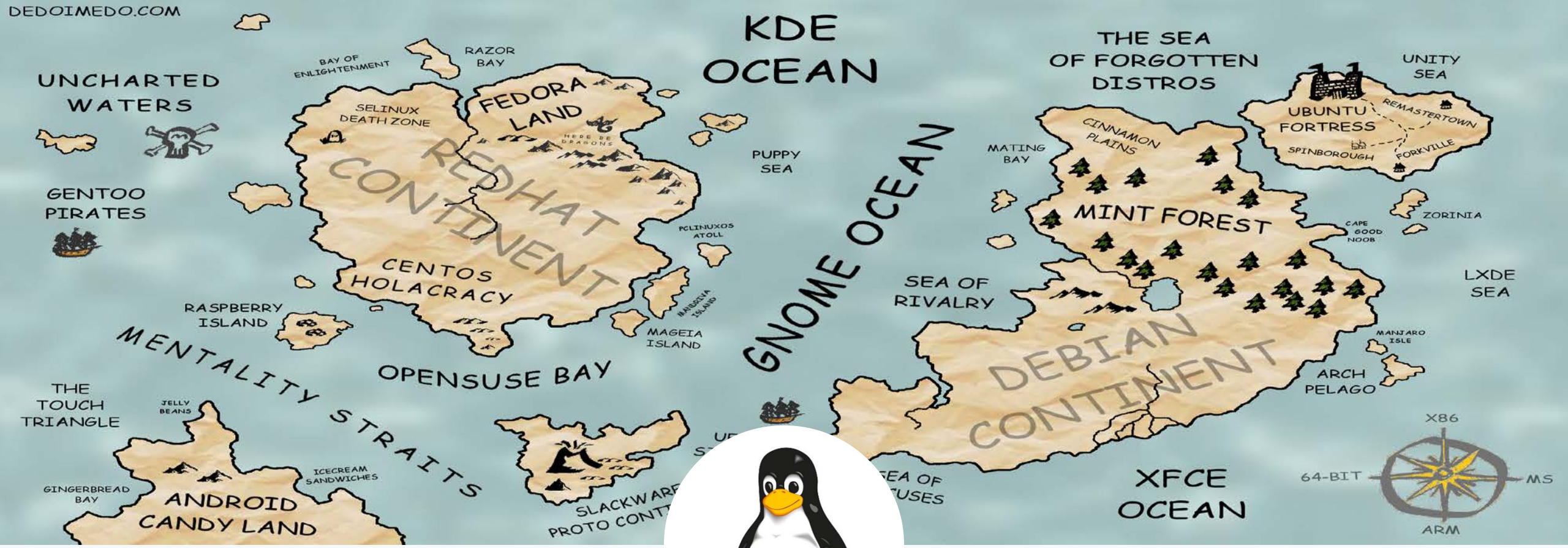


使用iptables与firewalld防火墙

任课教师：刘遄 www.LinuxProbe.com

课程概述

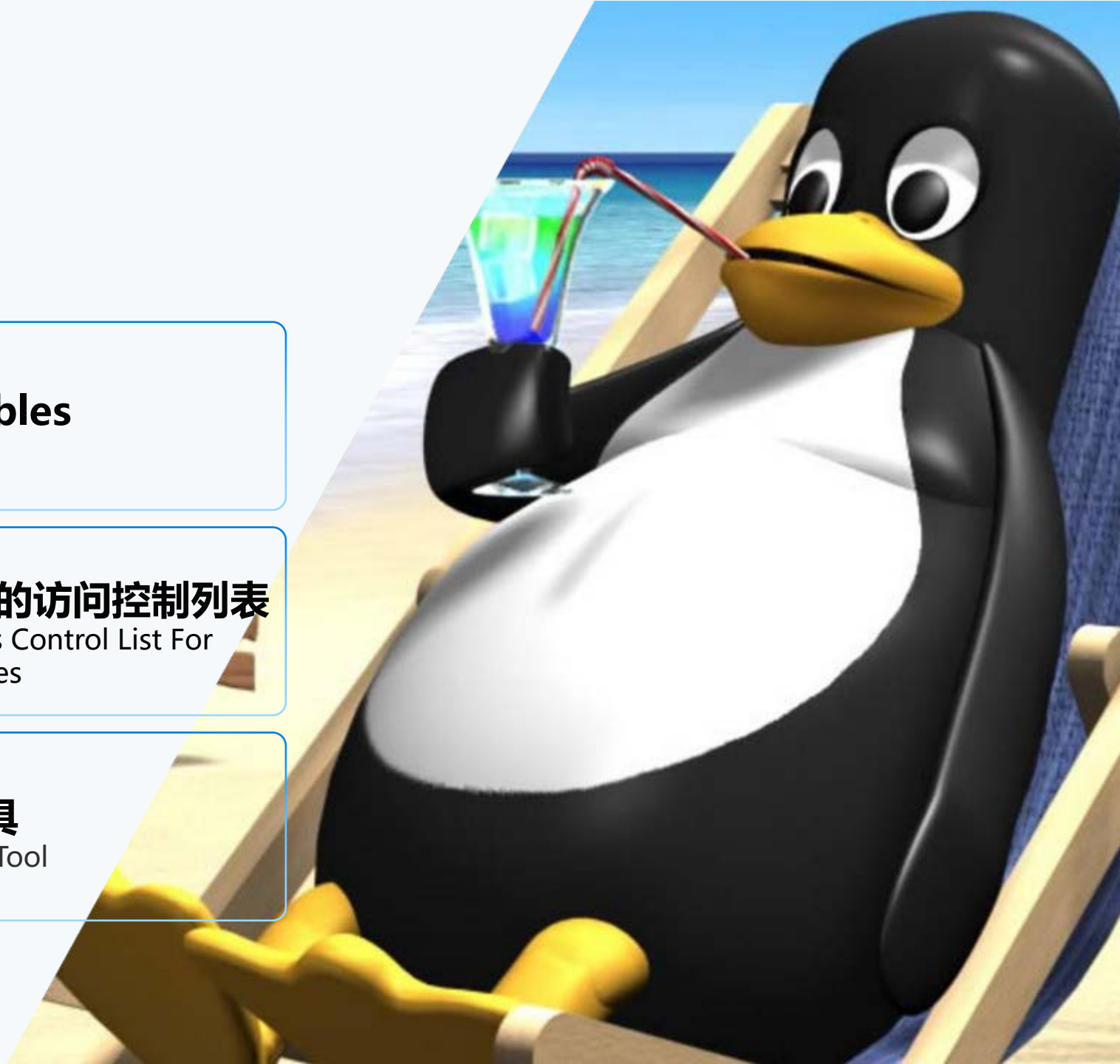
01 防火墙管理工具
Firewall Management Tools

02 iptables

03 firewalld

04 服务的访问控制列表
Access Control List For Services

05 Cockpit驾驶舱管理工具
Cockpit Cockpit Management Tool



前言

01 保障数据的安全性是继保障数据的可用性之后最为重要的一项工作。防火墙作为公网与内网之间的保护屏障，在保障数据的安全性方面起着至关重要的作用。

02 分别使用iptables、firewall-cmd、firewall-config和TCP Wrapper等防火墙策略配置服务来完成数十个根据真实工作需求而设计的防火墙策略配置实验。

03 在学习完这些实验之后，不仅能够熟练地过滤请求的流量、基于服务程序的名称对流量进行允许和拒绝操作，还可以使用Cockpit轻松监控系统的运行状态，确保Linux系统的安全性万无一失。

