

firewalld 简介

内容

了解 firewalld 这款用于保障 Linux 服务器和服务安全的重要工具。它是许多现代 Linux 发行套件中默认的主要网络防御机制。其基于区域的直观管理方式和动态配置功能可在不中断服务的前提下实现对网络流量的精确控制。

原因

firewalld 至关重要，因为它通过将复杂的防火墙规则抽象为直观的区域和服务，为 Linux 系统提供了现代化、动态且易用的网络安全管理方式。

工作量

读完本文最多需要 30 分钟。

目标

有效管理并提升 Linux 系统的安全性。

要求

- 拥有 `sudo` 或 `root` 权限，因为 `firewalld` 命令（尤其是对防火墙规则进行永久性更改的命令）需要高级权限。
- 系统中需安装 `firewalld`，它是许多现代 Linux 发行套件的默认防火墙，如果系统中未预装，您需要安装 `firewalld` 软件包。
- 基本了解 Linux 终端：这是操作的基础。

出版日期：2025 年 12 月 11 日

目录

- 1 关于 `firewalld` 3
- 2 管理防火墙规则和区域 6
- 3 常用 `firewalld` 命令 11
- 4 `firewalld` 查错 14
- 5 更多信息 18
- 6 法律声明 19
- A GNU Free Documentation License 19

1 关于 firewalld

firewalld 是一款动态防火墙管理服务，为 Linux 系统提供灵活高效的网络流量控制方式。它可在不中断现有连接的情况下修改配置。使用 firewalld 的优势如下：

- **动态配置**：即时应用更改，而不中断现有连接。
- **易用界面**：通过区域和服务简化复杂的防火墙规则。
- **抽象化**：普通场景下无需直接操作 nftables 规则。
- **持久化配置**：轻松管理系统重引导后仍生效的规则。
- **持久化配置**：firewalld 默认采用 deny-all 策略，除非明确允许，否则会阻止所有传入流量。

1.1 firewalld 区域

防火墙区域是一组预定义规则，用于指定特定网络接口或来源 IP 地址的传入和传出网络流量处理方式。每个区域代表与其关联的网络的不同信任级别。可根据网络连接的来源应用不同的安全策略。

区域类似于安全配置文件。例如，对于公共 Wi-Fi 连接和安全的家庭网络，您可能需要应用不同的防火墙规则。firewalld 区域允许您定义并相应应用这些不同的规则集。一个网络连接仅受一个 firewalld 区域的规则约束，而一个 firewalld 区域可关联多个网络接口或来源 IP 地址。

预定义区域存储在 /usr/lib/firewalld/zones/ 目录中。例如：

```
> /usr/lib/firewalld/zones ls
block.xml  dmz.xml  docker.xml  drop.xml  external.xml  home.xml  internal.xml
nm-shared.xml  public.xml  trusted.xml  work.xml
```

以下是部分预定义区域的默认设置：

drop

- **信任级别：**完全不可信。
- **行为：**所有传入网络数据包均被丢弃且不回复。仅允许系统主动发起的传出连接。这种“隐身”模式可使系统在外部攻击者眼中呈现不存在的状态。
- **适用场景：**用于实现最高级别的隐身性和安全性，完全忽略不必要的流量。适合作为严格的服务器默认配置，此类服务器不应接受任何传入连接。

block

- **信任级别：**极低。
- **行为：**所有传入网络连接都会被拒绝，对 IPv4 发送 `icmp-host-prohibited` 消息，对 IPv6 发送 `icmp6-adm-prohibited` 消息，以此告知发送方其连接已被明确拒绝。仅允许系统主动发起的传出连接。
- **适用场景：**希望明确告知发送方其连接尝试被阻止时使用。

public

- **信任级别：**不可信或公共。
- **行为：**代表公共、不可信的网络，在此网络中您无法信任其他系统。默认仅允许部分传入连接，例如 SSH、DHCPv6 客户端等。
- **适用场景：**通常作为直接连接互联网的接口（如路由器的 WAN 接口）的默认区域，也适用于连接到您无法控制其他设备的网络的场景。

