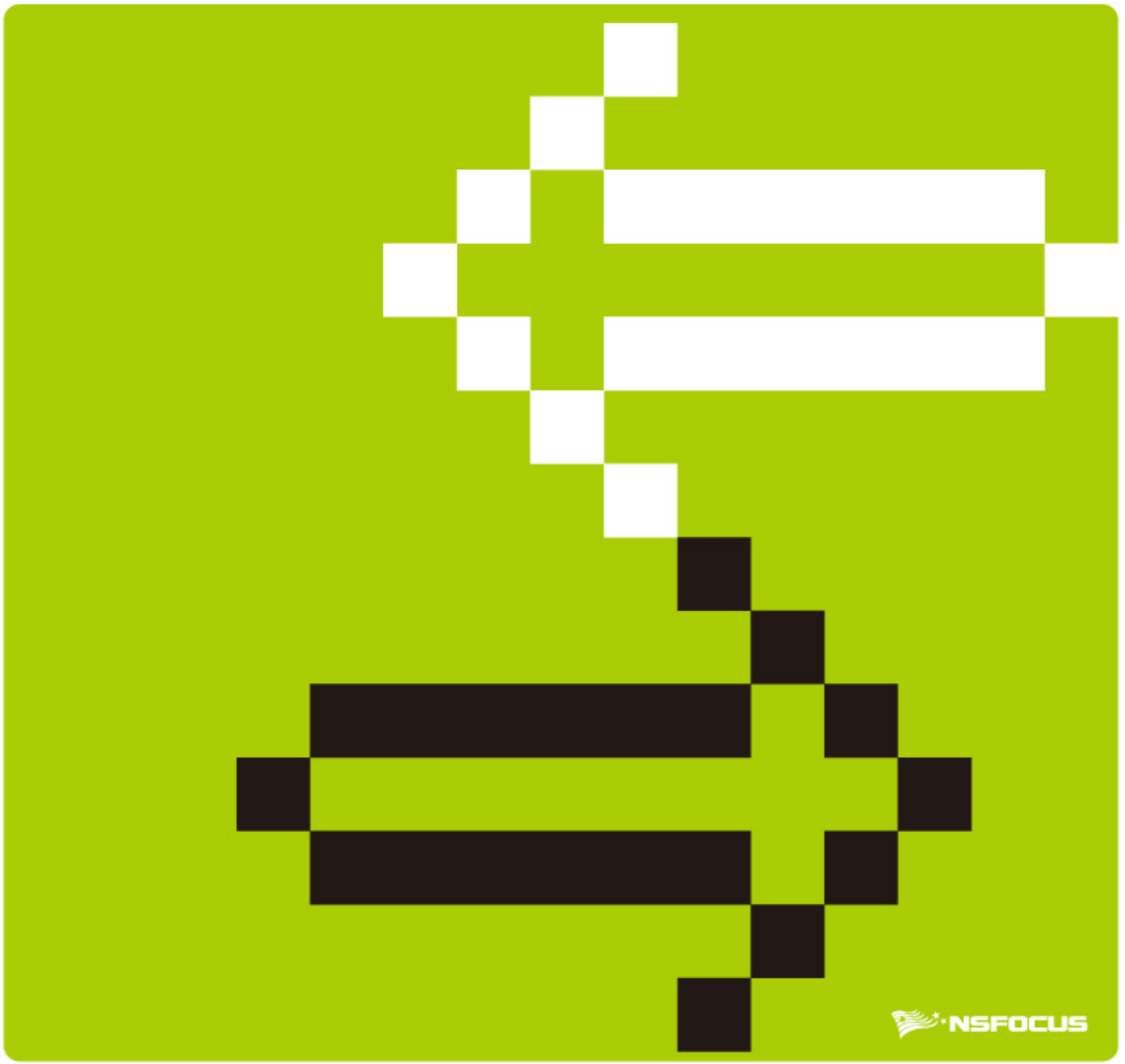
安全+ SECURITY

2008/04 总第 001

技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals



本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8668
传真：(010)6872 8708
网址：www.nsfocus.com

Nsmagazine@nsfocus.com

2008/04 总第 001

创刊号

安全+ SECURITY

Catalogue 目录

公告篇

观点篇

产品篇

方案篇

技术篇

研究篇

绿盟动态

公 告 篇

NSFOCUS 2007年十大安全漏洞

声 明： 本十大安全漏洞由NSFOCUS安全小组(security@nsfocus.com)根据安全漏洞的严重程度、影响范围等因素综合评出，仅供参考

1．Microsoft消息队列服务栈溢出漏洞（MS07-065）

2007-12-11
NSFOUCS ID:11263

综述：

Microsoft Windows是微软发布的非常流行的操作系统。Windows的消息队列服务在处理畸形请求数据时存在漏洞，在将输入字符串传递到缓冲区之前没有执行正确地验证。攻击者可以通过构建特制的MSMQ消息来利用该漏洞，这种消息在远程攻击情形下可能允许在Windows 2000 Server上远程执行代码，而在本地攻击情形下可能允许在Windows XP上进行本地权限提升。

危害：

远程攻击者可能利用该漏洞执行任意代码，本地攻击者可能利用该漏洞进行权限提升。

2．Cisco Security Agent for Windows SMB报文远程栈溢出漏洞

2007-12-05
NSFOUCS ID：11233

综述：

Cisco Security Agent是为服务器和桌面计算系统提供威胁防护的安全软件代理。CSA for Windows在处理畸形的SMB数据包时存在漏洞，其所带的一个驱动程序在处理SMB请求报文时没有正确检查用户提供的数据长度，可能触发一个系统内核中的栈溢出。通过精心构造数据，攻击者可以控制系统重启、蓝屏甚至执行任意指令。该攻击不需要认证即可完成。

危害：

远程攻击者可能利用该漏洞进行拒绝服务攻击甚至执行任意指令。

3．Microsoft DirectX SAMI 及 WAV／AVI 文件解析远程代码执行漏洞（MS07—064）

2007—12—11
NSFOUCS ID：11264

综述：

Microsoft DirectX 是 Windows 操作系统中的一项功能，流媒体在玩游戏或观看视频时通过这个功能支持图形和声音。Microsoft DirectX 处理畸形格式的媒体文件时存在漏洞，集成 DirectX 技术的 Microsoft DirectShow 没有对 Synchronized Accessible Media Interchange（SAMI）文件类型参数和 WAV、AVI 文件类型参数执行充分的分析。如果用户在 DirectX 中打开用于流式媒体的特制文件，这些漏洞就可能允许执行代码。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意代码

4．Microsoft IE DHTML 对象内存破坏漏洞（MS07—069）

2007—12—11
NSFOUCS ID：11270

综述：

Internet Explorer 是微软发布的非常流行的 WEB 浏览器。IE 显示包含针对 HTML 对象的某些异常方法调用的网页的方式中存在内存破坏漏洞。攻击者可以通过构建特制的网页来利用该漏洞，当用户查看网页时，就可能允许远程执行指令。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意代码。

5．HP-UX swagentd RPC 接口远程缓冲区溢出漏洞

2007-12-13
NSFOUCS ID：11287

综述：

HP-UX 是一款 HP 公司开发的 UNIX 操作系统。HP-UX 操作系统的 swagentd 中所定义的 sw_rpc_agent_init 函数中存在缓冲区溢出漏洞，如果远程攻击者向该函数传送了畸形参数，就可以触发这个溢出，导致覆盖指针，可能会出现拒绝服务或执行任意指令。

危害：

远程攻击者可能利用该漏洞进行拒绝服务攻击甚至执行任意指令。

6．Windows Media Format Runtime ASF 解析多个堆溢出漏洞（MS07-068）

2007-12-11
NSFOUCS ID：11265

综述：

Windows Media Format Runtime 用于向使用 Windows Media 内容的应用程序提供信息和工具。Windows Media Format Runtime 在处理畸形格式的 ASF 文件时存在漏洞，没有正确地对 ASF 流中 Degradable JPEG Media Stream 属性的相关长度项、audio_conceal_none 属性的相关长度项以及 Stream Property 项的错误修订数据长度及特定类型数据长度执行边界检查，如果用户受骗打开了特制的 ASF 文件的话，就可能触发堆溢出。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意代码。

7．Windows Vista 内核 ALPC 调用本地权限提升漏洞（MS07-066）

2007-12-11
NSFOUCS ID:11266

综述：

Microsoft Windows是微软发布的非常流行的操作系统。Windows的高级本地过程调用实现上存在漏洞，ALPC没有正确地验证就答复路径中某些条件。此漏洞可能允许攻击者运行代码，并完全控制系统。

危害：

本地攻击者可能利用该漏洞进行权限提升。

8．Yahoo！Toolbar yt.ythelper.2 ActiveX 控件栈溢出漏洞

2007-12-07
NSFOUCS ID：11242

综述：

Yahoo！Toolbar 是一个 IE 插件，能够通过嵌入 IE 的工具栏帮助快速使用 Yahoo 搜索引擎、收发 Yahoo 电子邮件等操作。Yahoo！Toolbar 的 ActiveX 控件实现上存在缓冲区溢出漏洞，其安装的 yt.ythelper.2 ActiveX 控件没有正确地验证对 c()方式所传送的参数，如果用户受骗访问了恶意网页并向该方式传送了超长参数的话，就可能触发栈溢出，导致浏览器崩溃或执行任意指令。

危害：

远程攻击者可能利用该漏洞以浏览者身份执行任意指令。

9．Samba Send_MailSlot 函数远程栈溢出漏洞

2007-12-10
NSFOUCS ID：11256

综述：

Samba 是一套实现 SMB（Server Messages Block）协议、跨平台进行文件共享和打印共享服务的程序。Samba 的 send_mailslot()函数中存在安全漏洞，如果远程攻击者所发送的特制 SAMLOGON 域登录报文中在奇数偏移包含有用户名字符串，然后跟随有超长 GETDC 字符串，就可能用全 0 的字节覆盖栈缓冲区。成功攻击允许执行任意代码，但要求打开了 domain logons 选项。

危害：

远程攻击者可能利用该漏洞以服务器身份执行任意指令。

10．Cisco 防火墙服务模块应用检查拒绝服务漏洞

2007—12—19

NSFOUCS ID：11296

综述：

Cisco FWSM是Cisco设备上的防火墙服务模块。FWSM在处理7层应用检查的控制面路径中数据时存在漏洞，可能导致设备重载。通过应用层协议检查过程所传送的标准网络通讯可以触发这个漏洞。即使用户没有发动蓄意攻击，满足条件的报文也可能在无意中触发这个漏洞。

危害：

远程攻击者可能利用该漏洞进行拒绝服务攻击。

绿盟科技紧急通告(Alert2008-01)

Nsfocus 安全小组(security@nsfocus.com)
http://www.nsfocus.com

Windows TCP/IP 协议栈存在严重远程安全漏洞

发布日期：2008-01-09

综述：

微软发布了1月份的2篇安全公告，这些公告描述并修复了3个安全漏洞，其中1个漏洞属于“紧急”风险级别。其中MS08-001中修复了两个Windows TCP/IP协议实现中的远程漏洞，攻击者无需身份认证即可匿名发起攻击，利用这些漏洞可能远程入侵并完全控制客户端系统。我们强烈建议使用Windows操作系统的用户立刻检查一下您的系统是否受此漏洞影响，并按照我们提供的解决方法予以解决。

分析：

微软发布了1月份的2篇最新的安全公告：MS08-001到MS08-002。这些安全公告分别描述了3个安全问题，分别是有关各版本的Microsoft Windows产品中的漏洞。详尽分析及解决方法，请参看绿盟网站http://www.nsfocus.net/index.php?act=alert。

观 点 篇

安全：这样把握

绿盟科技 李钠

“信息化安全就是对抗的过程”。在2006年的信息安全决策大会上，北京信息产业协会徐祖哲秘书长曾经这样不无感慨地说。

那么如何做到把握安全，做到心中有数呢？我们认为应该从以下几点着想：

TOP1 掌握一个概念

什么叫安全防护？安全防护就是某种预先用于降低被保护目标遭受损失可能或程度所采用的方法、手段。在这里我们讨论的安全防护专门针对信息的安全防护，因此并不涉及组织的人员安全防护或者相应资产的物理安全防护。

知道了安全防护是什么，进行安全防护的目的也就非常明确了——要降低被保护目标遭受损失的可能或程度。

TOP2 了解安全防护的分类

安全防护通常可以分为信息系统生命周期中的安全防护和信息系统拓扑结构中的安全防护两大类。它们一经一纬，恰好构成了贯穿信息系统生命周期的层次化安全防护网。

TOP3 明确安全防护的目标

对于安全感防护来说，希望达到的目标主要分为以下三种：

1、在可能的情况下，防止被保护的目标遭受损失；

2、在损失不可避免的情况下，降低损失程度（缩小损失范围、降低损失速度）；

3、在以上两点都无法保障时，使损失可以计量为弥补工作提供依据。

TOP4 懂得信息系统拓扑结构中的安全防护

信息系统拓扑结构中的安全防护主要涉及信息系统拓扑结构中的各个环节的安全防护——从客户端到服务器，从网络到主机，从设计文档到二进制文件。这里值得注意的是：在信息系统生命周期的各个不同阶段，信息系统的拓扑结构会有所不同。

TOP5 懂得信息系统生命周期中的安全防护

信息系统生命周期一般来说分为四个阶段，即：信息系统的设计、信息系统的实现、信息系统的运维和信息系统的消亡四个阶段。在各个阶段在系统中引入不同的安全防护手段就能够保证安全防护的有效性，使得信息系统安全达到理想状态。

懂得信息系统设计之初的安全防护

信息系统设计之初的安全防护主要集中在信息系统自身安全功能的设计和相应设计文档的安全两方面。通过信息系统设计之初引入安全防护能够为后续安全防护措施提供基础，从而有效地保证信息系统安全性。

懂得信息系统的实现过程的安全防护

信息系统的实现过程的安全防护，主要集中实现过程中相应文档的安全防护，并且在实现过程中对设计中未考虑到的安全隐患的发掘与修补。

懂得信息系统运行维护过程中的安全防护

在信息系统运行维护过程中的安全防护，主要集中在信息系统安全状态的监控和遗留安全隐患的发现与修补。

懂得信息系统消亡中的安全防护

在信息系统消亡中的安全防护，主要确保信息系统在消亡过程中相应的资料正确的被清除和销毁。

TOP6 坚决选择专业的信息安全服务商

只有专业的信息安全服务提供商，才会拥有国家最高级的专业信息安全服务资质认证和专业的安全研究和服务队伍。而且，通过大量的服务实践和执著实追求，他们已经形成了最完善的专业安全服务体系，有完善的安全服务方法论，可以提供多层次、全方位的安全服务。

UTM 时代是否真的来临？（市场篇）

绿盟科技 陶智

在最近几年里，一个名词频繁出现在报刊杂志、网站搜索、大型会议上，它就是UTM，中文名字为“统一威胁管理”。一时间，UTM风声水起，成为安全市场的“香饽饽”,受到媒体、用户、三商以及市场研究机构的广泛关注和追捧。

可是，UTM 时代是否真的来临？它能成为一个成熟的安全解决方案吗？

一、UTM 概念起源

说起UTM，大家首先想知道它是什么，准确地说，UTM 是统一威胁管理（Unified Threat Management）的缩写。它最早由FortiNet公司在2002年提出，当时因为混合威胁的频繁出现，为了满足中小企业对防火墙、IDS、VPN、反病毒等安全产品和功能的集中管理需求，FortiNet提出了试图将这些技术整合进统一的设备里，以用来实现统一威胁管理设备的整合。由此，一个新的概念诞生了。但在UTM发展的初期，安全厂商对UTM的解释不尽相同，主要体现在UTM 应该包含哪些功能。

直到 2004 年 9 月，美国著名的市场研究机构——IDC，首度为统一威胁管理提出明确定义，具体定义如下：

1．UTM安全设备是由硬件、软件和网络技术组成的具有专门用途的设备，它主要提供一项或多项安全功能。它将多种安全特性集成于一个硬设备里，构成一个标准的统一管理平台。

2．UTM 设备应该具备的基本功能包括网络防火墙、网络入侵检测／防御和网关防病毒功能。这几项功能并不一定要同时都得到使用，但它们应该是UTM 设备自身固有的功能。

3．UTM 安全设备也可能包括其它特性，例如安全管理、日志、策略管理、服务质量（QoS）、负载均衡、高可用性（HA）和报告带宽管理等。不过，其它特性通常都是为主要的安全功能服务的。

而国际权威的网络与安全测试机构NSS Group为了测试UTM设备，更明确定义出UTM是组合了防火墙、VPN、IDS/IPS、防病毒、防垃圾邮件、网址过滤、内容过滤等功能的单一设备，具体功能定义如下：

1．防火墙：部署在网络边界，状态防火墙支持NAT。

2．VPN：部署在企业广域网作为分公司网络解决方案之用，需要能建立少量的安全 VPN 通道。

3．IDS/IPS：IPS功能检测和阻挡企图利用网络边界闯入的入侵攻击，预防恶意的网络流量到达服务器。然而，IDS 功能可以检测出入侵攻击，并发出警告，但无法阻挡恶意流量。

4．防病毒：网关防毒过滤能预防网络边界上流入的病毒流量，提高计算机桌面安全，预防内部计算机遭到来自企业网络外的病毒感染。

5．防垃圾邮件：网关防垃圾邮件可以检查进入的电子邮件、过滤垃圾邮件，也可以阻止内部主机发送垃圾邮件到企业外面。

6．网址过滤：使用持续更新的网址分类数据库，防止员工访问违反企业规定的网站。

7．内容过滤：扫描网页和邮件流量的特定内容，防止违反企业规定的内容通过或由企业网络发出。

从UTM概念的形式上来看，既提出了具体产品的形态，又涵盖了更广泛的逻辑范畴。一方面，很多厂商提出的多功能安全网关、综合安全网关、一体化安全设备都符合UTM的概念；而另一方面，UTM的概念还体现了经过多年发展之后，安全行业对安全管理的理解以及对安全产品技术的研究。

目前UTM产品百花齐放，但国际、国内都没有统一的标准规定。UTM设备的功能、性能等指标，加之各家实现方法不同、包含功能也不尽相同，所以UTM还需进一步统一产品标准，加强规范性。

二、UTM逐渐升温

其实，UTM在国际上的发展一直不温不火，直到2005年，UTM似乎才真正开始得到用户的关注，并开始大规模销售和部署。据IDC提供的数据显示，2005年第一季度，UTM安全设备市场发展迅速，与2004年第一季度相比营收增长超过123%，销售数量增长近190%。而从2005年4月到6月，UTM设备在欧洲市场，从去年几乎为零发展为占欧洲信息安全设备出货量的11%。

IDC预测，从2003年到2009年，防火墙/VPN销售呈下滑趋势，达到-4.8%，而UTM市场将会有大幅度的增长，到2009年时达到23.6亿美元，并将占据整个信息安全市场的半壁江山，达到47.9%。

Worlwide Threat Management Security Appliance Revenue by Segment,2003-09($M)

	2003			2006	2007	2008	2009	2004-2009 CAGR(%)
Firewall/VPN	1,479.1	1,686.2	1,581.9	1,489.9	1,412.2	1,348.0	1,317.6	4.8
Intrusion detection and prevention	263.8	496.3	691.7	879.3	1,059.8	1,225.9	1,342.9	22.0
Unified threat management	104.9	333.6	677.0	947.0	1,282.0	1,870.0	2,364.0	47.9
Total	1,847.8	2,516.1	2,950.6	3,316.2	3,754.0	4,443.9	5,024.5	14.8

Source：IDC.2005

图表1：IDC数据分析表格

一时间，各种厂商开始纷纷进入UTM市场领域，这些厂商包括防火墙厂商、防病毒厂商、IDS/IPS厂商、内容过滤厂商，甚至网络设备厂商。2003年，全球市场上只有7家UTM厂商，而到了2005年底，数量超过了数十家。正因为UTM产品受到厂商技术背景的影响，所以UTM产品在涵盖功能及技术实现方面各不相同，从而引发UTM是以防火墙为核心还是以IDS/IPS为核心的争论。

我们从UTM厂商背景来看，目前UTM厂商分为几大类型：

第一类是传统的UTM厂商，例如FortiNet公司推出FortiGate病毒防火墙，这款UTM产品集成了防火墙、VPN、

IPS、流量控制、反病毒、内容过滤等多种功能，还获得四项ICSA认证，包括反病毒、防火墙、VPN、入侵检测；而SonicWALL 互联网防火墙 /VPN 安全设备是SonicWALL公司发布的UTM产品，把防火墙、VPN、网关防病毒、防间谍程序、入侵防护、内容过滤、防垃圾邮件集成在一个容易部署及管理的解决方案中。

第二类是主流的防火墙厂商，例如Check Point公司推出Safe@Office 安全专用设备，是专门为满足小型企业各种安全需求而设计的整合安全网关，易于使用及管理。

第三类是主流的IDS/IPS厂商，例如ISS公司的Proventia M系列，集入侵检测和防护技术、防火墙、虚拟专网(VPN)、网关防毒、内容过滤、反垃圾邮件和漏洞检测技术于一体，识别和阻止各种威胁；2005年11月份，3Com公司宣布推出一改以往以防火墙为UTM核心的技术架构，转而推出以IPS为核心的UTM设备TippingPoint X505，组合状态检测防火墙、VPN、宽带管理、网络内容过滤和动态路由技术。

第四类是综合的网络设备／安全厂商，例如Cisco公司发布Cisco ASA 5500 系列自适应安全设备，提供了先进、高性能的保护，集成防火墙、入侵防御系统、网络防病毒和IPSec/SSL VPN 技术，提供了强大的应用安全；2006年2月，Juniper公司推出安全业务网关500系列（SSG），集成了局域网和广域网界面的全新高性能防火墙／虚拟专网平台，并提供可选择的入侵防护、网页过滤、防病毒和防垃圾邮件能力；LinkTrust Border Protector是安氏中国公司专为企业设计的一款集防火墙、防病毒、VPN、内容过滤、反垃圾邮件、流量整形、IDS 等技术于一身的主动防御系统，为企业级用户提供高度安全的一体化解决方案；Symantec Gateway Security是Symantec公司推出的适用于中小企业的高性能、低维护成本的网络设备，采用全面检查防火墙、病毒防护、具有广告软件和间谍软件防御功能的入侵防御、反垃圾邮件、入侵检测、内存过滤、IPsec 和 SSL VPN 技术，提供全面的网络防护和集中的安全管理。

