Samba−Authenticated−Gateway−HOWTO

Table of Contents

Table of Contents

Samba Authenticated Gateway HOWTO

Ricardo Alexandre Mattar

v1.3, 2005−01−06

This document intends to show how to build a Firewall/Gateway with rules set on user basis having the users authenticated by a Samba Primary Domain Controller

---

7. User management

8. Group management

9. Bibliography

10. GNU Free Documentation License

---

1. Introduction

As you can see by the poorness of my language, English is not my native language. I am writing this document in English for the sake of the Linux community. So, please, excuse me for my poor English. And, please, if you speak Portuguese, address me in this language.

This document intends to enlighten you (and myself) in the process of building a Linux Gateway or Firewall, which modify rules on demand when users log in or out from their Windows workstations.

In this document, I will try to show how to build a gateway to NAT or MASQUERADE Windows workstations. Use your imagination to modify it to get any level of network management. You may use it to grant or deny access to services, servers or entire subnetworks on your network.

Imagine that you have to build a gateway to let Windows workstation access the Internet and that you need to authenticate each user before letting them access the external networks. The first solution you think about is Squid. It's indeed a great solution, when http and ftp access is enough for your users. When it comes to let them access other services like pop, smtp, ssh, a database server or whatever else, you immediately think about NAT or MASQUERADE. But what happens to the user authentication?

Well, this is my solution. It gives you user authentication and fine grain control over their access to the external networks.

1.1 Overview

We know that SAMBA can act as a Domain Controller and so it can authenticate users on Windows boxes. As a PDC, SAMBA can push netlogon scripts to the Windows workstations. We can use this netlogon scripts to force the Windows workstations mounting a given share from our Linux PDC. This "forced" share shall have preexec and postexec scripts which shall be triggered when the user logs in or out. There is a program named smbstatus which lists the shares being used, giving us also the username and ip address of the workstation.

We just need to grep this information from smbstatus output and update our firewall rules.

1.2 Candy

If you are impatient and don't like to read, go to http://sourceforge.net/projects/smbgate/, but in the end you may find yourself coming back here to read.

1.3 Disclaimer

No liability for the contents of this document can be accepted. Use the concepts, examples and other content at your own risk. As this is a new edition of this document, there may be errors and inaccuracies, that may of course be damaging to your system. Proceed with caution, and although this is highly unlikely, the author(s) do not take any responsibility for that.

All copyrights are held by their respective owners, unless specifically noted otherwise. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

Naming of particular products or brands should not be seen as endorsements.

1.4 New versions

The newest release of this document can be found at http://ram.eti.br or at http://www.tldp.org

Related HOWTOs can be found at the Linux Documentation Project homepage at http://tldp.org.

1.5 Translations

A Portuguese version is available.

A French translation by Guillaume Lelarge is available at http://www.traduc.org

A Hungarian translation is available at http://tldp.fsf.hu

If you want to contribute with a translation, please do.

1.6 Feedback

Contributions and criticism are both welcome.

Corrections to my English are also very welcome!

If you find any bugs in the scripts included, please tell me.

You can find me at ricardo@ram.eti.br or at ricardo.mattar@bol.com.br

1.7 Copyright and trademarks

1.8 Acknowledgments and Thanks

Thanks to Carlos Alberto Reis Ribeiro for introducing me to Linux.

Thanks to Cesar Bremer Pinheiro for motivating me to write this document.

Thanks to Guillaume Lelarge for the (continuous) help with the revision.

Thanks to Erik Esplund for further language corrections.

Thanks to Albert Teixidó for code improvements.

Thanks to Felipe Cordeiro Caetano for helping on my main testing site.

Thanks to the secure communications company RASEAC for sponsoring my work.

---

2. Requirements

2.1 Knowledge

This document is target at the seasoned systems administrator.