external

- **信任级别：**具有伪装功能的外部网络。
- **行为：**适用于防火墙作为网关或路由器时的外部网络。默认通常启用 NAT 伪装功能。仅允许部分传入连接，前提是您无法信任该网络中的其他系统。
- **适用场景：**当 Linux 计算机作为路由器，将内部专用网络连接到公共互联网时使用。将外部接口置于此区域可隐藏内部网络拓扑，同时允许内部客户端访问互联网等外部资源。

dmz (Demilitarized Zone)

- **信任级别：**有限公共访问权限。
- **行为：**适用于隔离区中可公开访问但对内部网络的访问受限的系统。仅允许部分传入连接。默认通常包括 SSH 及您对外开放的其他服务。
- **适用场景：**适合 Web 服务器、邮件服务器、DNS 服务器等面向公众的服务器。这些服务器有意在互联网中公开，但与内部更可信的网络隔离。当您想要托管需要能够访问互联网的服务，同时希望最大限度地降低核心内部基础架构风险时非常有用。

work

- **信任级别：**基本可信（工作环境）。
- **行为：**在工作环境中，您通常信任网络中的其他计算机。允许工作环境中常见的部分传入连接，例如 SSH、DHCPv6 客户端等。
- **适用场景：**适合办公网络和企业 LAN 中的系统。

home

- **信任级别：**基本可信（家庭环境）。
- **行为：**在家庭环境中，您通常信任网络中的其他系统。相比 public 或 external 区域，此区域允许更多服务，除 SSH、DHCPv6 客户端外，通常还包括文件共享、媒体服务器、打印机等常见家庭网络服务。
- **适用场景：**最适合家庭网络和小型家庭办公环境。

trusted

- **信任级别：**最高。
- **行为：**接受所有网络连接，不进行过滤。对分配到此区域的连接不实施防火墙功能。
- **适用场景：**保留给高度可信的连接。

1.2 firewalld 策略和规则

与传统区域相比，`firewalld` 策略提供更高级、更灵活的网络流量管理方式。您可以定义丰富的规则，指定流量的来源、目的地、服务、端口以及允许、拒绝、丢弃等操作。这些策略适用于设置复杂路由、端口转发，或在单台主机内创建隔离的网段。

`firewalld` 策略借助区域定义规则集。规则以有状态方式单向应用 - 即您只需定义一个方向的流量流向，`firewalld` 会自动允许返回路径的流量。这些策略将进站区域（流量进入的区域）与出站区域（流量离开的区域）关联，以此定义策略规则适用的特定路径和方向。例如，可通过以下方式查看策略：

```
> /usr/lib/firewalld/policies ls
allow-host-ipv6.xml
```

防火墙规则可精确控制网络流量，通过允许或阻止流量保护系统免受安全威胁的侵扰。防火墙规则根据来源 IP 地址、目标 IP 地址、端口、网络接口等多种属性定义特定条件。`firewalld` 会将防火墙规则划分到区域和策略中。`firewalld` 中的每个区域都有一组独特的规则，用于指定其关联网络接口的流量权限。

1.3 服务和端口

当存在预定义服务时，建议优先使用服务。例如，无需记住 HTTP 使用 TCP 80 端口，只需添加 `http` 服务即可。这种方式更不易出错，且更便于管理。当服务无预定义配置，或服务使用自定义端口时，可直接使用端口。通过以下命令可查看默认区域的活跃服务和端口：

```
> sudo firewall-cmd --list-services
```

```
> sudo firewall-cmd --list-ports
```

2 管理防火墙规则和区域

您可以通过图形 Web 界面 Cockpit 或命令行实用程序 `firewall-cmd` 配置 `firewalld` 区域及其规则。

2.1 使用 `firewalld-cmd` 实用程序管理防火墙规则和区域

可通过命令行界面管理 `firewalld` 区域。

2.1.1 添加 `firewalld` 区域

要添加新 `firewalld` 区域，请执行以下步骤：

1. 创建新区域，例如：

```
> sudo firewall-cmd --permanent --new-zone=test
```

2. 设置区域的信任级别以定义默认行为：

```
> sudo firewall-cmd --permanent --zone=example --set-target=trusted
```

