THEGREENBOW

TheGreenBow
VPN Linux Certified

Guide Administrateur

Table des Matières

1 Introduction

1.1 Présentation

Ce guide décrit les méthodes de déploiement, d'installation, de mise en œuvre et de configuration du logiciel Client VPN TheGreenBow VPN Linux Certified. Il s'adresse à l'administrateur du système d'information de l'entreprise.

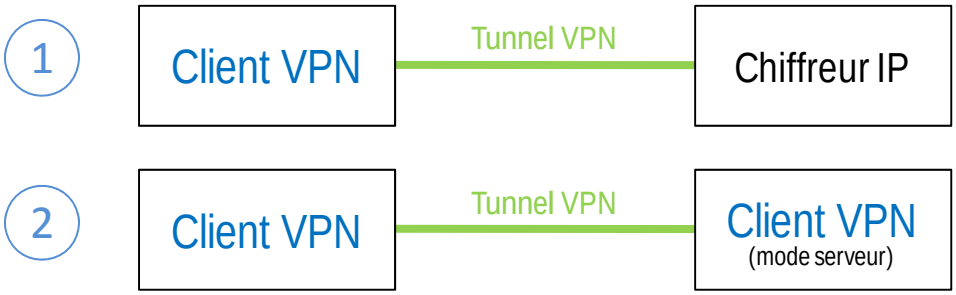
1.2 Références

Référence	Titre
[UG]	Documentation Strongswan (configuration de ipsec.conf et strongswan.conf) : tgbvlx_ug_strongswan.pdf
[RGS_B1]	RGS V2.0, Annexe B1. Mécanismes de cryptographie : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques V2.03
[RGS_B2]	RGS V2.0, Annexe B2. Gestion des clés cryptographiques : Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques V2.0
[RGS_B3]	RGS V2.0, Annexe B3. Règles et recommandations concernant les mécanismes d'authentification (1)
[ANSSI_IPSEC]	Recommandations de sécurité relatives à IPsec pour la protection des flux réseau Réf. DAT-NT-003/ANSSI/SDE version 1.1, 3 août 2015
[ANSSI_LINUX1]	Recommandations de configuration d'un système GNU/Linux DAT-NT-28/ANSSI/SDE/NP, 12 janvier 2016
[ANSSI_LINUX2]	Recommandations de sécurité relatives à un système GNU/Linux Réf. DAT-NT-002/ANSSI/SDE/NP, 27 juillet 2012
[GUIDE_DGAMI]	Recommandations pour la sécurisation des distributions GNU/Linux RedHat et Mandrake Réf. 2005/102317 / CELAR/SSI/SSY/EA / 51703616/NC V2.

2 TheGreenBow VPN Linux Certified

2.1 Présentation

Le logiciel TheGreenBow VPN Linux Certified est un logiciel VPN IPsec IKEv2 conçu et utilisé pour assurer la sécurité des communications entre un équipement mobile et une station fixe, ou entre deux équipements mobiles.



Le logiciel TheGreenBow VPN Linux Certified peut ainsi être mis en œuvre de deux façons :
1/ Client VPN initiateur de la connexion VPN
2/ Client VPN récepteur de la connexion VPN (mode serveur)

Le logiciel TheGreenBow VPN Linux Certified permet l'ouverture simultanée de plusieurs tunnels VPN.

2.2 Mise en œuvre et mode d'utilisation

Le logiciel TheGreenBow VPN Linux Certified est conçu et fourni pour s'exécuter en mode "embarqué".
Il ne propose pas d'interface d'administration qui permette la gestion de la configuration VPN (définition, modification, import, export) et ne propose pas non plus d'interface utilisateur qui permette à un utilisateur physique d'ouvrir ou de fermer un tunnel VPN.

Ainsi, les opérations d'administration du logiciel (déploiement, installation, mise à jour) sont du ressort de l'administrateur système et réseau. Les opérations de gestion de configuration VPN (définition, configuration, import) sont du ressort de l'administrateur sécurité.
Les opérations d'ouverture et de fermeture d'un tunnel VPN sont automatisées par des mécanismes logiciels externes au logiciel (applicatif, exécution de script ou mode d'ouverture automatique sur détection de trafic).

Ainsi, en utilisation nominale :
1/ le logiciel est démarré automatiquement en même temps que l'hôte/OS qui l'héberge
2/ lorsque le logiciel est en mode initiateur, les tunnels VPN sont ouverts automatiquement par mécanisme logiciel
3/ en mode serveur, le logiciel est en écoute permanente et finalise l'ouverture de la connexion VPN (le cas échéant, un mécanisme pourra être développé pour signifier graphiquement à l'utilisateur que le tunnel est ouvert).

2.3 Considérations de sécurité

Le logiciel TheGreenBow VPN Linux Certified s'appuie sur le logiciel opensource VPN Strongswan et implémente en standard les protocoles IKEv1, IKEv2. Toutefois, dans le cadre d'une utilisation en mode certifié, seul le protocole IKEv2 est mis en œuvre, conformément à la recommandation R8 de [ANSSI_IPSEC].

En standard, le logiciel TheGreenBow VPN Linux Certified permet d'établir des associations de sécurité sur la base de mécanismes d'authentification variés : clé partagée, utilisation de certificats aux formats X509, PKCS12 ou PEM.
Dans le cadre d'une utilisation en mode certifié, seule l'authentification par certificat est considérée dans le logiciel, conformément à [RGS_B2]. A noter que le mode EAP est exclu du logiciel TheGreenBow VPN Linux Certified.

Certificat

Le logiciel TheGreenBow VPN Certified permet l'utilisation de certificats, et en vérifie la validité, mais il ne permet pas leur génération. La génération des certificats, et en particulier la qualité et la conformité de ces certificats aux recommandations de l'ANSSI (RGS 2.0) est du ressort du Gestionnaire de l'IGC/PKI de l'entreprise concernée.
En particulier, il est recommandé que la durée de vie du certificat soit inférieure à 5 ans et que l'algorithme de signature du certificat soit d'une qualité suffisante.

