WHITE PAPER – **OCTOBER 2017**

VMWARE NSX WITH CHECK POINT vSEC

Enhancing Micro-Segmentation Security

vmware® | Check Point SOFTWARE TECHNOLOGIES LTD

Table of Contents

Executive Summary	3
VMware NSX Network Virtualization Overview	5
East-West Versus North-South Protections	6
Check Point vSEC for VMware NSX Overview	7
VMware NSX and Check Point vSEC Joint Solution Overview	9
VMware NSX and Check Point vSEC Integration Use Cases	16
Solution Benefits	23
Conclusion	24

Executive Summary

This document is targeted at virtualization, security, and network architects interested in deploying cloud and Software-Defined Data Center (SDDC) architectures based on VMware® network virtualization solutions with Check Point® Software Technologies vSEC advanced threat prevention technologies and services.

VMware pioneered the SDDC to transform data center economics and to increase business agility. The SDDC is rooted in virtualization and comprises server virtualization, storage virtualization, network virtualization, and automation. Although server virtualization has enabled organizations to speed application deployment and reduce data center costs, applications also need fast provisioning of networking and security services, including support for mixed trust level workloads to optimize infrastructure resources without compromising security.

VMware and Check Point have partnered to deliver a fully integrated solution that enables companies to realize the full potential of the SDDC while providing protection against potential vulnerabilities, malware, and other sophisticated threats. The joint solution effectively addresses the key challenges of modern data center networks, including:

- The shift in traffic behavior within the data center from "north-south" to "east-west" as a result of virtualization, shared services, and new distributed application architectures.
- Due to the lack of inter-system and virtual machine (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 VLANs. 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.
- Reliance on perimeter security leads to resource-intensive choke points on the network, impacting data center performance while increasing security complexity.
- Traditional security solutions are not designed to keep pace with dynamic virtual network changes that come with rapid application provisioning.

VMware NSX® is a complete network virtualization platform that makes micro-segmentation economically and operationally feasible. NSX provides the networking and security foundation for the SDDC, enabling automated deployment, orchestration, and scale-out of advanced security services from partners.

Check Point vSEC with advanced threat prevention delivers multilayered defenses to proactively stop malware and zero-day attacks within the SDDC. In addition, Check Point's unified management of virtual and physical gateways simplifies security management across the data center.

The joint VMware NSX and Check Point vSEC solution fully automates the distribution and orchestration of advanced security inside the data center to deliver the same threat protection for east-west traffic that Check Point provides at the data center perimeter gateway. The integrated solution has the following security benefits:

- Advanced security protections seamlessly enforced inside the SDDC.
  - vSEC security with NSX micro-segmentation coupled for advanced protection of east-west data center traffic.
  - Multilayered threat prevention with the highest catch rate against malware, for advanced protection of traffic between virtual machines.
  - Auto-detection, quarantine, and remediation of infected virtual machines.
- Agile security provisioning for the SDDC.
  - Fine-grained Check Point policies dynamically tied to NSX security groups and VMware vCenter® VM objects.
  - Security policy easily segmented into sub-policies servicing micro-segmentation.
  - Security services auto-provisioned in tandem with VMware ESXi™ host deployment and VM movement.
  - Security capacity that is elastically scaled, adjusting to dynamic data center environment.
- Comprehensive threat visibility across the SDDC and hybrid cloud workloads (such as AWS).
  - Unified management with single policy for both virtual and physical gateways simplifies security enforcement.
  - Centralized monitoring and logging ensures comprehensive threat visibility for virtual network–specific reports provide insight into SDDC threat trends.

VMware NSX Network Virtualization Overview

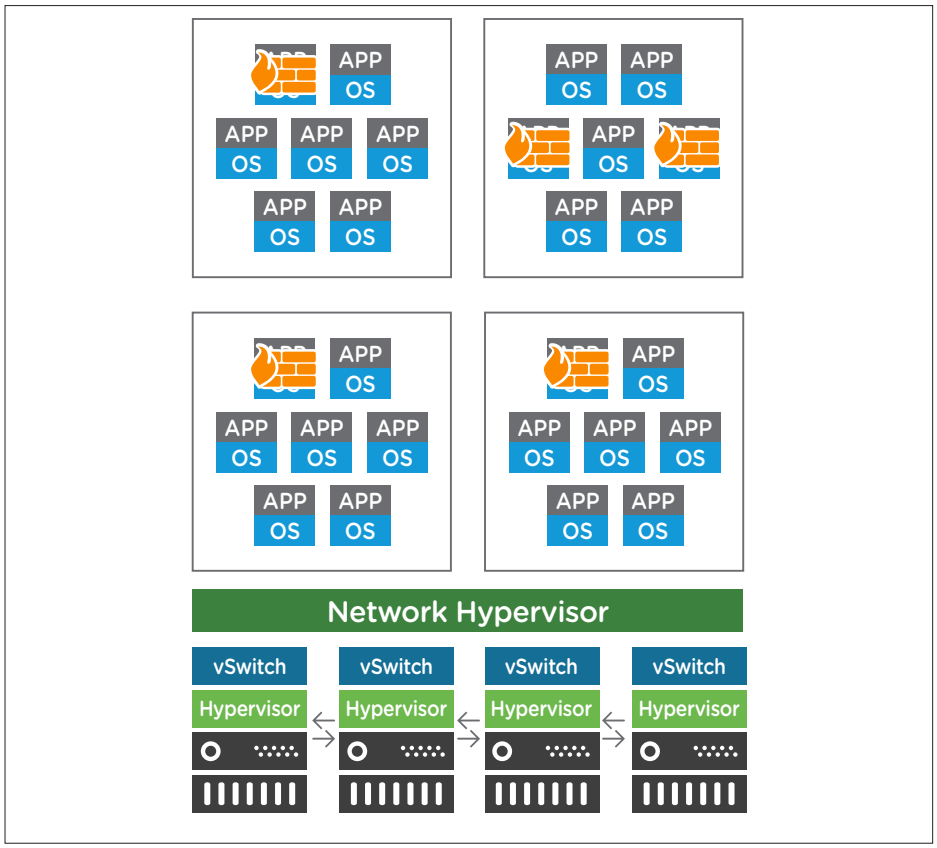


Figure 1. VMware NSX Overview

VMware NSX network virtualization decouples network resources from the underlying hardware. An abstraction layer makes the network a flexible pool of transport capacity that can be allocated, utilized, and repurposed on command. Virtual networks are built from logical switches, routers, firewalls, load balancers, and VPNs to connect workloads as needed, while the underlying physical network serves as a simple packet forwarding backplane. Network and security services can be consumed programmatically and automatically change as they follow virtual machines as they move within the data center.