3. 重新加载 `firewalld` 服务以应用新配置：

```
> sudo firewall-cmd --reload
```

2.1.2 向区域添加服务

要向区域添加服务，请执行以下步骤：

1. 列出所有服务，确认您需要的服务是否已预定义：

```
> sudo firewall-cmd --get-services
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client
amanda-k5-client amqp amqps anno-1602
anno-1800 apcupsd audit ausweisapp2 bacula bacula-client bareos-
director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc
bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter
ceph-mon cfengine checkmk-agent civilization-iv civilization-v cockpit
collectd condor-collector cratedb ctdb dds dds-multicast dds-unicast
dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quick dns-over-tls docker-
registry docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server
```

```
factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap freeipa-ldaps
freeipa-replication freeipa-trust ftp galera
    ganglia-client ganglia-master git gpsd grafana gre http http3 https
ident imap imaps ipfs ipp ipp-client ipsec irc ircs
    [...]
```

2. 可临时为运行时会话添加服务，也可永久添加服务，例如：

```
> sudo firewall-cmd --zone=public --add-service=http
```

```
> sudo firewall-cmd --zone=public --permanent --add-service=http
```

`--permanent` 标志可确保无论系统重引导多少次，更改都仍然生效。

3. 重新加载 `firewalld` 服务以应用新配置：

```
> sudo firewall-cmd --reload
```

4. 查看结果：

```
> sudo firewall-cmd --zone=public --list-services
```

2.1.3 向区域添加端口

如果应用程序无预定义服务，可开放特定端口或端口范围。

1. 可临时为运行时会话添加端口，也可永久添加端口，例如：

```
> sudo firewall-cmd --zone=public --add-port=8080/tcp
```

```
> sudo firewall-cmd --zone=public --permanent --add-port=8080/tcp
```

`--permanent` 标志可确保无论系统重引导多少次，更改都仍然生效。

2. 重新加载 `firewalld` 服务以应用新配置：

```
> sudo firewall-cmd --reload
```

3. 查看结果：

```
> sudo firewall-cmd --zone=public --list-ports
```

2.1.4 删除 firewalld 区域

要删除某个区域，请执行以下操作：

1. 确认该区域不是默认区域且未被使用：

```
> sudo firewall-cmd --get-default-zone
```

如果该区域已被使用或为默认区域，需要先将其他区域设置为默认区域，例如：

```
> sudo firewall-cmd --set-default-zone=NEW_DEFAULT_ZONE
```

2. 检查是否有网络接口绑定到该区域：

```
> sudo firewall-cmd --zone=ZONE_TO_BE_DELETED --list-all
```

3. 输出结果中的 `interfaces` 字段会列出所有绑定的接口。需要将这些接口重新分配到其他区域，例如：

```
> sudo firewall-cmd --zone=public --permanent --change-interface=INTERFACE_NAME
```

4. 删除区域：

```
> sudo firewall-cmd --permanent --delete-zone=ZONE_TO_BE_DELETED
```

5. 重新加载 `firewalld` 服务以应用新配置：

```
> sudo firewall-cmd --reload
```

2.2 使用 Cockpit 管理防火墙规则和区域

Cockpit 允许您创建新区域或更新现有区域。在防火墙设置中，可以向区域添加服务或允许访问端口。



注意：Cockpit 服务是必需的

请不要从默认防火墙区域中去除 Cockpit 服务，因为这可能会阻止 Cockpit 服务，导致您从服务器断开连接。

2.2.1 添加防火墙区域

public 区域是默认的防火墙区域。要添加新区域，请执行以下步骤：

过程 1：添加新的防火墙区域

1. 导航到网络页面。
2. 单击编辑规则和区域。
3. 单击添加区域。
4. 选择信任级别。网络连接的每个信任级别都有一组预定义的包含服务（Cockpit 服务包含在所有信任级别中）。
5. 定义区域内允许的地址。选择以下值之一：
 - 整个子网，表示允许子网中的所有地址。
 - 范围 - 一系列包含路由前缀的 IP 地址（用逗号分隔），例如 192.0.2.0/24, 2001:db8::/32。
6. 单击添加区域继续。

