

# CHECK POINT 3100 NEXT GENERATION SECURITY GATEWAY FOR THE BRANCH AND SMALL OFFICE



## CHECK POINT 3100 NEXT GENERATION SECURITY GATEWAY

Branch and small office security in a compact form factor

### Product Benefits

- Enable the most advanced threat prevention security
- Unique “first time prevention” for the most sophisticated zero day attack
- Optimized for 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 clustering technologies eliminate a single point of failure

## OVERVIEW

The Check Point 3100 Next Generation Security Gateway combines the most comprehensive security protections to safeguard your branch and small office deployments, all in a compact desktop form factor. This powerful Next Generation Security Gateway is optimized to deliver threat prevention for your business against present and future threats to secure your critical assets and environments.

## COMPREHENSIVE THREAT PREVENTION

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.

Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays, or let potential threats through while evaluating files, Check Point SandBlast stops more malware from entering your network. Our solution enables your employees to work safely - no matter where they are and without compromising their productivity.

## PERFORMANCE HIGHLIGHTS

| Firewall | IPS      | NGFW <sup>1</sup> | Threat Prevention <sup>2</sup> |
|----------|----------|-------------------|--------------------------------|
| 4 Gbps   | 1.1 Gbps | 850 Mbps          | 425 Mbps                       |

Performance measured under ideal testing conditions. Additional performance details on page 3.

1. Includes Firewall, Application Control, and IPS Software Blades.

2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10.

### 3100 SECURITY GATEWAY

- 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 3100 Next Generation Security Gateways offer a complete and consolidated security solution available in two complete packages:

- NGTP: prevent sophisticated cyber-threats with Application Control, URL Filtering, IPS, Antivirus, Anti-Bot 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

Check Point sets the standard for reliability and ease-of-use in security management. Consolidate all aspects of your security environment and ensure security consistency across your entire organization with unified policy management for users, data, applications and networks. In addition our integrated threat management provides full visibility into security across your infrastructure helping you monitor security continuously and stay alert to potential threats.

Every Check Point appliance can either be managed locally with the available integrated security management<sup>1</sup> or via central unified management. Using local management, the appliance can manage itself and one adjacent appliance for high availability deployments.

<sup>1</sup> not available when purchased with the SSD option

## PREVENT KNOWN AND ZERO-DAY THREATS

The 3100 Next Generation Security Gateway 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 (SandBlast)                   |
|-----------------------------|-----------------------|------------------------------------|
|                             | Prevent known threats | Prevent known and zero-day attacks |
| Firewall                    | ✓                     | ✓                                  |
| VPN (IPsec)                 | ✓                     | ✓                                  |
| IPS                         | ✓                     | ✓                                  |
| Application Control         | ✓                     | ✓                                  |
| URL Filtering               | ✓                     | ✓                                  |
| Anti-Bot                    | ✓                     | ✓                                  |
| Anti-Virus                  | ✓                     | ✓                                  |
| Anti-Spam                   | ✓                     | ✓                                  |
| SandBlast Threat Emulation  | ✗                     | ✓                                  |
| SandBlast Threat Extraction | ✗                     | ✓                                  |

## Performance

### Ideal Testing Conditions

- 4 Gbps of UDP 1518 byte packet firewall throughput
- 1.1 Gbps IPS
- 850 Mbps of NGFW<sup>1</sup>
- 425 Mbps of Threat Prevention<sup>2</sup>
- 1.7 Gbps of AES-128 VPN throughput
- 40,000 connections per second, 64 byte response
- 3.2 million concurrent connections, 64 byte response

### Real-World Production Conditions

- 160 SecurityPower Units
- 2.1 Gbps of firewall throughput
- 350 Mbps IPS
- 220 Mbps of NGFW<sup>1</sup>
- 130 Mbps of Threat Prevention<sup>2</sup>

Your performance may vary depending on different factors.

Visit [www.checkpoint.com/partnerlocator](http://www.checkpoint.com/partnerlocator) to find an appliance that matches your unique requirements.

1. Includes Firewall, Application Control and IPS Software Blades. 2. Includes Firewall, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Blades using R80.10.

## Network

### Network Connectivity

- Total physical and virtual (VLAN) interfaces per gateway: 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 failover for routing change, device and link failure
- ClusterXL or VRRP

## Networking (continued)

### IPv6

- NAT66, NAT64
- CoreXL, SecureXL, HA with VRRPv3

### 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
- 1x CPUs, 4x physical cores, 4x virtual cores (total)
- 8 GB memory
- 1 power supply
- 1x 320GB (HDD) or 1x 240GB (SSD) drive

### Power Requirements

- Single Power Supply rating: 40W
- AC power input: 110-240V, (47-63Hz)
- Power consumption maximum: 29.5W
- Maximum thermal output: 100.7 BTU/hr.

### Dimensions

- Enclosure: Desktop
- Dimensions(W x D x H): 8.3x8.3x1.65 in. (210x210x41.9mm)
- Weight: 2.9 lbs. (1.3 kg)

### Environmental Conditions

- Operating: 0° to 40°C, humidity 5% to 95%
- Storage: -20° to 70°C, humidity 5% to 95% at 60°C

### Certifications

- Safety: UL, CB, CE, TUV GS
- Emissions: FCC, CE, VCCI, RCM/C-Tick
- Environmental: RoHS, WEEE, REACH<sup>1</sup>, ISO14001<sup>1</sup> factory certificate

## ORDERING INFORMATION

### BASE CONFIGURATION <sup>1</sup>

|  |                   |
|--|-------------------|
| 3100 Next Generation Security Gateway base configuration, includes 6x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC power unit, Next Generation Threat Prevention (NGTP) security subscription package for 1 year | CPAP-SG3100-NGTP  |
| 3100 SandBlast Next Generation Security Gateway base configuration, includes 6x1GbE copper ports, 8GB RAM, 1 HDD, 1 AC power unit, SandBlast (NGTX) security subscription package for 1 year               | CPAP-SG3100-NGTX  |
| <b>SPARES AND MISCELLANEOUS</b>  |                   |
| Replacement power supply for 3100 Security Gateways  | CPAC-PSU-3100     |
| Single/Dual chassis rack shelf for 3000 Security Gateways  | CPAC-RM-DUAL-3000 |

1. SKUs for 2 and 3 years, for High Availability and Appliances with an SSD option are also available, see the online Product Catalog