看不见的威胁: 网络中的IPV6

随着操作系统种类的增加，服务器和主机均装有 IPv4 和 IPv6 双栈，你需要意识到在你的网络中已运行有 IPv6 这一事实。本文将解释为什么在你的网络中可能有 IPv6，及为什么拥有适当的工具可使网管专业人员迅速识别相关设备并确保网络的完整性。

目录

福禄克网络
学习更多的关于 IPv6 的测试，访问 www.flukenetworks.com/ipv6

为什么 IPv6 已可能存在于你的网络中?

IPv6 流量不可避免

因特网的爆炸性增长和对于额外地址的需求正以极快的速度消耗着 IPv4 的地址，大多数的信息来源预测 IPv4 地址空间将于 2010 年和 2011 年耗尽。使用 IP 地址的大多数设备如照相机，HVAC 控制，告警系统和传感器，也对这种状况有所贡献，此处也只列举了几种情况。

另外，将多个私有地址映射成一个公有 IPv4 地址的 IPv4 网络地址翻译（NAT ）的扩展应用正变得更加复杂，在某些情况下甚至可能防碍如 VOIP 等实时 IP 通讯的使用。因特骨干网路由器可能遭遇性能降级，因为它们需要维护超大的路由表，而这些路由表通常超过 85,000 条路由。

因此，许多操作系统，包括客户端和服务器以及一些应用已经支持IPv4和IPv6双栈架构，如Windows Vista, Windows Server 2008, 及 Apple OS X 10.3 已经缺省安装了IPv6，同时对于没有安装IPv6的操作系统用户也可很容易的自行安装。

IPv6 设备缺省具备为它的每个接口自动分配一个链路本地地址的能力，同时通过使用路由发现协议确定 IPv6 路由器的地址，接入配置参数和全局地址前缀。状态型配置协议如 DHCPv6 的缺少将无法预防 IPv6 设备为它的每一个接口配置 IPv6 地址。

隧道机制

现有 IPv4 网络很容易受攻击 ––– 若只有 IPv4 防火墙，黑客通过建立 IPv6 隧道轻松穿越防火墙，攻击内部网络

你可能认为“在我的网络中并没有 IPv6 的业务，为什么我要关心安装了 IPv6 的终端设备？”然而，隧道技术与此相关— 每一种操作系统都支持这一技术，并在 IPv6 协议栈安装时自动激活。隧道使 IPv6 通过 IPv4 连接传输，反之亦然；有时需要被加密，可能使用匿名（私有）地址，而非允许你追踪主机 MAC 地址的 EUI-64 结构化接口识别符。（注：EUI-64 地址由设备 MAC 地址构成，并在 MAC 地址的前 24bit 和后 24bit 之间加上十六进制的 FF-FE）。

