教育部师资实践基地系列教材——信息与网络安全

DCN | 神州数码 Digital China

信息系统安全项目实践

徐雪鹏　主编

全国职业技能大赛推荐参考书
神州数码网络认证指定教材
校企合作新课改教材

机械工业出版社
CHINA MACHINE PRESS

教育部师资实践 [redacted] 络安全

信息系统安全项目实践

主　编　徐雪鹏
副主编　岳大安　包　楠
参　编　孙雨春　赵　飞　张　鹏　李晓隆

机械工业出版社

本书是神州数码技能教室的配套指导教材，也是信息安全实践基地的指定训练教材。本书以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师人力资源岗位能力模型设置教学内容，建立以实际工作过程为框架的职业教育课程结构。全书共4章，分别为Flow Shape网络流量整形、Web安全、IPS入侵防御系统和网络安全数字取证。

本书可作为各类职业院校信息安全专业的教材，也可作为信息安全从业人员的参考用书。

本书配有授课用的电子课件，可到机械工业出版社教育服务网（www.cmpedu.com）免费注册下载或联系编辑（010-88379194）咨询。

图书在版编目（CIP）数据

信息系统安全项目实践/徐雪鹏主编. —北京：机械工业出版社，2017.4
教育部师资实践基地系列教材. 信息与网络安全
ISBN 978-7-111-56626-7

Ⅰ. ①信… Ⅱ. ①徐… Ⅲ. ①信息系统—系统安全性—教材 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字（2017）第082409号

机械工业出版社（北京市百万庄大街22号　邮政编码100037）
策划编辑：梁　伟　　责任编辑：李绍坤　陈瑞文
责任校对：马立婷　　封面设计：鞠　杨
责任印制：李　飞
北京机工印刷厂印刷（三河市南杨庄国丰装订厂装订）
2017年5月第1版第1次印刷
184mm×260mm · 7.25印张 · 162千字
0001—2000册
标准书号：ISBN 978-7-111-56626-7
定价：22.00元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务	网络服务
服务咨询热线：（010）88379833	机 工 官 网：www.cmpbook.com
读者购书热线：（010）88379649	机 工 官 博：weibo.com/cmp1952
	教育服务网：www.cmpedu.com
封面无防伪标均为盗版	金　书　网：www.golden-book.com

前　言

当前，信息技术产业欣欣向荣，处于空前繁荣的阶段，但是另一方面，危害信息安全的事件不断发生，信息安全的形势非常严峻。敌对势力的破坏、黑客入侵、利用计算机实施犯罪、恶意软件侵扰、隐私泄露等，是我国信息网络空间面临的主要威胁和挑战。我国已经成为世界信息产业大国，但是还不是信息产业强国，在信息产业的基础性产品研制和生产方面还比较薄弱，例如，计算机操作系统等基础软件和CPU等关键性集成电路，现在还部分依赖国外的产品，这就使得我国的信息安全基础不够牢固。

随着计算机和网络在军事、政治、金融、工业、商业等领域的广泛应用，人们对计算机和网络的依赖越来越大，如果计算机和网络系统的安全受到破坏，则不仅会带来巨大的经济损失，还可能引起社会的混乱。因此，确保以计算机和网络为主要基础设施的信息系统的安全已成为世人关注的社会问题和信息科学技术领域的研究热点。当前，我国正处在全面建成小康社会的决定性阶段，实现社会信息化并确保信息安全是全面建成小康社会的必要条件之一。而要实现我国社会信息化并确保信息安全的关键是人才，这就需要培养造就规模宏大、素质优良的信息化和信息安全人才队伍。

2014年，习近平主席在中央网络安全与信息化领导小组会议上指出：没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题，要从国际国内大势出发，总体布局，统筹各方，创新发展，努力把我国建成网络强国。

“十三五”时期，我国要积极推动网络强国建设。网络强国涉及技术、应用、文化、安全、立法、监管等诸多方面，不仅要突出抓好核心技术突破，还要提供更加安全可靠的软硬件支撑，加快建设高速、移动、安全、泛在的新一代信息基础设施，在不断推进新技术新业务应用、繁荣发展互联网经济的同时，要强化网络和信息安全，而培育高素质人才队伍是实施网络强国战略的重要措施。2015年，国务院学位委员会和教育部增设“网络空间安全”一级学科。我国信息安全学科建设和人才培养，迎来了全面高速发展的新阶段。

本书以培养学生的职业能力为核心，以工作实践为主线，以项目为导向，采用任务驱动、场景教学的方式，面向企业信息安全工程师人力资源岗位能力模型设置教学内容，建立以实际工作过程为框架的职业教育课程结构。全书共4章，主要内容如下：

