下一代防火墙分析指南

下一代防火墙分析指南

随着技术的进步，第一代防火墙已基本无法探测到利用僵尸网络作为传输方法的威胁。由于采用的是基于服务的架构与 Web2.0 使用的普及，更多的通讯量都只是通过少数几个端口及采用有限的几个协议进行，这也就意味着基于端口/协议类安全策略的关联性与效率都越来越低。2012 年伊始，NGFW（Next generation firewall）即下一代防火墙已经成为业界的热点声音。本技术手册将为你介绍其趋势、特色和相关产品。

下一代防火墙之趋势

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。Gartner 认为下一代防火墙是防火墙行业的未来。

- 魔术象限：部署下一代防火墙的时机到了
- 下一代防火墙何时会替换现有防火墙？
- 取代 UTM？下一代防火墙势不可挡
- 魔力象限：下一代防火墙将成为主流（一）
- 魔力象限：下一代防火墙将成为主流（二）

下一代防火墙之特色

下一代防火墙，也称为感知应用程序的防火墙，通常也具备有状态防火墙传统的端口和协议分析功能，但是它们还能够根据产生网络数据包的应用程序进行流量检测。下一代防火墙有独立的基于应用程序的策略。

- 网络安全呼唤下一代防火墙技术：特点与选择
- 下一代防火墙管理设备：更智能，也更复杂！（一）
- 下一代防火墙管理设备：更智能，也更复杂！（二）

下一代防火墙之产品

许多防火墙供应商现在已经有强大的企业级下一代防火墙产品。各个供应商相互争论，认为的产品是最好的，但防火墙用户必须自己评估这些产品，寻找最适合他们环境的产品。

- 下一代防火墙供应商对比
- 分支机构的下一代防火墙：Palo Alto & SonicWall
- Cisco 最新网络安全架构与下一代防火墙

魔术象限：部署下一代防火墙的时机到了

下一代防火墙——比端口扫描更深入的能识别应用的智能防火墙。关于这种说法，你应该有所耳闻了。虽然大多数供应商已经推迟了防火墙的发布，但是 Gartner 的魔术象限报告认为市场风向正在转变，曾经沉睡的市场开始复苏。

根据 Gartner Inc. 研究副总裁 Greg Young 的观点，现在的防火墙供应商面临的越来越大的压力不再只是来自于一个专注智能防火墙的新兴集成商 Palo Alto Networks。因此，他将公司定位为 2010 年魔术象限中网络防火墙的领导者。

那些仍然在吃老本的供应商现在发现他们的客户群已经被第二市场竞争对手所抢夺，这些公司专注于入侵防御系统 (IPS)和防火墙策略管理——这是网络安全人员无法从现有防火墙供应商处获得的技术和功能，Young 说道。

“用户需求现在已超出供应商研发水平几年了，”他说。“存在的共同问题是创新不足…… 客户一直在说，‘快点！我们急需这个功能！’而防火墙供应商太过于关注对手而不是[创新]。”

根据 Palo Alto 产品销售主管 Chris King 的观点，在企业中使用 Web 2.0 应用和社交网络 ——以及针对这些应用的安全威胁——已经转变了传统的防火墙概念。Palo Alto 在今年发布了它的第一个魔术象限产品，它被称为是主导了一场“迫使市场领导者应对的市场破坏。”

“防火墙的原始设计是，‘如果我能控制端口，我就能控制应用，’”King 说。“但现实情况是，每一个应用都能使用任何端口，而现在端口控制基本上没有意义了。如果您关掉 80 端口，那么您就关闭了您的业务 …… [所以]防火墙的确必须更智能。”

期望今天出现更真实的下一代防火墙

网络人员可以期望在今年看到更好的智能防火墙产品，Young 说。这意味着：

没有单独的 IPS —— 一个真正的下一代防火墙除了基本的防火墙功能，还将拥有“整合的高质量 IPS”，而不是将 IPS 作为一个单独的设备。

智能决策 —— 一个智能防火墙将以“将信息集中到防火墙中以便执行更佳决策”的方式工作，Young 说。“例如，如果一个 IP 地址只传输恶意软件 …… 那么为什么防火墙还要接收这个只发送攻击的位置的流量呢？”

不只是端口控制 —— 以前的防火墙是基于目标地址、IP 地址和端口号来应用策略的。下一代防火墙将分析每个 HTTP 和 HTTPS 请求，Young 说。

进入 7 层协议 —— 一个智能防火墙将在应用层评估流量，他说。“不仅仅是接管它们，还要能够标识应用：它是 Webmail？还是 P2P？还是 Salesforce.com？然后可以对应应用策略，而且还不仅仅是阻挡/允许两种操作。”

“防火墙市场的确需要苏醒，”Young 说。“当我看到围绕 IPS 这些市场增长成十亿级时，当我每天听到企业无法在供应商的解决方案找到他们需要的产品时……我认为情况要发生变化了。而我们最终也开始看到一些高质量的下一代防火墙产品的出现。”

发展智能防火墙的一些障碍

虽然他们不会无动于衷，但是现在的供应商想要改变并不是简单的事，他们已经在用户培训、支持团队和渠道伙伴方面投入很长的时间和很多的资金。可以肯定的是，魔术象限将唤醒大大小小在企业智能防火墙产品中碌碌无为的防火墙厂商 —— 包括 Check Point Software Technologies、Cisco Systems、Fortinet 等等。

“当您谈论防火墙分类流量的方法时，这就是关键。这是防火墙的灵魂，”King 说。“要改变它——就像洗脑一样。”

IT 部门也需要改变，Young 说。即使他们相信防火墙方面还没有令人信服的下一代防火墙网络，然而继续不断地改进而不是等待“老旧的防火墙退市”是更保险的做法，他说。

Ed Garcia 是位于 San Francisco 公共关系机构 Horn Group 的 IT 主管，他期望在明年更换新的防火墙，他坚持 SonicWALL 的“完美的” PRO 系列产品已经很多年了，但是他热切期盼更容易管理的下一代防火墙。

“我对有更多智能功能的防火墙感兴趣，但是[它们必须]能够[在]成本、性能和可用性上实现平衡，”Garcia 说。“较小的公司无法在所有位置都安排 IT 专家，所以我们通常都是多面手。我们需要能够[自己]实地工作的系统——只需要最少的管理。”

