山石网科 K 系列国产芯片防火墙

SG-6000-K9180

正面图

背面图

山石网科 K 系列是山石网科公司推出的国产芯片防火墙产品系列。K 系列首款产品 K9180 是高性能、高可靠、高扩展的国产芯片高性能安全平台，继承了 X 系列数据中心安全防护平台的硬件与软件自主设计优势，硬件设计、生产全流程国产化，成为业界首创采用国产关键元器件吞吐超百 G 的安全防护平台，填补了中国在国产化高端防火墙领域的空白。K9180 可广泛部署于高性能数据中心、大型互联网出口等大流量安全防护应用场景，并可广泛应用于政府、金融、电力、涉密等需要国产化产品的机构。

产品亮点

基于国产关键元器件的全分布式架构

爆炸式流量增长趋势，数据中心防火墙需要具备处理大流量、海量访问的强大能力，并可有效应对海量用户突发访问的情形，所以数据中心防火墙不仅要具有超高的吞吐量，而且要具备超高的并发连接和每秒新建连接处理能力。

山石网科国产芯片高性能安全平台 K9180 是业界首创采用国产关键元器件、自研操作系统，整机吞吐突破百 G 的安全防护平台，填补了中国在国产高端防火墙领域的空白。K9180 采用创新的全分布式架构，通过智能流量分配算法实现业务流量在业务模块（SSM）和接口模块（IOM）上的分布式高速处理；并通过资源管理算法专利技术充分发挥分布式多核处理器平台的潜力，进一步提升防火墙并发连接、每秒新建连接的性能，实现系统性能的全面线性扩展。K9180 处理能力最高可达 300Gbps，并发会话连接数最大可达 1 亿，设备可提供多达 10 个 100GE 和 80 个 10GE 接口的扩展能力。

电信级可靠性保障

K9180 的硬件和软件均采用高可靠设计，实现 99.999% 的电信级可靠性。可支持主 / 主或主 / 备模式的冗余部署方案，保证单台故障时业务不中断；整个系统采用模块化设计，支持主控模块、交换模块、业务模块、接口模块、电源模块、风扇模块等关键部件的冗余可靠性保证，同时所有模块均可实现热插拔。

领先的虚拟防火墙技术

虚拟化技术在数据中心被越来越广泛的应用，K9180 针对数据中心的虚拟化需求，可将一台物理防火墙在逻辑上划分成多达 1000 个虚拟防火墙，为数据中心提供大容量的虚拟防火墙支持能力。同时，用户可根据实际业务情况，动态设置每个虚拟防火墙的资源配额，例如 CPU、会话、策略数、端口等，保障了虚拟化环境中业务流量的弹性变化。K9180 的每个虚拟防火墙系统不但拥有独立的系统资源，还可独立精细化管理，为不同的业务或用户提供可视化的独立安全管理界面。

精细化应用管控与全面安全防护

K9180 采用先进的深度应用识别技术，可根据协议特征、行为特征及关联分析等，准确识别数千种网络应用，其中包括百余种移动应用以及加密的 P2P 应用，并可为用户提供精细而灵活的应用安全管控功能。

K9180 提供了基于深度应用、协议检测和攻击原理分析的入侵防御技术，可有效过滤木马、蠕虫、间谍软件、漏洞攻击、逃逸攻击等安全威胁，为用户提供 L2-L7 层网络安全防护。其中，专业的 Web 攻击防护功能，能够满足用户 Web 服务器深层次防御 Botnet 的需求，保障内网主机免受感染威胁。

K9180 的智能带宽管理基于深度应用识别和用户识别，结合业务应用优先级，可根据策略对流量进行两层八级的细粒度划分控制，并提供弹性 QoS 功能；与会话限制、策略路由、链路负载均衡、服务器负载均衡等功能配合使用，可以为用户提供更为灵活的流量管理解决方案。

K9180 支持千万级 URL 特征库的 URL 过滤功能。可帮助管理员轻松实现网页浏览访问控制，避免恶意 URL 带来的威胁渗入。

强大的网络适应性

K9180 完全支持下一代互联网部署技术（包括双栈、隧道、DNS64/NAT64 等多种过渡技术），同时具备成熟的 NAT444 功能支持固定端口外网地址向内网地址的静态映射，能够基于 Session 生成日志，并可基于用户生成日志，方便溯源。同时增强的 NAT 功能（Full-cone NAT 和端口复用等）能够充分适应目前运营商网络的特点，降低用户网络建设成本。

