Hillstone
山 石 网 科

山石网科智能下一代防火墙

SG-6000-A3600/A3700/A3800

随着 IT 技术的不断发展，新兴技术的不断涌现，攻击类型逐年增加，高级威胁攻击的攻击手段更加多样复杂，通常具有隐蔽性、目的性、持续性、多变性等特点，无法被基于签名技术检测方式的传统防火墙或者下一代防火墙有效检测。这也是目前 APT 等网络攻击屡屡得逞的重要原因。高级威胁攻击在我国不断威胁着政府、金融、军工、科研和教育等企事业单位。山石网科 A 系列智能下一代防火墙采用了全新的威胁检测技术，基于机器学习技术进行行为分析，准确发现变种恶意软件等未知威胁，从而弥补了传统检测技术的弊端。

安全防护正在从“个体或单个组织”的防护，转变为“安全情报驱动”的信息共享、集体协作的方式，山石智能下一代防火墙通过和山石云瞻威胁情报中心联动，掌握业界高危热点威胁事件及防护建议，以防御最新威胁；获取全面实时的攻击 IOC 特征，以提升威胁检测的有效性；对设备已发生的威胁事件，提供关联的攻击者的位置、攻击方式、技术手段以及攻击目标等情报信息，为客户进一步威胁处置决策提供有效建议。

随着万物互联时代的到来，网络不在由主机、服务器、移动终端等设备构成，还存在大量的物联网设备，网络安全防护能力需要关注物联网网络安全，识别物联网设备因失陷而产生的安全风险，以及增强对物联网设备的管控。而传统防火墙或者下一代防火墙仅能对主机、服务器、移动终端等设备进行防护和监管，无法对物联网设备提供有效的防护。山石网科 A 系列智能下一代防火墙可以识别网络摄像头等物联网设备，同时具备对物联网设备的安全防护与合规管控能力，可为客户打造融合网络的防护体验。

山石网科 A 系列智能下一代防火墙采用全新硬件架构，具备硬件解密引擎、高密接口、可扩展存储，提供业界领先的安全防护性能，可灵活部署于互联网出口、内网安全隔离、数据中心、分支机构安全互联等场景，致力为政府、金融、企业、教育、能源、运营商等客户提供专业的网络安全解决方案以及全面的安全防护能力。

产品亮点

全新硬件构架，性能超乎想象

随着信息化的进一步发展，网络流量日益激增，防火墙作为边界网络面向外部网络的桥梁，不但要提供可靠的安全防护能力，还需要具备强大的网络数据吞吐能力。时至今日，传输层中定义的网络端口号，已经不能满足精细化标记流量的诉求，只有深入解析应用所承载的内容，才可以深度感知网络行为。山石网科智能下一代防火墙，采用高性能通用架构处理器，提供极致的网络吞吐能力，特别是诸如IPS、AV等应用安全的处理能力，夯实了网络防护的基础。

随着信息安全技术的进一步发展，加密流量在整体网络流量中的占比也逐年提升，现阶段，约80%的网络流量都属于加密流量，不少安全威胁也混杂在加密流量之中。如何对加密流量进行高效解密，并感知其中的安全威胁，是下一代防火墙面临的挑战。山石网科智能下一代防火墙，采用SSL硬件解密引擎，相比于纯软件解密，SSL解密效率有着极大提升，有力的捍卫了客户的网络安全。

在操作系统层面，山石网科智能下一代防火墙采用自主研发的全并行安全

操作系统StoneOS，采用“一次解包，并行处理”的数据报文解析技术，即数据报文经一次解包后，由各个安全模块并行检测。同时，该技术向下延伸至硬件构架，即在多核CPU的每个核心上运行安全业务，最大化的利用了多核CPU运算处理能力，确保山石网科智能下一代防火墙在处理复杂网络流量和安全威胁的同时能够保持快速高效的处理效果。

