山石网科智能下一代防火墙

iNGFW T 系列

T1860 / T2860 / T3860
T5060 / T5860

随着互联网的发展，当前的网络安全形势面临着新的变化，APT、0-DAY 等网络攻击正在不断利用未知威胁对网络安全造成严峻挑战，而传统防火墙或是下一代防火墙对此无能为力。

传统防火墙采用基于签名技术的检测方式，只能发现特征库中所涵盖的威胁类型。而现代网络攻击具有隐蔽性、目的性、持续性、多变性等特点，导致传统防火墙无法识别威胁。这也是目前 APT 等网络攻击屡屡得逞的重要原因。

山石网科 T 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。同时，智能下一代防火墙在威胁检测的基础上，提供了核心资产重点防护、风险与威胁的可视化、策略联动实时风险减缓等功能，从而使安全防护成为闭环，为用户带来全新的安全体验。

产品亮点

基于行为分析，发现未知威胁

T 系列智能下一代防火墙内置了三大智能分析引擎——高级威胁检测引擎、异常行为检测引擎和关联分析引擎，可基于行为分析帮助用户发现未知网络威胁，定位风险主机，保护业务与数据安全。

高级威胁检测引擎收集终端主机的网络应用层行为，并将其与威胁行为集进行模糊匹配，根据两者相似程度可确定当前是否存在变种恶意软件等未知威胁。终端主机不论通过何种方式感染变种恶意软件，如网络传输或是 U 盘拷贝，T 系列智能下一代防火墙均可基于行为分析发现。T 系列智能下一代防火墙的威胁行为集来自于云端山石网科安全平台对海量威胁行为的大数据分析，提取为行为集后下发至本地设备中。

异常行为检测引擎能够持续学习所保护业务的应用层行为特征，并建立业务动态安全模型。通过将当前的网络层及应用层行为与安全模型进行偏离度分析，能够发现隐藏的网络异常行为，并根据行为特征确定攻击类型，如应用层 DDoS 攻击、扫描攻击、SSH/FTP 弱口令猜测等。

威胁关联分析引擎作为高级威胁和异常行为检测的连接桥梁，基于终端主机的网络行为和未知威胁进行关联分析，深度挖掘潜在的网络威胁之间的关联性，发现网络中的隐藏风险。

安全可视化，风险到威胁全面可视化

T 系列智能下一代防火墙提供了从风险到威胁的全面展现，包括网络风险指数、风险主机、核心资产及特定威胁的详细信息。通过多层次、立体展现，网络管理员可详细了解整体网络安全态势及风险背后的威胁根源。通过威胁关联分 析，T 系列智能下一代防火墙可展示风险主机所处的网络攻击链（Kill chain），揭示当前网络攻击所处的阶段及危害。此外，T 系列智能下一代防火墙提供了威胁报文的在线存储与解析功能。网络管理员不需借助其他工具，即可通 过浏览器查看报文协议及内容，帮助网络管理员对网络攻击事件进行取证与溯源。

策略联动，实时减缓风险

T 系列智能下一代防火墙在风险监测的基础上提供了策略联动功能，可在攻击发生时实时减缓风险。在检测到网络攻击并达到触发条件时，T 系列智能下一代防火墙启用减缓策略，通过自动或自定义的方式，实现会话限制、带宽限制、阻断等，从而及时将网络攻击抑制在低水平状态，避免攻击持续升级造成业务损害。通过实时的风险监测与策略联动，智能下一代防火墙能够帮助用户为业务提供实时的攻击防御，减缓风险。

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、风险等级等多维度的应用定义
- 多达几千种的应用特征库，支持网络实时更新

用户认证

- 支持本地用户Web认证
- 支持外部服务器用户认证(RADIUS、 LDAP、 MSAD)
- 支持MS AD用户组和OU同步
- 支持Web认证后的SSO
- 支持基于MAC的用户认证
- 支持微信连WIFI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

防火墙

- 基于深度应用识别的访问控制
- 基于应用/角色的安全策略
- 基于IP地理信息的访问控制
- 丰富的路由特性，强大的NAT及 ALG
- 防火墙策略重复与冗余规则检测
- 支持策略组的安全策略管理模式
- 全面的DNS策略，支持DNS黑白名单、DNS代理功能
- 支持netflow协议

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8000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

病毒过滤

- 基于流的病毒过滤
- 支持压缩病毒文件的扫描
- 超过200万的病毒特征库，病毒库支持网络实时更新

垃圾邮件过滤

- 实时的垃圾邮件分类和防御
- 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和POP3邮件协议
- Inbound and outbound 检测
- 免监控域白名单