You must have a fair knowledge about (at least know what these are):

- TCP/IP;
- Linux netfilter;
- A scripting language (bash?);
- SAMBA and Windows networking and domain controllers;

Fortunately, there is plenty of documentation on these topics on the Internet.

2.2 Software

Installed on your server, you will need at least:

- Samba;
- Iptables;
- A scripting language;

---

3. Linux box setup

This Howto assumes you have a kernel from the 2.4 series as it uses iptables. Other than that, there are no known issues why this should not work on a 2.2 kernel box with the scripts adapted to ipchains.

Of course, you need to install the iptables userland tools, an apache http server if you want to run a CGI tool to change passwords and SAMBA. And you will need a kernel compiled with iptables modules.

You may wish to use DHCP. If so, it is easy to set up. Remember to configure the dhcp server to give the nameserver IP address and the gateway IP address as well. The Windows machines will make good use of this information.

3.1 Basic system setup

Generally any basic system setup from the common Linux distributions will fit in this gateway example. Just check if you have Samba and IPTABLES.

3.2 Additional directory hierarchy

The additional directory hierarchy will be required to accomplish the example of this howto:

This is used to keep track of the users and IP addresses:

```
/var/run/smbgate/
```

This is where I place user specific scripts:

```
/etc/smbgate/users/
```

And group specific scripts:

```
/etc/smbgate/groups/
```

Directory for the netlogon share:

```
/home/samba/netlogon/
```

Directory for the tracking share:

```
/home/samba/samba/
```

These hierarchies are required by some of the scripts and daemons of the example.

3.3 Firewall setup

Its very unlikely that your distribution's kernel won't be compiled with Iptables and the userland tools won't be installed either. Anyway, if you don't have it, refer to http://www.netfilter.org or http://www.iptables.org to get the software and the documentation.

You will need a basic firewall setup in order to get the gateway working. Take a look at the iptables tutorial at IPTABLES TUTORIAL. It's an interesting reading. Anyway, if you have no time to spend, the following code is somewhat (very) loose but it may fit your needs:

```
#!/bin/sh
IPTABLES=/usr/sbin/iptables
/sbin/depmod -a
/sbin/insmod ip_tables
/sbin/insmod ip_conntrack
/sbin/insmod ip_conntrack_ftp
/sbin/insmod ip_conntrack_irc
/sbin/insmod iptable_nat
/sbin/insmod ip_nat_ftp
echo "1" > /proc/sys/net/ipv4/ip_forward
echo "1" > /proc/sys/net/ipv4/ip_dynaddr
$IPTABLES -P INPUT ACCEPT
$IPTABLES -F INPUT
$IPTABLES -P OUTPUT ACCEPT
$IPTABLES -F OUTPUT
$IPTABLES -P FORWARD ACCEPT
$IPTABLES -F FORWARD
$IPTABLES -t nat -F
```

You will notice that this code actually does nothing, but load the kernel modules related to nat and firewalling and turns the packet routing on. You can (and should) place any rules there to give your gateway a standard behavior, but the big magic will be done by scripts called by the SAMBA daemon.

Please, remember that this code doesn't have the least bit of security! Don't use these examples in production environments. This example intends only to be educational. You have to add a firewall configuration that suits your systems.

You have been warned!

3.4 SAMBA setup

Check if you have Samba installed. If your distribution doesn't come with Samba pre−packaged then refer to http://www.samba.org to get the packages and for documentation on how to install Samba. Brows around their web site and learn about it. The site has plenty of documentation and maybe your LINUX distribution also has plenty of SAMBA documentation.

We will need to setup SAMBA as a Primary Domain Controller. I will give an example configuration file here, but you should read the Samba HOWTO Collection and learn all you can about a PDC.

Basic SAMBA setup.

