5 STEPS TO BUILDING ADVANCED SECURITY IN SOFTWARE-DEFINED DATA CENTERS

INTRODUCTION

The modern data center is rapidly evolving. Virtualization is paving the way to the private cloud, enabling applications to be delivered at a fraction of the cost and time. Virtualization separates workloads from hardware for the pooling of resources to be dynamically allocated on-demand. This resource pooling enables the virtualized data center, and is a critical foundation for the Private Cloud. Private Clouds are implemented internally within the corporate firewall, and controlled by the IT department, bringing with it an element of trust that is less inherent in public clouds.

Private cloud doesn't mean only on-premise deployment. Cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination thereof, and it may exist on or off premises. Organizations may also implement hybrid cloud architectures, where some of the workloads can be offloaded to the public cloud.

Enterprises have long benefited from the virtualization of key infrastructure elements, compute and storage. However one the most basic components of the data center, the network, remained highly complex and lacked automation, relying on manual operations to function. Connecting anything to the network requires manually configuring switches, firewalls and other network devices. This is where the network became the bottleneck for applications.

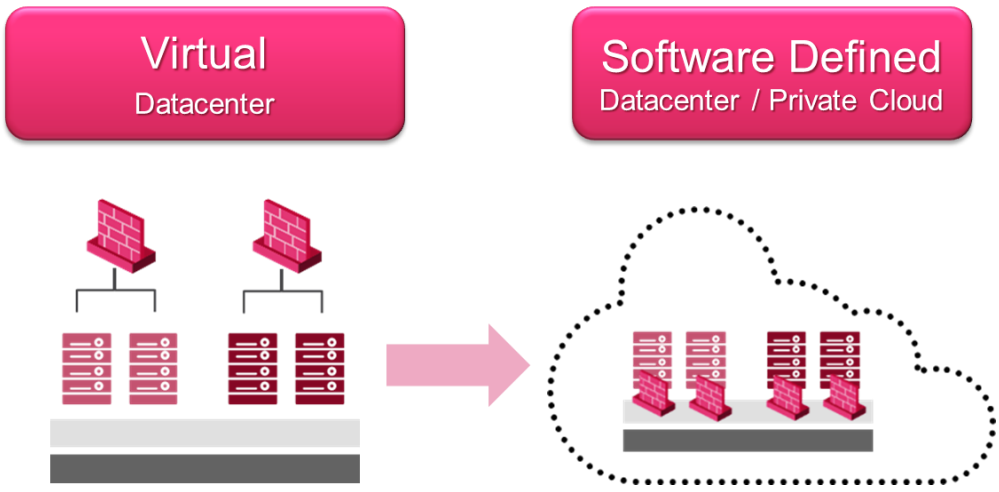

Figure 1: Modern data centers rapidly evolving due to virtualization

Now data centers are evolving to the next stage, virtualizing the network layer. Network virtualization unleashes the full power and benefits of virtualization which enables applications to be delivered at a fraction of the cost and time.

This has led to the Software-Defined Data Center (SDDC), where all the infrastructure elements - networking, storage, compute and security – are virtualized and delivered as a service. The entire infrastructure is automated by software, orchestrating user-defined services and integrating security and agility into the data center.

September 16, 2015

Today the SDDC can be fully realized through VMware NSX. NSX is a complete network virtualization platform that delivers better security through native capabilities including isolation, segmentation and automated security operations. Providing the foundation for the SDDC, NSX makes micro-segmentation economically and operationally feasible, enabling automated deployment, orchestration and scale-out of native and advanced security services such as Check Point vSEC.

The integration of vSEC with NSX helps automate and simplify the provisioning of advanced security services. NSX and vSEC together provide advanced threat prevention dynamically deployed and orchestrated into any software-defined data center environment.

MODERN DATA CENTER CHALLENGES

Traditional perimeter security solutions are not suitable to address the dynamic demands the modern data center. Some of the security challenges that must be overcome include:

- The shift in traffic behavior within the data center - Historically the majority of traffic loads were between entities that were external to the data center ("North-South" traffic) driven by the wide use of siloed client-server applications and secured by the perimeter gateway.

