Automating Advanced Security for the Software-Defined Data Center

VMware NSX and Check Point vSEC integrated solution offers dynamic orchestration of advanced threat prevention for all data center traffic

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 deployment
- Shared security context to enable better alignment across security controls
- Isolation and remediation of infected virtual machines

PROTECTION FOR EAST-WEST TRAFFIC

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. And sole dependence on perimeter security leads to choke-points on the network, impacting performance and increasing security complexity; thereby placing additional burden on security teams.

AUTOMATED SECURITY PROVISIONING AND ORCHESTRATION

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.

VMware NSX is the industry’s leading network virtualization platform that delivers the same benefits to the network that VMware delivered for compute. 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. 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.

NSX native security capabilities, automation and extensibility framework can be leveraged by NSX partners like 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, or the zero trust security model, allowing the SDDC to deliver a fundamentally more secure approach to data security. Policy is enforced at the virtual interface, and policies follow workloads.

Check Point vSEC uses these NSX capabilities and the integration brings together the best of both worlds - advanced security protection dynamically deployed and orchestrated into a software-defined data center environment.
Feasible Micro-segmentation: Inherent NSX network isolation and segmentation makes data center micro-segmentation feasible without the need to configure vLANs, ACLs, firewall rules, physical firewalls and routers. Security controls can be applied at the smallest unit level to allow the deployment of a security least privilege model. NSX basic firewalls 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.

Context-Aware Security Policy: NSX standard tags enable full-context sharing between VMware NSX, VMware vCenter and the Check Point vSEC management platforms ensures that security groups and Virtual Machine (VM) identities are easily imported and reused within the Check Point security policy. This reduces security policy creation time from minutes to seconds. Context-awareness of these security groups and VMs is maintained so that any changes or new additions are automatically tracked. This makes it possible for security protections to be enforced on virtual applications regardless of where they are created or located. In addition, predefined Check Point security templates automate the security of newly provisioned virtual applications. Check Point’s dynamic security policy seamlessly adapts to data center changes and can be enforced across virtual and physical security gateways.

Ubiquitous Security Enforcement: The VMware NSX network hypervisor is optimally located between the application and the physical infrastructure, enabling distributed enforcement at every virtual interface. By integrating with VMware NSX, Check Point vSEC can dynamically insert advanced security protection. Check Point’s Advanced Threat Prevention delivers multi-layered defenses, with the industry's best catch rates and comprehensive threat intelligence, to proactively stop botnets, targeted attacks, advanced persistent threats and zero-day attacks. VMware NSX makes it possible to chain Check Point’s advanced security protections between different workloads and to control communications between applications. This reduces network complexity and the need to use multiple VLANs inside the data center.

Automation and Orchestration: Check Point vSEC leverages NSX security automation for dynamic distribution and orchestration of vSEC for protecting East-West traffic. Check Point vSEC detects and tags malware-infected VMs, and automatically updates VMware NSX. Threats are quickly contained and the appropriate remediation service can be applied to the infected VM. 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 perform trusted connections provides security teams with the confidence to automate and streamline the entire security workflow.

Comprehensive Control and Visibility: Security management is simplified with centralized configuration and monitoring of virtual security gateways. Virtual workload traffic is logged and can be easily viewed within the same dashboard as other gateway logs. Security reports specific to virtual workload traffic can be generated to track security compliance across the virtual network. A layered approach to policy management allows administrators to segment a single policy into sub-policies for customized protections and delegation of duties by network segment. This ensures that the right level of protection is applied across both virtual and physical networks. 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.
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 cyber-attacks 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. Built 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.