网康科技
NETENTSEC

为什么部署了防火墙仍遭攻击？

为什么网络安全管理如此之难？

我要不要即刻升级防火墙？

我应该选择什么样的产品？

.....

NGFW

十万个为什么

北京网康科技有限公司

问答索引

概念篇

1. 下一代防火墙到底是概念炒作还是技术定义？

答：下一代防火墙是一款为应对当今网络威胁而定义的新一代网络安全设备，由 Gartner 于 2009 年提出。顾名思义，下一代防火墙是传统防火墙（包括传统 UTM）的替代产品。更强的应用识别能力、主动防御未知威胁以及多种威胁检测手段一体化融合，是下一代防火墙区别传统网络安全设备最显著的特征。

2. 下一代防火墙相比传统防火墙的区别和优势是什么？

答：传统防火墙基于三、四层工作，无法有效控制应用，并且无法识别病毒、木马等应用层威胁，此外传统防火墙仅提供有限的日志、报表功能，操作起来技术门槛较高。下一代防火墙则完全基于应用层构建安全，融合多种安全功能，有效应对应用层威胁，同时具有较友好的可视化界面，提供智能的分析和建议能力。

3. 下一代防火墙和统一威胁管理（UTM）的区别是什么？

答：UTM 将各功能的简单叠加，开启安全功能后性能急剧衰减，此外提供的日志、报表均为割裂的，分析能力较差，能够提供给管理的支撑较少。下一代防火墙的性能衰减可控制在 50%左右，通过智能挖掘和关联分析，可以对网络中的未知威胁做到一定程度的提前预警，并且在安全事件发生后的溯源方面，日志的关联分析能力能够以最简单的方式了解攻击的全貌。

4. 为什么常用“亡羊补牢”和“按图索骥”来形容说传统防火墙、UTM 设备的防护模式？这种模式有什么技术缺陷？

答：亡羊补牢指，传统威胁防御基于代码特征，需要首先有人中病毒，

然后进行恶意代码报告，进而安全厂商捕获威胁研究其特征，最终更新至特征库服务器中实现防御，每次都是在攻击发生之后才开始真正研究攻击。按图索骥是指，传统安全设备总是在进行特征码的简单匹配，对于病毒、木马的变种无能为力。

性能篇

1. 网康 NGFW 采用什么硬件架构？

答：网康 NGFW 采用了 Intel SandyBridge 多核专用通讯平台，在网络转发、应用层处理、数据分析方面保持有较高的性能。

2. 网康 NGFW 如何保证应用高性能以及功能全开启后的高性能？

答：防火墙设备的性能主要由其硬件及软件架构所决定，尤其是软件的处理机制往往会极大的制约安全设备性能的发挥。网康 NGFW 全线产品均使用了高性能的多核处理器架构，该架构在应用层数据处理、流量数据分析以及数据转发方面的综合性能均表现优异，在软件方面采用单路径异构并行处理引擎，将多种安全功能融入了同一个检测引擎中，在进行数据包检测时仅需一次解码便可匹配全部威胁特征，与传统多功能防火墙（如 UTM）普遍采用的多安全引擎串行通过、依次检测的机制相比，减少了数据包的解码次数，大大提升了安全检测性能。此外，网康 NGFW 在业界首家采用了病毒云查杀技术，将较消耗性能的病毒查杀工作交由资源更加充足的云端完成，对于保证下一代防火墙的高处理性能也起到了关键作用。

3. 网康 NGFW 标称的吞吐量、并发会话、新建会话等性能参数为什么较低？

答：今后的网络安全是应用层安全，所有的流量都要进行应用层的深入分析，因此下一代防火墙已将深度包检测（DPI，用于应用识别及其它应用层安全功能）作为其架构中的基础部件，设备开机即处于启动状态，并且鼓励用户打开全部安全功能，因此对于下一代防火墙用户而言，真正有价值的参数是其应用层吞吐量以及开启全部安全功能后的吞吐量。网康全线产品目前标称的吞吐量参数均为应用层的吞吐

量，而当前市场上多数防火墙产品仍依照传统习惯标称其网络层吞吐量，由于要对数据包进行更加深入的检测，同一设备的应用层吞吐量一定会低于网络层吞吐量，因此不少用户会误认为下一代防火墙的性能比较低。