Since I do not intend to rewrite the SAMBA documentation, here goes a sample smb.conf file:

```
# Global parameters
[global]
workgroup = DOMAIN
netbios name = LINUX
server string = Linux PDC
encrypt passwords = Yes
map to guest = Bad Password
passwd program = /usr/bin/passwd
```

```
unix password sync = Yes
max log size = 50
time server = Yes
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
add user script = /usr/sbin/useradd -d /dev/null -g 100 -s /bin/false -M %u
logon script = %a.bat
domain logons = Yes
os level = 64
lm announce = True
preferred master = True
domain master = True
dns proxy = No
printing = lprng
[homes]
comment = Home Directories
path = /home/%u
read only = No
[printers]
comment = All Printers
path = /var/spool/samba
printable = Yes
browseable = No
available = No
[netlogon]
comment = NetLogon ShARE
path = /home/samba/netlogon
guest account =
[samba]
comment = login tracking share
path = /home/samba/samba
browseable = No
root preexec = /usr/local/bin/netlogon.sh %u %I
root postexec = /usr/local/bin/netlogoff.sh %u
```

You will have to do with it or read the SAMBA documentation if you really want to control your server and network.

The "logon script"

Using "logon script = %a.bat" makes samba evaluate the guest os and call an appropriated logon script. If you want a static script, just change to "logon script = netlogon.bat". Actually you can do anything here and even generate any script during the logon.

The netlogon and the tracking shares

The netlogon share is where the Windows workstations download the logon script from. We need this share in order to place there a logon script, which will tell the workstation to mount a share that will be used to track the users ip addresses.

As you can see, there must be a line like the following in your smb.conf

```
logon script = netlogon.bat
```

This line will tell your Windows client to download and execute the script named netlogon.bat. This script must be placed at the netlogon share. So, we will also need a netlogon.bat script to your Windows workstations. You can use the following example and place it at the netlogon share, in this case:

/home/samba/netlogon/NETLOGON.BAT.

```
REM NETLOGON.BAT
net use z: \\linux\samba /yes
```

This script will tell the Windows workstation to mount the specified share, and so we will be able to keep track of the user and workstation through the output of the smbstatus program.

Quite simple! But not enough...

As you could see, we will need also a tracking share which, in this example, I named samba. You can see the tracking share configuration in smb.conf:

```
[samba]
comment = login tracking share
path = /home/samba/samba
browseable = No
root preexec = /usr/local/bin/netlogon.sh %u %I
root postexec = /usr/local/bin/netlogoff.sh %u
```

As you can guess or know if you read the SAMBA documentation, the root preexec and the root postexec lines tell SAMBA to run the indicated scripts when a user mounts or unmounts the share. In this case, we are passing the username to the script as a parameter. Note the %u at the end of the lines. These scripts are the beasts which will call a script or program to modify our gateway's packet filtering rules.

Note that the netlogon.sh script must check if the refered workstation has already mounted the tracking share.

Take a look at the netlogon.sh and netlogoff.sh scripts:

```
#!/bin/sh
#
# netlogon.sh
#
# usage:
# netlogon.sh <username>
#
if [ -f /var/run/smbgate/$1 ] ; then
    exit 0
fi
echo $2 > /var/run/smbgate/$1
IPTABLES='/usr/sbin/iptables'
EXTIF='eth0'
COMMAND='-A'
ADDRESS=`cat /var/run/smbgate/$1`
GROUP=`groups $1 | gawk '// { print $3 }'`
if [ -f /etc/smbgate/users/$1 ] ; then
    /etc/smbgate/users/$1 $COMMAND $ADDRESS $EXTIF
else
    if [ -f /etc/smbgate/groups/$GROUP ] ; then
        /etc/smbgate/groups/$GROUP $COMMAND $ADDRESS $EXTIF
    else
        /etc/smbgate/users/default.sh $COMMAND $ADDRESS $EXTIF
    fi
fi
```

This script (netlogon.sh) is intended to run when the user logs in and will select the which scripts will be executed based on the user name and to which group the user belongs. The user's ip address will be written to a file at /var/run/smbgate for tracking purposes. The file will take the user's name and will be later used when the user log off. The IP address will be passed as an argument to a script with the users' name which will finally update the firewall.

