1. 抗拒绝服务系统（抗DDoS系统）
   1. 功能对比

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **内容/品牌** | |  | | --- | |  | | |  | | --- | |  | |  |
| **绿盟ADS** | **启明星辰ADM-Guard** | **迪普DPtech Guard** |
| **防护功能** | | | |
| **方案集中度** | **由流量检测、流量清洗、集中管理设备构成完整的单点DDOS解决方案，也支持与第三方品牌的流量检测设备联动，形成一体化方案** | **整个方案由流量检测、流量清洗设备组成，缺乏独立可用的集中管理组件，设备管理和数据集中呈现能力较弱** | **拥有自研的流量清洗、流量检测和流量管理设备，不支持与其他品牌流量分析设备联动，支持DPI/DFI** |
| **防护算法** | **具备TCP/UDP/ICMP/DNS/连接耗尽/CC及变种/BGP路由/混合攻击检测算法  针对CS架构（游戏业务）的水印防护算法** | **主要亮点体现在流量管理、应用管理和应用识别，CC防护较弱，性能损失严重，且存在较高误检测率** | **SYN Flood、UDP Flood、ICMP Flood、DNS Query Flood、HTTP Get Flood、CC攻击** |
| **性能表现** | **在网络层泛洪攻击和应用层精巧型攻击背景下均具有稳定的性能表现，性能损失较小，小包处理能力较强，目前单体最大防护能力为120G** | **在小包性能测试时，其性能表现只有宣传值的40%，且流量检测设备分析性能不到1万FLOW/S** | **宣传最大吞吐为40G** |
| **产品成熟度** | **2002年发布抗DDOS产品，在金融、运营商、互联网等行业取得大量的产品部署案例和应急响应服务案例** | **2008年通过防火墙产品升级演进至抗DDOS产品，保留了大部分防火墙的功能，且增加了部分网络优化功能，国内市场案例和经验较少** | **2010年发布抗DDOS产品，以低价策略冲击渠道与SMB市场，在运营商、金融和互联网等行业的案例不多** |
| **产品开放性** | **支持与同品牌和第三方的NETFLOW异常流量检测设备联动** | **仅支持与自研流量检测设备联动** | **仅支持与自研流量检测设备联动** |
| **产品架构设计** | **基于多核平台的非防火墙架构设计，没有并发新建连接数的局限，有效避免自身成为瓶颈和故障点，且设备间呈松耦合，独立性高，容错能力强** | **由防火墙衍生而来，保留了防火墙大多数特性，自身容易成为性能瓶颈和故障点** | **——** |
| **产品目标市场** | **支持与自研的网络攻击态势监测系统、WEB应用防护系统和云监护服务形成纵深安全防护体系，有效解决大流量侵袭、资源耗尽、威胁溯源和设备运维管理的问题** | **不具备一体化纵深防护设计，主打单点(中小型网络节点)DDOS解决方案** | **不具备一体化纵深防护设计，主打单点(中小型网络节点)DDOS解决方案** |
| **规则过滤** | **基于ACL的黑名单、报文特征过滤、TCP正则过滤、HTTP协议验证、模式匹配、动态指纹、GeoIP过滤、云端IP信誉库** | **基于ACL的黑名单、报文特征过滤、TCP正则过滤、HTTP协议验证、服务器侧移动代码过滤、WEB关键字过滤** | **基于ACL的黑名单、报文特征过滤、HTTP协议验证** |
| **传输层防护** | **SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood、TCP Fragment Flood、UDP FragmentFlood、UDP Flood、ICMP Flood (3种SYN算法)** | **SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood、TCP Fragment Flood、UDP FragmentFlood、UDP Flood、ICMP Flood、(1种SYN算法)** | **SYN Flood、SYN-ACK Flood、ACK Flood、FIN/RST Flood、TCP Fragment Flood、UDP FragmentFlood、UDP Flood、ICMP Flood、(1种SYN算法)** |
| **Web防护** | **HTTP Get Flood、HTTP Post Flood、HTTP Slow header attack、HTTP Slow Post attack、HTTPS Flood、SSL-DoS/DDoS、HTTP代理检测，拥有8种CC算法** | **仅支持HTTP Get Flood、HTTP Post Flood，提供5种CC防护算法** | **HTTP Get Flood、HTTP Post Flood、HTTP Slow header attack、HTTP Slow Post attack，提供2种CC防护算法** |
| **游戏防护** | **提供2种防护算法** | **不支持** | **不支持** |
| **Connection flood** | **连接耗尽、TCP重传、TCP慢连接、Sockstress、空连接攻击、会话数限制** | **连接耗尽、TCP重传、Sockstress、会话数限制** | **连接耗尽、TCP重传、TCP慢连接、空连接攻击、会话数限制** |
| **VoIP** | **支持** | **支持** |  |
| **畸形包防护** | **IP Spoofing、LAND、Smurf、Fraggle、Winnuke、Ping of Death、Tear Drop、IP option control packet、IP fragment packet、ICMP fragment packet、Large ICMP control packet、ICMP redirect packet、ICMP unreachable packet** | **IP Spoofing、LAND、Smurf、Fraggle、Winnuke、Ping of Death、Tear Drop、IP option control packet、IP fragment packet、ICMP fragment packet、ICMP unreachable packet** | **IP Spoofing、LAND、Smurf、Winnuke、IP option control packet、IP fragment packet、ICMP fragment packet、Large ICMP control packet、ICMP redirect packet、ICMP unreachable packet** |
| **扫描防护** | **Port scanning、IP sweep、TRACERT packet、IP source routing option packet、IP timestamp option packet、IP route record option packet** | **Port scanning、IP sweep、TRACERT packet、IP source routing option packet、IP timestamp option packet、IP route record option packet** | **Port scanning、IP sweep、IP timestamp option packet、IP route record option packet** |
| **僵木蠕特征库** | **支持** | **不支持** | **不支持** |
| **引流回注** | **BGP、OSPF、PBR、MPLS VPN回注、MPLS LSP回注、GRE tunnel回注、Layer-2 回注** | **BGP、PBR、MPLS VPN回注、GRE tunnel回注、Layer-2 回注、QOS回注** | **BGP、PBR、MPLS VPN回注、GRE tunnel回注、Layer-2 回注、QOS回注** |
| **联动功能** | **支持与自研流量检测设备和第三方流量检测设备联动、支持NETFLOW，支持与其他安全系统联动、可提供云清洗与云监控服务** | **支持与自研流量检测设备和第三方流量检测设备联动、支持NETFLOW，支持与其他安全系统联动、** | **仅支持与自研流量检测设备联动、支持Netflow/镜像** |