“这就是更加智能的体现，也是能够帮助现有的正在使用的安全系统的方面，”他补充说。“它的确不是[要]替换其它系统，但是新产品将获得更大的价值。”

智能防火墙产品出现

根据 Juniper 的高端安全系统业务部门的高级产品销售经理 Don Meyer 的介绍，Juniper Networks 在市场上长期处于领先位置，在六年前就开始听到许多关于下一代防火墙的讨论，并因此研发了一个综合的 IPS。

“现在[企业]有着更多的要求。的确，我们能够过滤掉一些威胁，但实际上，我们想要在网关上实现更多智能，”Meyer 说。“使用通用端口和协议的应用真的正在飞速增长。”

在 2008 年 9 月，Juniper 提出了它的 SRX 系列产品——一组共八个分部和数据中心网关实现大量的综合特性，运行在它的 Junos 操作系统上。抛弃它的原有平台 ScreenOS 是它向下一代防火墙迈出的一大步，Young 和 flawless 的共同创建人 John Pescatore 指出。

ScreenOS 是针对防火墙创建的，所以设计上并不支持更多功能的整合，Meyer 说。Junos 使用多线程切换不同的原生应用，如在 2009 年末发布的 AppSecure 服务套件，以将动态和更细粒度的策略附加到不同的网站应用、用户组、一天的不同时间和其它参数上，他说。

“当然，不是每个人都需要这么强大的产品，”Young 说。“您必须知道，‘IT 对于我的业务有多重要？’而[这个问题的回答]对于每一个人都是不一样的。可以肯定的是，对于一个在线娱乐公司和一个制造公司—— 将得到非常不同的答复。”

（来源：TechTarget 中国　作者：Jessica Scarpati　译者：曾少宁 陈柳）

下一代防火墙何时会替换现有防火墙？

虽然网络工程师和分析师十分钟爱下一代防火墙，或称应用感知防火墙，但是技术仍在发展中。所以许多企业都保留着原有的防火墙和协议，至少到现在为止是这样的。

网络系统工程师 Mike Wade，是 Palo Alto Networks 最早的下一代防火墙使用者，他在 Summa Health（俄亥俄州医院与医学中心）系统的网络周边就部署了应用感知防火墙。Palo Alto 的防火墙位于网络 DMZ 的外围。然而，他的网站中仍然有传统的状态防火墙，如 Cisco ASA 5500s，就位于 DMZ 的内侧。这两个防火墙就这样背靠背地部署在他的主数据中心和次级"hot site"数据中心当中。

DMZ 两侧不同类型的防火墙服务于不同的需求，Wade 说。“DMZ 两侧的具体需求总是不一样的，”他说。“外侧的防火墙会受到不断的攻击，而内侧的防火墙只限于去处理路由至防火墙的一些流量而已。”

Palo Alto 防火墙可以扫描攻击数据中心的应用程序，而 Cisco ASA 可以检查端口和协议。分层防火墙的使用是安全策略的一部分，可划分职责，Wade 说。他现在就负责 DMZ 外围及周边的设备，同时还有一个单独的网络小组负责 DMZ 内侧的 ASA。

“如果有人能够破解我的密码或其他安全信息，那么攻击者到达二级防火墙时，需要面对复杂的个人化（内部网络管理人员）信息以及完全不同的其他设备，”Wade 说。“我们的设想是在如此机关重重的情况下，攻击者就不得不选择放弃。”

尽管最近一段时间应用感知防火墙被炒作的很厉害，但是至少在接下来的几年内，状态端口和协议防火墙仍会在大多数网络中博得一席之地。

状态防火墙在网络演进的十字路口

过去的 15 年当中，在网络安全领域，状态防火墙一直是处于第一道防线上。就像是嗅探端口和协议的交警，在网络工程师等制定的成千上万条规则的基础上为流量采取最恰当的措施。

但是网络不断变化的本质已经抛弃了这种陈旧的防火墙架构。网站上可以运行无数单独的应用程序——比如聊天、视频、文件传输，甚至是类似于 Salesforce.com 这样的企业应用程序。因为这些应用程序都需要在 Web 上运行，所以传统防火墙将其视为 HTTP 或 HTTPS 以及 Port 80 或 Port 443。黑客之所以把这些端口当做攻击目标是因为这些流量对于防火墙来说是不可见的，并且看起来类似于合法的 Web 流量。

传统防火墙的劣势带来了纷繁的网络世界，继而出现了多种多样的网络安全应用程序和软件。网络工程人员部署了许多产品来填补这个技术与市场的空白，这些产品的覆盖范围可以从入侵检测与防御系统(IDS/IPS)和杀毒软件到 Web 过滤和内容过滤产品等。

下一代防火墙的新品牌，或称应用感知防火墙的新品牌，它们更多地注重 OSI 模型中的应用层而不是端口和协议，目的在于实现基于策略的应用访问。几乎市场上的每一个防火墙供应商（除了 Cisco 之外）都有了自己的下一代防火墙产品。根据不同供应商对下一代防火墙的不同理解，其应用程序也都不尽相同。有些厂商的产品只可以识别到是来自 Facebook 的流量，而其他的一些产品则可以更加深入，它们可以把流量从 Facebook video，Facebook 聊天或简单的 Facebook 状态更新中区分出来。

供应商的发展是存在差异的。从最初开始，Palo Alto 公司就已经做应用感知防火墙了。竞争对手，比如 Sonicwall 和 Fortinet，都选择了把现有的 IPS/IDS 技术加入到防火墙平台中，实现应用感知。Mike Rothman 是 Securosis 的分析师兼安全研究总裁，说道：IPS/IDS 方法只是演化至应用感知防火墙的第一个阶段，到最后，采用这种方法的供应商往往都会再次修改防火墙配置，也会从根本上重新修改产品功能。在某种程度上这归根于 IDS/IPS 产品是由恶意应用程序签名所推动的，而下一代防火墙是通过挑选出这些特殊的网站和应用程序来实现应用感知的。

“把它想象成为一个主动与被动的安全模式，” Rothman 说。“如果你把他当做 IPS/IDS 附加模式，你就需要配置各种策略和规则来寻找不同的恶意程序。这样就显得过于复杂而且还要配置许多不必要的处理设备。如果在一个主动安全模式内，你就可以说‘这是我允许的应用程序和功能。’”