  Data Center traffic today has now shifted. Workloads are more heavily "east-west" – intra-data center traffic – as a result of virtualization, shared services and new distributed application architectures.

  Within virtual environments these complex communications get little to none of the advanced controls or protections from traditional security solutions that safeguard "North-South" traffic since it never passes through the network perimeter or gateway. Perimeter firewalls typically have limited visibility into this "east-west" traffic leaving it and the data center vulnerable to malware and other malicious payloads.

- Traditional security approaches are manual, operationally complex and slow to implement – Traditional security solutions are not designed to keep pace with dynamic virtual network changes that come with rapid application provisioning. And sole reliance on perimeter security leads to resource-intensive choke-points on the network. This has a tremendous impact on datacenter performance and increases security complexity, thus placing additional burdens on security teams.

- The wide use of VLANs in data centers increases the threat to all applications – Due to the lack of inter-system (and VM) advanced security, a breach of a single (virtual) host network can allow malware to spread laterally and propagate across the network, compromising all applications, including those residing on different VLAN's. Successful attacks on even low priority services can expose the most critical or sensitive systems because intra-VM / East-West security protections simply don't exist.

The Software-Defined Data Center with NSX network virtualization allows organizations to address these security issues in a way that works with the elasticity and automation which characterizes both public and private cloud architectures.

OVERVIEW – AUTOMATING SECURITY SERVICES IN THE SOFTWARE-DEFINED DATA CENTER (SDDC)

As mentioned above, integrated applications, the cloud, increasingly virtualized data centers and dynamic environments have led to a dramatic increase in traffic going East-West, or laterally within the data center. Legacy, hardware-based approaches for securing this traffic are operationally inefficient and cost prohibitive.

Micro-segmentation with VMware NSX addresses the security challenges outlined above. NSX micro-segmentation is built on the following principles:

1. **Automated security service insertion into the network.** A technique called security service-chaining enables security for all traffic in the virtual data center automatically that implicitly protects VM-to-VM traffic in the background. Service chaining is critical because it enables network functions such as security services and load balancing to be deployed on-demand, for specific traffic flows, or at any point in the virtual network through pre-determined and dynamic policies without manual effort or intervention.

2. **Context-aware policies.** To achieve effective micro-segmentation, policies need to be able to leverage the state of each application and their operational context and allow for integration into cloud orchestration and IT tools, such as ticketing systems, directory services, and SDN controllers. This integration enables the system as a whole to learn, create and apply the best policy based on state and context. It also enables secure, scalable deployments of applications in the data center with minimal effort.

3. **Trusted automation and orchestration.** To effectively facilitate automation, APIs need to be secure and trusted. Trust-based APIs enable critical self-service integrations with third-party systems that automate policy changes only within the scope of their privileges protecting the data center as a whole. This means administrators can allow or delegate changes only to specific rules within the policy.

4. **Threat visibility and analysis.** Once a compromised virtual machine is detected, it should be immediately and automatically quarantined with options for remediation. Comprehensive forensic reporting and analytics are necessary to uncover, understand and control traffic trends and security threats both within the datacenter and through the perimeter gateway.

5. **Centralized management.** Data center security management needs to include a unified view into the virtual environment – including virtual machines, VMware vSphere vApps™ and templates – across internal data centers and private or public clouds. This forms a single security management architecture across the organization for all network traffic and systems. These management controls should be flexible enough to also extend to advanced third-party security services which can be integrated into the network platform.

Environments that require advanced, application-level network security capabilities can leverage VMware NSX to distribute, enable, and enforce network security services in a virtualized context. Advanced third-party security services, like Check Point vSEC, integrate directly into the logical networks, providing visibility and safe enablement of virtual machine traffic, alongside continuous content inspection for all threats.

KEY INGREDIENTS FOR ADVANCED SECURITY IN SDDC

- **Check Point Appliances and Virtual Systems** – industry leading security solutions that combine high-performance, multi-core capabilities with fast networking technologies to provide the highest level of security available. Deployed to protect the data center perimeter and core, these security gateways protect traffic entering and leaving the data center.

