GNU/Linux, software libre para la comunidad universitaria

Administración de cortafuegos en GNU/Linux

COLABORADORES			
	TÍTULO : GNU/Linux, software libre para la comunidad universitaria		*REFERENCE* :
ACCIÓN	*NOMBRE*	*FECHA*	*FIRMA*
ESCRITO POR	José Ángel de Bustos Pérez	22 de abril de 2008	

HISTORIAL DE REVISIONES			
NÚMERO	FECHA	MODIFICACIONES	NOMBRE
1.0	10-04-2008		José Ángel de Bustos Pérez

Índice general

Capítulo 1

Introducción

Este manual se ha realizado como parte de la documentación del curso de que imparte la Universidad de Salamanca, Augcyl y GLiSA: *GNU/Linux, Software Libre para la Comunidad Universitaria*.

Una de las ponencias de curso es la Administración Avanzada del Sistema GNU/Linux, la cual se plasma en este manual. En esta ponencia se presenta todas las posibilidades de la administración del sistema, y en el resto de ponencias entrarián en detalle de algunos de los conceptos mís importantes de administración que en esta documentación encontramos.

1.1. Objetivo

En este manual vamos a intentar dar las características generales que tiene un sistema GNU/Linux y que la persona encargada, el administrador, debe conocer para "mantener" el sistema.

Un sistema GNU/Linux nos lo encontramos como un conjunto de aplicaciones reunidas entorno a núcleo del sistema, es lo que denominamos distribución. No vamos a entrar en las particularidades de cada distribución, aunque el curso se imparte con la distribución SuSE. Vamos a intentar ver las generalidades de todas ellas, que a su vez son parecidas a los sistemas operativos UNIX, del cual Linux hereda.

Tampoco intenta ser un manual de sistema operativo (SO) UNIX, pero si vamos a dividir los capítulos por componentes de un Sistema Operativo.

Con la ponencia y con este manual de apoyo queremos lograr que el alumno obtenga los conceptos básicos de la administración de GNU/Linux, las responsabilidades del administrador de GNU/Linux y pueda afrontar cualquier reto que la administración de GNU/Linux pueda plantearles.

Capítulo 2

Introducción a *Iptables*

GNU/Linux permite la gestión y filtrado del tráfico de red mediante netfilter.

Iptables es la interface de configuración para utilizar *netfilter* en el filtrado de tráfico de red.

Esta herramienta se ha venido mejorando desde hace mucho tiempo y su nombre ha variado dependiendo de la versión del núcleo:

- *iptables* introducido en las versiones del núcleo 2.4 y posteriores.
- *ipchains* utilizado en las versiones del núcleo 2.2.
- *ipforward* utilizado en las versiones del núcleo 2.0

2.1. Las *tablas* en iptables

Por defecto en *iptables* vienen definidas tres:

- *filter* en esta tabla se realiza el filtrado del tráfico permitido de entrada y salida al ordenador. Por defecto se trabaja en esta tabla.
- *NAT* se utiliza para la redirección de conexiones.
- *Mangle* se utiliza para la alteración de los paquetes. Cambio de direcciones de origen y destino, puertos de origen y destino, ...

2.2. Las *cadenas* en iptables

Existen cinco cadenas que nos indican en que punto se realiza el procesado de los paquetes:

- *PREROUTING* el procesado del paquete se realiza justo después de entrar el paquete por el interface de red y después de ser verificado como válido.
- *POSTROUTING* el procesado del paquete se realiza justo antes de dejar el interface de red.
- *OUTPUT* el procesado se realiza después de que el paquete sea generado por un proceso local.
- *INPUT* el procesado se realiza antes de que el paquete sea entregado a un proceso local.
- *FORDWARD* el procesado se realiza en la transición del paquete entre dos interfaces de red.

Las cadenas contienen reglas que son las encargadas de especificar las acciones a realizar sobre los paquetes. Estas reglas se ejecutan en orden secuencial y cuando existe una coincidencia se aplica la regla y se termina el proceso para ese paquete.

En caso de no existir ninguna coincidencia del paquete con las reglas existe una política por defecto que es la que se aplica.

2.3. Las *acciones* o *targets* en iptables

Cada cadena tiene que indicar la acción a realizar ocn el paquete en el caso de coincidencia:

- *ACCEPT* acepta el paquete.
- *DROP* rechaza el paquete sin ofrecer información.
- *REJECT* rechaza el paquete ofreciendo información al remitente.
- *QUEUE* envia el paquete al espacio de usuario donde puede ser tratado mediante scripts u otras herramientas no incluidas dentro del núcleo.
- *RETURN* si es desde una cadena definida por el usuario, se continua el procesado del paquete desde la cadena que invocó a la cadena definida por el usuario. Si es desde una cadena predefinida se aplica la política por defecto de esa cadena al paquete.