2.4 Fourniture

Le logiciel TheGreenBow VPN Linux Certified est certifié et fourni pour les deux systèmes d'exploitation :
- Linux ELinOS 6.1 64 bits
- RedHat Enterprise Linux 7 64 bits

La livraison du logiciel n'inclut pas les systèmes d'exploitation.

Le logiciel TheGreenBow VPN Linux Certified est fourni sous la forme d'un package, contenant les binaires issus du code source, de l'environnement de développement et des options de compilations maîtrisés par TheGreenBow à l'exception du composant IPsec issu du noyau Linux.

OS Cible	Fourniture
ELinOS 6.1	tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz
RedHat 7	tgbvpn-linux-certified-X.Y.Z-0.el7.x86_64.rpm

Une fois installée, la commande « ipsec statusall » affiche le numéro de version de la TOE.

3 Installation

3.1 Installation ELinOS

3.1.1 Pré-requis

La fonctionnalité ELinOS "basic networking support" doit être activée.
Le noyau Linux ELinOS doit supporter "PF_KEY socket".
Le noyau Linux ELinOS doit supporter les fonctionnalités "TCP/IP Networking" suivantes : "IP tunneling", "Virtual (secure) IP : tunneling", "ESP transformation", "IP : IPComp transformation", "IP : IPsec tunnel mode", "INET : socket monitoring interface".
Le noyau Linux ELinOS doit supporter la fonctionnalité "Network packet filtering framework (Netfilter)". L'administrateur doit s'assurer de la bonne configuration du firewall et n'autoriser que les ports 500, 4500 ainsi que le protocole ESP pour le bon fonctionnement du VPN.
Le noyau Linux ELinOS doit supporter les fonctionnalités "Cryptographic API" suivantes : "GCM/GMAC support", "CTR support", "CMAC support", "HMAC support", "SHA224 and SHA256 digest algorithm", "SHA384 andSHA512 digest algorithms", "AES cipher algorithms (x86_64)", "AES cipher algorithms (AES-NI)", "Pseudo Random Number Generation for Cryptographic modules".

Pour vérifier, la présence des différentes fonctionnalités dans le noyau, il faut que les fonctionnalités « kernel config support » et « enable access to .config through /proc/config.gz » soit activées. Ces fonctionnalités sont accessibles dans « General setup ».

Il faut vérifier que le fichier /proc/config.gz existe et contient les directives suivantes :

- CONFIG_NET_KEY
- CONFIG_NET_IPIP
- CONFIG_INET_ESP
- CONFIG_INET_IPCOMP
- CONFIG_INET_XFRM_TUNNEL
- CONFIG_INET_TUNNEL
- CONFIG_INET_XFRM_MODE_TUNNEL
- CONFIG_NET_IP_TUNNEL
- CONFIG_NET_IPVTI
- CONFIG_NET_UDP_TUNNEL
- CONFIG_INET_XFRM_MODE_TUNNEL
- CONFIG_INET_DIAG
- CONFIG_INET_UDP_DIAG
- CONFIG_NETFILTER
- CONFIG_NETFILTER_ADVANCED
- CONFIG_NETFILTER_NETLINK
- CONFIG_CRYPTO
- CONFIG_CRYPTO_GCM
- CONFIG_CRYPTO_SEQIV
- CONFIG_CRYPTO_CBC
- CONFIG_CRYPTO_CTR
- CONFIG_CRYPTO_CMAC
- CONFIG_CRYPTO_HMAC
- CONFIG_CRYPTO_SHA256
- CONFIG_CRYPTO_SHA512
- CONFIG_CRYPTO_AES
- CONFIG_CRYPTO_AES_X86_64
- CONFIG_CRYPTO_AES_NI_INTEL
- CONFIG_CRYPTO_DEFLATE
- CONFIG_CRYPTO_ANSI_CPRNG
- CONFIG_CRYPTO_HW

3.1.2 Vérification d'intégrité

L'intégrité du package d'installation du logiciel TheGreenBow VPN Linux Certified pour ELinOS peut être vérifiée en suivant les étapes ci-dessous :

Importer la clé publique PGP disponible sur le serveur de clé par la commande :

```
$ gpg –-keyserver keys.gnupg.net –-recv-keys 2FE199A5
```

La clé peut aussi être recherchée manuellement par la commande :

```
$ gpg –-keyserver keys.gnupg.net –-search-keys linux@thegreenbow.com
```

Note : Le package d'installation du logiciel et l'empreinte du package d'installation sont fournis ensemble dans l'espace partenaire sécurisé accessible à l'utilisateur du produit. L'utilisateur doit disposer des fichiers suivants :

- tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz
- tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz.sig

Pour vérifier l'authenticité du signataire, il faut que les fichiers tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz et tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz.sig soient présents dans le même répertoire.
Il faut ensuite taper la commande :

```
$ gpg –-verify tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz.sig
```

La commande doit retourner les messages suivants :
- « les données signées sont supposées être dans « tgbvpn_linux_certified_elinos_X.Y.Z.tar.gz » »
- « Bonne signature de « TGB Linux product manager <linux@thegreenbow.com> » »

Note : A la fin de l'installation il est recommandé d'effacer la clé publique PGP TheGreenBow avec la commande :

```
$ gpg –-delete-key 2FE199A5
```

3.1.3 Installation

- Copier l'archive contenant le binaire sur la cible
- Se mettre à la racine : cd /
- Extraire l'archive : `tar xvzf chemin/tgbvpn_linux_certified_ELinOS_X.Y.Z.tar.gz`

Pour vérifier l'installation, saisir les commandes suivantes :

```
# ipsec start
# ipsec statusall
```

Le numéro de la version installée est indiqué lors de l'exécution de ces commandes. Exemple de logs :

```
Starting strongSwan 5.8.4 IPsec (TGB version 1.5.0) [starter]...
Status of IKE charon daemon (TGB version 1.5.0, strongSwan 5.8.4, Linux
3.10.0-1062.18.1.el7.x86_64, x86_64)
```

Contrairement à Red Hat, ELinOS ne dispose pas d'un gestionnaire de services comme systemd. Tenant compte du fait qu'ELinOS permet une grande finesse dans la composition de ses éléments, le lancement automatique est laissé à l'appréciation de l'administrateur. Il est cependant possible de configurer un démarrage automatique en suivant les étapes suivantes :

