SUSE

Introduction to firewalld

WHAT?

Learn about firewalld an important tool for securing Linux servers and services. It is the default and primary network defense mechanism on many modern distributions. The intuitive zone-based management and dynamic configuration capabilities allow for precise control over network traffic without service interruption.

WHY?

firewalld is essential because it provides a modern, dynamic and user-friendly way to manage network security on Linux systems by abstracting complex firewall rules into intuitive zones and services.

EFFORT

It takes you up to 30 minutes to read through this article.

GOAL

To effectively manage and enhance the security of a Linux system.

REQUIREMENTS

- `sudo` or `root` privileges, because `firewalld` commands, especially those that make permanent changes to the firewall rules, require elevated privileges.
- `firewalld` is the default firewall on many modern Linux distributions, if it is not preinstalled on your system, you need to install the `firewalld` package.
- A basic understanding of the Linux terminal is essential.

Publication Date: 07 Nov 2025

Contents

1 About firewalld

firewalld is a dynamic firewall management service that provides a flexible and efficient way to control network traffic on Linux systems. It allows modifications without interrupting existing connections. The benefits of using firewalld are:

- *Dynamic configuration:* Apply changes instantly without breaking existing connections.
- *User-friendly interface:* Zones and services simplify complex firewall rules.
- *Abstraction:* There is no need to directly manipulate nftables rules for common scenarios.
- *Persistent configuration:* Easy management of rules that survive reboots.
- *Persistent configuration:* By default, firewalld operates on a deny-all principle by blocking all incoming traffic unless explicitly allowed.

1.1 firewalld zones

A firewall zone is a predefined set of rules that dictate how incoming and outgoing network traffic is handled for a specific network interface or source IP address. Each zone represents a different level of trust for the network it is associated with. You can apply different security policies based on where the network connection originates.

Zones are like security profiles. For example, you would want to apply different firewall rules for a public Wi-Fi connection and your secure home network. firewalld zones allow you to define these distinct sets of rules and apply them accordingly. A network connection is subject to the rules of only one firewalld zone. A firewalld zone can have many network interfaces or source IP addresses.

The /usr/lib/firewalld/zones/ directory stores the predefined zones. For example:

```
>  /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
```

Some of the default settings of the predefined zones are as follows:

`drop`

- *Trust level:* Completely untrusted.
- *Behavior:* All incoming network packets are dropped without any reply. Only outgoing connections initiated from the system are allowed. This provides a “stealth” mode where the system appears nonexistent to external attackers.
- *Use Case:* Used for maximum stealth and security, completely ignoring unwanted traffic. Suitable as a strict default for a server that should never accept incoming connections.

`block`

- *Trust level:* Very low.
- *Behavior:* All incoming network connections are rejected with an `icmp-host-prohibited` message for IPv4 and `cmp6-adm-prohibitedi` for IPv6. This informs the sender that their connection was explicitly rejected. Only outgoing connections initiated from the system are possible.
- *Use Case:* Applied when you want to explicitly signal to senders that their connection attempts are being blocked.

`public`

- *Trust level:* Untrusted or public.
- *Behavior:* Represents public, untrusted networks where you do not trust other systems. Only selected incoming connections are accepted by default for example, SSH, DHCPv6 client, etc.
- *Use Case:* Common default zone for interfaces connected directly to the Internet, such as your router's WAN interface. Also includes being connected to a network where you have no control over other devices.

`external`

- *Trust level:* External with masquerading.
- *Behavior:* Intended for external networks when the firewall acts as a gateway or router. Usually, NAT masquerading is enabled by default.Only selected incoming connections are accepted, under the assumption that you do not trust other systems on this network.
- *Use Case:* Used when your Linux machine acts as a router, connecting an internal private network to the public Internet. The external interface is placed in this zone to hide internal network topology while allowing internal clients to access external resources such as the Internet.

`dmz (Demilitarized Zone)`

- *Trust level:* Limited public access.
- *Behavior:* For systems in a DMZ zone that are publicly accessible but with limited access to the internal network. Only selected incoming connections are accepted. The default usually includes SSH and other services you expose.
- *Use Case:* Suitable for public-facing servers such as Web, mail and DNS servers. These servers are intentionally exposed to the Internet but are isolated from your internal, more trusted networks. Useful when you want to host services that need to be Internet-accessible while minimizing the risk to your core internal infrastructure.

`work`

- *Trust level:* Mostly trusted (work environment).
- *Behavior:* In a work environment, you usually trust other computers on the network. Allows selected incoming connections that are common in a work environment, such as SSH and DHCPv6 client.
- *Use Case:* Suitable for office networks and systems on a corporate LAN.

