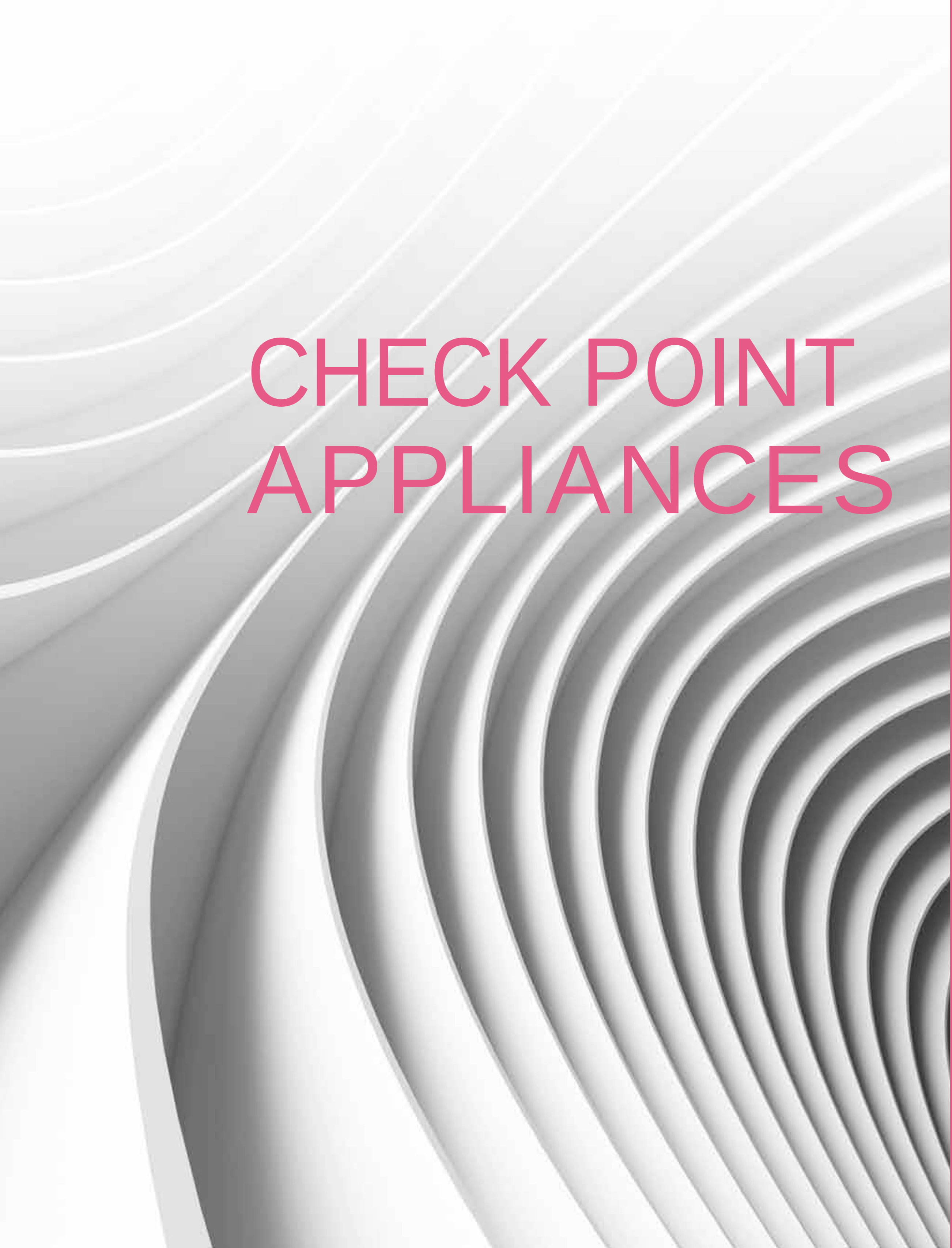
Check Point
SOFTWARE TECHNOLOGIES LTD.

