



Total Secure ***Community Edition***

Guide de démarrage

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Préambule

Nous vous remercions d'avoir téléchargé la version *Community Edition* de notre solution UTM (Unified Threat Management) **TotalSecure**, également appelée **TS CE**.

Les équipes WALLIX ont apporté le plus grand soin à l'élaboration de ce produit et souhaitent qu'il vous apporte entière satisfaction.

Copyright

Le présent document est la propriété de la société WALLIX et ne peut être reproduit sans son accord préalable.

Tous les noms de produits ou de sociétés cités dans le présent document sont des marques déposées de leurs propriétaires respectifs.

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

SOMMAIRE

1 Introduction.....	4
2 Installation de VMware.....	5
3 Module Security (Sec).....	7
3.1 Interfaces réseaux.....	7
3.2 Lancer et configurer l'appliance virtuelle.....	7
3.3 Accès aux services de l'appliance virtuelle.....	8
3.4 Exemple de configuration du filtre de contenu Dansguardian.....	8
3.5 Exemple de configuration de l'authentification des utilisateurs par Squid.....	10
4 Module Communication (Com).....	11
4.1 Interfaces réseaux.....	11
4.2 Lancer et configurer l'appliance virtuelle.....	11
4.3 Accès aux services de l'appliance virtuelle.....	12
4.4 Exemple de configuration du système MTA (relais SMTP sécurisé).....	12
5 Désinstallation de TS CE.....	15
5.1 Arrêt de la machine virtuelle TS CE.....	15
5.2 Désinstaller VMware.....	15
6 Contacts.....	17

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

1 Introduction

TotalSecure Community Edition (TS CE) est la version logicielle, librement téléchargeable et installable, de notre solution UTM **Wallix TotalSecure**.

TS CE se présente sous la forme de deux *appliances logicielles* pour VMWare, l'une correspondant au module "Security" (Sec) et l'autre au module "Communication" (Com). TS CE nécessite donc d'installer VMware "Server" ou Vmware "Player" sur la machine hôte, qui peut être une plate-forme Unix, Linux ou Windows.

Les fonctionnalités de TS CE sont mises en oeuvre à l'aide d'un assemblage de composants Open Source d'une part et de développements Wallix d'autre part.

Composants Open Source du module Security

- Linux Debian Etch de base (système d'exploitation)
- Netfilter/iptables (pare-feu L4 stateful)
- Openswan (vpn Ipsec)
- Squid (proxy-cache Web)
- Dansguardian (filtrage d'urls et de contenu Web)

Composants Open Source du module Communication

- Bind (cache dns)
- Postfix (relais smtp)
- ClamAV (anti-virus)
- SpamAssassin (*tm*), Pyzor, Postgrey (anti-spam)

Les licences utilisées par ces différents logiciels sont disponibles dans le répertoire `/home/adminlinux/licenses` de chacune des appliances "Sec" et "Com".

Pour toute information concernant les logiciels Open Source utilisés par TS CE, contacter Wallix au **01 53 42 12 89** ou envoyer un courriel à **oss@wallix.com**.

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

2 Installation de VMware

Cette installation a été testée sous :

- Linux Ubuntu 7.10 avec la version 2.0.4-93057.i386 de VMware Player.
- Debian Etch avec la version 1.0.6-91891 de VMware Server.
- Windows XP SP2 avec la version 2.0.4-93057 de VMware Player.
- Windows XP SP2 avec la version 1.0.6-91891 de VMware Server.

VMWare Player peut être téléchargé depuis le lien suivant :

<http://www.vmware.com/download/player/>

VMware Server peut être téléchargé depuis le lien suivant :

<http://www.vmware.com/download/server/>

Il est également nécessaire de télécharger le « Client Package » pour se connecter à la version "Server" de VMware.

Note : Sous Linux Ubuntu, les commandes nécessitant les droits « root » sont exécutées précédées de la commande « sudo ». Selon votre distribution Linux il est probable que cette commande ne soit pas disponible. Dans ce cas, passer « root » avec la commande « su - », (enter le mot de passe « root »), puis lancer la commande.

Installation du Player VMware sous Linux

```
$ tar xvzf VMware-player-2.0.4-93057.i386.tar.gz
$ cd vmware-player-distrib
$ sudo ./vmware-install.pl
Faire « entrée » à toutes les questions posées (réponses par défaut)
```

Installation du Player VMware sous Windows

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Suivre les instructions d'installation, puis redémarrer votre machine hôte.

