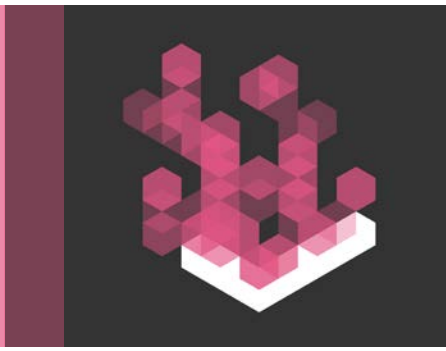
CHECK POINT VIRTUAL SYSTEMS



CHECK POINT TAPS THE POWER OF VIRTUALIZATION TO SIMPLIFY SECURITY FOR PRIVATE CLOUDS

Looking for ways to reduce complexity and simplify network security in your private cloud? Need customized and finely tuned solutions to better protect your growing network needs? You are not alone. In fact, you are among the majority of today's IT professionals who are faced with the challenging task of managing complex securities in an ever growing and more demanding network environment.

The increasing complexity of network security and new threats combined with a slowing growth of IT budget drive the need for a solution that improves operational efficiency, optimizes security and lowers costs.

Network security consolidation has become a strategic trend for IT professionals to deliver more effective security at lower costs. By consolidating multiple security gateways in a single solution, both enterprises and service providers have the opportunity to optimize productivity and minimize the total cost of ownership (TCO).

Organizations can achieve an overall reduction in capital equipment costs (CapEx) as well as in operating costs (OpEx) by reducing the hardware investment and streamlining the management of securing large segmented networks and data centers. Service Providers have the opportunity to increase revenue by delivering new security services easily and efficiency to customers through their managed services.

OVERVIEW

Check Point Virtual Systems enable organizations to consolidate infrastructure by creating multiple virtualized security gateways on a single hardware device, delivering deep cost savings, seamless security and infrastructure consolidation. Based on proven virtualized security design and the extensible Software Blade Architecture, Virtual Systems provide best-in-class customized security protections to multiple networks and simplify enterprise-wide policy by creating tailored policies for each network.

Administrators can replicate conventional physical security gateways with Virtual Systems to deliver advanced protection to multiple networks and network segments. Multiple fully independent Virtual Systems are supported on Check Point gateways or Open Servers, delivering scalability, availability and performance while dramatically reduce hardware investment, space requirements and maintenance costs.

KEY FEATURES

- Consolidate multiple gateways in a single device
- Separation of management duties
- Customized security policies per Virtual System
- Per Virtual System Monitoring of resource usage
- Linear scalability of up to 13 clustered gateways with VSLS technology
- Simple one-click conversion from physical to virtual
- Supported as software-only on Check Point Appliances or Open Servers and as pre-configured appliances

KEY BENEFITS

- Easily add virtual systems to any security gateway
- Out of the box complete solution with virtualized system appliances
- Reduce hardware cost and simplified network policy by consolidating multiple gateways into a single device
- Stronger performance and manageability enable enterprises to better leverage their investment
- More granularity and greater manageability with customizable policies per Virtual System
- Better usage-based resource planning with per Virtual System monitoring
- Boost performance with Multi-core CoreXL technology

INTEGRATED SECURITY ARCHITECTURE

Our integrated Software Blade Architecture delivers comprehensive protection. Administrators have the flexibility to configure any Software Blade with any security policy to any Virtual System.

	Gateway Mode	VS Mode
Firewall	✓	✓
IPsec VPN	✓	✓
Identity Awareness	✓	✓
IPS	✓	✓
Application Control	✓	✓
URL Filtering	✓	✓
Antivirus	✓	✓
Anti-Bot	✓	✓
SandBlast Threat Emulation	✓	✓
DLP	✓	×
Mobile Access	✓	✓

✓ supported, × not supported

STREAMLINED CENTRAL MANAGEMENT

Check Point Security Management and Multi-Domain Security Management solutions provide an effective tool for the administration of the Virtual Systems. Dedicated Virtual Systems for web security, threat prevention, firewall, and remote access enable separation of IT duties. Separation of management per Virtual Systems and data segregation support cloud based security-as-a-service needs.

INTEGRATED VIRTUAL ROUTERS AND SWITCHES

Complete virtualization of network infrastructure allows easy deployment and configuration of network topology with simpler inter-VS communication. Save the costs of external network routers and switches. The integrated virtual routers, switches and links direct traffics to their intended destinations with higher efficiency.

IPV6 READY

Control and manage IPv4 and IPv6 networks with Software Blades security using the same rule base and objects for both IPv4 and IPv6. Ease the transition to IPv6 with dual stack IPv4 and IPv6 architecture, IPv6 in IPv4 (RFC4213) tunneling and NAT66 network address translation.

HIGH PERFORMANCE

The latest Check Point technologies ensure best performance for virtualized security; CoreXL technology utilizes multi-core processors to increase throughput, 64-bit GAiA OS provides over eight times more concurrent connections, and patented VSLS technology delivers unmatched performance scalability with up to 8 members per cluster.

LINEAR SCALABILITY

Today's networks require flexibility and expandability to support the fast-evolving business needs. To meet this demanding business environment, Virtual Systems can be deployed on multiple gateways ensuring secure, resilient, multi-gigabit throughput. Virtual System Load Sharing (VSLS) distributes traffic load within a cluster, providing the ability to distribute virtual systems across multiple cluster members, without requiring any change to existing topology. Every addition of a cluster member effectively spreads the virtual system traffic load within the cluster, providing the benefits of throughput, concurrent connections, redundancy, cost efficiency, configuration simplicity, priority designation, and system scalability.

PER-VS RESOURCE MONITORING

Need to understand how your Virtual Systems are used to better plan your security resources or to create billable customer services? Granular resource monitoring of CPU and Memory for each Virtual System gives you the necessary insights to effectively plan for your network security resources, or to provide usage-based services to your customers.

Resource Control allows administrators to manage the processing load by guaranteeing that each virtual system will receive only the memory and CPU allocation it needs to deliver its functions. Resources not needed by one virtual system are automatically made available to other virtual systems. Administrators can also limit the CPU resource available to a lower-priority virtual system and assign more resources to mission-critical virtual systems.

FLEXIBLE PACKAGING OPTIONS

Check Point Virtual Systems are offered either as a software-only option or in pre-configured bundles with Check Point Security Appliances and Software Blades, providing the flexibility and convenience for different deployment situations.

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: 650-628-2117 | www.checkpoint.com