- **Check Point vSEC for VMware NSX** – purpose-built integrated solution offering advanced protections for east-west traffic within the Software-Defined Datacenter (SDDC). VMware NSX provides the foundation for securing east-west traffic by delivering micro-segmentation through a broad set of virtualized networking elements including logical switches, routers and firewalls. These services are provisioned programmatically within the SDDC when virtual machines are deployed, and move with virtual machines as they move. NSX also offers a platform to insert additional services such as advanced threat protection, allowing Check Point vSEC to be dynamically deployed, distributed and orchestrated through NSX for full SDDC security automation. The combined vSEC with NSX solution delivers best-in-class threat protection and malware prevention for comprehensive security of east-west traffic.

- **Centralized Security Management** – unified across both physical and virtual systems, allows IT to set security policies for both environments from a single interface. This ensures consistent security across all gateways without the expense of separate management consoles. Integrated with VMware NSX and vCenter, policies leveraging NSX and vCenter objects can be utilized across both Check Point vSEC (for East-West traffic inspection) and Check Point gateway appliances (for North-South traffic inspection).

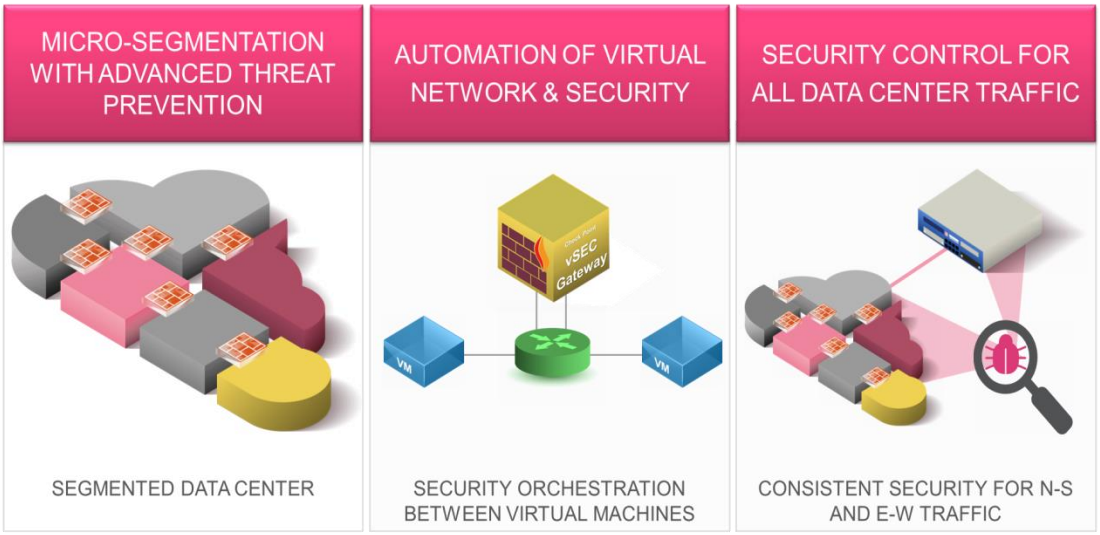

Figure 2: Check Point vSEC addresses the advanced security needs of SDDCs

5 STEPS TO BUILDING ADVANCED SECURITY INTO THE SOFTWARE-DEFINED DATA CENTER

1. **SECURE NORTH-SOUTH TRAFFIC WITH CHECK POINT SECURITY APPLIANCES:** We start with securing the North-South traffic moving in and out of the data center. Check Point appliances with Advanced Threat Prevention enable and effective multi-layered defense against both internal and external threats. For example, if an infected application inside the data center communicates with a Command & Control site, Check Point's anti-bot Software Blade service will catch it.

   Check Point's line of data center appliances and chassis protect high-speed networks with firewall throughput of up to 1 Tbps, with low latency impact, and modular scalability to grow and increase capacity when needed without compromising performance or security.