这些信号都表明，UTM正逐渐升温。IDC在去年的一份有关UTM的调查报告认为，UTM将有可能取代防火墙，成为人们首选的安全设备。

三、UTM市场表现有待提升

然而，不同的声音也不是没有，去年就有媒体称，“从面市的第一天起，UTM设备就成了安全市场上诱人的苹果，只不过，不管从技术还是从用户的介绍程度来看，这个高高挂在枝头上的苹果，还略带青涩。”

这似乎不无道理。日前，据IDC最新发布的报告显示，2005年中国IT安全市场总量为3.781亿美元，比IDC在2005年初预测的3.63亿美元高出1510万美元。但同时指出：大家寄予厚望的“统一威胁管理硬件”UTM市场，并没有像预期那样快速成长，进而成为中国IT安全市场的中间力量。

UTM时代是否真的来临?(技术篇)

绿盟科技 陶智

在市场篇中，我们讨论了UTM的概念和标准，分析了市场研究机构的预测，回顾了UTM产品的市场表现。UTM市场虽然火热，但这些来自市场的声音是否真正代表了用户的心声呢？本篇我们从根源着手，就用户需求、UTM技术的演绎为大家做深入的剖析 ，看看UTM时代是否真的来临？它是否已经是一个成熟的安全解决方案？

一、用户需求

用户为什么需要UTM产品？这需要从外因和内因两个方面来分析。

1.外因

从当前安全形势就可以看出端倪。近几年来，随着互联网的发展，黑客攻击技术也在不断变化，网络安全呈现出很多新的问题，表现为：

● 攻击手段更加灵活，混合攻击急剧增多。当前的黑客手段和计算机病毒技术结合日渐紧密，攻击效果更显著，例如Nimda、CodeRed等网络蠕虫造成很大危害。

● 系统漏洞发现加快，攻击爆发时间变短。近年来新的计算机安全漏洞不断被发现，使网管员疲于奔命，“零日”攻击威胁严重。

● 电子邮件问题严重，间谍钓鱼威胁安全。垃圾邮件和病毒是困扰电子邮件的两个主要问题，不仅占用网络带宽和服务器资源，浪费用户时间，还带来病毒和恶意代码。

所以传统安全解决方案，如单一的防火墙、单一的防病毒已经无法有效解决这些问题。

2.内因

UTM是统一威胁管理的缩写，是集成包括防火墙、VPN、IDS/IPS、防病毒、防垃圾邮件、网址过滤、内容过滤等多种功能于一体的安全设备，它具有以下优势：

● 提高安全性。UTM设备将多种安全功能融合在一起，成为防御混合型攻击的“利剑”。混合型的攻击可能攻破单点型的安全方案，但却很可能在统一安全方案面前“败下阵来”。

● 降低复杂性。UTM设备一体化的设计，简化了产品选择、集成和支持服务的工作量。简单的放置、方便的安装是UTM设备的优点。

● 减少维护量。UTM 设备通常都是即插即用的，只需要很少的安装配置。作为单一的设备，更容易排查故障。这项特性对于那些没有专职技术人员的小企业显得尤为重要。

二、技术实现

UTM 设备虽然集成包括防火墙、VPN、IDS/IPS、内容过滤等多种技术于一体，但由于目前的UTM 厂家没有能力掌握全部技术，往往在一种核心技术的基础上加入其他技术，从而衍生出来UTM。因此就出现了UTM 产品以什么为核心的纷争。

目前来看，UTM 设备主要有三种出身：一种是从防火墙技术衍生出来的，一种是从防病毒技术衍生出来的，还有一种是从入侵检测/保护技术衍生出来的。一时间，不同技术出身的UTM 产品厂商均表明自身技术上有优势，而对方技术有瑕疵。以防火墙为核心开发UTM 是目前大多数UTM 厂商的做法，正是因为如此，IDC 在一份调查报告中宣称“UTM 将有可能取代防火墙，成为人们首选的安全设备”。

从发展方向看，未来将不存在防火墙、防病毒、入侵检测技术等谁为核心的问题，因为UTM 设备中各种技术的“深度融合”才是大势所趋。在此之前的各种UTM 产品仅仅是打着UTM 旗号的防火墙、防病毒或入侵检测/防御产品，离真正意义上的UTM 差距还很远。

从技术角度来说，实现UTM 需要无缝集成多项安全技术，达到在不降低网络应用性能的情况下，提供2—7 层的安全防护，所以以下一些关键技术实现了，才能说是达到了 UTM 的部分预期目标：

1.高性能的硬件技术

UTM 产品相对于防火墙来讲，不仅仅是功能增加了很多，检测的层次也从防火墙的网络层上升到了应用层，这对于硬件资源的占用是成百倍甚至上千倍的。由此导致的结果就是，UTM 产品虽然功能很多，但在多种功能同时运行时，性能会大打折扣甚至无法运行。

只有采用高性能的硬件技术，才能实现实时的数据包检测、特征匹配、应用协议分析与处理、高速的 VPN 加密/解密、流量整形。显然，X86 架构不能够满足要求，NP 和 ASIC 加速技术是目前更好的选择。因此采用更优秀的硬件平台提高性能，是 UTM 产品的必然趋势。

2.深度融合的技术平台

UTM 产品包括防火墙、网关防病毒、IDS/IPS、VPN、内容过滤等功能模块，各种功能模块对数据的处理各有其处理方式及资源占用。如果基于某个功能模块发展起来的UTM 产品，没有充分考虑到技术的深度融合，只是一味地将很多功能“简单叠加”到一起，其结果将直接影响UTM 系统效率，造成整体性能下降，甚至整个设备的不可用。

所以，UTM 产品需要在一个统一平台基础上，深度融合各种技术，以达到产品技术组合的最优化。

三、冷眼旁观

虽然UTM市场喧嚣火热，但据IDC最新发布的报告显示，大家寄予厚望的“统一威胁管理”UTM市场，并没有像预期那样快速成长，进而成为中国IT安全市场的中间力量。不少用户对UTM仍持有怀疑的态度：

1.性能是关键

这是最受客户关心和最被业界质疑的因素。因为硬件平台及软件系统方面的问题，目前的UTM产品在多种功能同时运行时，性能会大打折扣。作为集成网关，这将直接影响到用户的业务应用。有些UTM厂家建议，在使用初期，先打开最需要的某一功能模块，再根据变化的使用要求，逐步打开其他功能模块。但这种变通的方法恰恰与UTM多功能特性相违背，根本之道还在于采用更优秀的硬件平台以提升整体性能，这还需要很长一段路要走。

2.稳定是前提

对于安全设备来说，稳定性是尤其重要的。UTM软件系统的复杂性带来了稳定性的损失和Bug的增加。尤其是当某项功能出现问题时，极有可能导致整个设备的不可用。这不仅需要在硬件平台上下功夫，还要考虑到技术的深度融合，提高软件系统的稳定性，减少当机率、重启率。

3.功能是保障

目前UTM产品多多少少还存在“单边产品”现象，所谓单边产品就是其中某一项功能强，而其他功能相对较弱。这是由UTM厂家技术背景决定的。用户在选择产品时，要注意了解UTM产品每个功能的技术实现程度，不要简单地以功能多少评判UTM产品优劣。

例如一些UTM厂家总会拿产品中装有IPS模块来说明自己系统的完善，实际上主流IPS厂商在IPS技术方面都有较强的实力和长期的技术积淀，这是UTM厂家做不到的，孰优孰劣只要进行产品测试就可见分晓。目前，绝大部分UTM产品所获得的产品资质证书上往往赫然写着“防火墙”的字样，这一方面表明目前的UTM产品在防火墙方面做得都不错，通过了产品评测，但另一方面，对于UTM其他功能，却也许没有获得相应的产品资质，这恰恰也从侧面反映出：其它功能技术还不够成熟是不可回避的现实。

4.询价要全面

除了设备采购价格之外，客户仍需关注UTM各功能模块的服务费用。不必说UTM厂家自己提供的防火墙等产品升级服务，单说第三方厂商的软件升级如病毒库、URL库、攻击规则库等每年都需要一笔不少的费用。因此用户考虑UTM的价格时，一定要全面分析。

5.标准是助力

目前国际、国内都没有统一的标准对UTM设备的功能、性能等指标做统一的规定，加之各家实现方法不同、包含功能也不尽相同，对UTM产品的评测对比产生很大的影响，在国内，很多项目投标时，UTM设备的标书还是按照防火墙类别制定的。所以UTM规范性还需进一步统一和加强，以推动UTM市场的进一步发展。

四、何时来临

IDC 预测信息安全市场将以“波浪形”的模式发展，2004_2005 年的增长速度加快，然后到 2006_2007 年将会下降，到 2008 年重新开始上升。这个预测同时考虑了新购买和以往设备更新替代的因素。根据常规，在厂商发布新型号产品之前，市场将会增长放缓，而当厂商发布新产品时，市场增长率会提高。

所以笔者认为，随着UTM性能的提升、功能的不断增强，至少在2008年以后，UTM的时代才会真的来临。

通过风险评估掌握当前的安全状况

绿盟科技 王红阳

前言

风险评估的极端重要性已经越来越被用户认同。在2000－2001年，大多数用户的安全评估需求主要集中于系统脆弱性评估和渗透性测试；在2001－2002年，多数用户的安全评估需求已经侧重于整个管理体系的评估和对特定应用系统的评估；从2002年开始，许多行业用户对全面风险评估提出了要求。

标准与理论

我们在风险评估实践中，主要参考了BS 7799（ISO/IEC 17799）、ISO/IEC 15408—1999（等同GB/T 18336—2001）、ISO/IEC 13335、SSE—CMM等标准。另外，我们也参考了GB 17859—1999《计算机信息系统安全保护等级划分准则》、中国信息安全产品测评认证中心《信息系统安全保障等级评估准则》、公安部《信息系统安全等级保护评估指南》、GB9361—88《计算机场地安全要求》，以及CAV公共漏洞和暴露标准、CRAMM/OCTAVE/ 等标准和法规。

信息安全管理标准BS 7799（ISO/IEC 17799）

BS 7799是国内外现在比较流行的信息安全管理标准，其安全模型主要是建立在风险管理的基础上，通过风险分析的方法，使信息风险的发生概率和后果降低到可接受水平，并采取相应措施保证业务不会因安全事件的发生而中断。BS 7799给出了10类需要进行控制的部分：安全策略、安全组织、资产分类与控制、个人信息安全、物理和环境安全、通信和操作安全、访问控制、系统的开发和维护、商业持续规划、合法性要求等方面的安全风险评估和控制，以及127项控制细则。

BS 7799中关于风险管理框架的构建过程对我们进行安全风险评估给予了宏观上的指导。

信息安全通用准则ISO/IEC 15408—1999

信息技术安全性评估通用准则ISO/IEC 15408—1999（等同GB/T 18336—2001），即通用准则CC，是评估信息技术产品和系统安全性的基础准则。该标准针对在安全性评估过程中信息技术产品和系统的安全功能及相应的保证措施提出一组通用要求，使各种相对独立的安全性评估结果具有可比性。

ISO/IEC 15408对确定安全风险评估模型及关键风险因素具有指导意义，但更重要的是它能比较好的指导我们对系统安全功能的各方面进行安全检查和分析，保证了安全风险评估的全面性和完整性，也使得信息系统在技术上能够符合国家安全测评认证的要求。最后，我们可以根据这个标准生成针对信息系统安全的规范化的安全评估方案，或者更确切叫信息系统安全规范。

系统安全工程能力成熟模型SSE—CMM

SSE—CMM是“系统安全工程能力成熟模型”的缩写。系统安全工程旨在了解用户单位存在的安全风险，建立符合实际的安全需求，将安全需求转换为贯穿安全系统工程的实施指南。系统安全工程需要对安全机制的正确性和有效性做出验证，证明系统安全的信任度能够达到用户要求，以及未在安全基线内仍存在的安全问题连带的风险在用户可容许、或可控范围内。

SSE—CMM针对风险评估过程提供了影响、风险、威胁和脆弱性的具体评估方法和过程，进一步为安全风险评估的实施提供了指导。

应用SSE—CMM模型，我们在实践中，将整个安全风险评估工程划分为以下几个阶段：安全需求分析阶段、安全系统规划阶段、安全系统实施阶段、安全系统确认阶段和安全需求验证阶段，并在安全工程的整个生命周期过程中，严格按照SSE—CMM的要求进行实施，以保证整个项目工程的质量。

信息安全管理指南ISO／IEC 13335

ISO/IEC 13335是信息安全管理方面的规范，给出了如何有效地实施IT安全管理的建议和指南。

ISO/IEC 13335为风险评估提供了方法上的支持，它所定义的安全概念全面覆盖了安全风险评估需要考虑的问题，使得最终生成的安全评估方案不但能够保证技术方面的完整，而且能够满足安全管理的要求。

风险评估模型

资产由于自身的脆弱性，使得威胁的发生成为可能，从而造成了不同的影响，形成了风险。换句话说，风险分析的过程实际上就是对影响、威胁和脆弱性进行分析的过程，而且都紧紧围绕着资产。在风险评估中，资产的价值、资产被破坏后造成的影响、威胁的严重程度、威胁发生的可能性、资产的脆弱程度都是风险评估的关键因素。

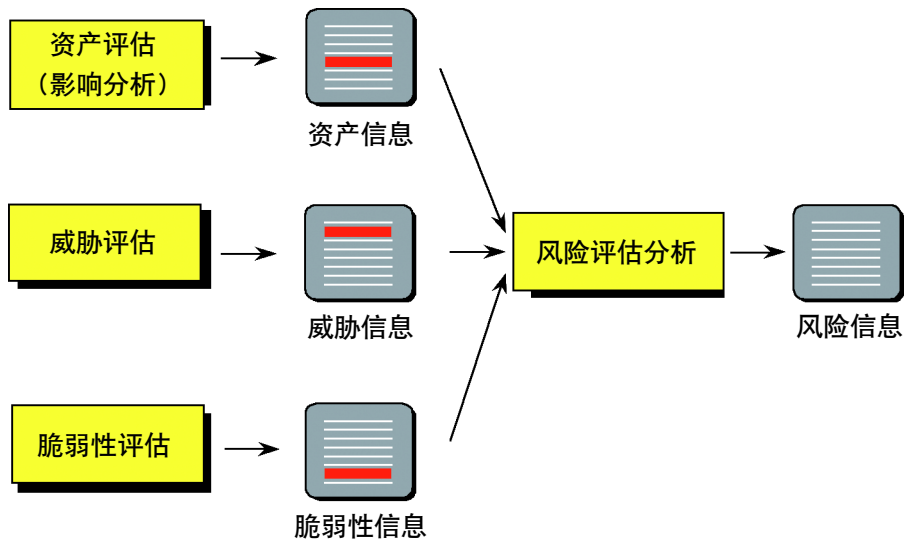


图 1：风险评估模型

风险评估的过程

安全风险评估过程方案是安全风险模型的体现，传统的风险评估过程可以分为以下几个阶段：

第一阶段：确定评估范围和资产识别阶段：调查并了解用户网络系统业务的流程和运行环境，确定评估范围的边界以及范围内的所有网络系统；识别和估价是对评估范围内的所有资产进行识别，并调查资产破坏后可能造成的影响大小，根据影响的大小对资产进行相对赋值；

第二阶段：安全威胁／脆弱性评估阶段：评估资产所面临的每种威胁发生的可能性；脆弱性评估则从技术、管理、策略方面进行的脆弱程度检查，特别是技术方面，以远程和本地两种方式进行系统扫描和手动抽查的评估；

第三阶段：风险的分析阶段：过分析上面所评估的数据，进行风险值计算、区分和确认高风险因素；

第四阶段：分险的管理阶段：这一阶段主要是总结整个风险评估过程，制定相关风险控制策略，建立风险评估报告，实施某些紧急风险控制措施。

八个方面分辨漏洞管理产品优异性

绿盟科技 董明武

如果你的网络计算机数量多到连管理员自己都不清楚: 每台主机使用的是什么操作系统？哪些打了最新的安全补丁？哪些没有打？就表明你已经需要购买一款漏洞管理产品了。然而，当前市场上的漏洞管理产品有很多，选择一台适合的漏洞管理产品，需要注意很多方面的问题。

漏洞管理产品选型指标分为核心必备指标和辅助指标。核心必备指标包括: 厂商自主研究、发现漏洞的能力；产品漏洞知识库的完备性、权威性；产品漏洞评估标准和漏洞识别的准确性；产品对漏洞评估结果数据的分析处理能力。辅助指标包括：产品的易用性、产品的管理功能、产品的扩展性、产品的价格。

厂商自主研究、发现漏洞的能力

纵观国内外的知名漏洞管理产品厂商，每个产品的背后都有一大批“默默无闻”的漏洞研究人员。目前国内的产品中除了ISS、绿盟科技等少数几家有自主研究、发现漏洞能力外，其他厂商都没有相应的技术团队作为后台技术支撑，多数厂商直接采用开源项目Nessus的漏洞及其免费插件。在选择产品时一定要考察厂商的漏洞研究能力，索取自主发现的安全漏洞的列表，并要求提供一年的升级包的具体说明。

厂商每年的规则升级包数量，可以从侧面反映厂商的技术实力和响应能力。如果厂商没有漏洞研究和发现能力，那么后期的规则升级也就得不到很好的保证，对于漏洞管理产品来说，检测规则的升级非常重要。

漏洞知识库的完备性、权威性

漏洞知识库对于漏洞评估类产品来说也是比较重要的，尤其是其全面性。对于网络漏洞管理产品来说，需要漏洞知识库涵盖的绝大多数的远程可以利用的漏洞和信息泄露。除了漏洞库的全面性之外，漏洞库应该具有一定的权威性，必须能够也业内的漏洞标准相兼容（如CVE、Bugtrap）。

目前很多国内的厂商都声称自己的漏洞库和CVE兼容，但是真正获得CVE兼容性证书的产品寥寥无几，用户可以通过让厂商提供CVE兼容性证书的方式来鉴别真伪。绿盟科技一直致力于漏洞研究和发现工作，并在网站上公布了自己的成果，目前拥有国内最为的权威的漏洞知识库。

漏洞评估标准和识别的准确性

目前大多数的漏洞管理产品，在进行评估时仅仅从漏洞的危害严重程度出发，没有从多个角度分析考虑风险，缺乏漏洞评估标准，因此在实际的评估过程中对漏洞的修补工作没有实际指导意义。漏洞管理产品只有将被评估的资产的重要性权值和漏洞威胁相结合才能有效地指导漏洞修补工作。产品的漏洞识别准确性对用户来说也是非常重要的，只有通过实际的测试才能够看出具体的产品之间的差距，同时通过测试也能反映出厂商的技术支持和服务响应能力。

厂商如果没有自主漏洞研究能力，那么漏洞识别的准确性肯定得不到保障，因为这些厂商大多采用的是免费的插件，这些插件的质量参差不齐，导致最后的检测结果存在大量的漏报和误报，甚至导致被扫描目标崩溃。用户在选择漏洞管理产品时一定要通过测试来进行对比测试才能辨其良莠。

对漏洞评估结果数据的分析处理能力

漏洞如果能被准确的识别但得到的结果不能很好的展示，那么再准确的结果也会使用户失去阅读结果的兴致。因此，对于漏洞评估类产品来说，最后的扫描结果的处理能力也是非常重要的。产品最好能够提供结果在线查询和分析的能力，以便用户能够更为准确的定位自己关注的问题；同时产品应该提供一些综合分析和趋势分析的工具，帮助用户从整体上把握资产存在漏洞的概况。用户能够通过一些过滤条件选择自己关心的问题生成相应报表。

产品的易用性

当产品的技术相当时，那么产品的易用性就成了用户非常关注的重点。除了少数专业用户希望使用英文界面产品外，大多数的用户还是希望使用中文界面，虽然一些国外的厂商注意到了英文不适合国内的情况，并翻译了自己的界面和漏洞知识库，但是翻译的准确性还存在一定的差距，可能会出现大量生硬的翻译，这样给用户将来的使用带来了很多麻烦。其次就是产品的安装和维护问题，目前很多厂商的产品，尤其是软件产品，安装和维护的工作量非常大，而这些工作大多需要用户自己来完成，或者通过购买厂商的服务来完成，给用户日后的正常使用带来了很多额外的工作。最后不得不提的就是产品任务的自动执行能力，很多产品宣称自己的产品能够不需要任务干涉自动执行任务，但是在实际使用过程中往往不能够实现自动化，需要自动化实现的工作主要有规则的升级、漏洞管理任务的周期与定时执行、漏洞管理结果的自动发送。这些功能用户需要进行实际测试检查，而不要轻易相信厂商所言。

产品的管理功能

产品除了具备一些核心功能之外，还应该具备一些辅助的管理功能，如系统管理、被扫描资产的管理功能、多用户及权限管理、用户行为审计功能、数据备份和恢复功能等。

产品的扩展性

产品的扩展性需要考虑到以下几个方面：系统是否能够进行大规模分布式部署、是否能够和其他的系统（网管平台或者安全管理平台）整合，最后要考虑产品是否有相应的漏洞管理支持扩展功能模块。

产品的价格

产品的价格在用户购买产品时成为决定因素，用户在购买时往往考虑初次购买成本，而没有从产品的生命周期角度去考虑用户拥有总成本，这是比较片面的。产品的首次购买价格只能作为一个参考指标，而不能作为产品购买的决定指标，如果用户花了很少的钱买到一个根本不能满足自己需求的产品，那又有什么意义呢？只有在产品的核心必备指标相当时，价格才能成为决定的指标；产品如果不具备上述的核心必备指标，价格再低也没有意义。

绿盟科技已经发布极光远程安全评估系统新品——“极光”V4。该产品主要服务于电信运营商、政府和企业，它是一款电信级和企业级的安全产品。该产品依托专业的NSFOCUS安全小组，综合运用了NSIP等多种领先技术，会自动、高效、及时、准确地发现网络资产存在的安全漏洞；尤其是可以对发现的网络资产的安全漏洞进行详细分析，并采用权威的风险评估模型将风险量化，给出专业的解决方案；最值得关注的是它可以提供Open VM（开放漏洞管理）工作流程平台，将先进的漏洞管理理念贯穿于整个产品实现过程之中，是一款不错的可选产品。

产 品 篇

冰之眼 WEB 应用防火墙 ICEYE WAF

绿盟科技 赵旭

业务挑战

随着互联网新兴应用所产生的，不仅仅是价值，还有众多的安全威胁，承载在新兴应用和技术上的攻击不断涌现。Web服务器以其强大的计算能力和处理性能及所蕴含的高昂价值，成为被攻击的主要目标。走在信息化与互联网经济前沿的政府、企业、IDC 等组织面临着各种针对 Web 的安全问题：

