

UTM背后深藏的秘密： 安全厂商不想让您知道的

介绍

直到上世纪 90 年代末，网络安全威胁主要是开发程序员为了寻求名声，或只是想测试一下他们本身的技能，甚至只是对此寻找一些乐趣，以至会破坏其他用户的计算机。因此，早期的威胁的范围和影响是有限的，通过反病毒软件和状态数据包检测(SPI)防火墙相结合即可以阻止。然而，互联网的发展演变出日益复杂的攻击。现在的许多威胁轻松地绕过这些传统防火墙。

为有效防止这些威胁，大多数大型企业采用了一个强大，多层次的安全解决方案，其中包括防护广泛的 Web 和电子邮件的攻击。这种多层防御战略需要复杂的系统，能够通过掌握该公司的网络流量，以确定是否有任何不正常的流量,从而有效地保证公司的所有的网络资产。最重要的是，该解决方案需要大量的人力和财政资源来购买和实施。

商用网络的安全需求

因为通过互联网传播的网络威胁是不分好坏的，商用网络也同样面临着象大型企业相同的安全威胁。然而，商用网络通常缺乏所需人力和财政资源来实施复杂的企业级安全解决方案 - 事实上，这使他们面临更大的风险。他们没有 IT 资源花在复杂的安装，维护多种的安全软件包，频繁的更新，或用户授权许可等问题上。

商用网络需要不但能提供象大型企业相同级别的安全的，而且易于部署和维护，自动运行，直观的图型界面，日志警告，和全面的报告等理想特点的典型的解决方案。为了解决满足上面这些要求，就必须在一个系统中，包含所有层次的安全需要。

乍看之下，统一威胁管理（UTM）设备，似乎最适合商用网络的安全需要，基于成本，简单和自动化这些特点集于一身（All-in-one）的设备。UTM 结合了传统的防火墙和 VPN 功能，增加了安全组件，例如入侵防御，防病毒，URL 过滤和反垃圾邮件。在集有这些安全功能的设备是一个更加经济和更易于管理而与企业级相当的设备，从而使 UTM 成为极具吸引力的商用网络解决方案。

传统UTM的问题

从表面上看，UTM 似乎提供的商用网络的安全解决方案正是他们所需要的。然而，很多安全厂商没有认识到在一个硬件设备上运行这么多的安全组件需要强大的处理能力。首先，UTM 所生产的硬件平台仅仅比那些独立的防火墙快一些，在 UTM 上启用额外的安全

性能，将明显增加网络流量的延迟- 特别是反病毒扫描。反病毒扫描所需要的性能大约比传统的防火墙数据包检测多 100 倍以上的处理器，因此，大部分 UTM 在启用反病毒扫描后，系统和网络流量将变得十分缓慢。

认识到这一性能问题，UTM 厂商通过不同的方法以尽量减少系统所需的资源来解决此问题。他们采用两种不同的方法试图解决延迟的问题。其中一种方法是减少安全程序的数量以控制这些有限的资源，从而保证他们的产品的性能和功能。企业级的安全系统可能会由最好的软件和技术所组成，但商用网络产品的版本很可能是缺乏关键的安全组件。必要的安全程序，例如入侵检测，或反病毒等组件取消，从而帮助提高网络的处理速度。在商用网络的版本中可能还会删除一特性，使产品的功能减少或用户界面没那么友好。

另外一个方法是利用削弱这些安全技术，从而减速少这些安全程序的进程。例如，一个厂商的企业级 URL 过滤功能共有 5000 万 URL 黑名单 - 但他们提供的小企业版本将削减只有几千条地址。同样，企业级的反恶意软件引擎包括 100 万的恶意软件特征库，可能将削减到只有 3,000 条的启发式恶意软件检测排除的特征库，或者，企业级的反病毒过滤器是在他们的内容或截住垃圾邮件和其它恶意软件的功能，可能将简化成只有一个已知的静态的垃圾邮件 IP 地址黑名单作为小型企业的版本。这已成为厂商填补 UTM “清单” 功能的一种普遍做法，从而使商用网络只得到最低的安全保障。

事实上在互联网网关上部署这些 UTM 产品，商用网络将面临着重大的安全风险。最糟糕的是，这为他们提供了虚假的安全感。这不是对于商用网络的最终解决方案，反而传统的 UTM 变成 “一个虚有其表的盒子”。

解决方案

我们应该重新考虑商用网络的安全需求，并建立一个适合这个市场需要的安全的解决方案，而不是削减企业级的产品并以较低的价格卖给商用网络，安全厂商必须认识到商用网络是一个独特的市场，并设法满足他们的需求。安全厂商必须为他们提供一个融合全面的必要性能，强大的安全特性，充足的网络性能的解决方案- 一个符合于典型的 IT /安全预算的商用网络的软件包。直观的 GUI 界面，主动的警告及日志，软件的自动更新，同时也需要提供卓越的易用性。