功能篇

1. 是否可简要概述网康 NGFW 的几大功能？

答：1）传统防火墙的全部功能，路由、NAT 等，换言之，下一代防火墙完全可以替代原有的传统防火墙；2）应用可视化，可基于应用层对网络中的人、应用、内容进行精细化的管控，同时通过可视化界面以人、应用、内容为维度呈现网路中的流量和行为；3）一体化威胁防护，将 IPS、AV、URL 过滤等功能融合在一个引擎中，在保证高性能的情况下实现了威胁的全面防护；4）数据防泄漏，可对 300 多种应用的文件传输、文件类型及 11 类文件的内容进行过滤，严防信息泄密；5）主动式防御，通过异常行为的分析，对于威胁特征库、病毒库无法识别到的未知威胁进行主动防御；6）高性能，通过软、硬件架构的技术创新实现了较高的应用层性能和安全功能全开启后的性能。

2. 网康 NGFW 有什么特点？和同类产品相比的主要优势在哪里？

答：网康 NGFW 是中国首款真正符合 Gartner 权威定义的下一代防火墙，具有超强的用户、应用和内容识别能力，拥有中国最大应用识别库以及全球最大中文网页分类库。此外病毒云查杀、僵尸主机预警以及一体化关联的设计等均是其相比同类产品独有的特性。值得强调的是，网康 NGFW 提供了便捷的管理操作、直观的异常输出呈现，其操作体验广受用户好评。

3. 为什么下一代防火墙需要融合应用识别技术？

答：应用识别之所以成为下一代防火墙的基础能力，主要出于几方面的原因。一是应用端口跳变、多种接入形式造成了端口不再等于应用、IP 也不再等于用户，要做到精细的访问控制，必须要基于应用层才能

实现。二是由于当今超过 75%的威胁均来自于应用层，要实现应用层威胁的有效应对，必须要基于应用层对数据包进行病毒、漏洞、间谍软件、恶意网址等的深度检测。此外，为了便于安全管理、提升安全防护能力，下一代防火墙应当具备的应用可视化、主动防御等能力也是在应用层上得以交付的。综上，以上的功能特性均需要精细的应用识别能力作为支撑。

4. 目前市场上几乎所有的防火墙都宣称支持应用识别和控制，网康在此方面的特点是什么？

答：网康 NGFW 内嵌中国最大的应用识别库，其支持识别的应用数量是同类产品的 3 倍，全部为中国大陆地区用户所常用的应用，并且对平台化应用的子功能具有深度识别能力。应用识别是下一代防火墙的核心技术，其不但是进行精准访问控制的前提条件，同时也有助于用户更加清晰的了解网络中的流量构成。此外，网康 NGFW 对所支持的 3100 余种应用均进行了安全特性研究，不但从用途、类型上进行了细致的分类，同时还基于“应用隧道”、“威胁利用”、“消耗带宽”、“文件传输”等安全属性进行了风险维度的分类，并分别为每一种应用赋予了从 1~5 不等的风险系数供管理者参考。

5. 网康 NGFW 的应用识别技术有什么技术特点？

答：首先，多数用户认为，所谓的应用识别技术只是识别应用，这是片面的，其实我们谈安全，应该关注三方面的内容，那就是人、应用和内容，因为安全管理就是要做到针对个体用户的管理，而管理的前提是了解流量类型，控制的核心目标则是对流量内容的过滤，所以说，要想提供完整的应用层安全，绝不仅仅是控制一些应用流量是否能够通过那么简单，我们不能忽视对于流量中用户和内容等信息的识别，只有具备用户、应用、内容的识别能力，才可以实现能够切实满足当今安全需求的多维度、细粒度访问控制。第二，之前大家评价应用识别能力，第一反应就是去比数字，看看谁的应用特征库更大，而我们

认为，今后的安全设备讲究的是深度应用控制，不但要看应用识别的广度(数量)，还不能忽视应用识别的深度，比如对于平台化应用的子功能的识别等，这些直接关系到安全管理的精细程度，而在此方面，网康无疑是业界的领先者，我们的应用识别库已经支持了 3100 多个互联网应用特征、700 多个移动应用，仅 QQ 一种应用，便支持识别其 10 余种子功能。除了广度和深度，还要充分考虑速度，对于新增应用的响应时间同样很重要，经过长时间的积累，网康目前对于绝大多数新应用识别均实现了自动化，具备了持续性高、速度快的应用特征生产能力。最后，我们还不能忽视应用有个最大的特点是地缘因素，为国内用户提供国外主流应用的控制是毫无意义的，所以还应关注应用与用户习惯的匹配度，网康的产品目前主要针对国内市场，因此我们内嵌了中国最大的应用识别库以及全球最大的中文网页分类库。