`home`

- *Trust level:* Mostly trusted (home environment).
- *Behavior:* In a home environment, you mostly trust the other systems on the network. Allows more services than public or external zones, often including common home network services like file sharing, media servers, and printers, along with SSH and DHCPv6 client.
- *Use case:* Best for home networks and small home office setups.

`trusted`

- *Trust level:* Highest.
- *Behavior:* All network connections are accepted without any filtering. Firewalling is not implemented for connections assigned to this zone.
- *Use Case:* Reserved for highly trusted connections.

1.2 `firewalld` policies and rules

`firewalld` policies provide a more advanced and flexible way to manage network traffic compared to traditional zones. They allow you to define rich rules that specify the source and destination of traffic, services, ports and actions such as accept, reject and drop. These policies are useful for setting up complex routing, port forwarding or creating isolated network segments within a single host.

`firewalld` policies leverage zones to define rule sets. They apply rules statefully and in one direction, which means you define traffic flow in one direction, and `firewalld` implicitly permits the return path. These policies link an ingress zone (where traffic enters) with an egress zone (where traffic exits). This defines the specific path and direction a policy's rules apply to. You can view the policies, for example:

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

Firewall rules let you precisely control network traffic, allowing or blocking it to protect your system from security threats. Firewall rules define certain criteria based on various attributes such as, source and destination IP addresses, ports and network interfaces. `firewalld` segregates firewall rules into zones and policies. Each zone in `firewalld` has a unique set of rules that dictates the traffic permissions for its associated network interfaces.

1.3 Services and ports

Services are recommended when a predefined service is available. For example, instead of remembering that HTTP uses TCP port 80, you can simply add the `http` service. This is less error-prone and easier to manage. Use ports when a service is not predefined or when you are using a custom port for a service. You can view the active services and ports for the default zones with the following:

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

2 Managing firewall rules and zones

You can configure `firewalld` zones and their rules with the graphical Web interface Cockpit or the **`firewall-cmd`**utility for command-line control.

2.1 Managing firewall rules and zones using the **`firewalld-cmd`** utility

You can use the CLI interface to manage `firewalld` zones.

2.1.1 Adding `firewalld` zones

To add a new `firewalld` zone:

1. Create a new zone, for example:

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

2. Set the trust level of the zone that defines the default behavior:

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

3. Reload the `firewalld` service to apply the new configuration:

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

2.1.2 Adding a service to a zone

To add a service to a zone:

1. List all services to check if your service is already predefined:

   ```
   > 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
      [...]
```

2. You can add a service either temporarily for the runtime session or permanently, for example:

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

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

   The `--permanent` flag ensures the change persists across all reboots.

3. Reload the `firewalld` service to apply the new configuration:

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

4. Verify the results:

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

2.1.3 Adding a port to a zone

If your application does not have a predefined service, you can open a specific port or a range of ports.

1. You can either add a port temporarily for the runtime session or permanently, for example:

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

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

   The `--permanent`flag ensures the change persists across all reboots.

2. Reload the `firewalld` service to apply the new configuration:

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

3. Verify the results:

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

2.1.4 Deleting `firewalld` zones

To delete a zone:

1. Verify the zone is not the default or in use:

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

   If the zone is in use or default, set a different zone, for example:

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

2. Check if any network interfaces are bound to the zone:

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

3. The `interfaces` field in the output lists all the interfaces. Theses interfaces need to be reassigned to another zone. For example:

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

4. Delete the zone:

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

5. Reload the `firewalld` service to apply the new configuration:

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

2.2 Managing firewall rules and zones with Cockpit

Cockpit enables you to create new zones or update the existing ones. In the firewall settings, you can add services to a zone or allow access to ports.

Note: Cockpit service is mandatory

Do not remove the Cockpit service from the default firewall zone as the Cockpit service may get blocked, and you may get disconnected from the server.

2.2.1 Adding firewall zones

The *public zone* is the default firewall zone. To add a new zone, proceed as follows:

PROCEDURE 1: ADDING NEW FIREWALL ZONES

1. Navigate to the *Networking* page.
2. Click *Edit rules and zones*.
3. Click *Add new zone*.
4. Select *Trust level*. Each trust level of network connections has a predefined set of included services (the Cockpit service is included in all trust levels). The description for each trust level appears in the *Description* section.
5. Define allowed addresses within the zone. Select one of the values:
    - *Entire subnet* to allow all addresses in the subnet.
    - *Range*—a comma-separated list of IP addresses with the routing prefix, for example, 192.0.2.0/24, 2001:db8::/32.
6. Click *Add zone*.

