SANGFOR
深信服科技

深信服下一代应用防火墙

NGAF

Next Generation Application Firewall

Gartner 定义下一代防火墙

源引自：Gartner《Defining the Next-Generation Firewall》

防火墙必须演进

防火墙必须演进，才能够更主动地阻止新威胁(例如僵尸网络和定位攻击)。随着攻击变得越来越复杂，企业必须更新网络防火墙和入侵防御能力来保护业务系统。

不断变化的业务流程、企业部署的技术，以及威胁，正推动对网络安全性的新需求。不断增长的带宽需求和新应用架构(如Web2.0)，正在改变协议的使用方式和数据的传输方式。安全威胁将焦点集中在诱使用户安装可逃避安全设备及软件检测的有针对性的恶意执行程序上。在这种环境中，简单地强制要求在标准端口上使用合适的协议和阻止对未打补丁的服务器的探测，不再有足够的价值。

为了应对这些挑战，防火墙必须演进为被著名市场研究公司Gartner称之为“下一代防火墙(NextGenerationFirewall，简称NGFW)”的产品。如果防火墙厂商不进行这些改变的话，企业将要求通过降价来降低防火墙的成本并寻求其他安全解决方案来应对新的威胁环境。

什么是NGFW?

Gartner将网络防火墙定义为在不同信任级别的网络之间实时执行网络安全政策的联机控制。Gartner使用“下一代防火墙”这个术语来说明防火墙在应对业务流程使用IT的方式和威胁试图入侵业务系统的方式发生变化时应采取的必要的演进。

NGFW至少具有以下属性：

1．支持联机“bump-in-the-wire”配置，不中断网络运行。2．发挥网络传输流检查和网络安全政策执行平台的作用，至少具有以下特性：

（1）标准的第一代防火墙能力：包过滤、网络地址转换(NAT)、状态性协议检测、VPN等等。

（2）集成的而非仅仅共处一个位置的网络入侵检测：支持面向安全漏洞的特征码和面向威胁的特征码。IPS与防火墙的互动效果应当大于这两部分效果的总和。例如提供防火墙规则来阻止某个地址不断向IPS加载恶意传输流。这个例子说明，在NGFW中，应该由防火墙建立关联，而不是操作人员去跨控制台部署解决方案。集成具有高质量的IPS引擎和特征码，是NGFW的一个主要特征。

（3）应用意识和全栈可见性：识别应用和在应用层上执行独立于端口和协议，而不是根据纯端口、纯协议和纯服务的网络安全政策。例子包括允许使用Skype，但关闭Skype中的文件共享或始终阻止GoToMyPC。

（4）额外的防火墙智能：防火墙收集外来信息来做出更好的阻止决定或建立优化的阻止规则库。例子包括利用目录集成将阻止行为与用户身份绑在一起，或建立地址的黑白名单。

NGFW将成为大势所趋

目前，有一些已经将他们的产品升级为提供应用意识和一些NGFW特性的防火墙和IPS厂商，以及一些关注NGFW能力的新兴公司。随着防火墙和IPS更新周期的自然到来，或者随着带宽需求的增加和随着成功的攻击，促使更新防火墙，大企业将用NGFW替换已有的防火墙。Gartner认为不断变化的威胁环境，以及不断变化的业务和IT流程将促使网络安全经理在他们的下一个防火墙/IPS更新周期时寻找NGFW。NGFW厂商成功的关键将是以同样或略高于第一代防火墙的价格，提供包含第一代防火墙和IPS特性的NGFW。

目前仅有不到1%的Internet连接采用NGFW来保护。Gartner认为，到2014年底，这个比例将增加到占安装量的35%，60%新购买的防火墙将是NGFW。

媒体观点

防火墙必须演进么？

随着互联网的发展，网络安全威胁也在不断发生变化。传统基于网络层的安全威胁已经转变为以应用层攻击行为为主的安全威胁。

—— 摘自赛迪

对于通过常用的80端口和443端口来访问的互联网应用来说，基于端口的传统企业防火墙与其说像警卫，还不如说是应用的中转地，传统防火墙此时所起的安全作用正在减弱，它也逐步让位于功能强大的新一代高速智能防火墙。