Notice that this netlogon.sh script tries a user script, then if it can't find the user script it tries a group script, and finally if it can't find the group script it tries the default.sh script. You can modify this logic and behavior as you wish and need, just remember to modify the others accordingly.

Chances are if the user belong to more than one that these scripts will fail. I did not have time to write a better code.

```
#!/bin/sh
#
# netlogoff.sh
#
# usage:
# netlogoff.sh <username>
#
IPTABLES='/usr/sbin/iptables'
EXTIF='ppp0'
COMMAND='-D'
TRACKSHARE="samba"
ADDRESS=`cat /var/run/smbgate/$1`
GROUP=`groups $1 | gawk '// { print $3 }'`
NM=`smbstatus -u $1 | grep $TRACKSHARE | wc -l`
if [ $NM -gt 0 ]; then
    exit
fi
if [ -f /etc/smbgate/users/$1 ] ; then
    /etc/smbgate/users/$1 $COMMAND $ADDRESS $EXTIF
else
    if [ -f /etc/smbgate/groups/$GROUP ] ; then
        /etc/smbgate/groups/$GROUP $COMMAND $ADDRESS $EXTIF
    else
        /etc/smbgate/users/default.sh $COMMAND $ADDRESS $EXTIF
    fi
fi
rm -f /var/run/smbgate/$1
```

This script (netlogoff.sh) is intended to run when the user logs off and will get the address from the /var/run/smbgate/user file which will be passed as an argument to the /etc/smbgate/users/user script which will update the firewall to the state desired when the user is not logged in.

Some versions of Windows, such as Windows 2000, mount the tracking share more than once per login. This may cause problems with the netlogon.sh and netlogoff.sh, triggering the scripts more the once. This can make a real mess. So, you may prefer to use a logout checking script at cron instead of a netlogoff.sh script triggered by SAMBA. Here is an example:

```
#!/bin/sh
# checklogout.sh
#
# usage:
# intended to run at cron (maybe each 10 minutes)

TRACKDIR="/var/run/smbgate"
```

```
DIRLENGTH=${#TRACKDIR}
TRACKSHARE="samba"
EXTIF='eth0'
COMMAND='-D'
if [ -d $TRACKDIR ]; then
  for n in $TRACKDIR/*; do
    [ -d $n ] && continue;
    if [ -f $n ] ; then
      IPADDRESS=`cat $n`
      USERNAME=${n:$DIRLENGTH+1}
      NMS=`smbstatus -u $USERNAME | grep $TRACKSHARE | grep $IPADDRESS | grep -v grep | wc -l`
      if [ $NMS == 0 ] ; then
        rm -f $n
        GROUP=`groups $USERNAME | gawk '// { print $3 }'`
        if [ -f /etc/smbgate/users/$USERNAME ] ; then
          /etc/smbgate/users/$USERNAME $COMMAND $IPADDRESS $EXTIF
        else
          if [ -f /etc/smbgate/groups/$GROUP ] ; then
            /etc/smbgate/groups/$GROUP $COMMAND $IPADDRESS $EXTIF
          else
            /etc/smbgate/users/default.sh $COMMAND $IPADDRESS $EXTIF
          fi
        fi
      fi
    else
      exit 0
    fi
  done
fi
```

In that case you should remove the root postexec clause from the tracking share on smb.conf:

```
root postexec = /usr/local/bin/netlogoff.sh %u
```

The following is a standard /etc/smbgate/users/user script. This is the one which will actually modify the firewall rules.

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
```

We should also have a default.sh script at /etc/smbgate/users/ to give the gateway a default behavior.