2.4. Usos de *Iptables*

Ya hemos visto algunos de los usos de *iptables*:

- *Filtrado de paquetes*, es el uso básico. Se inspeccionan los paquetes y se toman decisiones sobre que hacer con el paquete.
- *Accounting*, empleado para el control del volumen de tráfico existente.
- *Connection Tracking*, diferentes servicios utilizan varias conexiones. Por ejemplo FTP utiliza una conexión para control y otra para datos.
- *Mangling*, modificación de las cabeceras de los paquetes.
- *NAT*, *N*etwork *A*ddress *T*ranslation es un caso especial de *mangling* en el que se reescriben las direcciones de origen o destino de los paquetes.

  Existen dos tipos de *NAT*:

  - *SNAT*, NATTING sobre la dirección de origen del paquete.
  - *DNAT*, NATTING sobre la dirección de destino del paquete.
- *Masquerading*, es un caso especial de *SNAT* en el que un ordenador reescribe todos los paquetes como si fueran suyos. Se usa en funciones de PROXY o pasarela de acceso a internet.
- *Port Forwarding*, es un caso especial de *DNAT* en el que un ordenador actua como proxy para varios ordenadores. Es comunmente utilizado para ofrecer varios servicios en una ip. Los paquetes de tráfico http se reenvian al servidor web, los de correo al servidor de correo, ...
- *Balanceo de Carga*, se puede distribuir carga entre varios servidores.

Capítulo 3

Filtrado de paquetes

La configuración de *iptables* se realiza desde la línea de comandos mediante ordenes como:

```
iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j DNAT --to-destination ↩
    192.168.1.3:8080
```

3.1. Donde se aplicarán las reglas

Cada regla tendrá que aplicarse dentro de una cadena y una tabla y será necesario indicarle sobre el tráfico de que interface:

- *-t* indica la tabla.
- *-A* indica la cadena.
- *-i* indica el interface de entrada del paquete.
- *-o* indica el interface de salida del paquete.

Ejemplos:

- *iptables -t nat -A PREROUTING -i eth1*, se hace *NATTING* sobre el tráfico de la interface *eth1* y la regla se aplicará según entre el paquete por la interface.
- *iptables -t nat -A POSTROUTING -i eth0*,se hace *NATTING* sobre el tráfico de la interface *eth0* y la regla se aplicará justo antes de que el paquete salga por la interface.
- *iptables -A FORWARD -i eth0 -o eth1*, se hace forwarding de paquetes entre las interfaces *eth0* (entrada) y *eth1* (salida).

3.2. Políticas por defecto

Para establecer la política por defecto de una tabla:

```
iptables -t tabla -P cadena target
```

Ejemplos:

- *iptables -t nat -P PREROUTING ACCEPT*, en la tabla *nat* y dentro de la cadena *PREROUTING* se establece la política por defecto de *ACCEPT*.
- *iptables -t nat -P POSTROUTING DROP*, en la tabla *nat* y dentro de la cadena *POSTROUTING* se establece la política por defecto de *DROP*.
- *iptables -P INPUT ACCEPT*, en la tabla *filter* y dentro de la cadena *INPUT* se establece la política por defecto de *ACCEPT*.

La política por defecto es la acción a realizar sobre un paquete cuando ninguna cadena de la tabla coincide con el paquete.

3.3. Jugando con origenes y destinos

Podemos realizar el filtrado de paquetes basandonos en el origen y destino de los paquetes:

- *-p (--protocol) tcp|udp*, especifica el protocolo del paquete.
- *--source-port (--sport)*, especifica el puerto de origen del paquete.
- *--destination-port (--dport)*, especifica el puerto de destino del paquete.
- *-s (--source)*, especifica la dirección de origen del paquete.
- *-d (--destination)*, especifica la dirección de destino del paquete.

Ejemplos:

- *iptables -A INPUT -s 192.168.1.23 -p tcp --dport 3306 -j ACCEPT*, con esta regla permitimos todo el tráfico *TCP* desde la IP *192.168.1.23* con destino el puerto *3306* (MySQL).
- *iptables -A INPUT -i lo -j ACCEPT*, permitimos todas las conexiones al dispositivo de *loopback*.
- *iptables -A OUTPUT -p udp --dport 53 -j REJECT*, denegamos todo el tráfico *UDP* de salida hacía el puerto *53*.
- *iptables -A INPUT -p tcp --dport 20:21 -j ACCEPT*, permitimos el tráfico *TCP* de entrada hacía los puertos *20* y *21*.
- *iptables -A INPUT -p tcp --dport 1:1024*, se aplicará la políca por defecto a todos los paquetes de entrada con destino los puertos comprendidos entre el *1* y el *1024*.

