Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.

PRODUCT DESCRIPTION

The Check Point Security Gateway Virtual Edition (VE) protects dynamic virtualized environments and external networks, such as private and public clouds, from internal and external threats by securing virtual machines and applications with the full range of Check Point Software Blades.

Security Gateway Virtual Edition

Security Gateway VE provides one-click virtualization protection for private and public clouds

YOUR CHALLENGE

Server virtualization continues at a staggering pace and with it the need to address security. Virtual environments have not only the same challenges as physical ones—needing protection from external threats—but also those unique to virtualization. Virtualization can create gaps in visibility, including inter-Virtual Machine (VM) traffic within a platform hosting multiple VMs. Also, new VMs need to be automatically protected as they are brought online, as do VMs being migrated from one physical platform to another due to infrastructure expansion or hardware failure.

OUR SOLUTION

Check Point Security Gateway Virtual Edition—based on the Software Blade Architecture—provides a comprehensive virtual security solution for protection of VM environments and starts at only $2050. Streamlined deployment and full support for live migration of VMs means zero downtime. Also, as new VMs are brought online, they are immediately protected by automatic security policy enforcement.

INTER-VM TRAFFIC INSPECTION

Ensure virtual machine security by inspecting all inter-VM traffic with granular firewall policies and integrated best-in-class intrusion prevention. Security Gateway VE utilizes VMware's VMsafe technology to seamlessly enforce security within the hypervisor.

Security Gateway VE enables you to separate virtual applications, protecting them from each other as well as external threats. Integrated IPS utilizes signature and protocol anomaly-based intrusion prevention to protect business-critical services like FTP, HTTP and VoIP from known and unknown attacks. And, Check Point Update Services provide real-time updates to keep protections current with the latest defenses.

PRODUCT FEATURES

- Inter-VM traffic inspection
- Enforce security for dynamic virtualized environments
- Fully virtualized security gateway
- Virtualization enablement
- Easy-to-deploy security for virtual machines
- Unified management for physical and virtualized environments

PRODUCT BENEFITS

- Software Blade Architecture delivers comprehensive security to both external networks and virtual environments
- Ensures VM security by inspecting all inter-VM traffic with granular firewall policies and integrated best-in-class intrusion prevention
- Virtual gateway deployment requires no network changes
- Provides continuous protection during live migration of VMs from one host to another and when new VMs are added
- Single pane of glass for managing both physical and virtualized environments makes administration easy

software**blades**™

Classification: [Unrestricted] — For everyone | 1

ENFORCE SECURITY FOR DYNAMIC VIRTUALIZED ENVIRONMENTS

Virtual machine protection is continuous during live migration of virtual machines from one host to another and when new virtual machines are added. Full support for VMware VMotion and full-term Dynamic Resource Scheduler (DRS) allows the security policy to be enforced while maintaining open connections. This also ensures zero down time when virtual machines are moved from host to host for maintenance and dynamic resource allocation.

Virtual machines are so easy to create that it sometimes leads to VM sprawl. Security Gateway VE alleviates this concern by ensuring that newly added virtual machines are segregated from existing VMs with automatic security policy enforcement.

FULLY VIRTUALIZED SECURITY GATEWAY

Security Gateway VE provides comprehensive security based on the Software Blade Architecture, protecting both inter-VM traffic and external networks and assets. In addition to seamless hypervisor-layer security, VE also provides the flexibility to be deployed as a Layer 2 or Layer 3 default gateway.

Security Gateway VE simplifies security deployments by consolidating proven security functions within a single solution streamlining deployment and administration. Virtual machines are protected from external threats as well as from each other with best-in-class integrated firewall, IPS, DLP, application control, identity awareness, VPN, anti-virus, anti-spam, URL filtering, web security and mobile access. Where separation of servers and data is required for compliance, VE protects segregated applications and information from one another without the need for physical security appliances.