防火墙管理工具

Firewall Management Tools

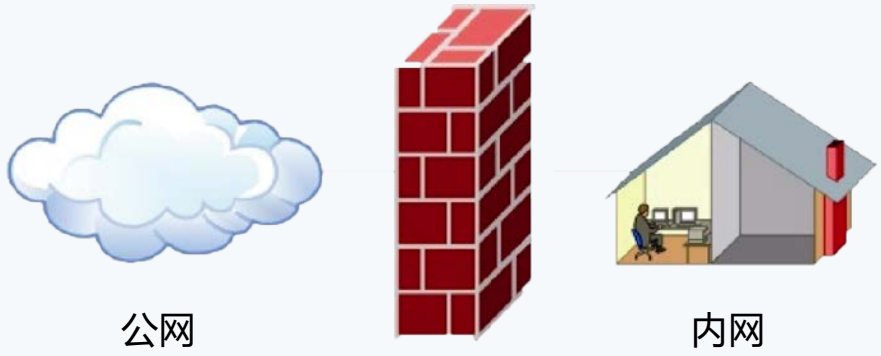
防火墙管理工具

01 在公网与企业内网之间充当保护屏障的防火墙虽然有软件或硬件之分，但主要功能都是依据策略对穿越防火墙自身的流量进行过滤。

02 防火墙策略可以基于流量的源目地址、端口号、协议、应用等信息来定制，然后防火墙使用预先定制的策略规则监控出入的流量，若流量与某一条策略规则相匹配，则执行相应的处理，反之则丢弃。

03 从RHEL 7系统开始，firewalld防火墙正式取代了iptables防火墙。iptables与firewalld都不是真正的防火墙，它们都只是用来定义防火墙策略的防火墙管理工具。

04 iptables服务会把配置好的防火墙策略交由内核层面的netfilter网络过滤器来处理，而firewalld服务则是把配置好的防火墙策略交由内核层面的nftables包过滤框架来处理。



防火墙作为公网与内网之间的保护屏障

iptables

Iptables—策略与规则链

01 防火墙会按照从上到下的顺序来读取配置的策略规则，在找到匹配项后就立即结束匹配工作并去执行匹配项中定义的行为（即放行或阻止）。

02 如果在读取完所有的策略规则之后没有匹配项，就去执行默认的策略。一般而言，防火墙策略规则的设置有两种：“通”（即放行）和“堵”（即阻止）。

03 当防火墙的默认策略为拒绝时（堵），就要设置允许规则（通），否则谁都进不来；如果防火墙的默认策略为允许，就要设置拒绝规则，否则谁都能进来，防火墙也就失去了防范的作用。

Iptables—策略与规则链

1. 在进行路由选择前处理数据包（PREROUTING）；
2. 处理流入的数据包（INPUT）；
3. 处理流出的数据包（OUTPUT）；
4. 处理转发的数据包（FORWARD）；
5. 在进行路由选择后处理数据包（POSTROUTING）。

Iptables—基本的命令参数

01 根据OSI七层模型的定义，iptables属于数据链路层的服务，所以可以根据流量的源地址、目的地址、传输协议、服务类型等信息进行匹配；

02 一旦匹配成功，iptables就会根据策略规则所预设的动作来处理这些流量。

参数	作用
-P	设置默认策略
-F	清空规则链
-L	查看规则链
-A	在规则链的末尾加入新规则
-I num	在规则链的头部加入新规则
-D num	删除某一条规则
-s	匹配来源地址IP/MASK，加叹号“!”表示除这个IP外
-d	匹配目标地址
-i网卡名称	匹配从这块网卡流入的数据
-o网卡名称	匹配从这块网卡流出的数据
-p	匹配协议，如TCP、UDP、ICMP
--dport num	匹配目标端口号
--sport num	匹配来源端口号

iptables中常用的参数以及作用

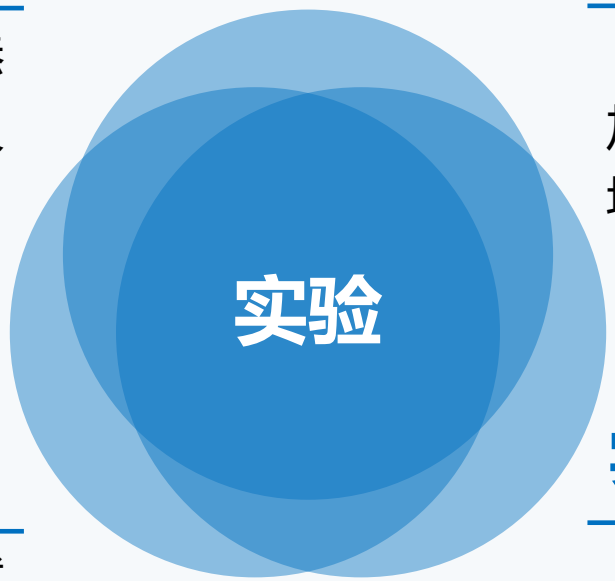
Iptables—基本的命令参数

实验1

在iptables命令后添加-L参数查看已有的防火墙规则链。

实验2

在iptables命令后添加-F参数清空已有的防火墙规则链。



实验3

把INPUT规则链的默认策略设置为拒绝。

实验4

向INPUT链中添加允许ICMP流量进入的策略规则。

Iptables—基本的命令参数

实验5

删除INPUT规则链中刚刚加入的那条策略（允许ICMP流量），并把默认策略设置为允许。

实验6

将INPUT规则链设置为只允许指定网段的主机访问本机的22端口，拒绝来自其他所有主机的流量。

实验9

向INPUT规则链中添加拒绝所有主机访问本机1000～1024端口的策略规则。

实验7

向INPUT规则链中添加拒绝所有人访问本机12345端口的策略规则。

实验8

向INPUT规则链中添加拒绝192.168.10.5主机访问本机80端口（Web服务）的策略规则。

firewalld

firewalld

01

firewalld （Dynamic Firewall Manager of Linux systems，Linux系统的动态防火墙管理器）服务是默认的防火墙配置管理工具，它拥有基于CLI（命令行界面）和基于GUI（图形用户界面）的两种管理方式。

02

相较于传统的防火墙管理配置工具，firewalld支持动态更新技术并加入了区域（zone）的概念。

03

在以往，我们需要频繁地手动设置防火墙策略规则，而现在只需要预设好区域集合，然后轻点鼠标就可以自动切换了，从而极大地提升了防火墙策略的应用效率。

firewalld中常用的区域名称及策略规则

区域	默认规则策略
trusted	允许所有的数据包
home	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh、mdns、ipp-client、smba-client、dhcpv6-client服务相关，则允许流量
internal	等同于home区域
work	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh、ipp-client与dhcpv6-client服务相关，则允许流量
public	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh、dhcpv6-client服务相关，则允许流量
external	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh服务相关，则允许流量
dmz	拒绝流入的流量，除非与流出的流量相关；而如果流量与ssh服务相关，则允许流量
block	拒绝流入的流量，除非与流出的流量相关
drop	拒绝流入的流量，除非与流出的流量相关