传统网络防火墙设备，主机固化的接口数量较少，在客户实际使用过程中，经常需要购买接口扩展卡来满足日渐复杂的接口适配需求，这使得客户的建设成本以及维护成本直线提升。山石智能下一代防火墙，在硬件设计上，采用高密接口的设计理念，主机固化类型丰富的高密接口，完全满足典型客户接口适配需求，助力用户降低硬件投入成本以及后续维护成本。

智能协同，未知威胁检测和防御

山石网科智能下一代防火墙具备本地智能、沙箱联动智能以及云端智能等三种智能能力，利用机器学习以及行为分析，帮助客户发现未知网络威胁，定位风险主机，保护业务与数据安全。

- 本地智能未知威胁检测和防御能力。山石网科智能下一代防火墙内置高级威胁检测引擎，通过感知恶意软件的行为，来进行未知威胁检测。此外，山石网科智能下一代防火墙还具备DGA动态域名检测、DNS隧道检测等检测能力，可有效识别僵尸网络和失陷主机。
- 沙箱联动智能未知威胁检测和防御能力。山石网科智能下一代防火墙能够将本地未识别的文件进行沙箱联动，可以精准检测试图利用网页、电邮等方式入侵内网的变种恶意软件，进而实现对未知威胁的防护。山石智影（本地沙箱）或山石云影（云沙箱）基于静态分析和动态行为捕获，全面检测未知威胁，帮助客户遏制由此带来的风险，如敏感信息泄露、业务中断等。并可提供恶意文件的详细行为报告，包括网络行为、进程行为、文件行为等，为客户提供威胁处理建议。
- 云端智能协同未知威胁检测和防御能力。当山石网科智能下一代防火墙检测到未识别的数据之后，会将该数据上送云端，云端结合第三方情报以及专家知识库进行大数据分析，生成单点安全信息，并同步至本地智能下一代防火墙，以抵御威胁事件。同时，云端会在全局的维度，将单点安全信息共享给其他智能下一代防火墙，实现从“单点未知威胁检测”到“全局已知威胁防御”的转变，进一步提升全局智能下一代防火墙的未知威胁检测和防御能力。

情报集成，提前一步发现威胁

山石云瞻威胁情报中心具备获取国内外知名安全情报供应商所提供的威胁情报的能力。山石智能下一代防火墙和山石云瞻威胁情报中心联动，提供贯穿“攻击前、攻击中、攻击后”等三个关键节点的全生命周期安全防护解决方案。

- 攻击前，热点威胁防御。山石网科智能下一代防火墙通过联动山石云瞻威胁情报中心，可第一时间获取热点威胁事件，同时根据设备现有策略，明确针对热点威胁事件的防御状态和防范措施。一方面，客户可根据防范措施进行主动防御。另一方面，设备可自动将热点情报和设备威胁检测结果进行关联，以方便客户能更进一步了解客户相关资产是否已存在热点高危漏洞或者已失陷主机。
- 攻击中，威胁特征实时赋能。山石网科智能下一代防火墙将山石云瞻威胁情报中心所提供的威胁情报自动化集成到本地，通过云端与本地的智能协同，提升客户威胁检测能力。
- 攻击后，威胁日志自动聚焦及关联分析。结合山石云瞻威胁情报中心，山石网科智能下一代防火墙可帮助客户从海量告警信息中自动聚焦重点威胁，提升运维效率；通过云端联动，获取攻击者和威胁事件更全面的上下文信息。

物联管控，构建融合安全

万物互联的时代已经到来，企业级客户的网络中，不单充斥着主机、服务器、移动终端等设备，也会根据客户实际的业务需求，部署大量如网络摄像头等物联网设备。物联网设备的安全防护以及合规管控，成为了山石网科智能下一代防火墙的发展方向。