EASY TO DEPLOY SECURITY FOR VIRTUAL MACHINES

Security Gateway VE reduces administration overhead by automatically applying security to virtual machines without the need to change network topology configuration for the VMs, VLANs or vSwitches.
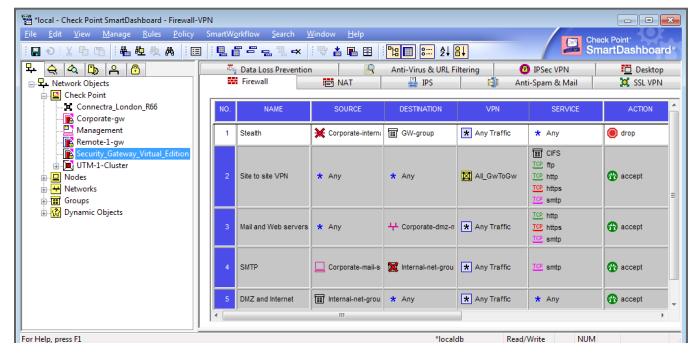
VIRTUALIZATION ENABLEMENT

Virtualization initiatives are driven by consolidation, optimization, and return on investment. Relying on traditional physical security appliances to inspect inter-VM traffic impacts performance and complicates topology. With VE, this complexity is avoided, boosting performance by inspecting virtual machine traffic inside the virtualized system.

UNIFIED MANAGEMENT FOR PHYSICAL AND VIRTUAL ENVIRONMENTS

Security management is simplified with unified administration of physical and virtualized environments including clear separation of administrative functions between virtualization and security administrators.

Security Gateway Virtual Edition is managed from the same Security Management or Multi-Domain Management (MDM) as all other physical Check Point security gateways and appliances. This enables you to deploy a single pane of glass to ensure consistent security at all gateways, while minimizing the expense of separate management consoles.

Check Point SmartDashboard GUI – Unified management for physical and virtual gateways

Traffic logging, reporting and full virtualization auditing solutions tailored for the virtual infrastructure enable users to accelerate and achieve compliance, with dedicated reports that are mapped to relevant requirements within the PCI, SOX, HIPAA, COBIT and ISO 17799 regulations and standards.

Check Point Security Management and MDM can also be deployed on virtual machines.

MULTI-DOMAIN SECURITY MANAGEMENT FEATURES

Feature	Details
Supported VMware servers	VMware VSphere
Supported Check Point solutions	• Security Gateway Software Blades R75.20 • Security Management R75.20
Minimum virtual appliance requirements	• Allocated Memory: 512MB (recommended 2.5GB) • Disk Space: 12GB

VIRTUALIZED SECURITY SCENARIOS

Secure the Virtual Environment
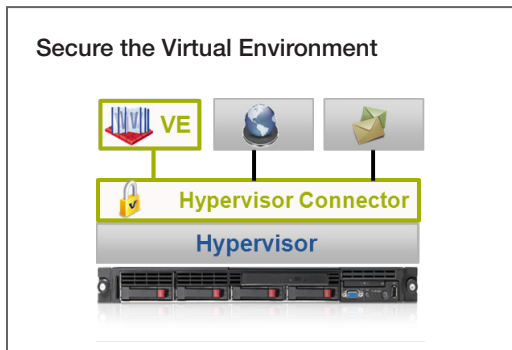
Use Security Gateway Virtual Edition to apply granular firewall and IPS policies for inter-VM traffic.

Office in a Box
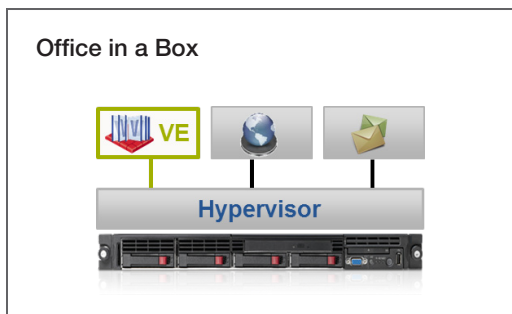
Use Security Gateway Virtual Edition (VE) with firewall, IPS, VPN and Software Blades to secure your office networks and assets.