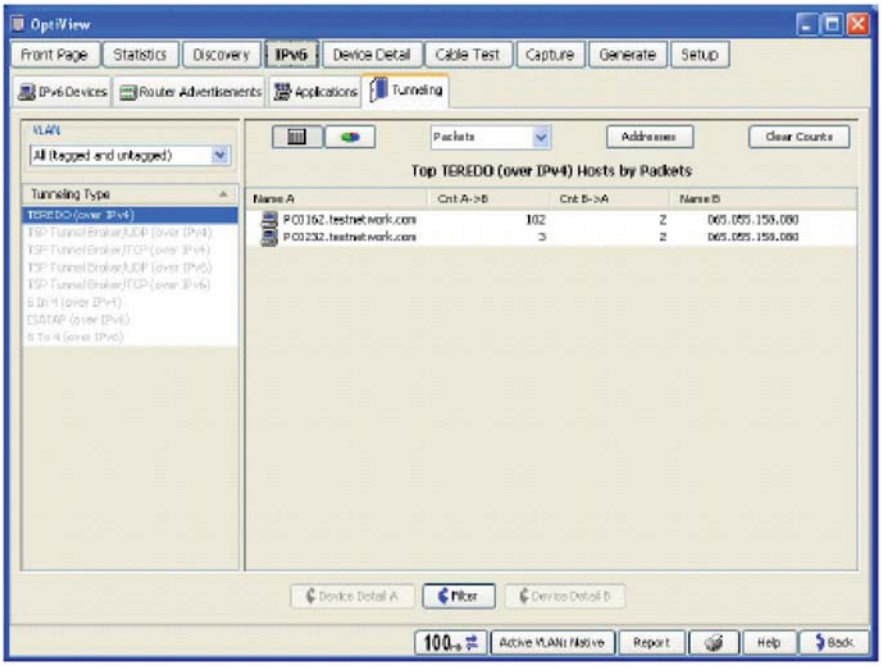

图 1 - 隧道视图

某些通用的隧道机制包括：

•Teredo- 用于 IPv4 因特网的连接。此协议将在防火墙上开一个孔洞，允许穿越网络地址翻译。然而 Teredo 通常用于家庭的网络，而在公司网络中不常用。

•建立于TCP，UDP，IPv4和IPv6之上的TSP隧道代理。这种方法使用服务器或路由器中隧道代理穿越NAT。

•6in4 是一种从 IPv4 到 IPv6 过渡过程中因特网穿越方法，意指将 IPv6 业务封装在明确配置的 IPv4 隧道中。这也被称为‘静态proto-41’，基于它所使用的端口号及终结点静态配置的事实。不应将此种方法与 6to4 或 6over4 混淆，后两种方法有着相似的名字但却是不同的方式。6in4 将整个 IPv6 包直接封装在 IPv4 的包头后，在 IPv4 的包头中的‘协议’字段设为 41， 指示 IPv6 在 IPv4 中（IPv6-in- IPv4）。

•站内自动隧道寻址协议（ISATAP）隧道提供客户端到客户端隧道或客户端到路由器隧道，且不需手工配置。

•6to4 – 使用 6to4 中继不需配置明确的隧道即可连接到 IPv6 网络。此种方法通常位于公司外部的第三方，使用 IPv6 地址前缀 2002::/16；这在 Windows 中被缺省设置。

在隧道中涉及到的风险为 – 如果你在你的内部网中有一个本地隧道，这将有较小的风险，但是如果你有一个本地设备，而此设备的隧道终结点在你的网络之外，它将可能允许外网访问你的内部网络，这将可能不被防火墙和入侵检测系统保护。

其他潜在的 IPv6 攻击

有许多其他的潜在攻击你需要注意，例如虚假路由器通告。这可能是不应在你网络中存在的非路由器通告子网地址，通常只是由 IPv6 路由器或主机配置错误引起，或者，更重要的是，这可能表明这是恶意行为。通过发送虚假路由器通告，攻击者假装成一个路由器，而使所有在这一子网上的主机发送的业务离开本子网，而发送到攻击者主机所在的子网，导致中间人（man-in-the-middle）攻击。这同样适用于 DHCPv6 欺骗，因此使用提供 IPv6 状态型地址的设备也很重要。

另外，既然 IPv4 比 IPv6 成熟的多，操作系统倾向于将 IPv6 端口保留开放，因此能够执行 IPv6 端口扫描以便识别那些开放的端口非常重要，在 IPv6 协议栈中 IPSec 被作为一种标准支持，设备可以更容易的加密端到端业务，防火墙无法检测到包的内容。

底线是－试图使用恶意业务攻击网络并不需要新的方法，只需要你网络中有 IPv6 激活的设备，这将允许攻击者（外部或内部的）通过传统的方法闯入你的网络，从你的网络中通过 IPv6 提取数据而不被觉察。