2.2.2 将允许的服务和端口添加到区域

可如下所述将服务添加到现有的防火墙区域：

过程 2：将服务添加到防火墙区域

1. 导航到网络页面。
2. 单击编辑规则和区域。
3. 单击添加服务。
4. 要添加服务，请选中服务，然后从列表中选择所需服务。

5. 要允许自定义端口，请选中自定义端口并指定 UDP 和/或 TCP 端口值。可为此端口指派标识符。
6. 要确认更改，请相应地单击添加服务或添加端口。

3 常用 firewalld 命令

firewall-cmd 命令行工具用于配置和管理 firewalld 守护程序。这是一款功能强大的动态工具，支持创建、修改和删除防火墙规则，且执行这些操作时无需重启整个服务，因而可避免活跃的网络连接中断。

以下是部分常用 **firewall-cmd** 命令示例：

- 检查 firewalld 运行状态。输出结果为 `running`、`not running` 或 `RUNNING_BUT_FAILED`。例如：

```
> sudo firewall-cmd --state
running
```

- 列出所有可用区域，例如：

```
> sudo firewall-cmd --get-zones
block dmz docker drop external home internal nm-shared public trusted work
```

- 查看默认区域，例如：

```
> sudo firewall-cmd --get-default-zone
public
```

- 查看活跃区域及分配的接口，例如：

```
> sudo firewall-cmd --get-active-zones
docker
interfaces: docker0
public (default)
interfaces: lo enp1s0
```

- 查看默认区域的所有规则，例如：

```
> sudo firewall-cmd --list-all
public (default, active)
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- 查看特定区域的所有规则，例如：

```
> sudo firewall-cmd --zone=public --list-all
public (default, active)
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces: enp1s0 lo
sources:
services: cockpit dhcpv6-client ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
```

```
rich rules:  
rule family="ipv4" source address="192.168.1.100" service name="ssh" accept
```

- 列出所有可用的预定义服务，例如：

```
> sudo firewall-cmd --get-services  
0-AD RH-Satellite-6 RH-Satellite-6-capsule afp alvr amanda-client amanda-  
k5-client amqp amqps anno-1602 anno-1800  
apcupsd audit ausweisapp2 bacula bacula-client bareos-director bareos-  
filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc  
bitcoin-testnet bitcoin-testnet-rpc bittorrent-lsd ceph ceph-exporter  
ceph-mon cfengine checkmk-agent civilization-iv civilization-v  
cockpit collectd condor-collector cratedb ctdb dds dds-multicast dds-  
unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-quic dns-over-tls  
docker-registry docker-swarm dropbox-lansync elasticsearch etcd-client  
etcd-server factorio finger foreman foreman-proxy freeipa-4 freeipa-ldap  
freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client  
ganglia-master git gpsd grafana gre http http3 https ident imap imaps  
ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin  
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-  
apiserver  
kube-control-plane kube-control-plane-secure kube-controller-manager  
kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-  
scheduler-secure  
[...]
```

- 列出默认区域中当前允许的服务，例如：

```
> sudo firewall-cmd --list-services  
cockpit dhcpv6-client ssh
```

- 向默认区域永久添加服务，例如：

```
> sudo firewall-cmd --permanent --add-service=http  
success
```

- 永久去除服务，例如：

