Guide pratique de la réalisation d’une passerelle d’authentification avec Samba

Adaptation française du Samba Authenticated Gateway HOWTO

Ricardo Alexandre Mattar

<ricardo POINT mattar CHEZ bol POINT com POINT br>

Adaptation française: Guillaume Lelarge

Relecture de la version française: François-Xavier Detournière

Préparation de la publication de la v.f.: Jean-Philippe Guérard

Version : 1.3.fr.1.0

17 février 2004

Historique des versions		
Version 1.3.fr.1.0	2005-02-17	GL, JPG
Mise à jour de la traduction française		
Version 1.3	2005-01-06	RAM
Version 1.2.1.fr.1.0	2004-11-06	GL
Mise à jour de la traduction française		
Version 1.2.1	2004-10-22	RAM
Version 1.2.fr.1.0	2004-06-04	GL
Version 1.2	2004-05-21	RAM
Version 1.1.1.fr.1.0	2003-07-15	GL
Version 1.1.1	2003-07-14	RAM
Version 1.1.0.fr.1.0	2003-05-08	GL, FXD, JPG
Version 1.1.0	2002-05-03	RAM

Résumé

Ce document a pour but d’expliquer la construction d’une passerelle pare-feu, utilisant un contrôleur primaire de domaine Samba (PDC ou *Primary Domain Controller*) et un ensemble de règles pour authentifier les utilisateurs.

Table des matières

1. Introduction

Ce document a pour but de vous faire comprendre (ainsi qu'à moi) le processus de construction d'un pare-feu ou d'une passerelle Linux, capable de modifier ses règles à la demande lorsque les utilisateurs se connectent ou se déconnectent de leurs postes de travail Windows.

Dans ce document, j'essaierai de montrer comment construire une passerelle pour faire du NAT ou du MASQUERADE avec des stations Windows. Utilisez votre imagination pour le modifier et avoir tout type de gestion des réseau. Vous pouvez l'utiliser pour autoriser ou refuser l'accès depuis votre réseau à des services, des serveurs ou à des sous-réseaux complets.

Imaginez que vous devez construire une passerelle pour laisser les stations Windows accéder à Internet et que vous avez besoin d'authentifier chaque utilisateur avant de le laisser accéder aux réseaux externes. La première solution à laquelle vous pensez est Squid. C'est en fait une bonne solution quand les accès HTTP et FTP sont suffisants à vos utilisateurs. Mais lorsqu'arrive le moment où vous devez les laisser accéder à d'autres services comme POP, SMTP, SSH, un serveur de base de données ou tout autre chose, vous penserez immédiatement à NAT ou MASQUERADE. Mais qu'en est-il de l'authentification de l'utilisateur ?

Donc, ceci est ma solution. Elle vous permet l'authentification de l'utilisateur et un contrôle beaucoup plus fin de son accès aux réseaux externes.

1.1. Aperçu

Nous savons que Samba peut agir en tant que contrôleur de domaine, et donc qu'il peut authentifier les utilisateurs de machines Windows. En tant que PDC, Samba peut envoyer des scripts netlogon aux stations de travail Windows. Nous pouvons utiliser ce script netlogon pour forcer les stations Windows à monter un partage donné à partir de notre PDC Linux. Ce partage « forcé » doit comporter les scripts preexec et postexec qui seront exécutés respectivement à la connexion et à la déconnexion de l'utilisateur. Un programme nommé **smbstatus** indique les partages en cours d'utilisation, ainsi que le nom de l'utilisateur et l'adresse IP de sa station. Nous avons juste besoin de récupérer cette information à partir de la sortie de **smbstatus** pour mettre à jour nos règles de pare-feu.

1.2. Pour commencer en douceur

Si vous êtes impatient et que vous n'aimez pas lire, allez sur http://sourceforge.net/projects/smbgate/. Plus tard, vous pourrez revenir ici pour continuer votre lecture.

1.3. Limitations de responsabilité

Important

Le texte ci-dessous est la version française de la mise en garde de ce document. Seule la version originale de cette mise en garde, présentée dans la section suivante, fait foi.

