下一代网络安全将如何应对？

——下一代防火墙产品公开比较测试计划

以高级持续性威胁（Advanced Persistent Threat，APT）攻击为代表的下一代网络威胁形式正呈现出飞速增长的态势。并对用户的网络应用安全产生了极其恶劣的影响。而传统的网络安全产品在对此类攻击的防护方面，基本上是形同虚设。目前绝大部分安全厂商把对下一代网络威胁安全防护的希望都寄托在了下一代防火墙这种可以基于网络应用及应用威胁进行防护的安全产品之上。然而目前对下一代防火墙产品的有效评估手段还十分匮乏。很难对不同厂商的相关产品进行综合性的评价、对比。初步分析有如下原因：

首先，在评测项目上，当前防火墙产品或多或少均加入了网络应用协议和文件内容分析功能，而在功能上尚未统一，自然在测试方法上，无法形成统一的评估测试方案。

其次，在产品性能测试指标评定上，缺乏统一的规范。引发厂商在选送产品时，无顾实际应用需求，竞相选送高端产品现象出现。

第三，单一的测试方案无法对厂商产品技术、服务能力进行综合评价。

第四，厂商产品性能及功能特性指标不公开，导致重复性测试工作增加。

因此导致用户在产品选型时会有无所适从的情况出现。有鉴于此，《网络世界》评测实验室准备进行一次“下一代防火墙产品公开比较测试”活动。期望通过本次活动，可以和众多网络安全厂商一起，对下一代防火墙产品的测试项目、测试方法、测试指标以及测试指标的评定方式进行一次深入的沟通。并组织整理出一套切实可以的测试方案，为日后用户选型测试提供切实可行的参考依据。

下一代防火墙产品公开比较测试方案

《网络世界》评测实验室准备与厂商沟通下一代防火墙产品公开比较测试方案如下：

基本性能测试

下一代防火墙产品基本性能指标，是用户选择下一代防火墙产品时重要的选型依据。但由于缺少统一的基本性能测试规范，使得某厂商有漏洞可钻，致使产品基本性能测试数据与实际应用处理性能脱节。为此用户只能被迫在选型时，提升被测设备的指标要求，以满足正常网络业务应用处理的需求。这也导致了低端网络应用环境，选择高端网络应用产品的无奈现象出现。

而下一代防火墙产品的基本性能应当如何评定，各个网络厂商所依照的标准并不统一，因此在本次公开比较测试中，将与各下一代防火墙厂商进行沟通，对下一代防火墙产品基本性能测试的项目、方法、指标及指标的评定方式进行明确。

现在，《网络世界》评测实验室将下一代防火墙产品基本性能测试的测试方法、测试项目、指标总结如下：

下一代防火墙产品基本性能测试分别在网络性及应用层下进行。

网络层基本性能测试指标

在网络层测试中，将依据 RFC 2544 规定的吞吐量、丢包率（二者可选一）、时延的测试方法对下一代防火墙产品吞吐量、数据包转发速率（pps）、数据包转发流量（bps）、时延（ms）分别进行测试。

网络层基本性能测试指标评价

一、吞吐量

对产品分别开启防火墙、NAT、路由（静态）、透明模式下的吞吐量进行测试。

在当前的下一代防火墙产品测试中，有些厂商过于注重小包数据转发性能和丢包情况。而现如今的网络环境中，正常小包数据应用所占比例极小，追求过高的小包数据转发性能本身会对整体网络带宽及产品硬件成本造成影响。

无论是在数据中心，还是在网关接入的正常网络应用场景中，都不会产生出很多的小字节数据包流量，基本上只有在网络连接建立、结束或数据包重传时才会出现。同样也很少有网络应用程序会生成大量的小字节数据包分片。在实际网络应用场景中，64 字节的小数据包所占的网络流量比例，几乎连 1%还不到，尤其是在网络连接带宽高、网络时延小的高质量网络中，这个比例还会再度减少。而小数据包转发时，对网络设备的转发性能还会有更高的要求，64 字节小包的转发速率是 1518 大包转发速率的 23 倍，当小字节数据包转发性能过高时，会极大减少网络应用的实际可用带宽。为了这并不常用的“1%”而成倍的牺牲网络带宽，或造成更高的网络硬件成本投入，这种牺牲已经不符合当前网络的实际业务应用需求。

