



# Check Point 2200 Appliance

Today the Internet gateway is more than a firewall. It is a security device presented with an ever-increasing number of sophisticated threats. As a security gateway it must use multiple technologies to control network access, detect sophisticated attacks and provide additional security capabilities like data loss prevention and protection from web-based threats. The proliferation of mobile devices like smartphones and Tablets and new streaming, social networking and P2P applications requires a higher connection capacity and new application control technologies. Finally, the shift towards enterprise private and public cloud services, in all its variations, changes the company borders and requires enhanced capacity and additional security solutions.

Check Point's new appliances combine fast networking technologies with high performance multi-core capabilities—providing the highest level of security without compromising on network speeds to keep your data, network and employees secure. Optimized for the Software Blades Architecture, each appliance is capable of running any combination of Software Blades—providing the flexibility and the precise level of security for any business at every network location by consolidating multiple security technologies into a single integrated solution.

Each Check Point Appliance supports the Check Point 3D security vision of combining policies, people and enforcement for unbeatable protection and is optimized for enabling any combination of the following Software Blades: (1) Firewall, (2) VPN, (3) IPS, (4) Application Control, (5) Mobile Access, (6) DLP, (7) URL Filtering, (8) Antivirus, (9) Anti-spam, (10) Identity Awareness and (11) Advanced Networking & Clustering.

## OVERVIEW

The Check Point 2200 Appliance is a compact desktop box using multi-core technology. The 2200 offers six onboard 1 Gigabit copper Ethernet ports for high network throughput. Despite its small form factor, this powerful appliance provides a respectable 114 SecurityPower Units, firewall throughput of 3 Gbps and IPS throughput of more than 2 Gbps, enabling security for small branch offices, providing an effective and affordable all-in-one security solution.

## KEY FEATURES

- 114 SecurityPower™
- 3 Gbps of firewall throughput
- 2 Gbps of IPS throughput
- 6 10/100/1000Base-T ports
- Desktop form factor

## KEY BENEFITS

- Trusted by 100% of the Fortune 100
- All-inclusive security appliance
- Unified management console
- Ensures data security with VPN
- Extensible Software Blade Architecture

## GATEWAY SOFTWARE BLADES

|                                  | FW | NGFW | NGDP | NGTP |
|----------------------------------|----|------|------|------|
| Firewall                         | ■  | ■    | ■    | ■    |
| IPsec VPN                        | ■  | ■    | ■    | ■    |
| Mobile Access (5 users)          | ■  | ■    | ■    | ■    |
| Advanced Networking & Clustering | ■  | ■    | ■    | ■    |
| Identity Awareness               | ■  | ■    | ■    | ■    |
| IPS                              | *  | ■    | ■    | ■    |
| Application Control              | *  | ■    | ■    | ■    |
| Data Loss Prevention             | *  | *    | ■    | *    |
| URL Filtering                    | *  | *    | *    | ■    |
| Antivirus                        | *  | *    | *    | ■    |
| Anti-spam                        | *  | *    | *    | ■    |
| Anti-Bot                         | *  | *    | *    | ■    |

\* Optional



## 2200

- ① Rack mount shelf (optional)
- ② 6 x 10/100/1000Base-T RJ45 ports
- ③ Two USB ports for ISO installation
- ④ Console port RJ45



## SECURITYPOWER™

Until today security appliance selection has been based upon selecting specific performance measurements for each security function, usually under optimal lab testing conditions and using a security policy that has one rule. Today customers can select security appliances by their SecurityPower™ ratings which are based on real-world customer traffic, multiple security functions and a typical security policy.

SecurityPower is a new benchmark that measures the capability and capacity of an appliance to perform multiple advanced security functions (Software Blades) such as IPS, DLP and Application Control in real world traffic conditions. This provides an effective metric to better predict the current and future behavior of appliances under security attacks and in day-to-day operations. Customer SecurityPower Unit (SPU) requirements, determined using the Check Point Appliance Selection Tool, can be matched to the SPU ratings of Check Point Appliances to select the right appliance for their specific requirements.

### SecurityPower Utilization



## ALL-INCLUSIVE SECURITY SOLUTIONS

The Check Point 2200 Appliance offers a complete and consolidated security solution in a desktop form factor. Based on the Check Point Software Blade architecture, this appliance is available in four Software Blade packages and extensible to include additional Software Blades for further security protection.

