

SecureBlue avec des applis compartimentées

Difficulté ★★☆☆★ Temps requis 🕒 1h

Objectif

Faire tourner chaque application dans sa propre machine virtuelle sur SecureBlue, pour séparer tes usages numériques



Étapes

- [keyboard_arrow_right](#) Installer l'outil
- [keyboard_arrow_right](#) Créer les bases et les compartiments dont tu as besoin
- [keyboard_arrow_right](#) Paramétrer chaque compartiment : réseau, chiffrement, stockage

✓ Prérequis

- [task](#) [Ordi secureblue](#)
- [task](#) Savoir utiliser un terminal

📦 Matériel requis

- [sell](#) un ordinateur sous Secureblue
- [sell](#) une connexion internet

🔗 Intérêts de la mesure

thumb_up Séparer fortement tes usages et tes identités numériques

thumb_up Isoler une application risquée du reste du système

thumb_up Chiffrer les données d'un compartiment, ou le faire passer par Tor ou un VPN

⚠ Inconvénients

thumb_down Tout se fait en ligne de commande dans un terminal

thumb_down Le presse-papiers est partagé entre l'hôte et les compartiments, sans possibilité de le désactiver

thumb_down L'outil est récent et encore peu testé

thumb_down Prévoir 15 à 45 minutes de compilation au premier lancement de chaque base

— Introduction et parti pris

SecureBlue est un très bon compromis comme système d'exploitation simple à prendre en main, robuste face à des attaques physiques et distantes, fonctionnel avec de nombreuses applications et fiable à l'usage.

Cependant, son système de virtualisation intégré est compliqué à prendre en main et ne permet pas de compartimenter fortement les usages numériques aussi facilement que sur **QubesOS**, un système bien plus poussé sur la compartimentation mais qui est très peu accessible pour un public non technique.

Cet outil s'intègre dans **SecureBlue** pour faciliter pour chaque besoin la création d'une VM dédiée à l'exécution d'une unique application isolée, avec de nombreux paramétrages de sécurité et en virtualisant complètement une autre machine peu lourde.

— Présentation de l'outil

Pour garantir une séparation forte avec le reste du système, cet outil fait tourner chaque application dans une **machine virtuelle**.

Intégration visuelle

Les applications compartimentées s'affichent de la même manière que n'importe quelle autre application, tu verras un petit badge bleu en bas à droite de l'icône officielle pour te rappeler qu'elle est compartimentée.

Le démarrage prend nécessairement plus de temps qu'une application de base, mais tu ne verras pas de différence à l'usage.

Lors des tests,  Firefox s'ouvre en 30s sur un ordinateur assez vieux avec son espace disque chiffré et à travers Tor.

Cette pratique est pertinente lorsque tu as un modèle de menace fort qui demande à compartimenter tes usages, et que tu as plusieurs identités numériques ou certains usages spécifiques comme par exemple :

- consulter/écrire les mails d'une adresse publique/exposée
- plusieurs comptes Signal pour des identités numériques distinctes
- navigation sur Internet dédiée à un objectif sensible/exposé, comme gérer des réseaux sociaux

Cet outil reprend des concepts de  QubesOS. Il installe l'application souhaitée dans une base (équivalent d'un  TemplateVM), ce qui crée un disque système minimal qui est partagé en lecture seule par plusieurs compartiments (équivalent d'une  AppVM).

Tu peux créer autant de compartiments que tu veux, et ils sont chacun configurables selon tes besoins :

- est-ce que tu as besoin d'une connexion Internet ? Qui garantit ton anonymat (Tor), avec un noeud de sortie Mullvad spécifique ou avec la même connexion que le reste des applications ?
- est-ce que le stockage des données doit en plus être chiffré ?
- est-ce que les données y sont persistantes ou jetables ( DisposableVM)
- est-ce que tu dois partager un dossier avec SecureBlue pour faciliter le transfert de fichiers, lequel ?
- combien de RAM et d'espace disque ce compartiment peut-il utiliser ?

Presse-papiers partagé

Ce que tu copies d'un compartiment sera disponible sur l'hôte SecureBlue et inversement. Ça ne peut pas être désactivé.

Trois bases sont fournies avec l'outil, avec pour chacune un compartiment par défaut :

Nom de la base	Application installée	Compartiment associé par défaut
mail	Thunderbird	mail
browser	Firefox	social-network
signal	Signal Desktop (via Flatpak)	signal

— Installation

Prérequis

Installe [SecureBlue](#) et suis le tuto [Ordi secureblue](#) avant de poursuivre.

