

高级威胁网络防护系统 【AIS EDGE】

如今，持续进化的网络威胁（APT）环境带来了更复杂的攻击场景。除了商业化的攻击行为，为了达到专业化的战术目标并在企业内部创建一个持续的攻击据点，黑客的攻击行为也不再仅仅是普遍的破坏行为（如之前爆发的蠕虫风暴），而是采用了多目标、多阶段、更低调的攻击方式。传统的防毒墙、防火墙、IPS等安全硬件已无法完全满足企业的安全防护要求。

亚信安全高级威胁网络防护系统 AIS EDGE 集多年积累的全球顶级内容识别技术，采用全新一代的高级威胁侦测及分析引擎，无缝对接深度威胁发现平台，颠覆传统架构，构建出基于深度内容安全的统一智能安全网关，在全面整合传统安全网关的同时，又提供了完整、深入、高效的内容安全防护，实现了功能和性能的全面提升，保护您的服务器与终端使用安全，确保您的核心数据资产免遭窃取或破坏，保障您的业务可持续运行。

应用情景

①VPN远程办公防护



在提供VPN的基础上，对传输的内容进行病毒和威胁的过滤，保障链路和内容的安全

②文件共享安全防护



支持win 7、win10的SMB安全防护

③互联网络出口防护



采用web信誉技术，对访被问的URL的安全等级实时进行评估及处理

④重要业务区域防护



支持虚拟补丁功能，在服务器安装补丁前屏蔽漏洞，阻止已知漏洞被利用

功能

优势



- **业界性能最好的“防毒墙”**
 - 采用基于深度包检测的高性能流扫描引擎，一次性扫描，全方位分析，解决了传统网关内容扫描所造成的性能瓶颈问题
 - 支持HTTP、FTP、SMTP、POP3、SMB等超过100种协议的识别和分析
- **具有病毒威胁防护的“绿色VPN”技术**
 - 支持SSL VPN PPTP VPN IPSEC VPN三种VPN技术，并能够对传输内容进行病毒扫描以及漏洞防护功能
- **无缝对接亚信安全防护产品，精密联动能力**
 - 无缝对接亚信安全其他高级威胁产品，例如：UAP、TDA、DDAN等，形成APT治理闭环