- Modifier /etc/inittab en ajoutant la ligne `tgb1:2345:wait:/etc/init.d/vlc start`
- Créer un fichier /etc/init.d/vlc sur le modèle de ceux déjà présents dans le répertoire :
  `cp /etc/init.d/devtmpfs /etc/init.d/vlc`
- Remplacer dans le fichier /etc/init.d/vlc le cas « start » par le code suivant :

```
start)
echo 'starting tgbvpn_linux_certified... '

while [ ! -c /dev/random -a ! -b /dev/random ]
do
```

```
        echo 'No file /dev/random. Waiting.'
        sleep 1
    done

    /usr/sbin/ipsec start
    echo 'done.'
    ;;
```

- Remplacer dans le fichier /etc/init.d/vlc le cas « stop » par le code suivant :

```
stop)
echo 'stopping tgbvpn_linux_certified... '
/usr/sbin/ipsec stop
echo 'done.'
;;
```

- Remplacer dans le fichier /etc/init.d/vlc les occurrences devtmpfs par vlc
- Redémarrer la VM

Le client a besoin de certaines fonctionnalités présentes dans le noyau pour pouvoir fonctionner (cf. section 3.1.1). Ces fonctionnalités peuvent être présentes sous la forme de modules et ne pas être intégrées dans le noyau. Dans ce cas, il faut charger les modules avec la commande « `insmod` ». Il faudra donc ajouter dans le script « `/usr/sbin/vlc` » des lignes du type « `insmod /lib/modules/4.1.36-ElinOS-709-rt42/kernel/*/module.ko` » avant « `/usr/sbin/ipsec start` ».

Par exemple, si l'administrateur a compilé le noyau avec la fonctionnalité cryptographique CONFIG_CRYPTO_CTR sous la forme d'un module, il faudra ajouter la ligne suivante avant « `/usr/sbin/ipsec start` » :

```
insmod /lib/modules/4.1.36-ELinOS-709-rt42/kernel/crypto/ctr.ko
```

Si cette fonctionnalité est intégrée dans le noyau, la ligne précédente n'a pas besoin d'être ajoutée.

Le code ci-dessous permet de générer le script « `modules.sh` » qui lancera toutes les commandes insmod nécessaires au chargement de tous les modules compilés:

```
#!/bin/sh

echo "This script read /lib/modules/4.1.36-ELinOS-709-rt42/modules.order content
and generate modules.sh that insert in the kernel all the generated modules"
echo "#!/bin/sh" > modules.sh
sed -e 's/^kernel/insmod \/lib\/modules\/4.1.36-ELinOS-709-rt42\/kernel/'
/lib/modules/4.1.36-ELinOS-709-rt42/modules.order >> modules.sh
echo "run : sh modules.sh"
```

Le script « `modules.sh` » peut ensuite être intégré dans « `/etc/init.d/vlc` » en le lançant juste avant « `ipsec start` » comme dans l'exemple ci-dessous :

```
    sh /home/elinos/modules.sh
    /usr/sbin/ipsec start
    echo 'done.'
    ;;
```

Pour garantir une source d'entropie forte, il est nécessaire d'avoir des scripts qui gardent l'alea à chaque redémarrage du système. Pour ce faire, ajoutez les lignes suivantes dans le script /etc/init.d/vlc dans le cas start avant le lancement du client VPN. Il sera exécuté pendant la séquence de démarrage du système :

```
echo "Initializing random number generator..."
RANDOM_SEED=/var/run/random-seed
if [ -f $RANDOM_SEED ] ; then
    cat $RANDOM_SEED > /dev/urandom
else
    echo "" > $RANDOM_SEED
fi
test -f $RANDOM_SEED && chmod 600 $RANDOM_SEED
POOLSIZE=/proc/sys/kernel/random/poolsize
[ -r POOLSIZE ] && BYTES=`cat $POOLSIZE` || BYTES=512
dd if=/dev/urandom of=$RANDOM_SEED count=1 bs=$BYTES
```

Le script suivant doit être mis dans /etc/init.d/vlc dans le cas stop qui est exécuté à l'arrêt du système.

```
echo "Saving random seed..."
RANDOM_SEED=/var/run/random-seed
test -f $RANDOM_SEED || echo "" > $RANDOM_SEED
test -f $RANDOM_SEED && chmod 600 $RANDOM_SEED
POOLSIZE=/proc/sys/kernel/random/poolsize
[ -r POOLSIZE ] && BYTES=`cat $POOLSIZE` || BYTES=512
dd if=/dev/urandom of=$RANDOM_SEED count=1 bs=$BYTES
```

3.2 Installation RedHat

3.2.1 Pré-requis

Sous RedHat, se loguer sur le poste en tant qu'administrateur et ouvrir les ports UDP 500 et 4500 avec les commandes :

```
firewall-cmd --permanent --zone=public --add-port=500/udp
firewall-cmd --permanent --zone=public --add-port=4500/udp
firewall-cmd --permanent --zone=public --add–rich-rule=’rule protocol value="esp"
accept’
firewall-cmd --reload
```

Mettre zone à "public" si l'interface est publique.

3.2.2 Vérification d'intégrité

L'intégrité du package d'installation du logiciel TheGreenBow VPN Linux Certified pour RedHat peut être vérifiée de la façon suivante :

Récupérer la clé publique depuis le serveur de clé par la commande :

```
gpg –-keyserver keys.gnupg.net –-recv-keys 2FE199A5
```

Sauver la clé publique PGP téléchargée dans un fichier :

```
gpg –-armor –-export 2FE199A5 > tgb_linux_product_manager.pgp
```

Importer la clé publique PGP dans la base de données RPM par la commande :

```
rpm --import tgb_linux_product_manager.pgp
```

Note : La liste des clefs PGP de la base de données RPM est accessible avec la commande :

```
rpm -qa gpg-pubkey*
```

Vérifier la signature par la commande :

```
rpm -K tgbvpn-linux-certified-X.Y.Z-0.el7.x86_64.rpm
```

Note : A la fin de l’installation il est recommandé d’effacer la clé publique PGP TheGreenBow avec la commande :

```
rpm -e gpg-pubkey-2fe199a5-5b968017
```

3.2.3 Installation

Le logiciel TheGreenBow VPN Linux Certified ne peut être installé en même temps que le package libreswan. Pour supprimer ce package, lancer la commande suivante en tant qu'administrateur :

```
yum remove libreswan
```

Pour installer le Client VPN, lancer la commande suivante en tant qu’administrateur :

```
rpm -i tgbvpn-linux-certified-X.Y.Z-0.el7.x86_64.rpm
```

Les distributions Red Hat disposent d’un gestionnaire de services appelé systemd. Celui-ci permet de démarrer automatiquement des applications serveurs, de les arrêter ou de les redémarrer après modification de paramètres de configuration. Le package d’installation ajoute automatiquement les fichiers nécessaires au lancement automatique du client VPN.