便携式分析仪如何帮助你

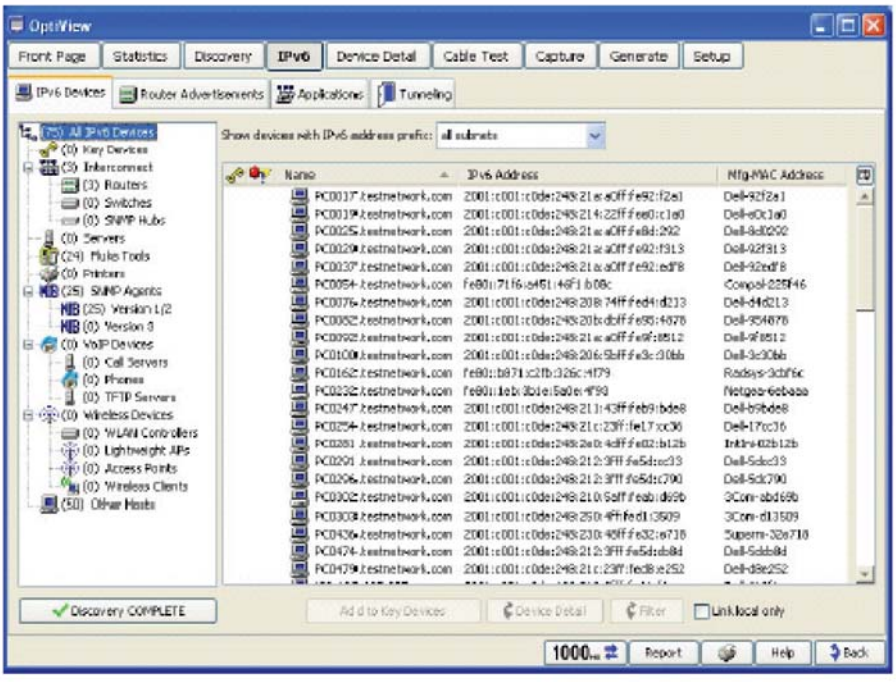

图 2 - IPv6 设备发现

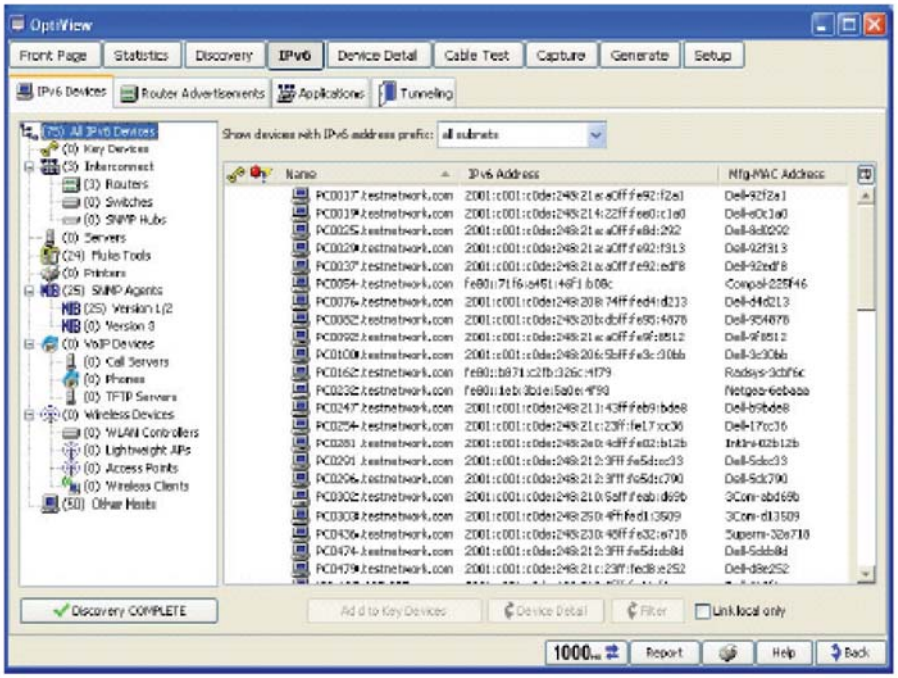

图 3 - IPv6 路由通告

使用便携式工具，网络专业人员可连接到每个子网中，很容易的识别IPv6 激活的设备，并在必要时采取措施关闭网络中的漏洞。

因为确保网络运行顺畅是一个网络工程师的基本职责，安全有时可能是第二需要关心的事情。通过使用工具，可同时提供灵活的对于日常维护及潜在的IPv6 和其他安全弱点的处理，网络工程师可以发现潜在的问题区，检测并改正它们，同时保持网络功能在一个高的水准上。