6. 为什么说网康 NGFW 提供了更完整的安全防护？

答：首先，网康 NGFW 提供了一体化的漏洞、恶意软件、病毒、恶意网址等防御，可全面对抗已成主流的应用层威胁。另外，得益于高性能的处理架构，以上所述所有安全功能同时开启后的性能衰减可控制在比较合理的范围内，用户可以切实的得到下一代安全技术的保护。

7. 网康 NGFW 的应用层一体化安全防护，具体包括那些？

答：网康 NGFW 通过业界领先的应用识别技术保证对网络数据中的人（用户）、应用、内容具有极强的洞察力，在此基础上运用一体化威胁检测引擎对流经其的恶意流量、非法流量进行甄别和拦截，具体包含以下几个方面：

1) 病毒防护：云端、本地双引擎可选，支持对 HTTP、FTP、SMTP、POP3 和 IMAP 协议流量，及 gzip，zip，rar 等压缩文件进行病毒查杀

2) 漏洞防护：6300 余种漏洞攻击防护

3) 间谍软件防护：8300 余种间谍软件防护

4) 网址过滤防护 :全球最大中文网页分类库 ,收录 3500 余万条 URL 分类信息，可对 URL 进行分类控制

5) 文件过滤：针对 300 余种应用的 66 类文件传输行为进行控制

6) 数据过滤：针对 300 余种应用的 11 类文件传输的内容进行过滤

7) 外发审计：QQ 上下线记录、邮件外发审计、论坛发帖审计

8. 网康 NGFW 如何应对流行的 DDoS 攻击？

答：网康 NGFW 支持防御洪水（Flood）攻击、扫描攻击、异常数据包攻击以及 ARP 攻击等共计 20 余类网络层攻击。对于 DDoS 攻击所惯用的 Flood 攻击，主要是通过限定同一源 IP 单位时间内的 SYN、UDP、ICMP、DNS 数据包流速来实现的。例如，设备默认同一源 IP 每秒钟发出的 SYN 包数量大于 10000 个（阀值可根据用户网络情况自定义），即判定为 SYN Flood 攻击。

9. 病毒云查杀的好处是什么？

答：云查杀的优势体现在三点：1）云端拥有最广泛的资源，网康病毒查杀云收录超过 80 亿的病毒文件样本，是传统本地查杀设备的数十倍；2）将病毒查杀的工作放至云端，可以有效降低设备本地的性能开销，因此使用云查杀后，网康设备的防病毒性能提升了 10 倍左右；3）云查杀可以有效规避传统本地查杀设备升级特征库时延的问题，对于最新发现的病毒、木马、恶意代码可做到 10~15 分钟内的快速响应。

10. 病毒云查杀要将数据送至云端检查，是否会消耗带宽并带来较长的响应延时？

答：所谓的病毒云查杀，并不是将全部流量镜像至云端，而是把流量进行摘要计算，仅将摘要值上传至云端进行比对，因此上传的数据量

很小，不会消耗大量带宽。经过反复测试，在一般链路质量下，病毒云查杀首次检查的延时大约为几十 ms，首次进行云端查询后，设备本地会对匹配到的病毒样本进行一定时间的缓存，进一步降低同类病毒再后续的检测时延。

11. 网康 NGFW 已经具备了病毒防护功能，是否可以取代安装在电脑上的桌面病毒查杀软件？

答：尽管网康 NGFW 采用的病毒云查杀技术具有极高的病毒识别率和快速的响应时间，但下一代防火墙仅对过往它的网络流量进行病毒查杀，在一个网络中，还有很多网络流量是直接通过二层交换设备进行转发的，例如在同一局域网内的流量多数情况并不通过网关设备转发和检查；另一方面，经验告诉我们，还有很多病毒是通过 U 盘等传统媒介进行传播的，对于此类病毒下一代防火墙也无法进行检查。因此，从安全角度考虑，我们仍强烈建议用户不要忽视桌面级病毒查杀的重要性，我们认为，目前业界任何网关级防病毒产品都不能取代桌面级病毒查杀工具。

