# FirewallD防火墙



### FirewallD防火墙简介

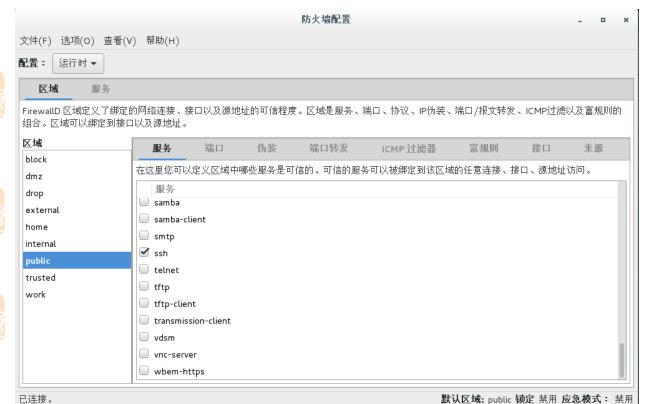
Linux为增加系统安全性提供了防火墙保护功能。防火墙存在于计算机和网络之间,用于判断网络中的远程用户的访问权限。在RHEL 7系统中默认使用FirewallD防火墙,FirewallD提供了支持网络/防火墙区域定义网络链接以及接口安全等级的动态防火墙管理工具。它支持IPv4、IPv6防火墙设置以及以太网桥接,并且拥有运行时配置和永久配置选项。它也支持允许服务或者应用程序直接添加防火墙规则的接口。以前的iptables防火墙是静态的,每次修改都要求防火墙完全重启。现在FirewallD可以动态管理防火墙,支持动态配置,不用重启服务。

**高** 新 東 新 東 通过将网络划分成不同的区域,制定出不同区域之间的访问控制策略,以此来控制不同程度区域间传送的数据流。比如互联网是不可信任的区域,而内部网络是高度信任的区域。数据包进入到内核必须要通过区域,而不同的区域定义的规则是不一样的。可以根据网卡所连接的网络的安全性来判断,这块网卡的流量到底使用哪个区域。可以把这些区域想象成进入火车站的安检,不同的入口检测的严格度不一样。默认情况下FirewallD防火墙的连接区域为public,public在公共区域内使用,指定外部连接可以进入内部网络或主机。



### FirewallD防火墙配置

在Linux系统图形界面中单击面板上的【应用程序】 -〉【杂项】 -〉【防火墙】,或在图形界面下的终端中输入firewall-config命令,打开下图所示的【防火墙配置】界面,默认使用public区域。







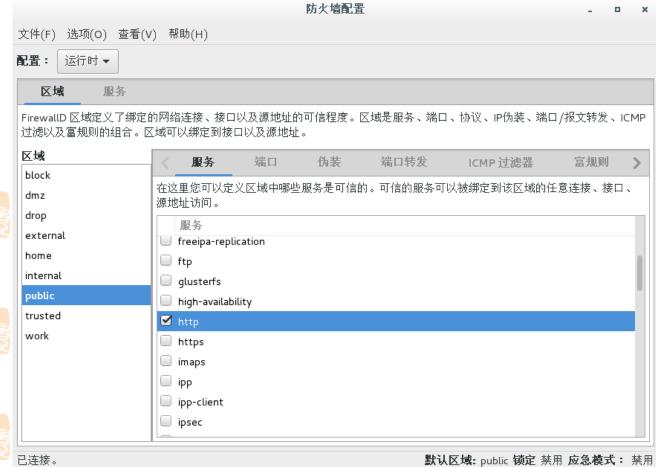






### 1、添加可信服务





















#### 防火墙配置

文件(F) 选项(O) 查看(V) 帮助(H)

配置: 运行时 ▼

#### 区域 服务

FirewallD 区域定义了绑定的网络连接、接口以及源地址的可信程度。区域是服务、端口、协议、IP伪装、端口/报文转发、ICMP 过滤以及富规则的组合。区域可以绑定到接口以及源地址。

端口转发

络将不可见,且该主机是以单一地址的形式出现在互联网中。伪装仅适用于 IPv4。

ICMP 过滤器

如果您要设置一台将您的本地网络连接到互联网的主机或者路由器,伪装是很有用的。您的本地网

#### 区域

block

dmz

drop

external

home

internal

#### public

trusted work

☑ 伪装区域 如果您启用伪装,将会为您的 IPv4 网络启用 IP 转发。

伪装

端口











默认区域: public 锁定 禁用 应急模式: 禁用

富规则

接口



## 4、端口转发