因此，每个网络工程师应该有如下问题的答案：

- 哪个设备使用了 IPv6，它们在和谁通信?
- 哪个 IPv6 端口是打开的，从而可造成潜在的攻击威胁?
- 哪个设备提供状态型 DHCPv6 业务?
- 是否有任何“非路由器”通告 IPv6 地址前缀?
- 是否有任何隧道打开，如果有，终结点是什么?
- 是否有设备使用私有地址?
- 是否有设备使用端到端 IPSec 加密，从而通过防火墙时不被检测?
- 是否有设备在扫描 IPv6 端口?

解决方案：集成便携式分析仪

为了对所有这些问题提供答案，网络专业人员需要一个设备，既能够被动地也能够主动地发现IPv6设备和服务。市场上有很多设备都能够提供被动发现，这主要通过监控IPv6业务，捕捉IP和MAC地址，但却不能基于识别的协议将设备分类。OptiView系列III分析仪是唯一提供主动IPv6发现的设备，这通过发送路由器申请请求以便识别子网所有的IPv6前缀，同时通过发送邻居申请请求以提供子网中其他IPv6设备上的信息。为了得到额外的信息，OptView提供路由器内IPv6网络-到-媒体（Net-to-Media）表的可见性（等同于IPv4 ARP表），以便发现所连接子网的链路-本地地址。另外，OptiView系列III还能访问思科路由器前缀表以提供其它子网的信息。

OptiView分析仪配备有几种重要特性允许网络专业人员从内部解决安全问题：

任意字符串匹配

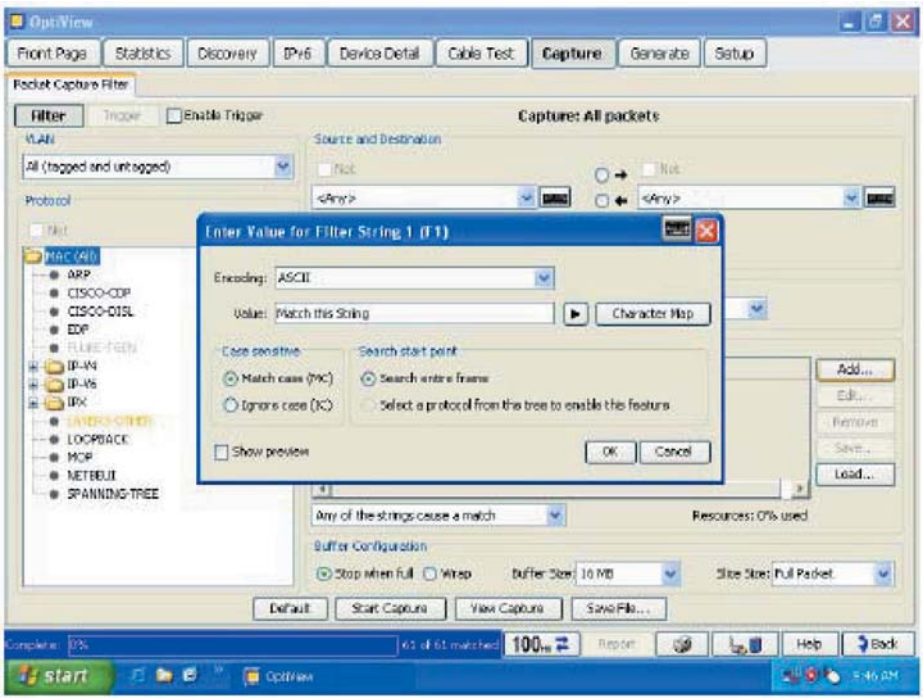

图4 - 任意字符串匹配

OptiView分析仪允许网络工程师使用任意字符匹配功能匹配任意单词或短语®不管数据包，负荷，或头部的位置－且实时的。一个工程师能在非加密的电子邮件中，web页中，文件传输或文档中，检测包含某单词或短语的业务。这允许工程师识别网络的不正确使用，同时基于文件内容或文件名字检测受限制文档的下载。任意字符串匹配特性，和深度协议识别，也帮助工程师识别和跟踪网络中不被允许使用的应用，例如占有宝贵带宽的流媒体，或带有安全危险的P2P业务。任何时候可定义最多8个触发器或滤波器，允许工程师在时间允许时分析捕捉到的信息。

