Check Point
5200 安全网关

Check Point 5200 安全网关

分支机构和小型办公室的安全性

产品优点

- 实现最高级威胁防御安全
- 针对 SSL 加密流量检测场景优化的最佳性能
- 面向未来的安全技术，防御未知的风险
- 集中管理和 LOM 远程带外管理提高运维体验
- 高性能套装优化设备性能
- 可扩展模块化机框带来灵活 I/O 选择

产品特点

- 易于部署和管理
- 从各种设备安全远程访问公司资源
- 网络扩展槽用来扩展端口数量、光纤端口以及 Bypass 端口
- 设备冗余集群技术彻底避免单点故障

概 述

Check Point 5200 安全网关综合了最全面的安全威胁防护，确保您的分支机构和小型办公室的安全部署。5200 安全网关是一种 1U 设备，具有一个 I/O 扩展槽，同时具备高端口密度、500GB 硬盘及可选的远程带外管理功能。这台强大的安全设备经过优化，向客户交付可满足真实场景需求的高级威胁防御能力，以保证关键资产和环境安全。

全面威胁防御

恶意软件的快速增长、越来越高的攻击技术及新型未知零日威胁的出现都要求采用一种不同的方法来保护企业网络和数据安全。Check Point 通过屡获殊荣的 SandBlast™ 威胁仿真和威胁净化技术，提供完全集成的全面威胁防御，可对最高级威胁和零日漏洞提供全面防护。

生产环境性能 [1]	
安全能力单元 (SPU – SecurityPower™ Units)	425 SPU
防火墙吞吐量	5.3 Gbps
IPS 吞吐量	810 Mbps
NGFW 吞吐量 (防火墙, 应用程序控制, IPS)	520 Mbps
威胁防御吞吐量 [2]	250 Mbps
实验室环境性能 (RFC 3511, 2544, 2647, 1242)	
防火墙吞吐量, 1518 字节 UDP	16 Gbps
每秒连接数	125,000
并发连接数	320 万至 640[3] 万
VPN 吞吐量, AES-128	1.88 Gbps
IPS 吞吐量	3 Gbps
NGFW 吞吐量(防火墙, 应用程序控制, IPS)	2.7 Gbps

[1] 性能数据基于真实混合流量和内容，典型安全策略，采用 IPS 推荐配置, 开启 NAT 和日志下测量得到, [2] FW, IPS, APPCTRL, AV, AB, URLF, [3] 基于最大内存配置

全面的安全解决方案

Check Point 5200 安全网关提供了全面的多层威胁防御解决方案，并提供给用户两种选择：

- **NGTP-下一代威胁防御**：通过 IPS, 应用程序控制, 反病毒, 反僵尸, URL 过滤和电子邮件安全来防御高级网络威胁.
- **NGTX-下一代威胁净化**：具有 SandBlast 零日威胁防护能力的 NGTP，增加了威胁仿真和威胁净化功能.

防御已知和零日威胁

5200 安全网关通过反病毒、反僵尸、SandBlast 威胁仿真（沙盒）和 SandBlast 威胁净化等安全技术保护企业免遭已知和未知威胁攻击.

作为 Check Point SandBlast 零日威胁防护解决方案的一部分，基于云的威胁仿真引擎可在漏洞利用阶段检测恶意软件，甚至在黑客应用规避技术尝试绕过沙盒之前完成检测。文件被快速隔离和检测，在虚拟沙盒中运行，以在其进入网络前发现恶意行为。这种创新解决方案将基于云的 CPU 级别检测与 OS 级别沙盒结合起来，防止最危险漏洞利用及零日和针对性攻击造成的感染.

