

NETGEAR®串流扫描技术

引言

随着 Web 2.0 技术的普及和在互联网的重要性日益增加，商业企业已越来越重视和关注，然而，它也带来新的攻击方法，黑客利用 Web 2.0 提供大量的连接以及它与用户之间的信任。P-to-P 网站提供了陌生人之间的文件共享方式；接受了浏览器被安装插件访问特定的网站，越来越多的网络站点告诉许多用户，点击 Email 上的链接是安全的，这些熟悉的行为，为黑客的攻击提供了新的渠道。

根据最近的 Gartner 的研究，在 2007 年里，基于 Web 的威胁增加超过 800%，多达 275 个浏览器插件漏洞被发现。另外一项研究发现，79%的合法网站被发现已经黑客通过注入恶意应用程序而劫持，其余的 21%发现流氓网站被设计成合法的网站一样，并通过 Email“推销”给直接用户。

面临的挑战

Internet 在商业企业的日常运作中变得越来越重要，关键业务的应用 90%都是基于 Email 和 Web 的访问，尽管大部分公司都知道一些恶意的插件通过 Web 流量引到他们的网络里，但很少公司引起足够的重视。

平均起来，安全厂商每天收到超过 20,000 个特有的恶意软件样本，而有超过一半的网络威胁是通过 HTTP 方式收集的。越来越多的个案，一个用户只需访问一下 Web 网站或浏览一下 Email 的 Web 链接就会被感染上木马或间谍软件。Email 也是恶意软件的一个重要来源，并经常被用来引导用户访问基于 Web 的攻击。

随着基于 Internet 威胁越来越多，促使需要一个强大的网关安全解决方案，能扫描入栈和出栈的流量，并在到达个人电脑之前检测和删除威胁。然而，全面的安全和网速的问题一起未得到有效解决，由于安全性和性能固有的反向关系，用户需要速度，特别是在 Web 浏览的速度需求上，如果一个 Web 安全解决方案不能解决延时问题，用户将第一时间抱怨。

传统批量扫描VS。串流扫描技术

最安全的解决方案-从桌面安全到网关设备-利用“批量”扫描技术。这意味着，只有在收到整个文件后，才开始扫描整个文件，扫描完后再输出(见图 1)。因此，由于文件传输和扫描的原因，最终用户经常感觉访问延迟，甚至有时出现超时的情况。

批量扫描是在病毒主要通过移动媒体感染的时代被开发出来的，因此，它采用的算法依据是实体在随机访问时被扫描，该技术非常用效，例如：媒体。然而，当用于基于 Internet 的威胁的实时 Web 流量扫描时，这个扫描方法因为延时的原因并不被用户所接受。

