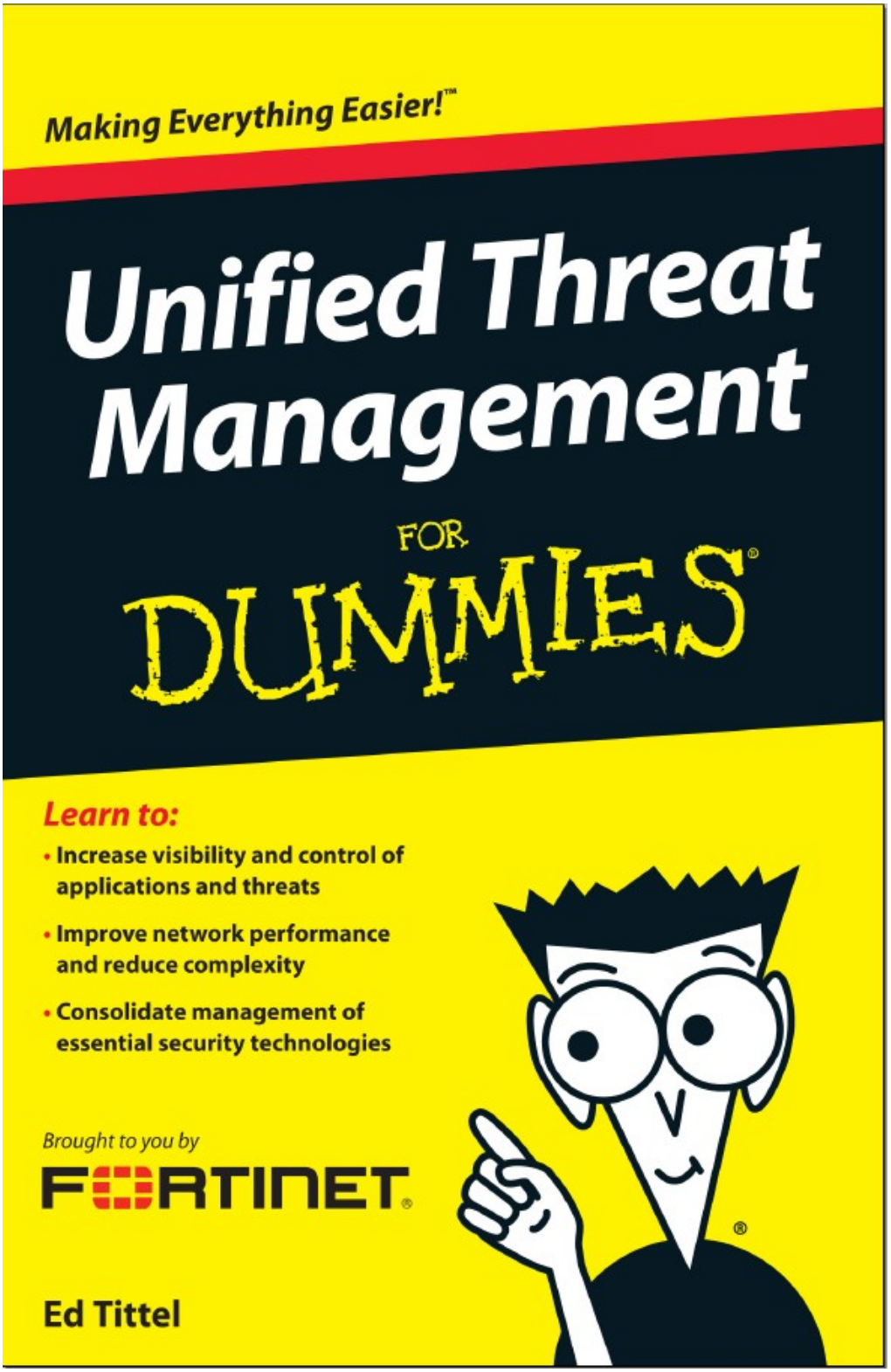
UTM（统一威胁管理）阿呆书



本书是 **Fortinet** 与你分享的一本有关 **UTM**（统一威胁管理）的深入浅出的探讨与说明。书中我们站在网络安全设备选购者、**IT** 技术管理者的角度谈到了网络应用以及安全的演变，防火墙以及防御技术的进化，以及如果是你来选购网络安全方案会怎样？内容简单明了。相信每一位读此书的人都会深有感受。

每本阿呆书都有图标标识说明，这本也不例外：

记着此段文字，有益于在 **UTM** 世界中继续阅读。

我们有时候会分享一些技术定义说明，如果你不感兴趣，可以跳过。

有益网络安全的关键点哦。

目录

第一章

综合网络安全需求所在

- 守护不断变化的网络安全
- 驾驭应用
- 抵御犯罪软件

在如今这个移动无所不在的世界里，网络无时不刻在变化。新的服务方式、网络接入方式、甚至新的工具设备都以迅捷疯狂的步伐出现在网络中。仅几年之前谁能够预见 Twitter 与 Facebook，亦或 iPad 与 Android 智能手机的影响？ 因此，所有不同规模的公司、企业、机构均面临维护控制网络与安全策略的挑战。不幸的是，尽管软件、移动设备、上网工具、用户习惯发生了如此的变化，很多公司仍然采取传统的方法维护网络安全。传统的方法不能与最新的趋势相适应，给当下的威胁与漏洞留了空子。为了保持应对不断变化的网络趋势，所有的公司机构都要采取不同的方式。在我们讨论保持与趋势同步的方法之前，在本章节，我们要简单回顾下过去几年网络的演化，以及网络安全定义的变化；其中，一些是好的方面，一些不尽人意，而另一些则十足的令人厌恶。

好的方面：更多更好的网络接入方式

网络化与安全技术的进化与惊人的传播，对信息化领域与用户带来了许许多多的好处。 这些好处包括无时无刻无处不在的网络访问。我们正在使用不断扩张的带宽，通过无线或有线访问更快的获取更多的数据/信息与服务。与此同时，各种各样的应

用（Apps）层出不穷提高了生产效率。

更快且安全的远程接入

如今，远程用户有多种方式从全世界各地访问公司的数据信息。可以使用与网络连接的任何设备包括智能手机、平板电脑，访问防火墙之内公司的系统与网络。

应用大爆发

每天每刻有大量的应用迸发，包括工具类型、移动软件、游戏以及五花八门的其他应用。 互联网速度的提高与随时随地的访问，使很多琐碎的内容能够面对呈现给终端用户。移动设备平台的构建例如 IOS与Android系统，将针对企业的应用从桌面或笔记本PC延伸到智能手机与平板电脑。

- ✓ 访问协议与兼容标准的改进使得如今的应用可以提供到网络“后端”与内部数据资源的更好的访问。这对于雇员、合作伙伴、供应商、客户之间的效率都是飞跃性的提高。
- ✓ App提供的模式与内容在过去十年也发生了显著的变化，应用起源于网络内部（也就是“on-premise”），亦可以是驻在云端，由应用服务提供商提供并管理。或者一些情况，可以是由以上两种方式的结合而提供的（也就是“hybrid”混合部署）。
- ✓ 最后，在商务活动中的社交媒体例如YouTube、Twitter、Facebook 与Google＋的不断增长的使用深刻的反映了潜在的客户、合作伙伴以及代理商收集数据的方式与地点的改变，从而影响了购买决定并建立了品牌意识。 在企业网络中发生了诸多好的方面的变化，在现有的系统架构与信息资产中，许多新兴事物涉及创新的技术与使用。但是这些变化也会是保持与维护系统安全增加负担，同时需要进一步思考与新的应用、访问方式与沟通方式相符合安全防御。

坏的方面：“混水难御”

同样，持续的应用爆发意味着，新的应用出现并在有组织有规模的系统与设备中运行。多数情况下，这些应用的使用不受网络管理员的监控，无计划性、无许可、甚至无知情同意的情况下出现。更为恼人的是，这样的应用潜入网络中带有未知的、可疑的或甚至完全的恶意内容。这确实非常的糟糕。

新应用难以检测

这也是为什么今天的网络应用程序的爆发使用是目前各种规模的公司机构正在面临的真正问题：传统的防火墙无法侦测到这些新的应用。传统或“第一代”防火墙根据端口号或协议标识符识别和分类网络流量，并执行相关的策略。

这种方法只对使用特定的端口请求或传输内容或要求使用独特和易于辨认的网络协议的程序有用。多年来，这是互联网接入服务交付和应用访问的标准方法，并协助保证不同应用与网络之间的互操作性。

使用特定的端口号或协议的应用程序，网络管理员也比较容易能够阻止不需要的流量：管理员只需创建一个防火墙策略基于端口号或协议类型，屏蔽该流量。例如，为了阻止通过网络传输电子邮件，网络管理员可以设置阻止邮件传输协议（SMTP）的端口25。如果管理员想阻止文件传输协议（FTP）流量，一种不安全的文档交换方式，管理员会阻止端口20和21。基于浏览器的应用程序经常使用的只有两个端口，这两个端口分别与用户的工作效率有关，且会产生大量的访问流量。这意味着80端口用于HTTP（超文本传输协议）或443端口用于HTTPS（安全，加密的HTTP版本经常用于商业交易或任何涉及敏感数据，如网上银行的Web交互）。

这意味着什么：对于传统防火墙来讲所有基于浏览器的应用程序的流量是完全一样的。传统防火墙不能区分各种应用程序，相应就没法实施策略区分哪些是不当的、

不需要的或不适当的程序，而是不设防的允许这些应用程序。在这些端口屏蔽流量或者协议，会导致阻止了所有基于web的流量，包括合法的商业用途的内容和服务。

应用爆发带来的混乱

如今持续的应用爆发意味着每一天越来越多的出现传统的防火墙不能检测或控制的应用程序。然而，建立和维护控制不仅是可取的，也是彻头彻尾的必要，否则接下来便是未经查看的应用程序的横行肆虐。 基于Web的应用，因其能够通过传统的防火墙而不被检测，这不仅是可以给一个网络带来恶意或有害的行为和内容的进口，同时也可能是专有技术、受管制的或者机密信息被泄露的出口。这些进进出出的数据和内容会对知识产权与自身的竞争优势带来泄露的风险，以及可能的法律责任或合规失败。这可不妙哟！

考虑下这些未经过检测的应用爆发对一个网络带来的令人生厌或者不良的负面影响，如下：

- ✓ 暴露于恶意内容：用户创建的内容包含了非常广泛的威胁，例如灰色软件或链接到恶意站点的连接。 用户内容可能是一条Twitter、一篇帖子、Flickr照片上传、或是一条餐馆的点评，都可能包含殃及用户系统或甚至整个网络的恶意代码。常见的风险包括网络访问者被要求下载驱动程序而含有的到恶意站点的链接，在用户不知情的情况下下载了恶意内容。
- ✓ 不必要的带宽消耗：带宽密集型的基于网络的应用，例如YouTube可以导致拥塞网络和阻碍关键业务内容的交付。文件共享应用，由于文件大小和数量之多以及文件之间的频繁交换，可能会导致网络陷入瘫痪。
- ✓ 数据泄漏的风险：可提供向外携带文件附件的软件程序可允许员工向外传输敏感、机密、或受保护的组织边界和控制之外的信息。这将带来潜在的民事和刑事责任，以及客户的信任和品牌价值的损失。

当新的应用程序出现在一个组织或机构的网络中时引起的后果是棘

手或危险的 —— 带来的问题是未引发大规模风险之前一直保持悬而未决的风险。

应用是怎样被避免检测和控制的

新的基于网络的应用，往往带来安全问题。 尤其那些避开检测的应用特别危险，因为他们可以在不引起网络管理员注意的情况下带来风险与对性能或者系统与网络的冲击。怎么会这样？这在企业网每日上演，因一些基于web的应用可以利用隐匿或含混的技术避开检测。

