Check Point vSEC for VMware NSX

Dynamic orchestration of advanced threat prevention for all data center traffic

VMware NSX

is the industry's leading network virtualization platform that delivers the same benefits to the network that VMware delivered for compute. Virtual networks can be programmatically managed and created on demand. The result is dramatically simplified network and security operations, fast provisioning of networking and security services - from weeks to minutes, and fundamentally better data center security.

Check Point vSEC for VMware NSX delivers advanced threat prevention security for VMware NSX software defined data centers. Designed for the dynamic requirements of VMware NSX deployments, vSEC provides automated security provisioning coupled with the most comprehensive protections. Fully integrated security features include: Firewall, IPS, Application Control, IPsec VPN, Antivirus, Anti-Bot and award-winning SandBlast sandboxing technology.

Centrally managed by the gold-standard in security management, vSEC provides consistent security policy enforcement, full threat visibility across physical and virtual data center network environments.

MODERN DATA CENTER SECURITY OVERVIEW

Organizations today demand an agile data center environment to reduce IT costs, increase business agility and remain competitive. At the same time, integrated applications, increasingly virtualized data centers and dynamic environments have led to a dramatic increase in network traffic going east-west, or laterally within the data center.

When it comes to security, the focus has mainly been on protecting the perimeter, or north-south traffic, going into and out of the data center. There are few controls to secure east-west traffic inside the data center. This presents a security risk where threats can traverse unimpeded once inside the data center.

Traditional security approaches to this problem are manual, operationally complex and slow, and are unable to keep pace with dynamic virtual network changes and rapid virtual application provisioning.

AUTOMATED ADVANCED FOR THE SOFTWARE-DEFINED DATA CENTER

The Software Defined Data Center (SDDC) is defined by three pillars – virtualized compute, virtualized storage and virtualized network, and NSX provides the network virtualization component. NSX provides the equivalent of a hypervisor for the network, and reproduces all networking and security services including switching, routing, firewalling, load balancing, etc., entirely in software.

NSX native security capabilities, automation and extensibility framework are leveraged by Check Point vSEC to dynamically insert, deploy and orchestrate advanced security services inside the Software-Defined Data Center. 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.

The integration of Check Point vSEC with NSX brings together the best of both worlds - advanced security protection dynamically deployed and orchestrated into a software-defined data center environment.

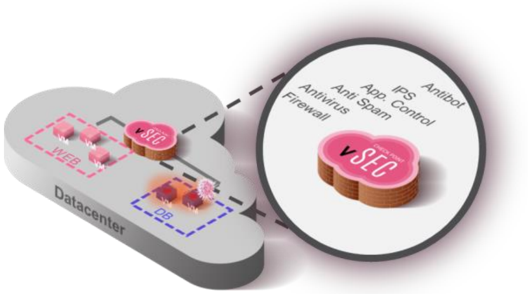
Comprehensive Threat Prevention

vSEC for VMware NSX provides industry-leading threat prevention security to keep data centers protected from lateral movement of threats and the most sophisticated attacks. Fully integrated multi-layer security protections include:

- **Stateful Firewall, Intrusion Prevention System (IPS), Antivirus and Anti-Bot** technology to protect data centers against lateral movement
- **SandBlast Zero-Day Protection** sandbox technology provides the most advanced protection against malware and zero-day attacks
- **Application Control** to help prevent application layer Denial of Service (DoS) attacks and by that protect the software defined data center
- **Data Loss Prevention** protects sensitive data from theft or unintentional loss

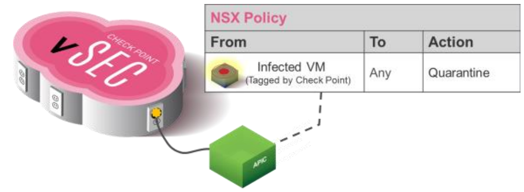
Ubiquitous Security Enforcement

Check Point vSEC integration with VMware NSX allows dynamic insertion of advanced security protection between workloads enabling distributed enforcement at every virtual interface. The integration automates and simplifies the provisioning of vSEC gateways into the NSX virtual fabric to protect east-west traffic from lateral movement of threats enabling feasible micro-segmentation. NSX basic firewalling capability can be extended with Check Point's vSEC, whose layered security policy approach makes it easy to segment a policy, and provide granular rule definitions specific to network segments.