Key to this is security policy based on VM characteristics or user-defined tags, to describe complex policy in a concise form while allowing changes dynamically as applications or security posture change. Examples include an application scaling out to additional VMs, a change of AD user logged into a VM, or a partner solution tagging a VM as vulnerable or infected. That partner solutions such as vSEC can then also act on these dynamic changes illustrates the power of NSX.

East-West Versus North-South Protections

The trend in enterprise IT to move from a hardware-centric to an application-centric network model enables businesses to streamline processes and improve end-user experiences, all while enhancing their competitive positioning. At the heart of this new infrastructure is the ability to treat all core tenants—servers, storage, and the network—as a pool of resources called upon at will to quickly provision new applications and services. However, this model defies traditional security capabilities, exposing modern data centers to a host of new challenges.

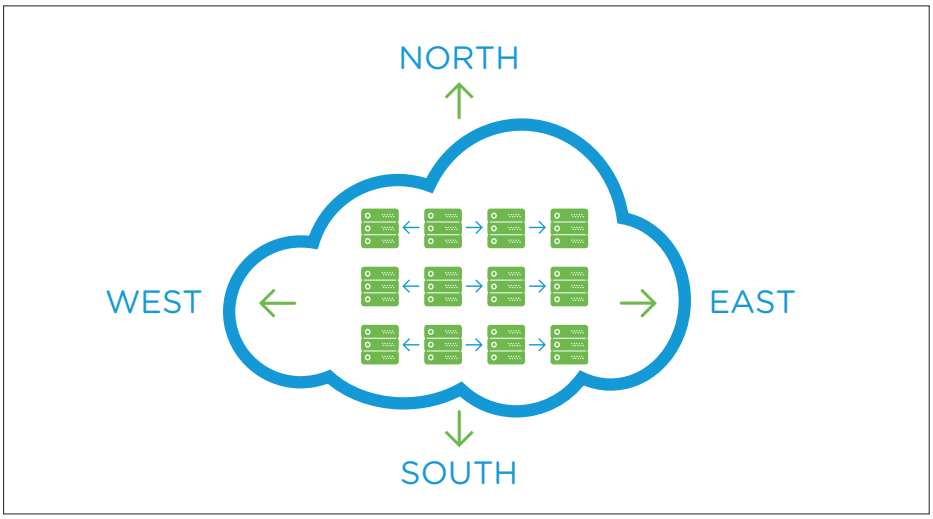


Figure 2. Changing Traffic Patterns Means More Data Now Moves East-West

Security has traditionally been focused on protecting perimeter, or north-south, traffic going into and out of the data center. But the dissolving network perimeter means there are multiple entry points into corporate data center networks—not just the "traditional" north-south gateway. In addition, server and network virtualization causes more and more data to move laterally, or east-west, within the data center. As more data is contained within the data center and no longer crossing the north-south perimeter defenses, security controls are now blind to this traffic—making lateral threat movement possible. Any threat introduced into the data center now can move and infect other hosts unimpeded, because traffic isn't being inspected by "traditional" security measures.

With the rising number of applications being deployed in modern data centers, hackers have a broader choice of targets. Compounding this challenge is the fact that traditional processes for managing security are labor intensive and slow. Applications are now being created rapidly and evolving more quickly than static security controls, processes, and workflows can keep pace with.

Strong perimeter security is still an important element to an effective defense-in-depth strategy, but perimeter security alone offers minimal protections for virtualized assets within the data center. It is difficult to protect data and assets that aren't known or seen. To address these challenges, a new security approach is needed—one that effectively brings security inside the data center to protect assets, data, and workloads against advanced threats, and enhances native micro-segmentation of the SDDC.

Micro-segmentation works by grouping resources within the data center and applying specific security policies to the communication between those groups. The data center is essentially divided up into smaller, protected sections (segments) with logical boundaries that increase the ability to discover and contain intrusions. However, despite the separation, application data must cross micro-segments to communicate with other applications, hosts, or storage devices. This makes lateral movement still possible, since perimeter security controls are not able to inspect the traffic contained within the data center for malicious payloads.

Solutions such as Check Point vSEC complement micro-segmentation and provide comprehensive threat prevention security to protect east-west traffic within the data center, and can provide the foundation for automating the quarantine of infected machines for remediation. This puts required protections inside the SDDC, securing assets and valuable data from attacks. By deploying advanced security solutions, organizations can better protect their data centers from undetected breaches and sophisticated threats.

Check Point vSEC for VMware NSX Overview

Network virtualization has created a shift in traffic behavior. Now, more and more traffic is going east-west in the data center, creating new security challenges. With few controls to secure this east-west traffic, threats can travel unimpeded once inside the data center. As a result, Check Point and VMware have teamed together to deliver advanced security services to prevent the lateral spread of threats within SDDCs, and to provide the visibility and control to effectively manage security in both physical and virtual environments—all from a single unified management solution.

Network isolation and segmentation inherent to the NSX platform enable feasible micro-segmentation, allowing the SDDC to deliver a fundamentally more secure approach to data security. Policy is enforced at the virtual interface, and security policies follow workloads. In addition, the native NSX security capabilities, automation, and extensibility framework can now be leveraged by vSEC to dynamically insert, deploy, and orchestrate advanced security services inside the SDDC for enhanced protection against malware and other threats.