- ✓ 一个应用程序可能通过隧道出现在另一个应用程序中使自身合法化并披挂伪装出“信任程序”的斗篷。 想想这样的隧道程序就是披着羊皮的狼，你就是它的目标。 如果羊群中只有一只这样伪装的羊，你就得提防着这样的隧道程序带来的问题了。
- ✓ 有些应用采用加密算法，可以防止其内容被查看与识别。除非采取措施检测与处理内容，恶意应用程序可以悄然的移动流量。
- ✓ 其他应用程序可以使用动态端口或伪装成不同的应用连接到一个系统。这样的应用通过特意伪装自身及其流量的技术可以避开基于端口的防火墙规则检测。恶意软件，尤其是木马程序，就是使用这种技术来逃避检测和越过网络边界输出敏感或机密数据而臭名昭著。 这些容易让数据失窃或泄漏的伪装和回避技术是公司机构网络的一大痛事。 由应用而传播的、以获取机密信息、被管理以及规范的数据为目的的新一代威胁是眼下最明显紧迫的存在的风险。

丑陋的：网络犯罪与破坏

今天的威胁环境中充满了大量怀有不良意图的危险份子。除了恶意软件渗入或数据损失的威胁之外，专业的犯罪分子已经通过在线的方式从事其讨厌的交易。 网络犯罪成为威胁大观中日益增加的一部分，但它不是唯一一种可以针对企业，组织和个人攻击。

其他常见的网络犯罪包括恶意的恶作剧（非利益驱动，而是破坏与窃取带来的兴奋

感），来源于对政治或个人的隐私的恶趣味。正值我们写这本书时，最近的新闻报道是是关于一个以“匿名者” 或“Lukzsec”命名的hacktivist的小组利用威胁漏洞进行恶搞的事件。这些阴影下隐秘群体的目标是各种机构组织的用户数据和内部网络内容盗窃与披露，而作为对一些政策、政治党派与社会机构的反对。

同时，从互联网上的阴影中不断增长的网络犯罪网络，通常扎根在网上执法不严或不存在网络立法的国家内。通常情况下，网络犯罪公司通过共享其获取而抵消犯罪行为。这些网上黑市的首选工具是犯罪软件和方法的服务产品。在接下来的章节中，我们将探讨互联网中最丑陋的元素。

犯罪软件的定义

犯罪软件是一类包含源代码和开发工具包的软件，能够帮助罪犯份子或其从事的活动用来攻击系统或建立由僵尸计算机组成的网络而从事交易。创造这些工具的黑客们像合法的软件开发公司，对其“客户”提供各种授权支持或每年签订合作合同。

提供服务性犯罪走得更远，“激进”份子付费窃取数据或发动网络攻击。这些“激进”份子没有明显依附任何组织或处于某种原因（除了赚钱）。这样的服务提供商作为承包人通过网上竞价对出价最高的买者提供犯罪服务。

僵尸网络与信息战

一个机器人程序是已经被犯罪份子通过恶意软件攻破的个人计算机。每一个这样的计算机被称为BOT（“机器人”的缩写），这样的计算机的集合被称为僵尸网络。犯罪组织可以创建和运行自己的僵尸网络，但最大的僵尸网络（其中包括几十万世界各地的机器人）通常是可供租用的。运行僵尸网络的骗子，被称为宿主（botmaster）或bot牧人，他们从从事犯罪活动的客户接受指示，而后设计僵尸网络进行各种犯

罪活动。

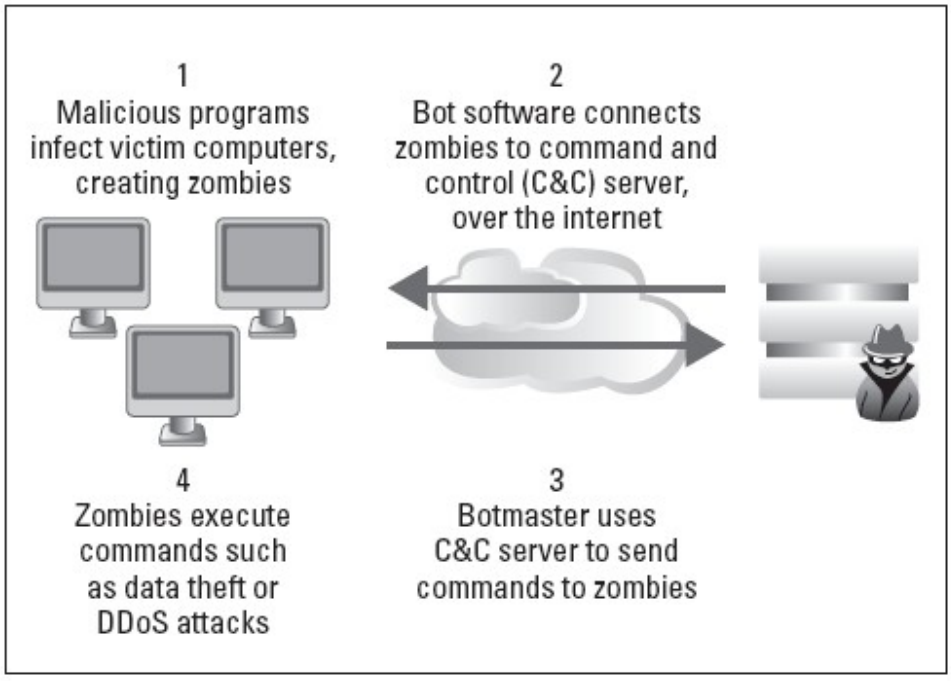


图 1-1: 僵尸网络示例

各种公司，事业单位，政府机构，和其他大型组织都是BOT攻击的牺牲品。 任何一个案例中，突破边界网络总是从塞入网络中的一个BOT开始的。受感染的计算机可以作为抢滩攻击其他系统（内部或外部），窃取信息，转移资金，或进行其他非法活动。下面是一些常见的形式，往往会在边界网络内产生更多的bot，也许超出许多IT专业人士准备接受或相信的范围：

钓鱼式攻击：公司网络内的一个雇员或其他操作计算机的人点击邮件中的一个链接或其他社会媒体信息与访问一个钓鱼网站。信任状将被钓取或窃取。通常情况下，该信息被用在第二阶段的攻击，利用一点社会工程学技巧去反串其他受害者。

- ✓ 搜索引擎优化（SEO）攻击：SEO攻击是由黑客在大众搜索引擎的搜索排名靠前的站点中植入恶意网站而实现的。 通过使用一个僵尸网络，使用流行的搜索

词组创造数以十万计的Web服务器和网页。一个潜在的受害者查询一些热门话题，点击了一个恶意的搜索结果，随之落地在一个虚拟的网站后被重新定向到一个恶意网站。一般的合法搜索网站都被作为目标，因其可以产生大量的点击量，以及带来潜在的受害者。与钓鱼式攻击一起，Bot的创建是渗透与攻击网络的大门。

- ✓ 牵连合法网站：合法网站在网站运营者没有发现的情况下因各种方法手段而受到牵连。例如，网页的广告被第三方利用将访问者重定向到恶意网站，在网站中注入恶意代码将访问者重定向到恶意网站，或取代合法的HTML代码包含恶意软件。
- ✓ 内部感染：海量存储设备，从随身碟到电子相册，都是可以携带病毒的载体。当这些设备一旦接触到一个网络，病毒便会通过一个自动运行的功能执行。然而，一些僵尸网络可以通过需求促发而感染受害人移动设备中的合法文件。

勒索软件：付钱或付出。。。。代价！！！！

勒索软件是一款“捆绑”设备直至“勒索费”支付了为止的一款恶意软件。勒索软件的目标是负载关键任务的系统或应用程序，一旦安装，非常难以摆脱。按照设计，没有开发者设计的密钥或代码，勒索软件几乎是不可能卸载的。原始的勒索软件可以从系统中清除，但是造成的损失是除非雇佣发起攻击的人而无法恢复的。

以下是勒索软件发生的案例：

当勒索软件感染了一个系统，会通过加密各种关键文件（通常使用严格的非对称加密）使系统陷入不可用的状态，并使恢复/修复功能失效。接管这些关键文件或性能后，将现在的系统状态展示给受害者。除非并直到受害者支付赎金，否则文件将继续保持锁定状态，系统无法使用。

这给了一些勒索者无以伦比的工具。只有在支付赎金后，受害人才可以获得解锁系统或恢复访问重要文件的密钥。其他勒索软件将系统锁定在启动项之外，所以根本无法进入操作系统进行系统恢复。 赎金通常浮动在100美元，但能跳跃的高太多，

如果这个目标足够高调。

当用户发觉他或她在阅读赎金支付须知时，数据已被禁用加密或基本功能已失效，勒索动作基本上完成。传统的防火墙对勒索软件的威胁基本是出于无能为力状态。

钓鱼与鱼叉式钓鱼攻击

在除了前面一节“僵尸网络和信息战”中所述僵尸网络的构成以外，直接的钓鱼攻击也时常发生。尽管这些攻击可能形成一个僵尸网络，但它们经常涉及敏感信息和/或管制信息不经意的披露。 这些数据一般包括信用卡号码和凭据、用户帐户名和密码这样的财务信息、以及银行，券商或其他金融服务提供商的金融账户信息。

钓鱼攻击形成的初始事件可能只是一个公司的雇员或客户点击了一封欺骗性的电子邮件、一条tweet信息、一则Facebook的帖子等等。这一动作可以使一个人访问看起来真实的要求登录的网站，否则将暴露信任状信息。

电脑犯罪分子使用此信息来冒充受害者窃取金钱，服务或其他有价值的东西。普通的钓鱼攻击并不针对特定的受害者。大多数钓鱼攻击会创建能够吸引尽可能广泛的观众的邮件作为诱饵。这些消息、帖子、tweet等等将得到广泛的传播，受害者或多或少被选择自己作为攻击目标。

然而，企业和机构组织越来越多地被作为一个钓鱼目标而落入攻击。众所周知，鱼叉式网络钓鱼这类攻击都是明确冲着某些员工或某个组织的成员而发起的。这些攻击通常设计伪装为来自内部用户或来自可信赖的合作伙伴或服务提供商（内部信用社，健康保险提供商，等等）。

鱼叉式攻击使用一点社会工程学技巧巧妙的说服用户打开链接到恶意网站或附有灰色软件附件的电子邮件，tweet信息或Facebook帖子。

有些时候，不是一个链接，而是一个通过邮件甚至电话发出的直接的沟通请求（也就是鱼叉式攻击）。修辞巧妙有趣的信息将吸引个人或小到一个特定的目标受众，提高了潜在受害者越来越吞下诱饵的可能性。犯罪分子将利用网络中有关在社交网站张贴个人日志与帖子的丰富资源，设计鱼叉式信息的内容。 鱼叉式钓鱼攻击也利用容易被感染的文件（PDF，DOC，DOCX，xls或xlsx格式，这些流行的恶意的有效载荷的文件格式）从而使系统感染恶意软件获得所需的信息。

例如，一些鱼叉式钓鱼攻击已经被报道以大型企业内的会计或金融服务专业人士为目标，因为这样的人最有可能为公司执行电子资金转移的业务。对这些人群设计的钓鱼信息会通常要求这些人打开一个文件,以检查一个所谓欺诈或可疑的交易细节。打开的附件会链接到恶意软件，会感染目标系统。

从此，与目标人群相互交互的任何系统都将被攻击者所密切监控。信任状与账户将在登录时被窃取。网络犯罪分子还开发了复杂的恶意软件配合这些使用攻击。恶意软件使用的技术称为注入式,它允许攻击者注入消息和/或问题和字段到诸如安全的银行网站实时的浏览会话中。这样一来，看起来是来自合法网站的访问实际上已经被注入恶意代码。这是一招是网络犯罪份子惯用的从受感染目标获取更多信息的方法。 参见图1－2攻击过程演示。