Auto-Quarantine of Infected Hosts

Hosts identified by vSEC as infected can be automatically isolated and quarantined. This is accomplished by vSEC tagging the infected hosts and sharing this information with the NSX controller. Additionally, automated remediation services can be triggered by an orchestration platform. Threats are quickly contained and the appropriate remediation service can be applied to the infected VM.



Context-Aware Security Policies

The integration with VMware NSX controller and vCenter shares context with the Check Point vSEC controller allowing security groups and VM identities to be imported and reused within Check Point security policies. This reduces security policy creation time from minutes to seconds. Real-time context sharing of security groups is maintained so that any changes or new additions are automatically tracked without the need for administrator intervention. Security protections are dynamically applied to newly created applications regardless of where they are hosted.

Check Point Access Policy

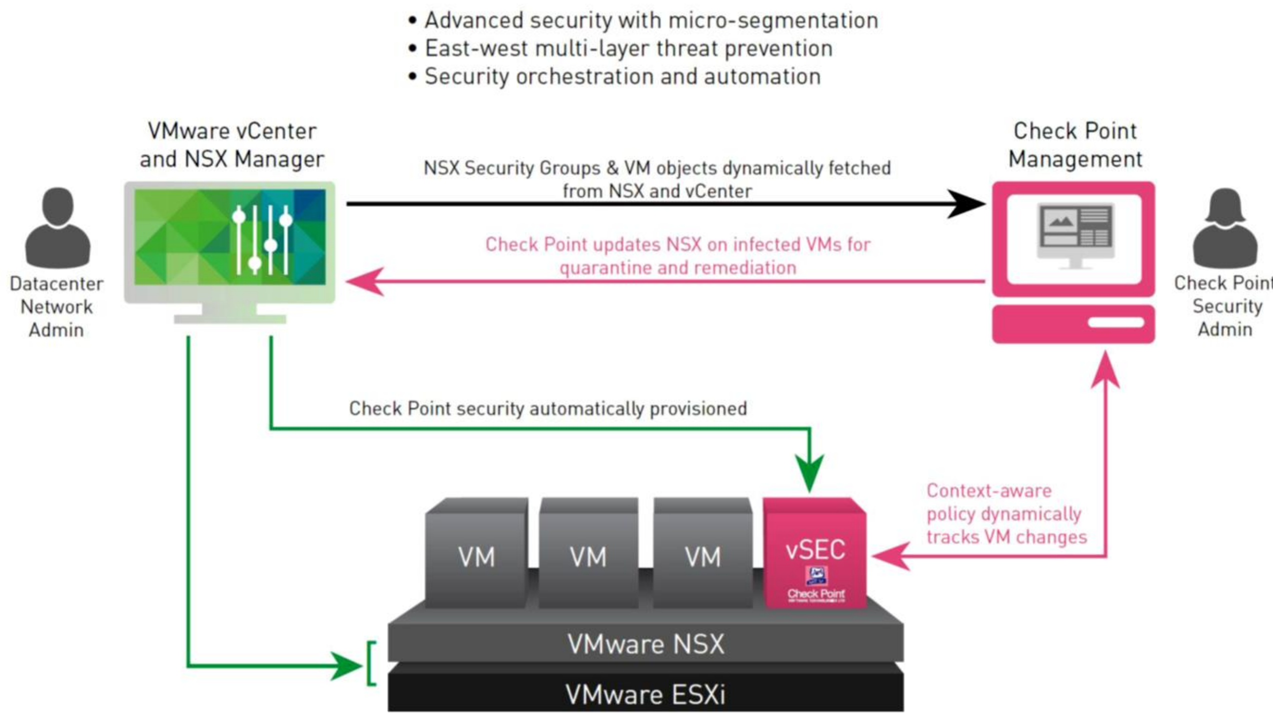
Rule	From	To	Application	Action
3	Finance_App1 (vCenter Object)	Database_Group (ACI EPG)	MSSQL	Allow
4	HR_App2 (ACI EPG)	Finance_Group (ACI EPG)	CRM	Allow
5	User_ID	SAP_App (vCenter Object)	SAP	Allow

Complete Visiblity and Control

vSEC for VMware NSX provides consolidated logging and reporting of threats and security events. Check Point logs are further enriched with NSX context including security group tags. Additionally, the Check Point SmartEvent platform provides advanced incident tracking and threat analysis across both the physical and virtual data-center network traffic.