但是根据 Nemertes Research 高级副总裁兼合伙人 Andreas Antonopoulos 的看法是：应用感知防火墙的处理器本质就是强制企业对防火墙做多层部署。

“如果想在细分的内部 VLAN，MPLS 以及管理虚拟服务器时实现 10 Gigabit-capable 防火墙的功能，那下一代防火墙可能就无法让你满意了，” Antonopoulos 说。“我认为在数据中心中连接数以百计的外联网及合作伙伴的连接时使用这样的平台并不是一个明智的选择。在管理内部分段网络、非常复杂的 DMZ 以及虚拟服务器网络时也没有什么好处。但是对于处理来自 Web 和用户流量中的威胁时它确实是一个很好的平台，有些是传统防火墙无法实现的。”

下一代防火墙可消除边缘蔓延

在 Summa 医疗机构安装 Palo Alto 应用感知防火墙之前，Wade 是通过 Microsoft Internet Security and Acceleration (ISA)服务器阵列来保护系统的。之后 ISA 就被面

向外部的网络连接替换，速度也从 50 Mbps 提高至 100 Mbps。此阵列上曾运行着防火墙、杀毒软件和内容过滤等。

“忽然间，ISA 就变得很不稳定了，”Wade 说。“当时在这个阵列中我们有三个面向外部的服务器。后来我扩充为五个，虽然数量增加了，但是系统仍然不稳定。我曾与 Microsoft 合作，修改了我们防火墙服务器上的缓冲，虽然情况有了些许好转，但是操作起来确实不如从前。Microsoft 说未来做面向外部 ISA 阵列扩容，这样的话整个企业服务器的数量就会达到 11 个。这种说法似乎有些不切实际。”

Wade 开始准备重新购置一套系统时，但没有想买下一代防火墙设备。过去，Wade 曾用过 Juniper Networks、Check Point Software 以及 Sonicwall 公司的传统防火墙，但是当他与网络安全方案供应商 FishNet Security 交谈时，Palo Alto 被推荐给了 Wade。

“我们把 Palo Alto 的产品部署到我们的环境中，并设置其与 ISA 并列，这样在做端口扫描时我们就可以观察到所有进入 ISA 的流量，”Wade 说。“我们的视野更加宽阔。很显然，在 ISA 上有一个内容过滤器错误，我们运行了一个不能处理 IP 地址的内容过滤器，所以除非把主机名传送给 ISA，ISA 完成主机名的解析，否则根本就就无法得知你浏览的到底是什么网页。唯一能够知道的只有 IP 流量是在 80 端口上以及它是允许通过的流量，”他继续说。“人们发现只要他们在工作站上安装了防火墙客户端以及不抑制 ISA 上的自动侦测，他们就可以去访问 YouTube，Facebook，porn 等。很多东西都会避开内容过滤器，成为漏网之鱼。”

Palo Alto 使 Wade 制定了一套新的基于应用的防火墙策略。该防火墙与 Microsoft 的 Active Directory 结合，可以使 Wade 更加细致地配置其策略。

“在我们组织中，有一部分人有参加在线研讨会的需求。他们需要上在线课堂并在医院的各种计算机上进行操作，”Wade 说。“我可以设定策略允许特定的用户使用 HTTP 视频和 HTTP 音频，但是我没办法禁止用户使用 YouTube。用 ISA 或 Check Point 我无法做到。虽然我可以阻止用户访问 YouTube 网站，但用户仍可以允许嵌入式的 YouTube 视频或者从别的站点进入。”

企业需要注意下一代防火墙的架构变化

由于大多数供应商都在销售应用感知防火墙，其实从根本上讲就是带有 IDS/IPS 功能的状态防火墙。为了确保所选择的防火墙能够很好地在自己的网络环境中使用，网络工程人员在开始时就需要留意，Rothman 说。

“随着时间的推移，所有的供应商势必都会改进他们的架构，”他说。“现实情况是，大多数安全产品都需要从根本上改变。问题是：什么时候才会发生？企业认为现在的下一代防火墙只是初期产品，他们可以通过绑定其他功能来解决当前问题，当产品成熟时再做彻底改变。其实，这对技术来说只是一个发展线路，但是对企业来说却是巨大的挑战，尤其是那些还没有树立正确期望值的企业。”

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：杨亚男 ）

取代 UTM？下一代防火墙势不可挡

互联网的普及，云计算的浪潮，我们越来越离不开网络环境。这种依赖，让网络犯罪分子们看到了巨大的机会，有针对性的攻击越来越多，网络安全形势严峻。

其中最为严重的是 WEB 应用安全问题。现在的攻击超过 75%甚至 80%以上都是针对 WEB 应用的。黑客一般要攻击一个网站，目的不再是刚开始的炫耀，而是为了获取信息、获取利益，这种攻击行为通常是来无影、去无踪的。最好的实例就是近日的索尼被黑事件，影响之严重，我们有目共睹。

如何更好的实现网络安全已迫在眉睫。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。

很多厂商都提出了各自下一代防火墙的概念，概念的不统一让我们对下一代防火墙充满疑惑，什么才是下一代防火墙？下一代防火墙究竟是干什么的？它比传统防火墙强在哪里？

前段时间，编者参加了梭子鱼 2011 年度战略新品发布会，会上推出了一款下一代防火墙，并就梭子鱼下一代防火墙概念进行了讲解。对于其中一些解释，编者认为值得借鉴。

梭子鱼技术总监谷新表示，“传统防火墙在设计之初就带有一个缺陷，可能在几年之前没什么问题，但是现在，这种缺陷越来越暴露出来。三大本质缺陷：第一是安全方面的缺陷，传统防火墙是控制三层，就是 OSL 的协议模型里，对应用层没办法进行控制和识别，它不知道到底是哪一种应用通过了防火墙，所以也没有办法防御。第二个缺陷，是流控方面的缺陷，如果你只有一条链路，但是你不同的应用在用不同带宽的时候，重要的应用怎么提取出来，在这个方面传统防火墙是没有办法做到的。”