Assure-toi d'avoir tous les outils nécessaires avec cette commande dans ton terminal (

`^ Ctrl1 + ⌘ Alt + T ) :`

Bash

```
1 # Indispensables
2 rpm-ostree install libvirt qemu-kvm virtiofsd passt waypipe cloud-utils
genisoimage
```

🔄 Redémarre ensuite ton ordinateur pour terminer l'installation :)

Installation de l'outil

Dans un terminal, pour installer cet utilitaire dans `$HOME/``bin``/secureblue-vms`, exécute les commandes suivantes :

Bash

```
1 # Change ce chemin par là où tu souhaites télécharger l'outil
2 DIR_TOOL="$HOME/.bin/secureblue-vms"
3
4 # Téléchargement de l'outil
5 mkdir -p "$(dirname "$DIR_TOOL")"
6 git clone https://0xacab.org/TheCodesUprising/tools/secureblue-vms
"$DIR_TOOL"
7 cd "$DIR_TOOL"
8
9 # Si tu veux Tor / Mullvad
10 ./src/secureblue-vms --install-tools
11 # Installe des applications optionnelles
```

```

12 ./src/secureblue-vms --install-tools=all
13
14 # Vérifie que tu n'as rien d'important ouvert avant de redémarrer
15 systemctl reboot

```

Après le redémarrage si tu veux passer par Tor :

Bash

```

1 systemctl enable --now tor

```

Tu peux vérifier que ton appareil est compatible et que tous les outils sont bien installés avec :

Bash

```

1 ./src/secureblue-vms --host-check

```

Si une entrée apparaît en rouge, tu verras dans la dernière colonne la commande à exécuter pour installer le bon logiciel.

Pour avoir un aperçu de toutes les commandes disponibles :

Bash

```

1 ./src/secureblue-vms --help
2
3 Usage: ./src/secureblue-vms [OPTION...] [COMMAND]
4     OPTIONS SUMMARY
5         -h | --help                Print help information
6         -v | --verbose              Increase verbosity
7         -q | --quiet               Suppress non-error messages
8     COMMANDS SUMMARY
9         -l | --list                 List bases and compartments
10        and their state
11        -s | --status                Show which compartments are
12        running
13        -S | --stop <compartment>   Stop a running compartment
14        -c | --host-check            Report what this host can
15        and cannot do
16        -g | --guest-build           Download and verify the
17        Alpine base image
18        -b | --build <base>          Provision a reusable base
19        rootfs
20        -L | --launch <compartment> Boot a compartment and open
21        its app
22        -r | --remove-base <base>   Delete an unused base
23        rootfs
24        --auto-clean                 Delete every unreferenced
25        base
26        --install-launchers          Add a menu .desktop entry
27        per compartment
28        --remove-launchers           Remove those menu entries

```

```
20 | --install-tools[=all] Layer host deps: tor, socat  
(=all adds the 3 optional ones)
```

— Mise en place et paramétrage de l'outil

Créer les bases des applications

Compilation automatique au premier lancement

Cette étape est optionnelle, au lancement de ton application la base sera automatiquement compilée si elle n'existe pas.

Ça te permet cependant de tout préparer en avance pour économiser 15 à 45 minutes d'attente au premier lancement sans que tu saches où ça en est.

C'est l'étape la plus longue : l'outil va télécharger une version de Linux minimale puis va télécharger chaque application pour créer une image template partagée entre tes différents compartiments.

Chaque ligne peut prendre entre 5 et 15 minutes, en fonction de ta connexion Internet. Il n'y en a besoin que d'une seule fois ; si tu n'as pas besoin d'un outil, épargne-toi la ligne.

Bash

```
1 # Firefox  
2 ./src/secureblue-vms -vv --build browser  
3 # Thunderbird  
4 ./src/secureblue-vms -vv --build mail  
5 # Signal Desktop (installé avec Flatpak)  
6 ./src/secureblue-vms -vv --build signal
```

Tu peux créer de nouvelles bases avec les fichiers `$HOME/.config/secureblue-vms/bases` grâce aux paramètres suivants :

Clef	Description
<code>packages</code>	Liste des paquets <code>apk</code> , séparés par des espaces
<code>flatpak</code>	Flathub app id : https://flathub.org/
<code>app_args</code>	Arguments supplémentaires donnés à l'application au lancement

Clef	Description
<code>app_env</code>	Variables d'environnement supplémentaires données à l'application au lancement

Premiers lancements des `compartiments`

Une fois que tu as défini tous tes compartiments, tu peux créer des `.desktop` pour pouvoir les lancer facilement avec leur icône depuis ton lanceur d'applications :

```
Bash
1 | ./src/secureblue-vms --install-launchers
```

Pour facilement distinguer les applications compartimentées, tu verras un petit badge bleu en bas à droite des icônes officielles.