终端管理工具

参数	作用
--get-default-zone	查询默认的区域名称
--set-default-zone=<区域名称>	设置默认的区域，使其永久生效
--get-zones	显示可用的区域
--get-services	显示预先定义的服务
--get-active-zones	显示当前正在使用的区域与网卡名称
--add-source=	将源自此IP或子网的流量导向指定的区域
--remove-source=	不再将源自此IP或子网的流量导向某个指定区域
--add-interface=<网卡名称>	将源自该网卡的所有流量都导向某个指定区域
--change-interface=<网卡名称>	将某个网卡与区域进行关联
--list-all	显示当前区域的网卡配置参数、资源、端口以及服务等信息
--list-all-zones	显示所有区域的网卡配置参数、资源、端口以及服务等信息
--add-service=<服务名>	设置默认区域允许该服务的流量
--add-port=<端口号/协议>	设置默认区域允许该端口的流量
--remove-service=<服务名>	设置默认区域不再允许该服务的流量
--remove-port=<端口号/协议>	设置默认区域不再允许该端口的流量
--reload	让“永久生效”的配置规则立即生效，并覆盖当前的配置规则
--panic-on	开启应急状况模式
--panic-off	关闭应急状况模式

firewall-cmd命令中使用的参数以及作用

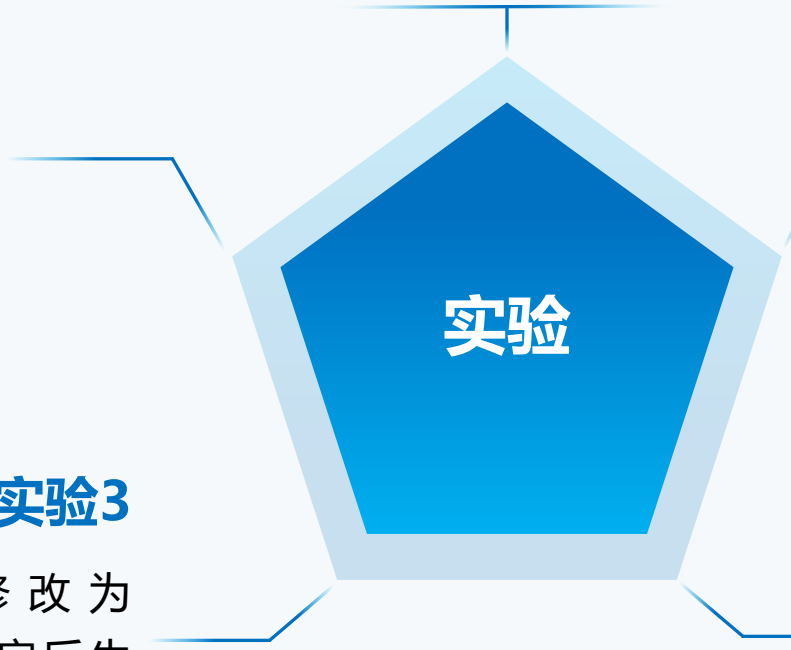
终端管理工具

实验1

查看firewalld服务当前所使用的区域。

实验2

查询指定网卡在firewalld服务中绑定的区域。



实验5

启动和关闭firewalld防火墙服务的应急状况模式。

实验3

把网卡默认区域修改为external，并在系统重启后生效。

实验4

把firewalld服务的默认区域设置为public。

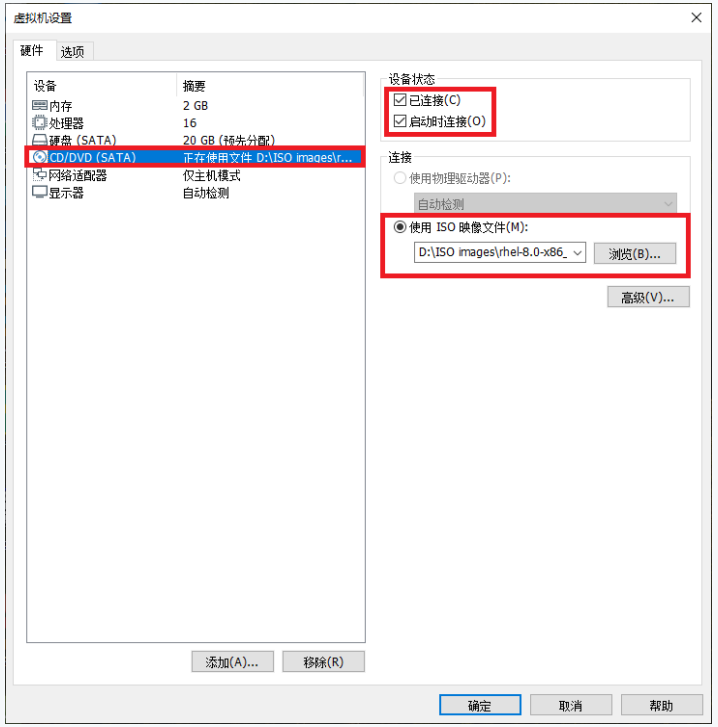
终端管理工具

实验6	查询SSH和HTTPS协议的流量是否允许放行。
实验7	把HTTPS协议的流量设置为永久允许放行，并立即生效。
实验8	把HTTP协议的流量设置为永久拒绝，并立即生效。
实验9	把访问8080和8081端口的流量策略设置为允许，但仅限当前生效。
实验10	把原本访问本机888端口的流量转发到22端口，要且求当前和长期均有效。
实验11	富规则的设置。它的优先级在所有的防火墙策略中也是最高的。

图形管理工具—配置软件仓库

首先

将虚拟机的“CD/DVD（SATA）”光盘选项设置为“使用ISO映像文件”，然后选择已经下载好的系统镜像。



将虚拟机的光盘设备指向ISO镜像

然后

把光盘设备中的系统镜像挂载到/media/cdrom目录。为了能够让软件仓库一直为用户提供服务，更加严谨的做法是将系统镜像文件的挂载信息写入到/etc/fstab文件中，以保证万无一失。

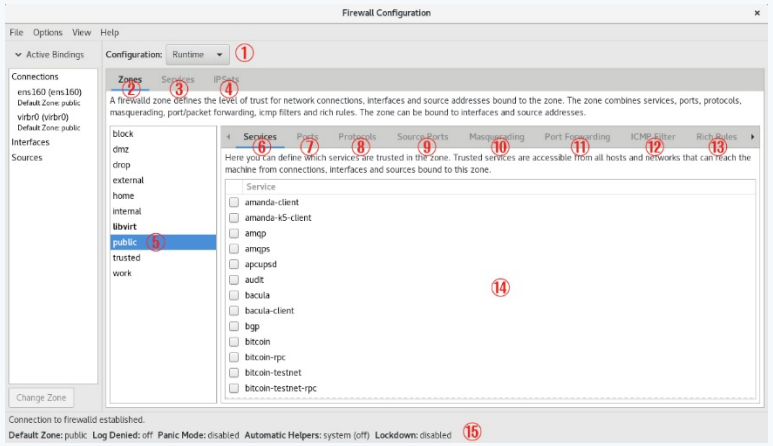
最后

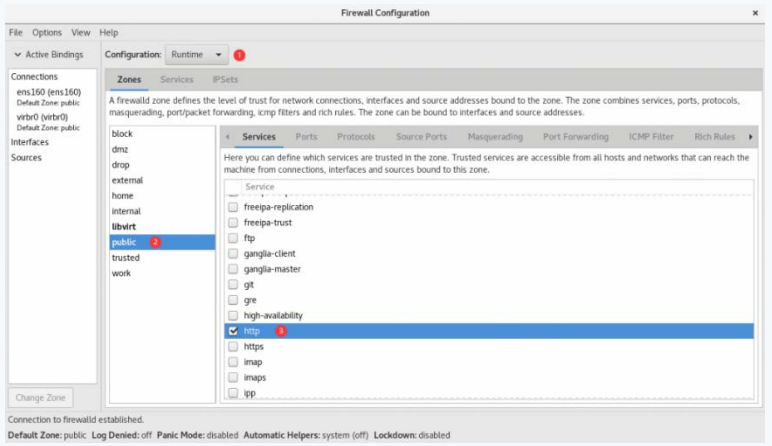
使用Vim文本编辑器创建软件仓库的配置文件。与之前版本的系统不同，RHEL 8需要配置两个软件仓库（即[BaseOS]与[AppStream]），且缺一不可。