—— 摘自网络世界

目前，防火墙仍是很多企业最重要的安全设备之一。但随着新型威胁造成的危害日益严重，传统防火墙越来越力不从心，下一代防火墙顺势而来。

—— 摘自TechTarget中国

显然，和其他网络设备一样，防火墙必须随需而变，升级到下一代防火墙，才能在变革的大潮中焕发新的生命力。

—— 摘自IT专家网

下一代的防火墙，这一概念必将为广大用户所接受并传播！

—— 摘自IT168

是时候用下一代防火墙了

下一代防火墙不但要能够检测并拦截复杂攻击，还要在应用层(包括端口和协议)执行细化安全策略，具备出色的可视化性能和控制能力，可以及时查看网络中应用程序和用户的相关信息以及整个企业网络的流量内容，并进行相应的控制。

——摘自IT专家网

传统防火墙能够很好地防范网络层攻击。但是，随着富媒体应用的爆炸性增长，以及Web 2.0应用快速向业务环境渗透，隐藏在应用层中的恶意威胁越来越多，用户要求下一代防火墙必须能够检测出隐藏在应用层数据流中的攻击。

——摘自比特网

是否能在性能和效率之间找到完美的平衡点，也成为衡量下一代防火墙产品的重要标志。

——摘自计世网

NGAF VS UTM?

不可否认，UTM由于具备2-7层的检测和控制能力，能够起到比较全面的防御作用。然而目前UTM却面临两个问题：一个问题是，对应用层检测的精度。

“对症下药”医学领域的一个原则，只有准确定位病情，才能适当下药以治疗。映射到网络安全上也是同样道理，应用层威胁的检测识别是进行控制防护的基础，是关键点和难点。与此同时，防御技术的发展，一些和UTM有类似功能的集成式的防火墙出现了。有一点已经引起了一些用户的注意：在现有防火墙基础上增加功能，肯定会影响到运行效率。若要解决这个问题，有硬件和软件两种解决方式：采用高性能的ASIC硬件平台或采用优化的软件体系架构和技术。

—— 摘自IT168

IDC分析师Charles Kolodgy创造了另一个术语UTM（统一威胁管理），很快便有了NGFW和UTM术语之争，Kolodgy说UTM和NGFW的含义大致相同，但Gartner却不这么认为，它指出UTM安全设备只适合中小型企业使用，而NGFW才适合员工大于1000的大型企业使用。

—— 摘自网络世界

需要马上升级到NGFW么？

目前仅有不到1%的Internet连接采用NGFW来保护。Gartner认为，到2014年底，这个比例将增加到占安装量的35%，60%新购买的防火墙将是NGFW。

—— GARTNER《Defining the Next-Generation Firewall》

安全威胁和IT流程总在不断变化，没有任何一款安全产品可以永久发挥作用。在更新换代到NGFW的步骤方面，我们比较认同Gartner的建议：无论用户现在使用的是防火墙、防火墙+IPS还是安全服务，都应在下一个更新周期来临时切换到NGFW。