第1章为Flow Shape网络流量整形，主要介绍针对网络带宽的DoS攻击及其解决方案；第2章为Web安全（Web Security），主要介绍Web开发三层架构概述、Web以及数据库安全概述、SQL注入攻击及其解决方案、XSS攻击及其解决方案；第3章为IPS入侵防御

系统，主要介绍缓冲区溢出攻击及其解决方案；第 4 章为网络安全数字取证，主要介绍网络安全数字取证及其解决方案。

本书由徐雪鹏任主编，岳大安和包楠任副主编，参加编写的还有孙雨春、赵飞、张鹏和李晓隆。

由于编者水平有限，书中难免存在不当和疏漏之处，敬请读者批评指正。联系邮箱为 ceo@knowskill.com。

编　者

登场人物介绍：

小李（姓名李子涛）：小李从小就对数字不敏感，小学时数学简单，他凭着一点小聪明还可以混个不错的分数，上了中学他还被不明真相的数学老师选中参加市里的华罗庚数学金杯赛。然而当小李沉着地看完试卷之后，才发现原来自己只知道“考生姓名”和“考生学校”这两个问题的答案。自此之后，小李终于彻头彻尾地明白了自己的终极归宿。高中毕业之后，小李的第一志愿不幸落空，他满腹悲愤地进入了一所理工大学的计算机系。小李一心向文，结果却要去学技术含量很高的计算机。更加让人想不到的是，命运对他眷顾良多，小李大学毕业后竟然被 TaoJin（韬金）电子商务公司录取。从业几年之后，小李居然也对计算机有了一点自己的心得，这也算是他人生中一段“东隅桑榆”的际遇。

Yueda（岳总，姓名岳大安）：Yueda 是 TaoJin（韬金）电子商务公司的 CSO（Chief Security Officer，首席安全官），主要负责监控、协调公司内部的信息安全工作，还负责制定公司安全措施和安全标准。此外，Yueda 还需要经常举办或参加相关领域的活动，如参与业务连续性、预防损失、诈骗预防和保护隐私等议题的相关活动。

Mr.White（白先生）：黑客并非都是黑的，那些用自己的黑客技术来做好事的黑客们叫“白帽黑客”。Mr.White（白先生）在某安全公司工作，负责检测计算机系统的安全性。Mr.White（白先生）被 TaoJin（韬金）电子商务公司首席安全官 Yueda 聘请来测试 TaoJin（韬金）电子商务公司的系统，以便进行安全审查。

故事梗概：

Yueda 为对 TaoJin（韬金）电子商务公司的系统进行全面的安全审查，聘请了某安全公司的白帽黑客 Mr.White 对系统进行了全面的渗透测试。渗透测试就是为了证明网络防御按照预期计划正常运行而提供的一种机制。不妨假设，公司定期更新安全策略和程序，时时给系统安装补丁程序，并采用了漏洞扫描器等工具，以确保所有补丁程序都已安装好。如果早已做到了这些，那么为什么还要请外方进行审查或渗透测试呢？因为渗透测试能够独立地检查网络策略，也就是给系统安了一双“眼睛”，保障公司对抗黑客对系统攻击的网络防御策略是有效的。通过 Mr.White 对系统进行了一系列的渗透测试，Yueda 指导员工小李实施了一系列安全有效的网络防御策略。

目　录

第1章 Flow Shape 网络流量整形

场景

在会议室里，Yueda、小李和白先生进行每天一次的例会。

白先生：根据贵单位对我提出的要求，今天我对贵单位的网络进行了针对网络带宽的DoS（Deny of Service）渗透测试，发现贵单位的网络在防御这种DOS攻击方面没有任何抵御的措施，一旦黑客对公司网络进行这种DOS攻击，那么公司的服务器将无法为客户提供服务。

小 李：什么是针对网络带宽的DoS呢？

白先生：在传统网络中，每个结点（包括主机和网络设备）对所有报文都无区别地等同对待，都采用先入先出的策略（First Input First Output，FIFO）处理，也就是说，它尽力而为（Best-effort）地将报文送到目的地，那么就有可能带来一个问题：黑客可以在用户使用网络之前，通过发出某种占用很高网络带宽的流量，这种流量可以是某种网络应用，如文件下载；也可以是专门设计出来针对网络带宽进行DoS攻击的流量，该流量可以占据网络中的绝大部分带宽，从而降低公司网络中的可使用的带宽。

如图1-1所示，就是我针对公司网络做的针对网络带宽的DoS渗透测试，可以提高Xunlei、Game以及专门设计出来针对网络带宽进行DoS攻击的带宽，从而降低用户访问公司网站的带宽。当这种DoS占用网络带宽的百分比为极限值100%的时候，用户访问公司网站的带宽就会为零，从而使公司的网站无法为用户再提供服务。