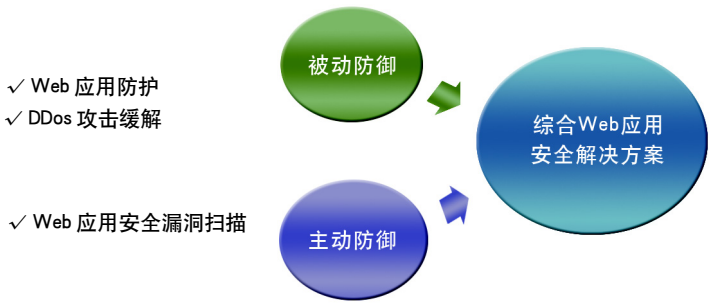
- 网页篡改
- 拒绝服务攻击
- SQL 注入、跨站脚本攻击
- 蠕虫、黑客攻击
- 内部维护人员疲于补救 Web 应用安全漏洞
- 需要付出高昂代价以获取第三方服务：应急响应、安全加固、渗透测试

随着攻击者知识的日趋成熟，针对Web应用的攻击工具与手法日趋复杂多样。传统的边界安全设备，如防火墙，局限于自身的检测机制和防护深度，已经不能满足日益发展的 Web 应用防护的全部需求。

新型 WEB 应用防护系统

Web 应用防火墙（Web Application Firewall，简称：WAF）代表了一类新兴的信息安全技术，用以解决诸如防火墙一类传统设备束手无策的 Web 应用安全问题。WAF 作为一种在国际安全市场上新起的专用设备，在世界范围的安全市场内有明确的功能定义。但国外WAF的定义在某些方面缺少对中国国情的特殊性考虑，比如目前国内比较泛滥的 DDoS 攻击等。

针对目前国内政府、企业各类组织所面临的众多Web应用安全问题以及由此衍生的维护、管理问题，绿盟科技国内首家推出了拥有自主知识产权的新一代安全产品：冰之眼 Web 应用防火墙（ICEYE Web Application Firewall，简称：ICEYE WAF）。该产品不仅从传统的防御思路出发，防护常见的 Web 应用攻击和现今较为泛滥的 DDoS 攻击，还集成了先进的 Web 应用漏洞扫描技术、提供主动的安全防护，为政府网站、商业网站、企业网站以及 IDC 提供了一种全新的、综合的 Web 应用安全解决方案。



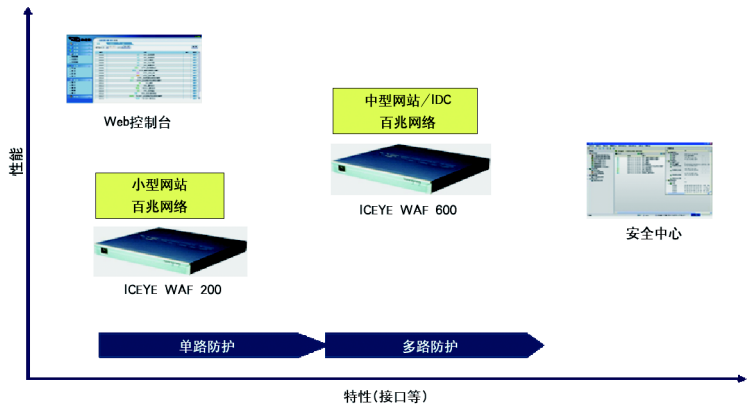
ICEYE WAF 产品设计思路

ICEYE WAF 为各类用户可带来以下收益：

客户群体	解决问题	收　益
政府／企业网站	网页篡改	降低重要无形资产损失风险
互联网企业	拒绝服务攻击、蠕虫攻击、SQL 注入导致的网页篡改、以及网页盗链等	减小交易量下降、广告损失、品牌损失、网站恢复付出较高代价等损失；提供Web应用安全漏洞扫描，以出色的性价比，为网站的维护人员免除后顾之忧
IDC	各类常见 Web 应用攻击以及拒绝服务攻击	确保业务的可用性和连续性，从而满足最终用户对 SLA 的高要求；可作为IDC 安全增值业务平台的重要组件，使安全增值成为可能

产品型号

ICEYE WAF 系列产品包括百兆级处理性能的 ICEYE WAF 200/600 两种型号，提供单路或多路防护，满足政府、企业和 IDC 的各种组网需求，保障客户 Web 系统平稳运行。



ICEYE WAF 产品型号

特性和优势

全面 Web 应用防护

防护各类常见的 Web 应用攻击，如蠕虫、黑客攻击、跨站脚本、网页盗链等。基于智能特征分析技术，提供对 SQL 注入的有效防护，从而在事前有效遏制网页篡改。

细粒度应用层 DDoS 攻击防护

对HTTP Get Flood等常见攻击行为进行有效识别，并实时阻断；基于智能关联分析技术对CC攻击进行检测、防护；提供针对传奇游戏的攻击防护，如常见的假人攻击、创建帐号攻击、数据库攻击等。

无缝集成 Web 漏洞扫描

检测诸如 SQL 注入、跨站脚本（XSS）等 Web 应用漏洞，提供主动防御，从而增强了 Web 应用自身的安全。

软／硬件 BYPASS 以及双机热备

消除传统串联设备可能形成网络单点故障的隐患，确保 Web 业务的可靠性和高可用性。

成熟管理功能

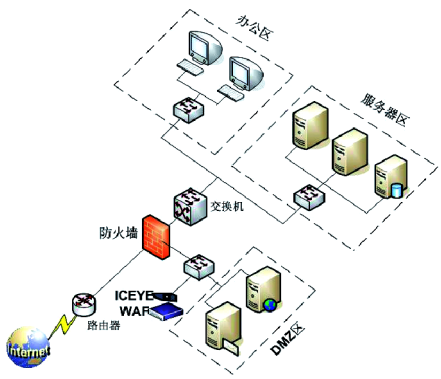
充分考虑了国内用户的使用和维护习惯，提供功能强大、易用性好、灵活的管理功能：

- 提供基于 IP、端口、协议类型、时间及域名的灵活访问控制；
- 基于对象的虚拟防护，为每位用户量身定制安全防护策略，轻松增值；
- 支持规则的在线升级和离线升级。

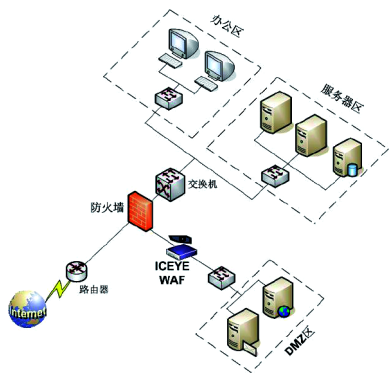
ICEYE WAF 功能特性

典型应用场景

ICEYE WAF 主要支持两种工作模式：在线部署及旁路监听模式。通常，ICEYE WAF 在接入到网络中、提供防护之前，一般先采用旁路监听的方式，学习网络环境及 Web 应用攻击特征，从而配置合理、有效的防护规则。对 Web 应用环境和攻击特征学习完成以后，ICEYE WAF 作为在线设备，串联部署在 Web 服务器前端，对进入 Web 服务器的流量进行有效检测，从而确保 Web 应用的安全。ICEYE WAF 作为透明网桥，接入到网络中即可使用，极大程度降低维护成本。



ICEYE WAF 旁路监听部署



ICEYE WAF 在线部署

产品功能

类别	功能	特性
安全防护	安全区模式	支持直通（Direct）、透明（Layer2）、监听（Monitor）及管理（Mgt）模式
	Web 应用防护	防护 SQL 注入、跨站脚本、目录遍历漏洞利用以及非法脚本执行等 Web 应用攻击
		支持对黑客扫描和攻击的防护（包括蠕虫等对HTTP 和HTTPS 的攻击）
		支持网页盗链防护
	DDoS 攻击防护	提供针对 SYN Flood、ACK Flood、UDP Flood、ICMP Flood 以及 CC 等 DDoS 攻击的防护
		支持针对传奇游戏等网游攻击（创建帐号、数据库攻击、假人攻击等）的防护
	Web 漏洞扫描	针对 SQL 注入及跨站脚本等 Web 应用漏洞进行扫描
	访问控制	支持基于 IP、端口、协议、时间以及域名的访问控制
	响应方式	支持丢弃数据包、丢弃会话的主动响应
		支持TCP Killer、安全中心显示、日志数据库记录、SNMP Trap（v1&v2&v3）等被动响应
网络协议	链路层协议	支持 802.1Q
	系统管理协议	支持 SNMP v1&v2&v3
管理功能	多链路防护	最多可支持两路防护
	业务管理	基于对象的策略管理，实现对不同的用户IP提供不同的防护策略
	设备管理	同时支持 B/S 和 C/S
		支持 Console 接口、SSH 终端服务
	规则升级	支持规则的在线升级和离线升级
	日志报表	提供攻击发生情况的监控、统计、日志功能
HA	BYPASS	当发生软件、硬件和电源故障时设备自动直通，保证网络可用
	双机热备	通过心跳线监控双机状态，实现会话同步和规则同步，提供 A/A 和 A/S
自身安全	管理通讯	高强度 SSL 加密
	其他	提供多点备份、日志缓存、用户分级、用户审计、口令认证、
		证书认证功能　支持安全内核 OS
		自主知识产权

性能指标

	ICEYE WAF 200	ICEYE WAF 600
吞吐量测试（bps）	200M	600M
延迟测试(us)	<60	<60
最大并发TCP会话数	10万	20万

攻击类型	新建连接成功率14.8万pps(64字节)	连接保持率14.8万pps（64字节）
SYN Flood	100%	100%
ACK Flood	100%	100%
UDP Flood	100%	100%
ICMP Flood	100%	100%
混合攻击	100%	100%

产品规格

	产品规格	ICEYE WAF 200	ICEYE WAF 600
接口	工作口	最多两个10/100Base-TX端口	最多四个10/100Base-TX端口
	管理口	最多四个端口	最多四个端口
	串口	一个RS232串口	一个RS232串口
物理特性	尺寸	390*430*44mm（1U）	390*430*44mm（1U）
	重量	7kg	7kg
	电源	100-250V，AC，(50-60HZ)，3A，250W	100-250V，AC，(50-60HZ)，3A，250W
	平均无故障时间（MTBF）	超过100,000小时	超过100,000小时
	工作温度	0~40℃	0~40℃
	非运行温度	-20~65℃	-20~65℃
	相对湿度	5%~95%，非凝露	5%~95%，非凝露
	高度	海拔0-5,000米	海拔0-5,000米
	执行辐射标准	Class A，EN55022，FCC Part15	Class A，EN55022，FCC Part15

软件要求

冰之眼安全中心要求

操作系统	MS Windows 2000 简体中文及以上版本
CPU	Intel Pentium III 800MHz
内存	256M（推荐 512MB）
硬盘	安装时需要 300MB，运行时需要 5GB
显示卡	Windows 兼容系列显示卡
网卡	Windows 兼容 10/100MB 网卡
特别需求	浏览器建议使用 IE6.0 或 Firefox2.0 及以上版本
数据库	MSDE 或 MS SQL 数据库，需要 10GB 硬盘空间

Web 控制台要求

操作系统	MS Windows 98/me/2000/XP/2003 简体中文及以上版本
CPU	Intel Pentium II 500MHz
内存	256MB
硬盘	需要 10MB
显示卡	Windows 兼容系列显示卡，1024X768 分辨率
网卡	Windows 兼容 10/100MB 网卡
特别需求	浏览器建议使用 IE6.0 或 Firefox2.0 及以上版本

冰之眼 Web 应用防火墙的典型应用

绿盟科技　赵旭

针对政府／企业以及IDC客户，冰之眼Web应用防火墙（ICEYE Web Application Firewall，简称ICEYE WAF）ICEYE WAF可提供不同环境下灵活、可靠的Web应用防护解决方案。

政府／企业网站防护

如图1.1所示，Web服务器部署在DMZ区，对外提供Web应用服务。ICEYE WAF作为串联设备，部署在DMZ区Web服务器群接入交换机前端，对进入Web服务器集群的流量进行有效监控，从而确保Web应用的安全。

通过对SQL注入等Web攻击的有效防护，可以极大降低政府网站遭受网页篡改的可能。ICEYE WAF作为透明网桥，直接接入到网络中即可使用，极大程度降低维护成本。

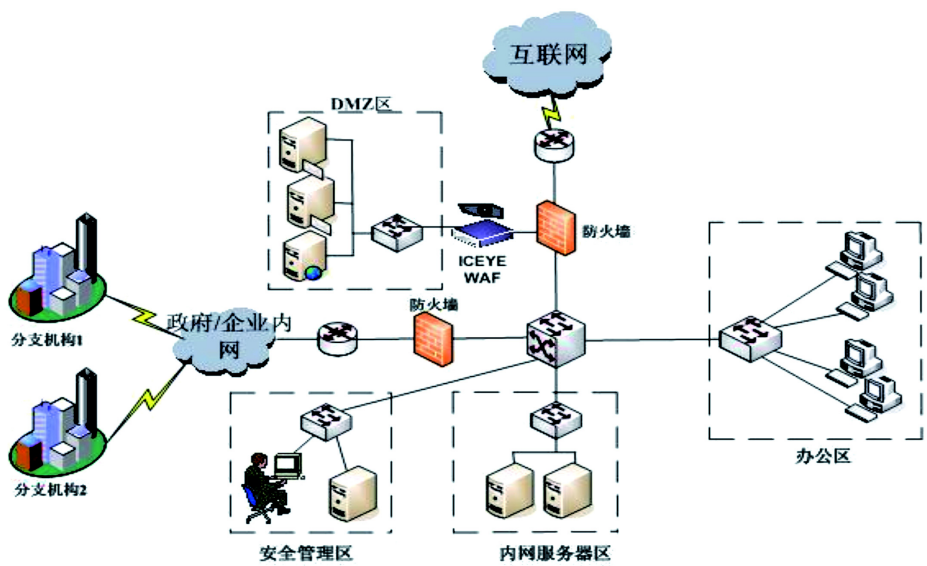


图 1.1：政府／企业 Web 应用防护系统部署

IDC 环境应用

在 IDC 环境的应用相对政府、企业的应用复杂。由于 IDC 提供多种应用服务，本身具备极大的攻击价值，从目前发生的案例来看，一是可能在网络出口处遭受带宽耗尽型的 DDoS 攻击，二是针对内部 Web 应用和网络游戏的攻击，后者防范的难度更大，需要更为细粒度的防护。在 IDC 中，可以考虑在出口处部署专业的流量清洗设备，应对带宽耗尽型的攻击，而在 Web 服务器前端部署 ICEYE WAF，应对各种 Web 应用攻击。

如图 1.2 所示，对于最为核心的 Web 服务，可以在 Web 服务器网络接入交换机前端部署 ICEYE WAF 双机。双机可采用 Load balance 或者 failover 的工作模式，提供高性能、高可靠性的 Web 应用防护，轻松应对百兆环境下网游最为敏感的 DDoS 攻击。

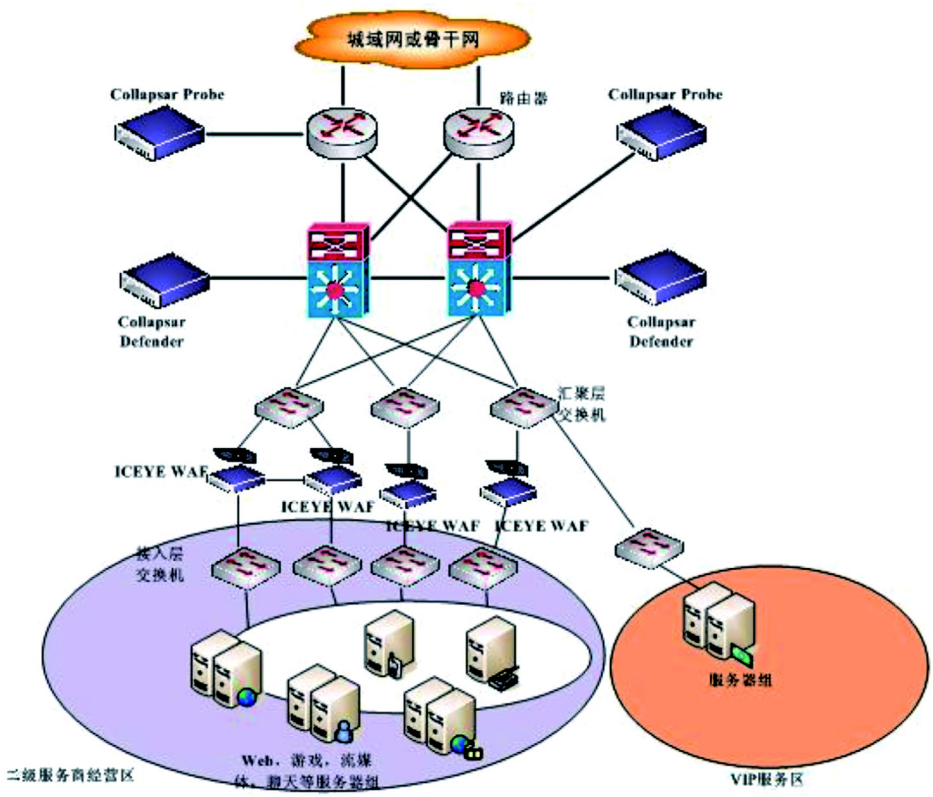


图 1.2：IDC 环境中 Web 应用防护系统部署

方 案 篇

电信运营商 IDC 安全建设方案

绿盟科技 万慧星

一、概述

IDC 即是 Internet Data Center，是基于 INTERNET 网络，为集中式收集、存储、处理和发送数据的设备提供运行维护的设施以及相关的服务体系。IDC 提供的主要业务包括主机托管（机位、机架、VIP 机房出租）、资源出租（如虚拟主机业务、数据存储服务）、系统维护（系统配置、数据备份、故障排除服务）、管理服务（如带宽管理、流量分析、负载均衡、入侵检测、系统漏洞诊断），以及其他支撑、运行服务等。

随着中国互联网以超常的速度向前发展，企业用户对IDC的需求也日益增长，而随着电信运营商业务转型，各种数据业务也层出不穷，比如中国电信开展的互联星空计划的实施、中国移动的ADC业务系统等也受到越来越多的用户认可，作为其主要业务平台 IDC 也受到越来越多的关注，而安全性则是焦点之一。

本文主要是通过对 IDC 网络系统和业务系统现状的介绍，分析其安全状况，然后对当前 IDC 存在的安全风险进行整理和分析，再提出针对 IDC 的网络安全解决方案。

二、IDC 安全现状

2.1 网络和业务现状

典型的 IDC 通常由网络骨干层、汇聚层和接入层 3 个层面构成，骨干层通过高性能路由器连接两个或者以上的运营商互联网骨干网，提供INTERNET接入，并实现链路备份，核心路由器以下则为两台核心交换机作为网络的汇聚层，在汇聚层以下由 L2/L3 交换机构成接入层，接入各种托管服务。

IDC 中主要的业务是主机托管业务，现阶段，IDC 中托管的主机系统主要分为两类：

自有数据增值业务，如互联星空、ADC等运营商自己运营的增值业务，这一类业务服务器是属于运营商自有的业务系统，由运营商自行进行日常维护。

托管服务器，如网游的服务器系统、网站系统等，这个部分是 IDC 机房收入的主要来源。在这类托管服务器中，一般有中小型客户和大客户之分，中小客户主要是一般的企业单位租用共享带宽资源，其维护力量较弱；大客户主要是大型的门户网站、专业的网游服务器等，这类用户往往是租用多个机柜部署自己的一整套系统，通常情况下都有自己的一组维护人员进行系统的日常管理和运维。

2.2 IDC 面临的主要安全风险

分布式拒绝服务攻击（DDoS）、蠕虫病毒等大规模的流量型攻击，不仅对 IDC 中直接受攻击的客户服务器带来影响，同时占用大量 IDC 的带宽资源，另外突发大数据流会造成路由交换等网络设备负荷过载，从而导致网络服务质量下降，甚至会出现路由器板卡转发异常以及网络中继拥塞等现象。

针对 IDC 的攻击可以导致企业客户网络的瘫痪，业务中断，这些攻击通常利用设备系统本身的安全漏洞，而且托管设备安全配置的不完善也可以给攻击者可乘之机。针对这些问题的攻击一旦成功，后果不堪设想，将会直接导致客户满意度降低，甚至客户流失。

IDC 机房中托管了很多客户的业务主机，当部分业务主机成为被攻击目标时，往往会影响其他主机的正常业务提供，这主要是由于缺乏有效的安全隔离、安全控制的技术和策略。

托管主机的安全代维服务需求，电子商务网站、政府、企业等大量的中小客户经常遭受网络攻击，服务质量下降，而由于其自身缺乏安全运维人员，迫切需要运营商提供安全服务，为客户的业务系统提供安全保障。

三、IDC 安全解决方案

3.1 方案总体思路

IDC 同行业之间的竞争越来越激烈，IDC 通常采用扩充出口带宽、提升网络核心设备处理能力等来开拓新的客户和留住已有客户，而建设、完善有效的安全管控体系，为 IDC 客户提供一个安全稳定的运行环境也成为 IDC 客户，特别是大客户在选择 IDC 时非常看重的一个硬性指标；同时，通过安全体系的建立能有效的降低由安全引起的运维成本。

建立一个有效的信息安全体系最有效的方式是采用系统化的方法，首先确定信息安全管理策略和范围，然后在风险评估的基础上选择适宜的控制目标和控制方式对风险进行处理，最后制定业务持续性计划，建立并实施信息安全体系。

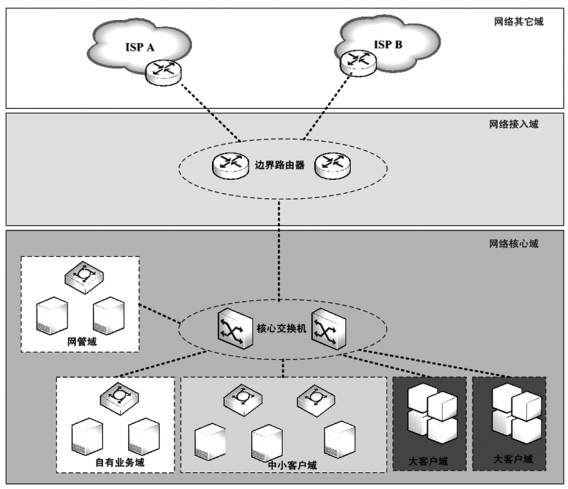
根据上述章节对 IDC 安全风险的分析，现阶段 IDC 的安全体系中需要解决的是构建一套有效的安全防护体系，因此，本方案主要是基于技术措施来构建 IDC 的技术体系，而对于组织管理体系和运维体系的建设不在本文中展开描述。