Tu peux ensuite ouvrir ton application comme tu lancerais n'importe quel autre programme.

Information

Le premier lancement sera plus lent que les suivants, ça ne sert à rien d'appuyer plusieurs fois sur l'icône 😊

Si tu as décidé de chiffrer le disque (configuration par défaut), tu verras une fenêtre s'ouvrir deux fois pour te demander de taper le mot de passe de chiffrement, de préférence unique par compartiment. Chaque nouveau lancement te demandera son mot de passe.

Si tu as besoin d'avoir plus d'informations sur ce qu'il se passe :

```
Bash
1 | # Savoir quels compartiments sont en train de tourner
2 | ./src/secureblue-vms --status
3 |
4 | # Remplace 'mail' par le nom du compartiment que tu souhaites démarrer
5 | ./src/secureblue-vms -vv --launch mail
6 |
7 | # Arrête le compartiment 'mail' proprement
8 | ./src/secureblue-vms --stop mail
```

Configurer les `compartiments` selon tes besoins

Plusieurs propositions de compartiments ont été générées dans

`$HOME/.config/secureblue-vms/compartments`, tu peux y créer/supprimer/éditer les fichiers de configuration selon tes besoins.

Par exemple, tu peux vouloir plusieurs comptes Signal, augmenter l'allocation de la RAM pour un usage de Firefox en particulier ou consulter tes mails à travers Tor.

Le nom d'un fichier correspond au nom de ton compartiment (`social-network.conf` créera le compartiment `social-network` par exemple), et tu peux changer les paramètres suivants :

Clef	Défaut	Description
<code>base</code>	obligatoire	Base utilisée : <code>browser / mail / signal</code>
<code>app</code>	obligatoire	Commande lancée dans chaque compartiment au démarrage
<code>ram_mb</code>	<code>2048</code>	Quantité de RAM assignée, en Mo
<code>data_size</code>	<code>8G</code>	Taille du disque persistant monté sur <code>/home</code> , comprend les suffixes <code>M / G</code> . Plafond, l'espace utilisé se remplit au fur et à mesure.
<code>persist</code>	<code>yes</code>	<code>yes</code> pour garder le contenu de <code>/home</code> entre plusieurs démarrages, <code>no</code> pour être temporaire
<code>encrypt_data</code>	<code>no</code> (configuration des compartiments par défaut sur <code>yes</code>)	<code>yes</code> chiffre le contenu de <code>/home</code> avec LUKS, mot de passe demandé à chaque lancement
<code>network</code>	<code>nat</code>	<code>nat / none / tor / socks</code>
<code>shared_folder_path</code>	-	Partage d'un dossier avec SecureBlue
<code>icon</code>	-	Change l'icône de la fenêtre



N'oublie pas ton mot de passe de déchiffrement !

Si tu as `encrypt_data=yes`, à chaque démarrage, tu devras entrer ton mot de passe. **Si tu l'oublies, les données seront définitivement perdues** sans moyens de les récupérer.

Paramètre `network`

4 modes sont disponibles :

Mode	Isolé ?	Fonctionnement
<code>nat</code>	Non	Le trafic sortant utilise l'IP de ton ordinateur directement
<code>none</code>	Oui	Aucun accès Internet
<code>tor</code>	Oui	Tout le trafic (dont DNS) passe par Tor, avec un circuit différent par compartiment
<code>socks[=server:port]</code>	Oui	Fait passer le trafic par un tunnel SOCKS, par Mullvad par défaut

En-dehors du mode par défaut `nat`, le paramétrage réseau est fait depuis SecureBlue, un compartiment n'a pas d'interface IP : cette isolation réseau garantit que même si un compartiment est compromis, l'attaquant ne peut pas récupérer ton adresse IP ni aucune information en-dehors du compartiment.

Si tu as besoin de plus que deux compartiments en même temps pour passer par Tor, il te faut augmenter la valeur de `SBVMS_TOR_POOL_N` et ouvrir de nouveaux ports :

Bash

```
1 # Change 'NN' par le nombre de compartiments dont tu as besoin + 9050
2 # Par exemple pour 15 compartiments : 9052-9065
3 run0 semanage port -a -t tor_port_t -p tcp 9052-90NN
```

Si tu veux utiliser le nœud de sortie Mullvad par Paris, tu peux utiliser l'option :

`network=socks=fr-par-wg-socks5-001.relays.mullvad.net:1080` (tu peux trouver la liste ici : <https://mullvad.net/en/servers?type=wireguard&status=true>)

Paramètre `shared_folder`

Si tu as besoin, tu peux partager **un** dossier entre SecureBlue et le compartiment pour faciliter le transfert de fichiers.