“还有一个缺陷是运维管理的缺陷。可能一台、两台没关系，但是当你的公司遍布全国，甚至全球有很多店，传统的防火墙没有办法去控制，它没有通过的策略管理。这就导致你部署的时候可能要花费大量的人力，在维护的阶段，也同样要花大量的人力，”他补充道。

传统防火墙的缺陷通常都能理解，那么可不可以部署一台 RPS，或者部署其他的来改善，或者可不可以用 UTM？

“到底是改良还是改革？改革就是要更新换代，改良就是修修补补。下一代是一个革新的东西，我们这里说革新，不是要改良，改良是解决不了更多问题的。”谷新说道，他举了个例子，“手机经历到现在已经是第三代了，第一代是大哥大，第二代是没有彩屏的，只能有简单的电话和短消息功能。当我们用这个手机的时候，很多人要拍照了，我这个手机不能拍照，那我就要买一台照相机，你可能还要听音乐、看电影，再买一台 MP3 或者 MP4。但是当机型发展到三代的时候，很多人就用这种手机了，比如 iPhone：这种手机具备前面所说的三种功能，除了这些功能之外，iPhone 还有很多其他功能，远远不只前面这三种。”

一个大哥大加上一个相机，再加上一个 MP4 小于一台 iPhone。“这个就是 UTM 和下一代防火墙的区别，下一代防火墙，不仅仅是 UTM，很多东西 UTM 实现不了，所以必须要改革，必须要革新，要更新换代，才能满足现代网络发展的需要。”谷新这样表示道。

梭子鱼下一代防火墙采用的是一个单引擎的技术。什么叫单引擎呢？就是当数据包过来以后，要把它打开，只要打开一次，不仅仅是端口要访问，应用要访问，所有该控制的模块都要来进行访问，一次性就完成了，不需要采用串联的方式。这是单引擎的工作模式，是一个本质的区别。UTM 要组合很多功能，它的工作模式是，通过防火墙过了一关，再过 IPS，IPS 过了，可能过 WEB 安全网关，是一个串联的形式，要一关一关的过，所以效率很低，因此 UTM 的性能很差。

“NG 防火墙会在未来的一段时间替代掉所有的网络防火墙，这是趋势。它自身有个应用安全的优势，这个产品或者这一类的产品会成为市场主流。NG 防火墙最大的一个贡献在于，原来网络防火墙更多的给用户的是一个物理感觉，端口，IP 地址，非专业人士还真不知道这是什么。”梭子鱼总经理何平表示，“但是我们每个用户应该知道自己的应用，QQ 我知道，邮件我知道，我在公司里什么位置也知道，我是网管员还是部门经理，还是总经理，所以可以这么讲，大家会发现进入 Windows，不同的帐号登录，配置是不一样的。NG 防火墙就相当于未来的一个操作窗口，所以 NG 防火墙应该是未来防火墙的一个主流，它实际上是从 DOS 系统升级到 Windows 系统。”

何平预言，“不出三年，大家会看到所有的传统防火墙厂商，都会提出他们也是 NG 防火墙，他们也要进行产品上的升级。传统防火墙厂商会增加应用层，应用层导向的厂商会加入网络层，最终会走向 NG 防火墙。”

这个预言或许已经开始应验，我们现在看到一些厂商都推出了下一代防火墙产品。下一代防火墙性能如何？是否能实现最初的目标？在不断的发展趋势中，让我们拭目以待！

（来源：TechTarget 中国　作者：刘平）

魔力象限：下一代防火墙将成为主流（一）

有了 Gartner 的新防火墙魔力象限，关于下一代防火墙的争论终将结束。现在，随着更多的企业部署了这项新技术，所有的问题都将迎刃而解。

Gartner 的研究结果表明，基于端口和协议作出决策的有状态防火墙现在已经变成一种落后技术，企业正在大规模评估和安装下一代防火墙。

新罕布什尔州首都地区医疗和协和医院的 CTO Mark Starry 说：“我认为传统防火墙并没能防御攻击公司网络的大多数威胁。每个月我都会接到电话通知，告诉我医院网络感染一些病毒，而他们只使用了一个有某种 IPS（入侵防御系统）的标准防火墙。”

两年前，Starry 将原来的 Check Point Software 和 Juniper 防火墙更换为 Palo Alto Networks 的下一代防火墙。今年，他发现新罕布什尔州所有大型医院都转而采用 Palo Alto 的产品。他说：“有一家医院曾经因为病毒感染而停止营业三天，现在这家医院正在考虑用 Palo Alto 的产品。”

防火墙魔力象限：下一代防火墙规则

下一代防火墙，也称为感知应用程序的防火墙，通常也具备有状态防火墙传统的端口和协议分析功能，但是它们还能够根据产生网络数据包的应用程序进行流量检测。在最近几年，Web 应用程序呈现爆炸性增长，这个功能也因此变得至关重要，因为大多数有状态防火墙只能够识别 80 端口的 HTTP 流量。

多年来，分析公司 Gartner 一直认为下一代防火墙是防火墙行业的未来，而在它最新发布的企业防火墙魔力象限中，它认为这个趋势变得比以前更为清晰。Gartner 推荐了 Palo Alto 网络公司，这家公司的技术在过去几年获得行业认可，与 Check Point Software 一起成为市场领跑者。

同时，作为长期占据 Gartner 魔力象限领军位置的 Juniper，仍然位列于传统的有状态防火墙，现在也已经落入挑战者象限，与思科、McAfee 和 Fortinet 处于相同的状态。思科的防火墙也只有有限的下一代功能。魔力象限定义的挑战者，是指那些拥有执行解决方案的销售与支持团队、但缺乏强有力技术计划的公司。

Gartner 公司的研究副总裁 Greg Young 说：“我们一直在等待防火墙供应商进入下一代防火墙市场。但是他们继续迷信 IPS。而这些 IPSec 的质量却非常差。它们无法与这些独立的下一代防火墙竞争。这些独立产品越来越多，而传统防火墙供应商仍然忽视这部分

市场。最终，客户需求超过了这个领域所有供应商所能够提供的产品。因此，我们调整了魔力象限的标准，规定领导市场的必须是那些拥有下一代防火墙产品的公司。”

Young 指出，在他接到 Gartner 咨询客户关于防火墙的所有咨询电话中，大多数是关于下一代防火墙的。他们或者希望购买这些产品，或者多了解相关的信息。“我认为，几年前客户对下一代防火墙持怀疑态度是合理的，但是现在市场上已经出现了可用产品和大量竞争。客户的想法已经开始转变。”