12. 网康 NGFW 是否可以替代单一功能的入侵防御（IPS）、防毒墙（AV）等设备？

答：新兴网络威胁的一大特点是手段多样，黑客为了实现攻击的目标，会持续采用不同的攻击方法尝试侵入网络并造成危害，因此传统基于单点技术的防范（例如部署单独的防火墙、入侵检测、防毒墙等设备）已经不再适用。下一代防火墙采用一体化威胁查杀引擎，将入侵防御、病毒防护等安全功能融入其中，并建议用户同时开启，因此，一般而言，下一代防火墙完全可以替换企业网中现有的入侵防御、防毒墙设备。相比独立的入侵防御设备而言，网康 NGFW 提供了对 6300 余种漏洞和 4000 余种间谍软件的识别和阻断能力，并且通过深度解码技术确保高检出率和零逃逸。此外，基于智能的可视分析技术，网康 NGFW 还提供了主动防御能力，对于 IPS 威胁特征库未识别的攻击，

可基于其可疑的行为特征进行快速告警，是对 IPS 特征匹配技术的有力补充。在病毒防护方面，网康下一代防火墙首创将病毒云查杀技术运用于防火墙设备，相比采用本地查杀技术的防毒墙，其病毒样本识别数量、病毒查杀效率以及新病毒响应速度均有了 10 倍左右的提升。多种功能融合已是边界安全设备的大势所趋，这样的产品设计有助于安全功能间的联动并降低用户投入、管理成本，以下一代防火墙为代表的此类产品已经在市场上赢得了广大用户的青睐。

13. 是否能举个例子说明什么是主动防御？网康 NGFW 是如何来实现的？

答：关于主动防御，可以举出不少生活实例。例如，在现实社会中，传统的安保措施主要是通过人的面部特征与数据库的照片进行比对实现，但无法规避嫌疑人乔装打扮或其信息在数据库中并未收录的问题，主动防御技术则通过关联分析某人的行为特征以确定其是否有作案嫌疑；又如，在我们日常使用电脑的过程中，若安装来源不明的应用程序，类似于 360 等的桌面安全软件经常会跳窗报出异常，提醒用户该应用正试图修改注册表、启动项等系统信息，其实也是在通过分析其异常行为以判别该应用是否有安全威胁。总而言之，主动防御技术的核心是通过异常行为分析判别、定位威胁，该技术是对现有代码特征比对技术的有益补充，应对未知威胁尤为有效。

网康 NGFW 已经具备了不少通过行为分析进行主动防御的特性。例如，基线对比功能就是在流量趋势统计的基础上，对比出某应用、IP 在一段时间内的同一时间点上所占用资源的变化幅度，并将全网范围内增大、减小、新增、消失的流量以基线的形式进行排名，这对于网络管理者及时发现有可能存在的问题则更有帮助，(例：例如某 IP 地址在今天之前的每天中午 12 点时所占用的带宽均为 1Mbps，但今天中午 12 点时的带宽占用却突然增加到了 5Mbps，尽管我们还不清楚流量增加的具体原因，但管理者却可以在第一时间注意到该 IP

的行为特征发生了变化，进而利用设备更加深入的挖掘具体信息）。又如，网康 NGFW 可根据僵尸主机的常见行为特征，通过大数据挖掘以判别网络中可疑的僵尸行为，当网络中发现异常的 IRC 流量或僵尸网络指令传输时，有可能是僵尸主机正在通过隐蔽通道与僵尸网络通信，当僵尸主机频繁访问恶意网址、动态域名、执行扫描探查或 DDoS 攻击，则有可能僵尸主机已经开始了攻击。对于这样的情况，设备可以自动的将可疑用户、IP 在日志界面中呈现出来，并根据对特征的符合程度提供“置信值”，帮助管理者分析并加以干预。

14. 网康 NGFW 对于僵尸主机是如何防御的？

答：僵尸主机的受控和攻击过程均极为隐蔽，依靠传统的代码特征匹配技术已不能有效防护。网康 NGFW 具备僵尸主机行为模型的建立和分析能力，首先对全网行为数据进行收集，在此基础上执行行为模型的大数据挖掘，根据僵尸主机常见的行为特征，发现网络内的可疑主机。例如，若某主机发出异常的 IRC 流量、或僵尸网络指令传输，则有可能是该主机正在通过隐蔽通道与僵尸网络通信，若某主机频繁访问恶意网址、动态域名、执行扫描探查或 DDoS 攻击，则有可能该主机已经受控开始进行攻击。对于上述情况，设备可以自动的将可疑的用户、IP 在僵尸网络日志中告警，由管理者进行人工分析和干预。