NETGEAR ProSecure™ UTM 采用了两个重要的因素妥善解决一直困扰着大多数 UTM 厂商的延迟问题。首先是硬件优化，因为硬件的处理能力不足会造成网络的延迟，有时甚至

会在系统扫描安全威胁时出现超时，NETGEAR 的 ProSecure™ 的 UTM 使用专门的处理器来优化网络处理过程，从而降低可能令人难以接受的网络延迟。

此外，NETGEAR 的 UTM 设备上的软件是经过优化用以处理网络流量的，大多数的安全解决方案 - 从桌面安全到网关设备 - 采用批扫描处理技术。这是采用同样的方法用于传统的桌面防病毒软件的解决方法对文件单元进行扫描，这意味着，收到整个文件后才开始扫描文件，在整个文件被扫描完成后才输出，因此，最终用户经常感到在文件传输和扫描时很长的延时。

与此相反，NETGEAR 的 ProSecure™ UTM 产品采用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。

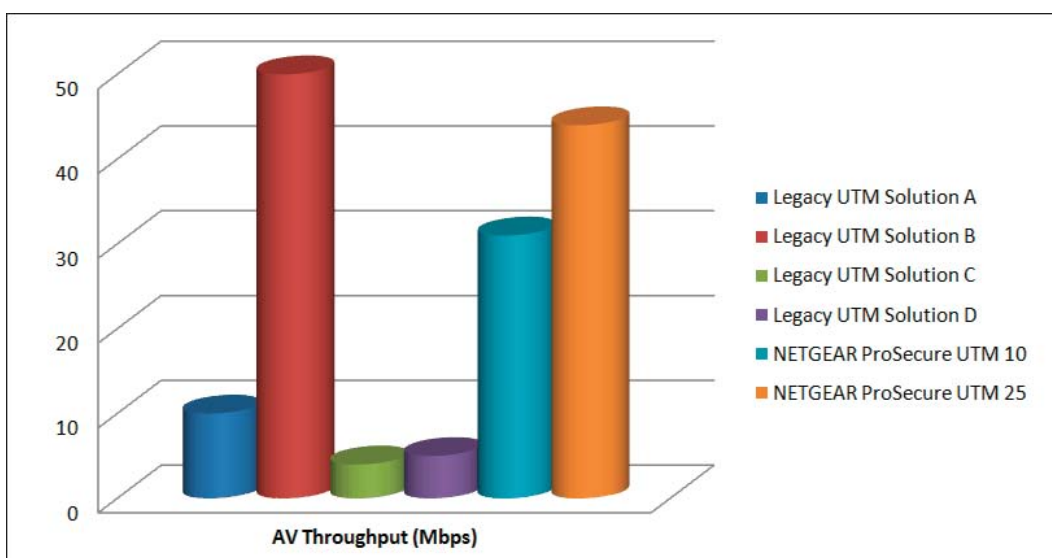


图 1: UTM 反病毒吞吐量对比

NETGEAR 的 ProSecure™ UTM 设备不是要等到整个文件到达后，才开始扫描和进入网络的处理数据流。一旦收到最小的字节数，扫描就开始，当另一个线程输出已经扫描的字节后，扫描引擎就继续扫描可以利用的数据。这种多线程的方法，除了处理复杂的串流处理算法外，在 NETGEAR 的 ProSecure™ UTM 设备的扫描过程中，几乎不会影响网络性能 - 从而消除在其它传统的 UTM 解决方案中出现的扫描时延时大的问题。