因此，在小包吞吐量的指标评价时，在 64（IPv4）、78（IPv6）字节小包时的处理性能应当处何去正确评估，是本次公开比较测试的一个重点，需要与各个厂商进行沟通，找到一个合理的评估指标项线出来。

二、时延

对产品分别开启防火墙、NAT、路由（静态）、透明模式下的时延进行测试。

虽然目前尚未收到因网络设备时延影响网络业务运行的案例，但网络时延依然是一个十分重要的网络产品性能测试指标。《网络世界》评测实验室建议在时延测试时，可以对最大吞吐量无丢包情况下，对下一代防火墙产品时延性能进行统一测试。

三、数据包转发速率

对产品防火墙、NAT、路由（静态）、透明模式下的数据包转发速率进行统计。

对数据包转发速率结果的指标分析可以参照小包吞吐量，主要是考查下一代防火墙产品的数据包转发能力。

四、数据包转发流量

对产品防火墙、NAT、路由（静态）、透明模式下的数据包转发速率进行统计。

统计在不同包长下数据包转发流量，以数据包转发速率×数据包长进行计算，主要是为直观了解下一代防火墙产品在网络层的转发性能。（建议以 64、512、1518 三种不同数据包长流量分别进行统计）

应用层基本性能测试指标

当前下一代防火墙产品基本上均具备了对 4~7 层网络流量进行分析、管理、控制的功能。因此需要对其应用层的处理性能进行测试。测试通常参照 RFC 3511 标准，对下一代防火墙产品在 HTTP 协议下，每秒新建连接数进行检测。

一、应用层新建连接处理速率（每秒新建连接数）

对产品分别开启 IPS、AV（防病毒）、URL 管理功能的新建连接处理速率进行测试。

在上次下一代防火墙公开比较测试（解惑下一代防火墙）中，对新建连接处理速率的指标做了一定分析。同时也指出了过高的新建连接处理性能并不是下一代防火墙产品网络处理能力的正确性能体现。

由于新建连接处理性能与下一代防火墙产品的 CPU 处理能力有很大关联，因此在测试时，有必要对设备的 CPU 占用情况同步进行统计。

二、并发连接用户数

对产品分别开启 IPS、AV（防病毒）、URL 管理功能的并发连接用户数进行测试。

这个测试指标在上次同样也简单进行了分析，在这里需要强调说明的是网络设备对并发连接的承载能力有限，过高的并发连接性能对网络应用来讲非福是祸。一个 32 位的服务器在运行简单业务时（最简单静态 Web 服务），可以支持的并发连接用户不超过 10 万，如要处理复杂业务，此性能指标还会急剧减低。客户端所能承载的并发连接性能更差，因此需要制订一个合理的每 Mbps 带宽并发连接用户数用户指导意见。

（建议在 90%新建连接处理情况下，对产品并发连接用户数进行测试，这也是 NSSLab 所采用的测试方案）

三、网络应用流量

对产品分别开启 IPS、AV（防病毒）、URL 管理功能的网络应用流量进行测试。

同样是一个老的应用性能指标，在这里我们还是建议采用 32KByte、64KByte 以及 1024KByte 大小的网页文件对网络应用流量进行测试。

产品功能测试

在产品功能测试中，最理想的状况是对产品的每项功能的基本网络性能均进行测试。然而，做为第三方评测实验室对如此众多厂商、不同的产品型号、不同的产品功能来讲，这个任务几乎是无法完成的。因此，在测试中将选择常见、有代表性的功能进行对比并对有创新、突破性的功能进行评估分析。测试方法如下：

《网络世界》评测实验室将依据已知应用、已知威胁、未知威胁、发生威胁四个方面进行归类，对功能进行对比。

测试方法：通过查看被测产品管理控制平台，对产品功能性进行简单确认。将对以下产品功能项进行功能性查看：

已知应用管理

对下一代防火墙产品对已知应用处理能力进行分析。按如下细项进行功能性查看：

一、网络功能

查看产品可支持的路由种类、是否支持 NAT 等

二、管理策略

查看产品管理策略（基于端口、Mac、IP、用户、用户组的策略管理）。、

[注：在有些产品中第（5）项及以下的功能均可在管理策略中进行灵活设置]

