defined using micro-segmentation, enhancing advanced threat protection inside the network perimeter. Software-defined availability enables IT to create resilient services and better satisfy changing business needs.

NSX on Intel architecture enhances IT's ability to support automated deployment and fast, scalable, and simplified provisioning of advanced threat protection services that secure consumption of all enterprise applications and services, on any device, with any cloud-management platform.

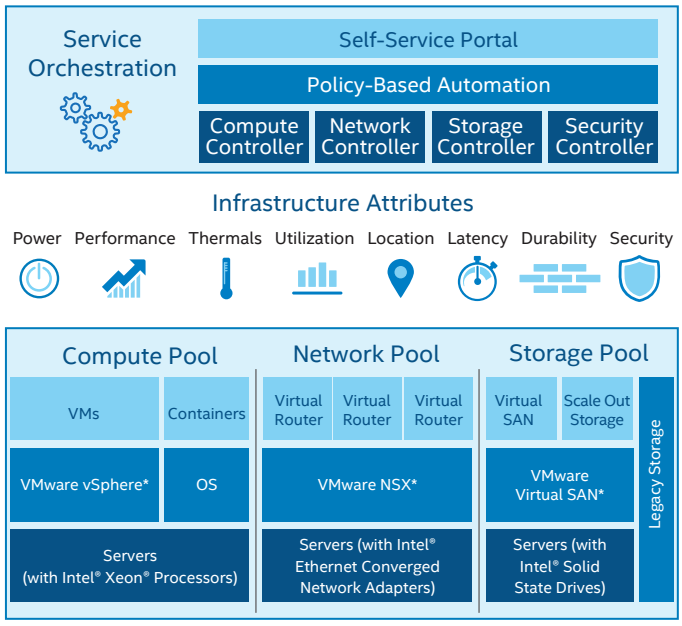

Figure 1. Solution architecture of the software-defined data center and software-defined infrastructure.

Use Cases: NSX and Intel Technology

Data center automation. Automated network provisioning and rich affinity among virtualized network, storage, compute, and security resources accelerate deployment of, and changes to, applications and services. Decoupling workloads from the physical network extends unified support for both physical and virtual resources.

Self-service IT. Efficiencies in the data center accelerate time to production. Network and security services are fully distributed and centrally managed, enabling robust capabilities for business units and isolated development, test, and production environments on the same physical infrastructure.

Multi-tenant clouds. Hardware sharing is optimized among tenants (even across separate physical sites), automated network provisioning streamlines operations, and applications and workloads are protected by means of isolation from other tenants.

VMware NSX and Intel Virtualization Solution

The optimization of NSX for Intel architecture is the culmination of over a decade of collaboration between Intel and VMware working together to enable the next generation of innovation in data center solutions. The NSX virtualization solution builds on the Intel® hardware stack based on the Intel® Xeon® processor E5 product family and Intel® Ethernet 10Gb/40Gb Converged Network Adapters. The Intel® Xeon® processor E5-2600 v4 product family enhances NSX virtualization, with increased parallelism (up to 22 cores/44 threads) and up to 1.5 TB of DDR4 memory supported per socket.[1] It provides up to 2.7x improvement in virtualized performance[2] compared to the Intel® Xeon® processor E5-2690, as well as reduced overhead for near-native I/O performance with SR-IOV.

Intel Ethernet 10Gb/40Gb Converged Network Adapters enable logical networks that allow VMs to communicate across subnets while dramatically reducing configuration and management requirements and increasing network responsiveness and flexibility. The network-virtualization solution based on NSX and Intel® technologies enhances agility, increases scalability, and provides advanced security automation of Intel security technologies.

Enhanced Agility

The NSX and Intel solution stack allows virtual networks to be spun up on demand and automates the provisioning, distribution, and delivery of virtualized IPS and VM anti-malware. Isolation among virtual networks simplifies the role of network administrators, who no longer need to scrutinize each network configuration change to avoid adverse effects on other applications. Instead, each virtual network can be configured specifically for the applications and workloads it supports.