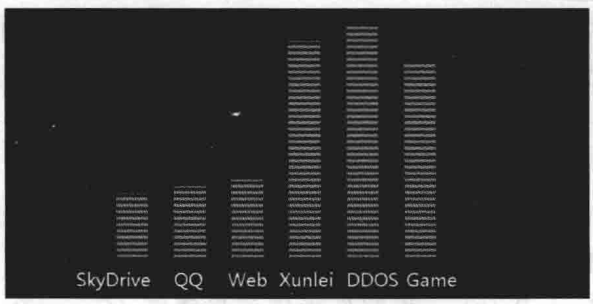

图1-1 针对网络带宽的DoS渗透测试

小 李：IP是“尽力而为”的，这个在上大学的时候曾经学过，但是没想到会带来这么严重的问题。

Yueda：小李，你觉得这个问题应该如何解决？

小 李：我觉得，既然这种攻击是利用某种流量可以占据网络中的绝大部分带宽，那么能不能针对这种流量进行限速呢？

Yueda：思路方向没错！接下来如何实现呢？

小 李：关于流量限速，我之前上学时，曾经学习过 QoS（Quality of Service，服务质量）这个技术。

Yueda：既然如此，你是否了解两个概念的区别：一个是流量监管（Traffic Policing），如图 1-2 所示；另一个是流量整形（Traffic Shaping），如图 1-3 所示。

小 李：流量监管的典型作用是限制进入某一网络的某一连接的流量与突发。在报文满足一定的条件时，如某个连接的报文流量过大，则流量监管就可以对该报文采取不同的处理动作，如丢弃报文或重新设置报文的优先级等。通常的用法是使用 CAR（Commit Access Rate）来限制某类报文的流量，如限制 HTTP 报文不能占用超过 50% 的网络带宽。

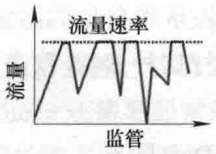

图 1-2 流量监管

Yueda：没错！那么流量整形呢？

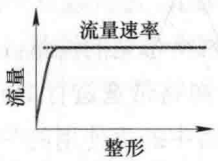

图 1-3 流量整形

小 李：流量整形与流量监管一样，典型作用是限制进入某一网络的某一连接的流量与突发量。主要区别在于：利用流量监管进行报文流量控制时，对不符合流量特性的报文进行丢弃；而流量整形对于不符合流量特性的报文则是进行缓冲，减少了报文的丢弃。

Yueda：概念没错！那么这两种技术是如何实现对流量进行控制的呢？

小 李：这两种技术都是通过令牌桶（Token Bucket）来判断流量是否违规。

Yueda：那么什么是令牌桶呢？

小 李：令牌桶是传送速率的定义，有以下 3 个参数。

1）数据突发量（Burst Size）：也叫作承诺的突发量（Committed Burst Size），指的是在给定的时间，允许一次发送的最大数据量。

2）平均速率（Mean Rate）：也叫作承诺信息速率（Committed Information Rate，CIR），指的是在单位时间内发送的数据量。

3）一定的时间间隔（Tc）：也叫作测量时间间隔（Time Interval），简称测量时间，指以秒为单位的时间定额。

这 3 个参数的关系可以表示为：

平均速率 = 数据突发量 / 一定的时间间隔

令牌桶的工作原理为：每一个令牌都代表发送数据的许可，没有令牌就不能发送数据。发送数据时，必须从令牌桶内移出与所发数据量等量的令牌，如图 1-4 和图 1-5 所示。

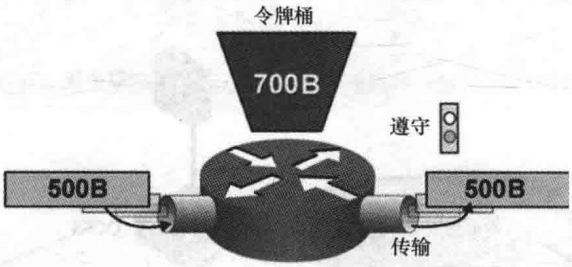

图 1-4　令牌桶的工作原理 1

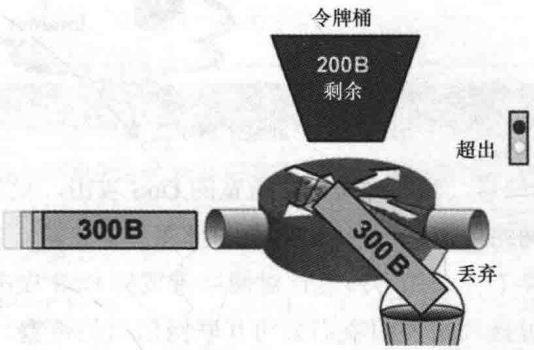

图 1-5　令牌桶的工作原理 2

如果桶内没有足够的令牌，则发送数据就必须等待，待有足够的令牌时再进行发送；如果令牌桶已经装满，后续来的令牌溢出，则溢出的令牌不能作为发送数据的许可。这样，任何时候，最大的突发数据量等于令牌桶的容量，如图 1-6 所示。

