网络安全技术系列丛书

Internet Firewalls and Network Secerity

Internet 防火墙与网络安全

（美）Chris Hare　Karanjit Siyan 著
刘成勇　刘明刚　王明苹　等译

机械工业出版社
西蒙与舒斯特国际出版公司
New Riders
CMP

网络安全技术系列丛书

Internet 防火墙与网络安全

（美） Chris Hare　Karanjit Siyan 著

刘成勇　刘明刚　王明举　等译

机 械 工 业 出 版 社

西蒙与舒斯特国际出版公司

本书介绍了网络安全和TCP/IP，讨论了防火墙和过滤路由器，以及各种理论和假定的例子。

本书可供系统管理员和对网络安全感兴趣的人员阅读。

本书版权登记号：图字： 01-98-0530

图书在版编目(CIP)数据

Internet 防火墙与网络安全/(美)海尔(Hare,C.),赛安(Siyan,K.)著；刘成勇等译，－北京：机械工业出版社，1998.5

(网络安全技术系列丛书)

书名原文：Internet Firewalls and Network Seccerity

ISBN 7-111-06273-6

Ⅰ.Ⅰ… Ⅱ.①海… ②赛… ③刘… Ⅲ.①因特网-防火墙②因特网-安全技术 Ⅳ.TP 393.4

中国版本图书馆CIP数据核字(98)第06014号

出 版 人：马九荣(北京市百万庄大街22号 邮政编码 100037)

责任编辑：蒋 克

三河永和印刷有限公司印刷 • 新华书店北京发行所发行

1998年5月第1版第1次印刷

787mm × 1092mm1/16 • 25印张

印数：0001-7000册

定价：43.00元

译 者 序

随着Internet在世界范围内的普及，网络安全问题变得愈来愈重要。1988年11月发生的“蠕虫”事件至今让人们记忆犹新。1996年初，美国国防部宣布其计算机系统在前一年中遭到25万次进攻，更令人不安的是，大多数进攻未被察觉。这些进攻给国家安全带来的影响程度还未确定，但多数已发现的进攻是针对计算机系统所存放的敏感和分类信息，其中2/3的进攻被认为是成功的，入侵者（黑客）盗窃、修改或破坏了系统上的数据。

正是由于这些在线犯罪，美国联邦调查局的国家计算机犯罪小组建议采用防火墙作为防止计算机犯罪的措施。目前看来，采用防火墙是防止Internet被入侵的最好办法。

网络安全问题也成了我国计算机业界的一个热门话题。网络管理员担心“黑客”的攻击，一般用户害怕电子邮件被人窃取，行政管理部门则关心如何把“黄货”拒于国门之外。许多人都殷切希望能有一本详细介绍网络安全的书。

我们可以欣慰地告诉读者朋友们，本书正是这样一本书。它既有令人信服的理论分析，又有详细的实例。它是系统管理员的必备的书，同时也可供对网络安全问题感兴趣的读者阅读。

细心的读者很容易看出本书的布局和安排。

第1章介绍了TCP/IP、寻址方式、TCP/IP守护程序和一些管理和用户命令。

第2章讨论了安全问题，包括安全级别、局部安全问题和网络等价，等等。

第3章详细阐述了如何设计一个网络安全策略，探讨了识别资源和威胁、网络使用和责任、安全策略遭到违反时的行动计划、使用加密和身份验证系统保护网络等诸多方面。这是建立高效防火墙的第一步。