Aucune responsabilité sur le contenu de ce document ne sera acceptée. Utilisez les concepts, exemples et autres contenus à vos risques et périls. Comme ceci est une nouvelle édition de ce document, il peut exister des erreurs et des inexactitudes qui peuvent bien sûr endommagées votre système. Faites attention et, bien que ceci est fort improbable, l'auteur n'en prend aucune responsabilité.

Tous les droits appartiennent à leur propriétaire respectif, sauf cas spécifiquement indiqués. L'utilisation d'un terme dans ce document ne doit pas être vu comme affectant la validité d'une marque ou du service d'une marque.

Le fait de citer une marque ou un produit particulier ne doit pas être perçu comme une approbation.

1.4. Disclaimer

Important

Le texte ci-dessous est la mise en garde de ce document. Ce texte fait foi.

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.

1.5. Nouvelles versions

La dernière version originale de ce document est disponible sur http://ram.eti.br et sur http://www.tldp.org.

Il est possible de trouver les guides pratiques relatifs à ce document sur la page du projet de documentation Linux (LDP) sur http://tldp.org/.

La dernière version française de ce document est disponible sur www.traduc.org.

1.6. Traductions

Une version portuguaise est disponible.

Une traduction française réalisée par Guillaume Lelarge est disponible sur www.traduc.org (NdT : Si vous voulez participer aux traductions, n'hésitez pas. Votre aide sera la bienvenue !)

Une traduction hongroise est disponible sur http://tldp.fsf.hu.

1.7. Commentaires et corrections

J'ai écrit la version originale de ce document en anglais dans l'intérêt de la communauté Linux. Cependant, l'anglais n'est pas ma langue maternelle. Si vous parlez portugais, adressez-vous à moi dans cette langue.

Vos contributions et critiques sont les bienvenues.

Si vous trouvez un bogue dans les scripts inclus, merci de me le dire.

Vous pouvez me joindre en portugais ou en anglais à l'adresse <`ricardo CHEZ ram POINT eti POINT br`> ainsi qu'à l'adresse <`ricardo POINT mattar CHEZ bol POINT com POINT br`>.

Les commentaires relatifs à la version française de ce document sont les bienvenus. N'hésitez pas à nous signaler les erreurs, coquilles ou à nous faire part de vos impressions sur ce document. Vous pouvez nous contacter à l'adresse commentaires CHEZ traduc.org.

1.8. Droits d'utilisation et marques déposées

Important

Le texte ci-dessous est la version française de la licence de ce document. Seule la version originale de cette licence, présentée dans la section suivante, fait foi.

Copyright © 2002-2003 Ricardo Alexandre Mattar

Vous est autorisé de copier, distribuer ou modifier la version originale de ce document selon les termes de la licence de documentation libre GNU (GFDL), version 1.2 ou ultérieure, telle que publiée par la Free Software Foundation ; sans section inaltérable, ni texte de première de couverture, ni texte de quatrième de couverture. Une copie de cette licence est incluse dans la section intitulée « GNU Free Documentation License ».

Copyright © 2003-2005 Guillaume Lelarge, François-Xavier Detournière et Jean-Philippe Guérard pour la version française

La version française de document a été réalisée par Guillaume Lelarge, François-Xavier Detournière et Jean-Philippe Guérard . La version française de ce guide pratique est publiée en accord avec les termes de la licence de documentation libre GNU (GFDL) sans section invariante, sans texte de première de couverture ni texte de quatrième de couverture. Une copie de la licence est disponible sur http://www.gnu.org/copyleft/fdl.html.

1.9. Copyright and trademarks

> **Important**
>
> Le texte ci-dessous est la licence de ce document. Ce texte fait foi. Il est composé de la licence en anglais du document orignal, suivi de la licence en français de sa traduction.

1.10. Remerciements

Merci à Carlos Alberto Reis Ribeiro pour m'avoir présenté Linux.

Merci à Cesar Bremer Pinheiro pour m'avoir motivé lors de l'écriture de ce document.

Merci à Guillaume Lelarge pour son aide (continue) sur les différentes versions.

Merci à Erik Esplund pour d'autres corrections d'anglais.

Merci à Albert Teixidó pour les améliorations sur le code.

Merci à Felipe Cordeiro Caetano pour son aide sur le site de tests principal.