- **Firewall (FW):** create user-based access control and secure connections to corporate networks for remote and mobile users, branch offices and business partners with IPsec VPN.
- **Next Generation Firewall (NGFW):** identify and control applications by user and scan content to stop threats — with IPS and Application Control.

- **Next Generation Data Protection (NGDP):** preemptively protect sensitive information from unintentional loss, educate users on proper data handling policies and empower them to remediate incidents in real-time — with IPS, Application Control and DLP.
- **Next Generation Threat Prevention (NGTP):** apply multiple layers of protection to prevent sophisticated cyber-threats — with IPS, Application Control, Antivirus, Anti-Bot, URL Filtering and Email Security.

## INTEGRATED SECURITY MANAGEMENT

The 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 purposes.

## GAiA — THE UNIFIED SECURITY OS

Check Point GAiA™ is the next generation Secure Operating System for all Check Point appliances, open servers and virtualized gateways. GAiA combines the best features from IPSO and SecurePlatform into a single unified OS providing greater efficiency and robust performance. By upgrading to GAiA, customers will benefit from improved appliance connection capacity and reduced operating costs. With GAiA, customers will gain the ability to leverage the full breadth and power of all Check Point Software Blades. GAiA secures IPv4 and IPv6 networks utilizing the Check Point Acceleration & Clustering technology and it protects the most complex network environments by supporting dynamic routing protocols like RIP, OSPF, BGP, PIM (sparse and dense mode) and IGMP. As a 64-Bit OS, GAiA increases the connection capacity of select appliances.

GAiA simplifies management with segregation of duties by enabling role-based administrative access. Furthermore, GAiA greatly increases operation efficiency by offering Automatic Software Updates. The intuitive and feature-rich Web interface allows for instant search of any commands or properties. GAiA offers full compatibility with IPSO and SecurePlatform command line interfaces, making it an easy transition for existing Check Point customers.



## TECHNICAL SPECIFICATIONS

|   |  |
|---|--|
| <b>Base Configuration</b>   | <b>Virtual Systems</b>                                 |
| 6 x 10/100/1000Base-T RJ45 ports  | Max VSs: 3   |
| 250 GB hard disk drive  | <b>Dimensions</b>                                      |
| External AC to DC power adaptor   | Enclosure: Desktop                                     |
| <b>Production Performance<sup>1</sup></b>                               | Standard (W x D x H): 8.27 x 8.25 x 1.65 in.           |
| 114 SecurityPower   | Metric (W x D x H): 210 x 209.5 x 42 mm                |
| 1.4 Gbps firewall throughput  | Weight: 2.0 kg (4.4 lbs.)                              |
| 150 Mbps firewall and IPS throughput                                    | <b>Power Requirements</b>                              |
| <b>RFC 3511, 2544, 2647, 1242 Performance Tests (LAB)</b>               | AC Input Voltage: 100 - 240V                           |
| 3 Gbps of firewall throughput, 1518 byte UDP                            | Frequency: 50 - 60 Hz                                  |
| 400 Mbps of VPN throughput, AES-128                                     | Single Power Supply Rating: 40 W                       |
| 2 Gbps of IPS throughput, Default IPS profile, IMIX traffic blend       | Power Consumption Maximum: 35 W                        |
| 300 Mbps of IPS throughput, Recommended IPS profile, IMIX traffic blend | Maximum thermal output: 119.4 BTU                      |
| 1.2 million concurrent connections, 64 byte HTTP response               | <b>Operating Environmental Conditions</b>              |
| 25,000 connections per second, 64 byte HTTP response                    | Temperature: 32° to 104°F / 0° to 40°C                 |
| <b>Network Connectivity</b>   | Humidity: 20% - 90% (non-condensing)                   |
| IPv4 and IPv6   | <b>Storage Environmental Conditions</b>                |
| 1024 VLANs  | Temperature: -4° to 158°F / -20° to 70°C               |
| 256 VLANs per interface   | Humidity: 5% - 95% @ 60°C (non-condensing)             |
| 802.3ad passive and active link aggregation                             | <b>Certifications</b>                                  |
| Layer 2 (transparent) and Layer 3 (routing) mode                        | Safety: CB, UL/cUL, CSA, TUV, NOM, CCC, IRAM, PCT/GoST |
| <b>High Availability</b>  | Emissions: FCC, CE, VCCI, C-Tick, CCC, ANATEL, KCC     |
| Active/Active - L3 mode   | Environmental: RoHS                                    |
| Active/Passive - L3 mode  |  |
| Session synchronization for firewall and VPN                            |  |
| Session failover for routing change                                     |  |
| Device failure detection  |  |
| ClusterXL or VRRP   |  |
| Link failure detection  |  |

