Broadview
www.broadview.com.cn

安全技术大系

UTM（统一威胁管理）技术概论

启明星辰　编著

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

安全技术大系

UTM（统一威胁管理）技术概论

启明星辰　编著

電子工業出版社
Publishing House of Electronics Industry
北京•BEIJING

内 容 简 介

本书从 UTM（统一威胁管理）的起源开始，立足于实际使用环境和技术，通过多种灵活的方式全面介绍了 UTM 的实现原理与关键技术，覆盖了访问控制、入侵防御、防病毒、VPN（虚拟专用网）、上网行为管理、流量管理、日志分析和审计以及应用等多个信息安全方面的技术；同时，对 UTM 技术的发展方向和产品形态方向给出了清晰、严谨的预期。

本书适合于有一定网络安全技术基础的中、高级读者，特别适合于网络安全相关专业的本科生以及从事网络安全工作的技术人员阅读，有助于他们快速、全面地了解 UTM 以及信息安全技术。

图书在版编目（CIP）数据

UTM（统一威胁管理）技术概论 / 启明星辰编著. —北京：电子工业出版社，2009.4
（安全技术大系）
ISBN 978-7-121-08443-0

Ⅰ. U… Ⅱ. 启… Ⅲ. 计算机网络－安全技术 Ⅳ. TP393.08

中国版本图书馆 CIP 数据核字（2009）第 030116 号

策划编辑：毕　宁
责任编辑：顾慧芳
印　　刷：北京智力达印刷有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编 100036
开　　本：787×980　1/16　印张：20.75　字数：422.4 千字
印　　次：2009 年 4 月第 1 次印刷
印　　数：6000 册　　定价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

序

UTM 出现的背景

随着各行业信息化进程的深入，网络边界安全正在进入一个全新的发展阶段。目前，各种威胁逐步呈现出网络化和复杂化的态势，威胁对象由主机资源转变为网络资源、数量呈现爆炸式增长、形式多种多样，混合型攻击层出不穷。尤其在网络边界，遇到了很多的麻烦，例如：通过系统漏洞自动攻击并繁殖的蠕虫病毒、寄生在计算机内提供各种后门和跳板的特洛伊木马、利用大量傀儡主机进行淹没式破坏的分布式拒绝攻击、利用各种手段向用户传输垃圾信息及诱骗信息等。在网络边界位置，传统的防护设备——防火墙主要工作在网络层，实现基于端口和 IP 地址的访问控制，而面对越来越多的蠕虫、木马等应用层的威胁便日益显得无能为力。威胁的不断智能化也需要防护设备加强智能化，而且为了在网络边界构筑起强有力的安全防线，实现对各层面威胁的有效防御，UTM（Unified Threaten Management）（统一威胁管理）的设备便应运而生。

为什么编著本书

国外的 UTM 技术和设备早在 2002 年就已经出现，这得益于国外市场的需求和企业对网络安全的重视，导致 UTM 蓬勃发展，以每年翻倍的速度迅速成为网络安全建设必备的主流设备，使用量已排在各类安全设备的榜首。目前 UTM 已经替代了传统的防火墙，成为主要的网络边界安全防护设备，大大提高了网络抵御外来威胁的能力。

在国内，网络安全技术和市场发展相对缓慢。从 2003 年就进入中国的 UTM，概念上接受很快，UTM 设备发展速度也较快，一度出现年增长率超过 80%情形；但总体上由于技术积累、硬件平台等方面的因素限制，UTM 设备在网络安全产品市场尚未形成主导局面，很多单位和用户仍然以使用防火墙设备为主。但在威胁日益复杂和多元化的今天，这无疑增加了用户网络和信息资产的危险系数。

为了让更多的用户认识 UTM，让更多的从业人员了解 UTM 相关技术，促进更多从事信息安全产品研发的企业开发出优秀的设备，为加快我国信息安全产业的发展，提升国家信息安全实力尽一份力，作者编著了此书。

本书的主要内容与特点

本书以 UTM 涉及的各项技术为主线展开，向读者介绍传统安全网关与 UTM 的区别，

传统的安全技术如何在 UTM 中应用并发挥更大的价值，UTM 中有何难点和关键技术，在提高 UTM 性能方面如何从软、硬件两个角度考虑，以及大规模部署 UTM 时如何有效管理等。此外，本书对 UTM 的来源、定义与发展历史做了必要的阐述，对 UTM 技术发展方向做了展望，同时结合典型用户的使用环境、给出了使用案例，以帮助读者深入理解 UTM 的使用。本书可以为各行业的网络管理与安全人员提供尽可能充分的学习资料，帮助读者系统了解安全技术、了解 UTM 设备。同时，本书也适用于大专院校计算机专业有关网络安全课程的教材。

