深信服下一代防火墙

产品名称	深信服下一代防火墙
公司名称	北京天际恒通科技有限公司
价格	面议
规格参数	
公司地址	北京市海淀区农大南路硅谷亮城2号210室
联系电话	86-010-62619156 15611565348

产品详情

NGAF是面向应用层设计，能够精确识别用户、应用和内容，具备完整安全防护能力，能够全面替代传统防火墙，并具有强劲应用层处理能力的全新网络安全设备。NGAF解决了传统安全设备在应用管控、应用可视化、应用内容防护等方面的巨大不足，同时开启所有功能后性能不会大幅下降。NGAF 不但可以提供基础网络安全功能，如状态检测、VPN、抗DDoS、NAT等；还实现了统一的应用安全防护，可以针对一个入侵行为中的各种技术手段进行统一的检测和防护，如应用扫描、漏洞利用、Web入侵、非法访问、蠕虫病毒、带宽滥用、恶意代码等。NGAF可以为不同规模的行业用户的数据中心、广域网边界、互联网边界等场景提供更加精细、更加全面、更高性能的应用内容防护方案。

更精细的应用层安全控制　　当前网络环境中，应用已成为网络的主要载体，而网络安全的威胁更多的来源于应用层，这也使得用户对于网络访问控制提出更高的要求。如何精确的识别出用户和应用、阻断有安全隐患的应用、保证合法应用正常使用、防止端口盗用等问题，已成为现阶段用户对网络安全关注的焦点。但IP不等于用户、端口不等于应用，传统防火墙基于IP/端口的五元组访问控制策略已不能有效的应对现阶段网络环境的巨大变化。

NGAF采用独创的应用可视化技术，可以根据应用的行为和特征实现对应用的识别和控制，而不仅仅依赖于端口或协议，摆脱了传统设备只能通过IP地址来控制的尴尬，即使加密过的数据流也能应付自如。

目前，NGAF可以识别700多种应用及其1000多种应用动作，还可以与多种认证系统（AD、LDAP、Radius等）、应用系统（POP3、SMTP等）无缝对接，自动识别出网络当中IP地址对应的用户信息，并建立组织的用户分组结构；既满足了普通互联网边界行为管控的要求，同时满足了在内网数据中心和广域网边界的部署要求，可以识别和控制丰富的内网应用，如Lotus Notes、RTX、Citrix、Oracle EBS、金蝶EAS、SAP、LDAP等，针对用户应用系统更新服务的诉求，NGAF还可以精细识别Microsoft、360、Symantec、Sogou、Kaspersky、McAfee、金山毒霸、江民杀毒等软件更新,保障在安全管控严格的环境下，系统软件更新服务畅通无阻。

因此，通过应用可视化技术制定的L3-L7一体化应用访问控制策略，可以为用户提供更加精细和直观化控制界面，在一个界面下完成多套设备的运维工作，提升工作效率。

更全面的内容级安全防护　　网络安全与黑客技术的发展使得用户面临的威胁不再单单是一个病毒一个木马、一次DOS攻击这样的简单攻击。黑客可采用丰富的工具，利用众多的漏洞，结合多种攻击手段进行混合型的破坏性攻击，具有代表性的如Slammer、Blaster等。而信息获取和攻击代码往往也隐藏在正常的应用访问中，这种混合型安全威胁的出现也给网络安全建设提出新的要求：需要采用更全面的防护手段，防止安全短板被利用；需要深入到应用内容的安全防护，以识别和预防潜在威胁。

NGAF融合了漏洞防护、web安全防护、病毒防护等多种安全技术，具备2000+条漏洞特征库、数十万条病毒、木马等恶意内容特征库、1000+Web应用威胁特征库，可以全面识别各种应用层和内容级别的各种安全威胁。通过灰度威胁关联分析技术将数据包还原的内容进行全面的威胁检测，并可以针对黑客入侵过程中使用的不同攻击方法进行关联分析，从而精确定位出一个黑客的攻击行为，有效阻断威胁风险的发生。灰度威胁识别技术改变了传统IPS等设备防御威胁种类单一，威胁检测经常出现漏报、误报的问题，可以帮助用户最大程度减少风险短板的出现，保证业务系统稳定运行。

此外，深信服凭借在应用层领域6年以上的技术积累，组建了专业的安全攻防团队，可以为用户定期提供最新的威胁特征库更新，以确保防御的及时性。

更高性能的应用层处理能力　　性能和安全往往是传统安全设备是无法权衡的问题。尤其在应用层安全防护功能开启时，该问题尤为明显。在带宽不断提升、威胁不断增多的网络环境下，用户不得不在两者做出艰难的选择。

为了实现强劲的应用层处理能力，NGAF抛弃了传统防火墙NP、ASIC等适合执行网络层重复计算工作的硬件设计，采用了更加适合应用层灵活计算能力的多核并行处理技术；在系统架构上，NGAF也放弃了UTM多引擎，多次解析的架构，而采用了更为先进的一体化单次解析引擎，将漏洞、病毒、Web攻击、恶意代码/脚本、URL库等众多应用层威胁统一进行检测匹配，从而提升了工作效率，实现了万兆级的应用安全防护能力。

更完整的安全防护方案　　只提供基于应用层安全防护功能的方案，并不是一个完整的安全方案。对于用户来说，还需要采购基础网络层的安全设备（FW、VPN），既增加了成本，也增加了组网复杂度、提升了运维难度。从技术角度来说，一个黑客完整的攻击入侵过程包括了网络层和应用层、内容级别等多个层次方式方法，如果将这些威胁割裂开处理进行防护，各种防护设备之间缺乏智能的联动，很容易出现“三不管”的灰色地带，出现防护真空。

NGAF涵盖传统防火墙、IPS的主要功能，内部能够实现内核级联动，是一个“L2-L7完整的安全防护产品”。这也是Gartner定义的“额外的防火墙智能”实现的前提，做到真正的内核级联动，才能为用户的业务系统提供一个安全防护的“铜墙铁壁”。