```
> sudo firewall-cmd --permanent --remove-service=http
```

```
success
```

- 列出默认区域中当前开放的端口，例如：

```
> sudo firewall-cmd --list-ports
22/tcp
```

- 临时开放特定 TCP 端口，例如：

```
> sudo firewall-cmd --add-port=8080/tcp
success
```

- 永久去除开放的端口，例如：

```
> sudo firewall-cmd --permanent --remove-port=8080/tcp
success
```

- 临时将接口添加到特定区域，例如：

```
> sudo firewall-cmd --zone=trusted --add-interface=eth1
success
```

4 firewalld 查错

`firewalld` 查错涉及检查服务状态、验证规则、重启或重新加载服务。如果遇到问
题，可启用调试模式、查看日志，并根据需要调整防火墙规则。

4.1 检查 `firewalld` 状态

- 使用 `systemctl status` 命令查看状态，例如：

```
> sudo systemctl status firewalld.service
● firewalld.service - firewalld - dynamic firewall daemon
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; preset:
enabled)
```

```
Active: active (running) since Thu 2025-07-17 09:47:36 CEST; 5min ago
Invocation: a7ea482f16d2431fa92d6204c297ebd9
Docs: man:firewalld(1)
Main PID: 921 (firewalld)
Tasks: 2
CPU: 262ms
CGroup: /system.slice/firewalld.service
        └─921 /usr/bin/python3.13 /usr/sbin/firewalld --nofork --nopid
```

- 使用 **firewall-cmd --state** 命令可快速查看状态，输出结果为 running、not running 或 RUNNING_BUT_FAILED。例如：

```
> sudo firewall-cmd --state
running
```

- 如果 firewalld 未运行，则使用 **systemctl start firewalld** 命令将其启动。

```
> sudo systemctl start firewalld
```

- 如果 firewalld 服务被屏蔽，需先解除屏蔽，然后再启用并启动服务，例如：

```
> sudo systemctl unmask --now firewalld
```

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 检查 firewalld 规则

- **firewall-cmd --list-all-zones** 命令可显示所有区域及其规则，例如：

```
> sudo firewall-cmd --list-all-zones
block
  target: %%REJECT%%
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
```

```
interfaces:
sources:
services:
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:

dmz
target: default
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
interfaces:
sources:
services: ssh
ports:
protocols:
forward: yes
masquerade: no
forward-ports:
source-ports:
icmp-blocks:
rich rules:

docker (active)
target: ACCEPT
ingress-priority: 0
egress-priority: 0
icmp-block-inversion: no
[...]
```

- **`firewall-cmd --list-ports`** 命令可查看开放的端口，例如：

```
> sudo firewall-cmd --list-ports
```

- **firewall-cmd --zone=YOUR_ZONE --list-all.** 命令可查看特定区域的端口，例如：

```
> sudo firewall-cmd --zone=dmz --list-all
dmz
  target: default
  ingress-priority: 0
  egress-priority: 0
  icmp-block-inversion: no
  interfaces:
  sources:
  services: ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

4.3 调试 firewalld

- 在 `/etc/sysconfig/firewalld` 中，通过向 `FIREWALLD_ARGS` 添加 `--debug=[level]` 启用调试模式，例如：

```
> sudo vi /etc/sysconfig/firewalld
# firewalld command line args
# possible values: --debug
FIREWALLD_ARGS=--debug=[level]
```