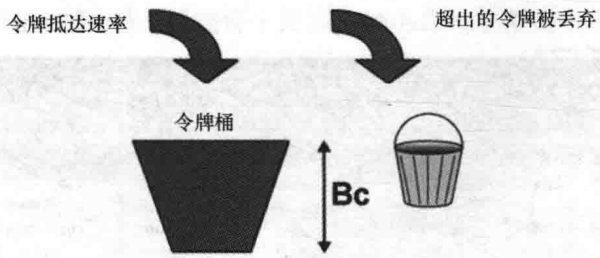

图 1-6　令牌桶的工作原理 3

Yueda：是的，我觉得还可以这样理解：假想除了令牌桶，还有一个数据桶，它的容量和令牌桶的容量相等；数据以 CIR 进入数据桶内，当数据桶被数据充满时，令牌桶刚好为空；如果进入数据桶的数据流速度过快，则数据桶溢出，令牌数为负数；溢出的数据如果被丢弃，则是流量监管；溢出的数据如果被缓存，则是流量整形。你们看这样理解是否可以？

小 李：这样理解太好了！

Yueda：下一个问题就是，使用哪个设备能够实现这样的功能。需要小李再去查询一下

公司的设备。还是先做出一个实施方案，然后进行模拟测试，再到实际网络中实施。

小 李：好的！

在第二天的讨论会上，小李首先开始介绍他为公司设计的方案，如图 1-7 所示。

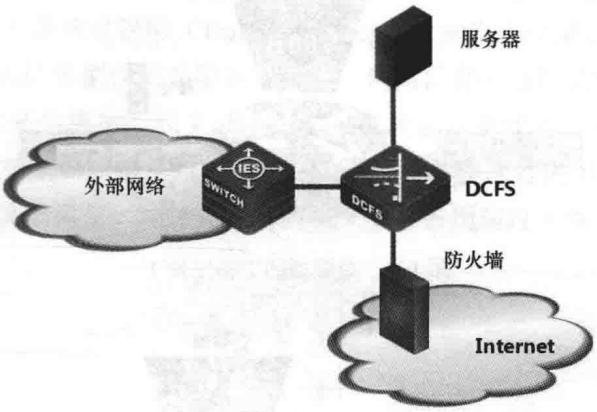

图 1-7　流量整形解决方案

小 李：各位领导和同事，为了应对网络带宽的 DoS 攻击，我为公司的网络设计了一个解决方案，在我们公司网络的 Internet 出口以及内部服务器之前，部署一个 DCFS（神州数码流量整形）设备，这样不管是黑客通过针对网络带宽的 DoS 攻击占用用户访问我们公司服务器的带宽，还是通过此攻击占用我们公司互联网出口的带宽，都可以进行限制，因为 DCFS 设备可以支持我们昨天谈到的流量整形技术。

Yueda：想法不错！那么具体应该如何实施呢？

小 李：如果我们要对 DCFS 设备的接口之间的流量进行限制，则必须先将 DCFS 的这些接口定义在同一个网桥中，相当于将这些接口定义在同一个 VLAN（Virtual Local Area Network，虚拟局域网）中，如图 1-8 所示。