<sup>1</sup>Maximum production performance based upon the SecurityPower benchmark. Real-world traffic, Multiple Software Blades, Typical rule-base, NAT and Logging enabled. Check Point recommends 50% SPU utilization to provide room for additional Software Blades and future traffic growth. Find the right appliance for your performance and security requirements using the Appliance Selection Tool.



## Datasheet: Check Point 2200 Appliance

### SOFTWARE BLADE PACKAGES SPECIFICATIONS

| Base Systems <sup>1</sup>  | SKU               |
|--|-------------------|
| Check Point 2200 Appliance with FW, VPN, IA, ADNC, and MOB-5 Blades; bundled with local management for up to 2 gateways.   | CPAP-SG2205       |
| 2200 Next Generation Firewall Appliance (with FW, VPN, ADNC, IA, MOB-5, IPS and APCL Blades); bundled with local management for up to 2 gateways.                                | CPAP-SG2200-NGFW  |
| 2200 Next Generation Data Protection Appliance (with FW, VPN, ADNC, IA, MOB-5, IPS, APCL, and DLP Blades); bundled with local management for up to 2 gateways.                   | CPAP-SG2200-NGDP  |
| 2200 Next Generation Threat Prevention Appliance (with FW, VPN, ADNC, IA, MOB-5, IPS, APCL, URLF, AV, ABOT and ASPM Blades); bundled with local management for up to 2 gateways. | CPAP-SG2200-NGTP  |
| Software Blades Packages <sup>1</sup>  |                   |
| 2200 Next Generation Firewall Appliance Software Blade package for 1 year (IPS and APCL Blades).   | CPSB-NGFW-2200-1Y |
| 2200 Next Generation Data Protection Appliance Software Blade package for 1 year (IPS, APCL, and DLP Blades).  | CPSB-NGDP-2200-1Y |
| 2200 Next Generation Threat Prevention Appliance Software Blade package for 1 year (IPS, APCL, URLF, AV, ABOT and ASPM Blades).  | CPSB-NGTP-2200-1Y |
| Additional Software Blades <sup>1</sup>  |                   |
| Check Point Mobile Access Blade for up to 50 concurrent connections  | CPSB-MOB-50       |
| Data Loss Prevention Blade for 1 year (for up to 500 users, up to 15,000 mails per hour and max throughput of 700 Mbps)  | CPSB-DLP-500-1Y   |
| Check Point IPS blade for 1 year   | CPSB-IPS-S-1Y     |
| Check Point Application Control blade for 1 year   | CPSB-APCL-S-1Y    |
| Check Point URL Filtering blade for 1 year   | CPSB-URLF-S-1Y    |
| Check Point Antivirus Blade for 1 year   | CPSB-AV-S-1Y      |
| Check Point Anti-Spam & Email Security Blade for 1 year  | CPSB-ASPM-S-1Y    |
| Check Point Anti-Bot Blade for 1 year - for low-end appliances and pre-defined systems   | CPSB-ABOT-S-1Y    |

<sup>1</sup>High Availability (HA) and SKUs for 2 and 3 years are available, see the online Product Catalog.

### VIRTUAL SYSTEMS PACKAGES

| Description                           | SKU            |
|---------------------------------------|----------------|
| 3 Virtual Systems package             | CPSB-VS-3      |
| 3 Virtual Systems package for HA/VSLs | CPSB-VS-3-VSLs |

### ACCESSORIES

| Description                                    | SKU           |
|--|---------------|
| Replacement DC Power Supply for 2200 appliance | CPAC-PSU-2200 |
| 2200 accessory, Single Rack Mount Kit          | CPAC-RM-2200  |

### CONTACT CHECK POINT

#### 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