Check Point vSEC for OpenStack

Comprehensive Protections for the OpenStack based cloud networks

OpenStack

is an open standard cloud computing platform for public and private clouds. It is designed by a global community of developers and organizations to address today's need to build a scalable and flexible cloud infrastructure to enable agility and to deliver speed and time-to-market advantages for the delivery of new services.

Check Point is one of the members and contributors to the OpenStack community and integrates with OpenStack to protect and secure cloud environments. Check Point vSEC has been validated and integrated in OpenStack based cloud environments developed by an ecosystem of partners.

Check Point vSEC for OpenStack

protects OpenStack cloud environments from internal and external threats with the full range of protections available in the Check Point Software Blade architecture. vSEC for OpenStack delivers best-of-breed security protection and management so your organization can focus on architecting dynamic cloud environments

Designed for the dynamic security requirements of cloud deployments, vSEC provides the most advanced threat protections to inspect traffic entering and leaving tenant subnets in the cloud. vSEC provides consistent security policy management, enforcement, and reporting, making migration to OpenStack cloud environments painless.

CLOUD & VIRTUAL DATACENTER SECURITY OVERVIEW

The wide adoption of cloud architectures—whether public, private or hybrid—is being driven by the desire to transform businesses for greater efficiency, speed, agility and cost controls particularly in the carrier and large enterprise networks which are primarily used for application delivery to large user base including customers and lines of business. OpenStack cloud networks helps CSPs and large enterprises thrive in this increasingly fast-paced environment by accelerating the journey from traditional networks built on monolithic, proprietary appliances to more agile cloud networks enabled by Network Functions Virtualization (NFV). Now enterprises and carriers can move to a virtualized network and instantly add capacity and manage the entire network from a single, unified control application and can achieve true agility in network configuration and management.

While the cloud offers many advantages over traditional infrastructure it also exposes enterprises and carriers and their end users to a whole new set of security challenges. The built-in security controls in the cloud lack advanced threat protection. The operational challenge of provisioning security for workloads is a manual operation that is complex, slow and error-prone. The cloud hosts multi-tenant environments where application workloads critically need to be isolated and protected from each other. The traditional approach to securing a data center with a perimeter gateway only provides visibility and control into north-south traffic. All internal or east-west traffic is unprotected and allows threats to spread laterally once a weaker system has been compromised.

ADVANCED THREAT PROTECTION FOR OPENSTACK CLOUD

Check Point vSEC for OpenStack offers an industry leading next generation threat prevention virtual security gateway integrated and validated on OpenStack environments allowing CSPs and enterprises to deliver comprehensive security services that include cyber-threat protection from internal and external threats. Enterprises can focus on developing a fully automated cloud environment with an orchestration capability that empowers line of business users to self-provision resources through a web interface. The OpenStack ecosystem of validated and integrated VNF's gives carriers the freedom to choose the best in class applications like Check Point vSEC that are ready to deploy in production networks.

The integrated solution provides advanced threat prevention security for east-west traffic seamlessly enforced inside the virtual infrastructure using dynamic service insertion and chaining; comprehensive threat visibility, monitoring and logging across both virtual and physical environments; agile and automated provisioning and scalability of security that adjusts to dynamic network changes; context aware security policies that leverage security groups, virtual objects defined in the virtual network.

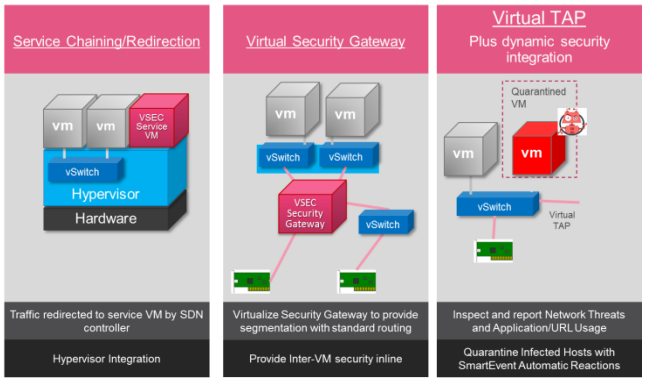
Comprehensive Security Protections

vSEC for OpenStack provides industry-leading threat prevention security to keep OpenStack cloud networks safe from even the most sophisticated attacks. Fully integrated security protections include:

- **Firewall, Intrusion Prevention System (IPS), Antivirus, and Anti-Bot** technology protects services in the cloud from unauthorized access and prevents attacks
- **Application Control** helps to prevent application-layer Denial of Service (DoS) attacks and protect hybrid cloud services
- **IPSec VPN and Mobile Access** allows mobile users to connect to hybrid clouds using an SSL encrypted connection with two-factor authentication and device pairing
- **Data Loss Prevention** protects sensitive data from theft or unintentional loss
- **SandBlast Zero-Day Protection** sandbox technology provides the most advanced protection against malware and zero-day attacks

Security Orchestration and Automation

OpenStack provides the framework to allow automated policy-based service insertion from a single-pane-of-glass management platform. The integration automates and simplifies the provisioning of vSEC gateways into the OpenStack controlled networking fabric to protect east-west traffic from lateral movement of threats. The integration of OpenStack and vSEC allows for single-click provisioning using HEAT (YAML) templates and the ability to configure security gateway via RESTful APIs, as well as gateway auto registration with defined policies for dynamic segmentation.