- 物联网设备准入功能。支持通过IP、MAC以及IP和MAC的绑定关系实现物联网设备的准入，同时可以杜绝物联网设备私自接入的行为。
- 物联网设备信息辨识。通过物联网设备的指纹信息，可以辨识物联网设备的类型、制造商、型号等相关信息，进而实现精确分类统计。
- 物联网设备安全防护。支持对物联网设备的行为进行监控，可以对异常行为进行检测与隔离，当物联网设备被攻陷后，山石网科智能下一代防火墙可对其采取隔离措施，确保用户网络安全。

硬件加速，带来极致安全体验①

随着全行业数字化转型加速，越来越多的场景面临着流量的激增，如何在较高流量场景下确保客户网络安全，成为山石网科智能下一代防火墙的探索方向。山石网科智能下一代防火墙搭载Hillstone Mars硬件加速引擎，专注较高流量场景下卸载CPU的压力，提供超高的网络防护性能，向客户带来极致的安全防护体验。

- 流量卸载。Hillstone Mars硬件加速引擎专注于流量卸载，在较高流量场景下，也可轻松卸载CPU的压力，使得CPU更加聚焦综合安全业务处理能力，向客户带来更极致的安全防护体验。
- 极致性能。在Hillstone Mars硬件加速引擎的加持下，山石网科全新智能下一代防火墙整机最大性能可达320Gbps，小包性能可达140Gbps，可满足数据中心等对流量要求较高的场景。
- 超低时延。采用Hillstone Mars硬件加速引擎的山石网科全新智能下一代防火墙，报文转发延时可低至几微秒，完全胜任对时延敏感的应用场景。

精细化多维管控

安全防护的基础是对用户网络业务环境的全面感知，山石网科智能下一代防火墙通过网络流量深度检测和解析技术，能够对应用、用户、内容、国家地理等进行多维度精准识别，为用户提供了丰富而灵活的安全管控功能。

- 应用精准识别及灵活控制。山石网科智能下一代防火墙采用深度应用识别技术，能够准确识别数千种网络应用，其中包括600余种移动应用、300余种云应用。并为用户提供包括应用类别、应用风险等级、所用技术、应用特征分布等多维可视化信息，从而帮助用户及时发现应用安全隐患。同时，山石网科智能下一代防火墙支持灵活的应用安全控制功能，包括策略阻止、会话限制、流量管控、应用引流或时间限制等，使得应用管控十分得心应手。
- 用户认证及管控。山石网科智能下一代防火墙支持一套丰富的用户认证系统，支持本地认证以及 TACACS+、RADIUS、LDAP 等多种外部认证协议，支持口令认证、短信认证、证书认证、令牌认证、邮件认证等多种认证方式。并可针对用户实施精细化的访问控制、应用限制、带宽保证等管控手段。
- 基于国家地理位置的访问控制。能够精确识别攻击源/目的IP所处的国家地理位置，从而可以根据业务通信要求实施基于国家地理位置的访问控制， 快速阻断攻击流量。
- 数据传输安全：基于数据深度检测技术，实现数据类型、大小、名称的文件传输控制，阻止关键性、敏感性、机密性数据及文件通过网络途径外发泄漏，满足企业数据传输行为的合规性管理要求。

全面威胁检测与防护

山石网科智能下一代防火墙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，可有效过滤病毒、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。

- 优化的攻击识别算法。能够有效抵御如SYN Flood、UDP Flood、HTTP Flood 等 DoS/DDoS 攻击，保障网络与应用系统的安全可用性。
- 专业Web攻击防护功能。支持SQL 注入、跨站脚本、CC 攻击等检测与过滤，避免Web 服务器遭受攻击破坏；支持外链检查和目录访问控制，防止Web Shell 和敏感信息泄露，避免网页篡改与挂马，满足用户Web 服务器深层次安全防护需求。
- 高性能的病毒过滤。领先的基于流扫描技术的检测引擎可实现低延时的高性能过滤。支持对 HTTP/HTTPS、FTP、SMB及各种邮件传输协议流量和压缩文件（zip，gzip，rar等）中病毒的查杀。
- 支持千万级URL。特征库的URL过滤功能可帮助网络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。
- SSL 加密流量全面的威胁防护。可针对SSL加密流量和加密邮件综合运用包括入侵防御、病毒防护、URL过滤在内的多种管控手段，实现加密流量应用层威胁的全面防护。