CHECK POINT APPLIANCES



2017

TABLE OF CONTENTS

CHECK POINT APPLIANCES

NEXT GENERATION THREAT PREVENTION

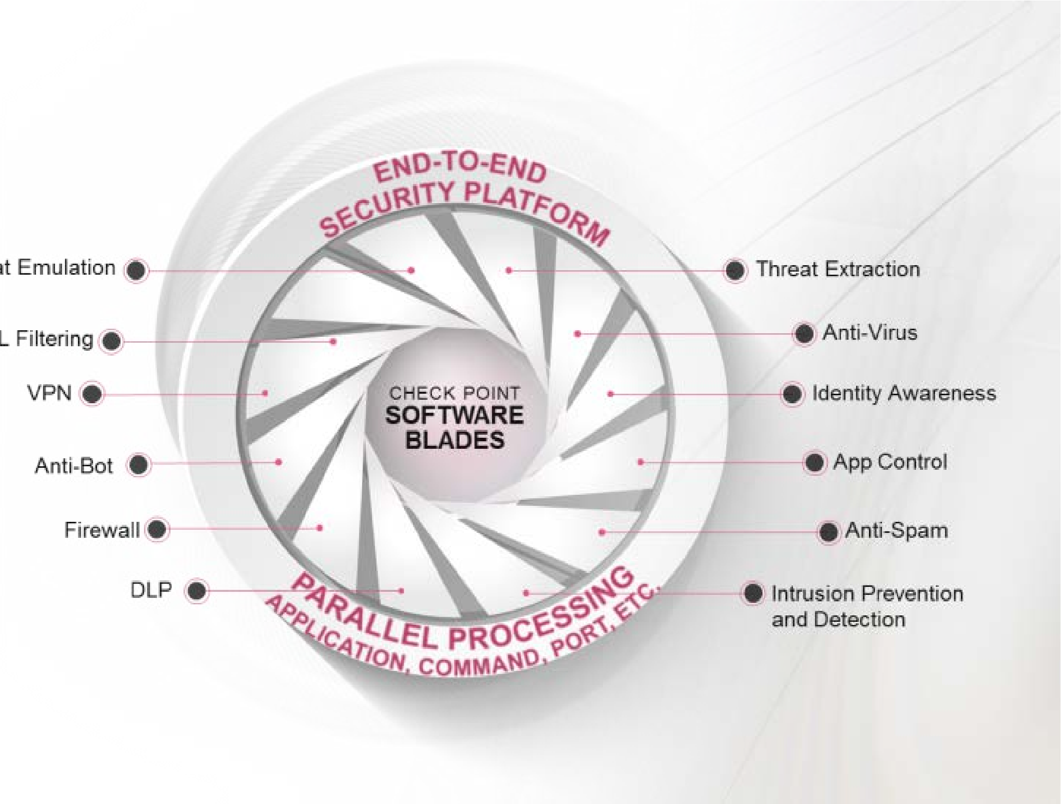
COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats requires a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention to combat these emerging threats while reducing complexities and increasing operational efficiencies. The Check Point Threat Prevention solution includes powerful security features such as firewall, IPS, Anti-Bot, Antivirus, Application Control, and URL Filtering to combat known cyber-attacks and threats – now enhanced with the award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

PREVENT KNOWN AND ZERO-DAY THREATS

As part of the Check Point SandBlast Zero-Day Protection solution, the cloud-based Threat Emulation engine detects malware at the exploit phase, even before hackers can apply evasion techniques attempting to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to discover malicious behavior before it enters your network. This innovative solution combines cloud-based CPU-level inspection and OS-level sandboxing to prevent infection from the most dangerous exploits, and zero-day and targeted attacks.

Furthermore, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, reconstructs files to eliminate potential threats, and promptly delivers sanitized content to users to maintain business flow.



A SECURE NEXT-GEN OS SIZED FOR YOU

GAIA – A UNIFIED SECURE OPERATING SYSTEM

Check Point GAiA™ is the next generation Secure Operating System for all Check Point Appliances, Open Servers and Virtualized Gateways. Customers benefit from the highly efficient 64-bit OS, improved appliance connection capacity and streamlined operational processes. GAiA simplifies management with segregation of duties among users with different privileges by enabling role-based administration. The automatic software update capabilities increases operational efficiency and the intuitive and feature-rich web interface allows for search of any command or property in a second. IPv4 and IPv6 networks are secure with acceleration and clustering technologies and support for the latest unicast and multicast routing protocols.