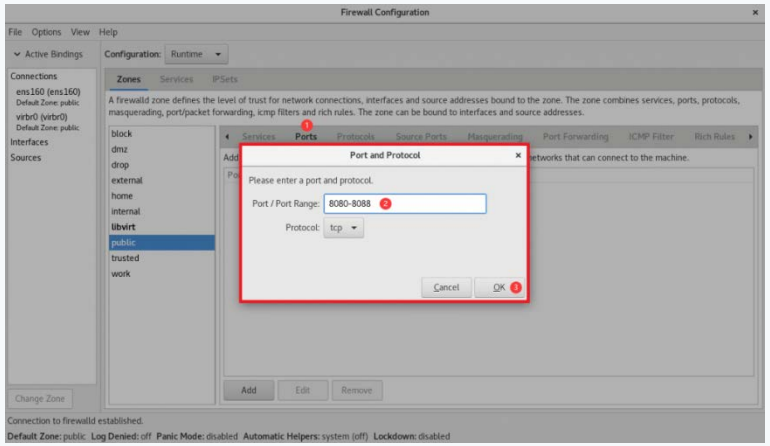
firewall-config工具的具体功能

- ✓ 1：选择运行时（Runtime）或永久（Permanent）模式的配置。
- ✓ 2：可选的策略集合区域列表。
- ✓ 3：常用的系统服务列表。
- ✓ 4：主机地址的黑白名单。
- ✓ 5：当前正在使用的区域。
- ✓ 6：管理当前被选中区域中的服务。
- ✓ 7：管理当前被选中区域中的端口。
- ✓ 8：设置允许被访问的协议。
- ✓ 9：设置允许被访问的端口。
- ✓ 10：开启或关闭SNAT（源网络地址转换）技术。
- ✓ 11：设置端口转发策略。
- ✓ 12：控制请求icmp服务的流量。
- ✓ 13：管理防火墙的富规则。
- ✓ 14：被选中区域的服务，若勾选了相应服务前面的复选框，则表示允许与之相关的流量。
- ✓ 15：firewall-config工具的运行状态。