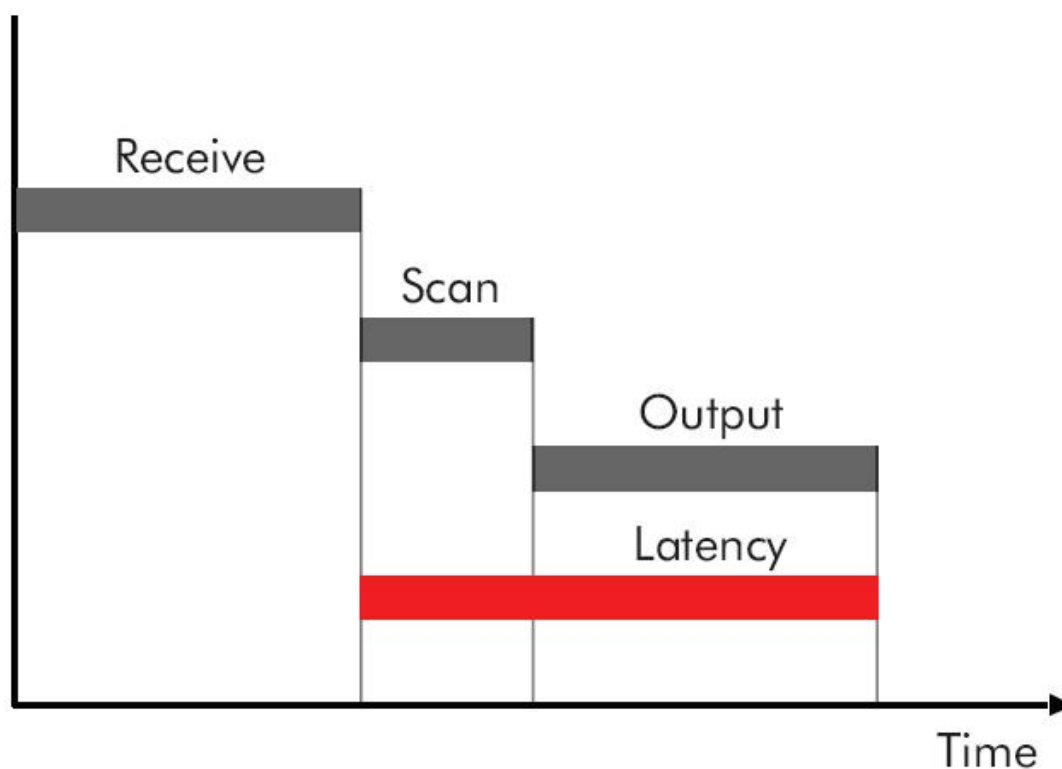


Figure 1: Traditional Batch-based Scanning

图 1:传统批量扫描技术

I

相比之下，串流扫描不是将网络数据作为文件传输，而是简单地作为流存在。NETGEAR® 串流扫描引擎在网络中同时开始接收和分析流量(见图 2)，一旦收到最小的字节数，扫描就已经开始了。扫描引擎在继续扫描另外的可用的字节时，另一个线程已在输出字节，这种多线程的扫描方法对网络的性能影响极小，文件的扫描速度比传统的安全解决方案快许多倍——在性能方面的提升是显而易见的。NETGEAR 串流扫描技术也是高度可扩展的，所以，随着流量的不断上升，性能上的优势变得越来越明显。企业因此能够负载巨大的峰值流量，例如基于互联网的威胁爆发时的巨大流量。

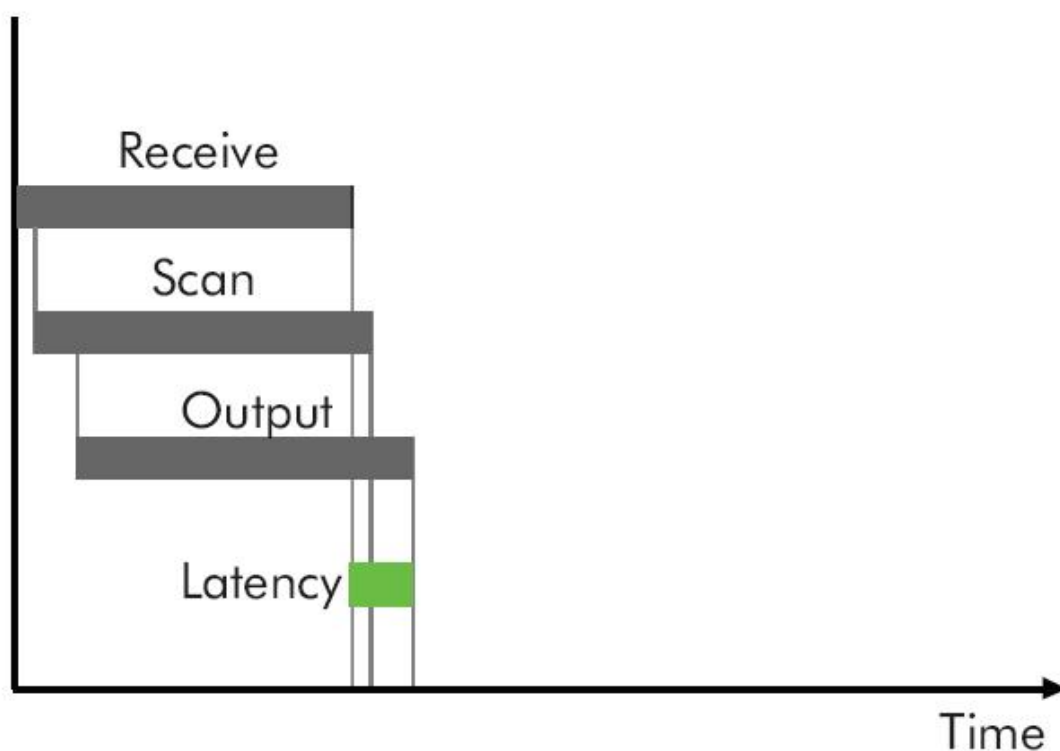


Figure 2: NETGEAR Stream Scanning

在综合测试中，NETGEAR 的串流扫描技术比传统的批量扫描技术快 5 倍，它已成功地用于广泛的行业，从政府，医疗保健，零售，部署在小于 50 个用户的商业企业，

结束语

在今天动态的商业环境中，商业企业要求在网络和安全之间找到一个平衡点，安全解决方案必须在没受到网络瓶颈的影响下，保护公司不受到基于 Internet 的威胁，NETGEAR 的专利技术串流扫描技术架构实现了这种平衡，NETGEAR 实时扫描网络流量，并不会使公司的网络速度受到影响或停顿的状态。

NETGEAR® ProSecure™ STM 内容安全网关解决方案

NETGEAR® ProSecure™ 采用特有的技术，通过爆发扩散的速度和广泛程度来检测并阻止爆发。通过这种方式，可以在垃圾邮件和恶意软件爆发产生的极短时间内检测出来，并且实时地阻止所有相关的信息。

ProSecure™ STM 平台采用了专利的串流扫描技术，能够在数据流进入网络的时候马上进行扫描。NETGEAR STM 使用单一的平台即可实现对垃圾邮件、恶意软件、安全破坏或不必要的应用程序进行扫描，通过串流扫描技术，能够实时地扫描大量的数据。这使得局域网中的用户可以接收到安全的 Email 和 Web 内容但却没有任何延时。

ProSecure™ STM 平台使用主动防御系统来避免漏洞从发现到修复之间的时间差。NETGEAR 的解决方案中采用“法医式鉴定方法”来识别进出网络数据流中的可疑的特征，并抵制这些特征直到它们能够更精确匹配。