Check Point vSEC for OpenStack deployment models

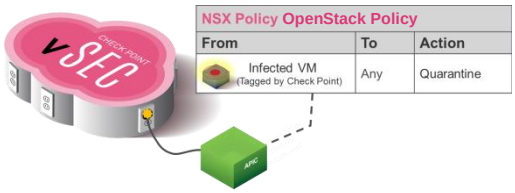
Context Aware Security Policies

The integration with OpenStack cloud controller shares context with the Check Point vSEC controller allowing OpenStack Metadata like security groups 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.

No.	Hits	Name	Source	Destination	VPN	Service	Action
OpenStack Dynamic Web Security Group Rules (Rules 1-5)							
1		ICMP Allow	openstack_web	Any	Any Traffic	icmp-requests	accept
2		Management Rule	Web_Admins	openstack_web	Any Traffic	ssh	accept
3		Inbound Rule	Any	openstack_web	Any Traffic	http https	accept
4		Drop Everything not Allowed	Any	openstack_web	Any Traffic	Any	drop
5		Drop Everything not Allowed	openstack_web	Any	Any Traffic	Any	drop

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 OpenStack controller. Additionally, automated remediation services can be triggered by an orchestration platform.

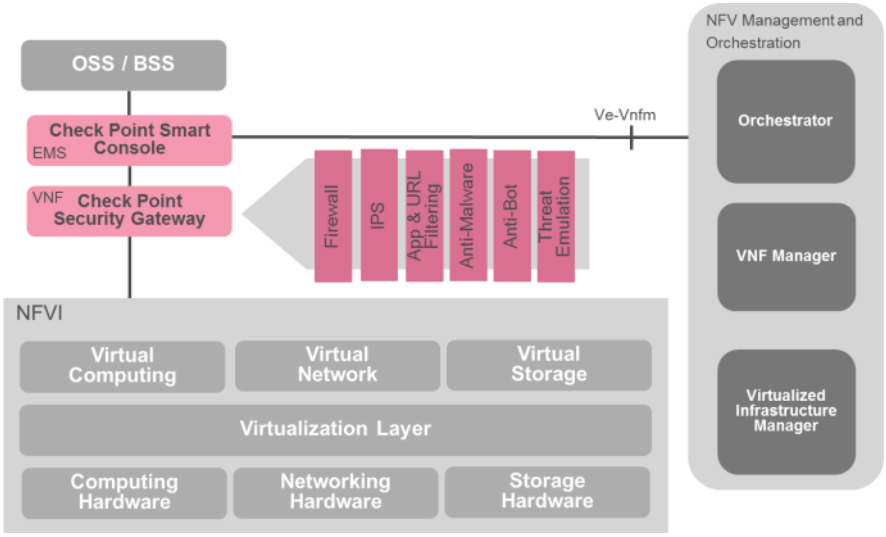


Centralized Visibility and Control

Check Point vSEC for OpenStack provides simplified and centralized security management across cloud environments. Manage vSEC for OpenStack using your existing industry leading Check Point Unified Security Management Solutions. Enforce a consistent security policy across both virtual and physical, on-premise and cloud infrastructures from a single console.

Unified Logs and Reporting

vSEC for OpenStack gives organizations complete threat visibility and enforcement for cloud infrastructures. Check Point SmartEvents software consolidates monitoring, logging, and reporting across cloud networks. Check Point logs are further enriched with OpenStack context including security group tags. Security reports specific to cloud workload traffic can be generated to track security compliance across the cloud network, simplifying reporting, compliance and audits. 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 their security posture across the entire organization. CSPs can provide automatically scheduled, periodic reports to their customers using the Smart Event Software Blade.



Check Point vSEC for OpenStack integration with NFV infrastructure

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 OPENSTACK

The OpenStack (www.openstack.org) project is a global collaboration of developers and cloud computing technologists producing the open and scalable standard cloud computing platform for both public and private clouds. The open source project is built by a vibrant community of developers in collaboration with users and some of the biggest names in the industry. OpenStack works with popular enterprise and open source technologies making it ideal for heterogeneous infrastructure. Hundreds of the world's largest brands rely on OpenStack to run their businesses every day, reducing costs and helping them move faster.

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