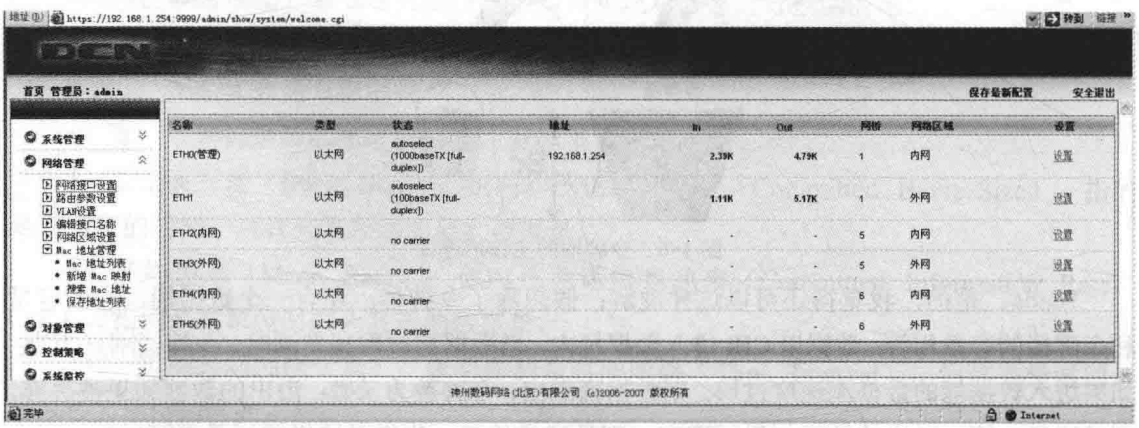

图 1-8　DCFS 接口网桥定义

另外，关于网络区域的定义，主要是为了定义接口需要具备的功能，如图 1-9 所示。

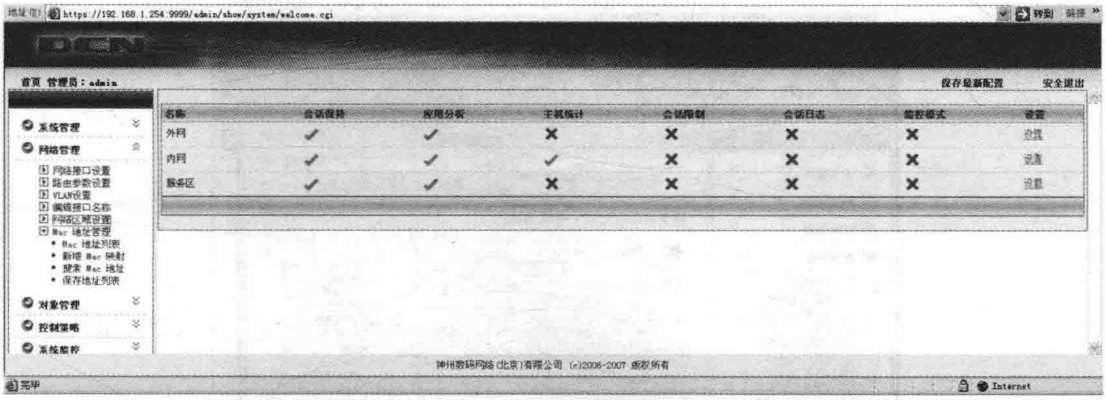

图 1-9　DCFS 接口区域定义

一般来讲，如果要进行流量整形，则接口需要具备会话保持、应用分析、主机统计、会话限制、会话日志这 5 个功能，如图 1-10 所示。

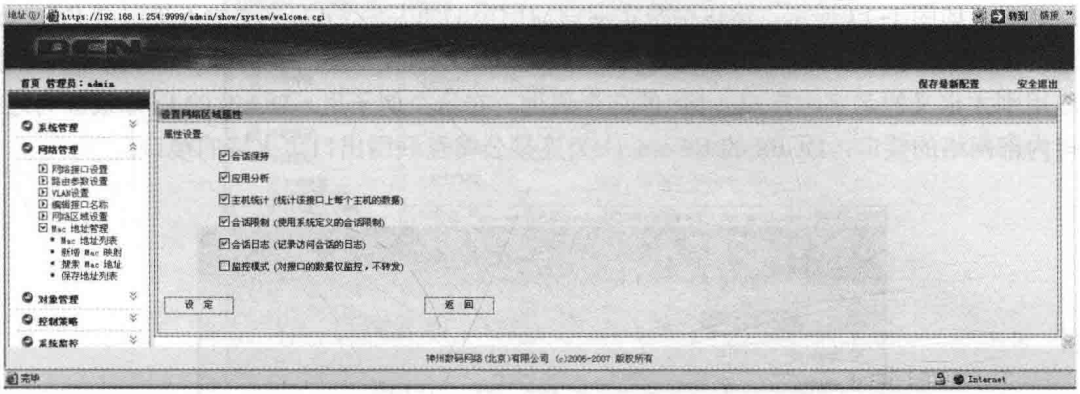

图 1-10　DCFS 区域功能定义

例如，想限制每个用户访问服务器的带宽不超过 1Mbit/s，则可以定义一个带宽通道。在以上这个带宽通道里，定义了这个通道的名字为 Outside，即将应用这个通道的接口带宽为 100Mbit/s，如图 1-11 所示。接下来，限制每个终端地址的带宽上限为 1Mbit/s，如图 1-12 所示。