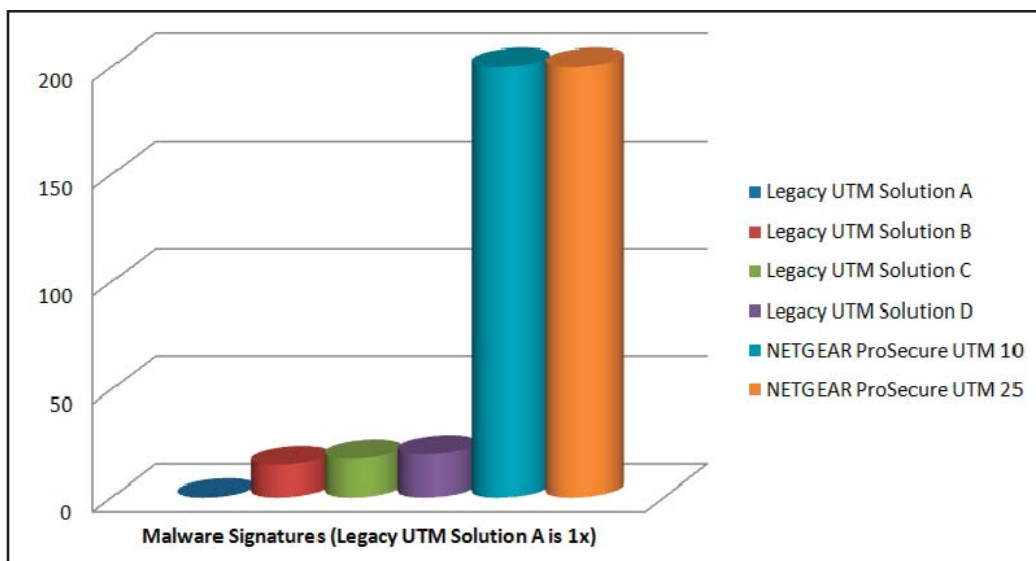


Figure 2. UTM Malware Signature Library Size Comparison

[†] Based on NETGEAR internal throughput measurements done on 4/8/2009

图 2：UTM 恶意软件特征库大小对比

拥有足够的吞吐量是不够的，UTM 解决方案还必须拥有不错的安全技术，以便有效地保护商用网络的免受多个载体的持续的威胁。

反病毒效果	传统 UTM 解决方案 A	传统 UTM 解决方案 B	传统 UTM 解决方案 C	传统 UTM 解决方案 D	NETGEAR ProSecure™ UTM
	无	RBL	基于云的分布式检测	RBL	混合云的垃圾邮件检测
			手动 Email 过滤	手动 Email 过滤	RBL
					手动 Email 过滤
总体	无	差	一般	差	极好

图 3:UTM 反垃圾邮件对比

NETGEAR 的 ProSecure™ UTM 采用了全功能企业级的恶意软件扫描引擎，用于扫描数据流的病毒，间谍软件，蠕虫，特洛伊木马，键盘记录器，以及其他网络和电子邮件的恶意软件。它包括了先进的扫描算法，全面的病毒/恶意软件特征库，是传统 UTM 解决方案的 200 倍以上。

绝大多数传统的 UTM 解决方案反垃圾邮件功能不足。许可基本特性如实时黑名单 (RBL) 只作为唯一的垃圾邮件检测方法，而另外一些厂商则删除了反垃圾邮件过滤的功能。NETGEAR 的 ProSecure™ UTM 的特性是采用云分布式垃圾邮件分析技术的一种混合的云

架构。这种形式的垃圾邮件检测是非常适应新类型的垃圾邮件，很少或几乎没有误报，而且并不需要用户手动调整。

通过这种方式解决小型企业的安全需求使 NETGEAR 能为他们提供他们与大型企业相同级别的安全，同时不会使他们的网络受到令人难以接受的延迟的影响。NETGEAR 的 ProSecure™ UTM 与现在的 UTM 设备完全不同的是，在没有影响网络带宽的情况下，提供一套全面的强大的安全功能的解决方案用以取代现有的 UTM 产品。

结束语

今天复杂的基于互联网的安全威胁，需要强有力的，多层次的安全解决方案，以提供有效的保护公司的网络。UTM 厂商提供全面的保护，在较大的风险中更有利于把更高的利润商用网络客户。解决他们的实际的安全需求，安全厂商必须提供真正的 UTM 解决方案与全面的安全。

随着一个完整的安全解决方案，使用最好的品种的安全技术，NETGEAR 的 ProSecure™ 的 UTM 的为商用网络提供全面的所有功能于一身的保护，先进的硬件和专利的串流扫描技术，避免了瘫痪网络延迟伴随传统的 UTM 解决方案。所有这些，再加上一个直观的图形用户界面，方便设置和管理，使 NETGEAR ProSecure™ 的 UTM 设备满足商用网络的需要。

NETGEAR® ProSecure™安全网关设备解决方案

ProSecure™ STM 和 UTM 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 和 UTM 平台使用下一代混合云分布式 Web 分析结构,不但查找本地缓存的 URL 网址,而且能在云中查找数亿条 URL 网址,从而在实际应用中提供无限制的覆盖范围。URL 网址的被分为 64 个不同的分类。禁止用户访问被认为不适当的网站,减少下载威胁到企业的可能性,同时提高员工的工作效率。

ProSecure™ STM 和 UTM 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。

ProSecure™ STM 和 UTM 安全网关设备采用特有的技术,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 和 UTM 安全网关设备提供了简单的安装和维护。STM 是可以在在现有网络架构无缝集成的一个透明网关,而 UTM 是一个集所有功能于一身的安全解决方案,能取代现有的防火墙或路由器,任一个解决方案都为您的企业提供所有安全软件,而没有每用户许可的要求。