深信服AF-1320 下一代防火墙 关注网络安全 提供网络安全服务方案

产品名称	深信服AF-1320 下一代防火墙 关注网络安全 提供网络安全服务方案
公司名称	东莞瀚晨计算机信息技术有限公司
价格	面议
规格参数	品牌:深信服 型号:AF-1320 VPN:支持VPN
公司地址	东莞市东城区东城中路南81号辉煌商务大厦5楼D 29-30
联系电话	0769-23607210 15322951118

产品详情

产品型号：af-1320

概述：

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 ”。

功能价值：

多种功能融合、纵深安全防御、一体化安全防护	
技术功能	功能价值
ips漏洞防护	基于漏洞以及攻击行为的特征库，提供自动或手动升级方式。防御包括蠕虫、木马、后门、应用层dos/ddos、扫描、间谍软件、漏洞攻击、缓冲区溢出、协议异常、ips逃逸攻击等
服务器防护	针对owasp提出的web安全威胁的防护，如sql注入、xss、csrf等；提供网站路径保护，暴力破解防护；web服务隐藏ftp隐藏、ftp、telent弱口令防护；文件上传过滤、url黑名单等多种服务器防护功能
病毒防护	基于流引擎查毒技术，可以针对http、ftp、smtp、pop3等协议进行查杀；可实时查杀大量文件型、网络型和混合型等各类病毒；并采用新一代虚拟脱壳和行为判断技术，准确查杀各种变种病毒、未知病毒

web安全防护	提供url过滤、文件过滤、activex过滤、脚本过滤等多种web安全防护手段

透视网络应用、精细控制策略、规避应用安全风险	
技术功能	功能价值
可视化应用管控	拥有国内最大的应用规则识别库，可识别数百种互联网应用，上千种应用规则策略
	可识别丰富的内网应用如：lotus notes、rtx、citrix、oracle ebs、金蝶eas、sap、ladp等
	精确识别microsoft、360、symantec、sogou、kaspersky、金山毒霸、江民杀毒等软件更新保障严格管控下系统软件更新畅通无阻
	提供基于应用识别类型、用户名、接口、安全域、ip地址、端口、时间进行应用访问控制列表的制定

丰富日志报表、统一集中管理、最优运维成本	
技术功能	功能价值
数据中心	提供内置数据中心和独立数据中心
详细报表	提供统计报表、趋势报表、汇总报表、汇总对比报表、指定对比报表危险行为报表、流速趋势报表等多种报表
统计分析	提供详细的ips/服务器防护统计、病毒信息统计分析
智能风险报表	提供根据管理者自定义的风险行为特征自动挖掘并输出风险行为智能报表

限制无关应用、保障核心业务、优化带宽利用率	
技术功能	功能价值
可视化流量管理	基于应用、网站、文件、时间、目标ip以及用户的多种流量控制
	多线路技术、虚拟多线路技术、智能选路技术对多线路分别实现流控
	保障核心业务、限制合法业务、阻断非法业务

适应复杂场景、抵御网络攻击、合理规划安全域	
技术功能	功能价值
包过滤与状态检测	提供静态的包过滤和动态包过滤功能
抗攻击	能够防御dos/ddos、land,smurf,synflood,icmpflood等网络层攻击

nat	提供一对一、多对一、多对多等地址转换方式；支持多种nat alg，包括dns、ftp、h.323、sip
vpn模块	内置vpn模块能实现vpn互联
ip协议/路由	支持静态路由、rip v1/2、ospf、策略路由等多种路由协议

产品方案：

需求概述 互联网及it技术的应用在改变人类生活的同时，也滋生了各种各样的新问题，其中信息网络安全问题将成为其面对的最重要问题之一。网络带宽的扩充、it应用的丰富、互联网用户的膨胀式发展，使得网络和信息平台早已成为攻击爱好者和安全防护者最激烈斗争的舞台。web时代的安全问题已远远超于早期的单机安全问题，尽管防火墙、ids、utm等传统安全产品在不断的发展和自我完善，但是道高一尺魔高一丈，黑客们不仅专门针对安全设备开发各种工具来伪装攻击、逃避检测，在攻击和入侵的形式上也与应用相结合越来越紧密。这些都使传统的安全设备在保护网络安全上越来越难。目前更多的出现了以下的安全问题：