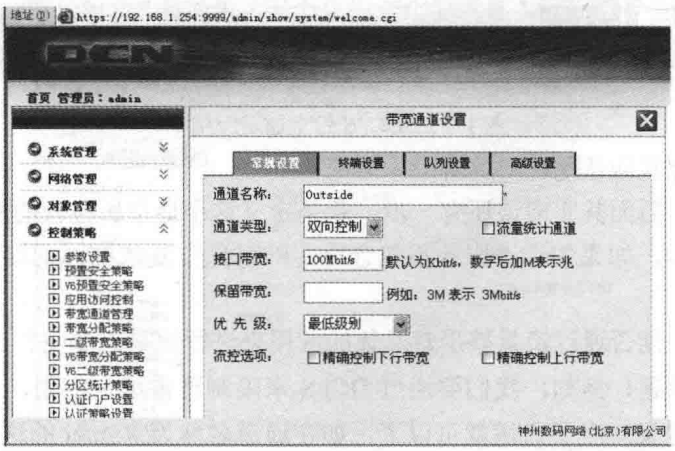

图 1-11　DCFS 带宽通道定义 1

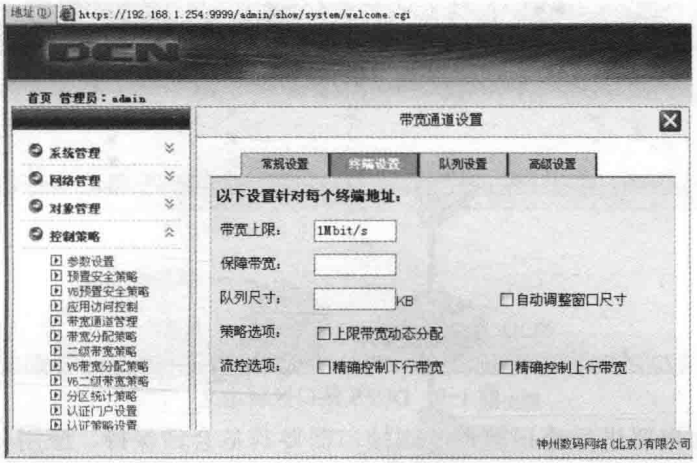

图 1-12　DCFS 带宽通道定义 2

然后，如图 1-13 所示，将这个带宽通道应用至 DCFS 的 Ethernet0 的入接口至 Ethernet1 的出接口，也就是说，从 DCFS 的 Ethernet0 进入，经过 DCFS 转发，再从 Ethernet1 流出的流量，将应用刚才定义的名字叫作 Outside 的这个通道。在这个例子里，DCFS 的 Ethernet0 为连接公司内部网络的接口，DCFS 的 Ethernet1 为连接公司互联网出口防火墙的接口。

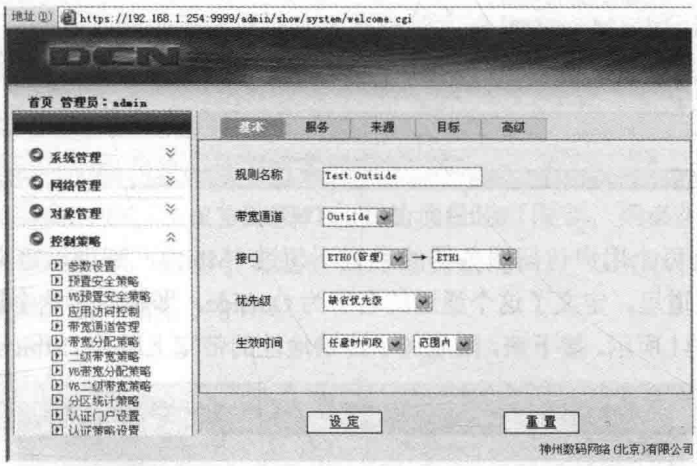

图 1-13　DCFS 带宽通道应用 1

Yueda：这个配置应该是针对所有应用的吧？

小 李：是的！后面其实应该还有一步，就是定义这个通道所包含的服务。

如图 1-14 所示，如果勾选“服务不包含选定的对象”复选框，则这个通道就包含了全部的应用。

Yueda：那么，能否通过流量整形对具体的应用来进行流量控制呢？

小 李：没有问题！例如，我们要通过 DCFS 来限制迅雷这个应用，只需要给刚才定义的 Outside 通道再定义一个子通道就可以了，如在通道名称为 Xunlei 的这个子通道中，定义迅雷这个应用的带宽上限为 20Mbit/s，如图 1-15 所示。