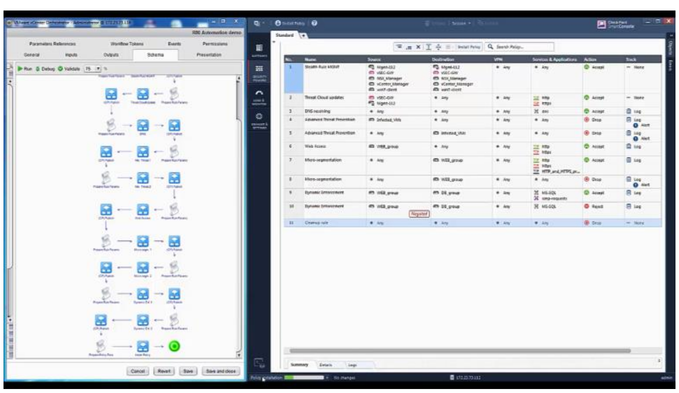
Centralized and Unified Management

Security management is simplified with centralized configuration and monitoring of vSEC. Traffic is logged and can be easily viewed within the same dashboard as other gateways. Security reports can be generated to track security compliance across the data center network. A layered approach to policy management allows administrators to segment a single policy into sub-policies for customized protections and delegation of duties per application or segment. With all aspects of security management such as policy management, logging, monitoring, event analysis and reporting centralized via a single dashboard, security administrators get a holistic view of security posture across their organization



Automation and Orchestration

Check Point vSEC leverages NSX security automation for dynamic distribution and orchestration of vSEC for protecting east-west traffic. In the data center environment, there is often a need to integrate different systems that manage the security workflow. Also, repetitive manual tasks must be automated to streamline security operations. Check Point's security management API allows for granular privilege controls, so that 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. This ability to automatically provision trusted connectivity provides security teams with the confidence to automate and streamline the entire security workflow. In addition, predefined Check Point security templates automate the security of newly provisioned virtual applications.



SOLUTION COMPONENTS

Check Point vSEC gateway

The vSEC gateway provides industry-leading advanced threat prevention security and is deployed into the NSX fabric to prevent lateral threat movement between applications inside the datacenter.

Check Point Smart Center with vSEC controller

The Check Point vSEC controller integrates with SDN and cloud controllers like the NSX controller. It supports the import of NSX and vCenter objects, dynamically tracks object changes and allows using NSX security groups in the Check Point security policy and logs.

VMware NSX fabric and controller
The VMware NSX fabric provides a high performance network virtualization platform for the software-defined data center. The NSX controller provides centralized configuration and management of the NSX fabric. It allows for advanced network security service insertion (L4-L7) and automation.

KEY FEATURES AND BENEFITS

- Dynamic insertion and orchestration of Check Point's advanced threat protection with highest malware catch rates
- Operationally feasible micro-segmentation for east-west traffic protection
- Fine-grained access control policies tied to NSX Security Groups and Virtual Machines
- Unified security management for control and visibility across virtual and physical environments
- Security services provisioned in minutes for fast application deployments
- Shared security context to enable better alignment across security controls
- Isolation and remediation of infected virtual machines
- Network complexity is reduced as well as the need to use multiple VLANs and ACL's inside the data center.

SUMMARY

This joint solution enables enterprises to have fast, simplified provisioning and deployment of Check Point's advanced security services in a Software-Defined Data Center, 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.

ABOUT CHECK POINT

Check Point Software Technologies Ltd. (www.checkpoint.com), is the largest pure-play security vendor globally, provides industry-leading solutions, and protects customers from cyberattacks with an unmatched catch rate of malware and other types of attacks. Check Point offers a complete security architecture defending enterprises' networks to mobile devices, in addition to the most comprehensive and intuitive security management. Check Point protects over 100,000 organizations of all sizes. At Check Point, we secure the future.

ABOUT VMWARE

VMware is a leader in cloud infrastructure and business mobility. Build on VMware's industry-leading virtualization technology, our solutions deliver a brave new model of IT that is fluid, instant and more secure. Customers can innovate faster by rapidly developing, automatically delivering and more safely consuming any application. VMware has more than 500,000 customers and 75,000 partners. The company is head-quartered in Silicon Valley with offices throughout the world and can be found online at www.vmware.com

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