Since 1993, Check Point has been dedicated to providing customers with uncompromised protection against all types of threats, reducing security complexity, and lowering total cost of ownership. Check Point is committed to staying focused on customer needs and developing solutions that redefine the security landscape today and in the future. The vSEC for NSX solution provides industry-leading threat prevention security to keep SDDCs protected from the most sophisticated attacks and to prevent the lateral movement of threats. Fully integrated multilayer security protections include the following:

- Stateful firewall, Intrusion Prevention System (IPS), anti-virus, and anti-bot technology protect data centers against lateral threat movement.
- IPsec VPN allows secure communication into cloud resources.
- Application control prevents application layer denial-of-service (DoS) attacks.
- SandBlast Zero-Day Protection sandbox technology provides protection against unknown malware, zero-day attacks, and other sophisticated threats.

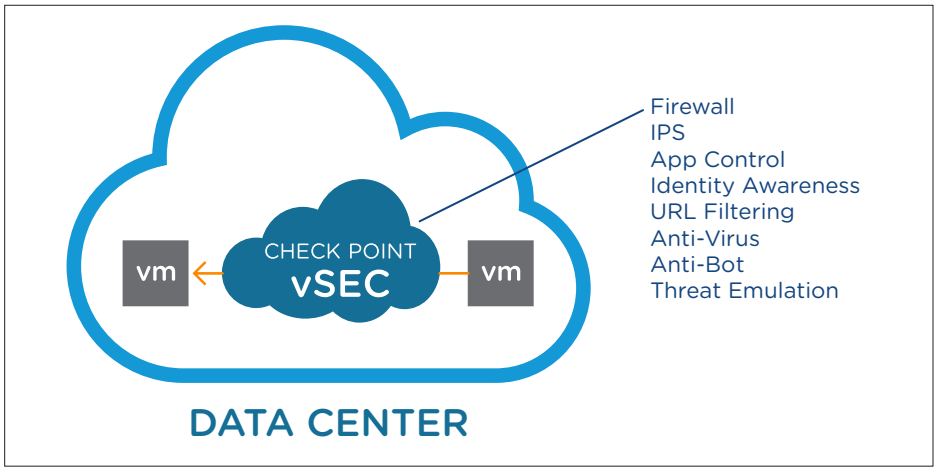


Figure 3. Check Point vSEC Complements Native NSX Micro-Segmentation to Deliver Security Protections Within the SDDC

The integration of vSEC with NSX brings together the best of both worlds—the economic and technological feasibility of micro-segmentation with advanced security protections dynamically deployed and orchestrated into an SDDC environment. vSEC for NSX delivers multilayered defenses to protect east-west traffic within the VMware deployed data center. In addition, vSEC transparently enforces security at the hypervisor level and between virtual machines, automatically quarantines infected machines for remediation, and provides comprehensive visibility into virtual network traffic trends and threats across the SDDC and hybrid cloud environments.

VMware NSX and Check Point vSEC Joint Solution Overview

VMware Components for Delivering the SDDC

The VMware Software-Defined Data Center consists of the following:

- VMware vSphere® and vCenter – x86 hypervisor to abstract compute resources from the physical server. With vCenter for management, high availability, and distribution of load across hosts, VMware vSAN™ for pooling local host storage, vStorage APIs for Storage Awareness (VASA) for storage abstractions, and rich APIs for extensibility.
- VMware vRealize® Suite – vRealize Automation™ for cloud automation, vRealize Operations™ for operational management and capacity planning, vRealize Log Insight™ for log analysis, and so on.
- VMware NSX – Abstracts networking from the physical hardware and provides common network services including routing, firewall, load balancing, and VPN. A distributed router and firewall run within the kernel on the hosts, offering a cost-effective high-performance scale-out architecture. NSX enhances security by providing a firewall at the NIC of every VM for zero trust micro-segmentation. NSX includes APIs for third-party extensibility: NetX for traffic steering, EPSEC for guest introspection, and a public northbound API for policy management.

Check Point Components for Delivering Advanced Security in the SDDC

- Check Point Virtual Appliances and Virtual Systems – Industry-leading security solutions that combine high-performance, multicore 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 Gateway for VMware NSX – A purpose-built integrated solution offering advanced protections for east-west traffic within the SDDC. The vSEC gateway is a service virtual machine (SVM) that is deployed per virtual host by VMware NSX Manager™. 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 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.

- vSEC Controller – 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, and enables vSEC Controllers to simply manage any security gateway even if there is no vSEC gateway deployment. The integration also allows the SDN controllers to provision vSEC gateways when needed, orchestrate new applications with security policy templates, update policies automatically, and even quarantine infected applications.
- Centralized Security Management Server (SMS) with SmartConsole – 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. Because of integration 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).

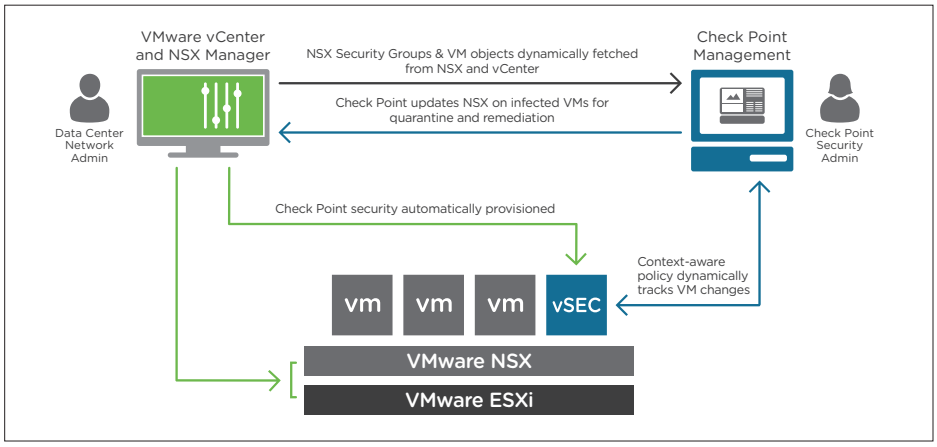


Figure 4. Check Point vSEC for VMware NSX Solution Components

Integration of Check Point vSEC with VMware NSX

The VMware NSX network virtualization platform provides L2-L4 stateful firewalling features to deliver segmentation within virtual networks. Environments that require advanced threat prevention and application-level security capabilities (L4-L7) can leverage NSX to distribute, enable, and enforce advanced network security services in a virtualized network context. NSX distributes network services to form a logical pipeline of services applied to virtual network traffic. vSEC for NSX integrates directly into this logical pipeline, enabling comprehensive threat prevention and complete visibility of VM traffic.