动手实践环节

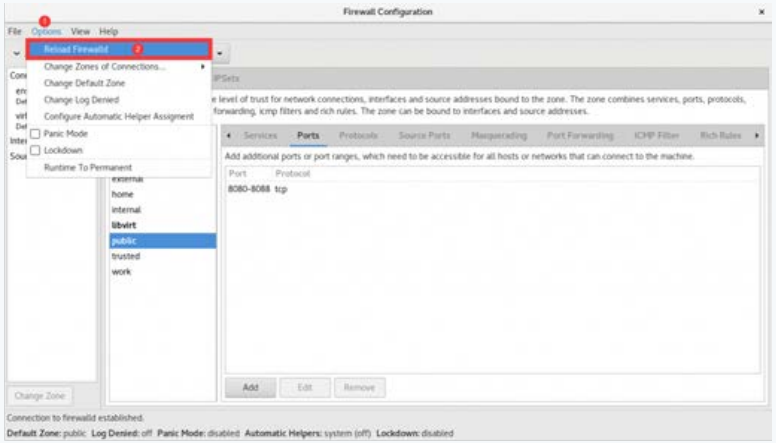


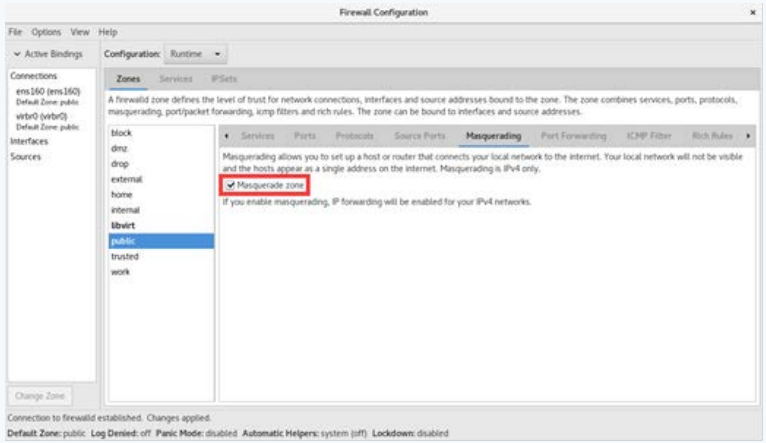


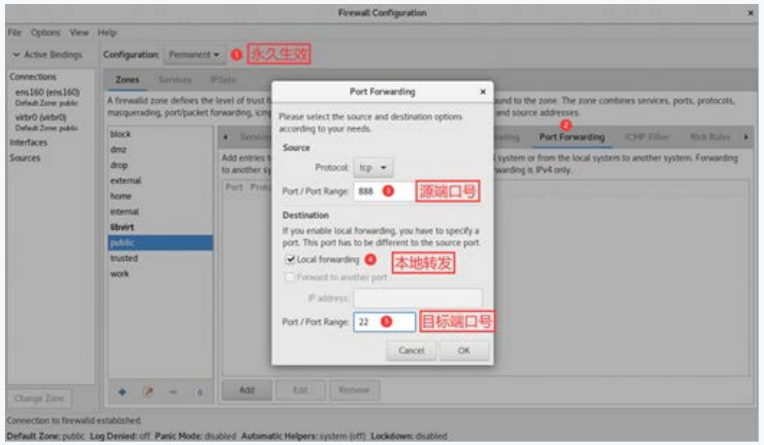


firewall-config的图形界面 → 允许放行请求http服务的流量 → 放行访问8080~8088端口的流量

动手实践环节





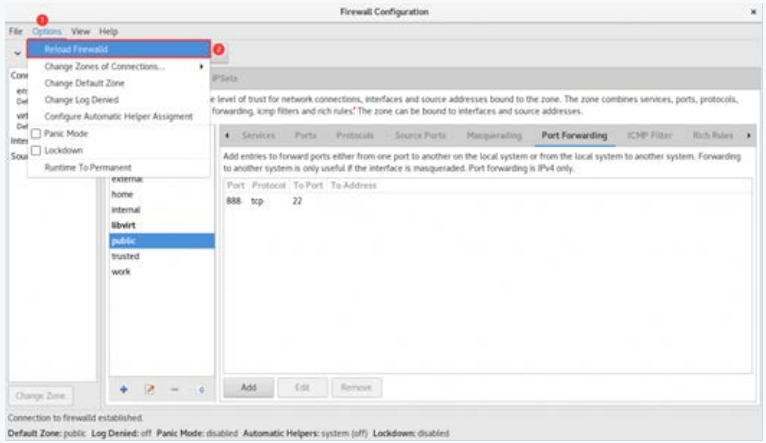


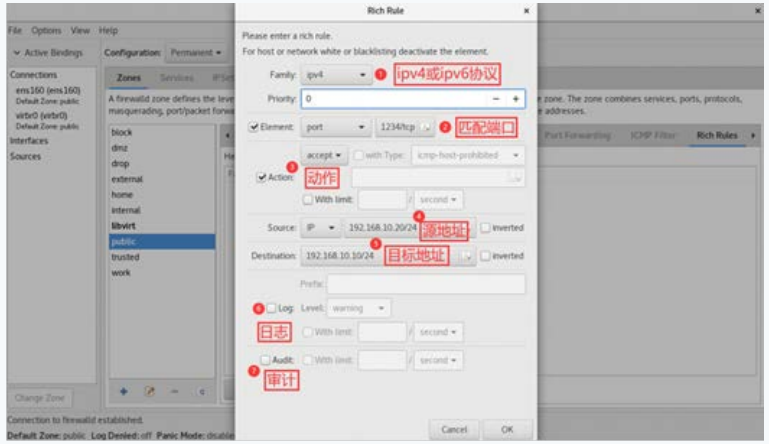
让配置的防火墙策略规则立即生效

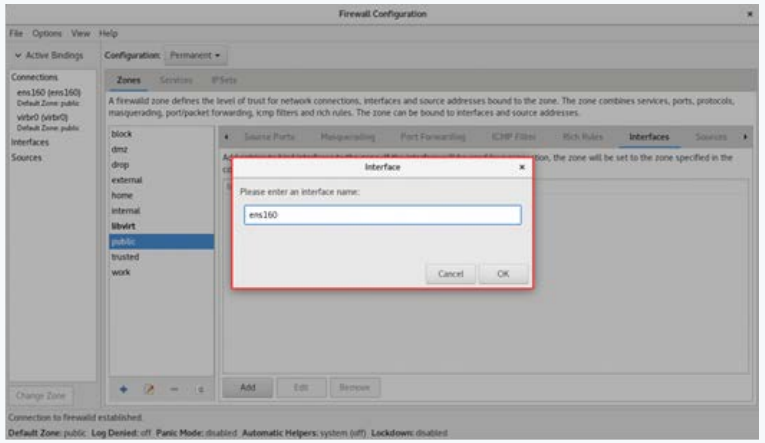
开启防火墙的SNAT技术

配置本地的端口转发

动手实践环节





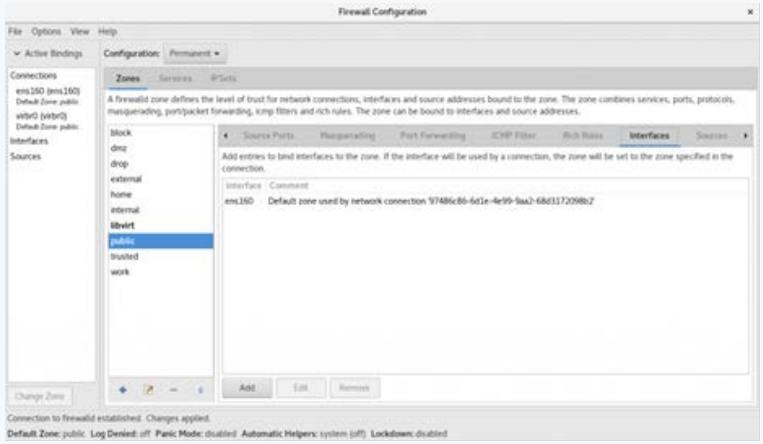


让防火墙策略规则立即生效

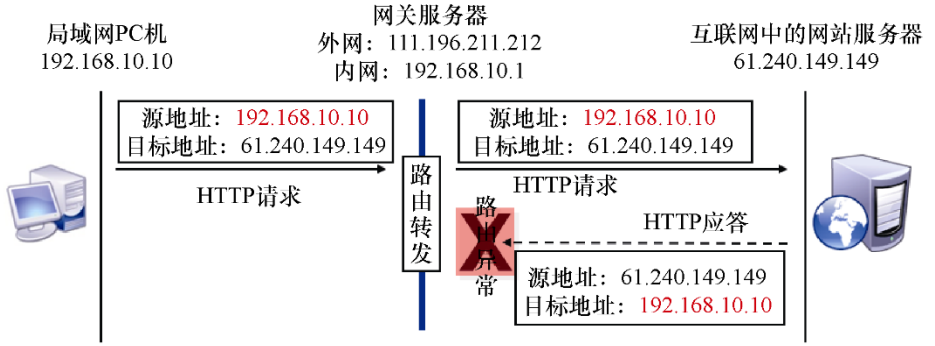
配置防火墙富规则策略

把网卡与防火墙策略区域进行绑定

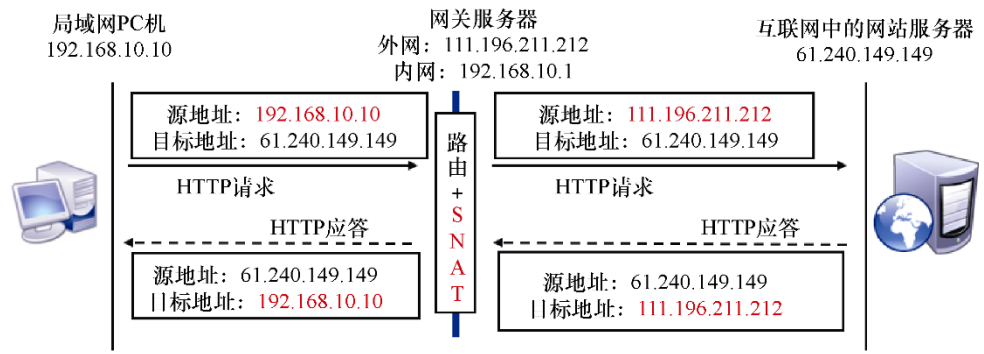
动手实践环节



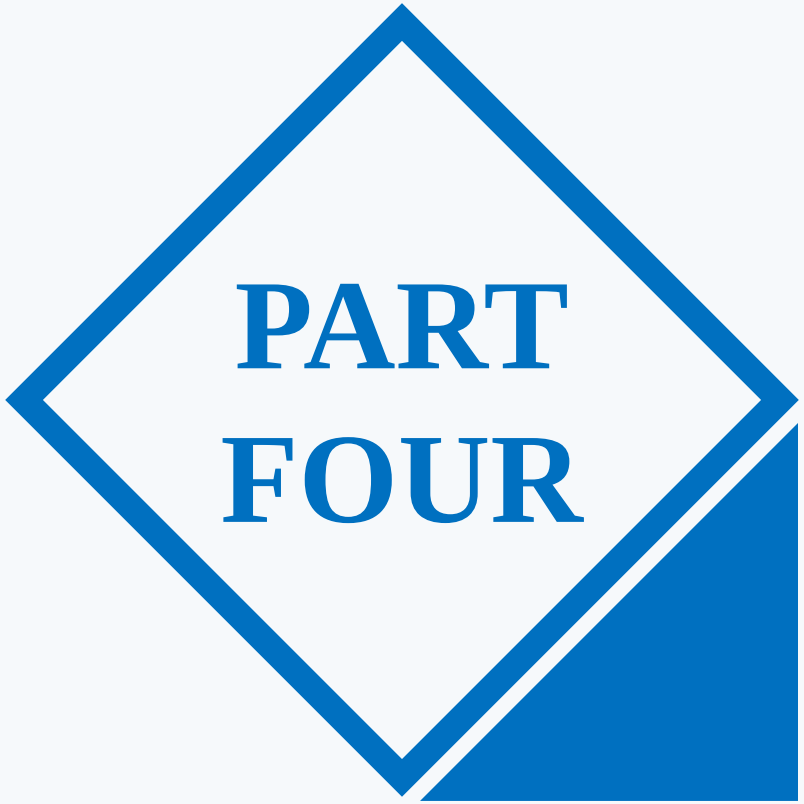
网卡与策略区域绑定完成



没有使用SNAT技术的网络



使用SNAT技术处理过的网络



服务的访问控制列表

Access Control List For Services

TCP Wrapper服务的控制列表文件中常用的参数

客户端类型	示例	满足示例的客户端列表
单一主机	192.168.10.10	IP地址为192.168.10.10的主机
指定网段	192.168.10.	IP段为192.168.10.0/24的主机
指定网段	192.168.10.0/255.255.255.0	IP段为192.168.10.0/24的主机
指定DNS后缀	.linuxprobe.com	所有DNS后缀为.linuxprobe.com的主机
指定主机名称	www.linuxprobe.com	主机名称为www.linuxprobe.com的主机
指定所有客户端	ALL	所有主机全部包括在内