* 1. 资质对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **资质和荣誉（独家优势）** | | | | |
| **权威机构** | **荣誉值** | **绿盟** | **启明** | **迪普** |
| **Frost&Sulivan** | 全球权威数据咨询机构。为用户提供可靠的市场投融资及战略与管理咨询服务 | 2011年，亚太第三。  2012年，无报告  2013年，亚太第三。  2014年，亚太第二。  （国内厂商在亚太的最高排名） | 无 | 无 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **资质** | **绿盟** | **启明** | **迪普** |
|  | **公安部销售许可证** | **具备** | **具备** | **具备** |
|  | **软件著作权登记证书** | **具备** | **具备** | **具备** |
|  | **软件产品登记证书** | **具备** | **具备** | **具备** |
|  | **涉密信息系统产品检测证书** | **具备** | **无** | **无** |
|  | **IT产品信息安全认证证书** | **具备** | **具备** | **具备** |
|  | **Veracode产品自身安全性认证** | **具备** | **无** | **无** |
|  | **IPV6 Ready认证** | **具备** | **无** | **无** |
|  | **国家信息安全测评信息技术产品安全测评证书（EAL3+）** | **具备** | **无** | **无** |

1. Web应用防护系统（WAF）
   1. 功能对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 产品功能 | 功能描述 | 绿盟 | 启明 | 天融信 |
| 智能引擎检测 | 传统WAF均能实现对SQL注入和跨站攻击的检测，但因其原理基于特征匹配，误报率较高，经常会造成业务请求误拦截。需具备新的防护机制减少误报率 | 绿盟新推出的智能引擎能够针对SQL注入和跨站攻击进行智能检测，从而提供更高的检测率和更低的误报率。该功能由绿盟攻防研究院直接对接维护，准确性非常高。 | 仅集成了传统SQL注入、跨站攻击防护的特征码，误报率高 | 仅集成了传统SQL注入、跨站攻击防护的特征码，误报率高 |
| SSL加速功能 | 支持SSL硬件加速卡，最大程度提升WAF在处理HTTPS站点时的性能 | 绿盟WAF在硬件底层集成了SSL加速插槽，支持在界面开启/关闭SSL硬件加速卡，提高HTTPS站点的防护性能 | 不支持 | 不支持 |
| IP信誉 | 从信誉云中获取IP信誉数据，并将其应用在WAF设备进行IP判断，为本地WAF提供更便捷、更准确的IP防护服务 | 绿盟WAF支持与绿盟信誉云对接，获取云端信誉数据，实现一点发现，全局获益 | 不支持 | 不支持 |
| 慢速攻击防护 | 慢速连接攻击针对目标服务器建立一个连接后，以非常低的速率向服务器发送数据包，使服务器的资源不能及时释放，如果有很多个客户端持续建立这样的连接，那么服务器的可用TCP连接数将很快被耗尽，不再接受新的请求，从而导致拒绝服务攻击 | 绿盟支持慢速攻击防护 | 不支持 | 不支持 |
| 会话跟踪 | 串联整个攻击链，将攻击的每个环节提炼成攻击事件，提升安全运维效果 | 绿盟WAF会话追踪功能：通过追踪用户向Web应用服务器发起的访问请求以及用户所有的Web操作，并记录详细的访问日志，为攻击事件事后分析、攻击场景还原、以及关联用户所有的Web操作提供关联分析数据基础，同时还能进行用户行为研究，了解用户操作背后是否隐藏了潜在的攻击动机。 | 需通过外置SOC产品实现该功能 | 需通过外置日志搜集产品实现该功能 |