K9180 提供完全兼容标准的 IPSec VPN 功能，集成第三代 SSL VPN，为用户提供高性能、高容量的全面 VPN 解决方案。同时，其独特的即插即用 VPN，大大简化了配置和维护难度，为用户提供方便快捷的远程安全接入服务。

功能规格

应用识别
- 全新一代基于应用特征、行为和关联信息的应 用识别
- 支持Windows、Android、IOS平台多达几千种的应用识别及控制
- 支持应用类别、风险等级、应用技术等多维度的应用定义
- 支持自定义应用及应用组
- 应用特征库支持网络实时更新

用户认证
- 支持本地用户的Web认证和短信认证
- 支持外部服务器认证（Raidus\Active Directory\LDAP\TACACS+）
- 支持AD和LDAP的用户组及OU同步
- 支持802.1X、SSO代理
- 支持WebAuth认证页面定制
- 支持基于接口的主动认证
- 支持基于MAC的用户认证
- 支持微信连WiFi功能
- 支持无Agent方式的AD SSO功能（AD Polling）
- 支持通过SSO-monitor协议标准进行认证用户同步

防火墙
- 基于深度应用识别的访问控制
- 基于应用/角色/国家地理IP的安全策略
- 丰富的路由特性
- 全面的DNS策略
- 强大的 NAT 及 ALG
- 策略自学习
- 垃圾策略检测与清理
- 防火墙策略重复与冗余规则检测

攻击防护
- 多种畸形报文攻击防护
- SYN Flood、DNS Query Flood 等多种 DoS/DDoS 攻击防护
- 支持 ARP 攻击防护

入侵防御
- 基于状态、精准的高性能攻击检测和防御
- 实时攻击源阻断、IP 屏蔽、攻击事件记录
- 支持针对 HTTP、SMTP、IMAP、POP3、VOIP、NETBIOS 等 20 余种协议和应用的攻击检测和防御
- 支持缓冲区溢出、SQL 注入和跨站脚本攻击的检测和防护
- 支持自定义入侵防御特征
- 提供预定义防御配置模板
- 提供 7000 多种特征的攻击检测和防御，特征库支持网络实时更新
- 支持专业的 Web Server 防护功能，含 CC 攻击防护和外链防护等

网页访问控制
- 基于角色、时间、优先级、网页类别等条件的 Web 网页访问控制
- 支持自定义 URL 类别
- 支持千万级 URL 特征库，URL 库支持网络实时更新

带宽管理
- 根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、VLAN 等信息划分管道
- 支持两层八级管道嵌套
- 对多层级管道进行最大带宽限制、最小带宽保证、每 IP 或每用户的最大带宽限制和最小带宽保证
- 基于时间和优先级的差分服务，支持带宽均分策略
- 支持针对每 IP 或每用户进行延迟限速
- 分布式 QoS 支持子管道策略
- 对剩余带宽根据优先级进行弹性分配
- 主动抑制服务器端传送流量
- 支持URL分类的流控控制策略

链路负载均衡
- Outbound 相关功能：PBR 支持 ECMP、时间以及权重、支持内置 ISP 路由和动态探测
- Inbound 相关功能：支持 SmartDNS（支持 DNS A 记录解析）、支持动态探测
- 可根据带宽占用及时延情况自动进行链路切换
- 支持通过 ARP、Ping、DNS 等方法来检测链路状态

服务器负载均衡
- 支持服务器健康检查和服务器会话保护、支持会话保持
- 支持加权哈希、加权轮询、加权最小会话数等算法
- 支持服务器会话状态的监控

VPN
- 支持 IPSec VPN 及创新的 PnPVPN
- 支持 SSL VPN(可选 USB-key)
- 支持 L2TP、GRE协议
- 支持 IKEv2 协议
- 支持 Xauth 协议
- 支持 OCSP 和 SCEP 协议
- VPN支持国密算法 SM2/3/4
- 支持 Android、IOS 等移动设备的安全接入