Partage uniquement un dossier dédié

Plutôt que de monter un dossier très gros qui contient trop d'informations (refus automatique de `$HOME`, `/`, dossiers cachés), restreins la taille du dossier aux seules informations nécessaires au compartiment.

Si Thunderbird se fait compromettre par exemple, un attaquant n'aurait accès qu'aux quelques fichiers contenus dans ce dossier.

Le dossier pointé par le paramètre `shared_folder_path=<dir>` est monté dans le compartiment sur `/mnt/shared` et est aussi accessible sur `$HOME/Shared` pour un accès plus simple.

Le presse-papier est partagé entre SecureBlue et tous les compartiments.

Mises à jour

Lorsque des mises à jour existent, il te suffit de :

Bash

```
1 cd "$HOME/bin/secureblue-vms"
2 git pull
```

Lorsqu'une base peut être mise à jour, elle le sera à la prochaine exécution.

Les configurations de tes compartiments ne seront jamais écrasées.

Un compartiment supprimé n'est pas récupérable.

Désinstallation

Bash

```
1 # Supprime les compartiments dont tu n'as plus besoin
2 rm ~/.config/secureblue-vms/compartments
3
4 cd "$HOME/bin/secureblue-vms"
5 ./src/secureblue-vms --auto-clean
6 ./src/secureblue-vms --remove-launchers
7
8 # Suppression des bases
9 ./src/secureblue-vms --remove-base browser
10 ./src/secureblue-vms --remove-base mail
11 ./src/secureblue-vms --remove-base signal
```

Si tu veux supprimer les disques qui contiennent tes données. **Attention, c'est irréversible !**

Bash

```
1 ls ~/.local/state/secureblue-vms/  
2 rm ~/.local/state/secureblue-vms/TON_COMPARTIMENT  
3 # Suppression du cache  
4 rm -rf ~/.cache/secureblue-vms/  
5 # Suppression de cet outil  
6 rm -rf "$HOME/bin/secureblue-vms"
```

— Troubleshooting

Mon application n'apparaît pas dans le menu ou son icône n'est pas bonne

Bash

```
1 cd "$HOME/bin/secureblue-vms"  
2 ./src/secureblue-vms --install-launchers
```

Si tu as une application différente de celles qui sont affichées par :

Bash

```
1 ls "$HOME/bin/secureblue-vms/share/icons"/badged-*.png
```

alors il te faut installer l'outil qui génère les icônes :

Bash

```
1 cd "$HOME/bin/secureblue-vms"  
2 ./src/secureblue-vms --build ta-base  
3 ./src/secureblue-vms --install-tools=all  
4 # Redémarre pour rendre disponible  
5 ./src/secureblue-vms --install-launchers
```

--host-check a encore des entrées rouges après l'installation

Redémarre ton ordinateur pour rendre `--install-tools` effectif.

Un compartiment avec `tor` n'a pas de réseau

Bash

```
1 systemctl enable --now tor
```

Pour t'assurer que le réseau passe à travers `Tor`, rends-toi sur <https://check.torproject.org> depuis le Firefox compartimenté avec `network=tor`.

— Plus d'informations

Cet outil est encore en phase de tests, n'hésite pas à l'utiliser pour en faire des retours !
Notamment est-ce que tu as détecté des bugs, est-ce que tu as des besoins qui ne sont pas couverts par l'outil ou est-ce que tu vois des améliorations à y faire ? → barricade-numerique@riseup.net

Pour plus de détails techniques, tu peux aller lire le README.md du projet : 
<https://0xacab.org/TheCodesUprising/tools/secureblue-vms>

Quiz

Question 1

Dans quoi tourne chaque application compartimentée ?

- ☐ Dans une machine virtuelle
- ☐ Dans un conteneur Flatpak
- ☐ Dans un simple onglet du navigateur

Question 2

Qu'est-ce qu'une « base » ?

- ☐ Un dossier partagé
- ☐ Un disque système minimal partagé en lecture seule par plusieurs compartiments
- ☐ Un compartiment persistant

Question 3

Quel mode réseau n'offre **pas** d'isolation ?

- ☐ nat
- ☐ tor
- ☐ none
- ☐ socks

Question 4

Le presse-papiers entre l'hôte et les compartiments peut-il être désactivé ?

- ☐ Non, il est toujours partagé
- ☐ Oui, dans les paramètres
- ☐ Uniquement en mode `tor`

Question 5

Que se passe-t-il si on oublie le mot de passe de chiffrement d'un compartiment ?

- ☐ Les données sont définitivement perdues
- ☐ On peut le réinitialiser par mail
- ☐ Le compartiment repasse en clair

Progression du quiz

0 / 5 questions répondues (**0%**)

0 correctes

2026-07-302026-10-17