TAP THE POWER OF VIRTUALIZATION

Check Point Virtual Systems enable organizations to consolidate infrastructure by creating multiple virtualized security gateways on a single hardware device, offering significant cost savings with seamless security and infrastructure consolidation. The streamlined management of the virtualized gateways further improves the operational efficiency of a resource-challenged IT department, bringing the needed simplicity to network security.

THE NEW WAY TO MEASURE THE REAL POWER OF SECURITY APPLIANCES

Unlike other vendors who provide performance numbers based upon optimal testing conditions and using a security policy that has only one rule, Accept Any, Check Point security appliance performance is based upon real-world customer traffic, multiple security functions and a typical security policy. SecurityPower™ provides an effective metric for selecting the right appliance that better predicts its current and future behavior under security attacks and in day to day operation. Customers are ensured they are getting a security appliance that meets their current needs and provides room for growth.

SecurityPower

SECURITY GATEWAYS

Check Point provides customers of all sizes with the latest data and network security protection in an integrated next generation threat prevention platforms, reducing complexity and lowering the total cost of ownership. Whether you need next-generation security for your data center, enterprise, small business or home office, Check Point has a solution for you.

Branch Office	Deployment	Branch or Small Office	1400
	Form Factor	Desktop	3100, 3200
	Interfaces	1 GbE, 802.11n/ac Wi-FI, 3G/4G, PoE	5100
	FW Throughput	750 Mbps to 14.5 Gbps	
	Special Features	Web management	
Enterprise	Deployment	Enterprise	5200
	Form Factor	1RU	5400, 5600
	Interfaces	1, 10, 40 GbE	5800, 5900
	FW Throughput	3 to 52 Gbps	
	Special Features	Flexible IO options, LOM	
Data Center	Deployment	Large enterprise, Data center	15400, 15600
	Form Factor	2RU	23500, 23800
	Interfaces	1, 10, 25, 40, 100 GbE	
	FW Throughput	25 to 128 Gbps	
	Special Features	25/40/100 GbE, DC power, LOM	
Chassis Systems	Deployment	Data center, Telco, Carrier	44000
	Form Factor	6RU to 16RU	64000
	Interfaces	1, 10, 40, 100 GbE	
	FW Throughput	80 to 880 Gbps	
	Special Features	DC power, scalable platform	
Rugged	Deployment	Harsh environments	1200R
	Form Factor	Desktop, DIN mount	
	Interfaces	1 GbE, 3G/4G support	
	FW Throughput	2 Gbps	
	Special Features	AC/DC power	

1400 APPLIANCES

BRANCH OFFICE SECURITY

1430-1450
(WI-FI OPTION)

1470-1490
(WI-FI OPTION)

OVERVIEW

Enforcing consistent network security throughout an enterprise is challenging when the enterprise border extends to remote and branch offices where there are a few users with little to no IT expertise. Remote and branch offices require the same level of protection from sophisticated cyber-attacks and zero-day threats as main corporate offices. The Check Point 1400 Appliances are a simple, affordable and easy to deploy all-in-one solution for delivering industry leading security to protect the weakest link in your enterprise network — the remote branch offices.

You can now protect your entire network from cyber threats with award-winning Check Point Threat Prevention — from the headquarters to the remote offices. The 1400 Appliances are ideal for small offices. For local management and support in a small office environment, an easy and intuitive web-based local management interface is available. Enterprises who want to manage security from a central office can leverage Check Point Security Management or Multi-Domain Security Management to remotely manage and apply a consistent security policy to hundreds of devices across the field offices.

ALL-INCLUSIVE SECURITY

THREAT PREVENTION

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

A wide variety of network interface options are available including 1GbE Ethernet ports, PoE, 802.11b/g/n/ac WiFi with guest acccess, 3G and 4G wireless connections.