3.2 基于安全域的防护策略

安全域是由一组具有相同安全保护需求、并相互信任的系统组成的逻辑区域，在同一安全域中的系统共享相同的安全策略，通过安全域的划分把一个大规模复杂系统的安全问题，化解为更小区域的安全保护问题，是实现大规模复杂信息系统安全保护的有效方法。

3.2.1 IDC 安全域划分

通过前面章节对IDC业务的分析，首先可以根据业务系统的不同来进行安全域的划分，主要分为自有业务域，中小客户域和大客户域，然后再根据托管厂商的不同在上述几个安全域中进行细分。



IDC 安全域划分示意图

安全域的划分是为了更好的对不同重要等级的安全域进行适当防护，而防护策略主要分为安全域边界和安全域内部的防护。安全域划分将网络系统划分为不同安全区域，分别进行安全保护的过程，通过安全域的划分和保护，将实现如下意义：

1．基于网络和系统进行安全检查和评估的基础；

2．有效建立安全管理控制点，指导系统安全规划、设计、入网等工作；

3．实现对系统进行重点保护，统一管理的策略，统一信息安全技术支撑；

4．安全域的分割能有效的防护攻击渗透；

5．基于网络和系统进行安全建设的部署依据；

6．安全域边界是灾难发生时的抑制点，防止影响的扩散；

7．有效的避免安全方面的重复投资。

3.2.2 IDC 安全域防护

安全域防护的根本目的是为了保证业务信息系统的稳定、安全运行，使其能够稳健、持续的提供业务服务，保障电信运营商IDC各种业务的正常经营和战略目标的达成。安全保护的对象是业务信息系统内的所有信息资产，包括硬件、软件、服务、信息等，其中重点是服务和信息。

基于 IDC 的业务需求，以及 IDC 面临的安全问题，单一设备或单一系统无法解决 IDC 的安全问题，需要采用多层面全方位的解决方案来应对 IDC 的安全问题，解决思路如下：

1．流量分析系统实时监控分析 IDC 的数据流，获取抗拒绝服务攻击（DDOS）等非法数据流信息。

2．流量净化系统过滤非法数据流信息，保障网络基础架构健康平稳运行，为大客户业务保驾护航。

3．网络入侵检测系统深度检测蠕虫、病毒等应用层攻击。

4．漏洞扫描系统及时发现系统漏洞和风险，为 IDC 安全未雨绸缪。

5．……

3.3 专业安全服务引入

IDC通过与专业的安全服务公司合作，为IDC客户提供专业的网络安全服务，主要包括安全预警通告、紧急事件响应服务、高级安全运维服务等。

3.3.1 安全预警通告

安全问题目前正以每周新增几十甚至几百例的速度在全世界得到反馈，同时涉及信息技术的众多领域，IDC维护人员在安全知识的更新速度方面面临更大的压力。

安全预警以安全通告的形式为IDC提供最新的安全动态、技术和定制的安全信息，包括实时安全漏洞通知、定期安全通告汇总、临时安全解决方案和安全知识库更新等。同时，这些通告信息可以定制化发送给不同的 IDC 托管客户，通过提供安全信息增值服务的方式来增加 IDC 客户的粘度。

3.3.2 紧急事件响应

目前许多IDC或者IDC的客户自身尚没有足够的资源和能力对安全事故作出反应。网络安全的发展日新月异，无法实现一劳永逸的安全，所以当紧急安全问题发生，一般技术人员又无法迅速解决的时候，及时发现问题、解决问题就必须依靠紧急响应来实现。

紧急响应服务提供高效的信息安全事故反应体系，可以帮助 IDC 尽快对信息安全破坏事故作出反应，包括事故处理及恢复、事后的事故描述报告以及后续的安全状况跟踪。同时，当 IDC 中托管的用户主机或 IDC 的网络系统正遭到攻击或发现入侵的痕迹，而又无法当时解决和追查来源时。紧急事件响应将以最快的速度赶到现场，协助 IDC 运维人员解决问题，查找受攻击系统，保存证据和追查来源。

3.3.3 高级维护服务

1．安全设备维护

随着网络安全的不断发展，IDC在信息安全方面的投资也越来越多，各种安全产品在的各个层面部署。而IDC中的安全设备往往买回来后，由于维护力量的不足，往往也搁置不用，在各IDC都多或多或少的存在这样的问题。因此可以通过引入专业的安全服务对各种安全设备进行专业的维护和照料，使之发挥相应的作用，从而有效保护已有安全投资，实现已有安全投资效益最大化的目标。

2．系统安全加固

网络安全是动态发展变化的，需要时刻关注最新漏洞和安全动态，制定更新的安全策略以应付外来入侵和蠕虫病毒等威胁。通过引入安全服务针对网络节点的漏洞和脆弱性，定期的进行安全加固，可以使系统有效的抵御外来的入侵和蠕虫病毒的袭击，使系统可以长期保持在高度可信的状态。

四、结束语

IDC的网络建设和发展是一个长期的任务，随着技术的发展和业务的更新，需要及时的调整已有的安全策略，设计新的网络安全方案。同时，计算机技术和网络技术具有的复杂性和多样性，使得网络安全越来越成为一种专门的技术和服务，需要与专业的安全服务组织合作来进行更全面和完善的网络安全规划和建设。

绿盟科技一直以“巨人背后的专家”为己任，致力于网络安全事业，经过几年的快速发展，已成长为面向国际市场的网络安全解决方案供应商。在本方案设计中，针对现有IDC的主要安全风险考虑了IDC迫切需要的安全措施，能比较好的解决IDC中的网络安全瓶颈。为了针对不同的IDC进行个性化安全方案的设计，我们建议根据IDC的现状进行全面的安全评估，导出需求再进行全面的安全体系设计和规划。同时，在整IDC的安全建设生命周期中，绿盟科技将始终坚持作为IDC最值得信赖的安全顾问，在双方深入合作中共同分享、共同创造，共同为IDC的网络安全建设贡献力量。

网上银行准入解决方案（简化版）

绿盟科技 徐一丁

一、商业银行与网银业务

目前国内银行的网银系统建设，一般会经过系统设计、软件开发、系统集成、内测、安全评估、审批后正式运行等几个过程。绿盟科技已经针对“安全评估——取得银监会许可”的环节设计了专门的评估服务，以满足商业银行在网银上线方面的需求。

1.1 银监会关于网银准入的规定

根据银监会颁布的《电子银行业务管理办法》第十二条的规定，金融机构申请开办电子银行业务，根据电子银行业务的不同类型，分别适用审批制和报告制。

其中，利用互联网等开放性网络或无线网络开办的电子银行业务，包括网上银行、手机银行和利用掌上电脑等个人数据辅助设备开办的电子银行业务，适用审批制。

1.2 银行如何得到网银准入许可

根据银监会的《电子银行业务管理办法》（以下简称《管理办法》），网上银行是电子业务的一种形式。在中国境内开办网上银行业务的金融机构都需要先得到银监会的批准，其中涉及到网上银行安全评估的内容。

首先，开始取得网银准入申请的基本条件是银行的网上银行系统与基础设施已经建成，并顺利完成内测。

《管理办法》第九条规定：“金融机构开办电子银行业务，应当具备下列条件：

其中第四项要求：

（四） 对电子银行业务风险管理情况和业务运营设施与系统等，进行了符合监管要求的安全评估；”

为了保证电子银行安全评估的客观性、及时性、全面性和有效性，银监会依据《电子银行业务管理办法》的有关规定，又制定了《电子银行安全评估指引》（以下简称《指引》）。

《指引》第四条规定：“金融机构可以利用外部专业化的评估机构对电子银行进行安全评估，也可以利用内部独立于电子银行业务运营和管理部门的评估部门对电子银行进行安全评估。”

安全评估是网银准入申请的一个重要部分。安全评估机构需要按照《指引》中的规范进行评估，评估应根据《管理办法》中的要求，出具相关材料，与银行自行准备的材料合在一起，向银监会相关部门提交，正式进行申请。如果银行的网银系统各方面都达到银监会规定的标准，就会得到网银准入的许可。

建议银行使用有经验的外部专业化评估机构提供的风险评估服务，以实现顺利得到银监会准入许可的目的。

1.3 绿盟科技网银准入评估服务

绿盟科技基于多年的金融行业安全服务经验，为银行业客户定制了“网银准入评估服务”（以下简称为“网银准入服务”），专门为各银行申请网上银行业务开办资质提供辅助性服务，在网上银行开通过程中负责安全方面的工作部分，进行安全评估并编写申请资料，作为网银申请材料的一部分；同时安全评估可以有效提高银行网银系统的安全水平，使系统符合自身业务需要和国家相关要求。

二、绿盟科技网银准入服务

2.1 服务目标

● 通过安全评估以及安全改进建议，使得银行网上银行系统符合银监会的《管理办法》中的规定，编写提交银监会的网上银行系统评估验收报告，使网上银行系统能顺利通过中国银行监督管理委员会的检查，正式开通运行。

● 通过安全评估以及安全改进建议，使得网上银行系统的安全保障能力符合国家的相关政策法规和自身业务的要求。

2.2 工作开展依据

银监会颁布的关于网银准入的规范：

● 《电子银行业务管理办法》

● 《电子银行安全评估指引》

2.3 服务内容

绿盟科技作为安全咨询与服务方

● 负责网银准入评估服务方案设计

● 负责具体的安全评估的工作实施

● 负责编写《管理办法》中规定提交的，与信息系统安全相关的申请材料

● 负责提出针对银行网银系统现状的安全现状报告、风险报告和安全改进建议

● 负责对其他应由银行负责准备的文件给出建议，以符合银监会要求

● 负责安全加固方案设计及实施工作（可选项）

2.4 绿盟科技网上银行安全评估内容

下面是绿盟科技安全评估内容的简要介绍，是网银准入服务的核心部分。具体实施内容需要根据银行的实际情况加以调整。

2.4.1 网上银行系统评估内容

根据《电子银行安全评估指引》要求，绿盟科技网银安全评估包括以下内容：

● 安全策略评估

包括安全策略制定的流程与合理性，及各类安全策略制定与执行情况等。

● 内控制度评估

包括内部控制体系的科学性与适宜性，管理层职责，内控机制运行情况等。

● 风险管理状况评估

包括网上银行风险管理架构的适应性和合理性，主要风险识别及管理，规章制度与操作规定、程序等的执行情况等。

● 系统安全性的评估。包括物理安全，数据通讯安全，应用系统安全，密钥管理，客户信息认证与保密，入侵监测机制和报告反应机制等。

● 业务运行连续性计划评估。包括业务连续运营的设备和系统能力和业务连续运营的制度安排和执行情况。

● 业务运行应急计划评估。包括网上银行应急制度建设与执行情况，应急设施设备配备情况，定期、持续性检测与演练情况，应对意外事故或外部攻击的能力等。

● 网上银行风险预警体系

● 其他重要安全环节和机制的管理

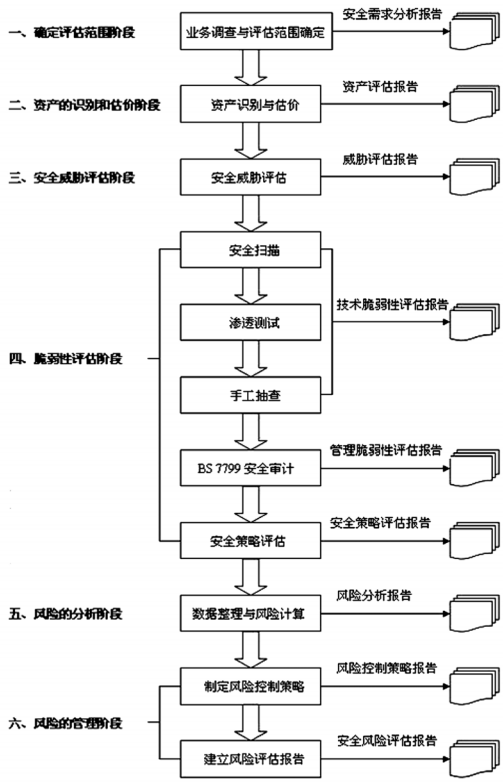
2.4.2 网上银行系统评估流程

2.4.2.1 确定评估范围

调查并了解银行网银系统业务的流程和运行环境，确定评估范围的边界以及范围内的所有网络系统。

2.4.2.2 资产的识别和估价

在资产的识别和估价阶段，对评估范围内的所有资产进行识别，并调查资产破坏后可能造成的影响大小，根据影响的大小为资产进行相对赋值。



2.4.2.3 安全威胁评估

在安全威胁评估阶段，即评估资产所面临的每种威胁发生的可能性。

2.4.2.4 脆弱性评估

脆弱性评估的阶段包括从技术、管理、策略方面进行的脆弱程度检查，特别是技术方面，可能以远程和本地两种方式进行系统扫描和手动抽查的评估。

2.4.2.5 风险分析

风险的分析阶段，即通过分析上面阶段所产生的数据与结果，进行风险值计算、区分和确认高风险因素。

2.4.2.6 风险管理

在风险的管理阶段，会总结整个风险评估过程，制定相关风险控制策略，建立风险评估报告，提出对那些高风险的设备进行安全优化的方案和加固建议。就网络拓扑优化和安全域划分提出建设性的建议。

三、典型案例：南京银行网银准入服务

南京银行的前身为南京商业银行，最初成立于1996年2月6日，现分设58家支行和泰州分行，以及营业部、国际业务部、资金营运中心和特殊资产经营中心4 个直属经营单位，从业人员1400多人，总部位于南京市淮海路50号。

南京银行现为中外合资银行，已经在国内上市。绿盟科技在2006年下半年为南京银行提供了网银准入服务，通过安全评估全面检查南京银行的网银系统，设计安全加固方案并实施，编写向银监会申报材料中安全相关的部分。

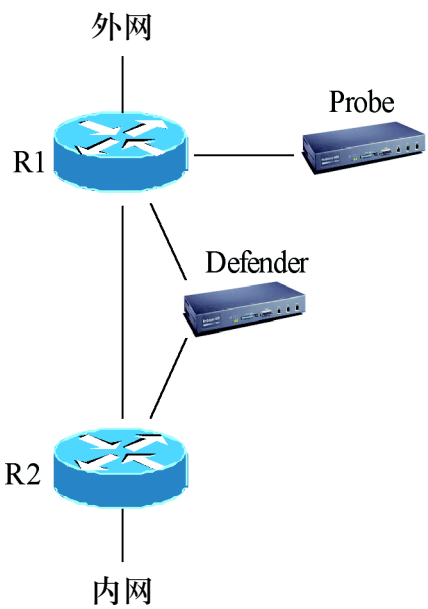
通过绿盟科技的服务，南京银行已经顺利地取得了银监会的网银准入许可，于2006年12月1日正式推出了网上银行业务。系统开通以来一直安全稳定地运行，为南京银行的业务发展提供了有力的支持。

技 术 篇

流量牵引技术在防 DOS 攻击中的应用

绿盟科技 欧怀谷

网络安全技术随着信息技术的发展而日新月异，许多安全技术成并行发展。现在网络安全领域又出现了一个新技术——流量牵引技术。什么是流量牵引？为什么要使用流量牵引技术？我们先从下面的拓扑开始介绍。



什么是流量牵引

上图中的 Defender 就是我们熟悉的抗 DDoS 设备，Probe 是一个专门用来分析网络流量的预警设备。对于这些网络安全设备我们并不陌生，但对于这样的拓扑结构恐怕就不常见了。两个路由器之间是两条并行的线路，在以往部署抗 DDoS 攻击设备的时候通常是把它直接串联在网络中，正常流量和攻击流量都穿过抗 DDoS 设备。让我们先根据这个简单的拓扑来解释一下什么是流量牵引。

在没有 DDoS 攻击的时候，流量直接从 R1 转发到 R2，不经过抗 DDoS 设备。当网络中存在攻击时，例如某台设备 server1 遭受到了 DDoS 攻击，Probe 监测到攻击行为后，目标为 server1 的流量将被转发到 Defender。这些流量到达抗 DDoS 设备后，经过一系列的检测、甄别、过滤等算法，剩余的合法流量将继续被转发到 R2。而此时其它的流量仍然保持原来的路线，即直接从 R1 转发到 R2。

流量牵引就是将攻击流量和正常流量进行分离，由抗DDoS设备来专门抵抗DDoS攻击，保证正常流量尽可能的不受到攻击的干扰。

为什么我们要实现流量牵引

上面我们简单解释了什么是流量牵引，现在分析第二个问题，为什么要进行流量牵引。

流量牵引技术是为了防御大规模DDoS攻击和避免单点故障问题而提出的。最初防御DDoS攻击是依靠防火墙上的抗DDoS模块来完成，后来人们意识到即使再优秀的防火墙产品，上面的抗DDoS模块的防御DDoS功能也都比较弱，由于防火墙自身构造原理造成了抗DDoS的瓶颈，这是一个根本上的障碍。这样人们才改变思路，开始在网络中部署专门的抗DDoS攻击设备。DDoS设备是串联在网络中的，我们大家都知道，网络的拓扑结构越简洁越好，在网络中每增加一个环节就可能会增加一个潜在的故障点。我们设想一下，一旦抗DDoS设备无力抵抗海量的DDoS攻击，那么很可能会造成抗DDoS设备失效，这样就导致了整个网络的断线。流量牵引技术的目的就是为了提高网络抗DDoS的容错性，这好比我们祖先大禹治水时用的策略，一面堆堵，一面疏导。堵也罢，疏导也罢，手段虽然不同但目的始终是唯一的，那就是治水。流量牵引技术使用的都是我们已经熟知的成熟技术，只是换了一种思考的方式，将我们祖先治水的哲学思想用在了抗 DDoS 攻击中。

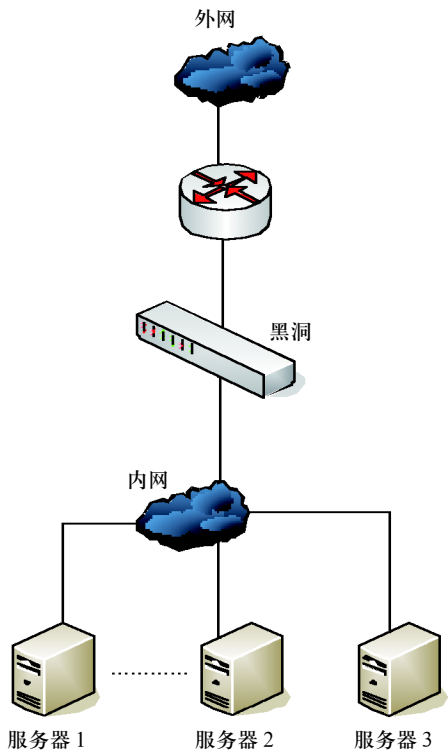
在这里我们继续以上图为例说明。当针对server1的DDoS攻击发生的时候，我们将针对server1的攻击流量牵引到抗DDoS设备上去，其他的流量继续沿原路转发，不受干扰。这样我们首先实现了一个目的，那就是保证多数正常流量不受攻击干扰。经过流量牵引后到达抗DDoS设备上的流量经过分流后必然有所减弱，流量越小抗DDoS攻击设备分析和防御能力就会越强，这样又实现了我们第二个目的，提高了抗DDoS设备的性能。当针对server1的攻击流量到达抗DDoS设备的时候，我们面临两种可能，一种是能够防御的住，一种是防御不住。如果防御的住，那当然就不存在问题了。如果防御不住呢？ 最多会造成被牵引的地址不能被访问，将攻击所能造成的危害降低到最小，不至于因为一个点的攻击而导致整个网络不能通信，这个代价相比而言是最小的。

流量牵引技术的实现

绿盟科技长期以来一直致力于抗DDoS攻击的探索，当流量牵引技术仅仅作为一种学术设想出现在国际网络安全舞台的时候，绿盟人就被其大胆的构想，巧妙的思维所打动，经过缜密的可行性研究后投入了流量牵引技术的研发工作。一方面继续对抗DDoS攻击的深入研究，拓展抗DDoS产品在应用层抵御DDoS的功能，确保绿盟科技的“黑洞”作为抗DDoS专用设备的的领先地位；一方面组织专门人员进行流量牵引技术的分析研究。由于绿盟科技在这两方面的知识储备都比较充足，研发进展很快，现已经推出流量牵引抗DDoS产品，并已在城域网核心，IDC入口大型门户网站，ICP网站等获得了广泛的引用，效果良好。

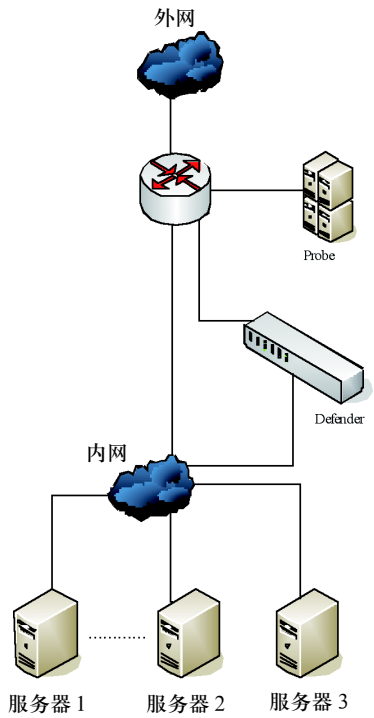
流量牵引技术的应用案例

一家长期和绿盟科技合作的IDC成为了流量牵引的第一个用户，他们三年前就使用绿盟的“黑洞”抗拒绝服务攻击系统来防御DDoS攻击。他们最感兴趣的就是利用流量牵引来避免“触一发而动全身”，也就是说避免因为他们IDC中的个别服务器被攻击而导致整个网络受影响。这是他们以前的一个拓扑，出于安全考虑这个拓扑进行了部分省略。



该IDC中有许多托管主机，每天都会遭受各种DDoS攻击。现在的网络攻击不同于以往了，以前的网络攻击多数属于恶作剧性质，随着网络经济的发展，现在的网络攻击更偏重于经济目的，攻击的组织性计划性很强，攻击目标非常明确。这些托管服务器往往都被放置在一个区域，当针对一台服务器进行攻击的时候也影响到了其他服务器的通信。