第4章探讨了一次性口令身份验证系统（OTP），并介绍了具体的实现产品。

第5章简单介绍了理解过滤路由器和包过滤所必需的一些基本概念，描述了过滤路由器和防火墙与OSI参考模型之间的关系。

第6章讨论了包过滤规则的具体实现，并提供了详细的实例。

第7章讨论了两个基于PC的包过滤例子。包过滤可以与防火墙组合起来，形成安全网络的第一道防线。

第8章探讨了防火墙体系结构和理论。

第9章讨论了几种防火墙产品，包括Internet安全公司的FireWall-1、ANS的InterLock和TIS的Gauntlet。

第10章详细介绍了TIS防火墙工具箱，你会学到使用工具箱构造防火墙的

技术和方法。

第11章讨论了加拿大Milkyway网络公司的防火墙产品Black Hole，这是目前市场上一个比较成功的产品。

本书主要由刘成勇、刘明刚、王明举翻译，由刘成勇统稿。参加本书翻译工作的尚有秦广平、刘云凤、刘云秀、刘修昌、冯宏、张振、田木、杜诗。

由于时间仓促，译者水平有限，书中错误在所难免，希读者批评指正。

另外，本书英文原书附带光盘一张，对此感兴趣的读者，请与机械工业出版社华章公司联系。

译 者

1998年2月

前　言

《Internet防火墙与网络安全》是为系统管理员和那些认识到将计算机系统连接到Internet所隐含的危险的用户所编写的。

从前，在公寓的建筑物之间建有砖墙，以便火灾发生时，大火不会从一栋建筑物蔓延至另一栋建筑物，这些墙就很自然地被称为“防火墙”。

当你将局域网连接到Internet时，你就允许了你的用户与外部世界接触联系。但是，同时你也允许外部世界与你的局域网接触并进行交互。从最简单明了的意义上说，防火墙是数据通信通过其进行流动的路由器。如果入侵者试图非授权访问你的网络，你可以在防火墙阻击他们，不允许他们进入系统。

读者对象

本书是专为高级用户和系统管理员而编写的。

本书结构

第一部分简要介绍了安全和TCP/IP。TCP/IP作为Internet的协议，理解它是如何工作的以及可以使用哪些实用程序是很重要的，理解安全的概念和为什么有必要限制对资源的访问也是比较重要的。

第二部分讨论了防火墙和过滤路由器，不仅讨论了各种理论和假定的例子，而且给出了现实世界中的实例。另外还介绍了各种防火墙产品，以及使你能够建造自己的防火墙的工具箱。

第三部分，附录部分提供了一种查找关键信息的快速方式。附录A列出了本书中包含的工作表例子，以及它们的位置。附录B列出了更多的信息源。附录C提供了一张销售商列表。附录D提供了OPIE和Log Daemon这两种形式的一次性口令身份验证系统的手册。

本书使用的约定

本书使用一些约定来帮助你区别各种防火墙元素、系统文件和例子数据。在翻看本书之前，应该花一分钟看一下这些约定。

- 文中适当的地方使用了快捷键和键盘组合。例如，在大多数应用程序中，Shift+Ins是粘贴命令的快捷键组合。
- 键盘组合的格式如下:

键1+键2。当你在键名之间看到“+”时，你应该按住第一个键，同时按下第二个键，然后同时松开两个键。

键1，键2。当键中之间出现“,”号时，你应该按下并松开第一个键，然后按下并松开第二个键。

- 在屏幕上显示但不是应用程序一部分的文本，如系统提示或消息，以一种特殊的字形显示。

本书使用的特殊文本

通读全书，你会发现许多特殊文本的例子，这些段落都已作过特殊的处理，所以你能够认识到它们的重要性，并很容易地找到，以供将来参考之用。

注意、提示和警告

本书使用三种不同类型的特殊文本：注意、提示和警告。

“注意”包含了有用的“附加”信息，它是对前面讨论的补充，“注意”可能描述当你在某种环境下使用防火墙时引起的特殊情况，并告诉你当这种情况出现时应该采取什么步骤。

“提示”在你遵循一般讨论描述的步骤时，提供了一个快速的指南。“提示”可能会教你在某些设置中保留内存、加速进程或执行一个节省时间和提高系统功能的技巧的方法。

“警告”告诉你进程何时处于危险之中，也就是说，你何时会遇到丢失数据、锁定系统，或者甚至破坏硬件的危险。“警告”一般都阐述避免这些损失的方法，或者描述你可以采取的补救措施。

目　录

第1章 理解TCP/IP

TCP/IP是数据通信协议的集合，这些协议允许从一台机器路由信息至另一台机器，发送电子邮件和新闻，甚至使用远程注册能力。

所谓TCP/IP，指的是两个主要协议：传输控制协议(Transmission Control Protocol)和网际协议(Internet Protocol)。尽管还有许多其它协议也提供服务，但它们是最普及的。

1.1 TCP/IP的历史

TCP/IP的使用已经很多年了，几乎与Unix的历史一样悠久。TCP/IP，或叫传输控制协议/网际协议，是由美国国防部高级研究计划局（Defense Advanced Research Projects Agency——DARPA）研究创立的。在1969年，DARPA赞助的项目，以ARPANET而著名。该网络主要为政府、教育和研究实验室的两个主要计算机站点间提供高级带宽连通性。

