Check Point vSEC for Cisco ACI

Advanced threat prevention security for next-generation data center networks

Cisco Application Centric Infrastructure (ACI) is a comprehensive software defined networking (SDN) architecture that supports a business-relevant application policy language to accelerate application delivery, reduce operating costs and greatly increase business agility. Cisco ACI helps customers dramatically reduce application deployment times from weeks to minutes while improving IT alignment with business objectives and policy requirements.

Check Point vSEC for Cisco ACI delivers advanced threat prevention security for Cisco ACI next-generation data centers. Designed for the dynamic requirements of Cisco ACI 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 and 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, the shift from a hardware-centric to an application-focused infrastructure has led to a dramatic increase in network traffic going east-west, or laterally, between applications in the data center.

Security has traditionally been focused on protecting perimeter, or north-south, traffic going into and out of the data center while east-west traffic between applications inside the data center is not inspected. This presents a host of new challenges where threats introduced into the data center can traverse unimpeded since they no longer pass through the security gateway.

What's more, traditional security approaches are manual, operationally complex, slow and unable to keep pace with dynamic changes and rapid application provisioning. Check Point vSEC for Cisco ACI addresses these challenges delivering comprehensive and dynamic security specifically architected for Cisco ACI enabled data centers.

DYNAMIC THREAT PREVENTION SECURITY FOR CISCO ACI

Cisco ACI provides effective micro-segmentation for next-generation data centers through the integration of physical and virtual environments under a common policy model for networks, servers, storage and security. Cisco ACI's application-aware policy model and native security capabilities are leveraged by Check Point vSEC to dynamically insert, deploy and orchestrate advanced security protections within Cisco ACI-enabled data centers.

Together, Cisco and Check Point provide a powerful solution that gives customers proactive protection from the most advanced threats as well as complete traffic visibility and reporting of both physical and virtual network environments. The joint solution forms the foundation of a dynamic application delivery architecture, where comprehensive security protections seamlessly follow workloads to accelerate application deployment while lowering the costs and complexities of securing private clouds.

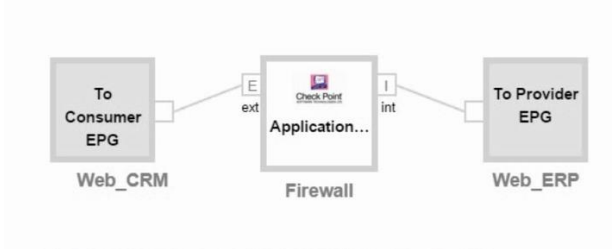
Comprehensive Threat Prevention

vSEC for Cisco ACI provides industry-leading advanced threat prevention security to keep data centers protected from lateral movement of even the most sophisticated threats. 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 of threats
- **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 next-generation data center
- **Data Loss Prevention** protects sensitive data from theft or unintentional loss
- **IPSec VPN and Mobile Access** allows secure communication into cloud resources

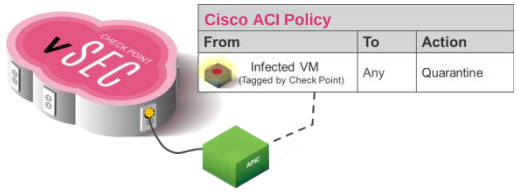
Automated Security Provisioning

Cisco ACI provides the framework to allow automated policy-based service insertion from a single-pane-of-glass management platform. The Check Point integration with Cisco ACI automates and simplifies the insertion of vSEC gateways into the ACI fabric to protect east-west traffic from lateral movement of threats.



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 ACI fabric. 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.



*Available in upcoming Check Point vSEC for Cisco ACI release

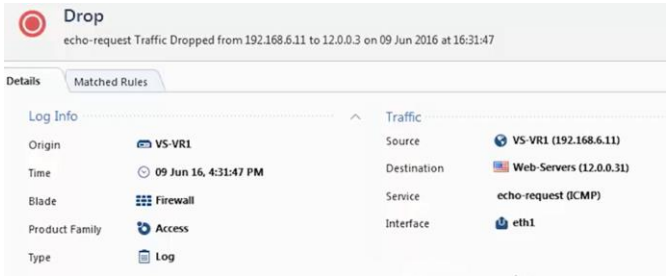
Automated and Dynamic Security Policy

The integration with Cisco's Application Policy Infrastructure Controller (APIC) shares infrastructure context with the Check Point vSEC controller, allowing Cisco ACI objects such as end point groups (EPGs) to be imported and utilized within Check Point security policies. This reduces the time it takes to create and update security policies from minutes to seconds. What's more, any changes or new additions to Cisco ACI objects are automatically reflected without the need for manual administrator intervention.