Another powerful benefit of the integrated NSX and vSEC solution is the ability to build policies that leverage NSX service insertion, chaining, and steering to drive service execution in the logical services pipeline, based on the result of other services, making it possible to coordinate otherwise completely unrelated network security services from multiple vendors.

Version Requirements

The VMware NSX and Check Point integration works with the following versions:

- Check Point GAIA OS R77.30 or later
- VMware vSphere 6.0, 6.5
- VMware vCenter Server® 6.0 or later
- VMware NSX Manager 6.2.x
- VMware NSX Manager 6.3.x

Provisioning Check Point vSEC

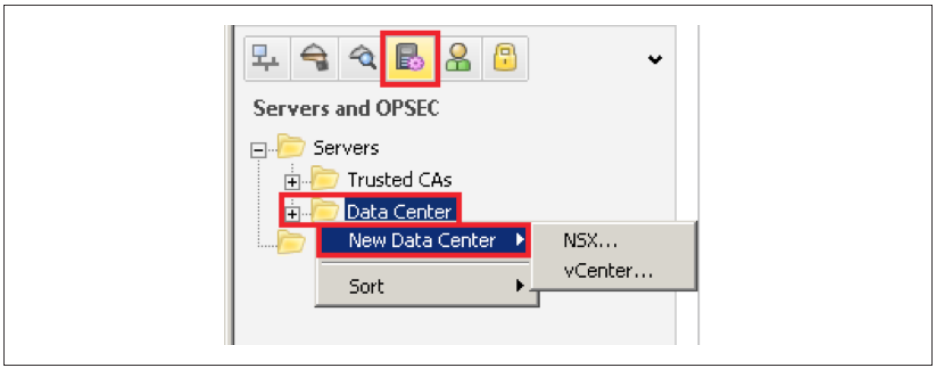
vSEC includes two components: the vSEC gateway and the vSEC Controller. The vSEC gateway is an SVM deployed on every VMware ESX® hypervisor that fully integrates with NSX and vCenter. It leverages the VMware NSX API for traffic redirection and inspection, securing traffic between VMs across the virtual 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, and enables vSEC Controllers to simply manage any security gateway even if there are no deployed vSEC gateways.

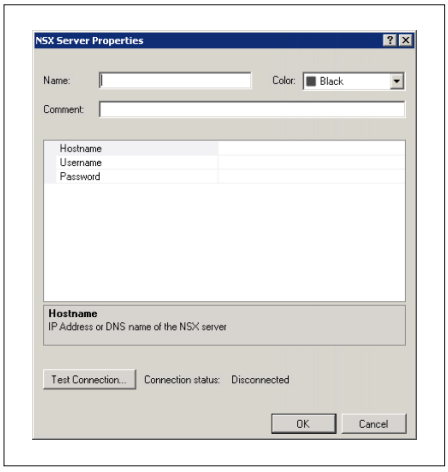
Defining NSX and vCenter Integrations with the Check Point vSEC Controller

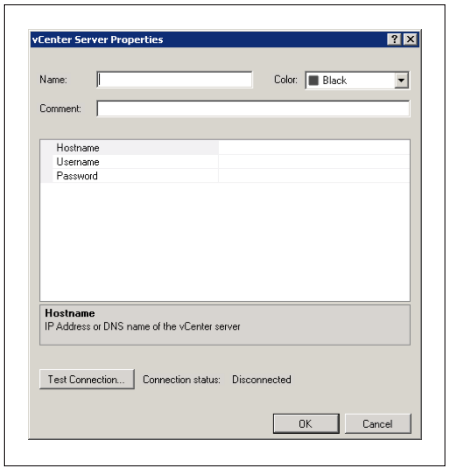
The first step in deploying the integrated solution is to define NSX Manager information (IP/host name and credentials) within the vSEC Controller so a vSEC gateway can be registered as an advanced NSX service. This registration process provides the necessary data to deploy vSEC as a service. The registration also allows NSX to update the vSEC Controller dynamically with all changes to the SDDC.

For R77.30, in the SmartConsole or SmartDashboard, create a data center server object for VMware vCenter integration. This is done within the Servers and OPSEC view; simply right-click on Data Center, go to the New Data Center menu, and select the VMware Server™ type NSX or vCenter.



Next, fill in the required fields for either NSX or vCenter integration:





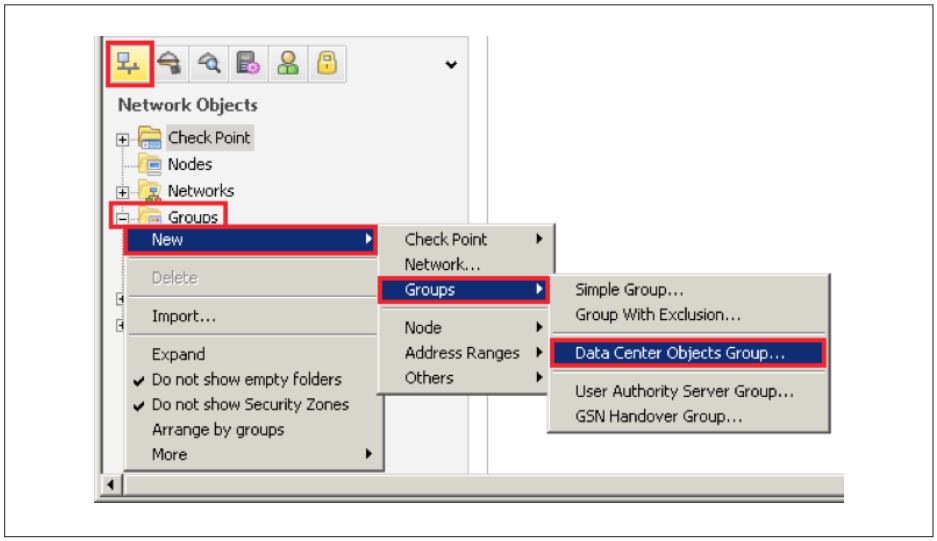
Note:

- In VMware vCenter, all roles must have at least read-only permission.
- In VMware NSX, define an Enterprise Administrator role for Check Point threat prevention tagging to work. Define at least an NSX Administrator role in order to register and deploy the vSEC service in an NSX environment (vSEC Gateway Hypervisor mode).