Maximum Capacities	1430	1450	1470	1490
Firewall throughput[1]	900 Mbps	1.1 Gbps	1.6 Gbps	1.8 Gbps
Threat prevention throughput[1]	90 Mbps	150 Mbps	175 Mbps	220 Mbps
1 GbE ports	1x WAN, 1x DMZ, 6x LAN switch		1x WAN, 1x DMZ, 16x LAN switch	
Wi-Fi option	802.11 b/g/n/ac, single band 2.4 or 5GHz		802.11 b/g/n/ac, dual band 2.4 and 5GHz	
PoE option	✗		✓	

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/1400-security-appliances

1200R RUGGED APPLIANCE

SECURITY FOR HARSH ENVIRONMENTS

1200R

OVERVIEW

Protecting critical infrastructure from cyberattacks poses unique challenges. The environments can be harsh and systems often use specialized protocols. Check Point's ICS/SCADA cyber security solutions provide advanced threat prevention paired with ruggedized appliance options and comprehensive protocol support to ensure vital assets such as power generation facilities, traffic control systems, water treatment systems and factories are never compromised.

The 1200R appliance complements our extensive appliance family to support a diverse range of deployment environments and meet specialized requirements. For instance, the 1200R complies with industrial specifications such as IEEE 1613 and IEC 61850-3 for heat, vibration and immunity to electromagnetic interference (EMI). In extreme temperatures from -40°C to 75°C where other appliances would fail, this appliance keeps you secure.

ALL-INCLUSIVE SECURITY PACKAGES

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

Copper and fiber 1GbE Ethernet ports are included as is 3G and 4G wireless connection support through compatible USB modems.

Maximum Capacities	1200R
Firewall throughput (Mbps) [1]	700
IPS throughput (Mbps) [1]	60
WAN	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
DMZ	1x 10/100/1000BaseT RJ45 or 1x 1000BaseF port
LAN	4x 10/100/1000BaseT RJ45 ports
Mount Options	DIN rail or rack mount
Industrial Certifications	IEEE 1613, IEC 61850-3
Power	AC or DC

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/industrial-control-systems-appliances

3000 APPLIANCES

ENTERPRISE SECURITY FOR BRANCH OFFICES

3100

3200

OVERVIEW

Seamless security requires consistent protections across all locations, not just at the main corporate network. The same level of protection is required for remote and branch offices—to form a unified and total defense against potential threats. The Check Point 3000 Appliances are an ideal solution for delivering security to small and branch offices.

The 3000 Appliances offer enterprise-grade security without compromise in a compact desktop form factor. Multi-core technology, six 1 Gigabit Ethernet ports and advanced threat prevention capabilities easily extends robust security to remote branch locations and small offices. Despite the small form factor, these powerful appliances provide up to 2.1 Gbps of real-world firewall throughput and up to 160 Mbps of real-world threat prevention throughput.

ALL-INCLUSIVE SECURITY PACKAGES

THREAT PREVENTION

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

The compact design, multi-core technology and SandBlast Zero-Day Protection available in the 3000 Appliances make these gateways ideally suited for deployment in small offices and remote branch offices.

Maximum Capacities	3100	3200
Firewall throughput (Gbps) [1]	2.1	2.1
NGFW (Firewall, Application Control, IPS) throughput (Mbps) [1]	220	260
Threat prevention throughput (Mbps) [1]	130	160
1 GbE ports (Copper)	6	
RAM	8 GB	
Storage	1x 320GB (HDD) or 1x 240GB (SSD)	
Enclosure	Desktop	

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/3000-security-appliances

5000 APPLIANCES

ENTERPRISE SECURITY, FLEXIBLE NETWORK OPTIONS

5100

5200

5400

5600

5800

5900

OVERVIEW

Security decisions no longer have to be a choice between features and performance. The purpose-built Check Point 5000 appliances provide the most advanced threat prevention security without compromise for demanding small to midsize enterprise networks.