Installation du serveur VMware sous Linux

```
$ tar xvzf VMware-server-1.0.6-91891.tar.gz
$ cd vmware-server-distrib
$ sudo ./vmware-install.pl
Faire « entrée » à toutes les questions posées (réponses par défaut)
```

Installation de la console VMware sous Linux

```
$ unzip VMware-server-linux-client-1.0.6-91891.zip
$ tar xvzf VMware-server-console-1.0.6-91891.tar.gz
$ cd vmware-server-console-distrib
$ sudo ./vmware-install.pl
Faire « entrée » à toutes les questions posées (réponses par défaut)
Lancer le serveur par : vmware-server-console
```

Installation du Serveur VMware sous Windows

Suivre les instructions d'installation, puis redémarrer votre machine hôte. Lancer la console VMware pour se connecter localement au serveur.

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

3 Module Security (Sec)

3.1 Interfaces réseaux

Votre machine hôte sur laquelle est installé VMware Player doit disposer d'au moins une interface réseau. L'appliance virtuelle *TS Community Edition* possède quatre interfaces réseaux virtuelles de type "bridge". Ceci signifie que ces interfaces virtuelles, et donc la machine virtuelle, seront accessibles depuis votre LAN.

Vous devez disposer d'au minimum deux adresses IP disponibles sur votre LAN pour les attribuer (les "bridger") aux interfaces virtuelles de l'appliance.

Lors de la configuration de l'appliance avec le configurateur de *TS Community Edition*, les interfaces réseau "EXTERNAL (eth0)" et "LAN (eth2)" doivent être configurées. Pour les autres interfaces, choisir "unconf".

3.2 Lancer et configurer l'appliance virtuelle

Après avoir décompressé l'archive contenant l'appliance virtuelle faire :

```
$ vmplayer
```

- sélectionner "Open an existing virtual machine".
- ouvrir le fichier ".vmx".
- au premier démarrage, VMware demande si vous avez copié ou déplacé l'appliance virtuelle : "Did you move this virtual machine, or did you copy it ?" . Répondez "I moved it".
- au prompt, se connecter en "root" avec le mot de passe : "SecureLinux".
- lancer le configurateur

```
# cd /opt/phoenix  
# ./config.sh
```

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Dans le menu de configuration :

- sélectionner "init" pour initialiser les services.
- sélectionner "Syssetting" pour configurer le "hostname", le "domaine", ...
- sélectionner "Netsetting" et configurer au moins les interfaces "EXT" et "LAN" avec des adresses disponibles dans votre sous-réseau.
- sélectionner "Config" pour configurer les services (Squid, Dansguardian, Openswan).
- sélectionner "ShowConf" pour vérifier la configuration entrée.
- sélectionner "Save", puis "Netstart", puis "Start" pour lancer les services, puis "Quit" pour sortir du configurateur.

3.3 Accès aux services de l'appliance virtuelle

Le module "Security" de *TotalSecure Community Edition* est, entre autres, équipé d'un proxy filtrant basé sur Squid et Dansguardian. Ce proxy écoute sur l'interface "LAN" et est accessible sur le port 8080/TCP.

Les navigateurs des postes de travail de votre réseau peuvent alors être configurés pour utiliser le proxy de l'appliance virtuelle.

Après configuration de l'appliance avec le configurateur, son administration à distance fait par ssh. Un serveur ssh est accessible par toutes les interfaces sur le port 39999/TCP, utilisateur "adminlinux", mot de passe "linux".

3.4 Exemple de configuration du filtre de contenu Dansguardian

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Dansguardian permet d'autoriser ou d'interdire les accès Web selon certains critères configurables par l'intermédiaire de fichiers plats situés dans le répertoire `"/etc/dansguardian/"`.

