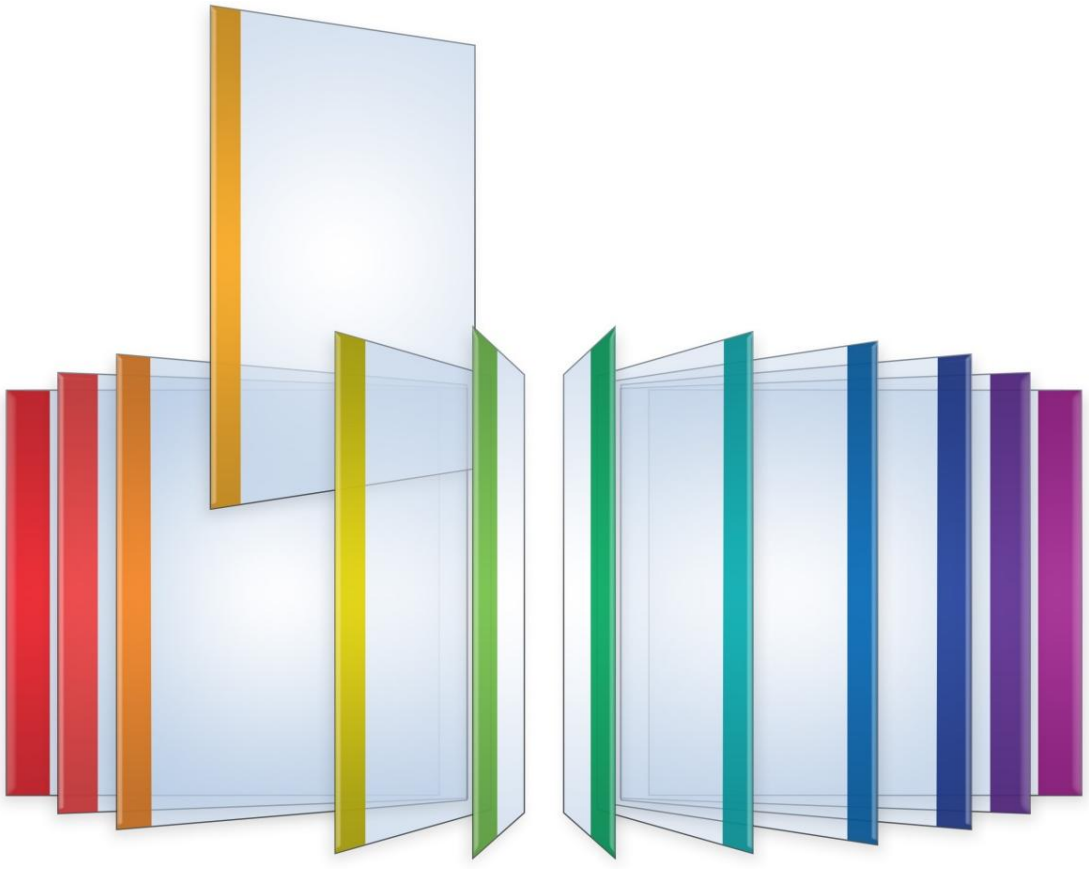
Check Point
SOFTWARE TECHNOLOGIES LTD.

Security Gateway - Virtual Edition

R71 EA

Release Notes

9 August 2010



softwareblades™

Important Information

Additional Information

For additional technical information, visit the Check Point Support Center (http://supportcenter.checkpoint.com).

Revision History

Date	Description
9 August 2010	Initial version

Feedback

Check Point is engaged in a continuous effort to improve its documentation.

Please help us by sending your comments (mailto:cp_techpub_feedback@checkpoint.com?subject=Feedback on Security Gateway - Virtual Edition R71 EA Release Notes).

Contents

Introduction

Security Gateway - Virtual Edition is a unique security solution that harnesses the power of network virtualization and provides comprehensive protection to secure your VMware virtual networks. Security Gateway - Virtual Edition provides many of the same security features found in physical Security Gateways, such as Firewall and IPS. You manage your security policies using Check Point centralized management tools, enabling a consistent and enforceable security policy across all physical and virtual networks.

Security Gateway - Virtual Edition supports ESX clusters using Check Point ClusterXL VE technology. All you need to do is install Security Gateway - Virtual Edition on each cluster member, connect the synchronization NICs, and configure ClusterXL VE.

When installed on an ESX server, Security Gateway - Virtual Edition has two working modes:

- The Standard mode supplies all of the security features found in physical security gateways, such as Firewall and IPS, URL Filtering and anti-virus protection.
- The Avatar mode supplies most of the security features found in physical security gateways, such as Firewall and IPS. Additionally, the Avatar mode integrates with the VMware hypervisor using vNetwork Appliance APIs (VMsafe APIs) to supply unique security features for VMware deployments.

This guide contains documentation for the Avatar mode only.

Note - This guide assumes that the reader has a thorough understanding of Check Point concepts and procedures as described in the R71 Security Management Server Administration Guide *(*http://supportcontent.checkpoint.com/documentation_download?ID=10315*),* as well as VMware® ESX Server 4.x concepts, procedures and terminology.

What's New

- Inter-Virtual Machine and external threats protection.
- Protection of individual Virtual Machines, even among virtual machines on a same vSwitch.
- High security granularity.
- Misconfiguration protection.
- Default security behavior for newly created Virtual Machines and vSwitches.
- Automatic, seamless vSwitch integration.
- Detect only mode.
- Logging of vSphere events in SmartView Tracker.
- Support for advanced VMware features such as VMotion, DRS, and HA.
- Support for Cisco Nexus 1000V.
- Support for DVSwitch.