The Check Point 5000 Appliances combine multiple network interface options with high-performance multi-core capabilities — delivering exceptional multi-layered security protection without compromising on performance. The 5000 Appliances pack a maximum of sixteen (26) 1 Gigabit Ethernet ports, redundant hot-swappable power supplies and an optional out-of-band LOM module into a compact 1U rack mountable form-factor. Supporting up to 26 Gbps of real-life firewall throughput and 1.65 Gbps of real-life threat prevention throughput, these appliances offer the best performance for its class.

ALL-INCLUSIVE SECURITY PACKAGES

THREAT PREVENTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 5000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	5100	5200	5400	5600	5800	5900
Firewall throughput (Gbps) [1]	4.2	5.3	10	17.5	22	26
Threat prevention throughput (Gbps) [1]	250 Mbps	290 Mbps	395 Mbps	645 Mbps	1.035	1.65
1 GbE ports (Copper)	14	14	18	18	26	26
1 GbE ports (Fiber)	4	4	4	4	8	8
10 GbE ports (Fiber)				4	8	8
RAM	16 GB	16 GB	32 GB	32 GB	32 GB	32 GB
Storage	1x 500GB (HDD) or 1x 240GB (SSD)					2x drives
AC or DC Power Supply Units	1	1	1	2	2	2
Lights Out Management	✓	✓	✓	✓	✓	✓
Network expansion slots	1	1	1	1	2	2

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/5000-security-appliances

15000 APPLIANCES

LARGE ENTERPRISE THREAT PREVENTION

15400

15600

OVERVIEW

Large enterprises have uncompromising needs for performance, uptime and scalability. The 15000 Appliances combine the most comprehensive security protections with purpose-built hardware. These powerful security appliances are optimized to deliver real-world threat prevention throughput of up to 3 Gbps to secure your most critical assets.

The Check Point 15000 Appliances are ideal for large enterprise networks that require high performance and flexible I/O options. If you're ready to move from 10 to 25, 40 or 100 GbE, so are the 15000 Appliances. These are 2U appliances with three I/O expansion slots for high port capacity, redundant AC or DC power supplies, a 2x 1TB (HDD) or 2x 480GB (SSD) RAID1 disk array, and Lights-Out Management (LOM) for remote management.

ALL-INCLUSIVE SECURITY PACKAGES

THREAT PREVENTION

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 15000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	15400	15600
Firewall throughput (Gbps) [1]	30	30
Threat prevention throughput (Gbps) [1]	1.695	3
1 GbE ports (Copper)	26	26
10 GbE ports (Fiber)	12	12
40 GbE ports (Fiber)	4	4
100/25 GbE ports (Fiber)	4	4
RAM	64 GB	64 GB
Storage	2x 1TB (HDD) or 2x 480GB (SSD)	
AC or DC Power Supply Units	2	2
Lights Out Management	✓	✓
Virtual Systems	40	80

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/15000-security-appliances

23000 APPLIANCES

DATA CENTER THREAT PREVENTION

23500

23800

OVERVIEW

Data centers have uncompromising needs for performance, uptime and scalability. The 23000 Appliances combine the most comprehensive security protections with purpose-built hardware. These powerful security appliances are optimized to deliver real-world threat prevention throughput of up to 4.5 Gbps to secure your most critical assets.

The Check Point 23000 Appliances are ideal for data center networks that require high performance and flexible I/O options. If you're ready to move from 10 to 25, 40 or 100 GbE, so are the 23000 Appliances. These are 2U appliances with five I/O expansion slots for high port capacity, redundant AC or DC power supplies, a 2x 1TB (HDD) or 2x 480GB (SSD) RAID1 disk array, and Lights-Out Management (LOM) for remote management.

ALL-INCLUSIVE SECURITY PACKAGES

THREAT PREVENTION

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

The modular design and the wide variety of network options available in the 23000 series of appliances not only provides a rich set of connectivity options for these gateways, they also make the gateways highly customizable to be suited for deployment in any network environment.