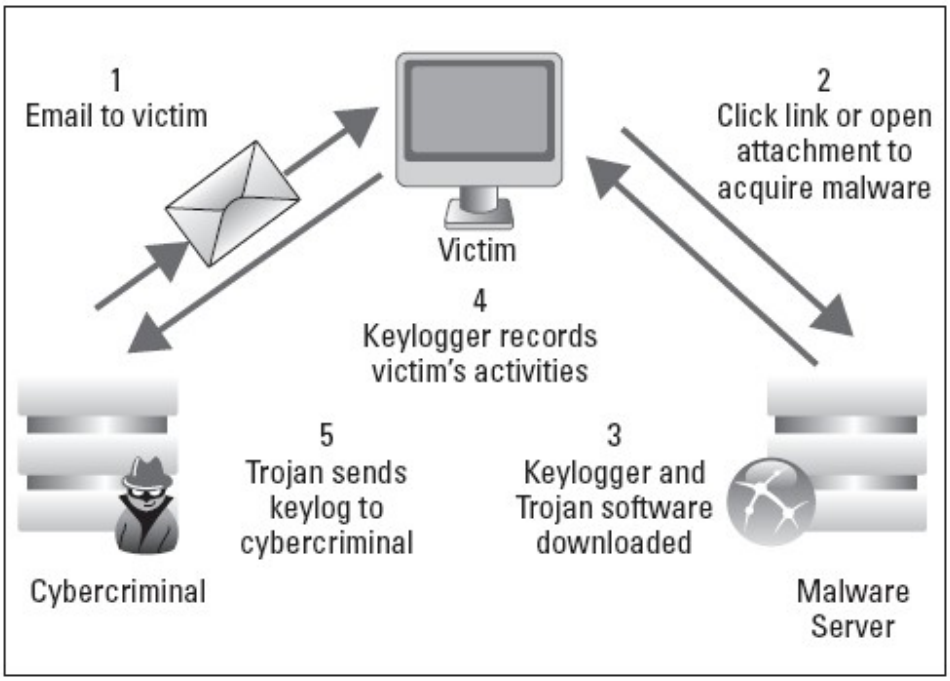


图 1-2：鱼叉式攻击是如何感染受害人计算机系统的

传统的防火墙因缺少检测内容并防止对恶意网站访问的能力，无法防御这些威胁。同样对网络犯罪的其他形式也不能够防御。一种不同的防御方法与工具需要应运而生。

在第二章，我们将叙述下阻止这些威胁的需求。

第二章

传统防火墙为啥挡不住如今的威胁

- 缺乏网络安全性带来的问题
- 单机安全设备是如何削弱了网络的可见性
- 通过单机应用评估防火墙性能
- 你网络中传统防御的花费
- 更佳的防御解决方案需要的具备的特点

基于web与应用的流量巨大，至少可以说过往的防御内部网络的安全技术面临越来越多的挑战。网络攻击已经变得愈发频繁与严重。每天，我们都能读到有关网络犯罪分子的攻击已能够避开检测以及出现了更多的获取我们信息的方法。他们都占上风了？

当网络攻击与其后果变得更加危险以及损失昂贵，企业以及公司机构开始从惊愕中认识到现有的安全架构已经跟不上威胁趋势了。传统的防火墙和安全设备已经失去了阻止此类流量的能力。这意味着，现行的工具和技术不能防止影响或破坏网络的最坏和最恶毒的攻击。

本章着眼于传统的安全技术和当今的网络流量的构成是如何影响了其防御能力。同时，我们探讨下多个传统安全设备组合的使用削弱网络的性能和增加的总成本（TCO）的问题。

充其量是不充分的防御

这些网络设备，粗犷的安放在各个内网的边界， 面对保持如今的网络安全要做的太多。 检测并管理通过网络边界的流量并执行策略、阻断病毒与恶意软件、防御潜在的入侵与攻击、防止未经授权的访问，如此这些已经变得老生常谈。 同时，监控出站网络流量、过滤各种入站流量，并查守和阻止潜在的入侵，对DOS攻击快速应对；这些都是必需的。

这是一个多样化的安全和网络技术需要去操作并管理。这也难怪，传统防火墙的弱势就在无法应对激增的流量且许多不同的过滤机制需要实时应用并调和。

传统防火墙的问题

首选最基础的网络防御就是防火墙，也就是对出入网络边界的流量检测设备。当互联网广泛开始使用，防火墙是最开始广泛部署使用的网络安全技术。防火墙的工作是查看流量并判断出站入站的被允许的流量。

但网络流量的复杂程度在过去10年间发生了太多变化（参见第1章）。互联网中以及公司网络中很大一部分流量是基于web的。

由于现代应用流量与日常网络接入混在一起，传统的基于端口的防火墙对于现在最常见的类型网络流量已经变得无视。这意味着传统防火墙不能区分使用相同的端口不同类型的流量，检测不到通过隧道的应用，以及加密后的数据包。甚至不能屏蔽使用非标准端口号溜入的流氓应用。

不断变化的防火墙技术仍然跟不上威胁出现的速度

由于简单的规则过滤防火墙的流量证明是过于宽松，防火墙厂商跟进新的技术要走在不断变化的威胁环境的步伐的前面。防火墙中应用的简单过滤规则被证明过于宽松，防火墙厂商应用的新技术与不断变化的威胁不相上下。因此，防火墙技术的发

展需纳入更复杂的方法以防止新的威胁。

防火墙技术的一个重要进展是代理服务器（或“代理”的简称），可以安插在网络连接一端的客户端与另一端的服务器之间。网络中的代理服务器是透明部署，在转发数据包之前根据设定的策略检测所有的数据包。 数据流中重组所有的数据包，检测全部的文件附件而不是一次只查看一个数据包。

状态包检测防火墙是创建用于跟踪网络连接的状态。状态防火墙从可疑或恶意的连接中识别合法的通信。 只允许有效的、确认的、活动状态的数据包在客户端与服务器之间进行，拒绝其他试图连接或传输的连接。

提供基本的内容检查，深度包检测（DPI）防火墙检查网络数据包的有效载荷或部分数据。深度包检测（DPI）根据数据包负载的类型集合匹配（也就是特征匹配）识别与分类网络流量，可以对病毒与蠕虫提供一些防御。特征检测比只对数据包头信息的识别检测更广泛且有效的控制与过滤。

尽管有这些技术上的进步，防火墙仍然跟不上威胁演化的速度，无法达到防御效果。防火墙每项新技术出现，黑客也随之设计新的逃避技巧。新的威胁只是简单的渗入传统的防火墙并一路向信任网络奔去，肆意的攻击客户端与服务器。网络安全厂商争相创新研发新的技术以对付新的威胁。

单机产品会降低网络安全的可见性

随着时间的推移网络威胁的演化，公司或组织机构纷纷开始在基础机构中添加专门或独立的安全设备（硬件设备或软件）。计划让这些设备能够弥补过去基于端口防火墙的不足而使出的变通方法。

每个设备对症具体的一项威胁：一台设备提供恶意软件扫描、另外一台设备专门执行网站内容和流量过滤。还有检测并阻断入侵的，或添加进行垃圾邮件过滤与邮件处理的设备。将这些设备都置于网络中，且机架上多了半打儿设备或更多，每台设备都要检测通过网络的数据包流。参见图2－1。

所有这些设备（软件或硬件）意在增加传统防火墙所没有的功能来提高网络的安全性。然而，单个技术之间的拼合对网络安全可视性与网络性能可能起到了相反的效果。这些防御威胁的具体技术因自行运行，之间互不兼容，缺乏中央管理和监控。此外，通过每个设备的数据不能汇总并创建完整或整体的查看报告。如果你不能真正看到它端到端，你怎么能管理网络的安全性？

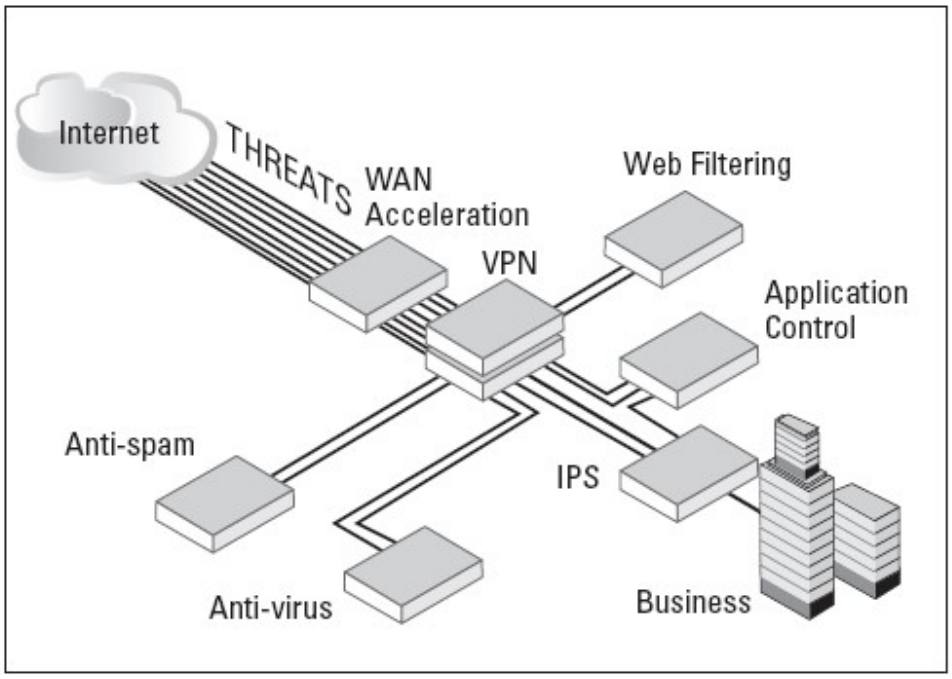


Figure 2-1:多台设备部署应对不同的威胁

当然管理员可以购买另外其他单独的工具在如此纷杂的网络环境中获得良好的安全分析能力。例如，收集网络设备的信息、评估，以确定安全事件，并提供了分析的安全信息和事件管理（SIEM）工具。这种方法的缺点是，虽然增加了能够聚合各

种产品数据分析得到的安全可视性， 但是不能进行集中管理控制。管理员仍然需要单独配置各种单机设备。

当然，还存在有收集、分析和评估安全性和风险的信息安全管理工具。但并不是每一个管理工具，能够特别是在异构环境中百分之百兼容每个软件与硬件设备。这样的工具可以提供足够的、综合性报告，但没有赋予一种能够在不断变化的威胁趋势下快速应对的配置能力。

不幸与万幸之间的扭转变换中，单机设备有意弥补防火墙的不足，自己却存在和防火墙一样的限制。例如许多IPS或DLP系统不能够检测加密的数据包。

单机安全设备举例

以下是网络部署中使用的单机安全设备的举例：

- ✓ 虚拟专用网（VPN）： VPN使用专用的协议在互联网中安全移动数据包信息。通常情况，VPN协议会加密从发送端到接收端的流量。这样便迷惑了意欲截取并检测这些数据流量的工具。 VPN加密数据以保护流量不会受到未授权的访问。因VPN数据包是被加密包裹在新的协议“信封”传输的——也就是“封装”技术——VPN即建立一个私密的、加密的隧道通过互联网进行数据包传输。
- ✓ 数据泄露防护（DLP：Data loss prevention）：DLP查询正在离开网络的机密、专利或监管数据信息。它可以防止意外的数据，如客户服务代表在回复客户邮件中的账户信息。也可以停止大规模的专有数据泄露，如一个心怀不满雇员将整个客户联系名单发给未来的雇主。
- ✓ 入侵防护系统（IPS）： IPS如同一个网络监控机制，查看网络流量与活动模式，并记录可能影响网络安全的事件。IPS系统会向管理员发出报警或警告信息并能够屏蔽不需要的流量。IPS系统可以定期记录事件发生的日志，也可以提供应对威胁的方法，或对可能的合法行为举证。
- ✓ 内容过滤技术：内容过滤机制可以根据IP地址、域名、URL、内容类型（例如成人网站或文件共享）或有效负载阻断来自网络或进入网络的流量。 并对信任站点与禁止站点设置了白名单与黑名单，防止用户违反适用政策或暴露给恶意内容。

多台设备部署造成性能碰撞

在本节中，我们探讨在添加了众多单机设备后对传统防火墙环境的性能影响。每个设备执行其自己的网络数据检测，这意味着数据被多个规则集多次检测。

进一步说，一个设备执行深度包检测（DPI），查看数据包的有效负载查看内容的细节。 这样的检测是查看常规的威胁，病毒、间谍软件、垃圾邮件等等。但也可能检测到未授权或可疑的网络协议，例如常用于下载音乐或视频的协议。 这些协议一般都是公司网络所禁止的，因其不仅占用网络带宽，也可能会招致版权侵犯的纠纷。

数据包深度检测（DPI）是根据数据包有效负载中收集的特征也就是特征模式集合对网络流量进行识别与分类。 这一机制比只检测数据包头更全面、有效的控制以及过滤数据。

尤其是，数据包深度检测对单个数据包的攻击非常有效，例如缓冲区溢出攻击、DOS攻击和分布式拒绝服务（DDoS）攻击，以及一些入侵企图。

因此，多重检测，尤其数据包深入检测是有益无害的，对么？ 从安全角度来看，是的；但是从性能的角度来看，没并非如此。所有这些检测都需要时间完成且多重检测增加了网络冗余，降低了数据传输的速度。对于那些依赖实时市场数据的行业来讲，例如金融服务行业或证券经纪公司，这样的延误将导致竞争的劣势。

任何时候添加单独设备或补强某种能力以提高安全性，都不如转为选择一种集成的安全解决方案，这些单机的安全防御会带来的负面影响是全范围的，但是主要是对网络性能的降低，延迟，管理复杂化，或者说：不完整或不可靠的安全性（你曾试图改善摆在首位的东西）。

一路飙高的TCO

拼凑式安全防御方法不仅使你的网络运行缓慢，还花费不少！当你寻求以弥补不足的防火墙的方法时，必须在多个安全设备投资，也就增加你的资本开支（CAPEX）。

这些设备需要进行安装、配置、测试、和维护。多个设备意味着必须使用许多控制台查看数据、配置策略，并运行报告。这些任务需要可靠的技术人员和/或管理员的时间花费，从而又拉动了你的经营开支（OPEX）。维护多个产品，也需要来自不同厂商的多种服务和支持合同，这使服务续约过程非常昂贵和费时。不同的产品需要不同的软件更新、测试，并得保证跨所有平台的不同软件版本的兼容性，这成了影响TCO（总成本）的另一个显着的管理开销。

你可以投资在SIEM（参见本节之前的“单机产品降低了网络可视性”），以减轻一些行政运营成本，但你不能降低运营成本费用中的大头儿，这甚至增加了CapEx（资本支出）更多。噢，没边儿了!!!!