2. **PROVISION CHECK POINT VSEC:** Check Point vSEC includes 2 components; the vSEC gateway and vSEC controller. The vSEC Gateway is a Service VM (SVM) deployed on every ESX hypervisor that fully integrates with NSX and vCenter. It leverages the VMware NSX API for traffic redirection and inspection, securing traffic between VM's across the virtual network without altering the network topology. The NSX controller enables the automated deployment of vSEC gateways on each host. The NSX Service Insertion Platform enables communication between the vSEC Gateway and the NSX distributed virtual switch.

   The vSEC Controller makes any Check Point Security Management server SDDC-aware through its integration with NSX and vCenter. This enables the vSEC Controller to dynamically adjust security policies and manage any vSEC and physical gateways while providing complete visibility into all data center traffic. The vCenter and NSX integration allows vSEC to dynamically fetch objects into the Check Point Security Management policy, as well as enables vSEC Controllers to simply manage any Security Gateway even if there is no vSEC Gateway deployment.

3. **SECURE EAST-WEST TRAFFIC WITH CHECK POINT VSEC**: As mentioned above, securing inter-data center traffic and devices is critical to all applications. NSX and vSEC can deliver the protections necessary to protect the entire virtual

network at the edge and inside the SDDC. Check Point vSEC integration with NSX goes beyond basic Layer 2-Layer 4 firewall capabilities provided by VMware's Distributed Firewall (DFW). vSEC provides additional Layer 5-Layer 7 security services including Intrusion Prevention (IPS), Antivirus, Antibot, Anti Spam, Application Control, Identity Awareness, and Advanced Threat Prevention.

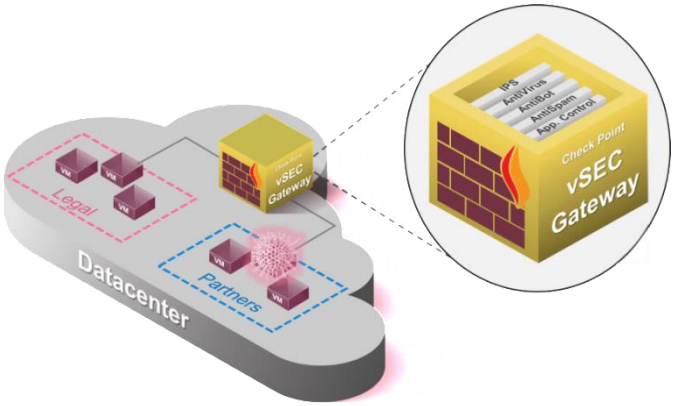

Figure 3: Check Point vSEC blocks lateral threat movement inside software-defined data centers

NSX micro-segmentation enables the coloring and grouping of VM resources that are applied with specific dynamic policies, directing traffic to vSEC virtual gateways. These gateways apply advanced threat protections to the East-West traffic to ensure that a single application or system breach doesn't compromise the entire infrastructure.

4. **CENTRALIZED SOFTWARE DEFINED DATA CENTER MANAGEMENT**: A fully automated software defined data center leverages best-of-breed partner services to extend visibility from individual devices and services to application-aware policies and fine-grained controls that automate the management and security of newly deployed applications and workloads.

   Check Point's SmartConsole management solution can manage both the physical and virtual gateways, as shown in the diagram below. The vSEC Controller integrates with both the NSX Manager and vCenter to learn about the virtual environment and gain contextual awareness. Virtual objects learned by vSEC, such as Security Groups or VMs can then be used in security policies defined via the SmartConsole management client and installed on the vSEC Gateways (service VMs) in each respective ESXi host.