Maximum Capacities	23500	23800
Firewall throughput (Gbps) [1]	34	43
Threat prevention throughput (Gbps) [1]	2.9	3.6
1 GbE ports (Copper)	42	42
10 GbE ports (Fiber)	20	20
40 GbE ports (Fiber)	4	4
100/25 GbE ports (Fiber)	4	4
RAM	128 GB	128 GB
Storage	2x 1TB (HDD) or 2x 480GB (SSD)	
AC or DC Power Supply Units	2	2
Lights Out Management	✓	✓
Virtual Systems	125	250

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/23000-security-appliances

44000, 64000 SECURITY SYSTEMS

SCALABLE MULTI-BLADE PERFORMANCE

44000 AND 64000 SECURITY SYSTEM

OVERVIEW

When it comes to protecting the most demanding network environments of data centers, telecommunication and cloud service providers, security and performance are two critical factors that cannot be compromised. The multi-blade hardware and software architecture in the 44000 and 64000 Security Systems is ideal for these environments. The platform provides scalable real-world firewall throughput up to 240 Gbps in the 44000 and up to 539 Gbps in the 64000 platform.

ALL-INCLUSIVE SECURITY PACKAGES

THREAT PREVENTION

Check Point SandBlast™ ZERO-DAY PROTECTION

THREAT PREVENTION + SANDBLAST

HIGH LEVEL OVERVIEW

Designed from the ground-up to support the reliability, availability and serviceability requirements of data centers and service providers, the carrier-grade ATCA chassis runs in High Availability and Load Sharing modes among Security Gateway Modules in one chassis. Add another chassis operating in High Availability mode to further improve redundancy — ensuring mission-critical assets are always available and protected.

Maximum Capacities	44000	64000
Firewall throughput (Gbps) [1]	up to 240	up to 539
100 GbE ports (Fiber)	up to 4	up to 4
40 GbE ports (Fiber)	up to 12	up to 12
10 GbE ports (Fiber)	up to 64	up to 64
Security Switch Modules	1 to 2	2
Security Gateway Modules	1 to 6	2 to 12
Power Supply Units	4 AC	6 AC or 2 DC

[1] performance with a real-world traffic blend, a typical rule-base, NAT and logging enabled and the most secure threat prevention

For more information: www.checkpoint.com/products/44000-64000-security-systems

VIRTUAL APPLIANCES

PUBLIC AND PRIVATE CLOUD SECURITY

The wide adoption of cloud architectures—whether public, private or hybrid—is being driven by the desire to transform businesses for greater efficiency, speed, agility and cost controls. While the cloud offers many advantages over traditional infrastructure it also exposes your company to whole new set of security challenges. Check Point offers a complete public and private cloud security portfolio that seamlessly extends security protections to any cloud environment, so you can feel as confident about the cloud as you do about your physical environment.

PUBLIC CLOUD SECURITY CHALLENGES

When you move computing resources and data to the public cloud, security responsibilities become shared between you and your cloud service provider. The loss of control in moving applications and data out of the enterprise to a cloud provider—such as Amazon Web Services or Microsoft Azure—and the resulting challenges in monitoring and governing those resources, create a variety of security concerns. This is especially true because of the anonymous, multi-tenant nature of the public cloud.

Many companies use hybrid clouds to maintain control of their private cloud infrastructure and protect confidential assets while outsourcing other aspects to public clouds. With the hybrid cloud the new challenge is to protect data as it moves back and forth from the enterprise to a public cloud.

Check Point vSEC delivers advanced threat protection and single pane-of-glass management for easily extending security to protect your data and assets in public cloud environments.

PRIVATE CLOUD SECURITY CHALLENGES

As enterprises adopt Software-defined networking and private cloud environments, the increased agility and efficiency has been a boon to the business but has led to dramatic increases in network traffic going east-west within the data center. This shift in traffic patterns introduces new security challenges. With few controls to secure east-west traffic, threats can travel unimpeded once inside the data center. And traditional approaches to security cannot keep pace with the dynamic nature of virtual environments where applications are constantly provisioned in and out.

Check Point vSEC seamlessly delivers advanced threat protections to private cloud infrastructure and provides the visibility and control effectively manage security in both physical and virtual environments–all from a single unified management solution.