Next, test the connection to ensure proper integration by clicking Test Connection. If the configured VMware Server was not approved before, then a certificate window opens. If you did not confirm the certificate before, click Trust. Once the connection status changes to green "Connected," click OK to complete the integration.

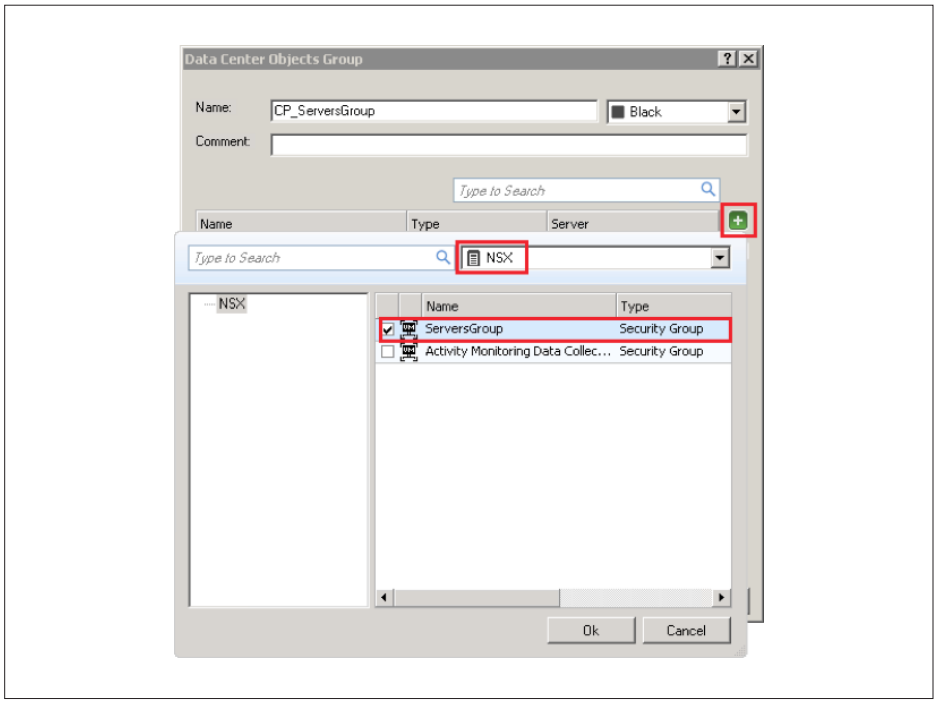
Defining Data Center Objects and Associations Within the vSEC Controller

The next step is to define data center objects and associations for all SDDC objects and groups. In the SmartDashboard, create an object of Data Center Objects Group to easily manage rules that are related to the selected data center servers. Start by navigating to the Network Objects view in the lower-left pane of the SmartDashboard, right-click Groups, select the New menu, select the Groups drop-down, and click Data Center Objects Group.

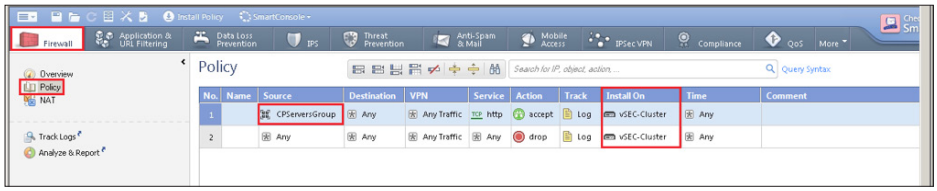


Note: When you add one Data Center Objects Group to a rule, all the associated objects are added.

Next, enter a name for the new Data Center Objects Group. Click the green picker icon [+] and select the VMware NSX server. Then select the relevant security group and click OK.



The vSEC Controller is now ready to use the Data Center Objects Group in security rules. To enable the Data Center Objects Group in security rules, navigate to the vSEC Controller Firewall tab, and in the upper-left pane, click Policy. Next, in the relevant rules section, change Source or Destination to the Data Center Objects Group object. Finally, install the policy.



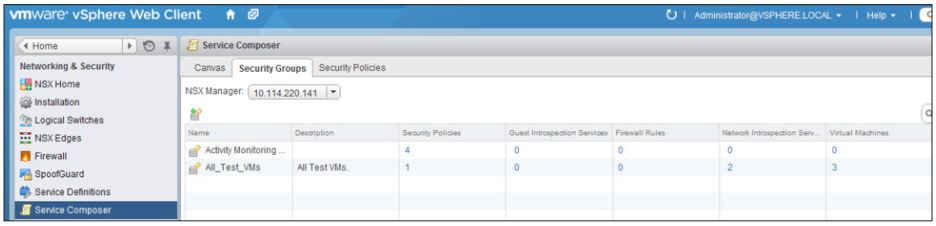
Traffic Steering to vSEC Gateways for L4-L7 Protections

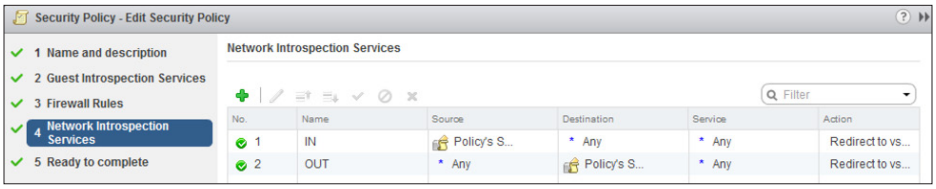
Traffic steering from one VM to a vSEC gateway is performed internally by leveraging the NSX shared memory space. Using the NSX redirect policy, the security team can granularly define traffic flows that will be sent to the vSEC gateway for enhanced security inspection and enforcement.