Moreover, all services across virtual networks can be configured from a single console, on the fly. New physical or virtual services can be inserted as needed, with workloads migrating freely across subnets and availability zones using VMware vMotion*. Because network resources are abstracted away from the physical network, placement of these workloads is not encumbered by physical topology or the availability of physical network services in a given location. Optimizations for features of Intel architecture such as Intel® Advanced Vector Extensions 2.0 accelerate processing of those workloads, wherever they reside.

Increased Scalability

The Intel architecture-based hardware stack helps enhance the scalability of the NSX environment as a whole, making it well suited to large and growing deployments. Scale-out server architecture allows NSX services to dynamically scale automatically, simply by adding new hosts to the environment. By extending Layer-2 subnets, the environment allows VMs to be migrated fluidly across WANs and clouds.

NSX also takes advantage of Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) to accelerate processor-intensive parts of encryption and decryption routines in hardware. That acceleration is beneficial to maintaining pervasive encryption as workloads and topologies increase in size.

Capabilities of NSX with Intel Technology

Fine-grained security based on virtual firewalls and other controls can be managed down to the level of the virtual network adapter. APIs provide for integration with leading security and management hardware and software solutions, connecting virtual networks to physical workloads and legacy VLANs. Examples include popular offerings from Intel Security, Palo Alto Networks, Symantec, and Trend Micro.

Advanced Security Automation

NSX offers deep capabilities for security automation. Micro-segmentation provides for logically subdivided subdomains that use per-VM security policies that are decoupled from the network hardware. This capability helps protect East-West traffic (internal to the network) as well as North-South traffic (from outside the network).

Hardware and software-based security measures are deeply integrated into the NSX and Intel technology solution stack, enabling security automation as a core network design principle, rather than as a bolted-on afterthought. In addition to Intel AES-NI—discussed above—key aspects of the advanced security natively integrated into virtualized networks based on NSX and Intel technology include the following:

- **McAfee® Virtual Network Security Platform (vNSP)** provides next-generation intrusion protection system (IPS) services that are automatically deployed across the environment to help protect East-West traffic inside the network perimeter.
- **Intel® Security Controller** provides a layer of abstraction between the security infrastructure and virtualization management, providing virtualized security services from a built-in security function catalog to enable software-defined security that automates security provisioning, policy management, protection, and remediation. Intel Security Controller is bundled with vNSP features.
- **McAfee® Management for Optimized Virtual Environments (MOVE) AntiVirus** automatically provisions security for VMs with antivirus policies and services throughout the environment, integrated with and centrally controlled by the McAfee® ePolicy Orchestrator® (McAfee ePO™) as well as the NSX Manager console.
- **McAfee ePO** software enables a consolidated view of all endpoint security, including risk and compliance across the organization and up-to-the-minute assessments of at-risk infrastructure based on system vulnerabilities, network defenses, and endpoint security levels.
- **Intel® Trusted Execution Technology (Intel® TXT)** moves the root of trust from software to the hardware level, checking the execution environment against a known good image at startup to verify that no unauthorized changes have been made that could jeopardize the security of application workloads.

NSX supports micro-segmentation of the environment into logical networks, as illustrated in Figure 2. McAfee vNSP, Intel Security Controller, and McAfee MOVE AntiVirus provide advanced security services to micro-segments that can enhance data protection and regulatory compliance. In this usage model, a conventional perimeter firewall is employed between the network and the outside world, and NSX micro-segmentation with advanced security from Intel helps protect internal segments of the network from threats.

The micro-segments shown here are logically isolated subdomains for the finance, HR, and R&D divisions of a company. They do not need to be physically partitioned from each other, allowing for free sharing and reuse of physical resources while retaining separation of network traffic and data. In addition to protection from threats that originate outside the network (North-South traffic), micro-segmentation is also effective against attacks that are detected in the network inside the data center (East-West traffic).