ARPANET向那些用户提供从一个站点向另一个站点传输电子邮件和文件的能力，而DARPA为整个项目提供研究资金。随着该项目的演变，它所带来的诸多利益和优点显而易见，并提供了将全国网络连接在一起的可能性。

在20世纪70年代，DARPA继续资助和鼓励研究ARPANET，主要坚持点对点的租用线路互连。DARPA也开始力图研究通信连接的交替形式，例如，卫星和无线电。与此同时，有关网络技术的公用装置的框架开始形成。TCP/IP应运而生。在努力增加对该协议的认可和使用的过程中，DARPA采取了向用户团体提供低成本的工具措施。这种工具的主要目标是研究伯克利的BSD Unix工具的加利福尼亚大学。

DARPA资助创建了Bolt Beranek and Newman Inc.(BBN)公司在 BSD Unix系统上开发TCP/IP的具体实现工作，这项开发项目是在许多站点采用和开发局域网技术的背景下开展的，它们主要是基于以前曾经使用的单机环境下的扩展。到1993年1月止，所有连接到ARPANET上的计算机都已运行了新的TCP/IP协议，另外许多没有连接到ARPANET的站点也在使用TCP/IP协议。

因为ARPANET一般限制于政府部门与代理商，美国国家科学基金会(National Science Foundation)创建了NSFNet，它也使用成功的ARPANET协议。在某种意义上说，该网络是ARPANET的扩展，它包括一个连接所有美国国内超级计算机中心的骨干网络，以及一系列连接到NSFNet骨干网络的较小网络。

由于NSFNet采取的方法，大量的网络拓扑技术就可以使用了，并且TCP/IP也不再限制于任何单一的网络。这意味着TCP/IP可以运行令牌环、以太网(Ethernet)和其它总线拓扑技术、点到点租用专线，等等。但是，TCP/IP已经与以太网紧密地连接在一起了，以至于这二者几乎可以互换使用。

从那时起，Internet的使用就开始以一种惊人的速度增加，Internet这个全球网络的网络连接的数目也以爆炸式的速度递增。使用Internet的人不计其数，而且在当前这种信息爆炸的大趋势下，它必将触及很多人的生活。

但是TCP/IP不是一个单个的协议。事实上，它包含了许多协议，每一个协议提供一些特定的服务。本章余下的部分将阐述在TCP/IP中网络寻址是如何执行的，网络配置，控制使用TCP/IP的文件、许多各种管理命令和守护程序（daemon）。

注意 守护程序执行一个特定的功能。与其它执行并退出的命令不同，守护程序执行其工作，然后等待。例如，sendmail就是一个守护程序，它始终是活动的，即使没有邮件要处理，也是如此。

1.2 探索地址、子网和主机名

Internet上的每台机器必须有一个完全不同的地址，就像你的邮件地址一样，以便发送给它的信息能够成功地接收。这种地址模式由网际协议（IP）控制。

注意 编著本书之时，Internet工程工作组（Internet Engineering Task Force——IETF）几乎完成了下一个IP版本的规范，它将包括更大的地址空间。更大的地址空间是为了响应现在连接Internet的更多的计算机所必需的。

每台机器都有它自己的IP地址，该IP地址由两部分组成：网络部分和主机部分。地址的网络部分用来描述主机驻留的网络，主机部分用来识别特定的主机。要保证网络地址是唯一的，一个中央代理机构负责这些地址的分配。

因为最初的Internet设计者并不知道Internet会发展到何种程度，它们决定设计一种足够灵活的地址模式，以便能够处理拥有许多主机的大型网络或者只有几台主机的小型网络。这种地址模式引入了地址类的概念，一共有四种。

IP地址可以用几种不同的形式来表示。第一种是带圆点的十进制表示法，它显示为一个十进制数字，每个字节由“.”分开，比如192.139.234.102。另一种方式是用单个的十六进制数字来表示，比如0xC08BEA66。但是，使用最多的地址方式还是带圆点的十进制表示法。