La commande suivante permet de vérifier le lancement du logiciel.

```
# systemctl status strongswan-starter.service
```

Les distributions Red Hat disposent d'un outil de contrôle de l'accès au système de fichiers appelé SELinux. Celui-ci doit être configuré de manière à pouvoir monter des tunnels.

Après installation et lancement du client VPN, taper les commandes suivantes :

```
ausearch -c 'charon' --raw | audit2allow -M my-charon
semodule -i my-charon.pp
ipsec restart
```

Si après redémarrage du poste, l'utilisateur ne peut monter un tunnel ou doit saisir la commande "ipsec restart", vérifier si le blocage ne vient pas de SELINUX. Taper la commande suivante pour le vérifier :

```
ausearch –m avc ---start recent
```

Si les logs confirment l'interdiction d'accès à un fichier par SELINUX, réexécuter les commandes suivantes :

```
ausearch -c 'charon' --raw | audit2allow -M my-charon
semodule -i my-charon.pp
ipsec restart
```

Pour garantir une source d'entropie forte, il est nécessaire d'avoir des scripts qui gardent l'alea à chaque redemarage du systeme.
Pour ce faire, mettre les lignes suivantes dans le script /usr/sbin/seed_load.sh :

```
#!/bin/bash
echo "Initializing random number generator..."
SEED_DIR=/var/spool/seed
test -d $SEED_DIR || mkdir -p $SEED_DIR
test -d $SEED_DIR && chmod 750 $SEED_DIR

# Carry a random seed from start-up to start-up
# Load and then save the whole entropy pool
RANDOM_SEED=$SEED_DIR/random-seed
if [ -f $RANDOM_SEED ]; then
    cat $RANDOM_SEED > /dev/urandom
else
    touch $RANDOM_SEED
fi
chmod 600 $RANDOM_SEED
POOLFILE=/proc/sys/kernel/random/poolsize
[ -r $POOLFILE ] && BYTES=`cat $POOLFILE` || BYTES=512
dd if=/dev/urandom of=$RANDOM_SEED count=1 bs=$BYTES
Mettre les lignes suivantes dans le script /usr/sbin/seed_save.sh :
```

Mettre les lignes suivantes dans le fichier /usr/sbin/seed_save.sh

```
#!/bin/bash
# Carry a random seed from shut-down to start-up
# Save the whole entropy pool
echo "Saving random seed..."
SEED_DIR=/var/spool/seed
test -d $SEED_DIR || mkdir -p $SEED_DIR
test -d $SEED_DIR && chmod 750 $SEED_DIR
RANDOM_SEED=$SEED_DIR/random-seed
test -f $RANDOM_SEED || touch $RANDOM_SEED
chmod 600 $RANDOM_SEED
POOLFILE=/proc/sys/kernel/random/poolsize
[ -r $POOLFILE ] && BYTES=`cat $POOLFILE` || BYTES=512
dd if=/dev/urandom of=$RANDOM_SEED count=1 bs=$BYTES
```

Créer le fichier /lib/systemd/system/random_seed.service avec le contenu suivant :

```
[Unit]
Description=Random seed backup and restore

[Service]
Type=oneshot
ExecStart=/usr/sbin/seed_load.sh
ExecStop=/usr/sbin/seed_save.sh
RemainAfterExit=yes

[Install]
WantedBy=multi-user.target
```

Lancer les commandes suviantes :

```
chmod 750 /usr/sbin/seed_load.sh
chmod 750 /usr/sbin/seed_save.sh
systemctl enable random_seed.service
```

4 Configuration

4.1 Fichier /etc/vpn/ipsec.conf

Editer en tant qu'administrateur le fichier avec un éditeur de texte comme nano ou vi.
Ce fichier contient les tunnels à monter ou à fermer. Un tunnel de base a la forme suivante :

```
conn tunnel
      left=192.168.32.3
      leftsubnet=192.168.56.0/24
      leftid= « C=FR, L=Paris, O=TheGreenBow, OU=support, CN=Utilisateur1,
E=utilisateur@thegreenbow.com »
      leftfirewall=yes
      right=%any
      authby=pubkey
      rightsourceip=10.10.20.1/16
      keyexchange=ikev2
      ike=aes256-sha384-modp2048!
      esp=aes128-sha2_256-modp2048!
      auto=add
      dpdaction=clear
      dpddelay=30
      lifetime=20m
      ikelifetime=25m
      rekey=yes
      forceencaps=yes
```

Un tunnel doit commencer par le paramètre « conn ». Le libellé suivant ce paramètre est le nom du tunnel qui pourra être utilisé pour monter ou fermer la connexion.