采用了绿盟科技的流量牵引技术后，网络拓扑变成了这样的结构：



流量牵引

流量牵引拓扑与上图相比发生了很大的变化，从路由器到内部网络变成了双链路，而且又增加了一个新设备——Probe。为了方便研究，我们假设服务器 1 正在受到攻击。

Defender 是在“黑洞”的基础上发展起来的，在已有技术的基础上加强了对应用层 DDoS 的防御。由于对针对服务器 1 的攻击流量被切换到了 Defender 上，外网到服务器 2 和服务器 3 的访问将不受到干扰，攻击的压力落在了 Defender 和服务器 1 上。这样我们就把被攻击事件限制在了局部。通常 DDoS 攻击目标明确，而且是持续不断的不定期的骚扰。必要的时候也可以通过Probe的监测功能来追踪攻击来源，Probe可以收集到整个网络的netflow信息，通过对这些信息的分析，判断出攻击流量进入网络的入口。层层追踪锁定攻击来源的范围。

检 测 Prode 旁路地部署在入口处，通过接受 netflow 信息或镜像流量，分析被保护网络是否遭受到 DDos 攻击。当检测到攻击事件后，将被攻击的 IP 地址等信息通告给 Defender。

分 流 Defender 接收到来自 Prode 的通告后，通过路由协议改变被攻击地址在路由器上的路由，实现攻击流量与正常流量的分离。

清 洗 Defender 内嵌了“反 IP 欺骗”、“协议行为模式分析”、“特定应用防护”、“用户行为模式分析”、“动态指纹识别”、“带宽控制”等技术。流量到达 Defender 后，通过层层过滤得以清洗。

回 注 Defender 将清洗后的正常流量送回网络中，从而保证网络正常运行。

互联网络的发展不断地改变我们对信息技术的观念，新的安全技术不断涌现，各种技术之间并行发展，作为网络安全管理者来说难度不断加大，网络攻防技术的发展速度是不以任何人的意志为转移的，各项技术未来几年的发展成果几乎没有人能预测的出来。流量牵引技术通过留出余地来防患未然是一个大胆而巧妙的想法，目前绿盟科技公司正率先将其应用于客户的网络中并收到了不俗的效果。在飞速发展的信息时代，站在安全技术的前沿，除了勇敢的去开拓外无他路可走。

绿盟科技“冰之眼”网络入侵检测解决方案

绿盟科技　陶智

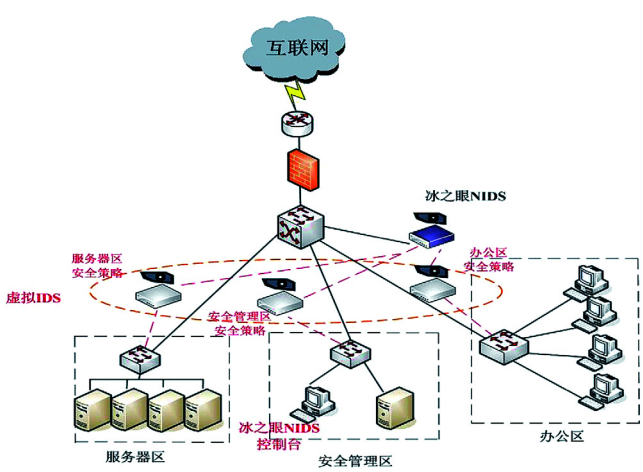
入侵者在实施入侵或攻击时，往往同时采取多种入侵的手段，以保证入侵的成功机率。而这些威胁会对企业造成巨大的损失，对于上述威胁，传统防火墙和防病毒系统都无法有效地检测。为了弥补防火墙的不足，我们需要利用入侵检测技术，实时监控网络资源，精确识别各种入侵攻击，防止入侵造成的危害。在检测到入侵攻击时，通过及时报警、动态防护，来减少入侵带来的损失。

绿盟科技经过多年的研发，可以为客户提供针对小型网络的精细管理方案；针对中型网络的集中管理方案；以及针对大型网络的分级管理整套入侵检测解决方案。从而实现从企业网络核心至边缘及分支机构的全面检测。

“冰之眼”网络入侵检测系统的部署方式灵活多样，能够快速部署在几乎所有的网络环境中，满足不同企业不同管理模式需要。

小型网络之精细管理方案

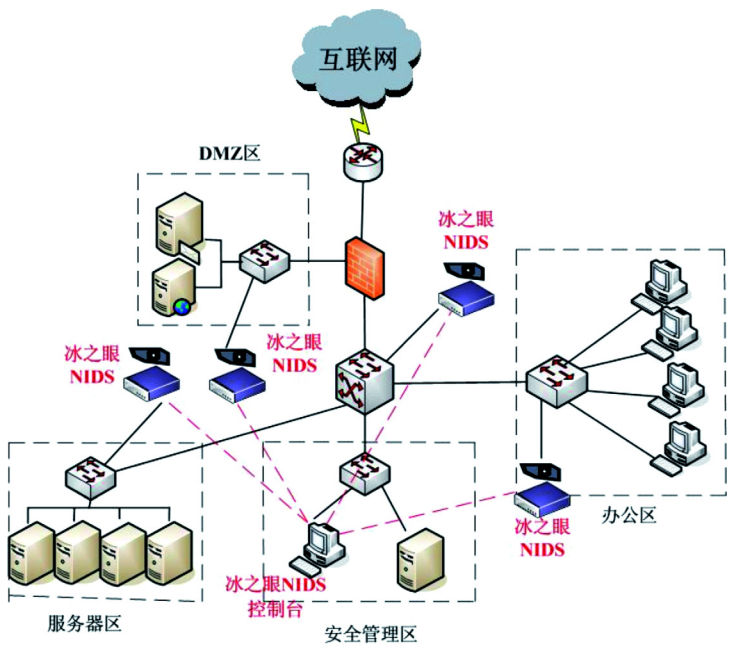
针对小型网络，绿盟科技入侵检测解决方案提供虚拟IDS精细管理方案，通过基于对象的策略管理，“冰之眼”NIDS针对不同部门／网段，制定不同的规则和响应方式，每个虚拟系统分别执行不同的安全策略，实现面向不同对象、实现不同策略的智能化、精细化的入侵检测。如下图 1 所示：



图表 1　精细管理方案

中型网络之集中管理方案

针对中型网络，绿盟科技入侵检测解决方案提供集中管理方案，通过将“冰之眼”NIDS部署在多个关键网段，如安全管理区、DMZ 区、服务器区及办公区，实现多处监控。利用“冰之眼”控制台集中管理多台网络探测器，便于安全信息的集中管理，以便实时掌握全网的安全状况。如下图 2 所示：

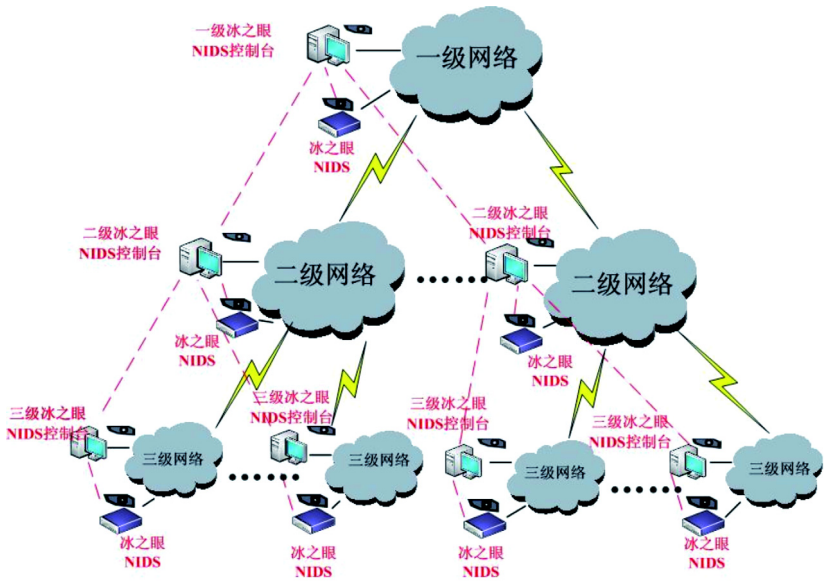


图表 2　集中管理方案

大型网络之分级管理方案

对于跨广域网的大型企业用户，其网络机构相对复杂，不仅有总部，全国各地还有分支机构，总部及下属各分支机构都建有自己的局域网络。用户租用 ISP 的专线建立自己覆盖全国的企业专网，各分支机构通过企业专网与总部建立业务信息交换。因此其对整个网络的管理比较重视，需要保证总部和各分支机构的安全策略的统一性。

针对大型企业用户，绿盟科技入侵检测解决方案提供分级管理方案，在各级网络上部署“冰之眼”NIDS的分级控制台，上级控制台对下级控制台进行统一管理，上级控制台可以将最新的最新升级补丁、规则模板文件、探测器配置文件等统一发送到下级控制台，保持整个系统的安全策略的完整统一性。如下图 3 所示：


一级冰之眼
NIDS控制台
一级网络
冰之眼
NIDS
二级冰之眼
NIDS控制台
二级网络
二级冰之眼
NIDS控制台
二级网络
冰之眼
NIDS
冰之眼
NIDS
三级冰之眼
NIDS控制台
三级网络
三级冰之眼
NIDS控制台
三级网络
三级冰之眼
NIDS控制台
三级网络
三级冰之眼
NIDS控制台
三级网络
冰之眼
NIDS
冰之眼
NIDS
冰之眼
NIDS
冰之眼
NIDS

图表 3 分级管理方案

绿盟科技“冰之眼”网络入侵防护解决方案

绿盟科技 陶智

作为国内的企业级网络安全解决方案提供商，绿盟科技可以为客户提供多链路防护、交换防护、路由防护、混合防护一整套入侵保护解决方案。

新近推出的“冰之眼”网络入侵保护系统（NIPS）V5.5改进版，通过高度融合的IPS/IDS/防火墙集成平台，能为用户提供从网络层、应用层到内容层的深度安全防护，圆满解决了防火墙静态防御和IPS动态防御的融合难题，实现了从企业网络核心至边缘及分支机构的全面保护，从而适用于不同环境、不同企业的安全需求。

多链路防护解决方案

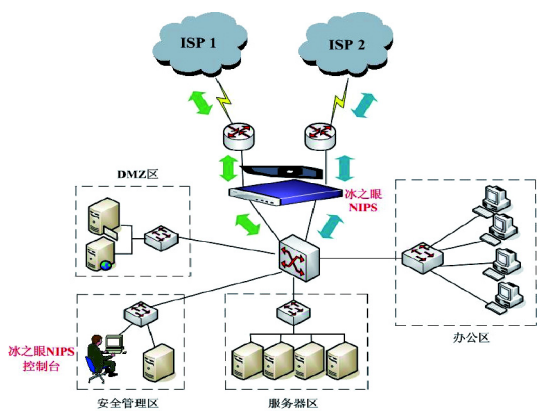
目前，很多企业为了保证网络带宽资源的充足和网络冗余，网络出口采用多链路连接方式，连接到两个或更多ISP服务商。

针对这种连接方式，绿盟科技入侵保护系统提供多链路防护的解决方案，在网络出口处部署一台“冰之眼”网络入侵保护系统，采用多路IPS的部署方式：

1、“冰之眼”NIPS支持多路IPS部署，一路IPS防护一个ISP接入链路，一台冰之眼NIPS可以同时防护多条链路，节约用户投资；

2、“冰之眼”NIPS的各路IPS是相互独立的，彼此之间没有数据交换，互不干扰，保证了各链路流量的自身安全；

3、“冰之眼”NIPS实时监测各种流量，提供从网络层、应用层到内容层的深度安全防护。



图表 1 多链路防护解决方案

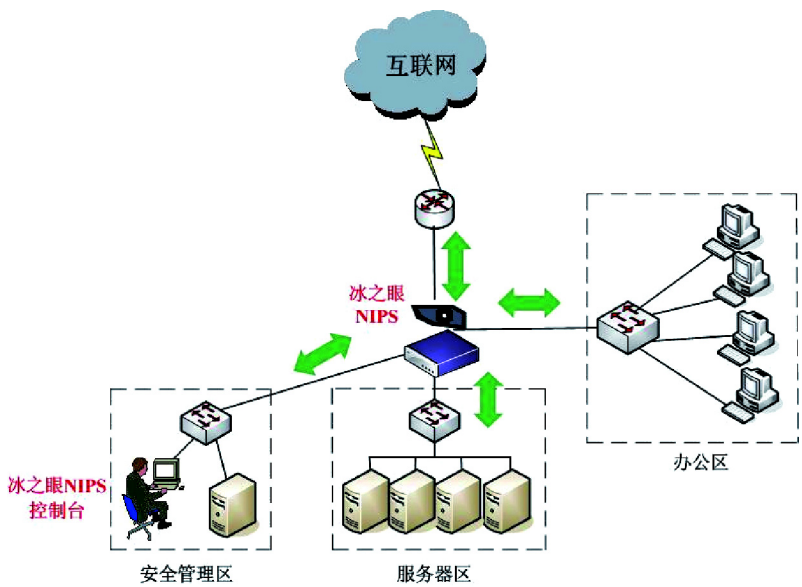
交换防护解决方案

企业内部网络根据工作地点和工作特性，划分为不同的网段。网段之间通过交换机连接，进行数据交换。如何有效检测不同网段之间内部数据交换的安全性，是很多网管员关心的问题。

针对以上需求，绿盟科技入侵保护系统提供交换防护的解决方案：

1、“冰之眼”NIPS 类似二层交换机一样，采用一进多出或多进多出的方式，同时与不同网段相连接，进行数据交换；

2、“冰之眼”NIPS 实时监测各网段之间的各种流量，提供从网络层、应用层到内容层的深度安全防护。



图表 2　交换防护解决方案

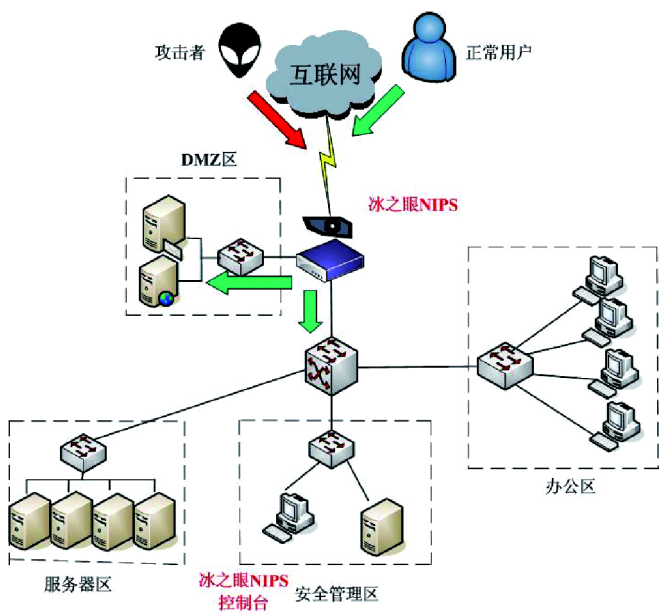
路由防护解决方案

目前，很多企业网络连接到互联网，一般在网络边界部署路由器、防火墙以及入侵保护／检测系统，串联的设备比较多，造成网络边界单点故障率提高，影响整个网络安全性。

针对以上网络特点，绿盟科技入侵保护系统提供路由防护的解决方案：

1、“冰之眼”NIPS 部署在网络边界，类似于一个路由器，提供静态路由和策略路由，又是一台防火墙，实现 NAT 地址转换和流量管理，提供网络层安全防护，还是一台入侵保护系统，实现应用层和内容层的安全防御；

2、“冰之眼”NIPS 深度融合的 IPS/IDS／防火墙集成平台，圆满地解决了防火墙静态防御和 IPS 动态防御的融合难题，为用户提供更全面的入侵保护解决方案。



图表 3　路由防护解决方案

混合防护解决方案

大型企业的网络规模很大，结构相对复杂，不仅有总部，还有各地的分支机构，既要保护网络边界的安全，同时又要保护企业内网的安全。

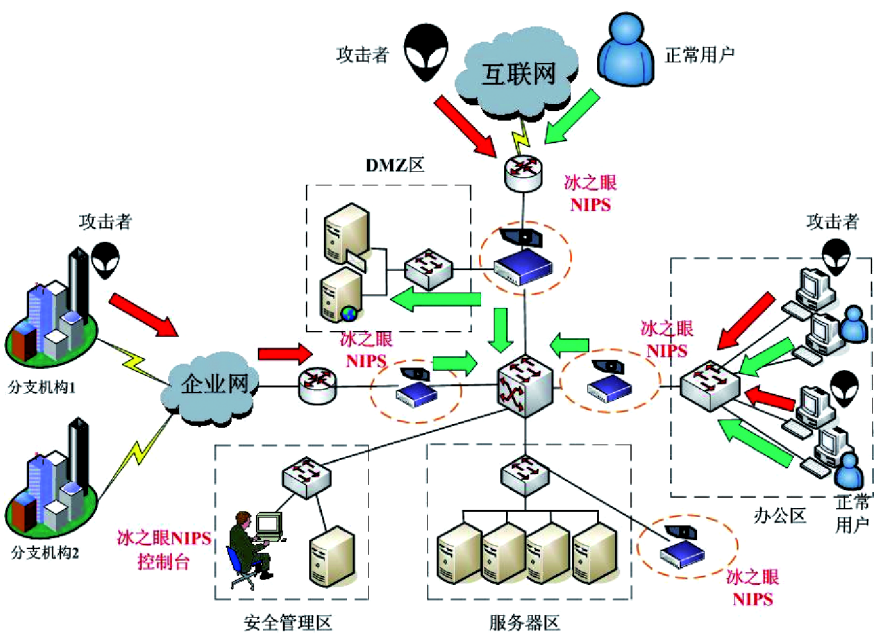
针对大型企业网络特点，绿盟科技入侵保护系统提供混合防护的解决方案：

1、在总部互联网出入口处在线部署“冰之眼”NIPS，实现路由防护，提供互联网的从网络层、应用层到内容层的深度安全防护；

2、在总部内部网段之间以及与分支机构网络之间在线部署“冰之眼”NIPS，提供透明接入的、独立多路 IPS 一进一出的、交换式 IPS 多进多出的全方位、立体式的安全防护体系，实现内网的安全区域划分和控制；

3、在企业服务器区旁路部署“冰之眼”NIPS，相当于入侵检测系统，监测、分析服务器区的安全状况，保护服务器安全；

4、通过一个“冰之眼”控制台，实现对全网 IPS 设备的集中管理、安全信息的集中分析和处理，有效解决企业面临的安全问题，提高投资回报率。



图表 4　混合防护解决方案

结论

随着安全漏洞不断被发现，黑客的技巧和破坏能力不断提高，网络受到越来越多的攻击。每天成千上万的蠕虫、病毒、木马、垃圾邮件在网络上传播，阻塞甚至中断网络；BT、电驴等P2P下载软件轻易的占据100%的企业网络上行下行带宽；员工沉浸在QQ、MSN等聊天或反恐精英、传奇等网游中不能自拔，从而影响了正常的工作。这些新型的混合威胁越来越给企业造成巨大的损失，而对于上述威胁，传统防火墙、入侵检测系统和防病毒系统都无法有效地阻止。

为了弥补目前安全设备（防火墙、入侵检测等）对攻击防护能力的不足，我们需要一种新的工具用于保护业务系统不受黑客攻击的影响。这种工具不仅仅能够精确识别各种黑客攻击，而且必须在不影响正常业务流量的前提下对攻击流量进行实时阻断。

绿盟科技的“冰之眼”网络入侵保护系统提供了业界领先的实时、主动的防护能力，通过新一代的入侵保护技术，绿盟科技的产品和技术能够有效的阻断攻击，保证合法流量的正常传输，这对于保障业务系统的运行连续性和完整性有着极为重要的意义。

研 究 篇

来自空中的威胁

绿盟科技 于旸

一、引言

凡是历史上传统网络设备出现过的问题，几乎都已经在无线设备上重演了。即使是Cisco、3Com、Motorola、Siemens 等大公司的产品，也已经发现了很多安全问题。随着信息技术的发展，以电磁波为载体的无线信息技术越来越普及。随之而来的，也有很多相关的安全问题和隐患。目前我们常用的无线安全技术大致涉及：无线数字语音及数据通信技术，如无线网络、移动电话等；无线个体识别技术，如电子标签；无线输入输出设备，如无线键盘、鼠标等。考虑到大多数人对电子标签技术比较陌生，所以用了一定的篇幅介绍相关的基础知识。

二、无线数字语音及数据通信

蜂窝通信网络的安全问题

日常生活中，我们最常接触的无线技术就是蜂窝通信网络，也就是常说的移动电话使用的技术。目前已经投入实际使用或实验性应用的蜂窝通信技术包括：2G 技术，包括GSM、CDMA 等；2.5G 技术，包括GPRS、GPRS/EDGE 等；3G 技术，包括EDGE、CDMA 2000、WCDMA 等。

现阶段应用最广的蜂窝通信技术是GSM 和CDMA。GSM 协议本身是加密的（A3、A8、A5），但是经过多年研究，已经有了很多公开或者未公开的破解GSM 网络的技术（参考资源[1]），可对手机进行窃听、定位。不过目前尚未看到明确表示可破解CDMA 网络的公开研究文献。

随着智能手机的普及和“彩信”等业务的开展，手机自身的安全问题也变得越来越突出。“彩信”是一种类似电子邮件的蜂窝通信增值业务，可用通过蜂窝通信网络在手机之间传递任何格式的文件。一旦手机对某些文件格式的解析出现类似缓冲区溢出的漏洞，就可能用于入侵以及编写蠕虫。这种漏洞的出现，现在只是个时间问题。

无线网络的安全问题

1．无线网络的范畴

我们通常说的“无线网络”是特指802.11 协议族所定义的无线局域网，实际上，“无线网络”包括：

⑴ 无线个人网，即WPAN（Wireless Personal Area Network）。

由802.15协议族所定义的，用于少量节点短距离通信的无线网络。目前主要是指蓝牙(BlueTooth)，多用于个人数字设备之间的通信，如手机、PDA、耳机、键盘、鼠标等。另外，由802.16协议族所定义的下一代无线个人网UWB（Ultra—Wide—Band）在2006年也将投入实际应用。UWB被设计为实现千兆带宽的无线连接，已经被纳入下一代蓝牙标准。