Merci à la société de communications sécurisées RASEAC pour sponsoriser mon travail.

2. Besoins

2.1. Connaissances

Ce document a pour cible les administrateurs système.

Vous devez avoir une bonne connaissance de (ou au moins savoir ce qu'ils sont) :

- TCP/IP ;

- Netfilter ;
- Un langage de script (bash ?) ;
- Les réseaux et les contrôleurs de domaine Samba et Windows.

Heureusement, Internet contient énormément d'informations sur ces sujets.

2.2. Logiciels

Vous devez avoir installé sur votre système :

- Samba ;
- Iptables ;
- Un langage de script.

3. Configuration de la machine Linux

Ce guide pratique suppose que vous avez un noyau de la série 2.4 car il utilise **iptables**. En dehors de ceci, il n'existe aucune autre raison pour laquelle il ne pourrait pas être utilisé avec une machine disposant d'un noyau 2.2 après avoir adapté les scripts à **ipchains**.

Bien sûr, vous avez besoin d'installer les outils utilisateur d'iptables, un serveur HTTP apache si vous voulez utiliser un outil CGI pour changer les mots de passe, et samba. Et vous aurez besoin d'un noyau compilé avec les modules iptables.

Vous pouvez utiliser DHCP. Si c'est le cas, il est assez simple de le configurer. Rappelez-vous de configurer le serveur DHCP pour qu'il donne l'adresse IP du serveur de noms ainsi que l'adresse IP de la passerelle. Les machines Windows feront bon usage de cette information.

3.1. Configuration basique du système

Généralement, toute configuration de base à partir des distributions Linux connues conviendra pour l'exemple de passerelle. Vérifiez simplement que vous disposez de Samba et d'**iptables**.

3.2. Hiérarchie des répertoires supplémentaires

Une hiérarchie de répertoires supplémentaires sera nécessaire pour accomplir l'exemple de ce guide pratique :

- `/var/run/smbgate/` : Ceci est fait pour conserver trace des utilisateurs et des adresses IP ;
- `/etc/smbgate/users/` : C'est ici que je place les scripts spécifiques aux utilisateurs ;
- `/home/samba/netlogon/` : Répertoire du partage netlogon ;
- `/home/samba/samba/` : Répertoire du partage de trace.

Ces répertoires sont nécessaires pour certains des scripts et démons de cet exemple.

3.3. Configuration du pare-feu

Il est très improbable que le noyau de votre distribution n'ait pas été compilé avec iptables et que les outils utilisateur ne soient pas non plus installés. Néanmoins, si vous ne les avez pas, référez-vous à http://www.netfilter.org/ ou http://www.iptables.org/ pour récupérer le logiciel et la documentation.

Vous aurez besoin d'une configuration basique du pare-feu pour que la passerelle fonctionne. Jetez un œil sur le tutoriel iptables disponible sur netfilter.org. Cette lecture est très intéressante. Néanmoins, si vous n'avez pas de temps pour cela, le code suivant est très basique mais il peut convenir à vos besoins :

```
#!/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
```

Vous remarquerez que ce code ne fait que charger les modules du noyau en relation avec NAT et le pare-feu, et mettre en place la transmission des paquets. Vous pouvez (et devriez) placer toutes les règles pour donner à votre passerelle un comportement standard, mais toute la magie sera réalisée par des scripts appelés par le démon samba.

S'il-vous-plait, rappelez-vous que ce code n'apporte pas la moindre sécurité ! N'utilisez pas cet exemple sur des machines de production. Cet exemple a seulement pour but d'informer. Vous devez ajouter une configuration de pare-feu convenant à votre système.

Vous êtes prévenus !

3.4. Configuration de Samba

Vérifiez que Samba est installé. Si votre distribution ne vient pas avec Samba préparé, alors référez-vous à http://www.samba.org pour obtenir le paquetage et la documentation sur son installation. Regardez sur leur site web et apprenez. Le site est rempli de documentations et peut-être que votre distribution Linux dispose elle-aussi de documentation sur Samba.

Nous aurons besoin de configurer Samba comme contrôleur principal de domaine. Je donnerais un fichier de configuration en exemple, mais vous devriez lire la collection de guides pratiques sur Samba et tout apprendre sur les PDC.