- 通过 `--debug` 选项启动 `firewalld`，例如：

```
> sudo firewalld --nofork --debug
2025-07-23 11:10:05 DEBUG1: start()
```

```
2025-07-23 11:10:05 DEBUG1: Loading firewalld config file '/etc/firewalld/
firewalld.conf'
2025-07-23 11:10:05 DEBUG1: CleanupOnExit is set to 'True'
2025-07-23 11:10:05 DEBUG1: CleanupModulesOnExit is set to 'False'
2025-07-23 11:10:05 DEBUG1: IPv6 rpfilter is enabled
2025-07-23 11:10:05 DEBUG1: LogDenied is set to 'off'
2025-07-23 11:10:05 DEBUG1: FirewallBackend is set to 'nftables'
2025-07-23 11:10:05 DEBUG1: FlushAllOnReload is set to 'False'
2025-07-23 11:10:05 DEBUG1: RFC3964_IPv4 is set to 'True'
2025-07-23 11:10:05 DEBUG1: NftablesFlowtable is set to 'off'
2025-07-23 11:10:05 DEBUG1: NftablesCounters is set to 'False'
2025-07-23 11:10:05 DEBUG1: Loading lockdown whitelist
2025-07-23 11:10:05 ipset not usable, disabling ipset usage in firewall.
  Other set backends (nftables) remain usable.
2025-07-23 11:10:05 iptables-restore and iptables are missing, IPv4 direct
  rules won't be usable.
2025-07-23 11:10:05 ip6tables-restore and ip6tables are missing, IPv6
  direct rules won't be usable.
2025-07-23 11:10:05 ebtables-restore and ebtables are missing, eb direct
  rules won't be usable.
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/
icmptypes/address-unreachable.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/
icmptypes/bad-header.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/
icmptypes/beyond-scope.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/
icmptypes/communication-prohibited.xml'
2025-07-23 11:10:05 DEBUG1: Loading icmptype file '/usr/lib/firewalld/
icmptypes/destination-unreachable.xml'
[...]
```

所有日志文件均存储在 [/var/log/firewalld](#) 中。

5 更多信息

有关 [firewalld](#) 的详细信息，请参考以下资源：

- [firewalld 官方资源](https://firewalld.org/documentation/): 包含概念、体系结构、操作指南及所有手册页链接。 (<https://firewalld.org/documentation/>) ↗
- [手册页](https://firewalld.org/documentation/man-pages/firewall-cmd.html): 理解 `firewalld` 命令行交互的核心资源。 (<https://firewalld.org/documentation/man-pages/firewall-cmd.html>) ↗
- [Arch Linux 维基](https://wiki.archlinux.org/title/Firewalld): 内容全面, 包含详细说明和实用示例, 也涵盖 `nftables` 相关内容。 (<https://wiki.archlinux.org/title/Firewalld>) ↗

6 法律声明

版权所有© 2006–2025 SUSE LLC 和撰稿人。保留所有权利。

根据 GNU 自由文档许可证 (GNU Free Documentation License) 版本 1.2 或 (根据您的选择) 版本 1.3 中的条款, 在此授予您复制、分发和/或修改本文档的权限; 本版权声明和许可证附带不可变部分。许可版本 1.2 的副本包含在“GNU Free Documentation License”部分。

有关 SUSE 商标, 请参见 <https://www.suse.com/company/legal/> ↗。所有其他第三方商标分别为相应所有者的财产。商标符号 (®、™ 等) 代表 SUSE 及其关联公司的商标。星号 (*) 代表第三方商标。

本指南力求涵盖所有细节, 但这不能确保本指南准确无误。SUSE LLC 及其关联公司、作者和译者对于可能出现的错误或由此造成的后果皆不承担责任。

A GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondly, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the Document is in part a textbook of

mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

- A.** Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.
- B.** List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.
- C.** State on the Title page the name of the publisher of the Modified Version, as the publisher.
- D.** Preserve all the copyright notices of the Document.
- E.** Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.
- F.** Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.
- G.** Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.
- H.** Include an unaltered copy of this License.
- I.** Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create

one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

- J.** Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.
- K.** For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.
- L.** Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.
- M.** Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.
- N.** Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.
- O.** Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original

English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See <https://www.gnu.org/copyleft/>.

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.  
Permission is granted to copy, distribute and/or modify this document  
under the terms of the GNU Free Documentation License, Version 1.2
```

or any later version published by the Free Software Foundation;
with no Invariant Sections, no Front-Cover Texts, and no Back-Cover Texts.
A copy of the license is included in the section entitled “GNU
Free Documentation License”.

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the
“with...Texts.” line with this:

with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.

If you have Invariant Sections without Cover Texts, or some other combination of the
three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing
these examples in parallel under your choice of free software license, such as the GNU
General Public License, to permit their use in free software.