⑵ 无线局域网，即常说的Wi—Fi（Wireless Fidelity)。

由802.11协议族所定义的，用于中距离通信的无线网络。可以通过调整部署方案从而容纳数十数百甚至更多的节点。

⑶ 无线城域网，即WMAN（Wireless Metropolitan Area Network)。

由802.16协议族所定义的，用于中远距离通信的无线网络。将来最可能普及的是WiMAX（Worldwide Interoperability for Microwave Access）方案。但也可能由于3G技术的冲击而胎死腹中。

很多人认为WLAN（Wireless Local Area Network）和Wi—Fi是同义词，事实上WLAN的概念还包括BlueTooth、HomeRF和WMAN，Wi—Fi只是它的子集。

目前无线网络中已经普遍应用的是Wi—Fi和蓝牙。这两个协议相关的安全问题也最突出。

2．Wi—Fi的安全问题

Wi—Fi使用的无线传输协议包括802.11b、802.11a和802.11g。其中802.11b和802.11g使用2.4GHz频段，802.11a使用5.8GHz频段。普通Wi—Fi网络大约可以覆盖数十米，而使用专门的设备，可以访问数公里甚至更远处的Wi—Fi网络。

802.11b网络是现在部署最多的。而新建设的Wi—Fi网络则多使用802.11g。由于不能兼容802.11b设备，所以纯802.11a网络很少见。

无论使用何种传输协议，Wi—Fi在安全上面临的威胁都是一样的：

⑴ WEP破解、Sniff、非法接入

目前国内部署的Wi—Fi网络大多数没有使用加密，或者使用早已被证明不安全的WEP加密方式，只有很少一部分使用了WPA。以现在的计算机运算能力，穷举攻击64位加密的WEP只需数分钟，而利用密钥弱点攻击128位加密的WEP最短也只需几十分钟。如果没有使用加密或者WEP被破解，入侵者就可以通过无线Sniff得到网络中的通信数据，或者直接接入网络，进行进一步的入侵。

如果没有可靠的加密措施，那么即使使用了基于MAC地址的身份鉴别甚至802.11x认证，也可以利用MAC欺骗或者中间人攻击来绕过。

⑵ 假冒接入点(Fake AP)

就是利用WEP客户端会自动连接信号最强的AP的特点，或者将自己伪装成合法接入点，诱使用户接入，然后窃取通信数据。目前已经有报道，国际信用卡犯罪集团开始用假冒接入点的方式进行钓鱼攻击，获取用户的信用卡账号密码。

⑶ 无线接入设备自身的安全问题

缓冲区溢出、默认管理口令、SNMP默认共同体字符串、认证绕过、非授权访问、拒绝服务、信息泄露

凡是历史上传统网络设备出现过的问题，几乎都已经在无线设备上重演了。由于无线接入设备的生产门槛低，所

以有大量中小规模的厂商都在生产。小厂商很难在安全上投入太多资源，所以必然会有大量安全问题出现。事实上，即使是Cisco、3Com、Motorola、Siemens 等大公司的产品，也已经发现了很多安全问题（参考资源[2]）。

绿盟科技安全研究小组在2002年底就曾发现某品牌的无线接入点可以匿名读写配置信息，甚至可以修改其固件。

⑷ 中间人攻击、拒绝服务

由于无线电波的无孔不入，所以Wi-Fi网络是真正意义上以“广播”方式工作的。进行中间人攻击和拒绝服务，较之传统网络更加容易。对于使用802.11x协议进行认证的网络，就可以使用中间人攻击。

3．蓝牙的安全问题

最早由爱立信提出的蓝牙原本不是IEEE的标准协议，事实上，IEEE的802.11小组对蓝牙很不欢迎。后来IBM、英特尔、诺基亚、东芝、3Com等业界巨头纷纷开始支持蓝牙。到了2003年4月，最终IEEE宣布批准了蓝牙技术，他们的802.15.1兼容BlueTooth 1.1，后来的802.15.1a基本相当于BlueTooth 1.2。

蓝牙和802.11b/g一样，也使用2.4GHz频段。常见的蓝牙设备有效工作距离大约10米，但是使用特别的装置，可以实现和1公里以外的普通蓝牙设备通信。

蓝牙和Wi-Fi协议栈的状况有所不同：Wi-Fi协议栈比较单纯，一般都在内核中实现，而蓝牙协议栈的实现从L2CAP开始还牵涉到应用层。所以，Wi-Fi协议栈本身通常不会带来类似缓冲区溢出这样的安全问题，而蓝牙则有可能。

事实上，几乎所有的蓝牙协议栈实现都已经被发现各种安全问题，其中很多问题可以直接导致系统被控制、数据被窃取。

绝大多数人对蓝牙的安全威胁都一无所知，也没有解决蓝牙安全问题的意识。另外，很多使用蓝牙的设备是手机、PDA等，普通用户根本不知道如何给这些设备升级以解决安全问题。

更糟的是，有些蓝牙协议栈开发商出于自身利益的考虑，甚至不肯为存在漏洞的软件发布补丁。所以使用这些软件的设备厂商即使在新生产的产品中也只得使用存在安全问题的蓝牙协议栈。以至于现在有大量的蓝牙设备处于随时可被攻击的状态。绿盟科技安全研究小组测试了市场上常见的四款PDA，发现全部存在安全漏洞。

蓝牙协议本身虽然是一套比较安全的协议，但也存在被攻击的可能。例如，通过发送强制认证请求，可以劫持蓝牙的配对过程，从而窃听甚至伪造蓝牙通信。一个突出的例子就对使用蓝牙耳机的移动电话进行窃听和语音插入。

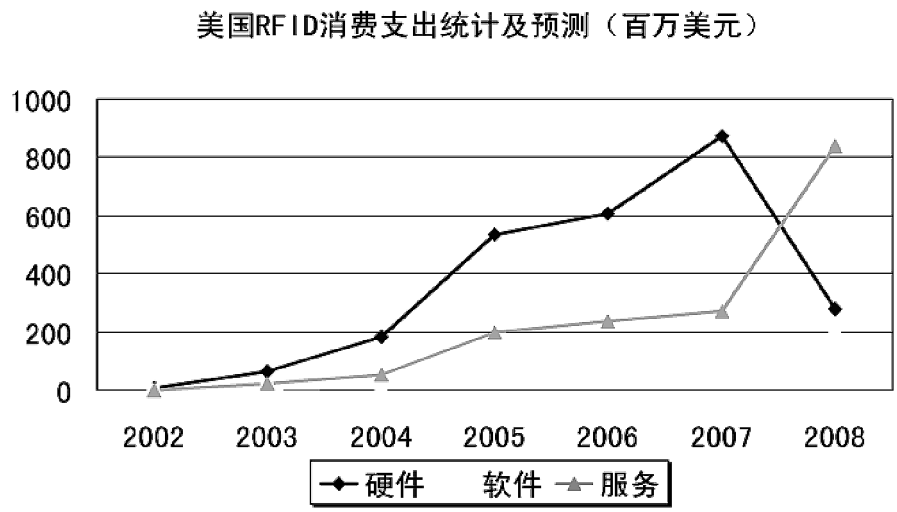
由于蓝牙技术被大量使用在手机、PDA等个人设备上，所以，蓝牙安全问题是个人隐私的一大威胁。随着蓝牙在个人电脑上的普及，它也许会成为继Wi-Fi之后，又一个通过无线技术绕过防火墙攻击内部网络的途径。

三、无线个体识别技术

电子标签介绍

电子标签的核心是用无线技术实现身份确认，即“无需接触，即可读取”。最初，它只是以条形码的替代者

面目出现，后来人们发现它成本低廉、效费比高、扩展性强，所以现在已经在越来越多的地方使用。已经投入大量应用的领域包括：门禁管制、文档管理、安全管理、畜牧管理、交通运输、医疗管理、生产链、物流链、供应链……等等。



目前针对电子标签技术，共有 117 个不同的协议。各个国家和地区使用不同的标准和不同的频段。

电子标签的分类

根据是否可写，可以将 RFID 分为：

1.可读写卡。相当于可擦写光盘，应用灵活但成本较高。我国的第二代身份证使用的就是这种卡。

2.一次写入卡。相当一次性刻录光盘，写入一次后即不可更改。

3.只读卡。相当于普通光盘，制成之后不可重写。一般门禁系统使用的就是这种卡。这种卡的成本最低廉，应用最广泛。

根据是否自带电源又可以将电子标签分为：

1.无源电子标签

无源电子标签依靠和阅读器之间的电磁耦合获取电能。工作距离取决于阅读器耦合线圈的尺寸和工作频率。一般小功率阅读器的读取距离在几厘米到几十厘米之间，大功率阅读器配合大型线圈，可以读取数米外的电子标签。由于成本低廉和体积小的优势，所以绝大多数的电子标签都是无源的。

2.有源电子标签

有源电子标签自带电源供能。发射功率较大，读取距离可达 10m~30m 或者更远。电源通常为锂电池，可工作 3~10 年，或者使用外接电源。由于体积大，成本高，所以目前主要用于车辆识别等需要远距离工作并方便得到电能的场合。

一些新款的手机内置了“电子钱包”功能，这其实就是有源电子标签的一个应用。结合相应的读取器，“电子钱包”可以方便地实现无人化支付。日本的一些地铁站已经开始尝试使用这种技术售票。

电子标签的安全问题

电子标签技术在方便我们生活的同时，也带来了一些相关的安全隐患：

1.仿冒

电子标签在读取的时候，电磁辐射可以被一定距离内的设备捕获。利用这些数据，就可能复制出一个完全相同的电子标签。譬如，某些高级轿车使用电子标签作为钥匙，这种“钥匙”被复制之后就可以轻而易举地将车开走。

我国一般的门禁系统使用125KHz的载波频率，还不是很容易被远距离接收，但是对于工作于高频段的电子标签，就是一个比较严重的问题。

2.泄露个人隐私

电子标签“无需接触，即可读取”的特点，很容易导致个人隐私问题。

通常在零售商品上使用的都是轻薄如纸的无源电子标签。用户购买的时候,很难了解其中是否包含电子标签。譬如说，一位女士在超市购买了包含电子标签的唇膏，付费的时候电子标签的信息会被收银机读取并记录到数据库。商家可以在门口设置一个读取器，如果这位女士随身携带着唇膏，再来这家超市的时候，就可以被识别出来。商家可以用这种方法了解客户的购买习惯，甚至可以通过在不同位置安放读取器，来了解客户在某些货架前停留了多长时间。

目前微型电子标签已经可以做到一粒米的五十分之一大小，这样的电子标签完全可以植入人体。前不久，美国国会就通过了一项法律，允许出于医疗的用途，在人体内植入电子标签。

“植入”距离我们还比较遥远，但是随着电子标签在身份证、护照等证件领域的应用，已经意味着任何人都可能在擦身而过的时候知道你叫什么名字，多大年龄，住在哪里　　甚至更多。

四、无线输入输出设备

无线键盘和无线鼠标的安全问题

目前的无线键盘和鼠标使用的无线技术有三种：

1.红外

由于普通红外通信装置只在1米左右内有效，而且收发装置间必须无遮挡，所以一般不会相互发生干扰。因而在设计这类产品的时候，几乎没有考虑互斥性和安全性。但事实上，通过使用多个红外发光二极管并联增大发射强度和透镜组等光学设备，可以在几十米甚至更远处发射出足够强度的红外信号来控制鼠标和键盘。我们在试验中，仅使用了一个直径10厘米的单片透镜就将两个普通红外设备间的通信距离扩大了至少五倍。

2.蓝牙

因为要在鼠标键盘和计算机上都安装蓝牙芯片，所以这是成本最高的一种无线鼠标键盘方案，但是安全性也最好。攻击难度等同于攻击其它蓝牙应用。

3.无线技术（不包括蓝牙）

这种无线鼠标键盘使用27MHz的无线电波进行通信，没有加密或者认证的措施。为了防止临近的同类设备间干扰，使用256个ID和2个频道来互相分辨。由于只有256 × 2 = 512种组合，所以很容易就可以遍历找出使用的ID和频道。事实上，通过分析接收到的电磁波，可以直接得到这些数据。

由于键盘和鼠标在工作的时候只需要发送数据而无需接收数据，所以虽然无线键盘和鼠标自身使用了相对较弱的功率，要在较远距离实现监听可能有难度，但要实现远距离控制则较容易。制作这种装置最简单的办法就是用一个大功率的无线发射电路，或者红外发射电路，替换掉普通无线键盘鼠标自带的部分。另外，无论是红外还是无线键盘鼠标，在不工作的时候都不会发射信号。这也给远程操纵带来了便利，因为无需用比目标设备更大的功率去压制正常信号，只需满足接受端的灵敏度即可。

参考文献

[1]Lauri Pesonen:GSM Interception，1999.

http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html

[2]绿盟科技漏洞库中的无线相关条目

http://www.nsfocus.net/index.php?os=&type_id=&keyword=%CE%DE%CF%DF&act=sec_bug

[3]Christian Barnes：Hack Proofing Your Wireless Network

http://www.amazon.com/gp/reader/1928994598/ref=sib_dp_pt/002-6338904-5126438

浅谈 Web 2.0安全性

绿盟科技 王红阳

Web 2.0的概念始于O eilly与 MediaLive International的一次会议，自此之后，尽管针对Web 2.0的准确定义还存在着许多争论，但无疑Web 2.0已经逐步生根了。无论是从技术角度还是人文角度出发，Web 2.0都被赋予了大量的应用，blog、TAG、SNS、RSS、wiki等均占据着显赫的位置。

Web 2.0拥有众多令人激动的崭新应用，新技术的采用所可能产生的新的安全问题逐渐成为了人们关注的焦点。一如Web 1.0应用的安全问题，在Web 2.0出现具体的、可验证利用的安全漏洞和威胁之前，在设计、发布Web 2.0应用时重点需要注意的安全问题也就自然成为了我们讨论的议题。

一、技术体系的演变

Web的发展基本同步了网络客户端的发展，客户端由早期近乎于哑终端的形态发展到今天所具有的强大处理能力，功能和性能的飞跃势必带动需求的不断提高，Web发展的每一步都有着客户端需求的印记。

早期的静态HTML页面只能显示一些简单的内容，也反映了当时客户端处理能力和需求的有限，这一时期的安全问题也并不引人瞩目，直到CGI脚本技术的出现和应用，Web安全问题才被作为一个单独的安全命题加以认识和讨论，当客户端强大到足以分担计算、实现令人炫目的功能时，Web 2.0安全问题也被逐渐关注。

Web 2.0既是人文概念也是技术概念，作为Web技术的发展和自然演进，Web 2.0并非脱离早期Web技术的更迭版本，也不是单纯的技术升级。应该认识到，很多技术已经存在并发展了很长时间，不应将其作为所谓Web版本区分的标准。因此，作为需求的产物，讨论Web 2.0的安全问题不能人为的割裂和原有技术的关联性，也就是不能孤立地讨论Web 2.0体系下发展出的技术，如仅仅讨论 Ajax 的安全问题。

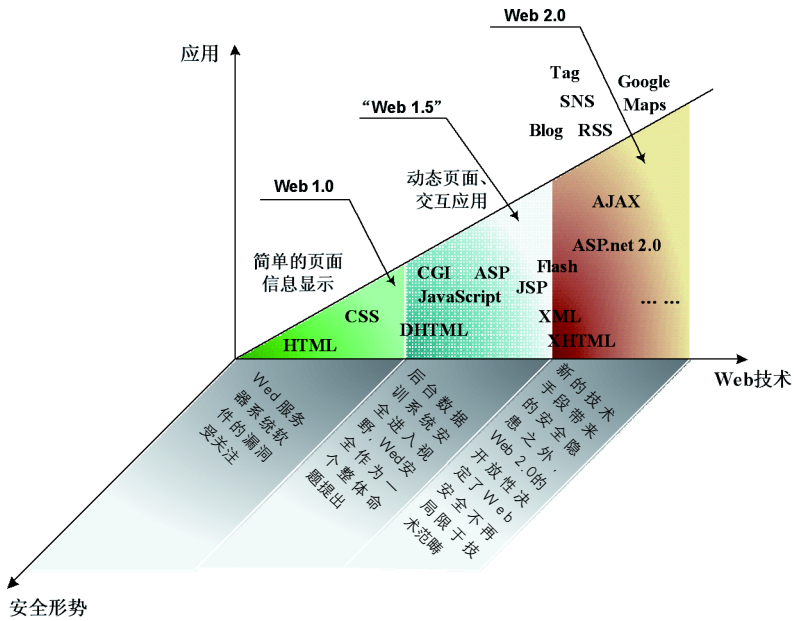


图 1　Web 的自然演进和安全问题

对于 Web 2.0 而言，Client/Server 结构向 Web Services 结构的转变使得讨论其安全性不能像早期的 Web 应用一样一概而论。但是，众所周知，要具体实现一项 Web 应用，无论是否是基于 Web 2.0 的，Web 服务器、实现 Web 服务的软件系统、后台数据库系统，以及具体的数据提交、组织、交互技术实现手段（如 XML、CGI、AJAX）等都是必不可少的。因此，和 Web 1.0 相同，Web 2.0 仍然需要关注服务端系统、数据库系统、实现技术等方面的安全问题，而相关问题的分类仍然是参照 Web 访问结构，即服务端、客户端、信道。

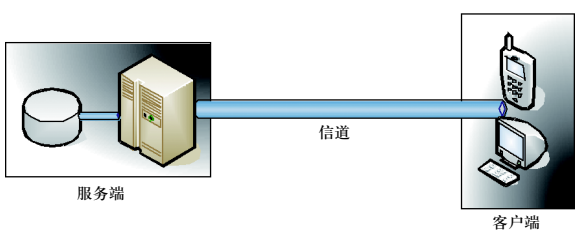


图 2　Web 2.0 安全的结构性划分

对于 Web 2.0 所充斥着的大量技术概念，零散的讨论其安全性是毫无意义的。因此，对于 Web 2.0 中具体的实现技术，如 AJAX（Asynchronous JavaScript And XML），套用 Web 2.0 中的原子内容（Atom Content）的概念，在讨论其安全性时，应该就其实现细节加以也鸥钟，在所获得的以　蛹际跤（Atom Technology）基础上入手加以分析。

二、Web 安全问题

在 Web 1.0 应用中，很多安全问题都是我们耳熟能详的，其主要的安全风险可概括为：

远程代码执行（Remote Code Execution）

权限提升（Privilege Escalation）

信息泄漏（Information Disclosure）

内容修改（Content Manipulation）

拒绝服务（Denial of Service）

无论是 Web 1.0 还是 Web 2.0，依照 Web 访问的结构，可将其分为对 Web 服务器的安全威胁、对 Web 客户端的安全威胁和对通信信道的安全威胁。因此，在讨论 Web 安全时，仅考虑 Web 服务端安全性的思维惯性是片面的。

Web 服务器的安全

在 Web 安全中，服务器的安全是最为人津津乐道的内容。针对 Web 服务器具体的安全威胁主要体现在以下几个方面：

服务器程序编写不当导致的远程代码执行（Buffer Overflow）。

CGI 程序编写不当、过滤不严格造成的代码注入（SQL Injection），可能引起信息泄漏、文件越权下载、验证绕过、远程代码执行等。

乐观相信用户输入、过滤不严格导致跨站脚本攻击（XSS，Cross Site Script），在欺骗管理员的前提下，通过精心设计的脚本获得服务端 Shell。

针对服务器系统的拒绝服务攻击（Denial of Service）。

Web 客户端的安全

Web 2.0 应用的迅速普及，客户端交互力量获得了极为充分的释放和发挥，客户端的安全必然会成为 Web 安全的下一轮焦点 —— 如同 eb 1.5 邮贝 筘ㄊ 据库系统进入 Web 安全视野一样。

Java Applet、ActiveX、Cookie 等技术的大量应用，当用户使用浏览器查看、编辑网络内容时，采用了这些技术的应用程序会自动下载并在客户机上运行，如果这些程序被恶意使用，可以窃取、改变或删除客户机上的信息。对于恶意程序的侵害，用户很难实时的判断程序性质，因此，在获得高度交互的 Web 服务时，如何抵御这些安全威胁绝非简单的客户端设置就可以解决的。

同时，跨站脚本攻击(XSS)对于客户端的安全威胁同样无法忽视，跨站脚本攻击属于被动式的攻击，因为其被动且不好利用，所以许多人常忽略其危害性。与之相对的是，利用 XSS 的 Web 2.0 蠕虫已经在网络中肆虐过。

Web 通信信道的安全

和其他的 Internet 应用一样，Web 信道同样面临着网络嗅探(Sniffer)和以拥塞信道、耗费资源为目的的拒绝服务攻击(Denial of Service)的威胁。

需要注意的是，很多针对 Web 应用的攻击并非只针对服务端、客户端或信道，综合利用各方面的安全漏洞进行攻击的案例数不胜数。

以上列举的安全威胁并非 2.0 版本之前 Web 所独有，正如前文所述，割裂、孤立的考虑 Web 2.0 的安全是有失偏颇的。分析 Web 2.0 的安全首先应考虑 Web 安全，其次考虑融合了新事物的 .0 安全樱 颐窃 eb 2.0 命题中至少应该注意以下潜在的安全威胁：

- SQL 注入
- 跨站脚本攻击(XSS)和脚本注入(Script Injection)
- 缓冲区溢出(Buffer Overflow)
- JavaScript 安全
- 客户端应用程序的安全
- 拒绝服务攻击(Denial of Service)
- 网络嗅探(Sniffer)

三、Web 2.0 实现技术的安全问题

Web 2.0 中，大量以 蛹际跤（如客户端 Script 技术）对于 Web 2.0 来说是作为其必要条件存在的，Web 2.0 诞生的新的技术和方法很难加以笼统的概括。因此，我们仅以 AJAX(Asynchronous JavaScript And XML)为例对特定的 Web 2.0 安全进行讨论。

AJAX 技术的动人之处在于异步(Asynchronous)，在提供流畅、快捷和人性化的 Web 体验的同时，对其安全性的疑问从未停止，而第一款开源 AJAX 扫描器 Sprajax 的发布再一次将 AJAX 安全推到了用户的面前。随着越来越多的使用 AJAX 技术的应用出现，很多组织将必须考虑潜在的安全缺陷以及性能问题。

- 脚本问题

AJAX 的安全威胁来自于日益复杂的服务端脚本和客户端脚本，采用优良的程序设计和编码方法可以有效降低风险。

- XMLHttpRequest 对象的安全问题

JavaScript 的 XmlHttpRequest 对象是 AJAX 的核心，XMLHttpRequest 对象允许客户端机器通过 HTTP 请求获得 XML 文档，如果服务器响应重定向到本地文件的请求，脚本安全检查将会绕过并且文件可访问，这将导致泄露敏感信息给远程攻击者。