The segments use security policies that are centrally managed and applied down to the VM level, decoupled from the physical network. NSX deploys a distributed firewall (Access Control Lists) that governs communication among the segments, and Intel technologies provide advanced security services such as IPS and antivirus that can be deployed and managed at the click of a button.

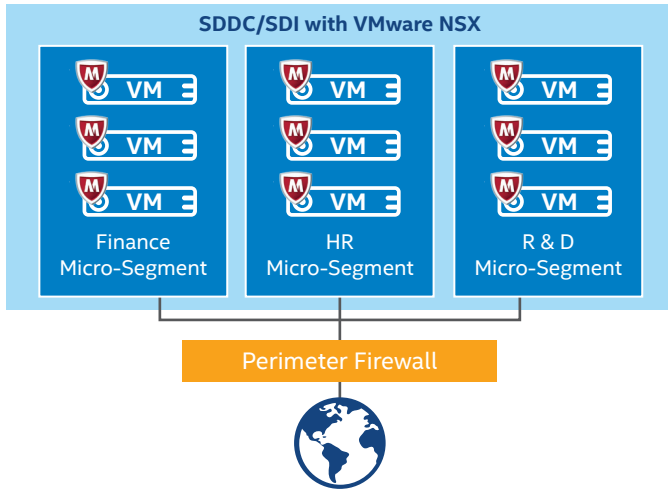

Figure 2. Micro-segmentation with VMware NSX* and Intel® technologies.

Conclusion

Using NSX and Intel technologies, IT organizations can implement virtual networking that enhances the agility, security, and scalability of operations. This set of solutions enables CIOs to optimize resource usage, implementing efficiencies to thrive in the face of shrinking budgets and rapidly changing and growing business demands. Automated provisioning, distribution, and delivery of security services provides advanced threat protection including IPS and antivirus protection features built specifically for virtual environments, including protection of East-West traffic within the network perimeter.

Micro-segmentation allows for robust isolation of logical subdomains while sharing physical resources, and policies are automatically maintained and applied to specific workloads. Centralized, granular control ensures streamlined management and consistent policy across the environment, using familiar tools. Collaboration between Intel and VMware delivers a solution that is highly optimized for Intel® processors and network adapters, fully integrated with Intel Security's solutions, setting the stage for the SDDC and SDI.

For more information, visit

intel.com/xeon

vmware.com/products/nsx

intel.com/vmware

Additional Resources

- Intel® Security Controller: www.intelsecurity.com/solutions/intel-security-controller.html
- McAfee Virtual Network Security Platform: http://www.mcafee.com/us/resources/data-sheets/ds-virtual-network-security-platform.pdf
- McAfee MOVE AntiVirus: http://www.mcafee.com/us/products/move-anti-virus.aspx

[1] Up to 3TB of memory supported per 2-socket server. Each socket supports 4 memory channels @ 3 DIMMs per channel = 12 DIMM slots per socket. Using 128GB memory DIMMS = 1.5TB per socket = 3 TB of memory per 2P server.

[2] Up to 2.7x improvement in virtualization throughput VMmark 2.x workload comparing baseline Fujitsu* PRIMERGY RX300 S7 server with two Intel® Xeon® processor E5-2690, 256GB memory with VMware ESXi* 4.1 scoring 12.51 @ 10 tiles (Source: http://www.vmware.com/a/assets/vmmark/pdf/2013-08-06-Fujitsu-RX300S7.pdf) to a Fujitsu* PRIMERGY RX2540 M2 server with two Intel® Xeon® processor E5-2699 v4, 512GB memory with VMware ESXi* 6.0 U1b scoring 34.74 @ 28 tiles (Source: http://www.vmware.com/a/assets/vmmark/pdf/2016-03-31-Fujitsu-RX2540M2.pdf).

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.

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.

0416/SA/MESH/PDF 333428-003US