

CHECK POINT 3200 APPLIANCE



CHECK POINT 3200 APPLIANCE

Branch and small office security
in a compact form factor

Product Benefits

- Enable the most advanced threat prevention security
- Optimal performance even when inspecting SSL encrypted traffic
- Future-proofed technology safeguards against tomorrow's risks
- Simplify administration with a single integrated management console

Product Features

- Compact desktop form factor
- Simple deployment and management
- Secure branch office connections with site-to-site and client-to-site VPN
- Redundant appliance clustering technologies eliminate a single point of failure

OVERVIEW

The Check Point 3200 Appliance combines the most comprehensive security protections to safeguard your branch and small office deployments. The 3200 appliance is available in a compact desktop form factor with a 320 GB hard disk. This powerful security appliance is optimized to deliver real-world threat prevention to secure your critical assets and environments.

COMPREHENSIVE THREAT PREVENTION

The rapid growth of malware, growing attacker sophistication and the rise of new unknown zero-day threats require a different approach to keep enterprise networks and data secure. Check Point delivers fully integrated, comprehensive Threat Prevention with award-winning SandBlast™ Threat Emulation and Threat Extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities.

Production Environment Performance ¹	
SecurityPower™ Units (SPU)	250 SPU
Firewall throughput	2.1 Gbps
IPS throughput	460 Mbps
NGFW throughput (Firewall, Application Control, IPS)	260 Mbps
Threat prevention throughput ²	140 Mbps
Ideal Testing Conditions Performance (RFC 3511, 2544, 2647, 1242)	
Firewall throughput, 1518 byte UDP	4 Gbps
Connections per second	48,000
Concurrent connections	3.2 million
VPN throughput, AES-128	2.25 Gbps
IPS throughput	1.44 Gbps
NGFW throughput (Firewall, Application Control, IPS)	1.15 Gbps

¹ Performance measured with real-world traffic blend and content, a typical rule base, updated recommended signatures, NAT and logging enabled, ² FW, IPS, APPCTRL, AV, AB, URLF

3200 SECURITY APPLIANCE

- 1 Management 10/100/1000Base-T RJ45 port
- 2 5x 10/100/1000Base-T RJ45 ports
- 3 2x USB ports for ISO installation
- 4 RJ45/micro USB console port
- 5 Power connector



ALL-INCLUSIVE SECURITY SOLUTIONS

Check Point 3200 Appliances offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with IPS, Application Control, Antivirus, Anti-Bot, URL Filtering and Email Security.
- NGTX: NGTP with SandBlast Zero-Day Protection, which includes Threat Emulation and Threat Extraction.

INSPECT ENCRYPTED CONNECTIONS

There is a shift towards more use of HTTPS, SSL and TLS encryption to increase Internet security. At the same time files delivered into the organization over SSL and TLS represent a stealthy attack vector that bypasses traditional security implementations. Check Point Threat Prevention looks inside encrypted SSL and TLS tunnels to detect threats, ensuring users remain in compliance with company policies while surfing the Internet and using corporate data.

BEST-IN-CLASS MANAGEMENT

Every Check Point appliance can either be managed locally with its available integrated security management or via central unified management. Using local management, the appliance can manage itself and one adjacent appliance for high availability deployments. When centrally managed administrators can define security policy for the entire network — including internal security, main sites, and remote sites — from a single, centrally located Check Point Security Management server.

PREVENT KNOWN AND ZERO-DAY THREATS

The 3200 Appliance protects organizations from both known and unknown threats with Antivirus, Anti-Bot, SandBlast Threat Emulation (sandboxing), and SandBlast Threat Extraction technologies.

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.

	NGTP	NGTX
	Prevent known threats	Prevent known and zero-day attacks
Firewall	✓	✓
VPN (IPSec)	✓	✓
IPS	✓	✓
Application Control	✓	✓
Anti-Bot	✓	✓
Anti-Virus	✓	✓
URL Filtering	✓	✓
SandBlast Threat Emulation	✗	✓
SandBlast Threat Extraction	✗	✓

TECHNICAL SPECIFICATIONS

Network

Network Connectivity

- Total physical and virtual (VLAN) interfaces per appliance: 1024/4096 (single gateway/with virtual systems)
- 802.3ad passive and active link aggregation
- Layer 2 (transparent) and Layer 3 (routing) mode

High Availability

- Active/Active and Active/Passive - L3 mode
- Session synchronization for firewall and VPN
- Session failover for routing change
- Device and link failure detection
- ClusterXL or VRRP

IPv6

- Features: Firewall, Identity Awareness, Mobile Access, App Control, URL Filtering, IPS, Anti-Bot, Antivirus
- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

Virtual Systems

- Maximum: 10

Routing

Unicast and Multicast Routing (see SK98226)

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

Hardware

Base Configuration

- 6 on-board 10/100/1000Base-T RJ-45 ports
- 8 GB memory
- 1 power supply
- 1x 320 GB hard drive

Power Requirements

- AC Input Voltage: 90-264V
- Frequency: 47-63Hz
- Single Power Supply Rating: 40W
- Power Consumption Maximum: 29.5W
- Maximum thermal output: 100.7 BTU/hr.

Dimensions

- Enclosure: Desktop
- Standard (W x D x H): 8.28 x 8.27 x 1.65 in.
- Metric (W x D x H): 210.3 x 210 x 41.9 mm
- Weight: 1.3 kg (2.9 lbs.)

Operating Environmental Conditions

- Temperature: 32° to 104°F / 0° to 40°C
- Humidity: 5% to 95% (non-condensing)

Storage Conditions

- Temperature: -4° to 158°F / -20° to 70°C
- Humidity: 5% to 95% at 60°C (non-condensing)

Certifications

- Safety: UL60950-1, CB IEC60950-1, CE LVD EN60950-1, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, *REACH, *ISO14001

ORDERING INFORMATION

BASE CONFIGURATION ¹

3200 Next-Gen Threat Prevention bundled with local management for up to 2 gateways	CPAP-SG3200-NGTP
3200 Next-Gen Threat Extraction bundled with local management for up to 2 gateways	CPAP-SG3200-NGTX
3200 Next-Gen Threat Prevention Appliance for High Availability	CPAP-SG3200-NGTP-HA
3200 Next-Gen Threat Extraction Appliance for High Availability	CPAP-SG3200-NGTX-HA

SPARES AND MISCELLANEOUS

Replacement AC/DC Power Supply for 3200 appliance	CPAC-PSU-3200
Single chassis Rack Shelf for 3200 appliances	CPAC-RM-3200
Single/Dual chassis Rack Shelf for 1400/3200 appliances ²	CPAC-RM-1400/3200

¹ SKUs for 2 and 3 years are available, see the online Product Catalog, ² will be available for order in Q3 2016

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