投资成本攀升，运维效率下降 许多企业为了应对复杂的安全威胁,购买了多个厂商的安全产品,安全建设犹如堆积木一般。购买的安全防护产品愈来愈多，问题也随之出现：大量的安全防护产品部署，需要大量专业安全管理人员负责维护，复杂的安全架构使得管理同样变得复杂化，由于企业采用了多套安全解决方案，这就要求有很多技术人员精通不同厂商的解决方案。购买产品很简单，日常运维很复杂，这对企业本来就有限的it人员、安全管理人员来讲是非常痛苦和困难的事情。而且不同厂商安全解决方案之间的协调性也有待商榷，当专业化的攻击和威胁来临时，这些安全产品之间能不能发挥协同作用抵御威胁这还是一个很大的问号。对企业的管理者来说，如何降低管理成本、提高运维效率、提升企业安全水平，是目前最急待解决的问题。

“ 数据库泄密 ”、“ 网页遭篡改 ”等应用层安全事件频现 2011年上半年，索尼超过1亿个客户帐户的详细资料和1200万个没有加密的信用卡号码失窃，索尼已花掉了1.71亿美元用于泄密事件之后的客户挽救、法律成本和技术改进这笔损失只会有增无减。 2011年5月10日上午消息，一些兜售廉价软件的黑客攻击了多个知名网站，包括美国宇航局(以下简称“ nasa ”)和斯坦福大学的网站。 有网友就在微博中反映：买家在自己开的网店购物之后，付款时却将货款打到一个不相干的帐户。后查明，是这个买家此前已经中毒。这种情况下，在中毒电脑上进行的所有交易都将给骗子付款。
尽管部署了众多安全设备,此类问题仍然频发,原因何在： >
当前攻击层次逐步向应用层转变，传统防火墙失效; >
黑客采取混合攻击，组合多种威胁方法，传统的单点式安全设备失效; >
黑客采取混合攻击,单点式安全设备串联,或是utm, 由于都未真正融合众多安全功能,无法将各种攻击信息关联和共享,无法跟踪黑客攻击攻击各个环节,漏网威胁与日俱增。

网管员对企业流量束手无策 当前网络中流量多为七层应用，传统安全设备对其不可见，致使it管理员无法了解哪些应用处于使用中以及哪些用户在使用这些应用，无法轻松区分好应用和坏应用，无法根据网络状况实施控制策略，如何将网络控制权重新还给it管理员亟待解决。

部署utm，网络中断或访问变慢 utm貌似可以解决以上问题，然而，utm非多种安全防护功能的真正集成，功能全开后性能大幅下降，花重金购置的设备被迫成为了摆设，客户急需真正的一体化安全设备且不应该导致网络运行中断。

内网出现威胁，追究责任困难 企业内网拥有强大的认证系统，传统安全产品无法与之有机结合，使之

孤立存在，从而内网安全机制无法定位到人员，出现问题只能定位于大量的ip地址，网管不是计算机，从一大堆的ip地址中，定位具体人员十分困难。
安全设备越快适应现网的认证系统，并充分融合，安全问题真正落实到位，是多年来企业it人员的梦想。

安全建设方案

为了能够更好的针对当前网络安全现状，控制好可能发生的各种安全风险，建议采用下一代防火墙深信服ngaf针对业务系统进行全面的安全加固。 首先，我们建议将整个业务系统划分为如下网络安全域：

数据中心安全域：包括各种应用系统和服务器，如oa、视频、erp、mail等，由于是整个it系统的核心，安全级别最高；广域网边界安全域：各个分支机构通过专网接入总部局域网，访问各种业务应用系统，主要包括构建专网的核心路由器、分支路由器；互联网接入安全域：由于内部终端、对外发布业务系统（如网上交易系统）都需要与互联网相连，访问互联网资源或者对外提供业务。此区域安全风险最高，需要重点隔离与控制；内网办公安全域：包括总部内网的办公终端，为不同的部门提供高速、稳定的网络接入；

其次，根据这些网络安全域之间的访问关系、安全级别，我们建议在如下位置部署ngaf进行一体化的l2-l7安全防护与控制，整体方案如下图所示：

ngaf部署的总体方案

数据中心服务器保护 内部数据中心的服务器承载的业务尤为重要，是整个ｉｔ系统的核心组成部分，因此需要从如下四个方面着重考虑：1）访问控制：谁可以访问数据中心？什么应用可以访问数据中心？盗用ip身份怎么办？如何防止应用的滥用和误用？传统防火墙基于端口/ip能否解决？
2）威胁攻击的问题：如何保护数据中心免受病毒、木马攻击；防止数据中心服务器被攻击
3）数据中心可用性：数据中心流量大，需要有效保证核心业务可用性
4）安全事件应用响应问题：如何了解数据中心安全风险问题？是否可以帮助管理员制定策略？