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
- 定期僵尸网络服务器地址升级更新
- 支持C&C IP和域名两种方式检测
- 支持TCP和HTTP、DNS协议检测
- 支持C&C IP和域名白名单
- 基于域名生成算法（DGA）的C&C通道检测

异常行为检测

- 通过建立行为数据模型对主机及服务器进行异常行为检测
- 支持Flood、 SockStress、反射放大等网络及应用层DDoS攻击检测
- 支持慢速DDoS攻击检测
- 支持HTTP扫描、 Spider、 SPAM、 SSH/FTP弱口令等异常行为的检测

未知威胁检测

- 基于威胁行为集的未知威胁检测，行为集支持网络实时更新
- 支持2000多种Malware Family的检测，包含Virus，Worm，Trojan，Overow等类型
- 支持未知应用的加密通道检测

关联分析检测

- 挖掘未知威胁、异常行为和应用行为之间的关联性，发现潜在网络威胁
- 支持多维度关联分析规则库的云端同步
- 支持不同的数据源查询和执行周期

风险可视与减缓

- 提供全网风险指数、主机与威胁风险级别及风险确定度
- 提供风险主机的网络攻击链展现
- 提供威胁详细信息展示、威胁数据报文、日志等威胁分析取证工具
- 可基于风险类型制定减缓措施，支持自动减缓或自定义减缓

威胁管理

- 提供网络风险指数、主机风险指数、威胁事件逐级的可视化呈现
- 重点监控及防护核心资产对象
- 提供威胁详细信息展示、威胁数据报文、日志等威胁分析取证工具
- 管理员可针对威胁事件进行批量的误判、已处理等人工仲裁的操作
- 支持基于威胁类型制定减缓措施，实现威胁减缓，支持安全策略阻断、会话限制和流量管理等措施

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

数据安全

- 支持基于文件类型进行数据传输安全控制
- 支持HTTP、FTP、SMTP、POP3协议文件传输的识别
- 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

终端接入监控

- 支持NAT及跨三层环境识别接入网络终端数
- 支持识别Windows、iOS、Android等9种操作系统
- 支持IP及终端接入数的条件过滤

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
- 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分类的流量控制策略
- 支持针对每IP或每用户进行延时限速

链路负载均衡

- 一次性和周期性生成报表
- Outbound 相关功能 PBR 支持 ECMP、时间以及权重、支持内置 ISP，可针对目的地址或子网实时探测链路质量状况
- 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 及TLS v1.2(可选 USB-key)
- 支持IKEv2协议
- 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
- 支持国密软算法

IPv6

- 访问控制
- ND攻击防护
- 隧道、 DNS64/NAT64等多种过渡技术
- IPv6路由（静态路由、 RIPng、 OSPFv3、 BGP4+）
- 支持应用识别、URL过滤和病毒过滤

高可用性(HA)

- 支持主/主模式（ A/A）、主/备模式（ A/P）
- 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

分析诊断

- 支持多维度全局故障点检测

- 支持多手段数据包路经检测及图形化展示

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
- 支持用户操作系统与网络浏览器的识别监控
- 支持自定义应用的流量统计及用户粒度的自定义应用流量统计
- 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，不同方向、不同策略的管道流量查看

日志报表

- 支持URL日志、 NAT日志、会话日志、威胁日志等
- 支持天、周、月、年等周期报表统计
- 支持应用、流量、威胁等统计报表
- 支持HTML、 PDF报表格式
- 支持FTP上传、邮件外发报表
- 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

山石云·影

- 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
- 支持HTTP、HTTPS、SMTP、POP3、IMAP4、FTP协议
- 支持PE、APK、JAR、MS-OFFICE、PDF、SWF、RAR、ZIP文件类型的检测
- 全局威胁情报共享，快速阻断未知威胁传播

山石云·景

- 支持将设备注册到山石云·景云服务平台
- 通过手机APP、Web方式实时集中管控多台设备状态、网络流量、网络攻击等，及时获知告警信息
- 报表生成及云端保存
- 日志云端托管