Capítulo 4

Haciendo Natting

Natting es la capacidad de un ordenador de distribuir conexiones que recibe hacía otro.

Los routers ADSL poseen tablas de NAT que nos permiten abrir el puerto 22, por ejemplo, y redirigir esas conexiones hacía nuestro equipo de sobremesa, el puerto 80 hacía otro equipo haciendo las funciones de servidor web, ...

4.1. Configurar el acceso a un servidor web con NAT (DNAT)

Vamos a ver como configurar un firewall con iptables que acepte conexiones a una ip pública y la reenvie a un servidor dentro de una red local sin acceso a internet.

Para ello necesitaremos que el firewall:

- Tenga dos interfaces de red, una conectada a internet y la otra a la red local donde estará el servidor web.
- El firewall pueda hacer routing de paquetes.

4.1.1. Activando el routing en el firewall

Será necesario que el núcleo tenga soporte para ello:

```
[root@dedalo ~]# sysctl -A | grep ip_forward
net.ipv4.ip_forward = 0
[root@dedalo ~]#
```

En el caso de no encontrar el parámetro *ip_forward* nuestro núcleo no estará preparado para hacer routing de paquetes y será necesario recompilarlo o instalar uno que si lo este.

Un valor de *0* significa que no está habilitado y debermos habilitarlo. Para ello añadiremos la siguiente línea en `/etc/sysctl.conf`:

```
net.ipv4.ip_forward = 1
```

y a continuación para que tenga efecto:

```
[root@dedalo ~]# sysctl -p
...
net.ipv4.ip_forward = 1
...
[root@dedalo ~]#
```

importante
El activar parámetros del núcleo en scripts ejecutando:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

es una muy mala costumbre demasiado extendida entre administradores. Todo esto se debe centralizar en el fichero `/etc/sysctl.conf`.

De esta forma activamos el reenvio de paquetes entre todas las interfaces del firewall. Si el firewall tuviera más de dos interfaces y quisieramos habilitar el reenvio de paquetes sólo entre dos de ellas, por ejemplo *eth1* y *eth2*, deberemos incluir en el fichero `/etc/sysctl.conf`:

```
net.ipv4.conf.eth1.forwarding = 1
net.ipv4.conf.eth2.forwarding = 1
```

y ejecutar *sysctl -p* para que tenga efecto.

4.1.2. Configuración de iptables

Supondremos que nuestro firewall está conectado a internet por la interface *eth0* y a la red local por el interface *eth1* siendo la ip del servidor web *192.168.1.2*.

Las reglas de iptables:

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j DNAT --to-destination  ↩
    192.168.1.2:80
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j DNAT --to-destination  ↩
    192.168.1.2:443
iptables -A INPUT -s 192.168.1.0/24 -i eth1 -j ACCEPT
iptables -t nat -A POSTROUTING -s 192.168.1.0/24 -o eth0 -j MASQUERADE
```

1. Todo el tráfico que entra por la interface *eth0* con destino el puerto *80* y protocolo *TCP* se hace *DNAT*, es decir se cambia la dirección de destino del paquete y se cambia por *192.168.1.2*.
2. Igual que el anterior pero con el puerto *443*.
3. Nos aseguramos que el firewall acepta todo el tráfico de la red local.
4. El firewall hace masquerading de todo el tráfico procedente de la red local y lo envia por el interface *eth0*.

importante
La última regla se podrí optimizar siempre y cuando el interface *eth0* no tenga asignación dinámica en el direccionamiento ip. Lo veremos en el siguiente punto.

4.2. Haciendo SNAT (Cluster de Correo)

SNAT es la funcionalidad para cambiar la dirección de origen del paquete.

En realidad *MASQUERADING* y *SNAT* son muy parecidos. La diferencia es que *MASQUERADING* introduce más carga en el sistema que *SNAT* ya que cada vez que tiene que actuar sobre un paquete la dirección que pone al paquete es la que tiene el interface por el que va a salir en lugar de la especificada y es la comprobación de esa IP se realiza por cada paquete procesado lo que introduce la sobrecarga en el sistema.

Por este motivo si tenemos que hacer *SNAT* deberemos utilizar *MASQUERADING* si el interface sobre el que se hace tiene asignación dinámica de IP por *DHCP*.

4.2.1. Descripción del escenario

Supongamos que tenemos un cluster de correo con dos nodos y por comodidad utilizaremos direccionamiento privado:

- *nodo1_mail.localdomain* con ip *192.168.1.21* en el dispositivo *eth0*.
- *nodo2_mail.localdomain* con ip *192.168.1.22* en el dispositivo *eth0*.

La ip del servicio de correo *192.168.1.100 (mail.localdomain)*. Está ip estará levantada en el nodo que esté dando el servicio como un alias *eth0:1*.

Todos los paquetes que salgan por el interface *eth0* saldrán con ip de origen la que tenga el interface *eth0*. Si el paquete está originado por el servidor de correo y el servidor de correo destino hace una comprabación por resolución inversa descubrirá que la ip de origen no está asociada a *mail.localdomain*.

Dependiendo de la configuración del servidor de correo de destino no podría pasar nada, podría no aceptar el correo o incluso incluir nuestro servidor de correo en las blacklists.

4.2.2. Configuración de iptables

Las reglas de iptables:

```
iptables -A POSTROUTING -o eth0 -p tcp --dport 25 -j SNAT --to-source 192.168.1.100
```

1. Todo el tráfico de salida por la interface *eth0* usando el protocolo *TCP* y con puerto de destino *25* será rescrito con dirección de origen *192.168.1.100*.

importante
En este caso no podrímos utilizar *MASQUERADING* ya que en ese caso la ip que se utilizaría como origen del paquete serí la de *eth0*.

Capítulo 5

Administración de iptables

Las reglas que configuramos en *iptables* desaparecerán en los reinicios y deberemos configurar *iptables* para que al reinicar el ordenador carge las reglas.

5.1. Reglas persistentes en *iptables*

*Iptables*incorpora una serie de comandos para volcar a disco las reglas del cortafuegos y poder restaurarlas más adelante como por ejemplo cuando reiniciamos la máquina:

- *iptables-save* sirve para volcar a la salida estándar las reglas de una tabla.
- *iptables-restore* se utiliza para restaurar las reglas desde un fichero.

5.1.1. Red Hat/Fedora

Una vez configurado *iptables*:

```
[root@dedalo ~]# service iptables save
Guardando las reglas del cortafuegos a /etc/sysconfig/iptables [  OK  ]
[root@dedalo ~]#
```

De esta forma se guardan las reglas en el fichero `/etc/sysconfig/iptables` y la próxima vez que arranque *iptables* cargará las reglas.

importante
Si queremos que el servicio *iptables* se arranque de forma automática en los inicios del sistema deberemos ejecutar:

```
[root@dedalo ~]# chkconfig iptables on
[root@dedalo ~]#
```

5.2. Añadiendo reglas

El saber añadir, eliminar y mover reglas es muy importante ya que las reglas dentro de una cadena se ejecutan en orden secuencial y el orden es muy importante.

5.2.1. Insertando reglas

Cuando añadimos una regla esta regla se añade al final de la cadena en la que estemos trabajando.

Podemos añdir reglas de dos formas:

- *APPEND*, este es el modo normal. Se utiliza el flag *-A* y la regla se añade al final de la cadena:

```
iptables -t tabla -A cadena regla
```

- *INSERT*, en este modo insertamos la regla en una posición determinada dentro de la cadena:

```
iptables -t tabla -I cadena posicion regla
```

importante
El orden de las reglas es importante.

importante
La primera regla de la cadena es la número uno.

importante
En caso de no especificar una posición para la regla se asume que es la número uno.

5.2.2. Borrando reglas

Podemos borrar reglas de dos formas:

- A nivel de regla:

```
iptables -t tabla -D cadena regla
iptables -t tabla -D cadena posicion
```

  Podemos especificar la regla a borrar o directamente su posición.

- A nivel de cadena:

```
iptables -t tabla -F cadena
```

  Con el flag *-F (--flush)* borramos todas las reglas de la cadena especificada. En caso de no especificar ninguna cadena se borran las reglas de todas las reglas de todas las cadenas.

5.2.3. Reemplazando reglas

Es posible reemplazar una regla por otra:

```
iptables -t tabla -R cadena posicion regla
```

Apéndice A

GNU Free Documentation License

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 noncommercially. 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 in order 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 noncommercially, 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.

Ñ. 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 http://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

To use this License in a document you have written, include a copy of the License in the document and put the following copyright and license notices just after the title page:

> 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.