Supported Builds and Platforms

This table shows the supported builds and platforms for Security Gateway - Virtual Edition.

Build, Platform, Server	Version
Security Gateway - Virtual Edition Build	976141006 To verify: `fw ver -k`
VMware Platform	VMware vSphere 4.0
Check Point Security Management Server or Provider-1 MDS	R71 or higher

Known Limitations

Note - The ID numbers next to each known limitation are for your tracking information. Check Point constantly makes an effort to improve released products. Check the tracking numbers in the next release for fixes.

Security Gateway - Virtual Edition in the Avatar mode

Non-supported R71 Features

ID	Unsupported Feature
00525721	Layer 3 topologies and Layer 3 features (NAT and VPN) are not supported.
00525807	The following features are not supported in the current version: • Mail Security • HTTP/FTP/SMTP with resource • User/client/session authentication • Anti-Virus in the proactive mode • Anti-Virus for FTP • Anti-Virus by file direction
00525819	ClusterXL High Availability and Load Sharing are not supported.
00525822	QoS is not supported.
00526867	Bridge mode configuration is not supported.
00527315	CoreXL is not supported.
00568259	You can only configure one virtual CPU for a Security Gateway - Virtual Edition.
00568687	VoIP is not supported.

VMware Feature Limitations

ID	Description
00525821	You cannot apply VMware Fault Tolerance to any Virtual Machines, including the Security Gateway - Virtual Edition Virtual Machine.

Network Limitations

ID	Description
00518814	If there is a Virtual Machine on the ESX host that works as a router for other Virtual Machines, make sure that you configure these settings: 1. Configure the routing Virtual Machine security setting (using sysconfig) as bypassed. 2. Do not configure IP Anti-spoofing for Virtual Machines that use the routing Virtual Machine as a default gateway.
00525805	VLAN configuration on the Virtual Machine guest operating system in an ESX environment is not supported. Configure the VLAN on a vSwitch.
00526860	If a Virtual Machine on the ESX host works as a bridge for other Virtual Machines, you must configure the bridge Virtual Machine security setting (using sysconfig) as bypassed.
00526946	Duplicate IP addresses or MAC addresses for separate Virtual Machines protected by the same ClusterXL VE are not supported.
00552805	You cannot change a vNIC MAC address using the guest operation system.
00566045	The SecurePlatform Web UI is disabled until you assign an IP address to one of its network adapters.
00557690	Dynamic Routing is not supported.
00560767	A Check Point management server cannot connect to a Security Gateway - Virtual Edition if all of these cases are true: • The management server is installed on an ESX cluster member. • The management server uses a dedicated network. • The Security Gateway - Virtual Edition is not directly connected to this network. Workaround: Connect the management server Virtual Machine to the ESX management network or connect the Security Gateway - Virtual Edition to the management network.
00568517	Microsoft Network Load Balancing (NLB) is not supported for Virtual Machines.
00568524	IPv6 is not supported.

ESX Configuration Limitations

ID	Description
00526845	You can only install one Security Gateway - Virtual Edition Avatar mode on an ESX host.
00528634	Security Gateway - Virtual Edition supports a maximum of 100 Virtual Machines on one ESX host.
00527283	When using the VMware Distributed Resource Scheduler, you must disable it on the Security Gateway - Virtual Edition.

General

ID	Description
00526862	VMware Tools are not supported on a Security Gateway - Virtual Edition Virtual Machine.

ID	Description
00525830	You must install Security Gateway - Virtual Edition as a clean installation. You must reinstall Security Gateway - Virtual Edition to upgrade to a later EA version or to the GA.
00527267	Performance Pack Heavy Load Quality of Service feature (HLQoS) is not supported.
00558889	After creating a Virtual Machine from a template or after cloning a Virtual Machine, the following entry may show in the SmartView Tracker logs: "*A misconfigured filter was created due to VM import, deployment of VM from template or VM cloning. Traffic is blocked for this new VM*. *Please reset the newly created VM in order to fix this issue.*" If this occurs, reset the new Virtual Machine. This message may also occur when powering on the source (original) Virtual Machine after cloning it. If this occurs, reset both the source and the newly cloned Virtual Machines.
00566886	CPU consumption for the Security Gateway - Virtual Edition might show inaccurate results. To resolve this issue, reserve CPU resources on the ESX: 1. In the vSphere client, right click the Security Gateway - Virtual Edition. 2. Select **Edit Settings**. 3. On the **Resources** tab, move the **Reservation** slider to allocate a guaranteed CPU share (in MHz).

ClusterXL VE with VMotion and Avatar mode

The following are known limitations that may occur in environments with ClusterXL VE, when VMotion is enabled and Avatar mode is installed.

Non-supported R71 Features

ID	Unsupported Feature
00527307	Enabling "Send Error pages" in IPS is not supported.
00527310	ISN scrambling (spoofing) protection is not supported.
00527312	The SYN attack protection in IPS is not supported.
00565933	vMAC is not supported for ClusterXL VE.

Network Limitations

ID	Description
00527318	After a Virtual Machine migrates from one ESX host (source) to another (destination), the Security Gateway - Virtual Edition member on the source ESX host continues to handle existing connections for this Virtual Machine. If the source member fails, existing connections are dropped.

General

ID	Description
00553212	ClusterXL VE supports up to four cluster members.
00528627	To work in Avatar mode, you must install Security Gateway - Virtual Edition on all ESX Cluster members.