另外，任何时候你在网络上安装额外的安全设备，同时意味着增加了潜在的故障点。任何此类故障的维修导致OPEX和CAPEX的消减，这得取决于故障的类型和其严重性，所需的时间和精力恢复正常运作。

底线是：由于网络的复杂性增加，同时管理费用也会增加。长远来看，经济有效的修复核心问题比放任运行有顾虑的系统更实际。

吃一堑长一智，每个管理员都应该在做出重要的架构设计之前认真衡量增补式安全设备与集成化方案的TCO比较。维护少量单机设备的隐性成本比通常认为的费用要高不少。一旦认定了单机策略，这些费用就成为不可避免的花费！

单机策略的背弃

如果不断增加单机设备的方法并不能真正解决你的网络不断变化的安全需求，那么什么样的方法是恰如其分值得考虑的呢？一个具备以上所有安全防御优点且经济可

靠理想的方案。

- ✓ 一个综合整体考察网络安全的方案：设计为静态数据包检测与IPS技术结合的数据包深度检测（DPI），一种整体集成的网络安全考察方式，能够防御所有类型的威胁流量信息，以推动全面和灵通的信息安全策略。
- ✓ 最优的TCO方案：降低部署设备的数量，并简化管理，降低资本支出和运营成本。此外，还可以减少每年的维护和服务订购费用以及供应商的合同数量。
- ✓ 最小延迟的影响：降低整体设备的数量也意味着，当数据通过一个安全设备时只需要被扫描、检测并过滤。而且，该安全设备需设计在技术允许范围之内能够如同线速般处理所有的这些任务的定制处理器。
- ✓ 全面的安全保障与覆盖：安全功能的整合意味着有着统一整体的安全观念最大化的安全部署防御。

建立并管理能够覆盖全网络的防御方法叫做深度防御。一个特殊处理的攻击必须先突破安全防御层才能够访问网络上的资源或服务。

真正深入的防御手段意味着在整个IT系统和基础设施中建立多重安全保护。深度防御旨在解决来自人为、技术或操作、处理造成的安全威胁漏洞。它可以提供应对当今复杂的攻击，如利用多种技术入侵网络混合持续性威胁（APT）。还可以保证即使某些技术能够入侵网络，也有能够制止该技术的其他安全技术（例如IPS）。

我们将进一步在第三章中的统一威胁管理章节中进行详细探讨这种综合的解决方案，克服传统防火墙造成的网络延迟，且是集成、有效的安全方案。

第三章

UTM：平复防御的混乱

- 怎样是统一威胁管理
- 灵活，设计为未来
- 透过“单窗口”查看并维护安全
- 避免众多设备的大杂烩
- 硬件加速实现同时提速业务效率
- 始终保持能够防御不断变化的威胁

许多公司机构希望找到某种方式，能够摒除传统防火墙使用带来的劳动力的密集、不安全以及混乱的特点，辅以多重独立的安全技术。统一威胁管理（UTM：Unified Threat Management）是一种已被许多公司机构采用的提高网络安全的可视性与控制性同时降低网络复杂性的方案。

UTM是创造一种环境使所有的网络安全统一在一个独立、一致的技术保护伞之下。UTM整合所有传统的以及下一代防火墙功能于一台设备。

本章中，我们开始谈谈UTM的定义。接着，探讨UTM是如何解决之前所述章节中传统防火墙的不足，正如我们的标题一样——拨混乱为有序，同时提供安全性与可管理性。

迈入 UTM 时代

UTM代表着网络安全技术与设备一种革新性的飞越 。通常所说的UTM指将多种安全功能包括下一代防火墙的技术例如应用控制整合到一台设备。

随着网络威胁的演变和新威胁的出现，网络安全必须随这些威胁而灵活改变防御。这种适应性使UTM难以界定，因为不同厂商之间的技术非常不同。然而，随着时间的推移，UTM涵盖的功能集合在不断扩大，且这一趋势没有逐渐减少的迹象。

在我们写这本书的时候，最好的网络UTM解决方案包括下列核心安全功能：

- ✓ 执行数据包状态检测的网络防火墙功能。
- ✓ IPS检测与阻断入侵以及某些攻击的功能。
- ✓ 应用控制，提供应用程序的行为和内容的可视性和控制。
- ✓ 远程网络安全VPN访问。
- ✓ 防止对恶意网站、不恰当，或可疑的网站和内容的访问的内容过滤功能。
- ✓ 从IPv4到IPv6迁移，以及IPv6环境下支持所有的网络安全功能。

支持虚拟域和虚拟设备的虚拟环境。还包括可以部署的其他安全技术，包括：

- ✓ 数据防泄漏，防止意外或故意地专有或监管数据的泄漏。
- ✓ 反病毒/反垃圾邮件保护，防止恶意的有效载荷或不需要的邮件进入网络。
- ✓ 终端控制： 远程用户以及设备与公司网络的安全策略保持一致。
- ✓ 无线局域网（WLAN）控制：巩固通过单一设备的有线和无线流量安全，简化策略创建和实施，同时降低网络的复杂性。

现代UTM设备的功能比细目清单还要长，实际上，你将会在本章节的剩下部分看到（即本书的剩下部分）。

UTM：灵活，为未来设计

UTM是提供灵活的、可以应对如今的网络环境所面临挑战的，前瞻性的解决方案。并非每个公司的部署都需要用到UTM设备中的每种功能，事实上，被使用的并不多。UTM是给公司或机构一种部署能力，可以灵活、按需的使用这些功能的一种能力。最好的UTM解决方案采用一个简单的许可模式，其中包括所有的技术，无需购买额外的模块，且消除因企业或公司经常增减人数而带来的按用户数计费的顾虑。

UTM提供了一个全面且功能强大的解决方案，以满足当今最复杂的网络环境带来的挑战。它克服了非集成的、围绕传统的防火墙和个人这类系统，单机设备和软件系统的缺点。

最先进的UTM设备可以拥有以下几个特点：

✓ 灵活的。

UTM设备能够部署多种技术，以满足现代公司企业网络环境的独特性、不断变化的需求和不断变化的威胁环境。实时更新，确保始终是最新技术，安全策略和其他安全措施。这些技术都是随机携带的，应用新的功能只是动动鼠标进行配置而已。

✓ 具有前瞻性的。

UTM设备设计采用通用且具有前瞻性的技术。这些设备可以应对功能与网络环境的变化的同时保持其性能。例如，对万兆以太网和IPv6的支持，意味着用户在未来网络环境变化时，安全架构不会遭遇“叉车式升级”。

✓ 强劲的。

UTM设备必须跟上网络性能不断增加的步伐，确保不会成为网络瓶颈。 UTM设备也要提供对安全事件的良好认知与控制，以及了解有关网络流量、用户行为与应用内容有关的潜在问题。 对安全威胁不断增加的感知能力使UTM比传统防火墙能够提供更成熟的检测与防御技术 。

本章之前提到UTM设备中包含的技术之一 ——应用控制 ——就是一个很好的成

熟检测与防御的技术举例。

高级应用控制允许管理员建立更细化的策略，而不是简单地在每一个应用程序的基础上设置允许或拒绝规则。应用控制对内容和行为提供了细粒度控制，这正是企业管理今天的应用爆发之需。应用控制技术可以控制每个用户的网络操作与操作的时间：

- ✓ 对单个应用（例如允许访问Facebook聊天，但是屏蔽点击链接到其他网站或下载文件）允许开启某些功能，或关闭其中另一些。
- ✓ 根据一天中的时间（如阻止访问在正常工作时间）或限制某些应用的带宽分配的应用程序允许访问
- ✓ 非必要的网站的设定访问的时间或者次数（例如对每个雇员设置每天只有一个小时访问在线购物或社交网站）。

单窗口管理

UTM设备与传统防火墙系统以及多个设备防御方法相比一个显着的优势就是集中管理。 传统防火墙系统，混合防御的每个组件（防火墙、VPN、应用控制、IPS等等）都有自己的管理平台。 操作者需要面对多个屏幕保持开启和运行的状态，所以他们必须从一个控制台跳到另一个直至查看完网络安全的各个方面。这使将这种安全事件的连接性与分析变得更加困难。

一个窗口的“管理控制台”，是指一个连贯和统一的管理界面，提供可以访问所有配置，管理和监控的功能。不是单独的控制台，而是这种方法是一个综合的显示所有的安全功能的面板。使操作它的人能够自行控制操作配置各种功能(或功能的集合)。

另一个优势就是从一个统一的接口，提供对整体安全状态的查看。直观查看各种攻击事件以及处理方式。单一防御的设备甚至没有查看攻

击报告的功能，更别谈如何处理。

在安全功能是孤立的状态下，容易导致以下结果：

- ✓ 安全事件的失察。
- ✓ 错过及时处理的时间。
- ✓ 合规与审计控制的失职。

在一个控制平台下出现这三种结果是不可能的。另外，为避免以上三种结果的产生，以及单一的控制平台的优点，下面章节慢慢道来。

成本效率

当一个公司加固网络与安全管理时，优先考虑的是减少需要管理、维护与更换的设备数量。同时，之前负责管理陈旧设备的员工可用来执行其他任务与活动。

增强防御意识

传统安全设备只能捕获其可以识别和衡量的攻击。从这个缺点延伸一点说就是传统设备不能应用当今复杂的混合型威胁（APT），和多态攻击：

- ✓ APT（又称多载体攻击）使用多种技术引诱和攻击受害者。这些攻击技术包括垃圾邮件、针对特定的用户的冒名邮件、虚假弹出报警信息、社交博客和论坛垃圾邮件、僵尸网络的感染和传播、中毒的搜索引擎显示结果，入侵网站广告和网站内容，等等。
- ✓ 多态性的攻击是定期变换恶意代码（例如伪装为反恶意软件的Total Security勒索软件）以逃避传统的基于签名的技术检测的攻击。

举例说明，在一些公司的安全边界是邮件系统、IPS、网页内容过滤系统，各自独立管理。一个APT攻击导致的结果是：每个系统的管理员在各自的管辖之内见证这个攻击的发生过程（如钓鱼网站的链接、传入的恶意文件、伪造的电子邮件，并试

图与外部网站通信的内部系统）。这可能是个很长的时间过程，在IT人员收集单个系统报警信息并得出结论之前，一个成功的攻击已经实现！

可是，随着统一威胁管理不断更新，这样的陌生行为会在一个管理接口中修复而不是分别出现在各个安全系统中。只有当APT攻击的各种特征之间建立起内部联系来显示时，IT工作人员才可以做出快速判断。