3.4.1. Configuration basique de Samba

Comme je n'ai pas l'intention de réécrire la documentation de Samba, voici un simple fichier `smb.conf` :

```
# 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
```

Vous devrez faire avec ou lire la documentation de Samba si vous voulez réellement contrôler votre serveur et votre réseau.

3.4.2. Le script logon

Utiliser « logon script = %a.bat » fait que samba évalue le système d'exploitation invité et appelle le script de connexion approprié. Si vous préférez un script statique, modifiez seulement cette ligne par « logon script = netlogon.bat ». En fait, vous pouvez tout faire ici, y compris générer un script lors de la connexion.

3.4.3. Partages netlogon et shares

Le partage netlogon est l'endroit où les stations Windows vont télécharger le script de connexion (logon). Nous avons besoin de ce partage pour y placer un script de connexion qui dira à la station de monter un partage que nous utiliserons pour tracer l'adresse IP de l'utilisateur.

Comme vous le voyez, il doit y avoir une ligne comme ci-dessous dans votre fichier `smb.conf`.

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

Cette ligne indiquera au client Windows de télécharger et exécuter le script nommé `netlogon.bat`. Ce script doit être placé dans le partage netlogon. Donc, nous aurons aussi besoin d'un script `netlo-gon.bat` pour vos stations Windows. Vous pouvez utiliser l'exemple suivant et créer un fichier nommé `NETLOGON.BAT` et placé dans le partage netlogon, dans ce cas dans `/home/samba/netlogon/NETLOGON.BAT`.

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

Ce script indiquera aux stations Windows de monter le partage spécifié, et donc nous serons capable de garder la trace de l'utilisateur et de la station au travers de la sortie du programme **smbstatus**.

Assez simple ! Mais pas suffisant…

Comme vous pouvez le voir, nous aurons aussi besoin d'un partage de traces que j'ai nommé samba dans cet exemple. Vous pouvez voir dans le fichier `smb.conf` la configuration du partage de traces :

```
[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
```

Comme vous pouvez le deviner, ou le savoir si vous avez lu la documentation de Samba, les lignes « root preexec » et « root postexec » indiquent à Samba de lancer les scripts indiqués lorsqu'un utilisateur monte ou démonte le partage. Dans ce cas, nous passons le nom de l'utilisateur comme paramètre au script. Notez le %u à la fin des lignes. Ces scripts vont appeler un script ou un programme pour modifier les règles de filtrage de paquets de notre passerelle.

Notez que le script `netlogon.sh` doit vérifier si la station en question a déjà monté le partage des traces.

Jetez un œil sur les scripts `netlogon.sh` et `netlogoff.sh` :

```
#!/bin/sh
#
# netlogon.sh
#
# usage:
# netlogon.sh <nom_utilisateur>
#
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
```

Ce script (`netlogon.sh`) a pour but d'être exécuté lors de la connexion de l'utilisateur et de sélectionner les scripts à exécuter suivant le nom de l'utilisateur et le groupe auquel celui-ci appartient. L'adresse IP de l'utilisateur sera enregistré dans un fichier sous `/var/run/smbgate` pour en conserver la trace. Le fichier prendra le nom de l'utilisateur et servira de nouveau lorsque celui-ci se déconnectera. L'adresse IP sera passée en argument à un script avec le nom de l'utilisateur qui mettra à jour les règles du pare-feu.

Notez que ce script commence par chercher un script utilisateur, puis, si il n'en trouve pas, il cherche un script groupe et, finalement, si il n'en trouve pas non plus, il utilise le script `default.sh`. Vous pouvez modifier cette logique et ce comportement si vous le souhaitez ou en avez besoin. Rappelez-vous simplement de modifier les autres de manières concordantes.