此外，SandBlast 威胁净化可清除可能被漏洞利用的内容，包括活动内容和嵌入式对象，通过文件重构，以消除潜在威胁，并迅速向用户交付重构净化后的内容，保持业务处理不中断。

	NGTP	NGTX
	防御已知威胁	防御已知和零日攻击
防火墙	√	√
VPN (IPSec)	√	√
IPS	√	√
应用程序控制	√	√
反僵尸	√	√
反病毒	√	√
URL 过滤	√	√
SandBlast 威胁仿真	×	√
SandBlast 威胁净化	×	√

检测加密连接

如今为了增强网络的安全性，越来越多的站点开始使用 HTTPS, SSL 和 TLS 加密。与此同时，通过 SSL 和 TLS 加密流量交付的文件传递至企业时，就可能产生一个隐藏的威胁来源，这个威胁来源可能会绕过传统的安全实现方式。

Check Point 威胁防御通过查看内部加密的 SSL 和 TLS 隧道来检测威胁，确保用户在上网和使用公司数据时能遵从公司的安全合规性。

高性能套装

具有高连接并发需求的客户可购买高性价比的高性能套装(HPP)。包括 5200 安全网关及 1 块 4 端口 1Gb SFP 模块、收发器和远程带外管理模块。

	基本	HPP	最高
1 GbE 端口（铜	6	6	14
1 GbE 端口（光纤)	0	4	4
光收发器 (SR)	0	4	4
内存	8GB	8GB	16GB
电源	1	1	1
远端带外管理模块	可选	包括	包括

远程管理和监控

远端带外管理（LOM）卡提供远程带外管理，管理员可从远端位置远程诊断、启动、重启和管理设备。管理员还可利用 LOM 网络接口从一个 ISO 文件远程安装系统镜像。

远程安全访问

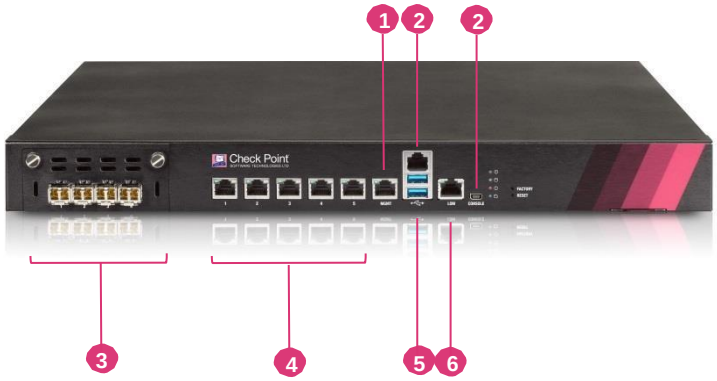
每台设备都通过移动接入刀片为 5 个用户提供远程访问连接。该许可证允许从各种设备安全地远程访问公司资源，包括智能手机、平板电脑、PCs、Mac 和 Linux.

集成安全管理

每一个 Check Point 设备，既可以利用其可用的集成安全管理进行本地管理，或者也可以通过中央统一管理。利用本地管理，设备可管理自身与另一台与其组成高可用部署的设备。

Check Point 5200 安全网关

1. 管理端口(10/100/1000Base-T RJ45)
2. Console 端口 (RJ45/Micro USB)
3. 一个网络模块扩展槽(右图为高性能套装)
4. 5 个板载端口(10/100/1000Base-T RJ45)
5. 2 个 USB 端口（用于系统镜像安装）
6. 远程带外管理端口



订购信息

基本配置 [1]	
5200 下一代威胁防御，捆绑多达 2 个网关的本地管理	CPAP-SG5200-NGTP
5200 下一代威胁净化，捆绑多达 2 个网关的本地管理	CPAP-SG5200-NGTX

高性能套装(HPP) [1]	
5200 下一代威胁防御高性能套装，包括 1 个 4 端口 1GbE SFP 模块,4 个 SR 收发器和远程带外管理模块	CPAP-SG5200-NGTP-HPP
5200 下一代威胁净化高性能套装，包括 1 个 4 端口 1GbE SFP 模块,4 个 SR 收发器和远程带外管理模块	CPAP-SG5200-NGTX-HPP