IPv6
- 访问控制
- ND 攻击防护

- 隧道、DNS64/NAT64 等多种过渡技术
- 应用识别
- URL过滤
- IPS攻击防护
- iQoS
- 支持DNS
- Track地址探测
- IPv6 路由（静态路由、策略路由、ISIS、RIPng、OSPFv3、BGP4+）

高可用性 (HA)

- 主 / 主模式（A/A）和主 / 备模式（A/P）
- 支持双主控
- 支持配置、会话同步

虚拟系统(Vsys)

- 支持对每个 Vsys 分配系统资源
- 支持 CPU 虚拟化
- 支持防火墙、IPSec VPN、SSL VPN、IPS、URL过滤等功能
- 支持监控统计
- vsys支持描述文件

监控统计

- 支持设备状态、网络连通性及可用性的主动检测和历 史信息统计查看
- 支持对Web、Mail、FTP、DNS等多种关键业务的可用 性主动检测和历史信息统计查看
- 支持应用的多维度统计监控，包括应用风险、类别、 特征、所用技术等
- 支持云应用（如云盘等）的多维统计监控
- 支持实时展现管道、用户及应用的流量、并发连接数 和新建连接数
- 支持iQoS管道策略实际流量情况监控，支持子管道叠加情况监控
- 支持链路状态监控，可查看指定应用/应用组详 情，支持选择多条链路进行对比分析
- 支持自定义监控
- 支持通过netflow v9 进行流量信息采集和外发
- 支持QoS两层策略管道实际流量处理情况监控，支持多个时间粒度，Top50~Top300的不同方向、不同策略的管道流量查看

日志

- 支持NAT日志、会话日志、策略路由日志、威胁日志、URL日志、IM上线日志等
- 支持通过二进制、文本格式外发日志
- 支持通过UDP、TCP、Secure-TCP协议进行日志传输

SDN

- 支持Fwaas解决方案

终端接入管控

- 支持跨三层识别接入网络终端数
- 支持识别 Windows、iOS、Android 等主流操作系统和终端类型
- 支持IP及终端接入数的条件过滤查询
- 支持 IP、管控规则、接入终端数、状态等条件过滤查询监控结果
- 支持对超限 IP 进行日志记录、干扰操作
- 支持自定义干扰操作后重定向页面显示内容
- 支持对超限IP进行阻断操作

IP 信誉库

- 对僵尸肉鸡、垃圾邮件发送者、Tor 节点、失陷主机、暴力破解等风险 IP 的流量进行识别和过滤
- 可对不同类别风险 IP 流量进行记录日志、丢弃数据包或阻断一定时间
- 定期 IP 信誉特征库升级更新

报表

- 报表内容包含网络及安全风险概况、网络流量详情、应用统计及风险详情、URL活动及风险详情、网络风险威胁详情和威胁说明等
- 支持预定义和自定义报表模板，可自定义报表内容
- 报表格式支持PDF、HTML、WORD
- 支持通过邮件或者FTP方式外发报表

关键指标

指 标	SG-6000-K9180
	
防火墙吞吐量	300Gbps
最大并发连接数	1 亿
管理接口	1 个 Console 口、1 个 AUX 口、1 个 MGT 管理、1 个 USB2.0 口（单 SCM-280ZKA 模块）
网络接口	1 个 1GE 电接口（MGT 接口，单 SCM-280ZKA 模块）
扩展模块槽	6 个 通用扩展槽，2 个系统控制模块扩展槽， 2 个交换模块扩展槽
扩展模块选项	SCM-280ZKA，SSM-300ZKA，SWM-280ZKA，IOM-P100-300ZKA
电源规格	N+M(1) 冗余热插拔电源，最大功率 3200W
外形尺寸(W×D×H，mm)	7U (440 x 735 x 308)

注：(1) 设备正常运行时，至少需要 2 个 220V 交流（在标准电压是 110V 的国家或地区，至少需要 3 个）或 2 个-48V 直流电源模块供电。

文档编号：DCFW-K-SG-6000-K9180-5.5R6-Y19M11-CH-V1

官方微信　　官方微博

中国 · 销售与服务热线：400-828-6655