关于本书作者

启明星辰公司编著本书的主要成员为：

陈胜权：具有 10 年的网络与信息安全领域工作经历，先后从事技术开发与支持、技术管理、产品运营与管理等方面的工作；自 2004 年开始潜心研究 UTM 技术与市场，对 UTM 实现原理与技术、产品与市场发展有深刻的理解。现任启明星辰公司产品管理中心副总监。

任平：具有 8 年的网络与信息安全领域工作经历，先后从事技术研究与产品开发、项目管理、产品管理等方面的工作，参与多个重大网络安全项目的设计实施，具有丰富的网络安全经验。现任启明星辰公司 UTM 产品线经理。

陈杰：具有 8 年的网络与信息安全领域工作经历，曾在部队从事多年网络攻防方面的工作，有丰富的实战经验，现主要从事信息安全培训工作，为政府、移动通信、银行、军队等多个大型单位进行过培训。现任启明星辰公司培训部高级培训讲师。

此外，邓轶、李光朋、万卿、沈颖、谭闯、褚小艳、肖小剑、黄宇明等参与了本书的编写修订工作。

由于水平有限，难免有错漏之处，请读者不吝指正，编者不胜感激，将在新的版本中改进和完善。

作者

2009 年 1 月于北京

目　录

CHAPTER 1

第 1 章　UTM（统一威胁管理）概论

1.1　网络边界的安全防护

1.1.1　网络边界

实现资源共享是网络出现的源动力，多年的发展使 Internet 成为现实，全世界的计算机都可以连成网络，连成一个整体；但计算机越多，网络规模越大，安全也成为问题。不管是通过 ADSL 连入 Internet 的家庭用户，还是通过专线连入 Internet 的企业用户，抑或通过专线连入专用网络的行业用户，都面临着越来越多的不安全因素影响。“划地而治”是现实中解决安全问题的通用办法，国家具有主权疆土、城市具有行政区域、企业具有自主园区、居民有个人空间，这些主体都具有物理空间和边界，那么在解决网络上的安全问题时，“划地而治”如何实现呢？网络的边界和空间在哪里呢？

边界是以要保护的对象作为前提的，个人网络、企业网络、行业专网，甚至运营商的运营网络，都可以作为保护的对象；我们把这些网络可以看作一个独立的对象，通过自身的属性，维持内部业务的运转。这些对象的安全威胁来自内部与外部两个方面：内部威胁是指网络的合法用户在使用网络资源的时候，发生的不合规的行为、误操作、恶意破坏等行为；外部威胁是指网络与外界互通引起的安全问题，有入侵、病毒、恶意代码与攻击等。既然威胁有内、外部之分，边界也就有了区别：人与内部计算机的交互界面称为人网边界；不同安全级别的网络相连接，网络与网络之间的交互界面称为网网边界，网络边界的定义如图 1-1 所示。

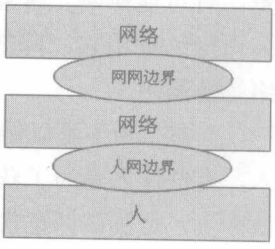

图 1-1　网络边界的定义

广义的网络边界包括了人网边界和网网边界，狭义的网络边

界指网网边界。本书提及的网络边界是狭义的概念，是指网络与网络之间的交互界面。

1.1.2 网络边界面临的威胁

随着网络的发展网络威胁的问题也与日俱增，并且目前还在呈现指数级别的增长：而且黑客仍在继续制造更为复杂的新威胁，不断地为网络互联的企业带来巨大的破坏；加之威胁的工具化、实施威胁更加容易，大大降低了攻击者的能力要求，进一步扩大了威胁。

一般情况下，网络边界面临的威胁可以分为三类：对网络自身与应用系统进行破坏的威胁、利用网络进行非法活动的威胁和网络资源滥用威胁。这种威胁分类的依据是其产生的后果。

1. 对网络自身与应用系统进行破坏的威胁：这类威胁的特点是以网络自身或内部的业务系统为明确的攻击对象，通过技术手段导致网络设备、主机、服务器的运行受到影响（包括资源耗用、运行中断、业务系统异常等）。ARP 欺骗、DDoS 攻击、蠕虫等均属于此类威胁。例如 DoS 攻击，虽然不破坏网络内部的数据，但阻塞了应用的带宽，对网络自身的资源进行了占用，导致正常业务无法正常使用。

2. 利用网络进行非法活动的威胁：此类威胁的特点是通过技术手段对主机或服务器进行入侵攻击，以达到政治或经济利益的目的。这类威胁有盗号木马、SQL 注入、垃圾邮件、恶意插件等。如通过盗号木马这个工具，不法分子可获得用户的个人账户信息，进而获得经济收益；又如垃圾邮件，一些不法分子通过发送宣传法轮功的邮件，毒害人民群众，以达到不可告人的政治目的。