在配置TCP Wrapper服务时需要遵循两个原则

1. 编写拒绝策略规则时，填写的是服务名称，而非协议名称；

2. 建议先编写拒绝策略规则，再编写允许策略规则，以便直观地看到相应的效果。

Cockpit驾驶舱管理工具

Cockpit Cockpit Management Tool

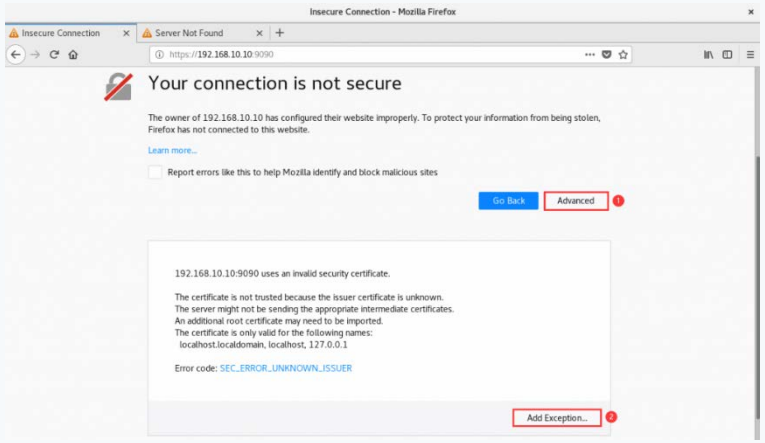
Cockpit驾驶舱管理工具

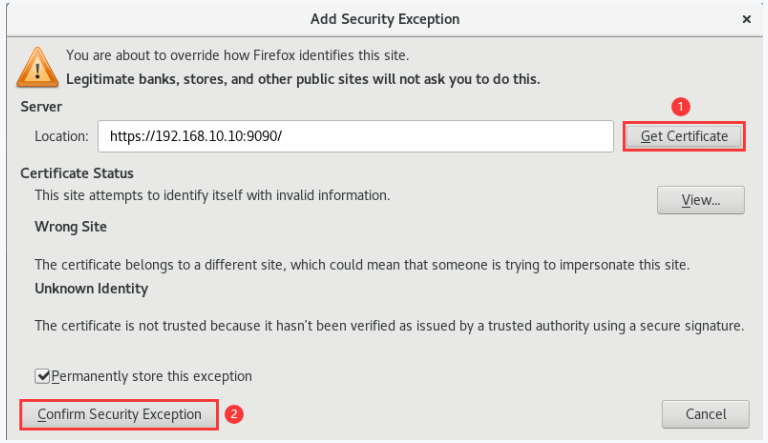
概念

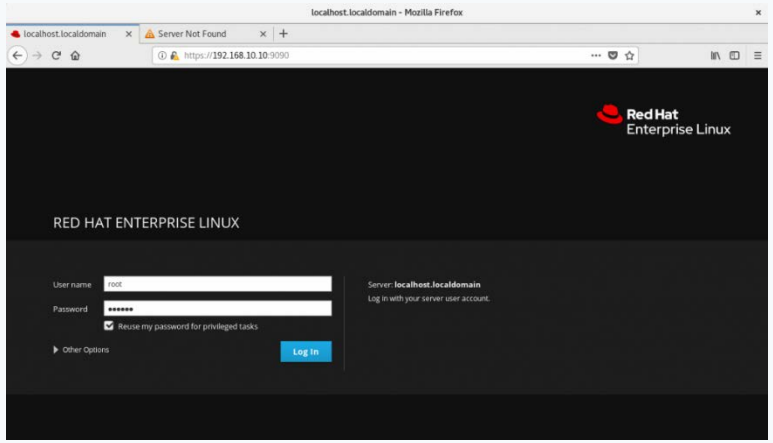
Cockpit是一个英文单词，即“（飞机、船或赛车的）驾驶舱、驾驶座”，它用名字传达出了功能丰富的特性。Cockpit是一个基于Web的图形化服务管理工具，即便是新手也可以轻松上手。它天然具备很好的跨平台性，因此被广泛应用于服务器、容器、虚拟机等多种管理场景。最后，红帽公司对Cockpit也十分看重，直接将它默认安装到了RHEL 8系统中，由此衍生的CentOS和Fedora也都标配有Cockpit。