减少安全的错觉

UTM设备，其增强的安全可视性和控制，会降低公司在不少安全防御保护时会妄加相信自己已经做得万无一失的错误判断产生的可能性。一个依赖传统的方法防御网络安全的公司对没被检测到的未知的威胁也不会有防范意识。 这导致的是IT团队认为网络是安全和有保障的，而未被发现的威胁实际已经出现并蠢蠢欲动。

没有任何解决方案可以独立于人机交互而完全运行的。但是，一个独立的面板便可以通过集成与内在关联的数据提供加固的、智能的管理。

小心弗兰肯斯坦的怪物！

你知道弗兰肯斯坦的怪物的故事，主要是描述一个科学家的疯狂计划。弗兰肯斯坦计划要靠自己的力量创造一个生命体，说是想打造一个完美的人，于是，他从坟场精挑细选后挖出的尸块，他以专业知识判断还能使用部分，再将之缝合成人型，并赋予他生命。

许多公司对待网络安全就是采取的就是类似弗兰肯斯坦式做法。从一个厂商选择一种安全防御的一台设备，从另一家厂商采购另一种，如此这般，将这些设备“拼”起来。所有的安全需求都需要满足的时候，最万无一失的办法是加固比需要的多还多的设备。 除了占用更多的机架空间、电源与冷却能耗外，额外的设备还可能导致性能的瓶颈与其他服务与合同支持的费用。

把事情搞得更糟的是，非必需的设备因互不干涉各自的能力与任务而经常性的重复

流量操作。其结果，一台设备可能执行了一些操作，然后发送到下游的下一个设备，重复上一台设备已经执行的相同的处理。

如此往复，之后的设备轮番操作。不同的设备因没有集成而互不感知对方。假如这是安装了数月或数年后，IT人员可能也感觉不到任何瘀滞。当考虑到增加更多额外的设备，而由此带来的反复冗余处理和成本增加，采用单一厂商解决安全问题的论证结果变得更为坚定起来。

硬件加速实现同时提速业务效率

当一个公司企业机构构建其安全架构时是基于使用多个厂商的不同设备时，在查看各项参数数据时势必就要造成低效以及很多冗余工作。每台设备执行各自要求的内容过滤，不论这样的操作是否会在下一台设备中重复。例如，防火墙不做深度包检测（参阅第2章），将数据包发送到下游的IPS做内容检查。这意味着，一个单一的数据包将被彻底拆分和分析两次，仅仅是因为防火墙不能共享其内容过滤结果。因各设备之间这种反复的处理操作会减缓流量。其结果是网络运行变慢、应用性能降低。 这在要求低延迟的业务例如语音、视频或金融交易中尤其是个麻烦。

相反，UTM设备的各种功能是集成的，各个模块的操作作为单个设备操作的一部分。这些模块之间相互协调工作。例如，根据多层网络防御的保护要求而执行操作，而不是各自独立执行安全功能的处理。集成的过滤操作的结果是减少彻底检测数据所需的操作时间与资源，加速了数据通过UTM设备的时间。

第四章中，我们将详细探讨UTM设备相比其他网络安全解决方案在网络性能方面的优势。

能够执行许多相关功能的单个集成的网络平台是硬件与软件结合的性能优化方案的最佳候选。毫无疑问，使用专用的、高速的定制处理器的称为ASIC芯片集成在UTM设备，远超越传统的防火墙的硬件水平（第

四章中，将有ASIC的一个更详细的说明）。

将多种功能整合在UTM设备是各种软件优化对整体性能的提高，这一点也许不太明显。这是因为UTM设备的设计者知道哪些类型的数据需要被访问、数据流向、以及共享操作结果、存储与输入/输出活动的优势。一个经过优化选择的方案比添加在旧有防火墙周边的分散、功能执行单一的方案更具优势。

优化后的软件借助集成在UTM设备中专有定制的硬件，使得流量能更迅速的通过网络。加速数据的传递，提高了性能的系统，执行更多的业务量。最终，对网络有利的事情同样对企业的业务也是。

始终保持能够防御不断变化的威胁

网络安全战略的另一个重要组成部分，是保持掌握变化的威胁环境安全技术的能力。这些变化可能是基于现有威胁的新的变种，或针对以前未发表的或未知漏洞的攻击。

无论涉及什么类型的新威胁，在损失发生之前必须迅速改变组成企业安全驾架构各种设备中的检测规则、定义、签名特征、并完成配置。这些更新需要基于广泛的威胁研究。如今，最先进的威胁研究需要具备成熟且广泛漏洞，攻击和威胁研究的能力。

为了保持目前的最新威胁的研究工具和技术，企业机构不得不投入大量资源。这意味需要创建一个颇具规模的内部团队和系统在全球范围内收集和综合大量数据，然后利用这些信息来确定必要的配置更改。 这是唯一检测新出现的威胁的方法，并快速对受影响的系统与设备更新规则，策略，与特征。这简直就是一个不可能完成的任务单，就如同在说像珠穆朗玛峰是一个非常高大的山！

对于大多数公司机构，创建一个内部的安全研究团队成本过于高昂。幸运的是，存在一个简单的自助方法：购买一台有一个广泛的全球威胁研究团队支持的UTM产品。一个大型的专业团队将确保支持该产品是最新的规则与策略防护。支付安全服务费用要远比建立和维护一个规模庞大的研究团队划算得多得多。

第四章中，我们讨论有关支持本章节描述的UTM优势的底层技术。

第四章

UTM 细节

- 数据流检测与代理检测之比较
- 一般处理器与ASIC之比较

UTM是一个具有广泛基础的网络安全平台，代表了传统防火墙进化的下一阶段。各种硬件集成与软件对网络的防御，功能包括防火墙、IPS、应用控制、内容过滤，防病毒和防垃圾邮件软件以及更多。 UTM是通过一个集成的平台，提供以上所述所有形式的防护。

UTM统一防御是通过一个集成系统中的单一界面管理的。这样便节省了负责安装，配置和维护多个安全设备，以及保持多个平台协调工作保护网络架构的网络管理员与工程师的人员开销与编制。所有的防护功能集中在一个设备并可以通过管理接口所配置管理，所有的防御方法被集成提供更佳的“统一”威胁覆盖。 且单台设备占用机架面积小，节省空间、用电、并产生更少的热量；即便是插槽都占用得较少。

本章中，我们深入探讨详细的UTM技术和优点 。

为你的网络选择对的检测技术

UTM设备检测流量并识别判断哪些流量违反了设定的策略。对不同的威胁采用多重的检测方式。每种检测方式都有其自有的特点、优势与劣势。

基于数据流的检测

基于流量的检查，也被称为基于数据流的检测，数据进入UTM设备并进行模式匹配以识别是否含有恶意内容。这样的检测并不如同基于代理的检测那样重组数据，基于代理的检测我们稍候讨论。

基于数据流检测是分析数据块，而不是完全的重建通信会话包括文件的所有组成部分。这样便大量消减了UTM设备分析数据所需时间。

数据流检测的优势

检测速度是基于数据流检测的主要优势。 因数据检测与数据处理的时间缩短，基于数据流检测要不基于代理的检测机制要快。不幸的是，基于流的检查机制不如基于代理的检测机制更具有完整性，这意味着可能会错过一些恶意内容。

基于数据流检测的优点，同时也是它的缺点。虽然忽略的具体内容检测，提高了速度，数据中数据包携带的数据仍是未经过检测的。根据入侵或攻击的类型，流量检测方法可能会错过某些漏洞的发现。

基于代理的检测

基于代理的检测机制是对进入UTM设备的内容进行重建并执行全面的内容检查，查看可能存在的安全威胁。它并不像基于流检测那样采样数据，而是检查的通信会话的全部内容包括其文件。

UTM设备在安全检查的环节中作为代理。设备下载内容的协议会话的负载，重新构建，然后进行内容检测。如果内容干净，则发送到客户端。如果检测到病毒或其他安全问题，在文件（或网页、或任何内容）发送到客户端之前删除问题内容。

基于代理检测的优势

基于代理检测相比数据流检测的主要优势是提供的安全级别。基于代理的检测更侧重于对内容的细节性检测，所以更彻底。比基于数据流检测机制能捕获更多的恶意内容与威胁。

另一方面，代理方式的深度检查，需要更多的处理能力，它会引起降低网络吞吐量和延迟增加。

基于代理的检测提供了一个高水平的安全性，并提供增强的协议的意识，但在延迟在高速环境中的吞吐量和更低的成本。

通用处理器与 ASIC 比较

防火墙和UTM设备执行所有任务，包括硬件系统运行的软件。在上一节中，我们考察了不同网络流量检测方法之间的差异，包括其利弊。软件管理所有的检查任务，但任务执行必须是依托在硬件平台的。因此，处理器不同，执行效果亦不同。

通用处理器的设计适合工作在各种计算机硬件环境和处理各种指令。通用处理器就是万金油，而不是专有芯片作专用之事。

相比之下，特殊用途集成电路（ASIC）的处理器是设计用于处理具体的应用程序或功能窄幅运行的指令。ASIC芯片的专用设计是提供特定的功能，用于UTM设备中，是提供加速处理安全功能。

通用处理器的优势

通用处理器的主要优势在于它的通用性。通用处理芯片设计能够在不同的条件下尽可能广泛的硬件平台工作和管理许多不同种类的软件指令。这种类型的芯片设计没

有锁定到一个特定的环境、平台、或指令集；所以可以很容易适应不同的计算和业务需求。

通用处理器缓存非常好，这对于例如需要快速解析的应用程序数据和缓存中迅速查找的防火墙的平台非常重要。 通用处理器架构的灵活性，非常适合防火墙的应用程序缓存的多样化需求。

通用防火墙的优势同时也造成了它的劣势。这种处理器架构的运作与一切都好，但不擅长处理应用程序特定的任务。这时，通用处理器有多好即意味着有多不好。如果您需要一个适合于特殊硬件平台处理的特殊任务的处理器，通用处理器很少是“最合适之选”。

ASIC处理器的优势

ASIC芯片的优势在于其专业化。一个ASIC芯片是设计以最高效、最佳性能与可扩展性执行设定的功能集合。对于网络安全，ASIC设计用于单独执行以安全为目的数据处理与检测。相同的设备条件下，以满足这些要求而设计的ASIC的表现将优于通用芯片。这种情况下，ASIC芯片是一个部件整体，高性能的硬件平台，用于运行网络与特定安全功能的软件。

市场上的表现最快的UTM设备利用相结合的ASIC处理器和通用CPU结合以非常低的延迟提供非常高的吞吐量。

将ASIC应用于数据流处理

虽然ASIC芯片可以设计用于执行许多任务，有几个是专门的UTM安全操作，如内容和网络处理器。也有其他特殊的处理器与定制的ASIC协同工作，提供其他的加速选项。

内容处理器

一个内容处理器，设计用于将在高速网络流量中获取的对象与的已知威胁的特点进行比对。基于内容特定的ASIC处理器的设计，用于检测网络数据包、压缩文件、或数据流中的其他对象。内容处理器能够迅速组织和检查这些对象的任何不寻常的模式或潜在的威胁变种。内容处理器是为协议识别和解析设计的，用于要求执行高度专业化检测的环境。

冠以他名的UTM

传统意义上个体网络安全在的衡量在新近的威胁例如僵尸与APT混合攻击面前已经变得不足。威胁防御必须做得全面而统一来防御不断变化的网络威胁。

客户规模和安全要求决定网络安全架构，UTM平台需要具有可扩展性。例如，小型和中小型企业（SMB）网络安全要求与全球性企业跨国机构组织的安全需求相当不同。考虑到“统一威胁管理”这一安全理念，没有任何一个集合技术的个体能够准确定义这一理念。因技术不同，通常这个理念是由厂商来定义的。

告诫写在前。许多UTM平台设计是用于符合小型网络的最小化需求，并不能扩展符合不断进化的安全需求。这些设备，因是单一设备具有多重安全，符合与UTM的一般定义匹配，但是既不能对应用控制或提供关键功能，又不能扩展符合性能要求。这些基本的一些UTM设备使用第一代防火墙技术和IPS，可能充其再加上数据包深度检测功能，但没有具备足够能够防御不断进化的威胁的功能。先进的UTM设备，专门为今天的高性能网络环境而设计，可以提供的企业级功能，例如万兆以太网的支持，通过定制处理器与通用CPU相结合而提供40 Gbps或更高的防火墙性能 。