[1] 提供 2 年和 3 年高可用性 (HA) 和 SKUs 可用，见在线产品目录

附件

接口模块和收发器	
8 端口 10/100/1000 Base-T RJ45 模块	CPAC-8-1C-B
4 端口 1000Base-F SFP 模块；需要另外购买 1000Base SFP 收发器	CPAC-4-1F-B
1000Base-LX SFP 光纤收发器 - 长距	CPAC-TR-1LX-B
1000Base-SX SFP 光纤收发器 - 短距	CPAC-TR-1SX-B
1000 Base-T RJ45 SFP 收发器(铜缆)	CPAC-TR-1T-B
4 端口 10/100/1000 Base-T RJ45（Fail-open）Bypass 模块	CPAC-4-1C-BP-B

备件和其它	
5200 安全网关 8GB 内存升级套件	CPAC-RAM8GB-5000
远程带外管理模块	CPAC-LOM-B
5000 系列安装导轨(22” - 32”)	CPAC-RAIL-5000
5000 系列扩展导轨 (26” - 36”)	CPAC-RAIL-EXT-5000

Check Point 5200 安全网关

1 电源
2 风扇

扩展选项

基本配置
• 6 个板载端口(10/100/1000Base-T RJ-45)
• 8 GB 内存(16 GB 可选)
• 1 个电源
• 1 个 500 GB 硬盘驱动器
• 固轨 (滑轨可选)
• (远程带外管理 (LOM) 可选)

网络扩展槽选项 （1 个槽可用）
• 8 端口 10/100/1000Base-T RJ45 模块，最大网络端口可达 14 个
• 4 端口 1000Base-F SFP 模块，最大网络端口可达 4 个

Fail-open/Bypass 模块选项
• 4 端口 10/100/1000Base-T RJ45 Bypass 模块

虚拟系统 [1]
• 最大数量(基本配置/高性能套装): 10/20

[1] 基于基本配置和高性能套装中的可用内存

网络

网络连接
• 每个设备的所有物理和虚拟（VLAN）接口: 1024/4096 (单个网关/带有虚拟系统)
• 802.3ad 被动和主动链路聚合
• Layer 2 (透明) 和 Layer 3 (路由)模式

高可用性
• 主用/主用和主用/备用- L3 模式
• 防火墙和 VPN 会话同步
• 路由变化引起的会话故障切换
• 设备和链路故障检测
• ClusterXL 或 VRRP

IPv6
• 特点：防火墙、身份感知、移动接入、应用控制、URL 过滤、IPS、反僵尸、反病毒
• NAT66, NAT64
• CoreXL, SecureXL, HA 带有 VRRPv3

路由

单播和多播路由(参见 SK98226)
• OSPFv2 和 v3, BGP, RIP
• 静态路由，多播路由
• 基于策略的路由
• PIM-SM, PIM-SSM, PIM-DM, IGMP v2, 和 v3

物理

功率要求
• AC 输入电压: 90-264V
• 频率: 47-63Hz
• 单电源额定功率: 250W
• 最高功耗: 62.9W
• 最高热功率: 214.6 BTU/hr.

尺寸
• 机箱: 1RU
• 标准 (W x D x H): 17.24 x 16 x 1.73 in.
• 公制 (W x D x H): 438 x 406.5 x 44 mm
• 重量: 6.22 kg (13.7 lbs.)

工作环境条件
• 温度: 32° - 104°F / 0° - 40°C
• 湿度: 5% - 95% (无冷凝)

贮藏条件
• 温度: –4° - 158°F / –20° - 70°C
• 湿度: 5% - 95% （ 60°C） (无冷凝)

认证
• 安全: UL60950-1, CB IEC60950-1, CE LVD EN60950-1, TUV GS
• 辐射: FCC, CE, VCCI, RCM/C-Tick
• 环保: RoHS, REACH*, ISO14001*

*制造商认证

联系Check Point

北京代表处
地址：北京市朝阳区东三环中路5号 财富金融中心21层2102室
电话：(86) 10 6590 7630

上海代表处
地址：上海市徐汇区龙华中路596号 绿地中心A幢1808室
电话：（86） 21 5461 0322

广州代表处
地址：广州市天河区天河路385号 太古汇一座702-11
电话：（86） 20 2886 1546/47/48/49