Il y a des chances pour que l'utilisateur appartienne à plus d'un des scripts et que ces scripts échouent. Je n'ai pas le temps d'écrire un meilleur 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
```

Ce script (`netlogoff.sh`) a pour but d'être exécuté lors de la déconnexion de l'utilisateur. Il récupérera l'adresse à partir du fichier `/var/run/smbgate/user`, adresse qui sera passée en argument pour le script `/etc/smbgate/users/user`. Ce dernier mettra à jour le pare-feu dans l'état désiré lorsque l'utilisateur ne sera plus connecté.

Certaines versions de Windows, telles que Windows 2000, montent le répertoire partagé plus d'une fois lors de la connexion. Ceci peut apporter des problèmes avec les scripts `netlogon.sh` et `netlogoff.sh` en les exécutant plus d'une fois. Donc, vous pouvez utiliser un script de vérification de déconnexion lancé par le **cron** au lieu d'un script `netlogoff.sh` lancé par Samba. En voici un exemple :

```
#!/bin/sh
# checklogout.sh
#
# usage:
# doit être lancé par cron (par exemple toutes les dix 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
```

Dans ce cas, vous devez supprimer la clause postexec de la déclaration du partage dans `smb.conf` :

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

La suite est un script standard `/etc/smbgate/users/user`. Ce script modifiera réellement les règles du pare-feu.

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

Nous devons aussi avoir un script default.sh sur /etc/smbgate/users/ pour donner à la passerelle un comportement par défaut.

```
#!/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. Autre solution

Le schéma complet de montage d'un partage de traces et de scripts déclenchés pour mettre à jour le pare-feu, et l'attente d'un nouveau déclenchement au démontage pour réinitialiser la règle du pare-feu pourraient trop porter à confusion, voire ne pas fonctionner. Cela pourrait même devenir obsolète lorsque le projet Samba apportera de nouvelles fonctionnalités.

La dernière version de Samba dispose de la capacité de lister les utilisateurs connectés. J'ai utilisé cette fonctionnalité dans un script pour tracer les utilisateurs et mettre à jour le pare-feu à leur (dé)connexion. Ce script ne requiert pas tout le travail décrit dans ce texte. En fait, il est très facile à utiliser.

Vous pouvez télécharger le code à partir du site du projet sur http://sourceforge.net/projects/smbgate/.

5. Configuration de SSH

Vous pouvez vouloir utiliser votre PDC sur une machine et avoir une autre machine réalisant la fonction de passerelle. Dans ce cas, vous devez configurer votre passerelle de façon à ce qu'elle accepte les connexions authentifiées avec RSA sans mots de passe du PDC.

Jetez un œil sur le site www.openssh.org pour une information sur une configuration propre pour votre serveur et votre client SSH.

5.1. Important

Vous devez lire la documentation ssh et vous assurez que vous comprenez pleinement ce que vous faites en configurant RSA ou tout autre mécanisme de cryptographie pour l'authentification.

Si la sécurité n'est pas un problème, utilisez simplement mon exemple et continuez.

5.2. Génération de paire de clés

Pour créer une paire de clés, lancez les commandes suivantes sur la machine correspondant au PDC :

```
pdc:~# ssh-keygen -t rsa
```

Répondez aux questions et copiez la clé publique résultante sur la passerelle. Habituellement, la clé publique va dans ~.ssh/id_rsa.pub.

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

5.3. Script de connexion activé par SSH

Ce qui suit est un script standard `/etc/smbgate/users/user` modifié pour utiliser l'authentification cryptée par SSH.

```
#!/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
```

Notez que le binaire **iptables** est appelé via SSH par la passerelle. De nouveau, assurez-vous d'avoir lu la documentation du serveur SSH.

6. Configuration des stations Windows

6.1. Introduction

Nous allons configurer le réseau, la gestion des utilisateurs et les politiques pour les stations Windows.

Je ne parcourrai pas toutes ces étapes en nommant chaque boîte de dialogue. Je présumerai que si vous pouvez lire et comprendre ce document, vous pouvez trouver votre chemin dans ce bazar.

6.2. Protocoles réseau

Tout d'abord, sauf si vous en avez réellement besoin, supprimez tous les protocoles réseau sauf TCP/IP. Même sans leur propre protocole, les machines Windows aiment diffuser à tous les nœuds (broadcast), et ceci ne plaît à personne. De toute façon, avec TCP/IP, qui a besoin d'autre chose ?