驾驶舱示意图

Cockpit驾驶舱管理工具

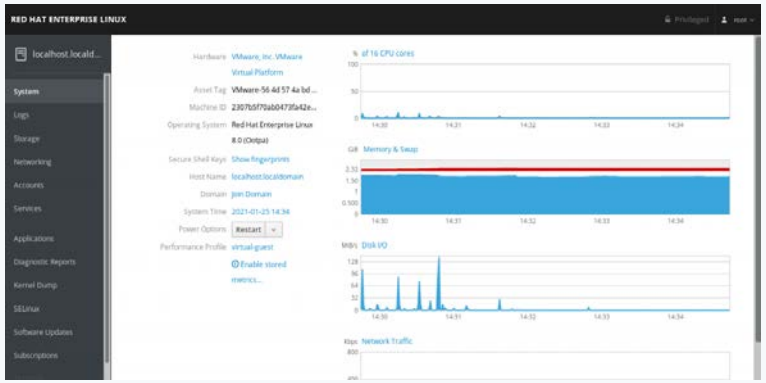


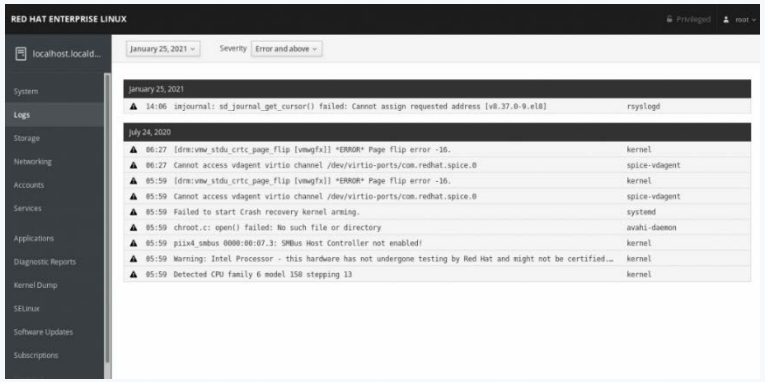


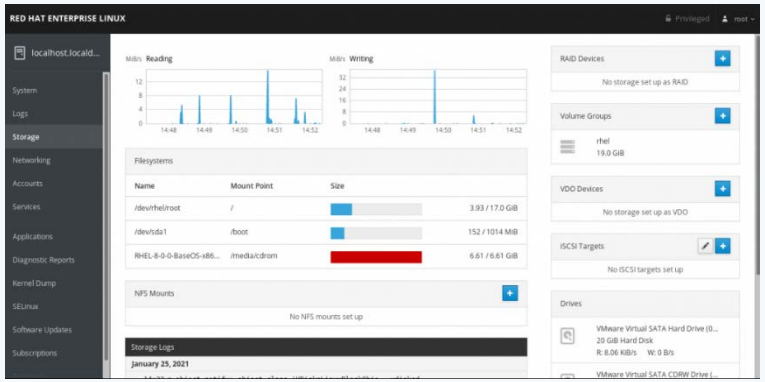


添加额外允许的证书 → 确认信任本地证书 → 输入登录账号与系统密码

Cockpit驾驶舱管理工具

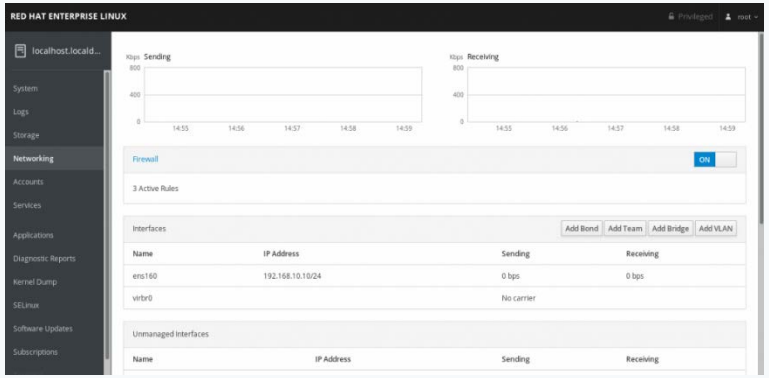


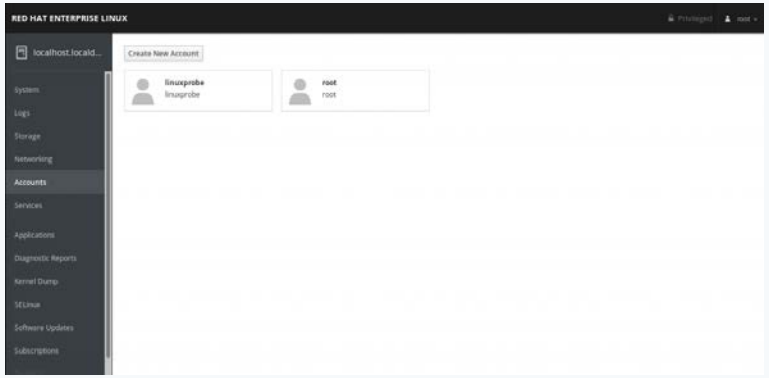


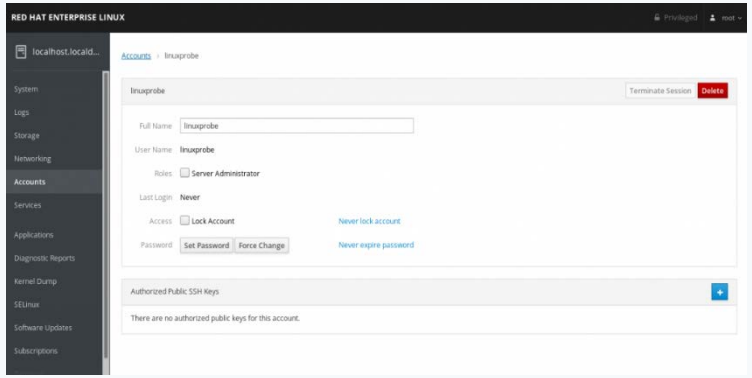


System界面 → Logs界面 → Storage界面

Cockpit驾驶舱管理工具

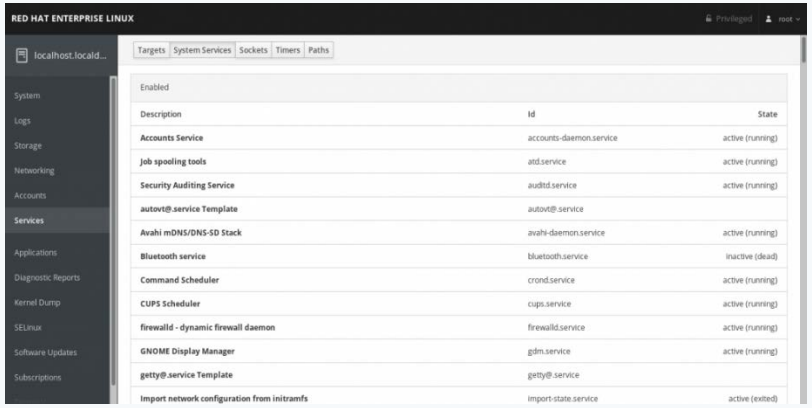


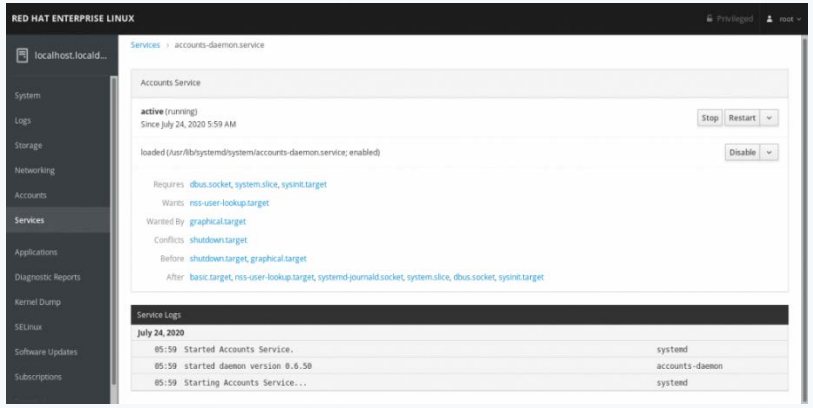


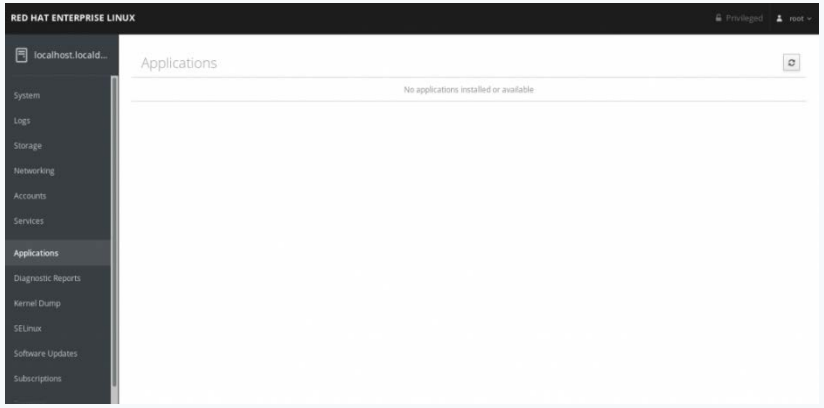


Networking界面 → Accounts界面 → 用户管理界面

Cockpit驾驶舱管理工具

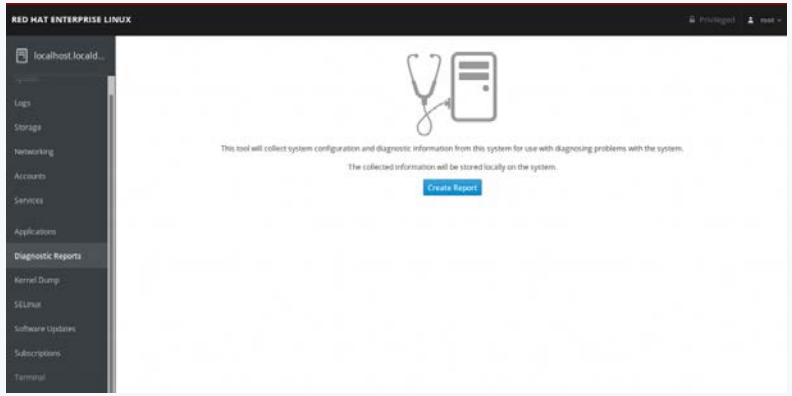


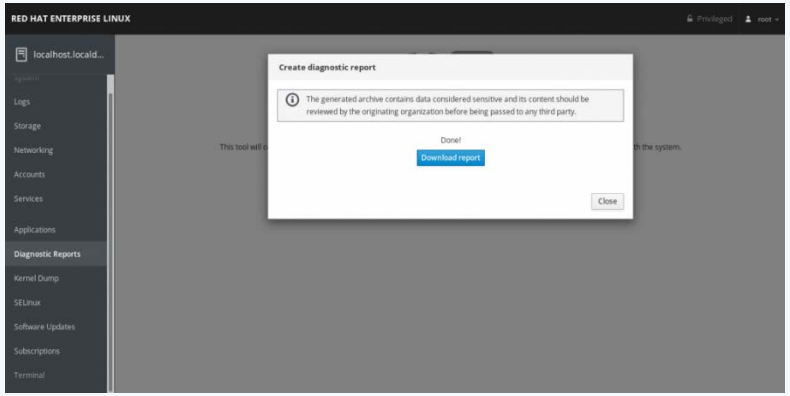


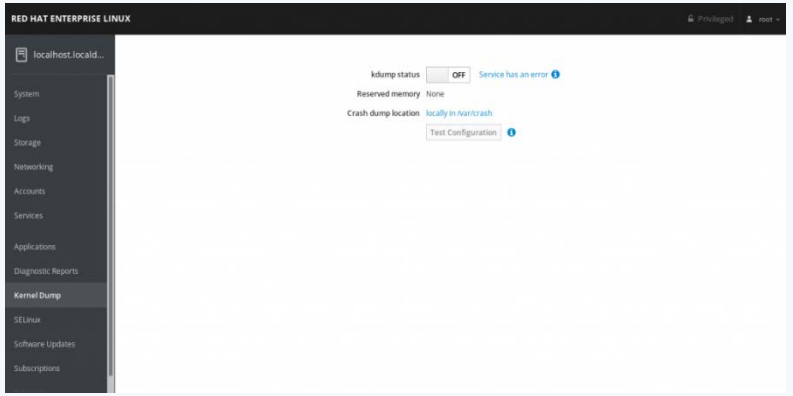


Services界面 → 服务管理界面 → Applications界面

Cockpit驾驶舱管理工具

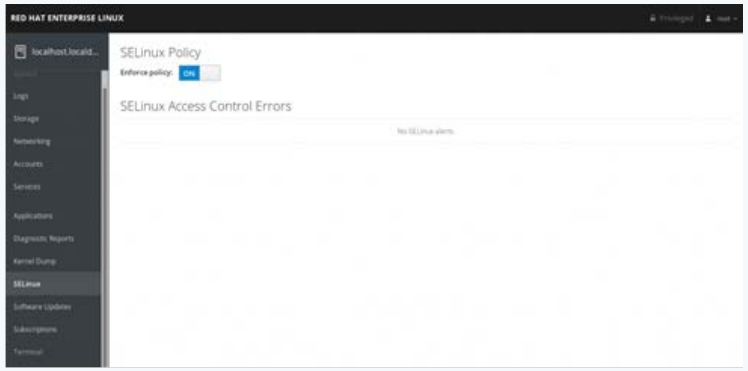


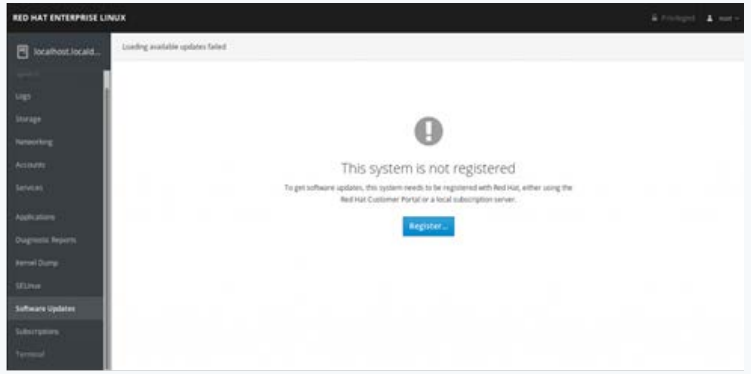


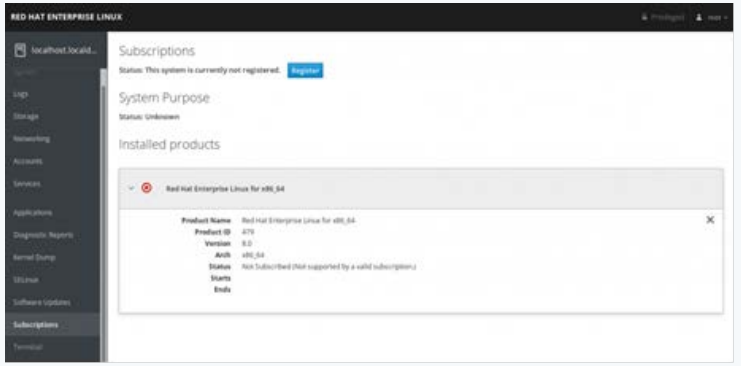


Diagnostic Report界面 → 报告生成完毕 → Kernel Dump界面

Cockpit驾驶舱管理工具







SElinux界面 → Software Updates界面 → Subscriptions界面

