Check Point
SOFTWARE TECHNOLOGIES LTD.

Security Gateway Virtual Edition

R71

Release Notes

29 September 2010

Important Information

Latest Version

The latest version of this document is at:
http://supportcontent.checkpoint.com/documentation_download?ID=11535

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

Revision History

Date	Description
28 September 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 Release Notes).

Contents

Introduction

Check Point Security Gateway Virtual Edition protects dynamic virtual environments and external networks from internal and external threats by securing virtual machines and applications. This solution uses proven security Check Point technologies: Software Blade architecture, Firewall with content inspection, IPS, central management, and more.

Security Gateway Virtual Edition has different operation modes. Decide which is best for your environment and plan the installation accordingly.

- **The Hypervisor Mode** enforces VM security within the VMware *Hypervisor* by inspecting inter-VM traffic, without changing the virtual network topology.
- **The Network Mode** is deployed as a virtual network device to protect virtual networks and physical environments. You can configure it as a router or a bridge, in the same way as a physical gateway.

What's New

Hypervisor Mode:

- Protects VMs and traffic between VMs.
- Secures dynamic virtual environments without network topology VM changes.
- Supports VMware VMsafe.
- Protects against security breaches caused by configuration errors.
- Gives out-of-the-box protection with easy configuration.
- Supports R71 Software Blade architecture.
- Maximizes security granularity at the vSwitch, port group, and VM levels.
- Supports ESX clusters for VM high availability and load sharing.
- Enforces security with no downtime during vMotion migration.
- Lets growing enterprises protect expanding virtual networks while reducing hardware investment, maintenance, energy, and site costs.
- Optimizes performance for virtual environments.

Network Mode:

- Operates as a layer-2 or layer-3 Security Gateway for virtual network environments.
- Supports ClusterXL for high availability and load sharing.
- Enforces security with no downtime during vMotion migration.
- Supports vMotion on the Security Gateway Virtual Edition virtual machine.
- Lets growing enterprises protect expanding virtual networks while reducing hardware investment, maintenance, energy, and site costs.
- Optimizes performance for virtual environments.

Selecting an Operation Mode

To select the mode that is optimal for your environment, compare VMware and Check Point features.

VMware Features	Hypervisor Mode	Network Mode
VMotion for 3rd party VMs	Yes	Yes
VMotion for the Security Gateway Virtual Edition VM	No	Yes
DRS	Yes	Yes
VMSafe Integration	Yes	No
vShield	No	No
Fault Tolerance	No	No
DVS	Yes	Yes
Nexus 1000v	Yes	Yes

Features and Software Blades	Hypervisor Mode	Network Mode
Firewall	Yes	Yes
NAT	No	Yes
VPN	No	Yes
IPS	Yes	Yes
URL Filtering	Yes	Yes
Email Security and Anti-Spam	No	Yes
CoreXL	No	Yes
ClusterXL	No	Yes
IPv6	No	Yes
Anti-Malware	Limited*	Yes

* See 00525807 in Known Limitations ("Non-supported R71 Features" on page 9).

System Requirements

Item	Minimum	Recommended	Notes
Memory	512 MB	2.5 GB	Add more memory to inspect many connections concurrently.
Disk Space	12 GB	12 GB	
Number of Virtual CPUs	1	2	

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	976141014 To verify: `fw ver -k`
VMware Platform	VMware vSphere 4.0
Check Point Security Management Server or Provider-1 MDS	R71 or higher

Note - Security Gateway Virtual Edition is based on the R71.10 Security Gateway.

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 Limitations

Note - All Security Gateway R71 and R71.10 limitations (http://supportcontent.checkpoint.com/solutions?id=sk44993) apply also to Security Gateway Virtual Edition.

In this section:

VMware Feature Limitations

ID	Description
00525821	You cannot use VMware Fault Tolerance on any VMs, including the Security Gateway Virtual Edition VM.
00575640	Cloning and templates are supported for Security Gateway Virtual Edition VM, if: • The VM is a newly deployed Security Gateway Virtual Edition (immediately following the first boot). • You have not yet configured any Check Point products. • You have not yet done any configuration steps, such as `sysconfig` or `cpconfig`.

Network Limitations

ID	Description
00566045	The SecurePlatform WebUI is disabled until you assign an IP address to one of its network adapters.
00557690	Dynamic Routing is not supported.

General Limitations

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

ID	Description
00525830	Upgrade to R71 is not supported. You must install Security Gateway Virtual Edition R71 as a clean installation.
00527267	Performance Pack Heavy Load Quality of Service feature (HLQoS) is not supported.
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).
00568259	You can configure up to 2 virtual CPUs for the Security Gateway Virtual Edition.

Hypervisor Mode Limitations

In this section:

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: • E-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 is not supported.
00527315	CoreXL is not supported.
00568687	VoIP is not supported.
00575642	Header spoofing protection is not supported.

Network Limitations

ID	Description
00518814	When a VM operates as a router for other VMs, you must configure these settings: 1. Run `sysconfig` to configure the routing VM security setting to **bypassed**. 2. Do not configure IP Anti-spoofing for VMs that use the routing VM as a default gateway.
00526860	When a VM operates as a bridge for other VMs, run sysconfig to configure the bridge-VM security setting to **bypassed**.
00525805	You cannot configure a VLAN using the VM guest operating system in an ESX environment. Configure the VLAN using a vSwitch.
00526946	Hypervisor Mode does not support duplicate IP or MAC addresses for different VMs.
00552805	You cannot change a vNIC MAC address using the guest operation system.
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 VM 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 VMs.
00568524	IPv6 is not supported.

ESX Configuration Limitations

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

General Limitations

ID	Description
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.

Hypervisor Mode Cluster Deployment Limitations

In this section:

Non-supported R71 Features

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

Network Limitations

ID	Description
00527318	After a VM migrates from one ESX host (source) to another (destination), the source member continues to inspect existing connections. If the source member fails, existing connections are dropped.

General

ID	Description
00553212	Hypervisor Mode supports up to ten cluster members.
00528627	You must install Hypervisor Mode on all ESX Cluster members.
00575645	VMs that operate as routers for other VMs are not supported in ESX cluster deployments.