6.3. Configuration de DHCP

Si vous configurez votre serveur DHCP sur votre machine Linux, rappelez-vous que les stations Windows peuvent obtenir les adresses des serveurs de noms et de la passerelle en plus de leur propre adresse IP. Donc, vous n'avez pas besoin de configurer toutes ces informations sur chaque station.

6.4. Joindre le domaine de votre serveur Linux

Configurez les stations Windows pour qu'elles se connectent sur le domaine et donnez le nom du domaine de votre serveur Linux. Ceci est essentiel pour le fonctionnement de la passerelle.

Vous devez savoir que pour faire joindre certaines versions de Windows à un contrôleur de domaine Samba, vous devez créer des comptes sur le PDC Linux. Regardez dans la documentation Samba pour comprendre comment configurer votre PDC pour la version spécifique de Windows que vous avez.

6.4.1. Windows for workgroups

Cette version semble ne pas avoir besoin d'une configuration particulière pour joindre le domaine PDC Linux.

Le script netlogon devrait être nommé « WfWg.bat » de façon à ce que le bon script soit choisi lorsque %a est traduit.

Exemple :

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

6.4.2. Windows 95/98/ME

Cette version semble ne pas avoir besoin d'une configuration particulière pour joindre le domaine PDC Linux.

Le script netlogon devrait être nommé « Win95.bat » de façon à ce que le bon script soit choisi lorsque %a est traduit.

Exemple :

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

6.4.3. Windows NT

Cette version requiert des comptes machine sur le serveur Linux. Vérifiez la documentation de SAMBA.

Le script netlogon devrait être nommé « WinNT.bat » de façon à ce que le bon script soit choisi lorsque %a est traduit.

Exemple :

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

6.4.4. Windows 2000

Cette version requiert des comptes machine sur le serveur Linux. De nouveau, vérifiez la documentation de SAMBA.

Le script netlogon devrait être nommé « Win2K.bat » de façon à ce que le bon script soit choisi lorsque %a est traduit.

Exemple :

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

6.4.5. Windows XP

Cette version a besoin d'un compte machine sur Linux ainsi que d'une petite modification dans la base de registres.

Cherchez la clef :

```
HKEY_LOCAL_MACHINE\
  SYSTEM\
    CurrentControlSet\
      Services\
        Netlogon\
          Parameters\
            RequireSignOrSeal
```

La valeur par défaut est 1. Mettez-la à 0 et vous n'aurez plus de plaintes pour joindre le domaine.

Si vous avez plusieurs stations de travail à configurer, créez un fichier nommé `quelquechose.reg` contenant ceci :

```
Windows Registry Editor Version 5.00

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

Vous pourrez ainsi modifier les bases erronées.

Cette version a aussi besoin d'un ajustement sur le script de connexion. Quelque fois, il insiste pour rendre les montages permanents. Le script netlogon devrait être nommé « WinXP.bat » de façon à ce que le bon script soit choisi lorsque %a est traduit.

Exemple :

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

6.5. Éditeur de politiques

Il existe un utilitaire nommé « *policy editor* » inclus sur le CD de Windows. Le nom du fichier est `poledit.exe`. Cet outil, comme le nom le suggère, permet de créer un fichier de politique pour l'utilisateur et le système.

Malheureusement, cet outil ne génère pas un fichier de configuration texte, donc je ne peux pas placer un exemple ici.

Utilisez l'éditeur de politiques pour créer une politique pour vos stations et utilisateurs. Vous devez désactiver le cache local des mots de passe et le cache de domaine pour avoir un peu de sécurité. Sauvegardez le fichier de politiques en tant que config.pol et placez-le dans le partage netlogon sur votre serveur Linux. De cette façon, vos stations Windows vont télécharger et utiliser le fichier `config.pol` pour configurer leur politique. Bien sûr, cette tâche doit être faite sur une machine Windows.

Si vous n'utilisez pas un fichier `config.pol`, vos stations Windows vous ennuieront à vous demander un mot de passe Windows et vous deviendrez dingue en essayant de synchroniser et gérer les mots de passe de Windows et du domaine. Il semble que le système d'exploitation ne sache pas qu'il a rejoint un domaine. Vous devez lui dire et lui taper sur la tête de façon à ce qu'il vous croie.

7. Gestion des utilisateurs

7.1. Ajouter des utilisateurs

Ajouter un utilisateur Linux par les moyens habituels et configurer un mot de passe Samba en utilisant **smbpasswd** devrait fonctionner. Si vous avez des doutes, référez-vous à la documentation Samba. Ce n'est pas un problème difficile.

7.2. Gestion des mots de passe

C'est à mon avis un thème majeur car je n'ai pas encore compris comment gérer les utilisateurs et leurs mots de passe à partir d'une station Windows sans utiliser une interface web. Je n'ai pas trouvé et ne sais pas comment construire des outils intégrés pour résoudre ce problème. Donc, j'utilise un programme CGI pour le faire.

Essayez le paquetage disponible sur http://changepassword.sourceforge.net. Il semble être un bon choix.

7.3. Autoriser ou non l'accès aux utilisateurs

Comme vous pouvez le voir dans la section précédente de ce guide pratique, le démon Samba sera appelé par un script `netlogon.sh` à chaque fois que le partage des traces sera monté. Ce script `netlogon.sh` appellera un script avec le nom de l'utilisateur, donnant ainsi l'adresse IP de la station de travail en question en paramètre. Ce script utilisateur appliquera les règles souhaitées.

Par exemple, si vous voulez donner à l'utilisateur un accès complet à internet :

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

Si vous ne voulez pas modifier quoi que ce soit pour un utilisateur particulier, créez-lui simplement un script vide :

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

Vous pouvez aussi ne pas créer de scripts pour les utilisateurs les moins privilégiés, en les laissant avec le script `default.sh`, qui sera aussi vide que le précédent, ou donnez un accès limité de cette façon :