另外，根据可验证的 XMLHttpRequest 的本地数据读取能力，以 XMLHttpRequest 与服务器之间的交互能力，存

在着客户端数据泄漏的可能。

- 拒绝服务更容易发生

由于使用了异步机制，攻击性客户端的负担比以往要轻的多，可以发动更多的资源发起拒绝服务攻击，例如发送大量的脏数据，服务器的拒绝服务很容易发生。一种结果就是服务器资源耗尽，或者因为拒绝服务而引起服务器宕机。

在简要描述 AJAX 应用过程中需要注意的一些安全问题的同时，也建议在具体的 AJAX 实现中参照下列要点给予必要的重视：

- 进行 SQL 注入测试
- 进行跨站脚本攻击和脚本注入测试
- 通过编码或借助于其他设备对收到的请求进行源验证
- 通过约束、拒绝和过滤对请求数据进行检查，确保数据的真实性、正确性
- 进行必要的身份验证

不要为了“AJAX”而“AJAX”

谈漏洞修补策略

绿盟科技 董明武

近几年来，令网络管理人员谈虎色变的网络安全问题莫过于蠕虫。蠕虫的爆发不仅导致个人电脑或服务器系统无法正常工作，还会造成网络系统的瘫痪。而系统漏洞作为网络安全的头号大敌，可谓万恶的根本。但要想在第一时间把每个漏洞都被及时修补好，基本是不可能的，即便可能做到，所需要的各种资源也是企业无法承受的。

打补丁不能盲目，不是每个补丁都需要在第一时间修补；不是每个补丁都可以随便打上。因为，漏洞的修补是需要策略的。

明确漏洞真相

漏洞所造成的安全问题具备一定的时效性，也具备很强的规律性。通过分析漏洞的生命周期，我们方可把握漏洞法则，寻找漏洞真相。从信息安全这个层面看，是先有漏洞和对漏洞进行攻击的可能性，才有补丁。漏洞是攻击者攻击的目标，而打补丁正是对漏洞的修补过程。

对于漏洞的定义，英汉双解计算机词典的解释如下：在计算机安全学中，漏洞是存在于一个系统内的弱点或缺陷，系统对一个特定的威胁攻击或危险事件的敏感性，或进行攻击的威胁作用的可能性。操作系统厂商微软对漏洞也给出了明确的定义：漏洞是可以在攻击过程中利用的弱点，可以是软件、硬件、程序缺点、功能设计或者配置不当。

由于漏洞所造成安全问题具备一定的时效性，也就是说，每一个漏洞都存在一个和产品类似的生命周期的概念。只有我们对漏洞生命周期的概念进行研究并且分析出其内在的一些规律，才能真正达到解决漏洞危害的目的。漏洞生命周期：简单而言，漏洞从客观存在到被发现、利用，再到大规模危害和之后的逐渐消失，这期间存在一个时间周期，这个周期称之为是漏洞生命周期。漏洞生命周期对于漏洞的管理有着极其重要的意义，下图是一个大家都较为熟悉的漏洞生命周期示意图。

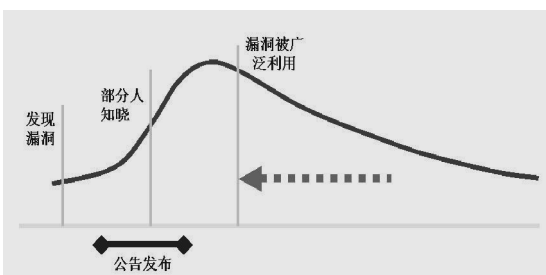


图 1 漏洞生命周期示意图

自2002年以来，国外知名漏洞管理厂商Qualys对大量真实的企业用户漏洞数据进行了长期的跟踪和分析，每年都会公布一些有关漏洞宏观规律的研究成果。该研究目前仍在进行中，本文中引用的数据是2005年的最新结果。

表1 2005年漏洞研究结果

研究目的	现实世界中的严重漏洞随着时间变化的特点
时间	2002年Q3至2005年Q3
数据来源	企业内部的互联网和企业的外部网络；70%来自于全球企业网络，30%来自随机扫描试验。
数据采集方法	自动数据收集，不局限于单独用户或系统。
扫描方式	远程扫描，未安装任何客户端。
扫描次数	32,000,000次漏洞扫描。
真实世界的原始漏洞数据	32,147,000个被扫描IP（2002年Q3至2005年Q3），发现21,347,000个被确认的漏洞。
研究的漏洞范围	1,556个惟一的严重漏洞中的1,060个，这里的严重漏洞指攻击者能够通过这些漏洞获得对系统的完全控制权或者获得系统的重要敏感信息。
漏洞总体趋势	由服务器端向客户端过渡，原来的漏洞主要集中在服务器端（Web服务、Mail服务、操作系统的服务等），现在超过60%的新的高风险漏洞来源于客户端应用程序（Web浏览器、备份软件、媒体播放软件、反病毒软件等）。

基于大量真实数据的研究得到了漏洞存在和发展的一些内在的规律，就是所说的漏洞法则。漏洞法则中每条法则都和漏洞生命周期有着密不可分的关系，漏洞生命周期的概念定性地对漏洞的时效性进行了说明，漏洞法则对漏洞的时效性进行了定量的分析，并且给出了具体的统计数据进行说明。下面我们就介绍几条通用的漏洞法则，并阐述该法则带给我们的启示。

半衰期：在某一范围内，某一漏洞影响到的主机的数量减少为一半的时间。

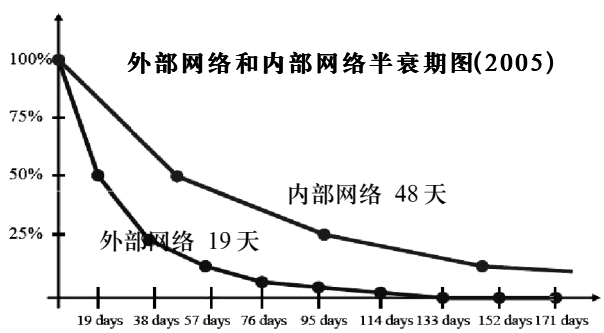


图2 漏洞半衰期

表 2 2003 年至 2005 年半衰期变化结果统计表

	2003 年	2004 年	2005 年	2006 年
External 半衰期	30 天	21 天	19 天	?
Internal 半衰期	N/A	62 天	48 天	?

半衰期法则带来的一些启示：

● 漏洞是从外部网络逐渐渗透到内部网络的，并且在内部网络的存活和危害时间较长，网络管理人员对内部网络的漏洞修补速度还需要进一步提高，这对漏洞的自动修补提出了较高的要求。

● 对于企业级网络，不可能一次把所有资产的所有漏洞立即修补，即使做到了，付出的成本也将相当可观，而收效却甚微。

● 尽量在半衰期内将高危漏洞修补，要对网络中的资产按照重要性列出清单并进行分类处理，把精力集中在与企业业务相关的重要资产，对于不同的资产采用不同防护措施进行处理。

● 2006 年内部网络用户需要将漏洞半衰期降到 48 天以下，才能有效降低内部网络存在的漏洞风险。

流行性：50%的最流行的高危漏洞的影响力会流行一年左右，一年后这些漏洞将被一些新的流行高危漏洞所替代。

流行性法则启示录：

● 漏洞流行期在一年左右，并且新的漏洞不断增加，需要对漏洞进行持续评估与审计，今天安全并不代表明天依然安全，安全是动态的、相对的，因此我们对漏洞的管理也必须是一个动态的过程，整个的过程需要自动化工具的辅助来提高工作效率。

● 一半漏洞在一年之后仍然在网络中存在，说明有些漏洞被检测出来之后并没有被修补或者规避，未修补的漏洞将导致整体安全性的下降。

● 漏洞管理的是一个循环、永无止境的过程，随着漏洞增加的趋势不断调整漏洞评估和审计的频率，尤其是涉及企业业务的重要资产。

持续性：4% 的高危漏洞的寿命很长，其影响会持续很长一段时间；尤其是对于企业的内部网络来说，某些漏洞的影响甚至是无限期的。

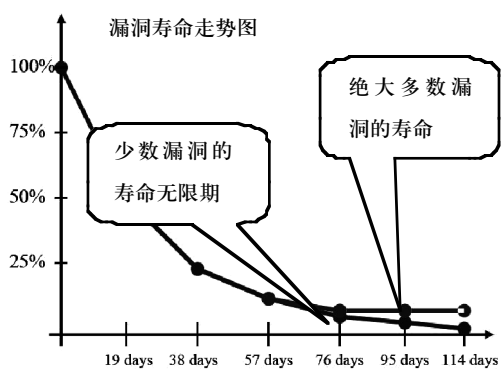


图 3 漏洞寿命走势图

持续性法则启示录：

● 某些漏洞很难被彻底根除，需要重点检测、确认、尽可能消除这些漏洞，有时可能需要通过专业安全服务人员的协助来完成。

● 网络中引入新设备、安装新应用软件等，均可能引入一些旧的漏洞，因此，网络中的任何资产变更，都需要重新进行漏洞评估和审计工作。

● 要特别警惕那些潜伏在应用程序的代码中的漏洞，比如一些内嵌Microsoft database engine（MSDE）的应用程序可能导致SQL Slammer蠕虫在内部网络的再次爆发。

可利用性：80%的利用漏洞的攻击发生在前两个半衰期内，85%的破坏来自于漏洞攻击开始的15天的自动化攻击，并且会不断持续，直到该漏洞的影响消失。

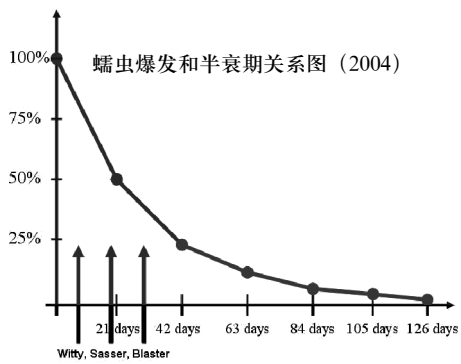


图 4 蠕虫爆发和半衰期关系图

可利用性法则带来的一些启示：

● 用户应该密切关注最新的漏洞动态信息，可以根据企业资产定制相关的专业安全厂商的通告，同时关注临时应急方案和补丁程序的发布。

● 通过制定合理的安全策略来实现来自外部网络对内部网络的攻击，尤其是针对终端设备实行集中化控制和管理。

● 尽可能通过自动化的漏洞评估、漏洞修补来加速漏洞修补过程，漏洞修补之后还要验证漏洞是否已经被清除。

打补丁要讲方法论

要从根本上有效地解决目前利用漏洞进行攻击的问题，就需要我们基于漏洞生命周期、漏洞法则的研究，结合人为管理方式，建立一套有效的漏洞管理工作流程，并通过漏洞管理类的自动化产品辅助执行漏洞管理的过程。自动化工具能够提高整个过程的准确性、缩短漏洞识别和修补的周期。

漏洞管理流程

一个较为完善的漏洞管理过程至少应该包括漏洞预警、漏洞检测、漏洞分析、漏洞修补与安全策略和修补跟踪几个阶段，同时在实际过程中，时刻要将漏洞的风险和资产相关联。

表 3 漏洞管理过程

过 程	解决方案
漏洞预警	专业安全服务厂商通告
漏洞检测	漏洞管理设备或专业安全服务
漏洞分析	漏洞管理设备或专业安全服务
漏洞修补与	补丁管理产品或专业安全服务；安全策略调整
安全策略	多数手工、一些通过终端安全产品完成
漏洞审计	漏洞管理设备或专业安全服务

1）漏洞预警：能够及时获得最新的漏洞通告信息，对于没有补丁程序的漏洞要给出临时的解决方案，要求提供漏洞管理产品的厂商应该有基础的漏洞研究和跟踪能力，能够及时准确的将最新漏洞信息传达给网管人员。该过程可以通过定制专业的安全服务厂商的安全通告来获得。

2）漏洞检测：检测之前需要对网络中的资产进行发现和跟踪，并且通过简便的方式展示，以便更快、更准确地识别、修补漏洞。必须周期性地对用户的网络中的所有网络资产进行检测，要求漏洞管理工具在保证一定的检测速度的前提下，要有较高的准确性，这里需要注意的是并不是检测到的漏洞越多越好，有些产品的误报率很高，要对漏洞的有效性进行验证和分析，必须支持国际上大多数的漏洞标准（CVE、CERT、BugTraq 等）。基于软件的解决方案大多需要人工进行维护，自动化能力较差。该过程可以通过购买专业的漏洞管理设备或专业的安全服务来完成。

3）漏洞分析：在漏洞检测之后需要通过具体的报告和数据来对资产的风险进行统计分析，清楚地显示漏洞的分布情况、详细描述和解决方案。其中特别需要注意的是要对网络中的资产的风险进行分类，以便对后续的漏洞修补工作进行优先级的划分。该过程可以通过漏洞管理设备或专业安全服务来自动完成。

4）漏洞修补与安全策略：通过统计分析的结果制定切实可行的漏洞修补方案并通知终端用户，可以通过文件服务器来提供最新的漏洞修补程序供终端用户下载和安装。特别需要注意的就是从合法的来源获取补丁程序，并且要对补丁进行测试，来保证安装补丁不会影响业务系统正常运行，还要有补丁回滚能力。该过程可以通过操作系统厂商或者第三方厂商的补丁管理软件或专业安全服务来完成。

安全策略：为整个企业的网络安全设备、服务器、网络设备、应用程序和终端主机制定严格的安全策略，并保证这些策略能够强制配置和下发。其中大多数需要手工进行配置，一些能够通过部署终端安全产品来自动完成。

5）漏洞审计：在每次漏洞修补之后监控终端用户是否及时地安装了漏洞修补程序。该过程能够通过漏洞管

理设备或专业安全服务完成。

网络管理人员在制定漏洞管理工作流程的时候，要根据自己实际需求情况将上述过程进行细化或者裁减，为了使整个流程更有效，需要注意以下几点：

第一，管理层的支持、工作流程的标准化对整个漏洞管理很重要；

第二，尽量使用专业的、自动化的漏洞管理工具，尽量避免人工操作；

第三，尽量不要中断企业的业务流程，保证业务系统正常运行；

第四，尽量保持整个网络环境的配置简单，最好对同样的系统采用类似的配置，并且能够进行集中管理。

要补的不只是漏洞本身

现实生活中人们对补丁这个东西都已经是不太陌生了，大多数情况下，厂商公布了补丁之后也都会及时地将补丁及时安装。对于绝大多数网络管理人员来说，打补丁其实已经是日常工作中的家常便饭了，而且整个打补丁的过程大多数都遵循这样一个非正式的通用模式，这个模式大致包括以下几个过程：

(1) 专业安全研究人员或者组织研究并发现一个漏洞；

(2) 该漏洞被提交给相关厂商，等待确认并为开发补丁争取时间；

(3) 厂商对漏洞进行确认并且发布补丁程序；

(4) 网络管理人员通过安全厂商或者软件厂商通告知晓该漏洞；

(5) 网络管理人员寻找、下载并且安装补丁；

(6) 网络管理人员将该漏洞和补丁尽可能通告相关人员；

(7) 假定该漏洞已经被补丁修补。

从个人用户的角度来说，采取这些措施应该能够有效地降低因漏洞带来的安全风险，打补丁在终端用户的安全防护方面起到了重要的作用。但是对于企业级用户而言，尤其是当他们的网络拥有了一定规模，同时网络中又有关键业务流存在时，这样的过程和方法是否依然能够奏效呢？

事实证明，这种传统的方法在对付企业中漏洞带来的安全风险时，还存在着很多局限性。

打补丁不能解决所有漏洞问题

打补丁不能解决所有的漏洞问题。没有一个规范的过程来对漏洞进行监控，企业就不会清楚网络环境中的漏洞是否被清除或者规避。一些漏洞是由配置不当或者配置错误导致的，这在前面的漏洞的概念中已经明确指出，没有补丁能够清除由配置导致的漏洞。

前面提到的传统补丁方法想要成为企业补丁管理方法还缺乏一定的规范性，更何况补丁管理也只是漏洞管理的一部分而已。普遍的看法是将补丁管理过程看成一种生命周期模型，一个封闭的循环。借用微软的补丁管理模型说明补丁管理过程。在这种模型中，一个循环的完成意味着新的循环的开始，新的循环继承了前一个循环的成果并在这个基础上有所提高。循环的过程分成评估、识别、计划和部署 4 个部分，对每一个新的漏洞以及相应的

补丁都要放在这个循环里面进行考察。

评估阶段——收集漏洞、补丁信息，收集企业资产信息并确定其价值，然后，在这个基础上，评估漏洞对企业的威胁，还要对前一次的执行结果进行评估，给出修补漏洞的要求以及其他防护措施建议。

识别阶段——这个阶段的工作依赖于评估阶段收集的信息作为基础，主要工作有下列内容：寻找补丁，并确定其来源可靠；测试补丁，以确定其能与企业IT环境兼容；计划阶段——给出在企业网络部署补丁的详细计划安排；

部署阶段——根据计划，在企业网络内部署补丁并进行确认。

上面这个划分适合企业从宏观的角度把握补丁管理。但及时部署补丁还是需要依靠自动化的工具来完成才有可能。

有效管理资产

当企业网络中的资产数量较多的时候，传统的方法不可能有效地将网络中所有资产存在的漏洞进行修补。在评估之前要对企业中资产要有明确的清单，企业网络中的资产不同于个人终端，有网络设备、网络安全设备、服务器、数据库等资产，其硬件、软件的复杂度要远远高于个人终端，并且网络设备、服务器等承载企业重要业务的资产的重要性也要远高于个人终端，同样一个漏洞对于不同的资产的威胁程度是不一样的，也就是说不同的资产存在的风险是不一样的。

据权威统计，企业90%的风险来自于10%的重要资产，传统的方法没有对威胁和风险进行等级划分，这也是它和漏洞管理较为不同的一点。传统的方法倾向于从纯技术角度看问题，如果有补丁我们就要打补丁，只是从眼前的角度去看一个问题，没有从长远角度去看这类问题，因此要对企业中的资产信息尽可能全面地进行收集，并且根据资产在企业业务流程中的角色进行合理分类，方便网络管理人员对企业中资产存在的风险有明确的了解，这样才能够有效地指导漏洞修补过程，将企业中的风险降低到一个较低的水平。

补丁本身的有效性

凡事都有两面性，打了补丁之后从一个角度来看是解决了一些问题，但是在打补丁之前，我们要从其他的侧面思考以下几个问题：

- 安装补丁程序需要哪些基本条件？
- 补丁的副作用，是不是会影响其他应用程序或者其他资产的使用，是否会引入新的未知漏洞？
- 补丁会不会影响一些企业正常的业务连续性？是否需要测试？
- 补丁安装失败或者补丁影响其他资产，如何将安装补丁的系统恢复到安装补丁之前的状态？

传统的方法不能够解决上面提到的几个问题。在企业网络中，用户使用的操作系统种类繁多，有微软的Win—

dows 操作系统系列和Linux 各种发行版本和类Unix 系统，这就导致了补丁获取、分发和安装过程比较复杂，而且只能由部分的工作有自动化的工具来完成，很多工作还是需要人工进行决策和实施的，补丁管理过程的成本还是比较高的。

一般情况下，安装补丁不会影响系统的正常使用，安装补丁存在风险，补丁可能引入一些未知的漏洞，安装补丁需要在风险和收益之间得到平衡。厂商发布的补丁都是针对某一特定的软件版本，而且安装补丁之前要了解安装补丁一些必要条件，要认真阅读补丁安装说明文件，尤其是Linux 和类Unix 操作系统，否则安装失败或者影响系统正常使用的可能性非常大。

在安装补丁之前，还要不得不考虑的一个问题就是安装补丁之后会出现什么不良的影响。对于很多应用软件来说，使用一些共享的库文件是很正常的事情，这就导致了不同应用服务之间可能存在一定的依赖关系，补丁程序很可能在安装之后会无形之中影响到其他的应用或者其他的资产，所以安装之前要在模拟的业务环境中进行先导测试成功之后，才能进入正式业务环境。

最后一点就是补丁的回滚问题，这也是目前所有的补丁管理程序共同面临的一个难题。补丁的分发和安装的自动化已经比较成熟，但是补丁的自动回滚实现方面还有一定的难度。对于一些配置特殊的系统来说，补丁程序可能安装不正确，补丁的安装可能修改了原有的一些配置文件，或更新了一些共享的库文件等导致了系统不稳定或者不能正常运行。传统的方法没有这些风险控制手段。

勿忘补丁变更记录

一些危害非常大的漏洞使大多数网络管理员处于“救火”的状态，因此很少有时间来进行补丁变更记录管理。比如，在爆发“冲击波”“震荡波”时候，大多数管理员首要的工作就是保护网络的基础设施，切断内部网络和外部网络的连接，将企业的重要服务器和企业的内、外网络隔离，将受影响的系统补丁并进行一些配置修改之后重新上线。但是，这种情况还是比较个别的案例。

缺乏变更也是传统方法的不足，变更文档的缺少经常导致大量重复的工作。传统方法缺少过程管理，不能对形成相对固定的工作流程，很难对整个过程进行监控、改进和重用，很多网络管理员大多将文档的中心主要放在漏洞的技术细节上，而很少关注网络中资产的系统配置情况。一个相对完整的漏洞工作流程（过程管理）应该包括以下几个元素：

- 漏洞确认、补丁和配置变更的工作步骤
- 确认补丁和配置变更是否合理的工作步骤
- 资产优先级划分的规则
- 补丁测试的工作步骤
- 补丁部署、配置变更和保护策略工作指南

参考资料：

http://www.qualys.com/research/rnd/vulnlaws/ The Laws of Vulnerabilities Presentation

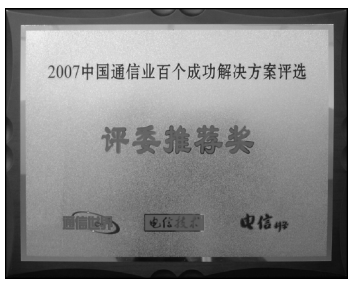
http://www.qualys.com/research/rnd/vulnlaws/ The Laws of Vulnerabilities White Paper

http://www.microsoft.com/china/technet/content/library/security.mspx 指南修补程序管理过程

动 态 篇

技术动态

绿盟科技“安全岛”方案受到中国通信业专家重视



2007年10月25日，由《通信世界》、《电信技术》、《电信科学》共同主办的“2007年（第五届）中国通信业百个成功解决方案评选颁奖”在京举行。

与前几届相比，本届百个成功解决方案评选活动的组织策划更加严密、公正，评委更加专业、权威，参选方案更加突出实用性与效益的紧密结合。作为经验丰富的专业安全解决方案提供商，绿盟科技电信运营商“安全岛”解决方案成功入选并获得“评委推荐奖”。