Cockpit驾驶舱管理工具

Terminal界面

复习题

✓ **1．在RHEL 8系统中，iptables是否已经被firewalld服务彻底取代?**

答：没有，iptables和firewalld服务均可用于RHEL 8系统。

✓ **2．请简述防火墙策略规则中DROP和REJECT的不同之处。**

答：DROP的动作是丢包，不响应；REJECT是拒绝请求，同时向发送方回送拒绝信息。

✓ **3．如何把iptables服务的INPUT规则链默认策略设置为DROP?**

答：执行命令iptables -P INPUT DROP即可。

✓ **4．怎样编写一条防火墙策略规则，使得iptables服务可以禁止源自192.168.10.0/24网段的流量访问本机的sshd服务（22端口）？**

答：执行命令iptables -I INPUT -s 192.168.10.0/24 -p tcp --dport 22 -j REJECT即可。

✓ **5．请简述firewalld中区域的作用。**

答：可以依据不同的工作场景来调用不同的firewalld区域，实现大量防火墙策略规则的快速切换。

复习题

✓ **6．如何在firewalld中把默认的区域设置为dmz?**

答：执行命令firewall-cmd --set-default-zone=dmz即可。

✓ **7．如何让firewalld中以永久（Permanent）模式配置的防火墙策略规则立即生效?**

答：执行命令firewall-cmd --reload。

✓ **8．使用SNAT技术的目的是什么?**

答：SNAT是一种为了解决IP地址匮乏而设计的技术，它可以使得多个内网中的用户通过同一个外网IP接入Internet。

✓ **9． TCP Wrapper服务分别有允许策略配置文件和拒绝策略配置文件，请问匹配顺序是怎么样的?**

答：TCP Wrapper会先依次匹配允许策略配置文件，然后再依次匹配拒绝策略配置文件；如果都没有匹配到，则默认放行流量。

✓ **10．默认情况下如何使用Cockpit服务?**

答：Cockpit服务默认占用9090端口号，可直接用浏览器访问Cockpit的Web界面。

祝同学们学习顺利，爱上Linux系统。