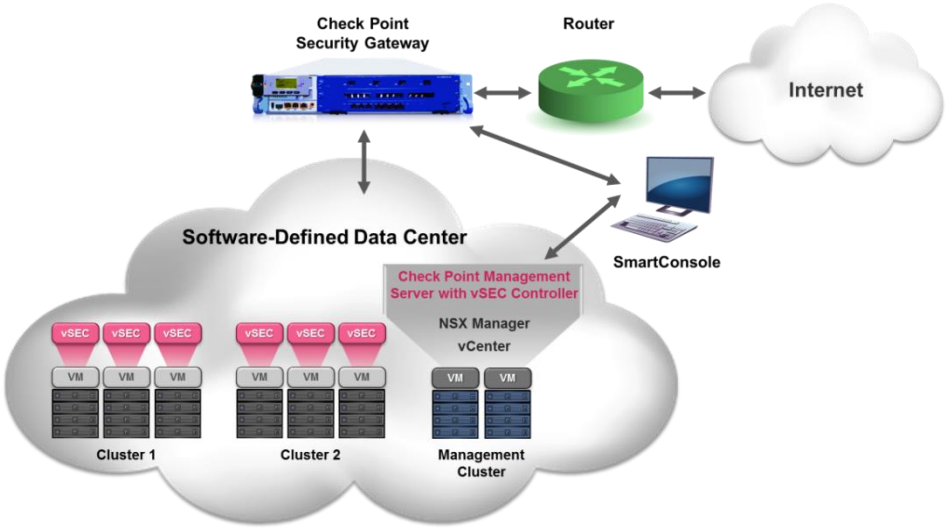

Figure 4: Check Point SmartConsole delivers consistent security management of SDDCs

NSX standard tags enable full-context sharing between VMware NSX, VMware vCenter and the Check Point vSEC management platforms. This ensures that the security groups and Virtual Machine (VM) identities are easily imported and reused within the Check Point security policy and reduces security policy creation time from minutes to seconds. Check Point vSEC is also agnostic to the network topology, and makes use of meaningful object names based on security groups, VM names, vCenter metadata, and data center management related metadata - not IP addresses. This makes it easier to manage policy using less abstract names while providing better visibility.

Context-awareness of these security groups and VMs is constantly maintained so that any changes or new additions, such as IP address, VM location, or NSX group members, for example, are automatically reflected in vSEC. This makes it possible for security protections to be enforced on virtual applications regardless of where they are created or located. This also enables business group or application aware policies that span and consolidate both North-South and East-West network traffic and across both virtual and physical security gateways. That consolidation extends to simplified operations management, including notification and reporting as well. Additionally, predefined Check Point security policy templates automate the security of newly provisioned virtual applications discussed next.

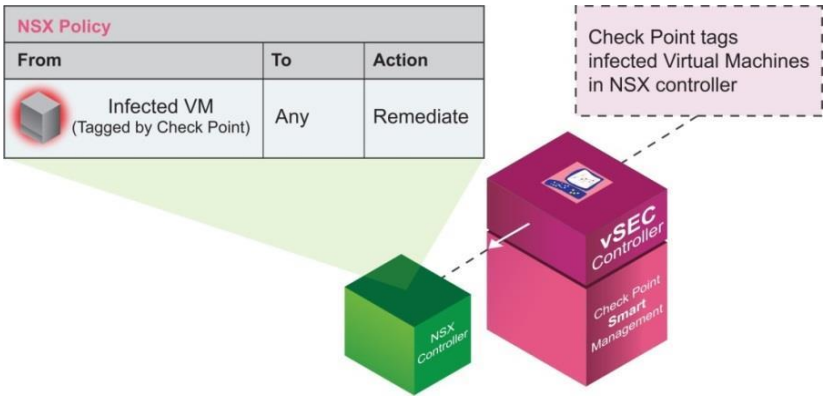

Figure 5: Shared context between vSEC and NSX triggers automatic remediation workflows

Effective monitoring and incident investigation requires robust security management. Enterprises expect their security visibility and monitoring solutions to provide a big picture view of relevant events without having to manually correlate a variety of screens, tools, or other resources.

Check Point smart management solutions centralize and simplify security management for SDDCs. Check Point's SmartDashboard tracks and logs threats across the organization from a single pane of glass, while SmartEvent provides visualizing and correlating of events across the entire data center.

5. SECURE ORCHESTRATION AND AUTOMATION: Check Point vSEC brings native NSX security features and integration together to achieve the best of both worlds - advanced security protection dynamically deployed and orchestrated into the highly automated software-defined data center environment.