强大的网络适应性

山石网科智能下一代防火墙具备强大的网络适应能力，具备复杂环境下的安全部署能力，满足用户多样化的网络功能需求。

- 智能链路负载均衡功能。其出站动态探测和入站SmartDNS等功能允许网络访问流量在多条链路上实现智能分担，极大提升链路利用效率和用户网络访问体验。
- 支持RIP、OSPF和BGP等动态路由协议。可根据网络系统的运行情况自动调整动态路由表，满足运营商、高校等复杂网络环境部署。

统一集中管理

山石网科智能下一代防火墙支持集中管理，借助HSM安全管理平台，可对多设备进行统一策略管理、设备配置管理及实时安全监控，从而实现网络的快速部署以及发生安全事件的及时响应，提高管理效率，降低运维成本。

山石网科智能下一代防火墙支持山石“云•景”云运维功能，支持通过web和手机APP实时监控多设备的CPU、内存、流量趋势，以及应用、用户排名、威胁信息，云景还为用户提供7×24 小时告警监控，便于用户能够及时获知网络中的动态变化及安全风险。

注：①此处所提及的特性，不同产品型号支持有差异。

功能规格

应用识别

- 支持基于应用特征、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
- 基于深度应用识别的访问控制全新一代基于应用特征、行为和关联信息的应用识别

用户认证

- 支持外部服务器认证，包括 RADIUS\Active Directory\LDAP\TACACS+
- 支持对接 AD/LDAP 服务器，基于安全组或 OU 进行用户账号同步
- 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
- 支持基于 MAC 的用户认证
- WebUI 支持导入本地用户
- WebAuth 和 AAA Framework 支持 IPv6 协议栈
- 支持阿里云短信服务网关
- 支持 ACC CEP2.0 协议的电信短信网关
- 支持设置本地用户的密码复杂度要求及首次登录强制修改密码
- 支持 Windows 环境下的 Terminal Server 客户端本地用户支持 Web 认证和短信认证

安全策略

- 基于应用 / 角色/国家地理 IP 的安全策略
- 支持自学习生成策略
- 支持垃圾策略清理
- 支持聚合策略
- 策略助手支持生成基于服务的安全策略
- 安全策略支持导出
- 支持安全策略重复与冗余规则检测
- 策略的服务元素支持直接配置端口和协议
- 支持秒级颗粒度的时间表
- 支持策略配置审计
- 支持 Mini-policy

路由

- 支持 IPv6 静态路由
- 支持静态路由、ISP 路由，OSPF、BGP、RIP、ISIS、策略路由。
- 支持 EBGP 的 multipath-relax 功能
- 支持组播 PIM-SSM

NAT

- SNAT/DNAT 支持命中分析
- NATv6 支持 WebUI 的配置
- 支持 NAT，包含 NAT444，NAT64，DS-Lite，Full-Cone-NAT 等地址转换技术
- 支持 NAT 规则冗余检测功能

攻击防护

- 支持多种畸形报文的攻击防护
- 支持 SYN Flood、DNS Query Flood 等多种 DoS/DDoS 攻击防护
- 支持 ARP 攻击防护
- 支持 IPv6 的 DNS query flood，支持 IPv4 和 IPv6 的 DNS reply flood
- AD 功能支持目的 IP 地址白名单
- 应用层安全功能支持一键 Bypass 功能

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 12000 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
- IPS 威胁抓包（需配置 SSD）
- IPS 日志记录完整 URL 和还原 SQL 注入语句
- IPS 模板支持描述
- IPS 模板支持规则可信度