Principaux paramètres :

Paramètre	Description	Valeur(s) recommandée(s)
Left	Adresse IP du client	
leftsourceip	Adresse IP récupérée de la passerelle	%config4
leftid	Identifiant du client	Sujet du certificat du client
right	Adresse IP ou adresse DNS de la passerelle	
authby	Méthode d'authentification	pubkey
rightid	Identifiant de la passerelle suivante	Sujet du certificat de la passerelle
rightsubnet	Plage d'adresses accessibles derrière la passerelle	0.0.0.0
keyexchange	Type d'échange IKE	(obligatoire, non modifiable) ikev2
ike	Propositions d'algorithmes pour la phase IKE SA. Le format suit la syntaxe suivante : encryptionalgo-integrityalgo-diffiehellmangroup	aes256-sha2_256-modp2048 Cf. liste complète des algorithmes disponibles ci-dessous
esp	Propositions d'algorithmes pour la phase CHILD_SA. Le format suit la syntaxe suivante : encryptionalgo-integrityalgo-diffiehellmangroup	aes256-sha2_256-modp2048 Cf. liste complète des algorithmes disponibles ci-dessous
auto	Mode de démarrage de la connexion	add : attente connexion entrante route : montée sur détection de trafic start : montée du tunnel au démarrage
dpdaction	Action à entreprendre en cas de fin de détection de DPD	clear
dpddelay	Intervalle de temps entre les messages R_U_THERE	
ikelifetime	Durée de vie de phase IKE SA	

lifetime	Durée de vie de la phase CHILD SA	
rekey	Renégociation après la fin d'une durée de vie	yes
forceencaps	Force l'encapsulation UDP pour les paquets ESP. Cette option est recommandée afin de passer au travers des pare-feux qui n'acceptent pas les paquets ESP strictement au-dessus de la couche IP.	yes

Les algorithmes de chiffrement possibles sont : aes128, aes192, aes256, aes128ctr, aes192ctr, aes256ctr, aes128gcm16, aes192gcm16, aes256gcm16.
Les algorithmes d'intégrité possibles sont : sha256 ou sha2_256, sha384, sha2_384, sha512, sha2_512.
Les algorithmes Diffie-Hellman possibles sont : modp2048, modp3072, modp4096, modp6144, modp8192, ecp256, ecp384, ecp521.

Pour le choix des algorithmes, se reporter à la section 6 « Recommandations de sécurité ».

Il est recommandé d'ajouter le caractère ' !' à la fin des propositions d'algorithmes définies pour IKE et ESP. Sans ce caractère '!', des algorithmes potentiellement non souhaités peuvent être ajoutés à la proposition. L'ajout du caractère '!' garantit que la proposition d'algorithmes qui le précède est bien celle qui est utilisée.

Pour le détail des paramètres de configuration, consulter la section 2 du document tgbvlx_ug_strongswan.doc

4.2 Fichier /etc/vpn/ipsec.secrets

Le fichier associe un identifiant avec un secret. Un identifiant peut être une adresse IP, un FQDN, une adresse électronique, un sujet de certificat ou %any ou %any6.

Note : Le fichier ne peut être lu qu'en tant qu'administrateur.

Le format d'une ligne du fichier ipsec.secrets est :

```
<id1> : SECRET <fichier> [ <mot_de_passe> | %prompt ]
```

Les types de secrets recommandés sont RSA et P12.
Le format des différents est présenté dans le tableau suivant :

Type de secret	Format
RSA	: RSA <fichier_clef_privée> [<mot_de_passe> | %prompt]
P12	: P12 <*fichier_PKCS#12*> [<mot_de_passe> | %prompt]
ECDSA	: ECDSA <*fichier_clef_privée*> [<mot_de_passe> |% prompt]

Exemple pour un fichier P12 :
"C=FR, L=Bordeaux, O=TGB, OU=Ventes, CN=utilisateur, E=utilisateur@tgb.com" : P12 B10001.p12 thegreenbow

4.3 Répertoire /etc/vpn/ipsec.d

Le répertoire contient les certificats utilisés par le client. Les principaux répertoires sont :

Répertoire	Description
private	Contient les clefs privées RSA. Si un fichier P12 avec clef privée est utilisé, il doit être mis ici. L'accès à ce répertoire doit être limité à l'utilisateur root.
Cert	Contient les clefs publiques RSA des certificats
cacerts	Contient les certificats racines
Crls	Contient les listes de révocation au format binaire ou PEM

Lors de l'utilisation de certificats P12 avec la clef privée, il faut mettre le fichier dans le répertoire /etc/vpn/ipsec.d/private.

4.4 Fichier strongswan.conf

Le fichier /etc/vpn/strongswan.conf décrit des paramètres globaux additionnels. Il peut inclure d'autres fichiers annexes pour faciliter son administration. Ces fichiers sont positionnés dans le répertoire /etc/vpn/strongswan.d/

Le détail des paramètres de strongswan.conf est décrit dans la section 3 du document tgbvlx_ug_strongswan.doc

L'adminstrateur peut activer des logs lui permettant de résoudre des problèmes de connexion. Par défaut, il existe le fichier /etc/vpn/strongswan.d/charon-logging.conf pour y définir la génération de log.

La configuration ci-dessous peut être utilisée :

```
charon {
    filelog {
        charon {
            path = /var/log/tgbvlc/charon.log
            time_format = %d %e %T
            ike_name = yes
            append = no
            default = 1
            flush_line = yes
            time_add_ms = yes
        }
    }
}
```

Le fichier de log est réinitialisé lors du redémarrage du daemon IKE

4.5 Ligne de commande

Toute modification de la configuration ne sera pas prise en compte tant que le daemon IKE ne sera pas redémarré. La commande de redémarrage est :

```
# ipsec restart
```

La commande permettant de monter un tunnel est :

```
# ipsec up <nom_du_tunnel>
```

La commande permettant de fermer un tunnel est :

```
# ipsec down <nom_du_tunnel>
```

5 Désinstallation

5.1 Désinstallation ELinOS

- Supprimer le répertoire /etc/vpn
- Supprimer /usr/libexec/ipsec
- Supprimer /usr/lib/ipsec/
- Supprimer /usr/sbin/ipsec
- Supprimer /usr/share/strongswan
- Supprimer /usr/share/man/man5/ipsec.conf.5, /usr/share/man/man5/ipsec.secret.5 et /usr/share/man/man5/strongswan.conf.5
- Supprimer /usr/share/man/man8/ipsec.8

```
#!/bin/sh

rm -r /etc/vpn
rm -r /usr/lib/ipsec
rm -r /usr/libexec/ipsec
rm -r /usr/sbin/ipsec
rm -r /usr/share/strongswan
rm /usr/share/man/man5/ipsec.conf.5 /usr/share/man/man5/ipsec.secret.5
/usr/share/man/man5/strongswan.conf.5
rm /usr/share/man/man8/ipsec.8
```

5.2 Désinstallation RedHat

Pour la désinstallation, lancer la commande : yum remove tgbvpn-linux-certified

La commande de désinstallation ne supprime pas les certificats et les clefs qui peuvent avoir été copiés après l'installation du package. Il faut supprimer le répertoire avec la commande suivante : rm -rf /etc/vpn

6 Recommandations de sécurité

6.1 Certification

Le logiciel Client VPN TheGreenBow VPN Linux Certified est le premier Client VPN IPsec Linux certifié selon les Critères Communs au niveau EAL3+, et qualifié au niveau standard.