```
#!/bin/sh
#
# default.sh
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
#$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
exit 0
```

4. An alternative solution

The whole scheme of mounting a tracking share and triggering scripts to update the firewall and waiting for them to be triggered again on unmounting to reset the firewall rule may be too confusing and loose. It may become even obsolete as the Samba project release new features.

The latest Samba release has the capability of listing the logged users. I used this feature in a script to track the users and update the firewall as they log in and out. This script does not require all the work described on this text. It is very easy to use actually.

You can download the code from the project site at http://sourceforge.net/projects/smbgate/

---

5. SSH setup

You may want to run your PDC on one box and have another box as a managed gateway for any reason. If so you must setup your gateway to accept rsa authenticated logins without passwords from the PDC.

Take a look at www.openssh.org for information on how to properly setup your ssh server and client for this.

5.1 Important

You should read the ssh documentation and make shure that you fully understand what you are doing when you setup rsa or any other kind of cryptographic authentication.

If security isn't an issue, just use my example and go on.

5.2 Key pair generation

To create a key pair issue the following commands on the manchine meant to be the PDC:

```
pdc:~# ssh−keygen −t rsa
```

Answer the questions and copy the resulting public key to the gateway it self. Usually the public key goes to "~.ssh/id_rsa.pub"

```
pdc:~# cd .ssh
pdc:~# scp id_rsa.pub root@gateway:/root/.ssh/authorized_keys2
```

5.3 SSH enabled logon script

The following is a standard /etc/smbgate/users/user script modified to use the ssh cryptographic authentication.

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/sbin/iptables'
ssh root@gateway $IPTABLES $COMMAND POSTROUTING −t nat −s $ADDRESS −o $EXTIF −j MASQUERADE
```

Note that the iptables binary in called through ssh at the "gateway". Again, make sure that you read the ssh server documentation.

6. Windows workstation setup

6.1 Introduction

We will stick to setting up the network, user management and policies on the Windows workstations.

I will not go through all those steps, naming each dialog box. I will presume that if you can read and understand this document you can find your way through that mess.

6.2 Network protocols

First, unless you really need, remove all network protocols but TCP/IP. Even without their own protocol, Windows machines like to broadcast a lot, and this doesn't please anyone. Anyway, with TCP/IP who needs anything else?

6.3 DHCP setup

If you setup a DHCP server on your Linux box, remember that Windows workstations can get the nameservers and gateway's address besides its own IP address from it. So, you don't need to set all these items on each workstation.

6.4 Join your Linux server domain

Configure the Windows workstation to log in a Domain, and give the domain name of your Linux server. This is essential to the gateway work.

You must know that in order to join some versions of Windows to a SAMBA domain controller, you must create machine accounts in your Linux PDC. Check the SAMBA documentation on how to setup your PDC to the specific version of Windows which you have.

Windows fo workgroups

This version seems to need no special configuration to join the Linux PDC domain.

The netlogon script shall be named "WfWg.bat" so when %a is translated the right script is chosen.

Example:

```
REM WFWG.BAT
net use z: \\linux\samba /yes
```

Windows 95/98/ME

These versions also seems to need no special configuration to join the Linux PDC domain.

The netlogon script shall be named "Win95.bat" so when %a is translated the right script is chosen.

Example:

```
REM WIN95.BAT
net use z: \\linux\samba /yes
```

Windows NT

This version requires machine accounts at the Linux box. Check the SAMBA documentation.

The netlogon script shall be named "WinNT.bat" so when %a is translated the right script is chosen.

Example:

```
REM WINNT.BAT
net use z: \\linux\samba /yes /persistent:no
```

Windows 2000

This version requires machine accounts at the Linux box. Again, check the SAMBA documentation.

The netlogon script shall be named "Win2K.bat" so when %a is translated the right script is chosen.

Example:

```
REM WIN2K.BAT
net use z: \\linux\samba /yes /persistent:no
```

Windows XP

This version needs a machine account at the Linux box and a tweak at the registry, as follows.