病毒过滤

- 支持基于流模式的病毒过滤
- 支持压缩病毒文件的扫描
- 病毒库支持网络定时更新
- 支持用户手动添加MD5特征码到AV病毒库中，也可以手动清除该特征码
- 支持针对 SMB 协议传输的文件进行病毒扫描

僵尸网络 C&C 防御

- 通过监控 C&C 连接发现内网肉鸡，阻断僵尸网络/勒索软件等高级威胁进一步破坏
- 支持定期更新僵尸网络库
- 支持 IP 和域名两种检测维度
- 支持 TCP 和 HTTP、DNS 协议检测
- C&C 地址库支持自定义 IP 和域名
- 支持 DNS sinkhole 检查
- C&Cprofile 支持 DGA 功能
- 支持 DNS Tunneling 检测
- 支持 DGA 域名检测
- 支持批量导入自定义域名

IP 信誉库/IP Reputation

- 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。
- 定期升级更新 IP 信誉特征库
- 支持通过 FTP/TFTP 方式获取 IP 外部动态列表

反垃圾邮件①

- 实时的垃圾邮件防御
- 支持明确的垃圾邮件、怀疑的垃圾邮件、群发垃圾邮件、正常群发
- 和语言、格式、内容无关的垃圾邮件检测能力
- 支持 SMTP、SMTPS、POP3、POP3S 邮件协议
- 支持 Inbound and outbound 检测
- 支持配置免监控域白名单

数据安全

- 支持基于文件类型、文件大小、文件名称进行数据传输安全控制
- 支持 HTTP、FTP、SMTP、POP3、IMAP 协议文件传输的识别
- 支持配合 SSL Proxy，对 HTTPS、SMTPS、POP3S、IMAPS 传输的文件进行过滤
- 支持近百种主流文件类型的特征码及后缀名双重识别
- 支持对网页关键字、Web 外发信息、邮件等内容进行过滤
- 支持新浪微博、微信 UID 和 QQ 虚拟身份的识别及相关上网行为的审计记录
- 文件过滤支持 SMB 协议

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
- 支持 url 黑白名单
- 支持自定义告警页面

带宽管理

- 支持根据安全域、接口、地址、用户/用户组、服务/服务组、应用/应用组、TOS、VLAN、TrafficClass 等信息设置管道匹配条件
- 支持两层八级管道嵌套功能
- 支持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
- 支持针对每 IP 或每用户进行延迟限速
- 支持基于时间和优先级的差分服务以及带宽均分
- 支持对剩余带宽根据优先级进行弹性分配
- 支持主动抑制服务器端传送流量
- 支持 URL 分类的流控控制策略
- VSYS 支持 iQoS 功能

流量配额

- 支持对用户/用户组限制指定时间段内的流量总额
- 支持限制每日总流量和每月总流量
- 支持手动清理和到期自动清理用户已使用流量

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
- 域名簿支持批量导入域名
- 针对特定域名进行链路质量探测并选择最优线路
- 链路状态监控增加主动探测方法
- 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
- IPSEC VPN 配置多条感兴趣流支持 DNAT 场景
- IPSEC VPN 支持 IKEV2 模式下的多条感兴趣流
- IKEv1 支持 DH group 19,20,21,24
- 支持 SSL VPN（可选 USB-key）
- 支持隐藏 SSL_VPN 认证登录 web 页面
- SSLVPN 客户端接入认证支持双因子认证，支持短信口令认证、令牌口令认证、邮件口令认证、证书口令认证等方式
- SSLVPN 支持从 RADIUS 服务器通过 CoA 消息获取用户安全策略
- 支持 IKEv2、L2TP、GRE 协议
- L2TPv3 支持 IPV6
- IKEV2 支持 DH14/15/16/19/20/21/24
- 支持 Xauth 协议
- 支持 OCSP 和 SCEP 协议
- 支持 Android、iOS 等移动设备的安全接入
- 支持国密算法 2/3/4
- 支持静态单播隧道类型的 VTEP
- 支持 VPN 配置向导