PUBLIC CLOUD				PRIVATE CLOUD			DATA CENTER
AMAZON WEB SERVICES	MICROSOFT AZURE	VMWARE VCLOUD AIR	GOOGLE CLOUD PLATFORM	vSEC FOR VMWARE NSX	vSEC FOR CISCO ACI	vSEC FOR OPENSTACK	VIRTUAL EDITION

For more information: www.checkpoint.com/products-solutions/private-public-cloud

SMART-1 APPLIANCES

CYBER SECURITY MANAGEMENT IN THE ERA OF BIG DATA

SMART-1 405, 410, 225, 3050, 3150 APPLIANCES

OVERVIEW

In order to manage the security environment efficiently and effectively, organizations need security management solutions to also be efficient, effective and to process more data faster than ever before. Check Point Smart-1 Appliances consolidate security management, including logging, event management, and reporting into a single dedicated management appliance. Organizations can now efficiently manage the data and event management requirements of the Bid Data era, gaining centralized visibility into billions of logs, visual indication of risks, and the ability to quickly investigate potential threats.

UNIFIED, INTELLIGENT SECURITY MANAGEMENT

SINGLE DOMAIN SECURITY MANAGEMENT

MULTI-DOMAIN SECURITY MANAGEMENT

MULTI-DOMAIN LOG MANAGEMENT

SMARTEVENT EVENT MANAGEMENT

HIGH LEVEL OVERVIEW

Organizations can leverage Smart-1 Appliances to manage from 5 to 5,000 gateways. With Smart-1 Multi-Domain Management you can segment the network into as many as 200 independent domains. In addtion Smart-1 Appliances provide up to 12 TB of built-in storage as well as high-performance fiber channel connectivity to Storage Area Networks (SANs) for external storage.

Maximum Capacities	405	410	225	3050	3150
Managed Gateways	5	10	25	50	150+
Maximum Domains (Multi-Domain Management)[1]	×	×	×	50	200
Indexed Logs/Sec	6,000	10,000	11,000	26,000	44,000
SmartEvent Log Size/Day (GB)	3.5	6.5	13	40	100
HDD	1x 1TB	1x 2TB	2x 2TB	4x 2TB	12x 2TB
RAM	16 GB	32 GB	32 GB	256 GB	256 GB
Fiber Channel SAN Card	×	×	✓	✓	✓

For more information: www.checkpoint.com/products/smart-1-appliances

DDOS PROTECTORS

STOP DENIAL OF SERVICE IN SECONDS

506 / 1006 / 2006

4412 / 8412 / 12412

10420 / 20420 /30420 / 40420

OVERVIEW

Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are increasing in number, speed and complexity in recent years. These attacks are relatively easy to carry out, and can cause serious damage to companies who rely on web services to operate. Many DDoS protection solutions are deployed by an Internet Service Provider, offering generic protections against network layer attacks. However today's DDoS attacks have become more sophisticated, launching multiple attacks at network and application layers. Successful DDoS solutions will offer companies the ability to customize their protections to meet changing security needs, fast response time during an attack, and a choice of deployment options.

DDoS Protector Appliances offer flexible deployment options to easily protect any size business, and integrated security management for real-time traffic analysis and threat management intelligence for advanced protection against DDoS attacks. Check Point also provides dedicated 24/7 support and resources to ensure up-to-the-minute protections.

MULTI-LAYERED PROTECTIONS

NETWORK & TRAFFIC FLOOD

APPLICATION BASED DOS/DDOS

HIGH LEVEL OVERVIEW

Check Point DDoS Protector™Appliances block Denial of Service attacks within seconds with multi-layered protection and up to 40 Gbps of performance. DDoS Protectors extend company's security perimeters to block destructive DDoS attacks before they cause damage.