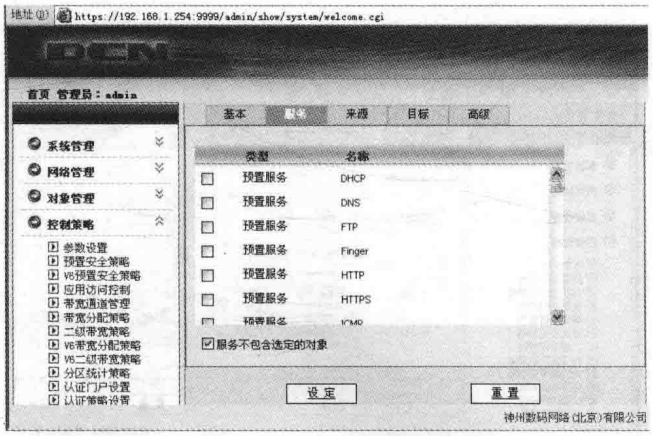

图 1-14　DCFS 带宽通道应用 2

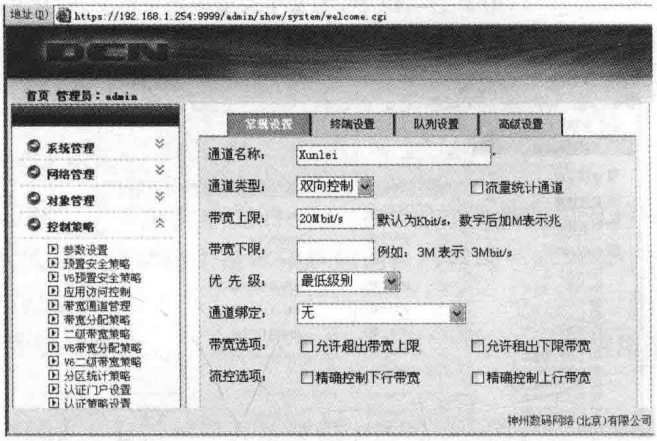

图 1-15　DCFS 带宽子通道定义 1

而且针对每个终端地址，迅雷的带宽上限为 512Kbit/s，如图 1-16 所示。

然后我们再将 Xunlei 这个子通道依旧应用至 DCFS 的 Ethernet0 的入接口至 Ethernet1 的出接口，如图 1-17 所示。但是这次，需要专门指定这个子通道包含的服务为 Xunlei。这里不能勾选“服务不包含选定的对象”复选框，因为我们选定的就是 Xunlei 这个服务，如图 1-18 所示。

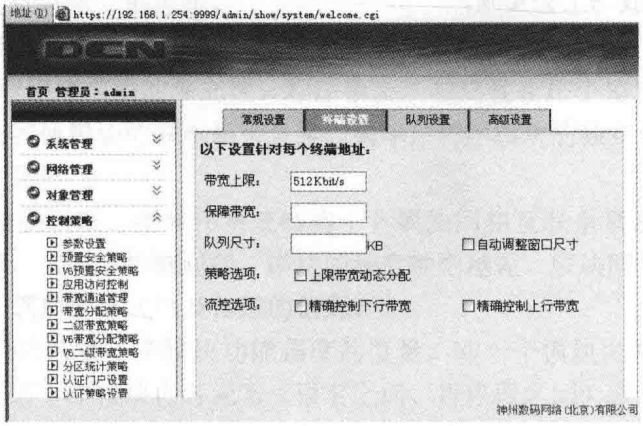

图 1-16　DCFS 带宽子通道定义 2

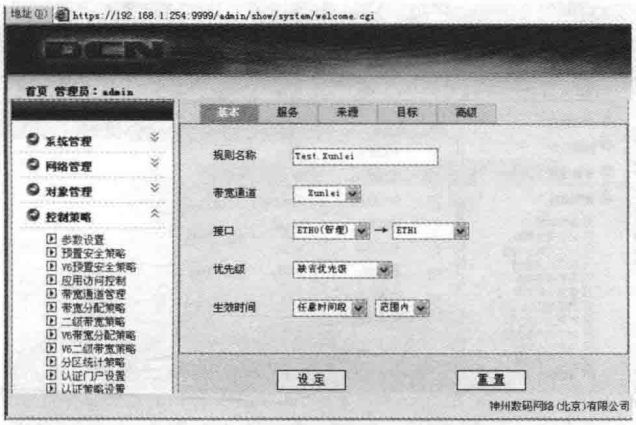

图 1-17　DCFS 带宽子通道应用 1

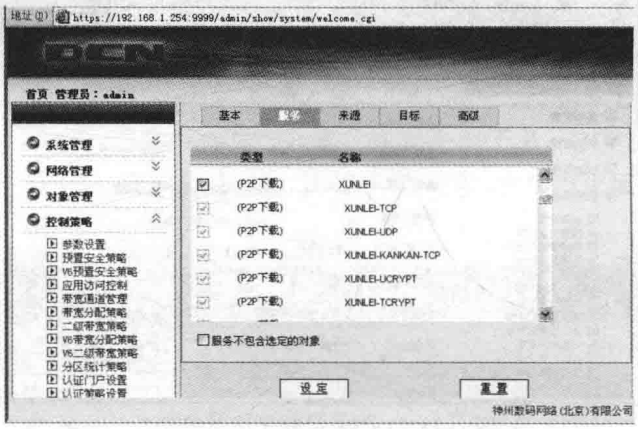

图 1-18　DCFS 带宽子通道应用 2

Yueda：既然你已经测试过了，这个技术就先介绍到这里吧！这里面还有两点也需要考虑：

1）来自公司内网的用户，访问公司服务器的流量，需要进行限制。

2）来自 Internet 的用户，访问公司服务器的流量，也需要进行限制。

小 李：好的！我马上去实施。

第2章 Web安全

2.1 Web开发三层架构概述

场景

在会议室里，Yueda、小李和白先生依旧进行每天一次的例会。

白先生：根据贵单位对我提出的要求，我开始了对贵单位的Web应用程序进行了渗透测试，首先需要确认一下：贵单位的Web应用程序是否是由贵单位内部的开发人员开发的？

Yueda：没错！这个程序是我们公司内部的开发人员自己开发的。

白先生：那就好办了！如果贵单位的Web应用程序是外包给其他软件公司的，那么为了解决开发中出现的问题，协调起来是比较麻烦的；现在由于是贵单位内部的开发人员开发的，有了问题就比较好协调了。