安全市场中对UTM和下一代防火墙（NGFWs）之间的差异也存在一些混乱。下一代防火墙类似UTM，因为它们是综合网络安全设备，且能够实时运行网络安全策略作为线内的安全屏障。最显着的区别是，下一代防火墙提供的安全功能是大多数UTM设备功能技术的一个子集。鉴于并不是所有的UTM设备都是相同的，你还需要做些鉴别研究与考察，选择最适合你网络安全需求的UTM设备。

网络处理器

网络处理器是在接口级别提供尽可能低延迟的网络数据路径。这些ASIC设计的出于提供高速处理，检测流量模式特点，而不是检测流量中的对象，查询威胁模式的。

这种处理器的主要任务之一是加速防火墙、入侵防御、应用控制的性能。网络处理器因是在接口级别操作生效，使多媒体服务、单播和组播流量，无论包的大小，都能提供犹如开关般流畅的极低延迟的线速性能。这些处理器还提供加速的IPSEC加密、TCP卸载，虚拟域的支持、服务质量、流量整形、日志管理处理。

安全处理器

还存在另一个类定制处理器，被称为安全处理器。这些都是多核，多线程处理器与内容处理逻辑的结合。安全处理器在接口或系统级操作，并添加额外的数据包处理和加速选项。

通用、内容、网络与安全处理器的集成

目前为止，我们已经谈到过通用处理器和ASIC处理器之间的差异。说到ASIC处理器时，我们已经对比过内容与网络处理器的不同。UTM系统中，不同类型的芯片可以集成在整体的一个架构中，优化不同威胁防御的处理。图4-1，显示的就是采用了所有这些处理器集成后的一个高层次的架构的UTM设备。

网络流量通过以太网接口进入UTM，将立即被发送到网络和安全处理器进行分析。根据分析结果通过或屏蔽流量，允许通过的流量将到达通用处理器单元。通用处理器将被要求内容检测的包含对象的流量发送到内容处理器进行威胁特征匹配过滤。

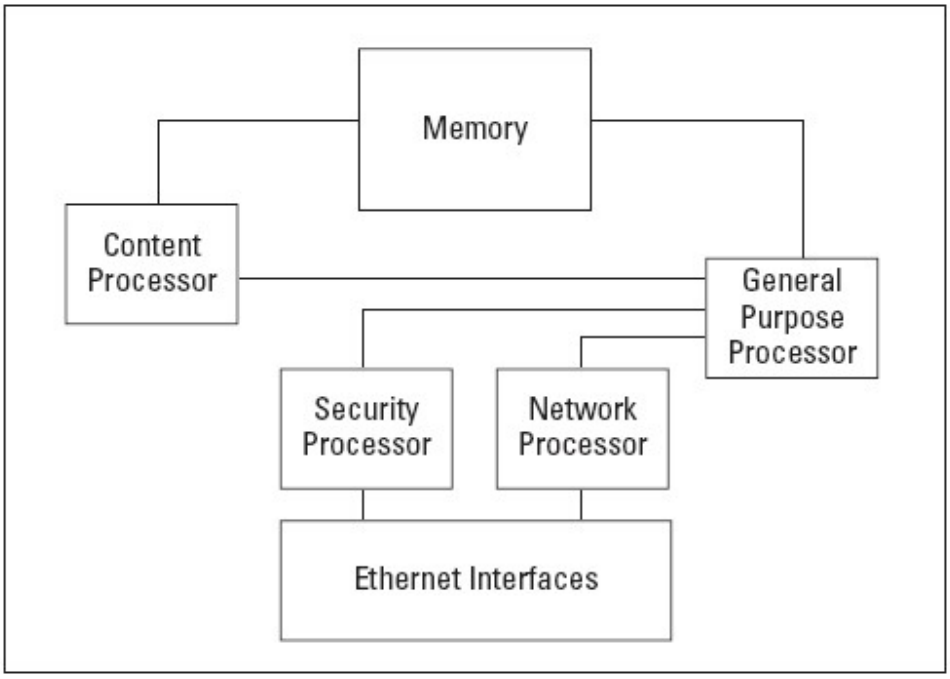


图 4-1:集成了内容、通用、安全与网络处理器的UTM处理平台

正如你可以看到在图4-1中，网络和安全处理器对进入UTM的所有网络流量进行过滤。除了执行威胁分析外，这样架构设计还需要执行例如TCP处理、网络地址转换（NAT）、加密/解密等任务。相比之下，内容处理器并介入数据流的操作，直到通用处理单元告知内容单元一些内容对象需要被检测，由此使检测操作的效率最大化。

第五章中，我们探讨下UTM的各种技术如何协同工作以提供全面的网络安全。同时还提供分析几个客户案例。

第五章

统一威胁管理的作用

- UTM的基本技术概览
- 端到端的彻底防御覆盖
- UTM用户的现身说法

今天的公司机构在谈到网络安全，尤其是涉及客户数据与法规遵从时，并不很认真。多层次的安全可以将攻击阻挡在外，免除敏感数据受人觊觎。 同时，实现强大的安全性不应以网络人员超负荷工作、网络性能下降为代价。统一威胁管理（UTM）系统整合安全技术为单台设备通过一个接口管理的专业设备。

本章中，我们将近距离谈一下UTM如何工作，我们从构成UTM的必要的技术：入侵防御、应用控制、网页过滤，数据防泄露、防垃圾邮件，防病毒谈起。从中，你可以看到UTM是如何做到从边界到核心的安全保护，以及一些实施技巧。最后，还与你分享三个公司机构使用UTM解决方案进行安全防御，以及使用后业务与客户服务得以改善的案例。

部分成就整体

UTM技术构成

一个UTM系统不只是安放在你网络中的一个硬件盒子。它囊括了多种功能，从应用控制到网页过滤至更多，都能够集中管理并协同工作。

接下来，我们讨论下网络安全部署的核心UTM防御技术。

应用控制

应用控制，一项非常重要的下一代防火墙功能，可以对你的网络中产生的流量的能见度掌控能力到应用级别。

应用控制可以识别和控制应用程序、软件程序，网络服务和协议。为了防御最新的基于web的威胁，应用控制应可以检测并控制web 2.0的应用，例如 YouTube，Facebook与Twitter。企业级应用程序的控制提供了颗粒度的策略控制，可以允许或阻止基于开发商、应用程序的行为、以及类型和使用技术的应用程序。例如，你可以屏蔽对特定网站的访问，阻断你网络内用户从网站转发链接或下载文件，或禁止游戏但允许聊天。

应用控制的另一个功能是对用户执行基于身份的策略。UTM系统跟踪用户名、IP地址和活动目录用户群体。当一个用户登录并试图访问网络资源时，UTM设备将根据其请求的应用与目的地执行相应的防火墙策略。只有当用户属于允许的用户群体之一时，才被允许访问。

流量整形，是对某类型的流量保持带宽的一种方法，通过限制其他一些流量的带宽从而优先一些应用流量。应用控制功能中包括流量整形，有利于保持流量占用型的应用，例如Skype、iTunes 或视频分享，得到较好的控制。

应用控制还延伸到网络终端，从工作站到智能手机。通过使用安全网关上的应用控制列表，可以在网关或终端设置允许、监控与阻断这些应用操作。

入侵防御(IPS)

IPS是防御来自外网威胁以及内网威胁传播，以此保护内网安全。IPS也被认为是下

一代防火墙的一个重要组成部分。在UTM解决方案中IPS模块提供范围广泛的工具来检测和阻止恶意活动，例如：

- ✓ 预定义的签名：攻击签名的数据库定期更新，如使用未打补丁的操作系统。
- ✓ 自定义签名条目：这些条目的收集是为了补充标准IPS签名可能无法提供完整的保护，主要是针对新的或未知的攻击。
- ✓ 带外模式：也称为单臂IPS模式，IPS在该模式下运行作为入侵检测系统，只检测但不对危机与威胁执行任何动作。在独立的交换接口中分析可疑流量。
- ✓ 数据包日志记录：这种类型的日志记录，截获与某些IPS特征匹配的数据包并通过日志分析工具分析日志文件。

网页过滤

网页过滤是控制用户可以查看各种网页内容。通过网页过滤功能，可以大大降低接触到间谍软件、钓鱼、网址嫁接、不适当的网站、网页重定向，以及潜伏在互联网上的其他威胁的风险。

网页内容过滤功能扫描通过防火墙策略的每一个网页的内容。内容过滤器允许你对被禁止的单次与短语创建一个黑名单，URL阻断，可以屏蔽未经授权的网站地址。分类阻断是网页内容过滤的第三种方式。通过URL的评分允许访问“评分高”的网站，并阻止访问“评分低”的网站。

厂商是十分能够体会安全管理人员和网络管理员们所面临的挑战的，因此许多厂商的设备自带URL黑名单，使该技术能够有效便捷的使用。

反垃圾邮件

反垃圾邮件过滤可以阻挡很多Web2.0的威胁，例如僵尸网络，其中许多这样的威胁是通过电子邮件传播渗透的。UTM设备纳入了多重反垃圾邮件技术可以检测各种途径进入的威胁。包括：

- ✓ 屏蔽已知的垃圾邮件发送者的IP地址，防止来自这些地址的邮件信息。

- ✓ 屏蔽与已知垃圾邮件有关的邮件正文中的任何URL的邮件信息。
- ✓ 创建一个消息散列，与已知的垃圾邮件的哈希值相匹配。不管内容与否，匹配的信息将被屏蔽。
- ✓ 将客户端的IP地址与发件人的IP地址与保护配置文件中黑名单/白名单相比较。在白名单所列通过，与黑名单匹配将被屏蔽。
- ✓ 开启SMTP会话时对域名进行DNS查询，是否在黑名单之列。
- ✓ 根据选定的垃圾邮件过滤禁止词名单进行内容匹配，符合的邮件信息将被屏蔽。

数据防泄漏

数据丢失防护（DLP），也称为数据泄漏保护，防止有意或无意将信息转移到公司机构以外的人。也可以应用那些要求数据只保留在某部门的场景，例如人事档案或会计数据。

UTM系统的DLP通过对进站与出站的数据过滤、指纹识别或其他机制来控制数据。DLP过滤扫描入站和出站的文件，查询文本字符串和模式，根据与DLP数据库的匹配采取允许、屏蔽或者存档内容的动作。指纹识别是指对每个文件分配一个独一无二的指纹。基于指纹，防止超越网络共享敏感文件。

反病毒

反病毒技术提供病毒、间谍软件和其他类型的恶意攻击的多层防护。反病毒技术可以应用于电子邮件的病毒扫描。还可以应用于文件传输协议（FTP）的流量、即时消息（IM）、和网络边界网页内容的反病毒防御。一些解决方案支持安全套接字层（SSL）的内容扫描，这意味着，同样也可以保护与SSL协议对等类型的流量，例如HTTPS、SFTP与POP3等等。

需要来个分类说明么？ HTTPS是超文本传输协议安全（Hypertext Transfer Protocol Secure）的缩写， POP3S表示邮局协议3通过安全套接字层（Post Office Protocol 3 over Secure Sockets

Layer）。 SFTP意思是“安全的FTP。”

从本质上讲，一个UTM病毒过滤机制根据已知病毒特征与感染文件模式检测所有的文件，是否受感染。如未发现任何感染文件，文件信息将被发送至收件人。如果检测到感染，UTM解决方案会采取删除或隔离文件的动作，并通知用户。

反病毒保护配置文件中包含的一些选项：

- ✓ 反病毒签名数据库：一些厂商提供了一个签名数据库，你可以在性能与防御之间权衡。一个更大的数据库，增加了识别准确性的同时必然会因匹配扫描庞大而降低系统性能。
- ✓ 文件模式：检查对系统配置的文件模式设置的文件名。
- ✓ 文件大小：检查邮件或附件是否超过用户可配置的阈值。
- ✓ 文件类型：配置检测文件与用户配置的文件类型设置匹配的文件类型识别过滤。
- ✓ 灰色软件：配置将通过文件模式匹配过滤的文件进行检测，以及间谍软件的病毒扫描。
- ✓ 启发式扫描：似病毒行为检测或其他已经病毒指示检测。
- ✓ 病毒扫描：对通过文件模式匹配的文件进行病毒扫描。