Maximum Capacities	Enterprise	Data Center	Carrier
Throughput (Gbps) [1]	500 Mbps to 2 Gbps	4 to 12 Gbps	10 to 40 Gbps
Max Concurrent Sessions	2,000,000	4,000,000	6,000,000
Max DDoS Flood Attack Prevention Rate (pps)	1,000,000	10,000,000	25,000,000
Latency	< 60 microseconds		
10/100/1000 Copper Ethernet	4	8	
10 GbE (SFP+)			20
40 GbE QSFP			4
Network Operation	Transparent L2 Forwarding		
High Availability	Active-Passive Cluster		

[1] Throughput is measured with behavioral IPS protections and signature IPS protections using eCommerce protection profile

For more information: www.checkpoint.com/products/ddos-protector/

SANDBLAST APPLIANCES

PRIVATE CLOUD ZERO DAY THREAT PREVENTION

TE100X

TE250X

TE1000X

TE2000X

OVERVIEW

With the increase in sophistication of cyber threats, many targeted attacks begin with exploiting software vulnerabilities in downloaded files and email attachments. These threats include new exploits, or even variants of known exploits unleashed almost daily with no existing signatures and therefore no standard solutions to detect those variants. New and undiscovered threats require new solutions that go beyond signatures of known threats.

Check Point SandBlast Zero-Day Protection, with evasion-resistant malware detection, provides comprehensive protection from even the most dangerous attacks while ensuring quick delivery of safe content to your users. At the core of our solution are two unique capabilities – Threat Emulation and Threat Extraction that take threat defense to the next level.

STOP NEW AND UNKNOWN THREATS

THREAT EMULATION

THREAT EXTRACTION

HIGH LEVEL OVERVIEW

We offer a wide range of SandBlast Appliances.These are perfect for customers who have regulatory or privacy concerns preventing them from using the SandBlast Threat Emulation cloud-based service.

Maximum Capacities	TE100X	TE250X	TE1000X	TE2000X
Recommended Files/Month	100K	250K	1M	2M
Recommended Users	up to 1,000	up to 3,000	up to 10,000	up to 20,000
Throughput	150 Mbps	700 Mbps	2 Gbps	4 Gbps
Number of Virtual Machines	4	8	28	56
10/100/1000Base-T RJ45	13	17	14	14
10 GBase-F SFP+	-	-	6	8
Enclosure	1U	1U	2U	2U
HDD	1x 1TB		2x 2TB RAID1	
Power Supply Units	1	2	2	2

For more information: www.checkpoint.com/products-solutions/threat-prevention-appliances-and-software

PROVEN SECURITY

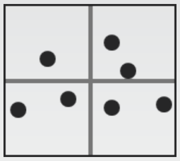
RECOGNIZED LEADER

When you purchase a Check Point product, rest assured that you are buying a product from a leader in the security industry and a product recognized by leading test and analyst firms.

GARTNER

ENTERPRISE NETWORK FIREWALLS

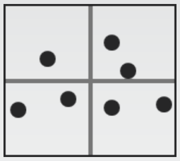
Leader Since1997[1]



GARTNER

UNIFIED THREAT MANAGEMENT

Leader 6 Years in a Row[2]



NSS LABS

RECOMMENDED

- Firewall
- Next Generation Firewall
- IPS
- Breach Detection Systems

NSS Labs RECOMMEND

ICSA labs CERTIFIED FIREWALL - CORPORATE

ICSA labs CERTIFIED IPSEC - BASIC

FIPS VALIDATED 140-2

Common Criteria

Additional certifications include; NATO Information Assurance Product Catalogue, Common Criteria Medium Robustness, Defense Information Systems Agency (DoD certification of firewall, VPN, IDS and IPS), Commercial Solutions for Classified Program, IPv6 Ready, VPN Consortium. Learn more at www.checkpoint.com.

[1] Gartner, Inc., Gartner Magic Quadrant for Enterprise Network Firewalls, Adam Hils, Jeremy D'Hoinne, Rajpreet Kaur, Greg Young, 25 May 2016.

[2] Gartner, Inc., Magic Quadrant for Unified Threat Management, Jeremy D'Hoinne, Adam Hils, Greg Young, Rajpreet Kaur, 21 June 2017.

Contact Check Point Now

www.checkpoint.com/about-us/contact-us

By phone in the US: 1-800-429-4391

1-650-628-2000

Check Point
SOFTWARE TECHNOLOGIES LTD.

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: 650-654-4233 | www.checkpoint.com

©2017 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content | August 30, 2017 | Page 18