Locate the key "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal". The default value is 1. Set it to 0 and it will no more complain about joining the domain.

If you have many workstation to configure create a file named anything.reg with the following content and use it to modify the "faulty" registry.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters]
"requiresignorseal"=dword:00000000
```

This version also needs an adjust at the logon script. Sometimes it insists on making the mounting persistent. The netlogon script shall be named "WinXP.bat" so when %a is translated the right script is chosen.

Example:

```
REM WINXP.BAT
net use z: \\linux\samba /yes /persistent:no
```

6.5 Policy editor

There is a utility named policy editor bundled on the Windows CD. The file name is poledit.exe. This tool, as the name suggest, allows to create a user and system policy file.

Unfortunately, this tool does not generate a plain text configuration file, so I can't place an example here.

Use the policy editor to create a policy to your workstations and users. You should disable the local password cache and domain cache in order to get some security. Save the policy file as config.pol and place it at the netlogon share of your Linux server. In this way, your Windows workstations will download and use the config.pol file to set their policy. Of course this task must be done on a Windows machine.

If you don't use a config.pol file, your Windows workstations will annoy you asking for a Windows password and you will become nuts trying to synchronize and manage your Domain and Windows passwords. It seems that the OS doesn't know that it joined a domain. You must tell it and then you have to slap it in the face so it will believe you.

---

7. User management

7.1 Adding users

Adding a Linux user by usual means and setting a samba password using smbpasswd will work. If you have any doubt, just refer to the SAMBA documentation. This is not a difficult issue.

7.2 Password management

I am issuing this a major topic because I couldn't learn yet how to manage users and users' passwords from a Windows workstation without using a web interface. I couldn't find and didn't know how to build integrated tools to solve this problem. So, I am using a CGI program to get it done.

Try the package at http://changepassword.sourceforge.net, it seems to be a good choice.

7.3 Granting or denying access to users

As you could see in a previous section of this howto, the SAMBA daemon will call a netlogon.sh script every time the tracking share is mounted. This netlogon.sh script will call a script with the user's name giving this script the ip address of the refered workstation as a parameter. This user script will apply the desired rules.

For example if you want to give the user full access to internet:

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF -j MASQUERADE
```

If you don't want to change anything to a particular user, just give him an empty script:

```
#/bin/sh
#
exit 0
```

Or just don't create any script for the less privileged users, letting them have the default.sh script, which would be empty as the previous or just give limited access as follows:

```
#!/bin/sh
#
COMMAND=$1
ADDRESS=$2
EXTIF=$3
EXTIFADDRESS=$4
IPTABLES='/usr/sbin/iptables'
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF --dport 25 -j SNAT --to-source $EXTIFADDRESS
$IPTABLES $COMMAND POSTROUTING -t nat -s $ADDRESS -o $EXTIF --dport 110 -j SNAT --to-source $EXTIFADDRESS
```

Remember that this script requires you to modify all the previous scripts to include the extra parameter ou just modify the script script. And remember that you will go nowhere whis this howto if you don't understand iptables.

---

8. Group management

8.1 Creating groups

Just create your user groups in the Linux PDC and add the users to the groups. This is it.

Remember that the example scripts in this howto will probably fail if you have users belonging to more than one group. If you need this, remember to adjust the scripts.

8.2 Group policy

You will need to define group specific scripts and place them in the directory "/etc/smbgate/groups/". Remember that the script must be named as the group, at least if you want to follow the examples in this howto.

The default scheme of this howto is to check for a user script, then for a group script and finally for the default script. If you want to modify this behavior remember to adapt the netlogon.sh, netlogoff.sh (or the checklogout.sh) scripts. The whole logic is in these scripts.

---

9. Bibliography

IPTABLES TUTORIAL by Oskar Andreasson

Samba HOWTO Collection by the SAMBA Team

---

10. GNU Free Documentation License

GNU Free Documentation License Version 1.2, November 2002

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. 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 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.