Le logiciel Client VPN TheGreenBow VPN Linux Certified est certifié sur les plates-formes ELinOS 6.1 64 bit et RedHat Entreprise Linux 7 64 bit.

La version du logiciel Client VPN TheGreenBow VPN Linux Certified objet de ce guide utilisateur est la version 1.5.

6.2 Recommandations

Les recommandations suivantes s'adressent à l'Administrateur du logiciel.

6.2.1 Recommandations générales

Afin de garantir un niveau de sécurité approprié, les conditions de mise en œuvre et d'utilisation suivantes doivent être respectées :

- L'administrateur système et l'administrateur sécurité chargés respectivement de l'installation du logiciel et de la définition des politiques de sécurité VPN sont considérés de confiance.
- L'utilisateur du logiciel est une personne formée à son utilisation. En particulier, elle ne doit pas divulguer les informations utilisées pour son authentification auprès du système de chiffrement.
- La passerelle VPN à laquelle se connecte le Client VPN permet de tracer l'activité VPN et permet de remonter le cas échéant les dysfonctionnements ou les violations des politiques de sécurité.
- Le poste de l'utilisateur est sain et correctement administré. Il est protégé par un pare-feu.
- Les bi-clés et les certificats utilisés pour ouvrir le tunnel VPN, sont générés par une autorité de certification de confiance.

6.2.2 Précaution de mise en œuvre

La machine sur laquelle est installé et exécuté le logiciel Client VPN TheGreenBow doit être saine et correctement administrée. En particulier :

1/ Elle est protégée par un pare-feu qui permet de maîtriser (cloisonner ou filtrer) les communications entrantes et sortantes du poste qui ne passent pas par le Client VPN,
2/ Son système d'exploitation est à jour des différents correctifs
3/ Sa configuration permet d'éviter les attaques menées localement (analyse de la mémoire, patch ou corruption de binaire).

Des recommandations de configuration pour durcir le poste de travail sont disponibles sur le site de l'ANSSI, par exemple (sans que cette liste ne soit exhaustive) :
Guide d'hygiène informatique
Guide de configuration
Mises à jour de sécurité
Mot de passe

En particulier, il est recommandé de mettre en place une politique de filtrage des flux entrants sur le poste sur lequel est installé le Client VPN, de manière à interdire les accès distants au logiciel.

6.2.3 Administration du Client VPN

Il est recommandé de veiller à ce que les utilisateurs utilisent le Client VPN dans un environnement "utilisateur", et d'essayer autant que possible, de limiter l'utilisation du système d'exploitation avec des droits administrateur.

6.2.4 Configuration de la politique de sécurité VPN

Authentification de l'Utilisateur

Seule l'authentification par Certificat est supportée par le Client VPN TheGreenBow.

Authentification de la Passerelle VPN

La vérification du certificat de la Passerelle VPN est faite par défaut.

Protocole IKE

La certification du logiciel TheGreenBow VPN Linux Certified porte sur le protocole IKEv2 exclusivement.
Le protocole IKEv1 n'est pas disponible à l'utilisation

Algorithmes cryptographiques et longueur de clés

Pour utiliser le logiciel TheGreenBow VPN Linux Certified conformément à l'annexe B-1 du RGS 2.0, il est recommandé de choisir les algorithmes suivants :

IKEv2	Chiffrement	AES128 minimum, AES192 ou AES256
	Authentification	SHA2 256 minimum, ou SHA2 384 ou SHA2 512
	Groupe de clé	DH14 (MODP 2048) minimum ou DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521)
ESP	Chiffrement	AES128 minimum, AES192 ou AES256
	Intégrité	SHA2 256 minimum, ou SHA2 384 ou SHA2 512
	Diffie-Hellman	DH14 (MODP2048) minimum ou DH15 (MODP 3072), DH16 (MODP 4096), DH17 (MODP 6144), DH18 (MODP 8192), DH19 (ECP 256), DH20 (ECP 384), DH21 (ECP 521)

Certificat

Le logiciel TheGreenBow VPN Linux Certified permet l'utilisation de certificats, et en vérifie la validité, mais il ne permet pas leur génération. La génération des certificats, et en particulier la qualité et la conformité de ces certificats aux recommandations de l'ANSSI (RGS 2.0) est du ressort du Gestionnaire de l'IGC/PKI de l'entreprise concernée.
En particulier, il est recommandé que la durée de vie du certificat soit inférieure à 5 ans et que l'algorithme de signature du certificat soit d'une qualité suffisante.
Les certificats manipulés par le Client VPN doivent posséder des dates de validité au format UTCTime.

CRL

Par défaut, lorsqu'une CRL est configurée mais qu'elle ne peut être récupérée, le tunnel se monte quand-même. Cette configuration permet d'éviter une attaque par déni de service.
Toutefois, il est possible dans ce cas de monter un tunnel avec un certificat révoqué. Ce comportement peut être évité en passant le paramètre "strictcrlpolicy" à "yes" dans le fichier "ipsec.conf". Dans ce cas, le tunnel ne se monte pas si la CRL ne peut être récupérée.

Recommandation : dans le cadre de l'utilisation du logiciel en "mode certifié" et pour garantir un accès fiable aux CRLs, il est recommandé d'avoir ces CRLs en local et non hébergées sur un serveur (Cf. chapitre 4.3 "Répertoire /etc/vpn/ipsec.d"). Le type d'accès aux CRLs est configuré dans les certificats, il est de la responsabilité de l'administrateur (en particulier de l'administrateur de l'IGC) de configurer les certificats de cette façon.

Recommandations de configuration IPsec de l'ANSSI

Les recommandations décrites ci-dessus peuvent être complétées par le document de configuration IPsec rédigé par l'ANSSI : Recommandations de sécurité relatives à IPsec pour la protection des flux réseau.