| 暴力破解细粒度防护 | 支持基于阈值检测以外的防爆破算法，提升防护准确性 | 绿盟WAF的暴力破解模块支持阈值统计、Referer检测、验证码算法、能够识别能够识别Form、Ajax、Jsonp等多种登录验证方式。 | 仅支持阈值统计，误报率高 | 仅支持阈值统计，误报率高 |
| 支持与云安全服务扫描服务或本地扫描器联动防护 | 通过安全厂商云平台提供的的WEB漏洞扫描服务，对WAF防护站点进行WEB漏洞扫描，WAF能获取被防护站点的WEB漏洞扫描报告，并根据自身已有的规则自动生成一套新的规则，应用于被保护站点。当被防护站点加载自动生成的新规则之后，之前被扫描出的WEB应用漏洞将无法重现。 | 绿盟WAF支持与绿盟云极光产品或绿盟扫描产品进行联动防护 | 不支持 | 不支持 |
| 扫描防护 | 防范恶意扫描 | 绿盟WAF的扫描防护策略中可以根据动作、规则、请求样本数值范围、应答成功失败比例关系、统计量、统计时间、阈值告警等多个维度进行配置，并可以针对不同站点提供不同的解决方案。 | 防扫描功能配置不灵活，只能对已知扫描器的特征进行防护 | 防扫描功能配置不灵活，只能对已知扫描器的特征进行防护 |
| 大规模DDOS流量清洗 | WAF本身提供TCP Flood防护功能，当DDoS攻击超过了本身防护阈值的情况下，还能跟专业抗拒绝服务攻击产品组成的清洗中心联动，达到分层清洗的目的。 | 绿盟WAF支持与绿盟抗拒绝服务系统（ADS）进行联动，对大流量DDoS进行分层清洗 | 不支持 | 不支持 |
| 支持移动终端手机APP管理 | 通过手机移动端查看WAF实时运行情况 | 绿盟开发了手机APP（android和ios版本），支持WAF手机运维 | 不支持 | 不支持 |

* 1. 资质对比

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **资质和荣誉（独家优势）** | | | | |
| **权威机构** | **荣誉值** | **绿盟** | **启明** | **天融信** |
| **Gartner** | 入选国际权威机构Gartner魔力象限报告 | 2014-2017，绿盟WAF连续四年入选Gartner魔力象限 | 2017年，启明WAF第一次入选Gartner魔力象限 | 无 |
| **Frost&Sulivan** | 全球权威数据咨询机构。为用户提供可靠的市场投融资及战略与管理咨询服务 | 2010~2015年，绿盟科技持续六年引领WAF国内市场，连续两年国内唯一一家入选亚太前三 | 无 | 无 |
| **ICSA Labs** | 国际信息安全实验室 ICSA\_国际认证机构 | 国内唯一通过ICSA Labs的WAF产品 | 无 | 无 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **资质** | **绿盟** | **启明** | **天融信** |
|  | **参与起草《信息安全技术WEB应用防火墙安全技术要求》GA/T1140-2014标准** | **具备** | **具备** | **具备** |
|  | **VERACODE认证** | **具备** | **具备** | **具备** |
|  | **军用信息安全产品认证证书（军B级）** | **具备** | **具备** | **具备** |
|  | **分级评估证书/型号证书（EAL3+）** | **具备** | **具备** | **具备** |
|  | **IPv6 Ready Logo认证** | **具备** | **具备** | **具备** |
|  | **OWASP** | **具备** | **具备** | **具备** |