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：曾少宁）

魔力象限：下一代防火墙将成为主流（二）

下一代防火墙：潜在的实现问题

根据 Gartner 公司 Young 的观点，下一代防火墙执行的应用层分析极耗费计算能力，所以企业在部署这些新型设备时必须仔细斟酌。例如，许多统一威胁管理（UTM）供应商将他们的设备称为下一代防火墙，但是企业很快发现这些设备更适合小型公司使用。当他们开启全部特性，包括应用程序检测，UTM 设备就会成为严重的瓶颈。

Young 说："我们已经发现规模问题，大多数都是因为开启了那些不是面向企业设计的特性。我们急需面向企业的 UTM。下一代防火墙还有许多其他的性能问题未得到解决。如果只是硬件整合，将大量的元件强加到一个设备上，那么这就是问题的根源，它的性能会很差。"

但是，Young 强调，许多防火墙供应商现在已经有强大的企业级下一代防火墙产品。各个供应商相互争论，认为的产品是最好的，但防火墙用户必须自己评估这些产品，寻找最适合他们环境的产品。

下一代防火墙还给运营团队带来一个文化转变。防火墙管理员长年都在规定处理端口和 IP 地址的规则，下一代防火墙将迫使他们离开自己经营多年的乐土。

首都地区医院的 Starry 说："它植入了防火墙概念。您编写的是基于应用程序的规则，而非基于端口和 IP 地址的。防火墙管理员适应基于应用程序的规则有一定的难度。但是，您能够掌握这两种方法，也必须掌握这两种方法。"

下一代防火墙：不要局限于精细应用程序管理

加州大学欧文分校的系统管理员 Steve Gilmer 指出，应用程序可见性是很重要的，但是在选择下一代防火墙时，这并非是他唯一的关注点。

Gilmer 在大学安装 WatchGuard 防火墙，以保护课堂网络。他介绍说，他曾经认真地研究每个下一代防火墙是如何进行 HTTPS 流量解密和检测。他认为 HTTPS 是一个重要的恶意软件威胁目标，但是大多数防火墙供应商不推荐对 HTTPS 进行解密和检测。相反，他们认为他们的产品能够检测出所有在网络内部发起攻击的恶意软件，允许网络安全管理员在网络中隔离感染病毒的机器。

Gilmer 说：“显然，恶意软件已经进入网络，这就是问题所在。”所以 Gilmer 研究了各个防火墙供应商是如何检测恶意软件的。许多供应商都通过第三方供应商产品来实现这个功能，但是很难评估每一个供应商的优劣。

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：曾少宁）

网络安全呼唤下一代防火墙技术：特点与选择

目前，防火墙仍是很多单位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，有些类型的防火墙，特别是全状态数据包检测（SPI）已经开始过时，虽然有人认为这种说法有点儿夸张。

状态检测的问题在于它仅重视端口和 IP 地址。端口就像电路断路器一样：在重要的流量流过时，用它作为过滤标准显得过于笨拙。而且，IP 地址没有与用户绑定，使得用户可以用一种完全不同的设备来逃避策略。

解决这个问题的关键在于：要重视用户，要重视用户所使用的应用程序以及用户用每一个应用程序正在做什么，尤其是那些容易被人利用其漏洞的应用程序。当前，80 号端口的“阻止/准许”已经不够精细。甚至像“阻止/准许”社交软件（如 Facebook）这样的操作也已经远远不够了。相反，防火墙必须支持准许用户从事与业务相关活动的策略，而不管他使用什么样的计算机。

当然，新技术绝不应当仅关注社交软件，公司使用的任何其它的 web2.0 软件，都应当包括其中。

下一代防火墙技术

下一代防火墙应当专注于应用程序、用户和活动，而不是端口和 IP。它可以控制用户的操作，从而保障 Web 和电子邮件等的安全，并将其应用于所有应用程序。其次，下一代防火墙还应拥有反恶意软件技术，并在底层完全集成到防火墙中，从而避免单独的组件在扫描同样的内容时所造成的延迟。集成的必要性还由于当今威胁的复杂性。

避免延迟至关重要，因为防火墙必须足够快，其目的是在不损失性能的情况下准许所有的网络通信通过防火墙。理想情况下，这种集中化的控制还包括云和移动通信。相比之下，典型的 UTM（统一威胁管理）解决方案太慢，因为它并没有完全地集成，只够中小型企业勉强使用。

每一个安全组件都应当是最优的。或者说，一群“平庸之辈”难成大事。下一代防火墙必须能够检测运行在 SSL 加密通信中的内容，或使用模糊技术，它必须建立在专用的特定硬件基础上。

下一代防火墙必须提供出色的透明性。在管理员设置策略之前，必须知道网络上正在发生什么，这对于当今的多数防火墙来说是很难实现的。它还必须提供杰出的精细度，同

时还要提供诸如“不允许在网络上进行基于浏览器的即时通信”之类的高级策略。下一代防火墙还必须拥有极低的总拥有成本，要富有成效。

最后，下一代防火墙还必须能够随着当今网络所面临的威胁的变化不断演化，即公司需要投资于能够解决网络黑手正在和将要触及的诸多方面。

如何识别下一代防火墙

那么，怎样区分一种防火墙是否是下一代防火墙呢？

首先，它应当拥有独立的基于应用程序的策略，而不是“双重”策略（基于应用程序和基于端口/IP）。下一步，你不妨访问一个 Web2.0 应用程序，如 SharePoint，检查这个防火墙是否能够识别它的名字，而不是仅将其识别为 Web 通信。要在应用程序水平上测试防火墙，而不是在传统的“位”的基础上测试。

其次，如果厂商向你列示了每个安全组件的不同吞吐量或速率，如 IPS、DLP、反病毒、防火墙等，而且每个组件的速度是在关闭其它组件的情况下测试的，就可断定，它集成得不太好。真正的下一代防火墙应当拥有一个统一的吞吐量数字。