7 FAQ, troubleshooting

Ce chapitre présente la liste des problèmes fréquemment rencontrés, ainsi que leur résolution.
Consulter le site : http://www.thegreenbow.fr/vpn_faq.html pour avoir la dernière version de cette liste.

7.1 Client VPN TheGreenBow

7.1.1 Quels sont les passerelles/routeurs VPN compatibles ?

Le client de TheGreenBow IPsec VPN est compatible avec tous les routeurs IPsec conformes aux normes IKE et IPsec. Visitez la liste des routeurs VPN qualifiés, qui augmente chaque jour, pour trouver votre routeur VPN.

Si l'équipement que vous recherchez n'est pas contenu dans cette liste, contactez notre support technique et nous travaillerons avec vous pour le qualifier.

7.1.2 Le NAT Traversal est il supporté par le Client VPN ?

Oui. Le Client VPN TheGreenBow supporte NAT Traversal full implementation, incluant NAT keepalive

7.1.3 Le Client VPN TheGreenBow supporte-t il DNS/WINS discovering ?

Le Client VPN TheGreenBow supporte le Mode-Config. Le "Mode Config" est une extension de Internet Key Exchange (IKE) qui permet de récupérer certains paramètres réseau comme les adresses IP des serveurs DNS/WINS depuis la gateway distante et de les utiliser dans la configuration VPN du Client VPN. Si le "Mode Config" n'est pas supporté par la gateway distante, le Client VPN permet aussi la configuration manuelle des serveurs DNS/WINS de l'entreprise.

7.1.4 Quels ports sont utilisés par le Client VPN TheGreenBow ?

Les ports UDP 500 et UDP 4500 doivent être ouverts et le protocole ESP (protocol number 50) doit être autorisé.

7.1.5 Est-il possible d'avoir des licences temporaires pour test ?

TheGreenBow peut fournir des licences temporaires permettant de poursuivre les tests du logiciel au delà de la période d'évaluation de 30 jours. Ces licences temporaires peuvent durer plusieurs semaines. Pour plus de détails, contacter notre équipe commerciale.

7.1.6 Le Client VPN est-il compatible avec les moyens d'authentification à deux facteurs ?

Oui. Le Client VPN TheGreenBow est compatible avec les fonctions d'authentification à deux facteurs et bidirectionnelle pour stocker les utilisateurs, les qualifications personnelles telles que des clefs privées, des mots de passe et des certificats numériques. Veuillez vous référer à la liste des Tokens qualifiés.

7.1.7 Configurer une connexion VPN dans un hôtel ou vers une borne wifi

Pour plus d'informations sur la négociation de NAT Transversal dans IKE, voir IETF RFC 3948 (UDP Encapsulation of IPsec Packets), IETF RFC 3947 (Negotiation of NAT-Traversal in the IKE). Regarder aussi la liste des ports TCP et UDP.

Les ports par défaut sont modifiables avec le paramètre rightikeport dans /etc/vpn/ipsec.conf

Dans certains hôtels, points wifi ou aéroports, les ports UDP 500 et 4500 pour le trafic sortant peuvent être bloqués, pour empêcher toute connexion étrangère à votre réseau. Il est donc nécessaire de configurer les ports IKE en conséquence.

7.1.8 Le Client VPN supporte-t-il SHA-2 ?

Le Client VPN TheGreenBow supporte SHA-1 et SHA-2 256 bit.

7.2 Troubleshootings

7.2.1 Erreur de configuration

En cas d'utilisation d'un paramètre non reconnu dans le fichier de configuration ipsec.conf, le Client VPN affiche un message d'erreur au démarrage :

```
# bad value: authby=psk
  bad argument value in conn 'tgbtest'
# ignored conn 'tgbtest' due to 1 parsing error
### 1 parsing error (0 fatal) ###
```

La connexion fautive (parameter conn) n'est pas prise en compte. Si le fichier de configuration contient d'autres connexions dont la syntaxe est correcte, ces connexions peuvent être lancées. Pour vérifier les connexions disponibles, lancer la commande suivante.

```
ipsec statusall
```

7.2.2 Module non chargé

Si au cours de la montée du tunnel, le message « Function not implemented » apparait, cela signifie qu'un module du noyau linux n'est pas chargé.

Exemple :

```
installing new virtual IP 10.10.20.1
received netlink error: Function not implemented (38)
unable to add SAD entry with SPI ce0699b5 (FAILED)
received netlink error: Function not implemented (38)
unable to add SAD entry with SPI c5f8555b (FAILED)
unable to install inbound and outbound IPsec SA (SAD) in kernel
failed to establish CHILD_SA, keeping IKE_SA
```

Il faut charger le module correspondant avec la commande insmod :

```
insmod /lib/modules/<chemin d'accès>/nomdumodule.ko
```

7.2.3 No response from the VPN server

Les traces suivantes indiquent que le routeur VPN distant ne répond pas aux requêtes IKE du Client VPN.

```
generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(FRAG_SUP)
N(HASH_ALG) N(REDIR_SUP) ]
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
retransmit 1 of request with message ID 0
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
retransmit 2 of request with message ID 0
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
retransmit 3 of request with message ID 0
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
retransmit 4 of request with message ID 0
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
retransmit 5 of request with message ID 0
sending packet: from 192.168.0.234[500] to 192.168.0.22[500] (1184 bytes)
giving up after 5 retransmits
```

Vérifier dans les traces du routeur VPN distant si les requêtes du Client VPN sont bien reçues. Si ce n'est pas le cas, cela signifie que les requêtes du Client VPN ont été perdues, ou filtrées par un logiciel ou un équipement de type firewall. Vérifier alors les règles des Firewalls (incluant le Firewall éventuellement installé sur la machine) qui peuvent être situés entre le Client VPN et le routeur VPN.