1.2.1 地址类

如上所述，有四种主要的地址类：A、B、C和D。A、B和C类用来标识共享一个公用网络的计算机。D类，或叫多路广播地址，用来标识共享一个公用协议的计算机集合。因为前三类更常用一些，所以本章主要讲述这三类地址。每类地址都是由32位或4个字节组成。每个字节通常称为8位字节（octet，长度为8位的数据单位，也称作byte，但Internet用户不太采用术语byte，因为与Internet互联的部分计算机采用word，而不是byte），所以一个IP地址由4个 8位字节组成。

每个8位字节可取值0～255。但是，某些值另有特殊含义，如表1-1所示。

1. A类地址

在A类地址中，第一个8位字节表示网络部分，其余3个8位字节用来标识主机，如图1-1所示。

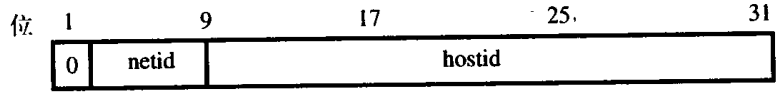

图1-1 A类地址格式

表1-1 保留的地址

带圆点的十进制地址	描 述
0.0.0.0	老的Sun网络的所有主机广播地址
num.num.num.0	标识整个网络
num.num.num.255	特定网络上的所有主机（广播地址）
255.255.255.255	当前网络的所有主机广播

这种地址类意味着，该网络可以拥有数以百万计的主机，因为它用24位来指定主机地址。在图1-1中，你可以看到第一个8位字节的首位被置为0。这意味着这类地址的网络部分必须小于128，实际上，A类地址的网络部分可取值1～127。

2.B类地址

B类地址的结构类似于A类地址，但有一点不同：B类地址使用两个8位字节作为网络部分，两个8位字节留给主机部分，如图1-2所示。这意味着，可以有更多的B类网络，每个网络拥有成千上万的主机。

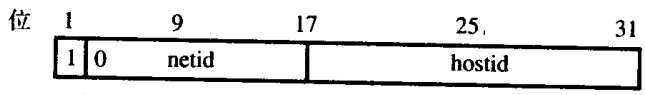

图1-2 B类地址格式

从图1-2中可以看出，B类地址配置为两个部分拥有相同数量的地址。该类网络地址的前两位被置为1和0，意味着网络地址的取值范围为129～191。使用这种格式，每个网络可拥有成千上万的主机。

3.C类地址

C类地址使用3个8位字节作为网络部分，只有1个8位字节留给主机。其结果是，可有更多的C类网络，每一个网络拥有很少的主机。因为1个8位字节的最大值是255，并且还有两个保留值，所以每个C类网络实际上可以拥有253台主机。这类网络格式，如图1-3所示。

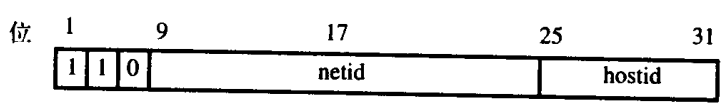

图1-3 C类地址格式

从图1-3中可以看出，该类网络地址的前两位被置为1，这意味着C类网络地址取值范围为192～223。余下的值为224～225，用于第四类地址。

4.特殊类

前面提到过，有一些用于特殊用途的保留地址类，参见表1-1。

这些保留地址不能用于任何主机或网络，它们已经预留作特殊的用途。还可能有其它的预留地址，这依赖于其它的一些因素。在本章稍后就会看到。

1.2.2 子网

一个网络上的每台主机都有一个特定的IP地址，以便其它主机能够与之通信。依赖于网络类别的不同，一个网络可以拥有的主机数从253至成千上万台不等。但是，将A类或B类地

址限制于一个拥有数以千计或数以百万计的网络是不切实际的。为了解决这个问题，人们开发出了子网(subnet)，将地址的主机部分分成附加的网络。

子网接收地址的主机部分，然后通过使用网络掩码（netmask）将其分开。实质上，网络掩码是将网络和主机间的分界线从地址中的一个地方移到了另一个地方，其产生的效果是增加了可用的网络数目，但减少了连接于每个网络的主机的数目。

子网的使用确实提供了很多好处。许多较小的公司只能拥有一个C类地址，但是它们的几间不同的办公室必须连接到一起。如果它们只有一个IP地址，路由器将不会连接两个地方，因为路由器要求每个网络拥有不同的地址。通过将网络分成子网，它们就能够使用路由器连接这两个网络，因为现在有了完全不同的网络地址。