IPv6

- 访问控制功能支持 IPv6
- ND 攻击防护功能支持 IPv6
- 隧道、DNS64/NAT64 等多种过渡技术
- 支持 IPv6 的 ISATAP
- 支持 IPv6 OVER IPv4 GRE 隧道
- IPv6 路由（静态路由、策略路由、ISIS、RIPng、OSPFv3、BGP4+）
- 应用识别支持 IPv6
- URL 过滤支持 IPv6
- 防病毒支持 IPv6
- iQoS 支持 IPv6
- 支持 DNS、DNS64
- Track 地址探测支持 IPv6
- IPS 攻击防护支持 IPv6
- TFTP、FTP、RSH、HTTP、SIP ALG 支持 IPv6
- 旁路模式支持 IPv6
- NTP 支持 IPv6
- ADMIN HOST 支持 IPv6
- Traceroute 支持 IPv6
- 支持 IPv6 RADIUS 认证功能

SSL 解密

- 支持基于 https 加密流量的应用识别
- 支持 SSL 加密流量开启入侵防御功能
- 支持 SSL 加密流量开启病毒过滤功能
- 支持对 https 加密流量进行 URL 过滤
- 支持加密流量白名单设置
- 支持 SSL 代理 offload 模式
- 支持资源列表
- 支持基于 URL 分类设置白名单
- SMTPS/POP3S/IMAPS 经过 SSL-PROXY 解密后的明文流量支持应用识别、DLP、IPS、sandbox、AV
- 提供 SSL 代理根证书供 PC 端使用，以消除浏览器告警提示，并能在浏览器上弹出下载提示

高可用性（HA)②

- 支持主备模式（A/P）
- 支持 peer mode 模式
- 支持同步配置、会话
- 心跳接口支持 IPv6
- Data link 接口支持配置 2 个物理接口
- 支持两组 HA 设备组成 Twin-mode HA
- 支持两组 HA 设备间配置和会话同步
- Twin-mode HA 支持 AA 和 AP 模式
- Twin-mode AP 模式支持 IPv6

虚拟系统(VSYS)③

- 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
- VSYS 配额支持 SSL VPN 用户数的预留及限制
- 支持统一备份所有 VSYS 的配置
- Simple-switch 支持 ipv6

云沙箱

- 基于云端架构的恶意软件虚拟运行环境，发现未知威胁
- 多重静态检测引擎快速过滤正常文件及已知威胁，提升沙箱检测效率
- 基于日志、报表、监控信息、文件行为报告等，提供未知威胁可视化能力
- 对于判断为恶意的文件，提供完整的文件行为分析报告
- 支持 HTTP、HTTPS、SMTP、POP3、IMAP4、FTP、SMB 协议
- 支持 PE、APK、JAR、MS-OFFICE、PDF、SWF、RAR、 ZIP、Script 文件类型的检测
- 云沙箱检测结果阻断能力，快速阻断未知威胁
- 全局威胁情报共享，全局阻断未知威胁
- 支持自研云沙箱-免费沙箱支持、一键开启沙箱及报告呈现改进
- **支持基于不同文件类型，配置云沙箱或本地沙箱，进行检测**

云景

- SaaS 公有云服务方式，按需使用
- 对多设备的 CPU、内存、流量趋势、应用、威胁等进行集中监控、可视化展现和告警
- 支持报表功能和云端存储，可自定义报表模板及生成计划
- 支持将设备日志上传云端进行存储，可按条件查询
- 支持手机 APP、WEB 访问方式

威胁情报

- 支持与云端威胁情报中心联动
- 支持威胁情报与防火墙威胁事件、威胁日志检测结果加强与取证，用户可通过手动触发与自动触发将日志元素上送威胁情报中心进行上下文查询
- 支持自动聚焦重点威胁
- 支持热点情报推送到设备，并提供配置向导协助用户生成安全防护策略