三、身份认证

四、VPN

五、流量管理

查看产品流量管理分析能力（应用流量的识别、管理、控制）

六、协议分析

查看产品网络应用协议分析能力。

七、URL 管理

需要了解产品对已知 URL 的分类、库表大小、更新频率。

已知威胁防护

一、防火墙

主要了解网络层功能防护处理功能

二、IPS

需要对攻击防护种类、更新频率进行统计

三、防病毒

需要了解病毒库大小、更新频率

四、URL 防护

需要了解 URL 防护库大小、更新频率

五、网络应用防护

库表大小、更新频率

未知威胁防护

一、未知应用统计

查看产品对未知应用的统计分析能力（可否按源 IP、目的 IP、用户、地域对未知应用进行统计）

二、主动威胁防护

查看产品针对未知威胁的分析处理能力

发生威胁管理

一、阻断

查看产品威胁阻断能力

二、报警

查看产品报警分级

三、日志

查看产品日志记录能力

产品功能确认性测试

仅依靠功能性对比，无法对下一代防火墙产品的实际处理能力进行评估。因此还需要对下一代防火墙产品的功能进行确认性测试。

目前计划对下一代防火墙产品的带宽管理、应用过滤、流量统计、IPS、防病毒功能进行确认测试，具体测试方法及其他测试项目将与厂商进一步沟通后再进行确定。

带宽管理

对不同用户、不同应用协议设置不同带宽流量限制后，发流量进行验证。

应用过滤

设置应用过滤规则后，发流量验证

IPS

利用测试仪表发出不同类型攻击，测试产品入侵防御能力。或采用抓包回放的方式，发送攻击报文，进行测试。

防病毒

利用测试仪表进行应用层流量测试同时加入 Eicar 病毒验证代码，进行防病毒功能验证。

应用性能验证

除了上述测试外，还需要对下一代防火墙产品的综合处理能力进行测试。这里计划对产品在不同应用协议的混合流量处理性能进行测试。将分别对产品的综合处理能力、应用分析、阻断能力进行验证。

综合处理能力

采用 IXIA BPS 测试仪表，模拟出 HTTP、MMS、P2P、IM 的多种协议混合流量后，测试产品在混合流量下的网络应用流量处理能力。

应用分析

测试产品混合流量的应用分析能力

阻断能力

对混合流量中 P2P 协议进行阻断后，测试产品阻断能力是否有效。

下一代网络安全厂商公开比较方案

选择一款产品尤其是网络安全产品，不能仅仅依靠一些有限的功能或性能测试指标。还需要对厂商的研发技术能力、技术服务支持等多方面进行全面了解。而目前在有些厂商中，还尚存在着产品型号、功能特性、性能指标不透明的现象存在。极大影响了用户对网络安全产品的正常选择。

因此，《网络世界》评测实验室将以第三方中立角度，对厂商从产品受众（覆盖范围）、产品技术、技术研发、技术支持四方面进行综合性点评。

点评结果将随后在“网界网”评测评道中新建一个产品专区中进行发布，并定时进行更新。

公开比较内容如下：

产品受众：

通过厂商发布产品信息，对其下一代防火墙产品的适用性进行分析，按以下受众进行分类评价：

SOHO 及个人用户（10 用户以内）

中小企业应用（10-500 用户）

大中企业应用（500-10000 用户）

电信及行业应用（10000 用户以上）

全方位覆盖（从个人用户到电信及行业用户）

产品技术：

通过下一代防火墙产品公开比较测试方案中各测试项对厂商产品功能、性能及适用性进行测试分析评价：

产品功能

产品性能

产品适用性

技术研发

通过厂商公开发布的技术研发相关信息对其技术研发实验进行分析评价：

研发技术投入/每年

研发规模

技术更新频率

技术支持

通过厂商可承诺的技术支持方式对厂商技术支持能力进行分析评价：
产品定时升级
间接性技术支持服务
24 小时内技术支持响应
专业人员企业常驻
7×24 小时专业人员技术支持

通过以上产品受众、产品技术、技术研发、技术支持的评价，《网络世界》评测实验室将对各网络安全厂商进行综合打分并实时进行公布。