子网是通过网络掩码或子网掩码(subnet mask)来解释的。在网络掩码中，如果某一位是打开的，那么地址中相应的位就被解释为网络位；如果该位是关闭的，它就被认为是主机地址部分。认识到下面一点是非常重要的：子网只在局部范围内被识别；对Internet的其余部分来说，该地址看起来像一个标准的IP地址。

从表1-2中可以看出，每一列IP地址都有一个与之相连的缺省网络掩码。

表1-2 标准网络掩码

地址类	缺省网络掩码
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

为了完全理解上述工作方式，我们来看一个例子。假定你有一个网络地址为193.53.64.0，你想把它分成子网。为了进一步细分该C类网络，你有必要使用主机部分的某些位，或该地址的最后一个字节作为网络部分。尽管这增加了你可以拥有的网络数目，但是减少了每个子网可有的主机数目。

Internet RFC 950也要求每个子网的第一和最后一个部分预留出来，这意味着实际的可用子网数目比总数少2。例如，如果你想将C类网络分成两部分，你将无法连接任何主机。如果你想拥有6个子网，就必须将网络分成8个部分。

下述例子描述了最后一个8位字节是如何设置的，以及每种情况可以创建多少子网和主机。字母V标识主机部分的可变部分，字母F标识地址的固定部分。

8	7	6	5	4	3	2	1	部分	子网	主机／子网
F	V	V	V	V	V	V	V	2	0	0
F	F	V	V	V	V	V	V	4	2	62
F	F	F	V	V	V	V	V	8	6	30
F	F	F	F	V	V	V	V	16	14	14
F	F	F	F	F	V	V	V	32	30	6
F	F	F	F	F	F	V	V	64	62	2
F	F	F	F	F	F	F	V	128	126	0

上述例子显示，你可以使用最少的4个部分、2个子网，每个网络有62台主机；或者使用最多的64个部分、62个子网，每个网络有2台主机。第一个例子可用于2个独立的以太网，而第二个例子可用于一系列点到点协议的连接。

但是，子网类型的选择是由任何子网所要求的用户的最大数目，以及所要求的子网的最少数目来决定的。

在分割过程中所形成的可能的网络部分，是通过计算最后一个字节的固定部分的值来形成的。再看一下上述例子，要将C类地址分成8个部分或6个子网，你需要固定最后一个8位字节的前3位。网络部分是通过计算最后一个字节的非固定部分来形成的。考虑下面的例子，它列出了位的组合，并描述了该类地址是如何分成子网的。

网络			主机					
8	7	6	5	4	3	2	1	十进制值
0	0	1	0	0	0	0	0	32
0	1	0	0	0	0	0	0	64
0	1	1	0	0	0	0	0	96
1	0	0	0	0	0	0	0	128
1	0	1	0	0	0	0	0	160
1	1	0	0	0	0	0	0	192

正如在上例中所显示的，最高的3位，即第8、第7和第6位，在它们用作主机地址部分时是固定的。这意味着可用的网络只有下述这些，其中N、O和P分别表示地址中的头3个8位字节:

网络
N.O.P.32
N.O.P.64
N.O.P.96
N.O.P.128
N.O.P.160
N.O.P.192

C类地址的标准网络掩码是255.255.255.0。对我们的子网网络来说，头3个字节是相同的，第4个字节通过设置网络部分为1、主机部分为0来创建。再重温一下前面的例子，你就会明白网络地址是什么样的。你使用相同的格式来决定网络掩码，这意味着这些子网的网络掩码是:

网络	广播	网络掩码
N.O.P.32	N.O.P.31	255.255.255.32
N. O.P.64	N.O.P.63	255.255.255.64
N.O.P.96	N.O.P.95	255.255.255.96
N.O.P.128	N.O.P.127	255.255.255.128
N. O.P.160	N.O.P.159	255.255.255.160
N.O.P.192	N.O.P.191	255.255.255.192

最终的结果是，你将此C类地址分成了6个子网，因此增加了可用的地址空间，而不必申请额外的网络地址。

当查看网络掩码时，很容易明白为什么许多管理员坚持面向字节的网络掩码——它们非常容易理解。但是，为网络掩码使用面向位的方法，可以完成许多不同的配置。例如，在C类地址上，使用网络掩码255.255.255.192可创建4个子网，但对于B类地址，相同的网络掩码可以