   NSX's native security, automation and extensibility framework can be leveraged by Check Point vSEC to dynamically insert, deploy and orchestrate advanced security services inside the SDDC. Network isolation and segmentation inherent to the NSX platform enable feasible micro-segmentation through reproducing network services in software, allowing the SDDC to deliver a fundamentally more secure approach to data security. Policy is enforced at the virtual interface, which transparently follow workloads reducing reconfiguration from days or hours to virtually nothing.

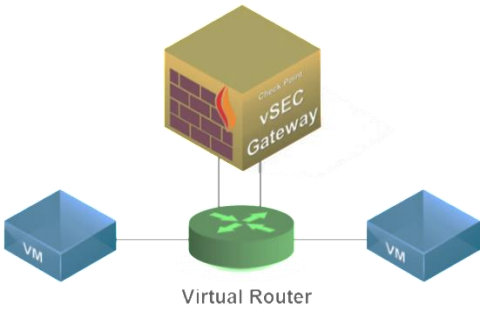

Figure 6: vSEC advanced security can be orchestrated and provisioned automatically between VMs

ENHACING MICRO-SEGMENTATION SECURITY WITH SUB-POLICIES

Micro-segmentation inherently delivers stronger security for the SDDC by being able to fully isolate and segment virtual networks. Sub-policies within micro-segmentation enhance the security of the overall virtual network, allowing organizations to define dedicated policies per micro-segment or delegate specific privileges to different levels of administrators.

Micro-segmentation sub-policies enable security policies that are easily automated to enforce segregation of duties. This unique and powerful ability enables delegation of actions with very fine granularity to advanced threats. This means more control and more effective real-time security in even highly automated environments.

This level of automation and simplification not only applies to the creation of services within the software defined data center, but in their maintenance, expansion or retirement as well. Since all elements are controlled through virtual devices and integrated security policies, management effort is greatly reduced as “physical” changes to policy can be quickly and effectively actuated without touching any physical hardware.

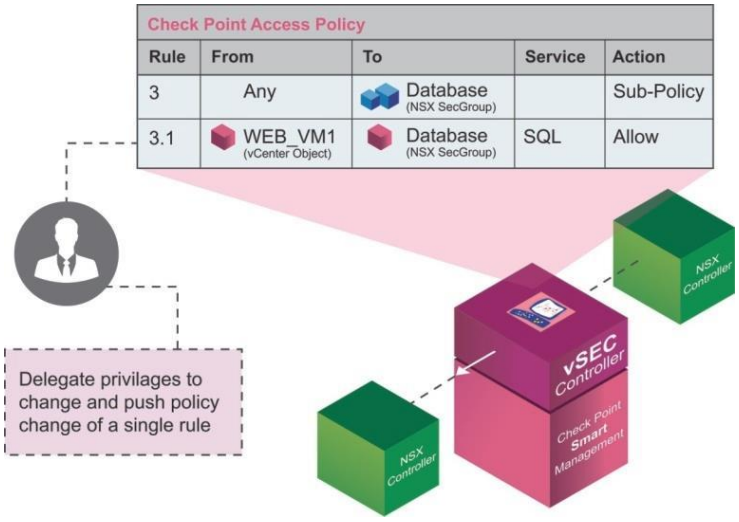

Figure 7: Security sub-policies automatically tied to NSX Security Groups and vCenter objects

SUMMARY

The Software Defined Data Center (SDDC) with VMware NSX network virtualization enables fundamentally more agile, efficient and secure data centers. Working together, VMware and Check Point have integrated their best of breed virtualization and advanced threat prevention technologies to enable the efficient delivery of applications and security assurance to realize the full value of Sofware-Defined Data Center architectures.

The combination of vSEC and NSX logically extends advanced threat prevention further into the data center fabric. This enhances NSX native micro-segmentation capabilities to deliver advanced security services wherever needed. In the event of a breach of a single node or segment of the network, the threat is easily and effectively contained and isolated. This distributed security architecture enables Check Point best-of-breed network security services to be inserted at the vNIC level, for extremely granular control, enhanced visibility and superior threat prevention.

CONTACT US

Worldwide Headquarters | 5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters | 959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com

September 16, 2015