3. 网络资源滥用的威胁：此类威胁的特点是正常使用网络业务时，对网络资源、组织制度等造成影响的行为，包括大量 P2P 下载、工作时间使用股票软件、工作时间玩网络游戏等。比如 P2P 下载是一种正常的网络行为，但大量的 P2P 下载会对网络资源造成浪费，有可能影响正常业务的使用；又如，使用股票软件是正常行为，但在上班时间利用公司网络使用它，降低了工作效率，对公司或单位造成了间接损失。这些行为都属于网络资源滥用。

当然，由于是以结果进行分类，那么有些威胁就可以同时归属于两个类，例如 SQL 注入，有些注入是为了获取信息，达到政治或经济目的，属于第 2 类；有些注入后是为了修改网页，达到破坏正常网站访问业务的目的，属于第 1 类。

黑客产业链的发展加重了威胁力度。

现在，不择手段的赚钱已成为新一代黑客们的主要动机。在网络信息系统存在的安全

漏洞和隐患层出不穷、威胁种类不断增加的情况下，利益驱使下的地下黑客产业链的发展，使基础网络和重要信息系统面临着严峻的安全威胁，网络犯罪行为的趋利性也表现得更加明显。黑客往往利用仿冒网站、伪造邮件、盗号木马、后门病毒等，并结合社会工程学，窃取大量用户数据牟取暴利，包括网游账号、网银账号和密码、网银数字证书等。特别是，木马、病毒等恶意程序的制作、传播、用户信息窃取、第三方平台销赃、洗钱等各环节的流水作业构成了完善的地下黑色产业链，为各种网络犯罪行为带来了利益驱动，加之黑客攻击手法更具隐蔽性，使得对这些网络犯罪行为的取证、追查和打击都非常困难。

据 CNCERT/CC 监测发现，我国大陆地区被植入木马的主机 IP 数量增长惊人，每年增长的数量超过 10 倍，木马已成为互联网的最大危害。地下黑色产业链的成熟，为木马的大量生产和广泛传播提供了十分便利的条件，木马在互联网上的泛滥导致大量个人隐私信息和重要数据的失窃，给个人带来严重的名誉和经济损失；此外，木马还越来越多地被用来窃取国家秘密和企业商业秘密，造成了无法估量的损失。因此，黑客产业链的发展对网络威胁的泛滥起到了推波助澜的作用，并且具有固化的趋势，这使得网络威胁具备了长期性的特点。

1.1.3　网络边界安全传统的防护方式

对于网络边界面临的各类威胁，应该如何防护呢？从网络产生开始，网络边界就一直重复着攻击者与防护者的搏斗，“道高一尺、魔高一丈”，防护技术在与攻击技术的搏斗中也不断地成熟。保护网络边界主要有如下几种传统的设备。

1．防火墙

网络早期是通过网段进行隔离的，不同网段之间的通信通过路由器连接，要限制某些网段之间不互通，或有条件的互通，就出现了访问控制技术，也就出现了防火墙，防火墙是早期不同网络互联时的安全网关。

防火墙的安全设计原理来自于包过滤与应用代理技术，两边是连接不同网络的接口，中间是访问控制列表 ACL，数据流要经过 ACL 的过滤才能通过。ACL 有些像海关的身份证检查，检查的是你是哪个国家的人，但你是间谍还是游客就无法区分了，因为 ACL 控制的是网络OSI参考模型的3～4层，对于应用层是无法识别的。后来的防火墙增加了NAT/PAT技术，可以隐藏内网设备的 IP 地址，给内部网络蒙上面纱，成为外部“看不到”的灰盒子，给入侵增加了一定的难度。但是木马技术可以让内网的机器主动与外界建立联系，从而“穿透”了 NAT 的“防护”，很多 P2P 应用也是采用这种方式“攻破”防火墙的。

防火墙的作用就是建起了网络的“城门”，把住了进入网络的必经通道，所以在网络的边界安全设计中，防火墙成为不可或缺的一部分。

防火墙的缺点是：不能对应用层识别，面对隐藏在应用中的病毒、木马是毫无办法的，所以作为安全级别差异较大的网络互联，防火墙的安全性就远远不够了。

2. VPN 网关

外部用户访问内部主机或服务器的时候，为了保证用户身份的合法、确保网络的安全，一般在网络边界部署 VPN（虚拟网）网关，主要作用就是利用公用网络（主要是互联网）把多个网络节点或私有网络连接起来。