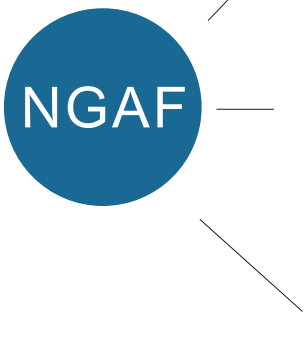
—— 摘自计算机世界

深信服下一代应用防火墙 NGAF

产品概述

深信服下一代应用防火墙（NGAF）是面向应用层设计，能精确识别用户、应用和内容，具备完整安全防护能力的高性能防火墙。

产品特点



1 基于内容的应用安全

有效识别用户、应用和内容：基于用户、应用和内容的策略配置更加清晰、完整，防止策略配置的疏漏。

应用内容的安全防护：基于业务内容进行防护，实现终端到应用的端到端深层次防护

2 可视化的业务安全

可视化安全策略：基于应用和用户，制定L2-L7一体化安全策略，易维护

可视化安全报表：提供服务器风险和终端风险报告以及应用流量报表

3 高性能的7层安全

全面的防护：融合了网络层安全、应用管控、应用防护多个功能，提高性价比，降低运维复杂度

单次解析架构：一次拆包一次解析，实现万兆性能，微秒级延迟，提升性能

产品优势

更精细的应用层安全：

- 贴近国内应用、持续更新的应用识别规则库
- 精确识别内外网超过650种应用、1000种动作（截止于2011年8月1日）
- 支持包括AD域、Radius在内的8种用户身份识别方式
- 面向用户与应用的可视化策略配置，减少复杂环境错误配置的风险

更全面的内容级安全防护：

- 基于攻击过程的服务器保护，支持防扫描、信息隐藏、弱口令保护、漏洞防护、防web攻击、防止网页挂马
- 强化的WEB应用安全，支持防SQL注入、OS注入、XSS攻击、URL权限控制
- 完整的终端内容防护，支持URL过滤、病毒防护、脚本/插件过滤、漏洞防护

更高性能的应用层处理能力：

- 单次解析架构实现了数据包的一次拆解、一次匹配，提升应用检测的效率
- 多核并行处理技术提升了应用层计算能力，真正实现万兆级应用安全

安全技术实力：

- 10年网络层安全技术积累、5年应用层安全技术积累
- 微软MAPP项目合作伙伴
- 北京、深圳设立攻防实验室

多种功能融合、纵深安全防御、一体化安全防护

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

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

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

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

包过滤与状态检测	提供静态的包过滤和动态包过滤功能
	能够防御DOS/DDOS、land,smurf,synflood,icmpflood等网络层攻击
	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
	内置VPN模块能实现VPN互联
	支持静态路由、RIP v1/2、OSPF、策略路由等多种路由协议

媒体眼中的深信服NGAF

深信服科技作为近年来崛起势头最为迅猛的本土信息安全解决方案提供商，深信服科技长期坚持专攻应用与内容安全领域的发展策略，在市场上有着广泛的认同度。就在NGFW 大潮在国内方兴未艾之际，该公司于近期发布了NGAF 系列下一代防火墙，成为首家推出NGFW 产品的国内厂商。

深信服NGAF 系列下一代防火墙提供了以传统基础网络安全、应用识别与控制、应用威胁防护为核心的多种安全功能，覆盖了NGFW定义中要求必备的所有特性。有国内市场上最成功的上网行为管理产品为基础，深信服科技的NGFW 产品在应用识别与控制能力方面显然有着先天优势。该公司还将WAF产品的主要功能集成到NGFW 产品中，结合应用识别与控制功能，为数据中心用户提供了新的安全防护接入思路。对于我们采访中问到的“之前没有防火墙/UTM 产品，在状态检测技术和入侵防御技术方面是否有足够积累”的问题，深信服科技市场行销部技术总监殷浩也没有回避。

据介绍，该公司在保持应用与内容安全领域技术领先的同时，也一直都在跟踪其他各类安全技术的发展。例如成为微软MAPP 计划合作伙伴，可以第一时间获得漏洞资料，提高IPS的防护效果和响应速度。NGFW产品的应用威胁防护功能将反恶意软件、漏洞利用、Web 入侵等威胁视为一个整体进行统一防护，正是技术积累的一次集中体现。产品规格方面，深信服科技的NGFW 产品线中包含了多达11 款产品，覆盖了几乎所有用户群体。其最低端AF-1100 系列产品标称提供200Mbps 的防火墙处理能力（按照深信服对产品的定义，应用识别与控制功能都默认开启，后同），最高端的AF-8000 系列则将该指标推向10Gbps。由于深信服科技NGAF 系列产品刚推出不久，我们还未能拿到更多的性能参数。但从厂商测试中得到的最新数据来看，其中端AF-1700 系列产品的防火墙吞吐量达到600Mbps；在此基础上开启IPS和WAF 功能，依然可以达到520Mbps 的处理能力。

摘自计算机世界