数据中心方案拓扑

通过在数据中心核心交换机外侧部署深信服ngaf可以帮助我们实现如下四个安全目标：1）面向用户、应用的安全访问：将访问控制权限精确到用户与业务系统，有效解决了传统防火墙ip/端口的策略无法精确管理的问题。让业务开放对象更为明了、管理更方便、策略更易懂。 2）7层的内容安全检测：7层一体化安全防护（包括漏洞防护、服务器防护、病毒防护等）以及智能的内容安全过滤功能，防止各种应用威胁干扰服务器的稳定运行，确保核心业务数据的安全。 3）核心业务有保障： 基于应用的流量管理，保证核心业务带宽充足。万兆的应用层性能，有效保障数据中心的可用性。 4）可视化安全风险评估：提供服务器风险和终端风险报告以及应用流量报表，使全网的安全风险一目了然，帮助管理员分析安全状况管理数据中心。

广域网边界安全隔离与防护 对于广域网边界安全防护需要从如下几个方面着重考虑：1）人员多，应用杂：如何制定有效的acl，acl是基于ip和端口的，这样的机器语言无法直观、清晰的制定访问控制策略，容易出现错配、漏配；2）传统fw缺乏应用层威胁防护，病毒木马在分支机构和总部间传播速度快
3）病毒木马占用广域网有限带宽，影响关键业务的传输
4）分支数量多，it管理水平层次不齐，设备多，成本高，组网杂，维护难

广域网边界安全防护方案拓扑

通过在核心交换机与核心路由器之间部署深信服ngaf，可以帮助我们实现如下安全目标：1）面向用户、应用的安全访问：将访问控制权限精确到用户与业务系统，有效解决了传统防火墙ip/端口的策略无法精确管理的问题。让业务开放对象更为明了、管理更方便、策略更易懂 2）广域网垃圾流量清洗：通过ngaf智能的内容安全过滤功能，将病毒、木马、蠕虫、ddos等各种垃圾流量清除，确保带宽纯净，防止病毒扩散 3）一体化部署，简化组网：
ngaf具备l2-l7一体化安全防护功能，可以简化组网，简便管理，提高性价比；

互联网出口边界防护 由于互联网边界实现了对外业务发布系统和内网终端的互联网接入，因此需要从如下几个方面着重考虑：对外业务系统发布：
1）网站被挂马、数据遭篡改，企业/单位形象受损，造成经济损失，带来负面影响
2）合理控制服务器外联权限，封堵黑客远程控制，上传病毒、木马；
3）响应速度要求快，系统稳定性要求高，需要简化组网，降低延时，减少单点故障；

内网终端互联网接入：1）浏览器、os、flash漏洞多，上网容易感染病毒、木马，窃取隐私
2）合理控制服务器外联权限，封堵黑客远程控制终端，将内网终端作为跳板，入侵服务器
3）用户权限多样，安全策略配置复杂

互联网边界安全方案拓扑

通过在互联网接入路由器后部署深信服ngaf，网上交易系统部署在dmz区，可以实现对内网终端和对外业务发布系统的双重防护 对外业务发布系统防护：1）防止黑客入侵，获取权限，窃取数据：通过ngaf的漏洞防护、服务器防护、病毒防护等多种应用内容防护功能，防止黑客入侵，保证服务器稳定运行；2）精确控制服务器外联权限：通过ngaf精确的应用识别，放行服务器补丁升级、病毒库升级等必要外联流

量，阻断各种无关非法外联流量； 3）简化组网、降低延时： ngaf具备l2-l7一体化安全防护功能，可以简化组网，减少故障点；通过单次解析引擎减低延时；

内部终端安全防护： 1）全面防护，标本兼治：通过ngaf的恶意网站过滤功能，防止终端访问威胁网站和应用；通过漏洞防护、病毒防护、恶意控件/脚本过滤功能，切断威胁感染终端的各种技术手段； 2）精确识别，防止非法外联：通过ngaf精确的应用识别，放行服务器补丁升级、病毒库升级等必要外联流量，阻断各种无关非法外联流量，防止终端被作为跳板入侵服务器 3）一体化部署，配置简单： ngaf具备l2-l7一体化安全防护功能，可以简化组网，简便管理，提高性价比；

本产品的品牌是深信服，型号是AF-1320，VPN是支持VPN，用户数限制是200用户，产品类型是中型企业级，并发连接数是300000（个），最大吞吐量是300Mb，NAT是支持NAT，OEM是不可OEM，质保是一年（年）