Check Point
SOFTWARE TECHNOLOGIES LTD.
SECURE YOUR EVERYTHING™

CloudGuard Network Security
Gateway Performance for VMWare ESXi

CloudGuard Cloud Network Security, part of the CloudGuard Cloud Native Security platform, provides advanced threat prevention and automated cloud network security through a virtual security gateway, with unified security management across all your multi-cloud and on-premises environments.

For public clouds, CloudGuard provides automated and elastic public cloud network security to keep assets and data protected while staying aligned to the dynamic needs of public cloud environments.

For private clouds, CloudGuard delivers dynamic security within virtual datacenters to prevent the lateral spread of threats while consolidating visibility and management across physical and virtual networks.

Advanced Threat Prevention

Provides North-South and East-West protection of cloud assets

Automated Network Security

Supports rapid deployment, agility and automation of CI/CD workflows

Unified Management Across All Clouds

Consistent policy to manage security across on-prem and multi-cloud environments

Performance: CloudGuard Network Security (R80.30/R80.40) on VMWare ESXi

Notes:
- Next Generation Firewall (NGFW) throughput is measured with FW, IPS, Application Control features enabled (see table 2 below), using Check Point Enterprise testing conditions.
- Next Generation Threat Prevention (NGTP) throughput is measured with FW, IPS, Application Control, URL Filter, Anti-Virus, Anti-Bot features enabled (see table 2 below), using Check Point Enterprise testing conditions.
- Testing conducted on PowerEdge R630 with Intel® Xeon® CPU E5-2630 v3 @ 2.40GHz, Testing RAM size was 8GB, Network Interface: Intel® 82599EB 10-Gigabit SFI/SFP+ Network Connection.

It is recommended to run additional testing within your environment to ensure your performance requirements are met. Your performance may vary depending on underlying cloud vendor infrastructure performance.

	2 vCPU	4 vCPU	8 vCPU
Virtual network adaptor/device driver	VMXNET3	VMXNET3	ixgben
CPS (connections per second)	40K*	70K*	140K*
FW Only	7.5Gbps	10Gbps	10Gbps
FW + IPS	4Gbps	6Gbps	10Gbps
NGFW (FW + IPS + Application Control)	2.8Gbps	4.6Gbps	9Gbps
NGTP (NGFW + URL Filter + Anti-Virus + Anti-Bot)	1Gbps	1.8Gbps	4.5Gbps
*Accuracy range: +/-15% Concurrent Connections depending on the size of the RAM: 240K per 1GB of RAM			

Check Point®
SOFTWARE TECHNOLOGIES LTD.

WELCOME TO THE FUTURE OF CYBER SECURITY

Content Security

First Time Prevention Capabilities

- OS-level and static file analysis
- File disarm and reconstruction via Threat Extraction
- Average emulation time for unknown files that require full sandbox evaluation is under 100 seconds
- Maximal file size for Emulation is 100 MB
- Emulation OS Support: Windows XP, 7, 8.1, 10

Applications

- Use 8,000+ pre-defined or customize your own applications
- Accept, prevent, schedule, and apply traffic-shaping

Data Loss Prevention

- Classify 700+ pre-defined data types
- End user and data owner incident handling

Dynamic User-based Policy

- Integrates with Microsoft AD, LDAP, RADIUS, Cisco pxGrid, Terminal Servers and with 3rd parties via a Web API
- Enforce consistent policy for local and remote users on Windows, macOS, Linux, Android and Apple iOS platforms

Network

High Availability

- Active/Active L2, Active/Passive L2 and L3*
- Session failover for routing change, device and link failure

*Not applicable for cloud service providers usage

IPv6

- NAT66
- CoreXL, SecureXL

Unicast and Multicast Routing (see SK98226)

- OSPFv2, BGP, RIP
- Static routes, Multicast routes
- Policy-based routing
- PIM-SM, PIM-DM, IGMP v2, and v3

All-inclusive Security

	NGFW	NGTP	NGTX
	Basic access control	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓	✓
VPN (IPsec)	✓	✓	✓
IPS	✓	✓	✓
Application Control	✓	✓	✓
Content Awareness	✓	✓	✓
URL Filtering		✓	✓
Anti-Bot		✓	✓
Anti-Virus		✓	✓
Anti-Spam		✓	✓
SandBlast Threat Emulation			✓
SandBlast Threat Extraction			✓

Each gateway requires a license for the enabled security feature.