此外，网康 NGFW 对的应用控制、文件传输控制、病毒防护、间谍软件防护等，能够极大的降低僵尸程序植入的风险。

15. 网康 NGFW 是否可以进行内容传输控制？能够做到什么程度？

答：网康 NGFW 具备数据防泄漏（DLP）功能，能够针对 300 多种具有文件传输功能的应用进行传输行为的控制，例如可以对 66 种文件类型进行控制，并对.csv/.docx/.pptx/.xlsx/.txt/等 10 余种文件内容的过滤。网康 NGFW 在对文件进行甄别时，完全基于文件自身的

属性，而非传统的文件扩展名识别技术，大大降低了通过修改文件名绕过检测的风险。此外，为了防止信息通过其它方式泄漏，网康 NGFW 还支持对邮件外发和论坛发帖的内容进行控制和审计。

16. 网康 NGFW 一再强调的全网可视化、数据钻取、关联分析的好处分别是什么？

答：全网可视化可以帮助管理员掌握全网动态，更好的进行安全管理的调整。数据钻取可以方便管理员查看某一连接的详情，以更加简单的方式帮助管理员进行现状、趋势和事件的分析。日志关联的好处是将各个安全模块输出的异常信息结合在了一起，一个连接进入防火墙直到判定为威胁的全过程都清晰可见，帮助用户在安全事件溯源时以更短的事件看到整个威胁的全貌。

17. 网康 NGFW 能够提供哪些类型的日志？

答：网康 NGFW 能够记录流量日志、威胁日志、网址过滤日志、数据过滤日志、用户上下线日志、配置日志、系统日志、告警日志等共计 11 类日志。值得强调的是，所有与安全事件相关的日志均被记录在“威胁日志”中，威胁日志提供了与流量日志、网址过滤日志、数据过滤日志等的关联，可帮助管理员在极短的时间内进行安全事件溯源，了解整个攻击过程的全貌。

18. 网康 NGFW 支持什么类型的 VPN？分别适用于哪些场景？

答：网康 NGFW 支持三种类型的 VPN，分别为 IPSec VPN、SSL VPN、L2tp Over IPSec VPN。IPSec VPN 属于站到站的 VPN 连接，要求站点两端均部署具有 VPN 功能的设备，普遍用于机构间的互联，如总部与分支机构间的 VPN 组网。SSL VPN 适用于移动办公用户的安全远程接入，如在外出差的员工使用 Windows 系统的笔记本电脑从任意第三方网络接入企业内网访问资源。L2tp Over IPsec VPN 主要

用于非 Windows 系统终端的安全远程接入，例如 Android、IOS、Linux 等系统的终端从任意第三方网络接入企业内网访问资源。SSL VPN 和 L2tp Over IPSec VPN 仅需要在机构总部或数据中心一侧部署设备即可。

19. 网康 NGFW 的 VPN 兼容性如何？是否可以与其它品牌的设备协商、互联？

答：网康 NGFW 采用标准的 IPSec 协议，支持 3DES、AES、MD5、SHA 等国际通用的加密、认证算法，因此可与所有支持标准 IPSec 协议的设备协商互联。需要注意的是，IPSec VPN 的配置步骤较为繁琐，不同厂商设备在配置方法上存在差异。

售后篇

1. 网康 NGFW 服务到期后安全功能是否可以继续使用？

答：为保障用户安全投资的合理性，帮助更多用户的网络迅速处于下一代防火墙的保护之下，网康科技为用户提供了“服务”、“设备”两种订购模式。“服务”模式服务期终止后，设备硬件平台不回收，但病毒防护、入侵防御、URL 过滤、SSL VPN 功能失效，仅保留基本防火墙功能。“设备”模式服务期终止后，设备所有功能可继续使用。另外，以上两种订购模式在服务期终止后，软件版本、病毒特征库、IPS 特征库、URL 分类库、应用识别库均停止升级。

网康官方微博：

网康官方微信：

北京网康科技有限公司
地址： 北京市海淀区中关村东路 66 号世纪科贸大厦 A 座 3 层
邮编： 100190
电话： 010-62670909
传真： 010-62670958
www.netentsec.com

欢迎访问 www.netentsec.com/ngfwwhy 提交您所关心的产品问题