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

关键指标

指 标	SG-6000-T1860	SG-6000-T2860	SG-6000-T3860	SG-6000-T5060	SG-6000-T5860
					
防火墙吞吐量（最大）	8Gbps	10Gbps	20Gbps	25Gbps	40Gbps
IPS吞吐量 (1)	3Gbps	4Gbps	8Gbps	12Gbps	18Gbps
AV吞吐量 (2)	1.6Gbps	2Gbps	6Gbps	7Gbps	10Gbps
IPSec吞吐量 (3)	3Gbps	3.8Gbps	12Gbps	15Gbps	28Gbps
最大并发连接数	150万	300万	400万	500万	600万
每秒新建连接数(TCP)	100,000	130,000	40万	45万	50万
每秒新建连接数(HTTP)	80,000	100,000	25万	30万	45万
IPSec隧道数	6,000	10,000	20,000	20,000	20,000
SSL VPN用户数（最大）	4,000	6,000	10,000	10,000	10,000
管理接口	1个CON口、 1个HA口，1个MGT口，1个USB2.0口，1个AUX口	1个CON接口，1 HA口，1 MGT口，1个USB口，1个AUX口	1个CON口，1个AUX口，1个USB口，2个HA口，1个管理口	1个CON口，1个AUX口，1个USB口，2个HA口，1个管理口	1个CON口，1个AUX口，1个USB口，2个HA口，1个管理口
网络接口	6个千兆电口，4个SFP接口	6个千兆电口（含一对Bypass接口）、4个SFP口、2个万兆SFP+口	2GE+4SFP	2GE+4SFP	2GE+4SFP
扩展模块槽	2个通用扩展槽	2个通用扩展槽	2个通用扩展槽	4个通用扩展槽	4个通用扩展槽
扩展模块选项	IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M	IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M	IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M、IOC-2SFP+-Lite	IOC-4XFP、IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M、IOC-2SFP+-Lite（在slot-3、4支持）、IOC-4SFP+、IOC-8SFP+	IOC-4XFP、IOC-4GE-B-M、IOC-8GE-M、IOC-8SFP-M、IOC-2SFP+-Lite（在slot-3、4支持）、IOC-4SFP+、IOC-8SFP+
电源规格	单150W，可选双冗余	单150W，可选双冗余	双冗余热插拔电源，最大功率450W	双冗余热插拔电源，最大功率450W	双冗余热插拔电源，最大功率450W
电源输入范围	交流100-240V，50/60Hz 直流-40V~-60V	交流100-240V，50/60Hz 直流-40V~-60V	交流100-240V，50/60Hz 直流-40V~-60V	交流100-240V，50/60Hz 直流-40V~-60V	交流100-240V，50/60Hz 直流-40V~-60V
产品形态	1U	1U	2U	2U	2U
外形尺寸(W×D×H, mm)	436.0mm× 366.0mm × 44.0mm	436.0mm× 366.0mm × 44.0mm	440.0mm × 520.0mm × 88.0mm	440.0mm × 520.0mm × 88.0mm	440.0mm × 520.0mm × 88.0mm
重量	5.6KG	5.6KG	15.5KG	15.8KG	15.8KG
工作环境温度	0-40℃	0-40℃	0-40℃	0-40℃	0-40℃
工作环境湿度	10-95%(不结露)	10-95%(不结露)	10-95%(不结露)	10-95%(不结露)	10-95%(不结露)

扩展模块

指 标	IOC-8GE-M	IOC-8SFP-M	IOC-4GE-B-M	IOC-2SFP+-Lite	IOC-4XFP	IOC-4SFP+	IOC-8SFP+
							
名称	8×GE接口扩展卡	8×SFP接口扩展卡	4×GE Bypass接口扩展卡	2SFP+接口扩展模块	4×XFP接口扩展卡	4SFP+接口扩展模块	8SFP+万兆光口扩展模块
网络接口	8端口千兆电接口	8端口千兆SFP接口 不含SFP模块	4 端口千兆电接口， 含2对Bypass接口	2端口万兆SFP+接口 不含SFP+模块	4端口万兆XFP接口， 不含XFP模块	4端口万兆SFP+接口 不含SFP+模块	8端口万兆SFP+接口 不含SFP+模块
外形尺寸	半U高，占用1个通用扩展槽	半U高，占用1个通用扩展槽	半U高，占用1个通用扩展槽	半U高，占用1个通用扩展槽	1U高，占用2个通用扩展槽	1U高，占用2个通用扩展槽	1U高，占用2个通用扩展槽
重量	0.8kg	0.9kg	0.8kg	0.26kg	0.9kg	0.7kg	0.7kg
适用平台	全系平台	全系平台	全系平台	T3860\T5060\T5860	T5060\T5860	T5060\T5860	T5060\T5860

除非另有说明，否则所列出的性能，容量和特性是基于运行StoneOS®5.5R5的系统，实际结果可能会因StoneOS®版本和部署情况而异。

注：(1) IPS吞吐量采用HTTP的1M字节payload，扫描32K字节长度测试得到，(2) AV吞吐量采用HTTP的1M字节payload测试得到，
(3) Ipsec吞吐量用Presharekey+AES256+SHA-1，用1400字节数据流测试得到。