针对不同的用户要求，VPN 有三种解决方案：远程访问虚拟网（Access VPN）、企业内部虚拟网（Intranet VPN）和企业扩展虚拟网（Extranet VPN），这三种类型的 VPN 分别与传统的远程访问网络、企业内部的 Intranet 以及企业网和相关合作伙伴的企业网所构成的 Extranet（外部扩展）相对应。

典型的 VPN 网关产品集成了包过滤防火墙和应用代理防火墙的功能。企业级 VPN 产品是从防火墙产品发展而来的，防火墙的功能特性已经成为它的基本功能集的一部分。如果 VPN 和防火墙分别是独立的产品，则 VPN 与防火墙的协同工作会遇到很多难以解决的问题；有可能不同厂家的防火墙和 VPN 不能协同工作，防火墙的安全策略无法制定（这是由于 VPN 把 IP 数据包加密封装的缘故）或者带来性能的损失，如防火墙无法使用 NAT 功能等。而如果采用功能整合的产品，则上述问题就不存在或能很容易解决。

3. 防 DoS 攻击网关

拒绝服务攻击（DoS，Denial of Service）是一种对网络上的计算机进行攻击的一种方式。DoS 的攻击方式有很多种，最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，从而使合法用户无法得到服务的响应。常见的拒绝服务攻击有 SYN Flood、空连接攻击、UDP Flood、ICMP Flood 等。

SYN Cookie 是应用非常广泛的一种防御 SYN Flood 攻击的技术，在攻击流量比较小的情况下，SYN Cookie 技术可以有效地防御 SYN Flood 攻击；从路由器上限制流向单一目标主机的连接数或者分配给单一目标主机的带宽也是一种常用的防御手段。另外，由于一些攻击工具在攻击之前往往对攻击目标进行 DNS 解析，然后对解析之后的 IP 进行攻击。因此如果对于被攻击的服务器分配一个新 IP，在 DNS 进行重新指向之后，攻击工具往往还会向原来的 IP 发送攻击，这样，被攻击的服务器就可以躲开攻击。这种方法被称为“退让策略”。

由于防 DoS 攻击需要比较多的系统资源，一般使用单独的硬件平台实现，与防火墙一起串联部署在网络边界。如果与防火墙共用平台，只能防范流量很小的 DoS/DDoS 攻击，实用性较差。

4．入侵防御网关

入侵防御网关以在线方式部署，实时分析链路上的传输数据，对隐藏在其中的攻击行为进行阻断，专注的是深层防御、精确阻断，这意味着入侵防御系统是一种安全防御工具，以解决用户面临网络边界入侵威胁，进一步优化网络边界安全。

入侵防御网关一般串行部署在网络边界，以边界防护设备的形式接入网络，任何对受保护网络的访问数据都将穿过入侵防御引擎。其标准的接入方式如图 1-2 所示。

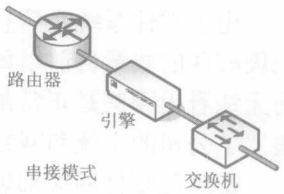

图 1-2　串接模式的部署

与旁路的 IDS（入侵检测系统）相比，入侵防御可以进行实时的防御；与基于静态规则进行边界防护的防火墙相比，入侵防御可以实现动态的深层次的、精确的防御，如图 1-3 所示。

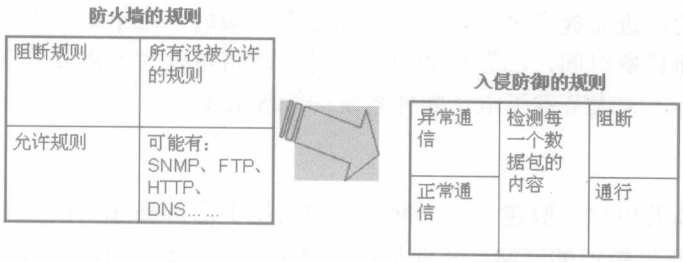

图 1-3　防火墙与入侵防御规则的对比

在发现攻击行为之后，入侵防御系统可以主动地阻断这些攻击行为，对内部网络的系统实现免疫防护。即使内部系统存在相应的风险漏洞，也可以由入侵防御引擎来实现先于攻击达成的防护。

5．防病毒网关

随着病毒与黑客程序相结合、蠕虫病毒更加泛滥，网络成为病毒传播的重要渠道，而网络边界也成为阻止病毒传播的重要位置；所以，防病毒网关应运而生，成为斩断病毒传播途径最为有效的手段之一。

防病毒网关技术包括两个部分，一部分是如何对进出网关的数据进行查杀；另一部分是对要查杀的数据进行检测与清除。综观国外的防病毒网关产品，至今其对数据的病毒检