端到端的彻底的防御覆盖

企业需要防御从边界到核心网络的网络安全。我们在前几章已经讨论UTM设备中诸如应用控制与网页过滤的功能。本节中，我们将涉及到更多的技术，使UTM防御战略更丰满，更贴合到最终用户级别的功能，包括集成的无线局域网安全，端点控制和安全的远程访问。

无线LAN部署

分别部署单独的局域网和无线局域网（WLAN）安全系统，会导致安全策略执行不

能连续一致，以及出现潜在的盲区。为了控制包括有线与无线的所有流量，需要一套单独的策略体系。

一个无线控制器便可以将无线网络集成到当前的网络架构中。每个WiFi网络或服务集标识符（SSID）都代表一个虚拟的网络接口。你可以在虚拟接口上设置介于UTM的安全策略与控制好，如同在有线环境下的操作，消除潜在的盲区。

这种方法还可以检测和消除无线接入点，帮助防止恶意或未经授权的接入点连接到你的网络。一个集成的WLAN符合包括支付卡行业数据安全标准（PCI DSS）的监管要求。

信息传输安全：IPsec 与 SSL VPN

VPN技术允许你加密在互联网中传输的流量，使从远程设备到公司接入点之间的流量不被截取查看内容。有两种类型的VPN：IPsec和安全套接字层（SSL）。

基于SSL的VPN允许几乎任何互联网存在的位置使用Web浏览器及其本地SSL加密连接。 SSL VPN的有两种不同类型：

- ✓ 无客户端的SSL VPN不需要专门的软件和部署，是在你不能对用户提供一个客户端的环境例如员工自有的PC、合约商与合作伙伴，的理想选择。只有能使用web与一些客户端应用如内联网，网络接口的应用和e-mail，就可以使用客户端连接的访问。
- ✓ SSL VPN客户端提供更完整的网络资源的访问。远程设备上安装一个客户端，并允许员工在办公室使用相同的应用程序和网络资源的访问。

基于IPsec的VPN不同与SSL VPN的不同在于一个加密的隧道是如何形成的。但是，如同基于客户端的SSL VPN，IPSec VPN连接建立在用户桌面上使用预装VPN客户端软件。也可用于远程分支机构通过Internet连接的站点到站点连接的IPsec VPN。如果你支持多种远程用户，可以考虑部署SSL和IPsec技术。例如，你可以

把这些系统上的IPsec客户端纳入你的控制，并对那些你无法控制的系统使用无客户端的基于SSL的连接。

加密本身并不能提供完整的保护。因数据在网络中传输并不一帆风顺，加密只是防止他人破译。没有其他的保护，恶意软件和合法流量将可以共行一个“安全”的VPN隧道。

用户身份认证

在允许用户访问你的网络时对其进行验证是至关重要的。不幸的是很多情况下，简单的用户名与密码验证并不可靠。公司通常需要更强大的针对访问信息价值较高系统（例如网络管理员系统与财务系统）的用户群体的验证。

双因子身份验证是根据“你知道的”和“你拥有的”为条件结合进行验证，比简单的用户名与密码方式更安全。 “你知道的”，是指个人用户的名称和密码。“你拥有的”是用户手中的一个令牌，令牌是一个小装置，或在手机上运行的应用程序。

输入密码后，该令牌提供与总公司同步的一次性密码访问服务器。这样一来，任何未经授权的个人必须同时具备个人密码和令牌本身才被允许访问。先进的UTM设备支持双因子认证，这大大降低了未经授权的个人可以访问网络资源的风险。

如同身处办公室：WAN优化

用户希望从互联网不同的地点访问网络都如同身处办公室的环境般。这可能是一个问题，因数据密集型应用程序的网速往往不理想，或因高速连接的价格昂贵。这种情况下，使用各种技术提高WAN性能的广域网优化便起着至关重要的作用。这些技术包括协议优化，字节缓存、Web缓存、SSL卸载和安全隧道，更好的应用优化与高效的使用。

以下是这些技术的一些介绍：

- ✓ 协议优化： 提高使用FTP，HTTP，TCP和其它协议流量的效率，加速网络性能。
- ✓ 字节缓存：缓存文件和其他数据，可以减少在广域网上传输的数据量。
- ✓ 网页缓存：存储或缓存网页，经被请求后发送，可以减少广域网和Web服务器之间的延迟和延误。
- ✓ SSL负载： 从Web服务器上卸载SSL解密和加密SSL到SSL加速硬件，提高Web服务器的性能，。
- ✓ 安全隧道：保护通过WAN的流量安全。

同时提供广域网优化功能安全设备，可以降低成本，使管理更加便捷。将设备安装在两个广域网与WAN之间，为了获得最佳性能，安装两个设备上的广域网链路两侧，如图5-1所示。此配置可以优化所有通过广域网的流量。

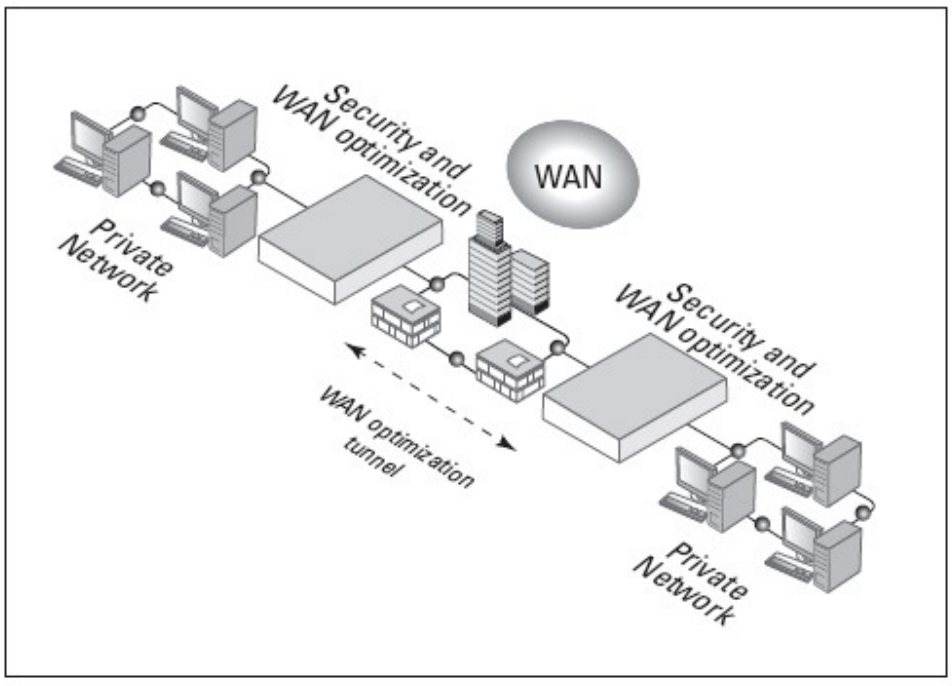


图 5-1: 部署在WAN两端私网前面的WAN优化设备

终端控制

“办公室”在当今的概念已不仅权限在大厦中的隔间。员工使用访问公司数据的设备

也越来越多样，例如笔记本电脑、平板电脑、以及智能手机。他们需要企业的网络接入，但这些设备本身具有的移动性同时也增加的安全挑战。使用以下远程访问连接解决方案，可以终端控制：

对远程通信应用IPsec和SSL VPN

- ✓ 对终端应用安全策略，例如禁用文件共享应用程序或确保防病毒应用程序的最新更新。
- ✓ 使用Web过滤和其他UTM技术，减少暴露给恶意的网页内容和网站的可能。
- ✓ 使用带有内嵌广域网优化的安全设备，确保所有远程用户连接企业数据时尽可能安全。

UTM 用户的现身说法

到这里，你已经了解UTM是如何工作的以及它的优点。接下来，我们再查看下一些用户案例，从金融行业到零售业，以及政府机构在部署UTM安全解决方案后，网络安全与生产率的提高效果。

米德兰联邦储蓄与贷款保险公司（Midland Federal Savings & Loan）

米德兰联邦储蓄与贷款保险公司对当地企业和消费者提供贷款检查和储蓄账户，贷款，保险，以及更多其他业务。总部雇员超过100名，在芝加哥设立了三家分行。

该银行的核心需求是保护如顾客银行账户和保险信息这样的重要资产。 几年前，美联在对其IT基础设施和安全的评估结果比较难堪。其中最薄弱的一点是三个分行与总公司共用一个Internet连接。一旦连接被攻破，将殃及整个公司的网络。

美联与第三方解决方案供应商合作，决定投资使用一套全面的UTM解决方案。方案包括IPS边界防病毒，间谍软件和恶意软件防护、垃圾邮件与电子邮件内容过滤、VPN接入和网站过滤。这样将保护客户数据的安全推向一个新的境界。员工的工作

效率也相应提高了，例如，垃圾邮件过滤，阻止垃圾邮件每月超过50万。同样，网页过滤系统每月阻断未经授权的网站达到几千个之多。这不仅使员工专注工作，也防止了恶意网站重定向和减少法律责任的涉及。由于UTM解决方案使安全管理更流畅且提高网络性能，美联在第一年就看到了安全投资的回报。

胜牌即时换油（Valvoline Instant Oil Change）

大家都对胜牌即时换油（VIOC）略有所知，一家全美超过800多快速换油站点。VIOC总部设在肯塔基州列克星敦，由阿什兰公司拥有。VIOC之前旧有的拨号系统保留备份，同时决定升级到无线网络。因为VIOC接受信用卡支付服务，必须遵循支付卡行业数据安全标准（PCI DSS）。

本标准包括严格的IT和安全要求。每个站点需要对销售系统端、在停车场雇员需要无线手持扫描器服务于顾客，以及店经理使用无线编辑本电脑设置独立安全的无线网络环境。VIOC也想对等待换油的客户提供免费的WiFi。本着使VIOC公司免于法律责任，加强管理，与获得用户满意度的原则，在肯塔基州总部部署了集成的解决方案，包括集中的网络管理，以及VPN、网页过滤网关，以及在俄亥俄州部署了备份设备。每个VIOC站点使用一台WiFi设备提供无线架构以及安全的SSID。网页过滤过滤防止顾客访问到“不合适”的网络站点。

这种新的解决方案，既使阿什兰公司满足了合规需要，又对到店顾客提供了良好的服务，同时提供了员工的工作效率。

PSC公司（PSC Info Group）

总部设在历史悠久的宾夕法尼亚福吉谷，力晶信息（PSC Info group）主要提供报表打印和邮寄、数据管理、信息管理服务，拥有1000多家客户，其中包括医疗保健机构、金融机构、政府机构和公用事业。PSC每天处理一百万以上的客户端文件，其中大多数是直接通过网上或通过电子邮件处理。很多客户都受行业管制，也这意味着PSC需要严密的安全措施，保障客户的数据。

PSC公司对网络安全性和可扩展性经历过一些顾虑。例如，因文件传输基于网络的性质，网络有时充斥着大量的病毒。此外，公司希望从站点到站点的VPN网络切换到多协议标签交换（MPLS），以简化管理。PSC选择部署了集成了防病毒功能、防火墙和IPS功能的UTM设备。

同时在网络入口安装了几台设备，因其出色的网络管理能力，PSC可以弃用其他不同厂商的安全设备，整合减少管理时间和成本，处理与多个供应商、合同和许可证的繁琐程序。新的UTM设备，持续自动更新检测特征库，防御了企图进入内网的web与邮件威胁。 PSC公司发现恶意软件的数量急剧下降，从从前5000多个病毒下降到每天都小于10个，减少了99.8％！

第六章

评估 UTM 解决方案的十大关键问题

（Ok，准确说是十一个）

- 从市场鼓吹中辨清性能级别的事实
- 站在当下与未来衡量安全功能需求
- 功能集成与管理集中的程度决定IT的边界
- UTM的价值所在

UTM是一个快速增长的市场。研究机构IDC预计到2012年UTM产品将占据整个网络安全市场的33.6%。这么巨大的比例意味着你的竞争对手很多正在转向使用UTM或者已经使用了UTM统一威胁管理设备。 是时候采用UTM了么？因为任何涉及网络安全的问题都是一个重要的决定，应该仔细调研。这并不容易。本章我们谈谈做购买UTM决定之前应该衡量的关键问题。