随着通信业的发展，目前传统电信技术无法适应电信运营商的转型步伐。传统的电信运营市场重视网络，主要原因在于电信网是电信建设的核心，而新的电信运营市场将更加重视应用，所以电信运营商在完成电信网络建设的基础上，需要搭建新的业务平台、完善新的业务理念、形成新的产业价值链。

绿盟科技以此为战略契机，率先提出了电信运营商“安全岛”方案。该方案一方面减缓了DDoS攻击对基础电信网络运行的影响，另一方面又协助电信运营商为其众多终端客户提供安全增值服务，尤其是可以在保障业务顺畅运行的同时，达到电信运营商与终端用户的双赢局面。

绿盟科技协助思科查出严重安全漏洞

绿盟科技研究部门在安全测试中发现思科 Security Agent for Windows存在远程缓冲区溢出漏洞。利用这个漏洞，攻击者可以通过发送恶意的请求而远程执行任意代码。

鉴于此漏洞的严重性，绿盟科技在第一时间已经将此信息通知思科。日前，思科公司在最新发布的安全公告中业已经提醒用户，由于该安全代理存在漏洞，可导致安装该软件的Windows系统被入侵，建议用户尽快升级到最新版本的思科安全代理，以避免安全风险。思科对绿盟科技在技术上的援助致以谢意。

思科安全代理作为一款安全保护产品，在企业中应用相当广泛，而漏洞本身的危险性又非常大，入侵者向安装该软件的Windows系统发送特殊构造的恶意网络数据，可导致系统蓝屏崩溃，甚至完全控制系统，思科因此将该漏洞的安全风险评分定义为最高的10分。

绿盟科技在安全基础研究方面投入了大量的精力，从成立之初到现在，在漏洞安全问题研究方面，绿盟科技已经自主发现了30多个得到国际厂商和第三方权威机构认可的安全漏洞，位居国内安全漏洞研究发现数量之首。在漏洞研究方面的成果经过转化，已经成为绿盟科技自主研发网络安全产品的得力武器，这使得绿盟科技的安全产品具有了有别于同类产品的全面漏洞扫描能力，特别是在中国的特殊环境下，更具有适用性。绿盟科技依靠长期研究积累的成果与安全产品开发能力，为政府、电信、金融、能源等行业客户提供高端安全产品与全面的网络安全解决方案，协助客户建立起安全可靠的绿色网络环境。

产品动态

绿盟科技自主研发的高性能流量清洗系统正式上市

2007 年 11 月 15 日，专为运营商行业定制的高端流量清洗系统——黑洞 Defender 4000 正式上市 。绿盟推出高性能的黑洞 Defender 4000 产品，旨在提供高性能、组网更为灵活的 Anti-DDoS 解决方案。

该系统传承了绿盟科技自主研发的血脉，汇集了绿盟科技最新的研究成果。黑洞 Defender 4000 系统具备如下优势：作为异常流量清洗设备，与监测中心、监控管理中心共同构建异常流量净化系统，充分满足电信运营商对大型 Anti-DDoS 系统“可管理、可运营”的需求；黑洞 Defender 4000 系统采用了多个并行的专业高性能网络处理器，实现了单机 4G 线速分析和处理 DDoS 攻击的能力，通过集群部署，可以轻松应对 10G+ 海量型拒绝服务攻击。该系统具备高密度 GE 接口（8 光 4 电），满足网络发展和客户的需求，持续保护用户设备投资。同时组网更为灵活，具备大型、复杂网络的优良适应性；按性能区分提供了两款产品（2G/4G），可以帮助客户优化建设成本。

随着黑洞 Defender 4000 的上市，绿盟科技将持续致力于保护用户投资、降低用户设备维护费用，并通过产品的差异性能，极大增强黑洞产品在运营商市场的角逐能力，进一步拉开与同类产品竞争的距离。

绿盟科技受到国家网络与信息安全信息通报中心表彰

1 月 2 日，绿盟科技荣获由国家网络与信息安全信息通报中心授予的“2007 年度信息通报技术支持工作先进单位”荣誉称号。一并获得该项荣誉的还有：国家计算机病毒应急处理中心、国家计算机网络入侵防范中心、中国教育和科研计算机网络中心等 8 家单位。

国家网络与信息安全信息通报中心是遵照胡锦涛总书记指示，于 2003 年 10 月筹建的。该中心的工作重点是做好重要敏感期、重大政治活动和重大网络安全事件的信息通报工作。为进一步拓展信息来源，借助社会技术力量提高分析研判水平，国家网络与信息安全信息通报中心建立了由有关企业、应急响应机构和研究机构组成的技术力量支持体系。本着自愿和择优相结合的原则，国家网络与信息安全信息通报中心选择了国内具有较高技术实力的多家企业、院校和研究机构作为支持单位，组建了信息通报技术支持体系。

几年来，绿盟科技高度重视、认真落实信息通报技术支持工作，向通报中心及时提供了大量国内外网络与信息安全信息，圆满地完成了“两会”、“十七大”以及日常信息通报技术支持任务，为有关领导和部门及时了解国内外网络安全形势、网络技术动态，研判网络信息安全状况，制定相关决策和防范措施提供了重要依据，出色的工作成绩受到了通报中心的肯定。

绿盟科技顺利通过二级服务资质复审

11 月 6 日，国家信息安全产品测评认证中心服务资质审核小组到绿盟科技进行现场二级服务资质复评审核，主要就服务队伍的建设和经验积累、三年来完成的项目情况、工程技术能力（解决方案、安全管理、质量保证）几个方面进行审核。 经过严格复审，审查小组对绿盟科技的安全服务水平及项目管理能力给予了较高的评价，认为绿盟科技在队伍保持、服务能力、服务创新等方面均能满足或超过国家标准的要求，无不合格项，一致同意通过复审，并颁发了新的二级服务资质证书。

信息安全服务二级资质是国内目前最高级别的专业安全服务能力认定，绿盟科技这次顺利通过复审，说明绿盟科技在专业安全服务工作上具备了领先的安全服务理念、全面的工程技术能力和经验丰富的专业服务队伍，能够承担起“巨人背后的专家”的使命，有实力保障客户业务的顺畅运行。

绿盟科技率先推出国内首款 IPS 千兆线速精品

继2005年底绿盟科技在国内首家推出入侵防御系统的两年后，绿盟科技宣布再次率先推出“冰之眼”高端千兆安全防御产品与解决方案。

两款“冰之眼”新锐精品分别为 2000P（入侵防御系统）和 2000D（入侵检测系统），其研发宗旨在于进一步满足电信、金融、IDC、ISP、大型企业等用户的高性能安全防护需求。而目前国际上仅有极少数顶尖安全厂商，才有能力研发出此类高端产品。

“冰之眼”入侵防御系统发布之初曾引发了国内入侵防御硬件市场的一场变革，在众多国内IDS主流厂商仍对IPS产品持观望态度的时候，绿盟科技已率先启动了对这一市场的开发研究，而两年的市场应用实践成效尤为显著。两年多来，“冰之眼”入侵防御系统为政府、企业、能源、金融、教育等大量用户提供了全面、深度的安全防护，得到了用户一致的高度认可，并以绝对领先的市场份额和产品技术优势牢牢占据了国内IPS市场第一品牌的地位。

“冰之眼”2000P的推出，主要是对绿盟科技现有入侵防御系统产品线的一次品质再提升，该系统采用高性能多核处理器，配置 8_12 个千兆位网络接口，具备卓越的处理性能。对于 64Byte 数据包，达到 2Gbps 双向全线速转发处理能力，完全适用于下一代高带宽、多链路的网络安全防护环境，可以为用户提供具有高性能、高可靠的主动防御解决方案。

“冰之眼”2000P 和 2000D 正式推出后，绿盟科技已成为国内首家拥有千兆线速入侵防御系统，并且具有完全自主知识产权的安全厂商，这也进一步凸现并巩固了绿盟科技在国内网络入侵检测和防御市场的领导厂商地位。

市场动态

绿盟科技“中国信息安全服务与管理论坛”上受好评

1月10日，由中国信息安全专业委员会主办，国家信息中心信息安全研究与服务中心和深圳市信息安全测评认证中心承办，主题为“探索 、实践 、发展”的“中国信息安全服务与管理论坛”在深圳隆重召开。国信办领导、深圳市政府信息化主要领导、业界专家、政府行业用户代表、金融行业用户代表，以及来自台湾、香港、澳门等地区的专家、学者参加了本次论坛。

论坛以安全管理和技术趋势探讨为主要内容,信息安全专家和典型用户代表介绍了行业安全标准和安全建设经验。绿盟科技、IBM和微软等企业应邀参加了会议。绿盟科技就目前网络安全现状和存在的问题发表了精彩演讲，受到与会安全专家和代表的好评和高度认可。

绿盟科技运营商“安全岛”解决方案专家研讨会顺利召开

2007年11月23日，由绿盟科技主办的运营商“安全岛”解决方案专家研讨会在京顺利召开。各主管机构领导及行业著名专家齐聚一堂，共同探讨应对抗拒绝服务攻击的热点问题，交流宝贵的安全经验。

出席本次会议的专家和领导有：中国工程院何德全院士、孙玉院士、方滨兴院士，南湘浩将军，国信办熊四皓副司长，公安部顾建国副局长，中国信息产业商会信息安全产业分会屈延文副理事长，信产部产品司侯建仁处长，中国信息安全产品测评中心王军总工程师，中国电信大客户部技术总监万军先生等。

会议中，与会的领导及专家们就绿盟科技专门针对运营商应对DDoS攻击的提出的安全岛解决方案进行了点评，对该方案在识别、牵引、过滤、回注DDoS信息流方面的显著效果以及增值价值给与了高度的认可与关注。

专攻术业，成就所托。绿盟科技一直秉承着这个理念，以“巨人背后的专家”为己任，为客户定制网络安全解决方案，提供全面的安全服务和多种先进的安全产品。

绿盟科技两款“黑洞”高端流量分析新品成功上市

经过近一年的紧张研发和测试，日前，绿盟科技成功地推出两款高端流量分析产品—“黑洞”流量分析系统NTA SP2000 和 NTA SE2000。

作为绿盟科技“黑洞”品牌下的一个重要产品线，“黑洞”流量分析系统是一款基于流技术（如 Netflow、sFlow等）的骨干网流量分析产品。主要功能包括异常流量检测和流量的统计分析。它既可以作为流量分析产品单独部署，也可以作为异常流量检测产品与黑洞的 Defender 产品一起构成流量清洗与净化的解决方案进行部署。

与业界同类产品相比，“黑洞”流量分析系统具有四大特点：算法先进、结构灵活、性能强大、即插即用。算法先进性体现在基线的全自动生成和可检测异常流量种类丰富两个方面，异常检测算法的种类超过50种，覆盖几

乎全部攻击型的异常流量。而其系统的软件架构采用结构化设计，可以动态加载检测算法，具有很强的灵活性。黑洞流量分析系统的数据处理能力也非常强大，每秒钟可以处理超过8万条记录。而系统上线也只需要非常简单地配置操作，即插即用。

SP2000 主要适用于运营商环境，包括路由分析功能以及与路由和自治域相关的流量分析；SE2000 主要适用于企业办公网和校园网环境中，主要功能与SP2000 相同。二者在流量数据处理性能、动态流量建模、异常检测精度、检测算法动态加载技术、攻击监控和分析报告、可靠性等方面均做了很多优化，功能特性指标显著。

绿盟科技“黑洞”流量分析系统具有业内非常多的成功应用案例，而高端新品的成功上市，将进一步提升用户对骨干网络流量的监控能力，也使“黑洞”流量清洗解决方案更加完善。

绿盟科技“冰之眼”IPS 连续两年引领国内安全市场

日前，国际权威调查机构IDC 公布了最新的2007 年上半年《中国IT 安全市场分析与预测》报告，根据IDC 报告的统计数据显示，新兴的入侵防御硬件市场增长迅猛，2007 年上半年的市场规模为1140 万美元，较2006 年同期增长159.4%，为整个IT 安全市场中增长速度最快的子市场。

绿盟科技的“冰之眼”网络入侵保护系统（ICEYE NIPS）表现强劲，作为惟一的国内IPS 品牌，再次迈入中国入侵防御市场的领导者行列。继2006 年以来，“冰之眼”网络入侵保护系统已经连续两年获此殊荣。

获得此殊荣，主要源于“冰之眼”网络入侵保护系统很好地解决了用户“网络保护”、“应用防护”和“内容管理”三大方面的难题，可以为企业提供一个动态、深度、主动的入侵保护解决方案。作为国内IPS 第一品牌，“冰之眼”网络入侵保护系统自2005 年率先上市以来，一直引领着国内IPS 技术的发展潮流，其提倡的“下一代防火墙”思想更是IPS 产品未来形态的完美诠释。

相比新兴的入侵防御市场，传统的入侵检测市场依旧保持平稳的增长，但增长速度明显减缓，2007 年上半年的市场规模为3570 万美元，较2006 年同期增长6.3%。在入侵检测市场整体趋于饱和的情况下，“冰之眼”网络入侵检测系统仍表现得十分出色，凭借接近1/5 的市场份额，继续领跑国内入侵检测硬件市场。

绿盟科技运营商“安全岛”解决方案在安全标准化论坛受关注

12 月6 日，由中国通信标准化协会主办，中国通信标准化协会标准化推进中心和中国通信标准化协会网络与信息安全技术工作委员会承办，主题为“推进安全防护体系建设，探索安全保障长效机制”的“第二届电信网络信息安全标准化论坛”在京召开。作为国内网络安全界的领军企业，绿盟科技应组委会的特别邀请出席了论坛，行业技术部总监陈珂代表公司发表了主题为《网络安全：挑战？机遇？》的精彩演讲。

目前，随着信息网络技术的快速发展和智能网、软交换、NGN、IMS、3G 等的逐步演进，多网融合、IP 化、智能化、宽带化、移动化的趋势日益明显。电信网络也逐渐从过去的封闭式业务体系，走向分布式、开放式的灵活

架构；从过去分散式调度控制，走向集中式、自动化的调度控制。但是在开放性、灵活性、智能化程度提高的同时，电信网络安全问题日益凸现，电信网络安全越来越成为人们关注的重点。

论坛上，绿盟科技针对电信网和运营商面临的转型现状，从战略的高度提出运营商“安全岛”解决方案。运营商通过采用“安全岛”解决方案的部署，一方面可以减缓DDoS攻击对基础电信网络运行的影响，另一方面又协助运营商为其众多终端客户提供安全增值服务，尤其是可以在保障业务顺畅运行的同时，达到电信运营商与终端用户的双赢局面，从而引起论坛与会专家和运营商的高度重视。

绿盟科技荣获中国信息安全产业十大品牌企业称号

由《信息安全与通信保密》杂志社主办的第二届中国信息安全产业界“双十评选”活动颁奖会12月18日在北京召开，会上绿盟科技荣获“中国信息安全产业十大品牌企业”称号。

经过多年的发展，绿盟科技已经成为国内规模最大、业绩最好、成果最多、业务范围齐全的信息安全企业之一，目前有员工430多人，在全国各地设立近30个分支机构，可以为客户提供最快捷、方面的支持和服务。

基于多年的持续研究，绿盟科技协助Microsoft、Sun、Cisco等公司解决了30个以上的系统安全漏洞问题，共同保护用户的利益不被安全隐患所侵害。绿盟科技建立并维护的全球最大的中文漏洞库已经成为业界广泛参考的标准。同时，在入侵与反入侵技术、异常流量分析、检测与清洗、操作系统与应用安全、安全漏洞发掘技术、安全产品缺陷与检测、蠕虫及病毒原理与防范等领域，绿盟科技进行了深入的基础性研究。

多年的努力赢得了客户的认可，绿盟科技提供的行业解决方案、专业安全服务和领先的安全产品已经帮助电信运营商、金融、政府、能源和互联网等行业用户构建安全、可靠的应用环境，真正保证客户的网络和业务系统能够稳定、高效地运营，帮助客户提升安全体系建设和运行水平。

面对荣誉，绿盟科技将继续努力发挥在信息安全方面的技术与服务优势，更好地为国内安全客户服务，让“巨人背后的专家”这句口号更加深入客户心中。

绿盟科技精彩亮相“中国网络管理技术大会”

12 月 19 日，一年一度的“中国网络管理技术大会”在京召开，会议旨在对我国的网络应用现状和网络技术发展趋势进行探讨，对企业应用中的网络管理问题进行分析梳理，以帮助政府、企事业单位提升网络应用水平。

绿盟科技应邀出席了本次大会，解决方案中心产品市场经理陈星霖代表公司做了题为《理性评判 IPS “五指论”》的主题演讲，实用的内容博得与会代表的一致好评。

会上宣布了《网管员世界》杂志社一年一度的大型优秀网络产品调查活动评选结果，绿盟科技凭借技术上的雄厚实力，再次获得专家组颁发的多项奖项：

冰之眼网络入侵防御系统：网管员最喜爱的 IPS 产品

极光远程安全评估系统：网管员最喜爱的安全扫描评估系统

黑洞抗拒绝服务攻击系统：网管员最喜爱的抗拒绝服务攻击系统

冰之眼网络入侵检测系统：2008 最值得推荐产品奖

矩阵内网安全管理系统：2008 最值得推荐产品奖

目前，由于网络应用的多样性，结构的复杂性，设备的多种性以及用户要求的方便性、透明性、安全性、可靠性和可管理性的需求变化，致使对 IT 基础设施的要求也日趋明显和具体。如何很好的支撑业务的灵活性，已经成为摆在网络信息安全企业的重要课题。

绿盟科技提供的解决方案可以为电信运营商、金融、政府、能源和互联网等行业构造一个安全、可靠的应用环境，使客户对现有的网络进行有效的管理和监督，充分有效地利用各种 IT 资源。同时保证 IT 基础设施能够建立透明、方便、智能、安全、可靠的使用环境。

绿盟科技远程安全评估系统获得国际权威认证

3 月 10 日，绿盟科技“极光”远程安全评估系统一举获得英国西海岸实验室（West Coast Labs）的权威认证，这是国内也是亚太地区漏洞扫描产品首次通过西海岸实验室的认证 。之前，从 1996 年至今，全球只有 IBM、McAfee 等五家企业通过该项认证。

西海岸实验室 Checkmark 认证系统是一个质量测试和认证服务，具有确定、独立的产品有效性标准。十年多来，西海岸实验室与世界上的主流安全技术开发商和用户群密切合作，是世界上最具权威的安全产品测试和研究实验室之一。

在严格的测试中，绿盟科技安全产品的表现和国际顶尖公司的产品相比毫不逊色。成熟的技术优势、完善的功能应用、稳定的系统给实验室的专家们留下了极为深刻的印象。该认证的通过，标志着中国安全产品的漏洞扫描核心技术已达到世界水平。

在国内的网络安全领域，绿盟科技远程安全评估系统已连续多年占据绝对优势地位。在国内优异表现的基础上，绿盟科技积极准备参加国际安全市场竞争。通过认真准备，通过了全球的权威认证，拿到了国际化的品质保证书和市场通行证，走出了迈向国际市场的第一步。

面对这个伴随着春天来到的喜讯，绿盟科技员工们毫不掩饰自己的自豪，在当今全球经济一体化的时代，有了这个含金量极高的国际认证，具有中国自主知识产权的“极光”产品必将在全球安全市场上赢得一席之地。

绿盟科技亮相美国 RSA 安全峰会

美国时间 4 月 7 日，全球顶尖的信息安全盛会—RSA Conference 2008 在美国旧金山隆重开幕。作为中国网络安全界的领导厂商，绿盟科技携带其业界领先的入侵检测／防护系统、远程安全评估系统、抗拒绝服务系统、内容安全管理系统、安全审计系统、内网安全管理系统等安全产品远赴美国旧金山参加了峰会，并成为本届 RSA 峰会新锐参展厂商之一。

历经 17 年的磨砺，RSA Conference 确立了自己全球领先的电子／数据安全技术峰会的地位，吸引着来自全球各地的政策制定者、行业领袖、IT 专家、程序开发者等人士。峰会上，业界将一起分享各自在不同安全领域的信息安全技术、成功解决方案，相互交换意见，交流沟通学术。

今年 4 月，恰逢绿盟科技 8 周年的庆典，秉承“专攻术业，成就所托”的理念、“巨人背后的专家”的使命和“在全球范围内，提供基于自身核心竞争力的企业级网络安全解决方案”的战略定位，绿盟科技拥有了较快的发展速度。在中国，很少有一家本土企业能像绿盟科技一样以自主创新、自主研发的领先技术立足，并在短短几年的时间完成产品研发、营销架构和服务体系建设，直至走入国际化发展道路。

3 月份，绿盟科技代表产品之一—极光远程安全评估系统获得了国际权威的西海岸认证，证明绿盟科技产品已达国际水平，本次参加RSA 大会，势必增加绿盟科技产品在国际市场的品牌影响力，也标志着绿盟科技产品与解决方案进军国际市场的号角已经吹响。

巨人背后的专家

- 2008年：绿盟科技“极光”远程安全评估系统成为1996年以来全球六家获得英国西海岸实验室权威认证的漏洞扫描产品之一
- 2007年：再次入选国家级应急服务支撑单位
- 2006年：连续四年荣获中计报“值得信赖的安全服务品牌”
- 2005年：囊括年度入侵检测\保护系统全部奖项
- 2004年：入选公共互联网应急处理国家级服务试点单位
  首批荣获国家二级安全服务资质
- 2003年：进入中国电子政务IT百强
- 2002年：承担全国性电信网安全评估
- 2001年：入选国家网络安全服务试点单位
- 2000年：绿盟科技成立

www.nsfocus.com

THE EXPERT
BEHIND GIANTS

长期以来，绿盟科技致力于网络安全技术的研究，为政府、电信、金融、能源等行业提供优质的安全产品与服务。在这些巨人的背后，他们是倍受信赖的专家。

NSFOCUS

SECURITY+

THE EXPERT BEHIND GIANTS 巨人背后的专家

安全+ 技术版

与安全人士分享技术心得

Share technique experience with security professionals

Nsmagazine@nsfocus.com