当然，上述标准也许过于苛求，选用与否主要取决于防火墙所适用的信息安全需要和网络环境。

（来源：TechTarget 中国　作者：茫然）

下一代防火墙管理设备：更智能，也更复杂！（一）

下一代防火墙将通过集成入侵防御和应用与用户监控功能来提升网络安全性，但是它们也会带来新的管理挑战。由于传统防火墙充斥了大量废弃的规则，所以防火墙管理总是一个有挑战的工作。但是，在使用下一代防火墙管理技术之后，网络安全专业人员将需要维护更多的规则和策略。

斯坦福德 Gartner 公司研究副总裁 Greg Young 说：“防火墙规则总是到处泛滥，但是入侵防御和应用控制使问题更加复杂。现在正是使用下一代防火墙降低复杂性的时机，但是如果实施不当，则可能会适得其反。”

最近，Osterman Research 代表安全与风险管理公司 Skybox Security 对 209 家企业进行了一次关于下一代防火墙管理的调查。在调查中，他们邀请网络安全人员列举下一代防火墙管理的三大挑战，其中包括：确认访问策略与网络分片策略是否正确实施（39%）；维护入侵防御系统(IPS)签名（37%）；以及优化防火墙规则集（36%）。

在有状态防火墙中，规则与策略的复杂性迫使网络安全管理员在防火墙管理方法中整合更多的业务逻辑。Skybox 的 CEO 及创始人 Gidi Cohen 说：“下一代防火墙规则将控制哪些用户群组在哪个时间段可以访问 Web 应用或社交网络。不仅规则变得更加复杂，而且组织的安全策略逻辑也变得更加复杂。这是一个计划挑战、协调挑战，也是一个技术挑战。”

Young 指出，网络安全人员需要抛弃“老派的”防火墙管理方法，转而采用下一代产品。例如，他说，改变对应用控制规则和策略的控制不可能像基于端口的传统规则一样。

在传统防火墙上，任何变更都需要发起一个变更请求。如果开发团队希望启动一个新应用程序，那么它会发送一个变更请求到防火墙上要求打开端口。这种细致方法不适用于下一代防火墙的应用监控。Young 说：“要采用不同的方法。您可以批准特定类型的应用程序。您可以说：‘除了特定的情况，我们不允许使用任何点对点应用程序。’所以如果发现一个点对点应用程序，而防火墙管理员又希望批准这条规则，那么它应该以预先批准的方式进行处理。”

Young 指出，网络安全人员需要抛弃“老派的”防火墙管理方法，转而采用下一代产品。例如，他说，改变对应用控制规则和策略的控制不可能像基于端口的传统规则一样。

在传统防火墙上，任何变更都需要发起一个变更请求。如果开发团队希望启动一个新应用程序，那么它会发送一个变更请求到防火墙上要求打开端口。这种细致方法不适用于

下一代防火墙的应用监控。Young 说：“要采用不同的方法。您可以批准特定类型的应用程序。您可以说：‘除了特定的情况，我们不允许使用任何点对点应用程序。’所以如果发现一个点对点应用程序，而防火墙管理员又希望批准这条规则，那么它应该以预先批准的方式进行处理。”

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：邹铮）

下一代防火墙管理设备：更智能，也更复杂！（二）

下一代防火墙管理是一种成熟且协调的方法

企业管理联盟研究主管 Scott Crawford 指出，在广义上，防火墙管理就是变更控制。拥有成熟防火墙变更管理方法的企业更能避免安全漏洞和性能破坏问题。在下一代防火墙中，随着防火墙环境变得越来越复杂，自动化也变得越来越重要。Skybox 的调查发现，有 58%的企业在他们的下一代防火墙上部署了 100 条以上的规则，而有 35%的公司每个月执行 100 次以上变更。

Crawford 说，在这些复杂环境中，用户必须利用自动化方法，因为他们通常过于复杂，而无法通过手工流程进行可靠管理。在部署之前，一定要在您的建模范围内验证您规划的所有变更，然后跟踪这些变更，保证它们按预期方式部署。此外，您需要设定一个回滚变更的流程，这样才不会产生其他问题。

Skybox、Tufin Technologies、AlgoSec 和 Athena Security 等供应商在专门研究这些问题。他们提供了防火墙变更控制产品，其中大多数都可以对这些变更影响网络的方式进行建模。此外，这些供应商正在将他们的产品更新到下一代防火墙管理技术。

如果一个 IT 组织的下一代防火墙管理团队与网络运营团队属于独立实体，那么网络安全团队还应该保证要这两个团队协调一致。Crawford 说：“即使在下一代防火墙出现之前，我们也发现一些组织遇到一些预料到的性能水平和可用性中断的问题，因为安全策略在不知道会产生什么影响的情况下就应用了。”

“当您增加了感知应用的防火墙，这个挑战越来越大。即使在分布式网络的客户端，如果您部署 WAN 优化设备，那么您会希望将它是专门为应用程序的设备。您需要在网络性能、可用性与安全性需求之间做出协调，以避免出现冲突和增加暴露风险。”

另一个问题：防火墙的入侵防御

Skybox 的调查证明，许多企业在管理下一代防火墙上的入侵防御签名时举步维艰。有 86%的公司计划在他们的防火墙上使用 IPS 模块；他们中有 65%处于在线防御模式。管理这些模块的 IPS 签名并不容易。只有 54%的公司由供应商自动更新。三分之二的公司正尝试手动管理这些签名。

Gartner 的 Young 说：“默认签名集只是一个入口。接着是优先值。例如，如果您没有 Oracle 数据库，则不要启用 Oracle 签名。相反，如果您有大量的 Oracle 流量，则确实需要进行优化和调优这些 Oracle 签名。”

根据 Skybox 全球销售副总裁 Michelle Johnson Cobb 的观点，有一些企业希望了解这些签名如何有效地阻挡威胁。她说：“他们是否真的阻挡住了原本我想要阻挡的威胁？有一些方法可以检验它是否真的有用。”

如果用户实施了大量潜在威胁的默认签名，那么它将会减慢流量传输速度。Cobb 说：“所以，如果您的目标之一是保证最高性能，同时有效阻挡威胁，那么这里需要一种平衡。此外，事情总会发生变化。在网络中，每天都会出现新的漏洞或威胁。您可能要确定是否需要激活新的签名。”

SkyBox 刚刚增加了对 Palo Alto Networks 的 IPS 功能支持，它可以分析签名，然后将它们映射到漏洞上。“您可以在一个控制面板显示哪些签名已激活，哪些漏洞被阻挡住，以及您可以打开哪些控制，从而得到更多的保护。”