Network traffic comes from the User Mode NetX API into the vSEC gateway. The API places traffic to be inspected by vSEC in shared memory. In vSEC, the gateway secure network dispatcher (SND) receives the traffic and forwards it to a gateway firewall (FW) Instance. The vSEC FW performs advanced security services according to firewall policies and then returns the traffic to the vSEC SND. Finally, the vSEC SND sends traffic over the VMware API via the NSX DFW (Distributed Firewall).

Traffic redirection (as defined by the NSX security policy network introspection services) can be defined in the following ways:

- From security group (SG-1, for instance) to security group (SG-2, for instance)
- From any source to security group (SG-1, for instance)
- From security group (SG-1, for instance) to any destination





VMware NSX and Check Point vSEC Integration Use Cases

Use Case #1: Advanced Security Services for Multizone Virtual Environments (Zone-Based Segmentation)

This use case is ideal for customers that require advanced security services (URL filtering, application control, IPS/IDS, anti-virus, etc.) to protect workloads connected to virtual environments. For this use case, an SDDC is created and segmented with three internal zones:

- Dev Zone – Used for developers to create, test, and validate new enterprise apps
- Prod Zone – Used for all applications running under production in the SDDC
- PCI Zone – Used for VMs that require access to customer personal information and payment card identification

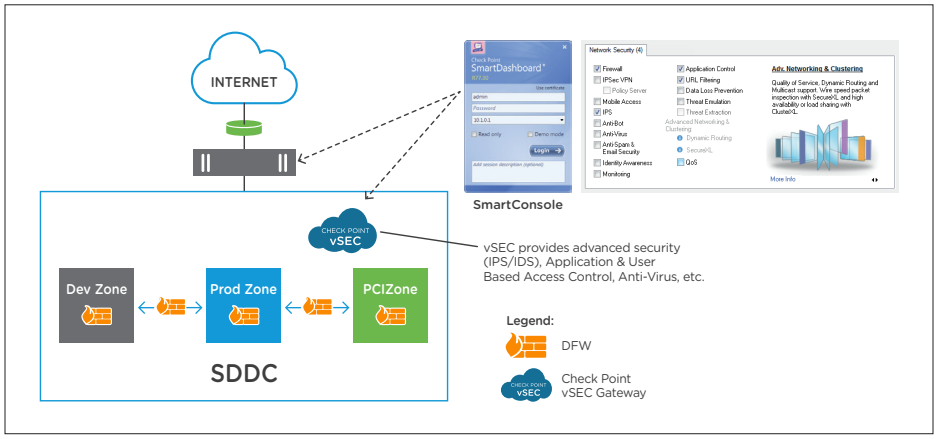


Figure 5. Zone-Based Segmentation with vSEC

Traffic from Dev Zone to Prod Zone is protected by the SDDC DFW. Traffic from Prod Zone to PCI Zone is redirected and protected by vSEC, leveraging Check Point advanced threat prevention security features such as: anti-virus, Intrusion Prevention System (IPS), and advanced malware prevention. vSEC provides vital security features for complying with PCI DSS requirements.

Implementing this use case requires the creation of the following three security groups:

DATA CENTER SECURITY GROUP NAME	SDDC ASSETS INCLUDED
SG-DEV-ZONE	All logical switches used in Dev Zone (or all virtual switches port-group)
SG-PROD-ZONE	All logical switches used in Prod Zone (or all virtual switches port-group)
SG-PCI-ZONE	All logical switches used in PCI Zone (or all virtual switches port-group)

To provide enhanced security protections for traffic between Prod Zone and PCI Zone, traffic needs to be redirected to vSEC. The following is a typical security policy example for this scenario:

SECURITY POLICY	SDDC ASSETS INCLUDED	APPLIED TO
Dev_to_Prod	Source: SG-DEV-ZONE Service: Any Action: Do not redirect	SG-DEV-ZONE
Prod_to_PCI	Source: SG-PROD-ZONE Service: Any Action: Redirect to vSEC	SG-PROD-ZONE

In this scenario, the security groups defined by NSX are automatically absorbed and available to the vSEC Controller to leverage in policies, logging, and reporting. This level of integration dramatically simplifies management of advanced security services within the SDDC and enables the rapid deployment of new services or the logical expansion of existing services.

Use Case #2: Secure Web DMZ with Advanced Threat Prevention Within a Segmented SDDC

In this scenario, tiered applications or services are buffered by web demilitarized zones (DMZs). At the ingress and egress ports of each web DMZ, vSEC gateways are deployed to protect any external facing services while allowing hosts to communicate with both the internal and external SDDC network.

The following diagram shows a high-level view of this example topology. In this topology, tiered applications are clustered to a common transport zone, meaning any logical switch can be expanded to any host within that cluster. Even if WEB DMZ 1 and WEB DMZ 2 are created on different hosts, they are connected to the same L2 domain. To enable communication between WEB, APP, and DB tiers, the logical routing function of NSX is leveraged so that a single logical router instance connects all logical switches.