无线欺诈设备识别和定位

图5 - 使用OptiView 集成网络分析仪进行欺诈搜索

OptiView 分析仪可快速追踪到欺诈和非安全设备，包括 ad-hoc 网络。音频及视频指示将网络工程师引导到入侵设备的位置。

用户帐户限制和移动硬盘

OptiView 分析仪的用户帐户界面允许工程师为每个单独用户添加修改分析仪安全信息。这可防止对于分析仪的某些特性的非授权使用，从而更容易与政府条文相吻合，包括 HIAA 和 SOX。潜在的关闭的特性包括：包捕获和解码，业务生成，远端用户接口和分析仪配置。OptiView 系列 III 集成网络分析仪搜索到的网络信息可被存储在可选的移动硬盘中，从而确保任何存储在网络分析仪硬盘上的敏感性数据永远不离开相应的环境。只需更换硬盘，分析仪即可在不同级别的分类环境，分类和未分类的系统或私有和公共网络中来回使用。

便携式集成网络分析仪的商业应用情景

OptiView 系列 III 集成网络分析仪帮助网络专业人员管理 IT 项目，解决网络问题，支持 IT 提升，从而得到减少的 IT 费用和提高的用户满意度。这给你一个对于整个网络的清晰的认识- 提供你网络中每一种硬件，每一种应用和每一个连接的可视性。没有其他便携式工具提供如此的可视性和一体化的能力帮助你：

- 部署新的技术和应用
- 管理并验证基础架构的变化
- 解决网络和应用性能问题
- 保证网络的安全免受内部威胁

这一工具向你展示当前你的网络的状况，帮助你准确地评估网络是否已具备了你当前或将来要做的改变的准备条件。OptiView 的强大功能将给你对于网络的前瞻和控制。

福禄克网络

学习更多的关于 IPv6 的测试，访问 www.flukenetworks.com/ipv6

总结

新的因特网协议 IPv6 代替当前的 IPv4 可能还需要一些时间，但是许多网络可能已经通过设备中激活的支持 IPv6 业务的机制对攻击开放。

网络工程师如果没有设备分析他们的网络，以便确定在他们的网络中与安全 IPv6 相关的有什么，及什么已被激活，那么这不仅将他们自己向攻击者开放，而且可能被认为不符合 Sarbanes-Oxley, HIPPA 及其他规则，即使这些规则不需要审核员验证 IPv6 是关闭的。

我们不提倡您关闭 IPv6，因为你必须面对它，在不久的将来你将需要将你的网络过渡到 IPv6 ®，我们只是想要你意识到当前有些什么在你的网络中，以及如何能够使网络安全，并且现在学习明天当你部署 IPv6时需要做什么。

IPv6的安全威胁可能是无意识的，但他们不能再隐藏在后面…这种危险是巨大的。为了处理这些威胁网络专业人员将得益于一个新的工具，这个工具帮助找到网络中的弱点，允许他们追踪到潜在攻击。OptiView 系列 III 集成网络分析仪更额外增加了便携性的分层保护。通过这些额外的保护，网络专业人员能够发现并处理这些可能危及网络安全－甚至商务的潜在问题。

福禄克网络

学习更多的关于 IPv6 的测试，访问 www.flukenetworks.com/ipv6

网 络 超 级 透 视
NETWORKSUPERVISION

美国福禄克网络公司
http://www.flukenetworks.com.cn
http://www.flukenetworks.com

北京办事处：(010)65123435
上海办事处：(021)61286200
广州办事处：(020)38795800
成都办事处：(028)85268810
西安办事处：(029)88376090
武汉联络处：(027)85743397
重庆联络处：(023)89038590
沈阳联络处：(024)22813669
深圳联络处：(0755)83680050
北京维修站：(010)65123436
全国免费服务热线：4008103435

中国印刷 8/2009 1609426