```
#!/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
```

Rappelez-vous que ce script nécessite la modification de tous les scripts précédents pour inclure le paramètre supplémentaire. Et rappelez-vous que vous n'irez nulle part avec ce guide pratique si vous ne comprenez pas iptables.

8. Gestion des groupes

8.1. Créer les groupes

Créez seulement les groupes d'utilisateurs sur le PDC Linux et ajoutez les utilisateurs aux groupes. C'est tout.

Rappelez-vous que les scripts d'exemple dans ce guide pratique vont probablement échouer si vos utilisateurs appartiennent à plus d'un groupe. Si vous avez besoin de plus d'un groupe, n'oubliez pas d'ajuster les scripts.

8.2. Politique des groupes

Vous aurez besoin de définir les scripts spécifiques aux groupes et de les placer dans le répertoire `/etc/smbgate/groups/`. Rappelez-vous que le script doit être nommé comme le groupe, au moins si vous voulez suivre les exemples de ce guide pratique.

Le schéma par défaut de ce guide pratique est de vérifier le script utilisateur, puis le script du groupe et enfin le script par défaut. Si vous voulez modifier ce comportement, rappelez-vous qu'il est nécessaire d'adapter les scripts `netlogon.sh`, `netlogoff.sh` (ou `checklogout.sh`). Tout le travail se fait dans ces fichiers.

9. Bibliographie

- Tutoriel iptables (netfilter.org) par Oskar Andreasson

- Collection de guides pratiques sur Samba par l’équipe de Samba

A. Adaptation française

1. Traduction

La traduction française de ce document a été réalisée par Guillaume Lelarge.

2. Relecture

La relecture de ce document a été réalisée par Francois-Xavier Detournière.

3. Préparation de la publication

La publication de ce document a été préparée par Jean-Philippe Guérard <`fevrier CHEZ tigre-raye POINT org`> :

- transformation des adresses électroniques pour éviter les faucheurs d’adresses ;
- transformation des oe appropriés (dans œil, œuvre, etc.) en « œ » ;
- intégration de la partie copyright et disclaimer en v.o. en plus de la v.f. conformément à la licence ;
- ajout de blancs insécables ( ) devant les ponctuations doubles ;
- transformations des guillemets en guillemets français "« " et " »" ;
- correction du lien vers la « collection des howto samba ».

B. GNU Free Documentation License

1. 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.

2. 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.

3. 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.

4. 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.

5. 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 [p 25] 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.

6. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 [p 22] 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".

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.