Yueda：没错！是这个情况，不知白先生在对我们公司的Web应用进行渗透测试时，发现了什么问题呢？

白先生：问题比较多！利用程序开发过程中的某些漏洞可以对Web服务器发起攻击，还有某些漏洞可以对Web客户端发起攻击。

Yueda：既然是程序开发过程中的某些漏洞，那么必须先将程序开发过程进行重现。小李，你是否了解Web应用程序的开发过程？

小 李：我之前了解过，Web应用程序有三层架构，通常意义上的三层架构就是将整个业务应用划分为表示层（UI）、业务逻辑层（BLL）和数据访问层（DAL）。区分层次的目的即为了“高内聚，低耦合”的思想。

Yueda：那么，请你解释一下，什么是“高内聚，低耦合”的思想。

小 李：为了实现程序模块的独立性。程序模块的独立性指每个模块只完成系统要求的独立子功能，并且与其他模块的联系最少且接口简单；程序模块的独立性有两个定性的度量标准，即耦合性和内聚性。

耦合性也称为块间联系，指软件系统结构中各模块间相互联系紧密程度的一种度量。模块之间联系越紧密，其耦合性就越强，模块的独立性则越差。模块间的耦合高低取决于模块间接口的复杂性、调用的方式以及传递的信息。

内聚性又称为块内联系，是模块功能强度的度量，即一个模块内部各个元素彼此结合的紧密程度的度量。若一个模块内各元素（语名之间、程序段之间）联系得越紧密，则它的内聚性就越高。

将软件系统划分模块时，尽量做到高内聚低耦合，提高模块的独立性，为设计高质量的软件结构奠定基础。

Yueda：其实你再举个例子就更加清楚了！一个程序有 50 个函数，这个程序执行得非常好；然而一旦你修改其中的一个函数，则其他 49 个函数都需要修改，这就是高耦合的后果。所以，在编写程序的时候自然会考虑到“高内聚，低耦合”。接下来再把 Web 应用程序的三层架构（见图 2-1）介绍一下吧！

小 李：

图 2-1　Web 开发三层架构

1）表示层：位于最外层（最上层），离用户最近，用于显示数据和接收用户输入的数据，为用户提供一种交互式操作的界面。

2）业务逻辑层：是系统架构中体现核心价值的部分。它的关注点主要集中在业务规则的制定、业务流程的实现等与业务需求有关的系统设计，也就是说，它与系统所应对的领域（Domain）逻辑有关，很多时候，也将业务逻辑层称为领域层。例如，Martin Fowler 在《Patterns of Enterprise Application Architecture》一书中，将整个架构分为三个主要的层：表示层、领域层和数据源层。作为领域驱动设计的先驱 Eric Evans，对业务逻辑层做了更细致的划分，细分为应用层与领域层，通过分层进一步将领域逻辑与领域逻辑的解决方案分离。业务逻辑层在体系架构中的位置很关键，它处于数据访问层与表示层中间，起到了数据交换中承上启下的作用。由于层是一种弱耦合结构，层与层之间的依赖是向下的，底层对于上层而言是“无知”的，改变上层的设计对于其调用的底层而言没有任何影响。如果在分层设计时，遵循了面向接口设计的思想，那么这种向下的依赖也应该是一种弱依赖关系。因而在不改变接口定义的前提下，理想的分层式架构应该是一个支持可抽取、可替换的“抽屉”式架构。正因为如此，业务逻辑层的设计对于一个支持可扩展的架构尤为关键，因为它扮演了两个不同的角色。对于数据访问层而言，它是调用者；对于表示层而言，它却是被调用者。依赖与被依赖的关系都纠结在业务逻辑层上，如何实现依赖关系的解耦，则是除了实现业务逻辑之外留给设计师的任务。

3）数据访问层：有时候也称为持久层，其功能主要是负责数据库的访问，可以访问数据库系统、二进制文件、文本文档或 XML 文档。简单的说法就是实现对数据表的 Select、Insert、Update 和 Delete 的操作。

Yueda：我总结一下，表示层（UI）通俗讲就是展现给用户的界面，即用户在使用一个系统的时候他的所见所得。业务逻辑层（BLL）也称为逻辑层，针对具体问题的操作，也可以说是对数据层的操作，对数据业务逻辑做处理。数据访问层（DAL）也称为存储层，该