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 Threat Visibility and Control

vSEC for Cisco ACI provides consolidated logging and reporting of threats and security events. Check Point logs are enriched with ACI infrastructure context including EPG names. Additionally, Check Point's SmartEvent platform provides advanced incident tracking and threat analysis across both physical and virtual data-center network traffic.



Centralized and Unified Security Management

Security is simplified and operationally efficient with centralized configuration and monitoring of all physical and virtual vSEC gateways. Security reports can be generated to track compliance across the ACI-enabled private cloud networks. Granular administrative privileges allow segmenting a single policy into sub-policies for customized protections as well as delegation of duties per application or segment. With Check Point vSEC for Cisco ACI, security administrators get a holistic view of their security posture and complete threat forensics with unified logs and reporting across their physical and virtual networks.

SOLUTION COMPONENTS

Check Point Security Gateways
Check Point security gateways provide industry-leading advanced threat prevention and zero day protections for applications and workloads inside private cloud data centers. Providing consistent security across the entire next-generation data center infrastructure. Check Point security gateways are deployed as either physical or virtual appliances and provide support for popular hypervisors such as and VMware ESX, Microsoft Hyper-V and KVM.

Check Point Smart Center with vSEC Controller
A component of the Check Point Smart Center management platform, the Check Point vSEC controller seamlessly integrates with popular SDN and cloud controllers such as the Cisco APIC controller. The integration supports the import of ACI objects within Check Point security policies for dynamically tracking object changes as well as populating end point group names in Check Point SmartLogs.

Check Point vSEC Device Package
The vSEC device package enables seamless integration of Check Point advanced threat prevention security with the Cisco APIC controller, providing automated vSEC security gateway insertion in the ACI fabric. Once uploaded to the APIC controller, the vSEC device package facilitates the use of Cisco ACI service graphs to insert security between end point groups (EPGs).

Cisco ACI Fabric and APIC
The Cisco ACI Fabric provides a high performance next-generation data center fabric. The APIC controller provides centralized configuration and management of the ACI fabric. It allows for advanced network security service insertion (L4-L7) and automation.

KEY FEATURES AND BENEFITS

- Automated insertion and orchestration of Check Point vSEC gateways to prevent lateral movement of threats in Cisco ACI next-generation data centers
- Dynamic policies leveraging ACI objects (EPGs) for improved security operational efficiency
- Operationally feasible micro-segmentation for East-West traffic isolation for both physical and virtual data center servers
- Full forensic analysis, enhanced visibility and unified logs across the network perimeter as well as physical and virtual data center traffic
- Tagging infected hosts for network isolation (auto-quarantine) or remediation
- Ability to absorb context from multiple cloud management systems such as Cisco ACI, OpenStack and VMware vCenter for dynamic security policies
- Rapid deployment of security policies throughout the application deployment lifecycle

SUMMARY

Check Point vSEC for Cisco ACI delivers accelerated, automated, simplified provisioning and deployment of Check Point's advanced security services in next generation data centers built on Cisco ACI technology. vSEC integration with Cisco ACI enables customers to have the same level of security for traffic inside the data center as Check Point provides at the perimeter. The integration securely enables the rapid deployment of applications while providing full control and visibility across both physical and virtual data center infrastructures.

.

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 CISCO

Cisco is the worldwide leader in IT that helps companies seize the opportunities of tomorrow by proving that amazing things can happen when you connect the previously unconnected. Cisco powers the world's Internet experiences and connects people, processes, data and things to enable innovation that benefits business and society. The company is head-quartered in Silicon Valley with offices throughout the world and can be found online at www.cisco.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