2.2.2 Adding allowed services and ports to a zone

You can add services to an existing firewall zone as described below:

PROCEDURE 2: ADDING SERVICES TO A FIREWALL ZONE

1. Navigate to the *Networking* page.
2. Click *Edit rules and zones*.
3. Click *Add services*.
4. To add a service, select *Services* and choose the services from the list.
5. To allow custom ports, select *Custom ports* and specify the port value for UDP and/or TCP. You can assign an identifier to this port.
6. To confirm the changes, click *Add services* or *Add ports*, respectively.

3 Common `firewalld` commands

The **`firewall-cmd`** command-line tool is used to configure and manage the `firewalld` daemon. It is a powerful, dynamic utility that allows for the creation, modification, and deletion of firewall rules without requiring a full service restart, which prevents interruption of active network connections.

Some common **`firewall-cmd`** command examples include:

- Checking if `firewalld` is running. The outputs are `running`, `not running` or `RUNNING_BUT_FAILED`. For example:

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

- Listing all available zones, for example:

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

- Viewing the default zone, for example:

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

- Viewing the active zones and the assigned, for example:

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

- Viewing all rules for the default zone, for example:

  ```
  > 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
```

- Viewing all rules for a specific zone, for example:

```
> 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
```

- Listing all available predefined services, for example:

```
> 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
  [...]
```

- Listing the services currently allowed in the default zone, for example:

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

- Adding a service to the default zone permanently, for example:

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

- Removing a service permanently, for example:

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

- Listing the ports currently open in the default zone, for example:

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

- Opening a specific TCP port temporarily, for example:

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

- Removing an open port permanently, for example:

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

- Adding an interface to a specific zone temporarily, for example:

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

4 firewalld troubleshooting

Troubleshooting firewalld involves checking its status, verifying rules, and restarting or reloading the service. If you encounter issues, you can enable debugging, examine logs and adjust firewall rules as needed.

4.1 Check firewalld status

- Use the **systemctl status** command, for example:

```
> 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
```

- The **firewall-cmd --state** command gives a quick status check with running, not running or RUNNING_BUT_FAILED outputs. For example:

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

- If firewalld is not running, use the **systemctl start firewalld** command.

```
> sudo  systemctl start firewalld
```

- If the firewalld service is masked, unmask it first, then enable and start it, for example:

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

```
> sudo systemctl enable firewalld
```

```
> sudo systemctl start firewalld
```

4.2 Check `firewalld` rules

- The **`firewall-cmd --list-all-zones`** command displays all zones and their rules, for example:

```
> 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
          [...]
```

- The **`firewall-cmd --list-ports`** command shows open ports,for example:

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

- The **`firewall-cmd --zone=`***`YOUR_ZONE`* **`--list-all.`** command lists ports for specific zones, for example:

```
> 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 Debugging firewalld

- Enable debugging in `/etc/sysconfig/firewalld` by adding `--debug=[level]` to `FIREWALLD_ARGS`, for example:

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

- Start `firewalld` with the `--debug`option, for example:

```
> 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'
[...]
```

All log files are available at `/var/log/firewalld`.

5 More information

To learn more about `firewalld`, refer to the following resources:

- The official source for concepts, architecture, how-to and links to all man pages. (https://firewalld.org/documentation/)
- Man page essential for understanding command-line interaction with `firewalld` (https://firewalld.org/documentation/man-pages/firewall-cmd.html)
- A comprehensive resource with excellent explanations and practical examples that also cover `nftables`. (https://wiki.archlinux.org/title/Firewalld)

6 Legal Notice

Copyright© 2006–2025 SUSE LLC and contributors. All rights reserved.

Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or (at your option) version 1.3; with the Invariant Section being this copyright notice and license. A copy of the license version 1.2 is included in the section entitled “GNU Free Documentation License”.

For SUSE trademarks, see https://www.suse.com/company/legal/ ↗. All other third-party trademarks are the property of their respective owners. Trademark symbols (®, ™ etc.) denote trademarks of SUSE and its affiliates. Asterisks (*) denote third-party trademarks.

All information found in this book has been compiled with utmost attention to detail. However, this does not guarantee complete accuracy. Neither SUSE LLC, its affiliates, the authors, nor the translators shall be held liable for possible errors or the consequences thereof.

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. Secondarily, 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.