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：邹铮）

下一代防火墙供应商对比

下一代防火墙产品的供应商有很多，但是他们一直都在为谁的技术最好争论着。下一代防火墙是应用感知型的。不同于传统的基于端口和协议的状态防火墙，下一代防火墙能通过流量识别网络上的应用程序。如今把应用放到公有云或者通过软件运营即 SaaS 的这一趋势,使我们需要一个更高的尺度来确保进入企业网络的数据是合适的。

每个厂商都有他自己的方法在防火墙里实现应用感知。TechTarget 记者采访了一些知名的防火墙供应商，本文将逐一介绍各供应商的防火墙产品的与众不同之处。下面是我们了解到的信息。

Astaro 使用来自合作伙伴 Vineyard Networks 的应用特征数据库将应用感知发送到 Astaro 安全网关。通过这个合作伙伴，Astaro 防火墙可以辨别出来自同一网站的不同应用并且可以启用服务质量选项为这些应用优先分配带宽。Astaro 安全网关的最新版本加强了对于这个功能的描述。他提供了一个全网络视图使得管理员能够基于实时情况定义安全策略。按照 Astaro 所说的，其关键目标就是当发生新的威胁时，IT 能通过调整防火墙迅速而又轻松的做出反应。

Astaro 同样致力于辨别新的未知的应用类型，只要新的应用开始触及客户网络。接下来他们可能会发布允许管理员选择性加入及匿名提交未知数据包类型给 Astaro 工程师审核的系统。公司会用收集到的数据来识别这些应用并把他们加入到特征数据库中。

Check Point 开发了 AppWiki 应用库，并声称其可以识别超过 5000 种应用和 100000 个社交网络小插件。这些应用特征被导进了公司的 check point 应用控制和识别感知软件刀片上。同时该软件结合了活动目录来识别用户和终端,允许管理员自定义安全策略。Check Point 还可以对用户进行实时的指导。当用户违反安全策略时，用户电脑上的代理软件 UserCheck 会弹出一个窗口，来解释违反的内容并帮助用户纠正。这款软件同时让用户可以提供反馈意见给管理员，有效地根据用户的需求自定义安全策略。

Cisco Systems 发布了在 Adaptive Security Appliance (ASA)里增加新的应用可见性的计划，这也是其最新 SecureX 安全构架的一部分。Cisco 声称这一新的构架重心将不只是应用感知，同时也能进行用户和设备识别，目前关于 Cisco 如何改善应用可见性的细节仍然很模糊。

Fortinet 的 FortiGate 设备的应用控制功能用协议解码器和网络流量解密来识别应用的。该公司的 FortiGuard 实验室团队保留了一个应用特征数据库，并且会为新应用添

加特征同时为升级的应用更新特征。该应用库能使 Fortinet 产品对单一网站上的不同应用进行分离，比如 Facebook 或 Google,还允许单独分配策略。Fortinet 声称他们的产品与其他厂商相比有性能和集成上的优势，因为所有的技术都是自己开发的。

Juniper Networks 使用一套叫 AppSecure 的软件产品，为 SRX 服务网关提供下一代防火墙能力。被称为 AppTrack 的应用感知组件，依据 Juniper 的特征库和企业管理员建立的通用应用特征来为网络提供可见性。利用 AppTrack 提供的可见性，AppFirewall 和 AppQos 组件套就能够对应用进行策略实施和流量控制。同时，Juniper 还声称其平台具有很好的扩展性，并且交付应用的速度可达 100Gpbs。

McAfee 最近被 Intel 收购了，McAfee 是利用它的 McAfee AppPrism 技术进行应用发现和感知的。借助 Mcafee 全球威胁智能团队独立研发应用特征，AppPrism 可以识别成千上万个应用，无需考虑端口或协议。AppPrism 也提供更高级别的应用控制，允许管理员关闭应用中存在风险的部分。例如，管理员可以利用该技术关闭即时聊天软件中的文件共享功能而不影响用户的正常聊天。McAfee 声称它的下一代防火墙具有一定的优势，因为它的应用感知技术是它防火墙架构的核心部分，所有组件包括应用特征都是内部研发的。

Palo Alto Networks 表示它是第一个推出下一代防火墙的厂商，并且是第一个用应用感知代替端口式流量分类的厂商。公司的产品是基于一个叫 App-ID 的分类引擎。App-ID 通过多种技术队应用进行识别，包括解密，检测，解码，签名以及试探等技术。对于已知应用的个别 App-ID 可以依靠这些技术中的任何一种组合，用引擎来识别该应用的所有版本以及该应用运行的所有平台。App-ID，作为 Palo Alto 防火墙的核心部分，会一直运行着，所以当应用启动了一个功能时，它就可以识别到，比如文件传输，它还可以为特殊功能申请策略。该厂商还表示 App-ID 是可扩展充的，只要新的技术可用，就可以加到分类引擎中。

(来源：TechTarget 中国　作者：　Michael Brandenburg　译者：潘天禄)

分支机构的下一代防火墙：Palo Alto & SonicWall

Palo Alto 和 SonicWall 推出了适合分支机构价格的下一代防火墙。

Palo Alto 这周发布 PA-200，它是价值 2000 美金，具有 100Mbps 吞吐量的下一代防火墙。SonicWall 上周发布了 2 款针对分支机构的下一代防火墙：NSA220 和 NSA250M，它们的起始价格分别是 1095 美金和 1495 美金。下一代防火墙所包含的应用智能和控制功能在 SonicWall 设备上是可选的，它需要额外的授权费，但这在发布会中没有详细说明。使用下一代防火墙模式，SonicWall 设备大概可以达到 110Mbps 的速度。

传统的状态防火墙检验端口和协议是为了判断，例如是否经过 TCP 80 端口的流量确实是合法的 HTTP 流量。下一代防火墙超越了端口和协议安全的做法，应用深层报文检测来识别用 HTTP 协议的请求和用 80 端口接入的应用程序。这项功能在今天尤为重要，特别是当企业的应用程序愈来愈多的基于网页，而且客户网页应用程序可以在企业中合法使用。