监控统计

- 支持用户应用流量、URL 访问等统计分析
- 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 URL 访问和 URL 类别统计分析
- 支持实时流量统计和分析功能
- 支持安全事件统计功能
- 支持自定义监控
- 支持设备并发连接
- 支持设备 CPU、内存、温度等状态监控
- 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

终端接入监控

- 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

视频管控

支持识别 IP 摄像头、网络视频录像机等各类网络终端

支持终端类型、IP、终端状态等条件过滤查询终端监控结果

支持自定义准入名单，对接入的终端进行管理

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
- Syslog 支持 IPv6 传输

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

日志存储④

- 支持事件日志、网络日志、配置日志存储到本地存储（emmc）
- 支持事件日志、网络日志、配置日志、威胁日志存储到硬盘（需配置 SSD）
- 支持存储寿命的阈值配置以及告警（需配置 SSD）
- 支持各日志配置单独的存储空间
- 支持至少存储 6 个月日志（需配置 SSD）

北向开放

- 支持 Fwaas 解决方案
- 支持 Netconf
- 支持 RestfulAPI

系统管理

- 支持提示系统默认账户名的修改
- 支持管理员登录失败指定次数后锁定账户
- 支持开机自动加载 USB 设备中的配置文件
- 优化 U 盘加载配置功能，支持出厂配置启动时增量注入 HSM 导出的配置
- WebUI 支持查看系统关键进程
- 支持 LLDP 协议

无线控制⑤

- 支持双 SSID
- 支持无线流量控制

支持 4G 接入⑥

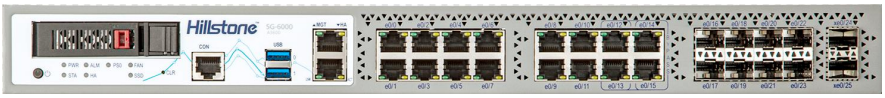
- 支持有线链路与 4G 链路备份
- 支持基于 4G 的 IPSec VPN

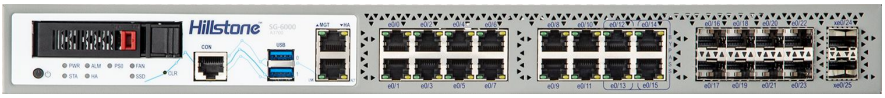
零信任访问⑦

- 支持以零信任理念实现终端用户接入
- 支持独立的零信任策略
- 支持基于账号密码和终端状态的终端标签
- 支持基于终端标签和应用资源配置零信任策略
- 支持应用资源管理
- 支持当用户终端状态变化时，动态调整其策略授权
- 支持应用发布，推送授权应用给终端用户

