

电子商务概论知识辅导：防火墙的配置 PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/170/2021\\_2022\\_\\_E7\\_94\\_B5\\_E5\\_AD\\_90\\_E5\\_95\\_86\\_E5\\_c40\\_170723.htm](https://www.100test.com/kao_ti2020/170/2021_2022__E7_94_B5_E5_AD_90_E5_95_86_E5_c40_170723.htm)

一、防火墙的基本配置方法

1、网络过滤防火墙图7.2 网络过滤防火墙

Internet 过滤  
路由器 Intranet

最简单的防火墙是只使用过滤路由器上的包过滤软件来实现数据包的筛选。这一配置如图7.2所示。这种配置使所有Intranet的出入都必须通过过滤路由器，由过滤路由器的规则确定允许什么通过。

(1) 网络过滤的优点对小型的、不太复杂的站点网络过滤比较容易实现。如果在您的网络与外界之间已经有一个独立的路由器，那么可以简单地加一个包过滤软件进去，只须一步就给您的整个网络加上了保护。包过滤不要求对运行的应用程序做任何改动，也不要求用户学习任何新的东西。除非用户试图做什么违反规则的事情，否则他们根本不会感觉到过滤服务器的存在。

(2) 网络过滤的不足网络过滤在安全管理上存在明显的不足，由于过滤路由器很少或根本没有日志记录能力，所以网络管理员很难确认系统是否正在被入侵或已经被入侵了。在实际应用中，过滤路由器的规则表很快会变得很大而且很复杂，应用的规则很难进行测试。随着规则表的增大和复杂性的增加，规则结构出现漏洞的可能性也会增加。不仅如此，这种防火墙的最大缺陷是依赖一个单一的部件来保护系统。如果这一部件出现问题，会使网络的大门敞开，而您甚至可能还不知道危险的来临。

2、双宿主网关Internet 双宿主主机 Intranet图7.3 双宿主网关

用一个单一的代理服务器可以建一个双宿主网关，如图7.3所示。双宿主主机是一台有两块网络接口卡（NIC）

的计算机，每一块网卡都有一个IP地址，如果网络上的一台计算机想与另一台计算机通信，他必须与双宿主主机上能“看到”的IP地址联系，代理服务器软件查看其规则是否允许连接，如果允许的话，代理服务器软件通过另一块网卡启动网络的连接。但值得注意的是，如果您建立了一个双宿主主机，那么应该确认操作系统的路由能力是关闭的。如果路由开着，从一块网卡到另一块网卡的通信可能会绕过代理服务器软件，造成网络管理的漏洞。

(1) 双宿主网关的优势

- n 双宿主网关其最主要的优势是网关可以将受保护的网络与外界完全隔离，从而提高网络的安全性能。
- n 代理服务器提供的安全日志，能有助于发现入侵。
- n 因为双宿主网关就是一台主机，所以可以用于诸如身份验证服务器及代理服务器等其他功能。
- n 由于使用代理服务器，DNS信息不会通过受保护系统到外界，所以站点系统的名字和IP地址对Internet系统是隐蔽的。

(2) 双宿主网关的不足

- n 代理服务器必须为使用它的每一项服务而专门设计，也就是说，每一项服务使用不同的代理服务器，如果您想增加一个代理服务器所不能提供的服务的话就会出现这个问题。
- n 如果IP发送以某种方式成为可能，如重新安装操作系统或忘记关掉路由，那么所有的安全性就都没有了。
- n 如果双宿主网关是防火墙的唯一部件，就存在一个单一失败点，它可能使您的网络安全受到危害。

### 3、主机过滤

图7.4 网络过滤防火墙

Internet 过滤 路由器 应用网关

Intranet

主机过滤防火墙既采用过滤路由器又采用了应用网关来实现高层次的安全，这是其中任何一个单独使用所不能达到的，其配置见图7.4所示。在一个主机过滤防火墙中来自Internet的所有通信都直接到过滤路由器，它根据所给规则

过滤这些通信。多数情况下所有与应用网关之外机器的通信都将被拒绝。在这种情况下，应用网关只有一块网络接口卡（也就是说它不是双宿主网关）。网关的代理服务器软件使用它自己的规则，将被允许的通信传送到受保护的网络上。

（1）主机过滤防火墙的优点n 主机过滤防火墙的配置比双宿主网关防火墙更灵活，它可以设置使过滤路由器将某些通信直接传到Intranet的站点而不是到应用网关。n 因为多数或所有通信将直接到应用网关，所以包过滤器的规则比网络过滤配置更简单。（2）主机过滤防火墙的不足n 防火墙的两个部件须认真配置以使其能共同准确地工作，如路由器应设置成将所有通信路由到代理服务器。尽管包过滤规则不太复杂，但配置整个防火墙的总的工作也会很复杂。n 系统的灵活性会导致走捷径从而暗中破坏安全。例如，用户可能试图避开代理服务器直接与路由器建立联系。因此，在实际工作中维护安全策略，需要管理员付出更大的努力。 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](http://www.100test.com)