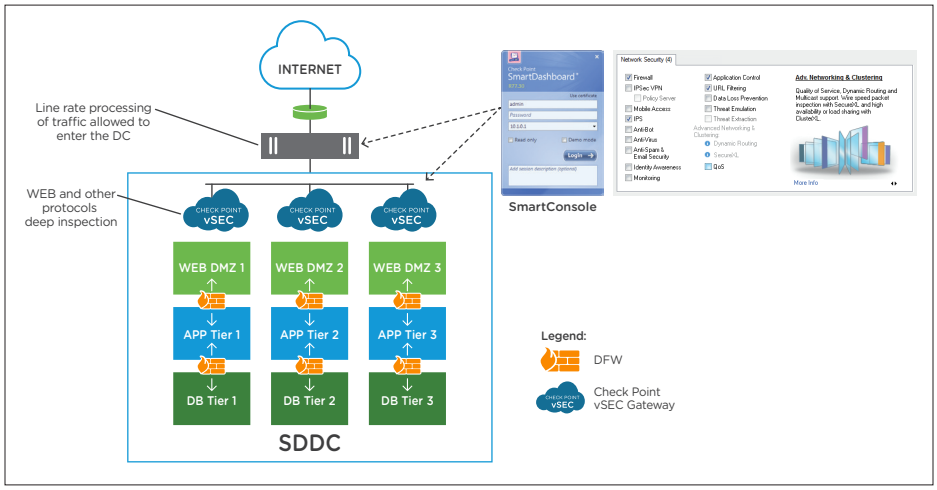


Figure 6. Secure Virtual DMZ with vSEC

In a typical three-tier application topology, traffic needs to flow from web-facing services to application servers and databases. Notice in this topology the Distributed Firewall (DFW) module operates natively between the various tiers to enforce SDDC micro-segmentation rules. The DFW is a key NSX element for traffic redirection to the vSEC gateways.

In terms of traffic steering, the following traffic configurations will be applied:

- From the DB tier to APP tier, traffic is protected by the DFW.
- From the APP tier to WEB DMZ, traffic is protected by the DFW.
- From the WEB DMZ, because it has connections external to the SDDC, traffic is directed to vSEC for enhanced threat protection.

This is not an exhaustive list and depends largely on customer traffic engineering.

Once traffic reaches the vSEC security gateway, security policies defined on the vSEC Controller dictate the defined enforcement action for the identified application.

vSEC provides comprehensive security protections to keep web-facing applications and services secured from even the most sophisticated threats. Key web-facing protections of vSEC include Next-Generation Firewall, Intrusion Detection and Intrusion Prevention System (IDS/IPS), web filtering, anti-virus, anti-bot, identity control, and Threat Emulation.

To implement this use case scenario, we need to create the following security groups (SGs):

DATA CENTER SECURITY GROUP NAME	SDDC ASSETS INCLUDED
SG-WEB-DMZ-XX*	All logical switches used in the WEB tier (or all virtual switches port-group)
SG-APP-XX*	All logical switches used in the Application tier (or all virtual switches port-group)
SG-DB-XX*	All logical switches used in the Database tier (or all virtual switches port-group)
*Indicates specific application/service security group (i.e., 1, 2, or 3 as in the diagram above)	

Security groups by nature are dynamic constructs. As defined in the above table, any VM (existing or new) connected to the WEB logical switch is automatically part of SG-WEB-DMZ group. The same applies for all VMs connected to the APP or DB logical switches.

Now, we are ready to configure our security policy to add a layer of protection beyond the DFW to our WEB DMZ tier:

SECURITY POLICY	NETWORK POLICY	APPLIED TO	COMMENTS
WEB DMZ_to_ INTERNET	Source: Any Destination: WEB-DMZ Service: Any Action: Redirect to vSEC	SG-WEB-DMZ	Any traffic from INTERNET to WEB-DMZ tier is redirected to vSEC

Note: The vSEC security policy allows for a more granular configuration for traffic redirection and type of advanced protections desired. For example, instead of redirecting all traffic, you can define particular traffic services—such as the need for only HTTPS traffic inspection by vSEC, simply by enabling inspection of TCP service port 443. Likewise, security protections are easily tailored to suit the exact needs of any external-facing web service or DMZ by selecting the desired features from the Network Security section of the vSEC Controller gateway window. Security protections are enabled per gateway or cluster.

Use Case #3: Threat Prevention Tagging with vSEC Gateways in the SDDC

Threat prevention tagging automatically assigns security tags to data center objects based on analysis conducted by vSEC as well as object group affiliation. This enables the use of dynamic security groups in security policy rules.

When a threat from an infected VM reaches a vSEC gateway and is denied entry, it is tagged as an infected VM. The tagging information is shared with the NSX Manager via the API integration of the vSEC Controller. This level of integration between NSX and vSEC allows for the automated reclassification of VMs to trigger additional functions such as remediation workflows that can be preconfigured within the NSX controller.

Using either use case #1 or use case #2 above, this feature can enable automated workflows to ensure that an infected VM is immediately identified, quarantined, remediated, and placed back into service—without requiring any manual intervention. In doing so, security, engineering, and operations teams along with other DevOps functions are aligned to the dynamic needs and nature of the SDDC.

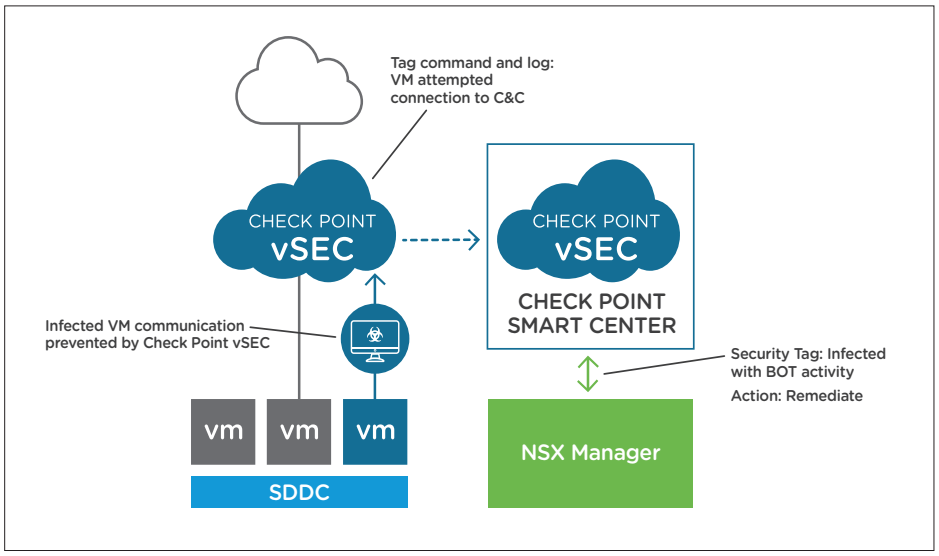


Figure 7. vSEC Threat Prevention Tagging Triggers Auto-Remediation Workflows in the SDDC