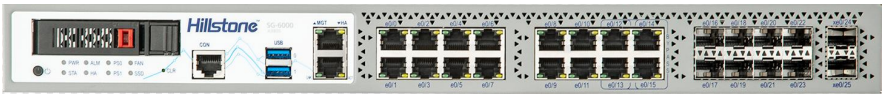
注：①、②、③、④、⑤、⑥、⑦功能不同产品型号支持有差异。

硬件规格

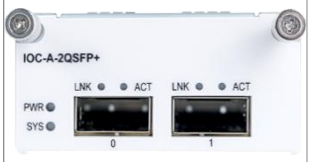
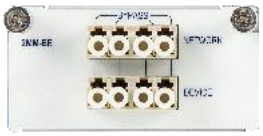
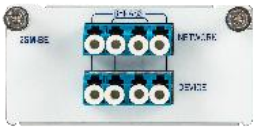
型号	A3600
产品图片	
网络层吞吐	20Gbps
最大并发连接数	3,000,000
每秒新建连接数	140,000
Ipsec 最大隧道数	10,000
IPsec VPN 吞吐	6 Gbps
IPS 吞吐	8.5Gbps
AV 吞吐	5.0Gbps
管理接口	1 个 CON 口，2 个 USB3.0 口，1 个 HA 口，1 个 MGT 口
固定业务接口	2 × SFP+，8 ×SFP，16 × GE（2 对 bypass）
可选配硬盘规格	500GB/1TB/2TB SSD
产品形态	1U
电源规格	交流单电源（默认），交流双电源（可选），直流单电源（可选）
电源输入范围	交流 100-240V，50/60Hz，直流-36V~ -72V
外形尺寸（WxDxH）	436.0mm*437.0mm*44. 0mm
设备重量	6.0kg
额定功率	100W
工作环境温度	0℃~40℃
环境相对湿度	10%~95%（不结露）

型号	A3700
产品图片	
网络层吞吐（标配）	20Gbps
最大并发连接数	6,000,000
每秒新建连接数	140,000
Ipsec 最大隧道数	20,000
IPsec VPN 吞吐	6.5Gbps
IPS 吞吐	8.6Gbps
AV 吞吐	5.2Gbps
管理接口	1 个 CON 口，2 个 USB3.0 口，1 个 HA 口，1 个 MGT 口

固定业务接口	2 × SFP+，8 ×SFP，16 × GE（2 对 bypass）
扩展模块槽位	1 个
扩展模块选项	IOC-A-4SFP+，IOC-A-2QSFP+，IOC-A-2MM-BE，IOC-A-2SM-BE
可选配硬盘规格	500GB/1TB/2TB SSD
产品形态	1U
电源规格	交流单电源（默认），交流双电源（可选），直流单电源（可选）
电源输入范围	交流 100-240V，50/60Hz；直流-36V~ -72V
外形尺寸（WxDxH）	436.0mm*437.0mm*44. 0mm(不含扩展模块)
设备重量	6.1kg
额定功率	100W
工作环境温度	0℃~40℃
环境相对湿度	10%~95%（不结露）

型号	A3800
产品图片	
网络层吞吐（标配）	20Gbps
最大并发连接数	8,000,000
每秒新建连接数	310,000
Ipsec 最大隧道数	20,000
IPsec VPN 吞吐	12Gbps
IPS 吞吐	17.5Gbps
AV 吞吐	9.4Gbps
管理接口	1 个 CON 口，2 个 USB3.0 口，1 个 HA 口，1 个 MGT 口
固定业务接口	2 × SFP+，8 ×SFP，16 × GE（2 对 bypass）
扩展模块槽位	1 个
扩展模块选项	IOC-A-4SFP+，IOC-A-2QSFP+，IOC-A-2MM-BE，IOC-A-2SM-BE
可选配硬盘规格	500GB/1TB/2TB SSD
产品形态	1U
电源规格	交流双电源（默认），直流双电源（可选）
电源输入范围	交流 100-240V，50/60Hz；直流-36V~ -72V
外形尺寸（WxDxH）	436.0mm*437.0mm*44. 0mm(含电源模块把手)
设备重量	6.8kg(不含电源)
额定功率	100W
工作环境温度	0℃~40℃
环境相对湿度	10%~95%（不结露）

扩展模块

指 标	IOC-A-2QSFP+	IOC-A-4SFP+	IOC-A-2MM-BE	IOC-A-2SM-BE
产品图片				
名称	2QSFP+40G光口扩展模块	4SFP+万兆光口扩展模块	两端口多模Bypass光口模块卡	两端口单模Bypass光口模块卡
接口描述	2端口40GQSFP+接口扩展卡	4端口万兆SFP+接口扩展卡	2对多模Bypass光口	2对单模Bypass光口
重量	0.96kg	0.96kg	0.96kg	0.96kg

文档编号：HS-NGFW-A-5.5R8P3.9-CH-202107-V1.0

官方微信　　官方微博