7.2.4 Authentication failed

Les traces suivantes indiquent que le routeur VPN n'a pu authentifier le Client VPN :

```
[ENC] generating IKE_AUTH request 1 [ IDi CERT CERTREQ AUTH CPRQ(ADDR DNS) SA TSi
TSr N(MOBIKE_SUP) N(ADD_4_ADDR) N(ADD_4_ADDR) N(ADD_6_ADDR) N(ADD_6_ADDR)
N(MULT_AUTH) N(EAP_ONLY) N(MSG_ID_SYN_SUP) ]
[ENC] splitting IKE message with length of 2152 bytes into 2 fragments
[ENC] generating IKE_AUTH request 1 [ EF(1/2) ]
[ENC] generating IKE_AUTH request 1 [ EF(2/2) ]
[NET] sending packet: from 192.168.0.234[4500] to 192.168.0.22[4500] (1244 bytes)
[NET] sending packet: from 192.168.0.234[4500] to 192.168.0.22[4500] (988 bytes)
[NET] received packet: from 192.168.0.22[4500] to 192.168.0.234[4500] (88 bytes)
[ENC] parsed IKE_AUTH response 1 [ N(AUTH_FAILED) ]
```

Plusieurs points peuvent être à l'origine de cette erreur. :

- Vérifier dans /etc/vpn/ipsec.conf que le paramètre « authby » est bien à « rsasign » ou « pubkey »
- Vérifier dans /etc/vpn/ipsec.conf que la valeur du paramètre « leftid » est aussi présente dans /etc/vpn/ipsec.secrets et que cette valeur est associée à un certificat existant

7.2.5 Tunnel VPN ouvert mais le ping ne fonctionne pas

Si vous avez les traces suivantes, le tunnel VPN IPsec est établi. Vous devriez pouvoir faire un ping sur n'importe quel adresse du réseau LAN. La configuration du Client VPN TheGreenBow est correct dans ce cas.

```
authentication of 'CN=130.255.153.70, unstructuredName=130.255.153.70,
unstructuredAddress=130.255.153.70' with RSA signature successful
IKE_SA test[2] established between 192.168.0.234[CN=tgb-test-
user]...130.255.153.70[CN=130.255.153.70, unstructuredName=130.255.153.70,
unstructuredAddress=130.255.153.70]
scheduling reauthentication in 9880s
maximum IKE_SA lifetime 10420s
installing new virtual IP 192.168.20.1
received ESP_TFC_PADDING_NOT_SUPPORTED, not using ESPv3 TFC padding
CHILD_SA test{1} established with SPIs c86b5106_i d777b047_o and TS
192.168.20.1/32 === 0.0.0.0/0
connection test established successfully
```

Si vous ne pouvez toujours pas "pinguer" le réseau LAN distant, voici quelques directives :

- Une fois le tunnel ouvert, des paquets sont envoyés avec le protocole ESP. Ce protocole peut être bloqué par un Firewall. Vérifiez que chaque élément entre le client et le serveur VPN accepte ESP
- Vérifiez vos traces de serveur VPN. Des paquets peuvent être éliminés par une des règles du Firewall.
- Vérifiez que votre FAI support ESP. Les principaux le supportent.
- Si vous ne pouvez toujours pas faire de ping, suivez le trafic ICMP sur l'interface LAN du serveur VPN et sur l'interface LAN de l'ordinateur (avec Ethereal par exemple). Vous aurez une indication que le chiffrement fonctionne.
- Vérifiez le routeur "par défaut" dans la configuration LAN du serveur VPN. Une cible sur votre LAN distant peut recevoir des ping mais ne répond pas parce qu'il n'y a pas de routeur "par défaut" configuré.
- Vous ne pouvez pas accéder aux ordinateurs par leur nom dans le LAN. Vous devez indiqué leur adresses IP à l'intérieur du LAN.

8 Contact

8.1 Information

Toutes les informations sur les produits TheGreenBow sont disponibles sur les sites :
Anglais : www.thegreenbow.com
Français : www.thegreenbow.fr

8.2 Commercial

Contact téléphonique : +33.1.43.12.39.30
Contact mail : sales@thegreenbow.com

8.3 Support

Les sites TheGreenBow proposent plusieurs pages concernant le support technique des logiciels :

Support

Anglais : http://www.thegreenbow.com/support.html
Français : http://www.thegreenbow.fr/support.html

Aide en ligne

Anglais : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=en
Français : http://www.thegreenbow.com/support_flow.html?product=vpn&lang=fr

FAQ

Anglais : http://www.thegreenbow.com/vpn_faq.html
Français : http://www.thegreenbow.fr/vpn_faq.html

Contact

Le support technique est accessible via les formulaires disponibles sur le site TheGreenBow ou directement par email à l'adresse : support@thegreenbow.com

9 Annexes

9.1 Empreinte clé GPG

L'empreinte de la clef GPG utilisée pour signer les différents packages est la suivante :

EF44 CB41 7249 358E 2A97 8942 4503 8D5E 2FE1 99A5

Note : L'empreinte peut être vérifiée avec les commandes :

```
gpg –-keyserver keys.gnupg.net –-recv-keys 2FE199A5
```

```
gpg –-fingerprint 2FE199A5
```

9.2 GNU General Public License, version 2

- The latest version of the GPL, version 3
- What to do if you see a possible GPL violation
- Translations of GPLv2
- GPLv2 Frequently Asked Questions
- The GNU General Public License version 2 (GPLv2) in other formats: plain text, Texinfo, LaTeX, standalone HTML, Docbook, Markdown, ODF, RTF

9.2.1 Table of Contents

9.2.2 GNU GENERAL PUBLIC LICENSE

```
Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies
of this license document, but changing it is not allowed.
```

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the

software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.
Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.
The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program 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.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.
7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public 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.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

```
one line to give the program's name and an idea of what it does.
Copyright (C) yyyy  name of author

This program is free software; you can redistribute it and/or
modify it under the terms of the GNU General Public License
as published by the Free Software Foundation; either version 2
of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
GNU General Public License for more details.

You should have received a copy of the GNU General Public License
along with this program; if not, write to the Free Software
Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA  02110-1301, USA.
```

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

```
Gnomovision version 69, Copyright (C) year name of author
```

```
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details
type `show w'.  This is free software, and you are welcome
to redistribute it under certain conditions; type `show c'
for details.
```

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

```
Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989
Ty Coon, President of Vice
```

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

THEGREENBOW

Secure, Strong, Simple

TheGreenBow Security Software