Check Point supports threat prevention tagging for anti-bot and anti-virus services on the vSEC gateway or cluster. To perform threat prevention tagging, it is important to ensure that the anti-bot and anti-virus functionality is enabled on the appropriate vSEC gateway or cluster. When it is activated, the cluster automatically tags infected VMs in the NSX Manager Server. The following security tags are available from vSEC:

- Default Anti-Bot Security Tag: Check_Point.BotFound
- Default Anti-Virus Security Tag: Check_Point.VirusFound

When security tags are configured, you can create policy rules based on the security groups containing those tags to augment existing policies as established in the use cases above. vSEC supports the following advanced tagging options:

- Show Activated Gateways – Lists the activated clusters and the status of each vSEC for NSX Gateway.
- Modify Anti-Bot Security Tag – Enables or disables the tagging for the anti-bot blade and changes the security tag.
- Modify Anti-Virus Security Tag – Enables or disables the tagging for the anti-virus blade and changes the security tag.
- Modify White List – IP addresses listed in the White List are not tagged.
- Create New Security Tag – Creates a new security tag in the NSX Manager Server.
- Update Data – When you add a new ESX server to a cluster, vSEC for NSX Gateway automatically updates the threat prevention tagging data within 15 minutes. Select this option to manually update the data on the new vSEC for NSX Gateway.

For added security and convenience, Check Point's security management API allows for granular privilege controls. Edit privileges can be scoped down to a specific rule or object within the policy, restricting what an automated task or integration can access and change. The ability to automatically provision trusted connectivity gives security teams the confidence to automate and streamline the entire security workflow. In addition, predefined Check Point security templates help automate the security of newly provisioned virtual applications.

Solution Benefits

The VMware NSX and Check Point vSEC integration provides numerous benefits, including the following:

- **Advanced security seamlessly embedded into SDDC** – Dynamic insertion, distribution, and orchestration of vSEC into SDDC environments provide the same advanced security protections for east-west traffic as Check Point physical gateways provide for north-south traffic.
- **Feasible, scalable, and secure micro-segmentation** – Virtual networks are created in isolation and remain in isolation unless specifically connected. Segmentation is related to isolation but is applied within a multitiered virtual network. Now, micro-segmentation can include the insertion of advanced services from third-party partner solutions such as Check Point vSEC. The NSX service composer can chain vSEC for securing traffic among virtual machines of different security groups for in-line, line-rate advanced threat prevention security within the SDDC. The advanced security services of vSEC with NSX micro-segmentation ultimately deliver better security throughout the SDDC without complex VLAN sprawling or hairpinned traffic configurations that create choke points for securing traffic inside the data center.
- **Automated deployment and scale-out of vSEC** – You can rapidly extend NSX micro-segmentation with vSEC advanced threat prevention including firewall, IPS, anti-virus, anti-bot, anti-spam, URL filtering and application control to deliver comprehensive protection against sophisticated malware and zero-day attacks for east-west traffic. You can also autoscale vSEC security services by simply adding additional network hypervisors.
- **Automatic isolation to prevent the lateral spread of threats inside the SDDC** – Advanced integration with NSX allows vSEC to share security context via threat prevention tagging. When an infected VM is detected, vSEC can automatically update the security tag within NSX. NSX can then quarantine the VM and trigger other services to remediate the infected VM. Regardless of whether the infected VM is detected by a physical (perimeter) Check Point gateway or a vSEC gateway, the vSEC Controller automatically updates NSX with the proper threat prevention tag.
- **Context-aware and topology-independent security policies** – All NSX security group objects and vCenter VM objects are dynamically fetched by the vSEC Controller. Check Point security policies can then use these objects for contextually aware security, instead of relying on IP addresses. Check Point security policy is dynamically updated when a new VM joins a security group or when a VM changes its IP address. The same policy with NSX security groups and vCenter policy objects can also be applied on Check Point perimeter security gateways as well as vSEC gateways. Check Point policies can also use dynamic objects from other IT services such as Active Directory and Radius for enhanced contextual awareness. Keep in mind that this contextual awareness can also extend to public and hybrid cloud environments.

- Granular assignment of administrative privileges to simplify security operations – The vSEC Controller enables correlation between NSX security groups and Check Point sub-policies to enable granular administrative privileges. Using the granular Check Point sub-policies construct, administrators and other automated actions can be granted permission to change only rules or commit changes within a specified sub-policy or specific rule of a policy, thus not affecting the entire security policy. Check Point sub-policies also allow multiple rule changes to occur simultaneously. This provides the foundation for IT to confidently automate specific services by using scoped privileges to change rules that affect only a single virtual application, dramatically simplifying security operation within the SDDC.
- Security keeps pace with dynamic changes in SDDC – SDDC IT administrators no longer need to guess how much network security capacity is needed. NSX automatically deploys and provisions vSEC gateways on all ESX cluster members, even when a new ESX host joins the cluster. Additionally, vSEC continues securing VMs as they migrate around the SDDC without any downtime. NSX automatically updates vSEC for any vSphere vMotion® or Distributed Resource Scheduler™ (DRS) event.
- Consistent visibility and control across physical and virtual networks – Check Point SmartEvent offers centralized monitoring and logging for east-west and north-south data center traffic. Traffic logs, reports, and security events include information about NSX security group and VM attributes. Check Point security policies are enriched with NSX context to ensure that all gateways—both vSEC and physical—stay up-to-date on any changes within the SDDC.

Conclusion

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 SDDC 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.

This joint solution enables enterprises to have fast, simplified provisioning and deployment of Check Point's advanced security services in an SDDC, enabling customers to have the same level of security for east-west traffic inside the data center as Check Point provides at the perimeter gateway. Security teams will be better able to collaborate with network teams and maintain full control and visibility across both physical and virtual networks.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com