根据 ZK Research 首席分析员 Zeus Kerravala 所言，今天企业正在它们的中心位置部署大型且昂贵的下一代防火墙。为了使它们的分支机构能够感知应用安全，企业为了检测要么回程分支机构网络流量到中央防火墙，要么在分支机构部署轻量级安全设备，比如统一威胁管理设备。

而在分支机构直接部署下一代防火墙，企业可以将广域网的安全问题降入分支机构，节省回程流量消耗的带宽。

Kerravala 说：“其实没必要在核心跑所有因特网流量，但是如果你转到一个分离的隧道模式，并且希望分支机构的用户能直接访问因特网，那么和核心位置一样，你需要在分支机构使用相同的应用感知防火墙。想要分支机构的下一代防火墙价格便宜，并且吞吐量尽可能高。显然你的分支机构的技术不能昂贵到超过了回程因特网流量的费用。”

根据信息技术总监 Michael Giorgio 介绍：“ SonicWall 客户 Connex 信用合作社使用中央 SonicWall NSA 3500 统一威胁管理防火墙，将流量从银行分支回程到网络核心。从用户的观点看，我更愿意把流量分散，它可以减轻网络的负荷，通过取消回程流量到 WAN 上的 hub，每个分支机构的下一代防火墙可以减少分支机构的 WAN 链路。”

分支机构下一代防火墙功能：选择还是必须？

Current Analysis 研究总监 Andrew Braunberg 说：“这仍然有待观察，我们不知道分部很多的企业，它们对下一代防火墙应用智能技术有多大需求。在分支机构使用状态防火墙很不明智。但是小型分支机构可能不需要下一代防火墙的精细应用控制功能。如果你想在每个设备上安装这个功能，它会在哪里开启，会到什么程度？你知道一旦你开启了额外的深层报文检测，你会进行性能检测。我认为分支机构会使用该功能，但是我好奇它的使用情况以及使用方式。”

如果将来证实确有必要，他相信许多企业将部署 SonicWall 设备，因为将来状态防火墙可以升级为下一代防火墙。

Palo Alto 产品市场总监 Chris King 提到，Palo Alto 的 PA-200“天生”就可以在下一代防火墙模式中工作。PA-200 根据对应用程序的识别来决定允许或拒绝流量。他提到了其他厂家，也包括 SonicWall 在内，是根据端口来决定的。他们在流量中应用一个单独的深层报文检测引擎来识别应用程序，做出不同的策略决定。哪种做法更优现在还无定论。

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：潘天禄）

Cisco 网络安全架构与下一代防火墙

近几年来，在以网络安全为主题的交谈中总会提到应用感知，并且许多新型公司推出了下一代防火墙，下一代防火墙能很好地实现了基于应用的安全策略，而非从前基于端口和协议的简单制定方式。在沉寂了一段时间之后，Cisco 也终于推出了其下一代防火墙。

Cisco 公司宣布，最新推出的网络安全架构——SecureX，将会超越应用感知，给用户带来耳目一新的使用体验。

Cisco 的目标是处理使网络安全架构变复杂的一系列技术内容，包括虚拟化、云计算、移动性以及其他用户设备的扩展性。

此次 Cisco 公司推出的 SecureX 网络安全架构能够“验证用户身份，用户网络接入方式，用户使用设备，以及设备归属权（是否为公司资产）等，” Kennedy 说道。“它还可以识别所使用的应用程序等等，而且还能确定他们的位置，是在室外还是在室内？对设备安全状态的识别等等。上述所有功能都有相应的规则和策略做支持。”

情境感知功能在下一代防火墙背后迅速成长

防火墙是 Cisco 最初发布 SecureX 的重点，是源于 Cisco 的自适应安全设备（ASA）5000 系列的软件升级。但是 SecureX 同样有分配网络安全功能的特性，Kennedy 说。最终，企业都将会把这些安全网关的性能应用在其他各种各样的平台上，包括 Nexus 数据中心交换机，综合服务路由器（ISR）以及云计算。

通过结合 TrustSec 与基于 802.1x 接入控制技术中的数据，SecureX 能够获得情境感知；Cisco 安全智能运营（SIO），是一个全球安全运营中心，它可以提供各种潜在威胁的分析并提供必要的数字签名，对任意连接以及 Cisco 的 VPN 客户。

2011 年全新的网络安全架构发展态势引人注目

在 2011 年，Cisco 计划逐步提高其情境感知功能的影响力，首先是对设备型号与用户位置的可视性，其次是用于用户身份的轻量目录访问协议（LDAP）。之后 Cisco 会逐步推出应用感知，这是下一代防火墙的核心功能，Kennedy 说道。

SecureX 网络安全架构的推出，虽然显示了 Cisco 超乎寻常的市场前瞻性，但是在技术上 SecureX 网络安全架构是否能够成功实现，还拭目以待，Forrester Research 公司高级分析师 John Kindervag 说道。

“SecureX 网络安全架构需要大量的 TrustSec 用户。它们正试图做像 Palo Alto 以及其他应用级防火墙供应商已经实现的事，但是为了快速推广产品，他们不得不为客户增加产品的技术力度，” Kindervag 说道。

Cisco 表面上使用的网络流量已经被软件代理商贴上了数据的标签，这让 Kindervag 非常担心。除非 Cisco 能够提供强有力的，集中式的管理软件，否则广泛地部署客户端软件，将会为企业带来整体的网络安全架构方面的威胁，他说道。

“从我的立场来看，我认为管理的难度还是非常大的。就像 CSA（Cisco 安全代理）一样。Cisco 最终还是不得以不停产 CSA 来收场，倒不是因为 CSA 不是一款好产品，只是因为对于客户来说，管理 CSA 过于复杂，”他说道。

在推出 SecureX 网络安全架构的同时，Cisco 还面临着来自其他供应商的竞争，比如那些已经推出了下一代防火墙，以及那些正着手提供除应用可视性以外其他功能的供应商，所以说，Cisco 所面临的威胁不可小视。

Palo Alto 发布的最新技术合作伙伴规划中提出，允许客户通过第三方安全供应商扩展 Palo Alto 的应用可视性，供应商名单包括，ArcSight，NetWitness Corp.，Q1 Labs，RSDA 以及 Solera 网络。

（来源：TechTarget 中国　作者：Shamus McGillicuddy　译者：杨亚男）