

使用IP链建立Linux操作系统防火墙 PDF转换可能丢失图片或格式，建议阅读原文

https://www.100test.com/kao_ti2020/145/2021_2022__E4_BD_BF_E7_94_A8IP_E9_93_c103_145162.htm 虽然Linux操作系统具有很多优点，其安全性也较高，但是你不应当由此产生一种虚假的安全感，因为你的Linux系统的安全性仍旧可能受到损害。现在就让我们来看看如何通过使用IP链（IPchains）来建立Linux系统的防火墙，保护你的系统不受侵害。先假设你已经具备了一些关于因特网的基本知识。应当说，熟悉像IP地址、TCP端口和网络传输数据之类的词汇是很有用处的。对防火墙有一个大概的了解也是十分有必要的。命令：我们需要确立起一系列的规则，这样IP链才能进入来来往往的网络路径。每一条规则都被置于三链之一，这三个链分别为：存放输入数据的输入链、存放输出数据的输出链和传输链。每增加一条规则，都要从IP链开始，并且要增加下面的某些或全部步骤。附加(Append)、删除>Delete)、插入(Insert)和替换(Replace)，这些命令通常是跟在起始的IP链命令之后，并且指示程序应当把规则命令添加在哪条链上以及如何添加。添加时，以-A、-D、-I，或者-R开始，这些字母的后面再加上链的名称（输入链或输出链）。当你要使用插入命令时，必须在要加入该命令的位置上，在链的名称后面，具体指定行号。在使用替换命令时，需要指定被替换的行号，使用删除命令的时候，也必须指定删除的行号。在使用删除选项时，无须在行号后面再输入什么别的内容。你只要键入ipchains -L，就可以发现命令所作用的行号。协议(Protocol)：在这里你要针对每一条规则命令具体地指明某种协议。在大多数情

形下，使用TCP/IP协议。也有可能你不想让你的计算机对另一台计算机发出的Ping信号做出反应。为了做到这一点，需要具体指定ICMP（互联网控制报文协议）。在具体地指定某个协议的时候，要使用-p命令，如：-p icmp。源(Source)：源可以确定从某个特定的IP地址而来的路径以及使用-s命令的端口。如果你知道一个标准的IP地址，就可以直接使用IP地址，或者干脆指定一个域名（比如www.ccidnet.com）。假如你想指定任意一个地址，不妨用0.0.0.0/0。我们可以在IP地址的后面用数字来指定某一个端口（比如110），也可以用服务器的名称（pop3）来指定某一个端口。使用冒号可以将两个端口数字分隔开，这样就能指定一连串的端口。例如：-s mail.mailserver.com pop3 -s 127.0.0.1 139:164目的(Destination)：用法与源地址是一样的，只要指定目的地址和端口即可。

100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com