新手入门之Linux防火墙配置基础篇 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/224/2021_2022__E6_96_B0_E6_89_8B_E5_85_A5_E9_c103_224241.htm RedHat Linux 为增加系统安全性提供了防火墙保护。防火墙存在于你的计算机和网络之间，用来判定网络中的远程用户有权访问你的计算机上的哪些资源。一个正确配置的防火墙可以极大地增加你的系统安全性。 为你的系统选择恰当的安全级别。 「高级」 如果你选择了「高级」，你的系统就不会接受那些没有被你具体指定的连接（除了默认设置外）。只有以下连接是默认允许的： DNS回应 DHCP 任何使用 DHCP 的网络接口都可以被相应地配置。 如果你选择「高级」，你的防火墙将不允许下列连接： 1.活跃状态FTP（在多数客户机中默认使用的被动状态FTP应该能够正常运行。） 2.IRC DCC 文件传输 3.RealAudio 4.远程 X 窗口系统客户机 如果你要把系统连接到互联网上，但是并不打算运行服务器，这是最安全的选择。如果需要额外的服务，你可以选择 「定制」 来具体指定允许通过防火墙的服务。 注记:如果你在安装中选择设置了中级或高级防火墙，网络验证方法（NIS 和 LDAP）将行不通。 「中级」 如果你选择了「中级」，你的防火墙将不准你的系统访问某些资源。访问下列资源是默认不允许的： 1.低于1023的端口 这些是标准要保留的端口，主要被一些系统服务所使用，例如： FTP 、 SSH 、 telnet 、 HTTP 、和 NIS 。 2.NFS 服务器端口（2049） 在远程服务器和本地客户机上，NFS 都已被禁用。 3.为远程 X 客户机设立的本地 X 窗口系统显示。 4.X 字体服务器端口（ xfs 不在网络中监听；它在字体服务器中被

默认禁用）。 如果你想准许到RealAudio之类资源的访问，但仍要堵塞到普通系统服务的访问，选择 「中级」 。你可以选择 「定制」 来允许具体指定的服务穿过防火墙。 注记:如果你在安装中选择设置了中级或高级防火墙，网络验证方法（NIS 和 LDAP）将行不通。 「无防火墙」 无防火墙给予完全访问权并不做任何安全检查。安全检查是对某些服务的禁用。建议你只有在一个可信任的网络（非互联网）中运行时，或者你想稍后再进行详细的防火墙配置时才选此项。 选择 「定制」 来添加信任的设备或允许其它的进入接口。 「信任的设备」 选择「信任的设备」中的任何一个将会允许你的系统接受来自这一设备的全部交通；它不受防火墙规则的限制。例如，如果你在运行一个局域网，但是通过PPP拨号连接到了互联网上，你可以选择「eth0」，而后所有来自你的局域网的交通将会被允许。把「eth0」选为 “ 信任的 ” 意味着所有这个以太网内的交通都是被允许的，但是ppp0接口仍旧有防火墙限制。如果你想限制某一接口上的交通，不要选择它。 建议你不要将连接到互联网之类的公共网络上的设备定为「信任的设备」。 「允许进入」 启用这些选项将允许具体指定的服务穿过防火墙。注意：在工作站类型安装中，大多数这类服务在系统内没有被安装。 「DHCP」 如果你允许进入的 DHCP 查询和回应，你将会允许任何使用 DHCP 来判定其IP地址的网络接口。DHCP通常是启用的。如果DHCP没有被启用，你的计算机就不能够获取 IP 地址。 「SSH」 Secure（安全）SHell（SSH）是用来在远程机器上登录及执行命令的一组工具。如果你打算使用SSH工具通过防火墙来访问你的机器，启用该选项。你需要安装openssh-server 软件包以便

使用 SSH 工具来远程访问你的机器。 「Telnet」 Telnet是用来在远程机器上登录的协议。Telnet通信是不加密的，几乎没有提供任何防止来自网络刺探之类的安全措施。建议你不要允许进入的Telnet访问。如果你想允许进入的 Telnet 访问，你需要安装 telnet-server 软件包。 「WWW (HTTP)」 HTTP协议被Apache（以及其它万维网服务器）用来进行网页服务。如果你打算向公众开放你的万维网服务器，请启用该选项。你不需要启用该选项来查看本地网页或开发网页。如果你打算提供网页服务的话，你需要安装 httpd 软件包。 启用 「WWW (HTTP)」 将不会为 HTTPS 打开一个端口。要启用 HTTPS，在 「其它端口」 字段内注明。 「邮件 (SMTP)」 如果你需要允许远程主机直接连接到你的机器来发送邮件，启用该选项。如果你想从你的ISP服务器中收取POP3或IMAP邮件，或者你使用的是fetchmail之类的工具，不要启用该选项。请注意，不正确配置的 SMTP 服务器会允许远程机器使用你的服务器发送垃圾邮件。 「FTP」 FTP 协议是用于在网络机器间传输文件的协议。如果你打算使你的 FTP 服务器可被公开利用，启用该选项。你需要安装 vsftpd 软件包才能利用该选项。 「其它端口」 你可以允许到这里没有列出的其它端口的访问，方法是在 「其它端口」 字段内把它们列出。格式为 ： 端口:协议 。例如，如果你想允许 IMAP 通过你的防火墙，你可以指定 imap:tcp 。你还可以具体指定端口号码，要允许 UDP 包在端口 1234 通过防火墙，输入 1234:udp 。要指定多个端口，用逗号将它们隔开。 窍门:要在安装完毕后改变你的安全级别配置，使用 安全级别配置工具 。 在 shell 提示下键入 redhat-config-securitylevel 命令来启动 安全级别配置工具 。如

果你不是根用户，它会提示你输入根口令后再继续。 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