UTM 方案的选择方法？

UTM产品设计大小与优势不同，每款产品均是为了满足一定的性能级别，如基于连接数的吞吐量、延迟性。

随着网络从1千兆到10 GbE以及更快的翻番，其安全基础架构也应亦步亦趋。否则便会成为流量速度与威胁检测的瓶颈。

实现高性能源于UTM的设计。硬件组件集成化、模块化，协调流畅且高效。应该寻找能够提供专有设计的方案，集高性能的硬件满足专用的软件与网络服务于一体。这样的解决方解决方案应该包括网络级的定制处理，如防火墙和带宽控制，以及内容层的定制处理，如网页过滤和防病毒保护，能够施展最多功能和最佳的性能。是否经过第三方的技术验证也是衡量这样的厂商的一个标准。 缩短你采购清单的同时，从第三方，例如ICSA实验室或者NSS实验室获取所测试产品的评估报告。你还要不遗余力的查看所选择的产品的运行是否符合你网络环境所要求。选取三到四个方案进行实际环境测试。没有比测试更能发现优劣的方法了，且在做最终购买决定之前。

UTM 方案中包含哪些安全技术？

UTM解决方案的主要优势之一便是多重安全保护功能，如防火墙，应用控制，入侵防御，虚拟专用网的整合性。但并不是每个厂商都提供相同的功能集合，或跨越其产品线的所有型号具有相同的功能。假设你所需要是一款能够应对网络威胁的面面俱到的防御产品，所要寻找的UTM解决方案中应该包括如下功能：

- ✓ 防火墙
- ✓ 应用控制
- ✓ IPsec 与 SSL VPN
- ✓ IPS
- ✓ 网页内容过滤
- ✓ 反垃圾邮件信息
- ✓ 数据丢失与泄露防御
- ✓ 反病毒与灰色软件防护

- ✓ IPv6 支持
- ✓ 流量整形/宽带控制

选择正确的安全技术组合意味着了解当下与未来的安全需求。你认为的是怎样的核心功能应该集成到一台单一设备中以取代来自多个不同厂商的其他设备拼凑？怎样的新功能是你在未来两到三年所需要的？

是否有远程用户或分支机构需要使用VPN支持？你是否想过用一个管理接口对远程办公室或分支机构实施与总部相同的安全策略？所有的这些想法都会使你的网络安全变得不同！

像应用程序控制这样的新技术也是重要的考虑因素。由于在基于网络的应用数量的大爆发，各种不同规模的公司都希望能够执行颗粒度的控制策略 —— 什么应用用户可以访问，这些应用程序内的操作权限等等。

找出你的UTM解决方案短名单中的设备都是如何处理应用流量的。是功能完全集成到管理控制台，还是需要提供附加服务模块？一个成熟的UTM解决方案应解决所有IT基础架构安全元素，包括网络、系统、服务、应用程序和数据。覆盖范围应包括一切从网络边界到核心，从DMZ的Web服务器到内部网络的交点，以及移动设备中的数据。

UTM 设备支持哪些网络功能？

一个UTM解决方案必须能够支持多种网络拓扑结构和功能 ——无论你将其部署在哪，未来几年用于实现怎样的功能。找找看你所研究购买的UTM解决方案是否允许你监控网络的延迟和吞吐量，并自动关联事件和日志。最后，看看这个UTM解决方案是否支持你分网段的独立设置策略控制与事件。

UTM 支持 IPv6 么？

随着IPv4地址空间耗尽，IPv6的应用正在加速。重要的是你的网络安全解决方案对基于IPv6流量能够提供如同基于IPv4流量相同安全检测与威胁防御功能。请问你未来的UTM解决方案是否能够进行IPv6无缝处理？它是否可以不受任何影响的检测IPv6？ UTM解决方案应本身防火墙、透明模式下的域名系统（DNS），会话发起协议（SIP）便支持IPv6。一个优秀的解决方案还应该能够基于IPv4的动态路由（如如RIP、OSPF、IS-IS、BGP、组播协议）与基于IPv6路由（如 RIPng、OSPFv3和BGP4+），以及基于策略的路由。

是否在虚拟环境下运行良好？

一些UTM解决方案提供灵活处理虚拟局域网（VLAN）也称为虚拟域（VDOM）与虚拟设的方式。 VDOM的功能是允许你对多个部门甚至不同公司创建的独立的安全域。各个安全域内，你可以创建独立的区域、防火墙策略、用户认证、VPN配置。如果你运行一个多租户网络或多个网络，确保你考虑的UTM解决方案提供虚拟网络分割。这可以大大的节省IT员工的时间和提高基础设施的效率。 此外，如果你已经部署了虚拟机作为一种方法来改善IT环境的可扩展性和灵活性，确保解决方案支持虚拟以及物理设备。

UTM 解决方案是否具有可扩展性？

未来的一年或两年是否有扩张的趋势？公司的变化无时不在，主要是为了满足客户的需求，或区别于竞争对手中脱颖而出。扩张往往是这种变化的一部分。无论你选择任何的UTM解决方案都应该具有一定的灵活性。你应该能够使用现在需要的功能，并同时“切换”或添加其他功能或更多的用户。模块化增补方法会将一切又归于

复杂。

是否提供高可用性（HA）？

当今对通讯的依赖，每一个公司，无论何种任何规模都需要考虑到可用性的问题。一台设备故障可能是会毁掉一个公司。高可用性是确保你的网络安全是可持续的，即使在一台设备发生故障时。来确保高可用性，你可以部署为主动-主动或主动-被动的架构。一个主动-主动的架构下，由一个主设备接收所有的通信会话和并在其他主设备与从属设备之间进行负载。主动-被动的架构下，由一个负责处理数据的主设备，和一台或多台从属设备构成。从属设备在被需要之前一直是待机状态。另外，查看设备本身的旁路端口上是否提供“故障开启”功能。

集群的UTM解决方案是实现高可用性的理想方式。将群集设备通过交换机与你的网络连接。冗余设置可以确保即使一台设备故障，网络通信也可以保证。没有群集部署的情况下，公司的一台设备发生故障，可能导致与互联网、分公司以及远程用户之间统统切断了通信，且各自被孤立。对于达到更高的可用性，可以考虑从不同的互联网服务提供商（ISP）加入另一个互联网连接。

管理与报告功能怎样？

集成、集中管理是一个UTM必须具备的功能，但这在很多解决方案中却是缺失的。管理员必须能够使用一个接口“看到”整个网络以及策略变化的配置更改情况。

并在该系统中，一个应用程序的政策应该是能够自动管理或影响其他政策。例如，网页过滤，应用控制和IPS的配置文件，应包括在防火墙策略。

这样一来，便于从一个集中的console口向多台设备发出更新。具有集成管理功能

的UTM解决方案应可以在多个模块之间共享威胁事件。举例说明，如果防病毒功能模块屏蔽或隔离了威胁文件，其他模块应被通知关于此事件。对一个模块的更新会联动到其他功能模块。完美的UTM解决方案，在报告生成功能发面也应该是友好便捷的简单的鼠标点击选择生成模版即可。你选择的UTM方案应该包括如下管理功能：

- ✓ 集中管理：你可以远程管理多台设备同步策略与配置。
- ✓ 综合管理：“单窗格式”管理，你可以远程同时管理多台设备同步策略与配置。
- ✓ 高级管理：让你进行更高级别的管理任务，例如基于不同管理员角色的管理，详细的记录和报告等。当然，UTM解决方案的用户界面必须是基于web界面的，易用性和通用的无障碍性管理。如果你管理的是一个分布式网络，需要确认下所选择的UTM解决方案是否提供了收集和分析模式。具有这两个模式，部署在远程的分析设备收集数据并以存储－转发的方式发送到主分析设备。这样一个解决方案，使大型公司机构能够更容易的处理所产生的大量数据。

UTM 解决方案如何领先于安全威胁？

随着成千上万的恶意软件与恶意网站、以及漏洞泛滥，今天的UTM解决方案必须使用领先的技术结合方能击退攻击。厂商也必须不断发送更新到客户，以保证客户的设备和网络得到充分的保护。 UTM厂商通过客户订购软件与服务，推送更新，保持客户的UTM防御系统处于最新的防御状态。然而，并非所有的厂商都具有非凡的攻击与病毒分析实验室。你的选择要具有以下几个标准：

- ✓ 哪些厂商有自己的研究实验室，跟踪来自世界各地的新兴威胁，并确定如何恶意软件？依托第三方更新会比较滞后。
- ✓ 厂商的研究团队是否分布在不同的国家，并且直接处理软件更新与硬件生产？
- ✓ 对新发现的威胁或者其变种，各个厂商采取行动的响应时间如何？

购买费用如何？

任何网络安全解决方案的开支对于采购者都是一个艰难的决定，—— 但也是购买选择中的关键要素。

增补式安全系统特别强调，购买的费用应包括防火墙、VPN、应用控制、入侵检测、内容过滤、防病毒、流量整形等，随时增加的模块的总价。也有考虑防病毒、IPS、内容过滤等软件更新与订购费用 。

无论何种技术，你的流量要求越高，花费也越高。UTM解决安全通过整合多个系统从而降低总体费用支出（TCO：total cost of ownership）。别忘记将你的IT雇员花费算在内。鉴于新的UTM系统操作与管理更加高效，IT雇员可以适当减少释放从事其他工作。并不是所有的公司或机构对每项安全功能都是需要的，添加多余的安全功能模块以及其设计的安装与维护会抬高整体解决方案的花费。选择那些必需的功能，在需要时在开启其他功能。

是简单许可或不需许可么？

查看所选择的UTM解决方案提供厂商是否需要基于每个用户的许可方式。厂商之间有关许可方式是不同的。基于每个用户许可，或需要授权附加模块，这也是UTM预算需要的一项。尽可能的考虑那些提供无用户数许可限制或需添加许可模块的厂商。

成本与收益的衡量

想必您考虑的是UTM解决方案的好处而不是只是简单的价格优势。性能、可扩展性和管理是在多个UTM解决方案之间相互比较中三项可以放入重点加分考虑的方面。难道不是一个可以从根本上消除吞吐量和延迟问题，即使在高并发数的情况的解决方案更价值？如果你需要迅速地扩展系统的话？ 一笔能够覆盖当下以及不断变化

网络安全威胁UTM解决方案，是否比需要不断重新衡量安全趋势反复进行加固与费用支持的方案是否更具吸引力？能够释放IT雇员的精力处理其他更重要的事务的集中与集成管理功能的方案是否更人性化？卓越的性能、优良的可扩展性、高效的集中管理是否会赢得更多的得分点？

可提供哪些支持？

您公司的IT人员会忙于处理各种设备和服务，他们无法知道基础设施架构中每个硬件或软件的所有细节。另外，你还要指望从厂商那获得定期的固件与软件更新。一个最佳的UTM方案实施中需要有给你提供所需支持的厂商，无论是全球各地的时钟技术支持或区域工作日/每周工作的支持。厂商应具有出色的服务响应速度、合格技术支持，以及优良的客户服务声誉。此外，你公司可能需要现场服务支持例如项目切割与迁移等。这样的专门服务往往价格不菲。但厂商的工程师们往往对更具实施经验与技巧，可以加速整个过程。

售后培训如何？

找出什么样的培训选项可直接通过一个供应商或第三者，这对供应商的产品认证，。在线培训是必不可少的控制成本，给繁忙的专业人士的能力培训，而不是其他方式，以适应他们的日程安排。这种类型的培训应包括高品质的视频和指导材料，接近教室体验。

厂商是否可以提供全球性服务支持？

一些公司的全球性问题，给安全解决方案的实施与维护带来一些额外需要考虑的问题。如果全球范围内不少地区内均设置有分支机构，你需要考察下UTM解决方案提

供商是否也在你公司营业的地区设有本地服务相应与支持中心。

在用客户的评价如何？

总是要考察UTM解决方案提供厂商的用户使用经历。如果时间允许，可以拜访几家在用客户。查看下操作产品所需的技术级别与管理水平、使用是否困难、以及在使用中其他的问题。 找出需要操作的产品，多么困难，他们使用的其他问题，来研究产品的同时管理水平。具有较高用户规模的客户需要有经验的厂商以及优秀的网路产品。缩小你的UTM选择范围同时，考虑能够使各地各行业包括政府机构均满意的UTM厂商。