- "bannedextensionlist" et "bannedmimetyplist" :
 - permettent d'interdire un type de fichier transitant sur le flux http. Dans sa configuration par défaut, Dansguardian interdit les fichiers de type Mime "application/zip" et l'extension ".zip".
Pour autoriser le téléchargement de ce type de fichier, commenter (#):
".zip" dans le fichier "bannedextensionlist" et
"application/zip" dans le fichier "bannedmimetyplist".
Puis faire : `# /etc/init.d/dansguardian restart`
- "bannedregexprlist"
 - Dansguardian filtre les URLs transitant dans le flux http selon les expressions régulières définies dans ce fichier de configuration. Par exemple, l'ajout en fin de fichier de la ligne
`(forum|phpbb)`
interdit l'accès à `fr.wikipedia.org/wiki/phpbb`.
De même pour les URLs contenant le mot "forum".
- "bannedsitelist"
 - permet d'interdire l'accès aux sites définis dans ce fichier. L'ajout de `alltheweb.com` interdit l'accès à l'ensemble de ce domaine.

Des archives contenant une base de sites "blacklistés" sont disponible sur le site web de SquidGuard à l'URL : <http://www.squidguard.org/blacklists.html>

Ces archives peuvent être utilisées en renseignant le fichier "bannedsitelist".

Dans le cas d'un accès interdit, Dansguardian renvoie au navigateur une page explicative contenant la raison de l'interdiction.

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Si le support du filtre antivirus a été activé durant la configuration de *TS Community Edition*, alors Dansguardian essaiera de détecter d'éventuels virus dans le flux http. Si cela est le cas, alors l'accès à l'URL suivante sera interdite :

<http://www.rexswain.com/eicar2.zip>

Attention : le type mime "application/zip" et l'extension "zip" doivent être autorisés comme expliqué ci-dessus.

3.5 Exemple de configuration de l'authentification des utilisateurs par Squid

Lors de la configuration des services de *Total Secure Community Edition*, il est possible de configurer le proxy pour demander l'authentification de l'utilisateur soit par fichier plat, soit par annuaire LDAP.

Pour configurer l'authentification par fichier plat, il faut ajouter dans le fichier "/etc/squid/squid.auth" les utilisateurs autorisés à naviguer . Il faut tout d'abord installer le paquet "apache2-utils" puis ajouter les utilisateurs avec l'utilitaire "htpasswd".

```
# aptitude install apache2-utils
# htpasswd /etc/squid/squid.auth user
```

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

4 Module Communication (Com)

4.1 Interfaces réseaux

Votre machine hôte sur laquelle est installé VMware Player doit disposer au minimum d'une interface réseau. L'appliance virtuelle *Total Secure Community Edition* possède quatre interfaces réseaux virtuelles de type "Bridge". Ce qui signifie que ces interfaces virtuelles, et donc la machine virtuelle, seront accessibles depuis votre LAN.

Vous devez disposer d'au minimum une adresse IP disponible dans votre LAN pour l'attribuer à l'interface externe de l'appliance virtuelle.

4.2 Lancer et configurer l'appliance virtuelle

Après avoir décompressé l'archive contenant l'appliance virtuelle lancer le player VMware :

```
$ vmplayer
```

- sélectionner "Open an existing virtual machine".
- ouvrir le fichier ".vmx".
- au premier démarrage, VMware demande si vous avez copié ou déplacé l'appliance virtuelle "Did you move this virtual machine, or did you copy it ?" . Répondez "I moved it".
- au prompt, se connecter en "root" avec le mot de passe "SecureLinux".

Puis lancer le configurateur de *Total Secure Community Edition* :

```
# cd /opt/phoenix  
# ./config.sh
```

Dans le menu de configuration :

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

- sélectionner "init"» pour initialiser les services.
- sélectionner "Syssetting"» pour configurer le "hostname", le "domaine", ...
- sélectionner "Netsetting et configurer l'interface "EXT" avec une adresse disponible dans votre sous réseau.
- sélectionner "Config" pour configurer les services (cache DNS, Mail Transfert Agent).
- sélectionner "ShowConf" pour vérifier la configuration entrée.
- sélectionner "Save", puis "Netstart", puis "Start" pour lancer les services, puis "Quit" pour sortir du configurateur.

4.3 Accès aux services de l'appliance virtuelle

Le module "Communication" de *TotalSecure Community Edition* est équipé d'un cache DNS basé sur Bind V9 mais aussi d'un MTA, d'un anti-spam et d'un anti-Virus. Le MTA est accessible sur le port 25/TCP.

Pour utiliser le MTA de l'appliance virtuelle il est nécessaire de configurer le gestionnaire DNS de votre domaine. L'entrée MX (Mail Exchange) du DNS (Domain Name Server) doit pointer vers l'appliance virtuelle. Par l'intermédiaire du configurateur, vous avez configuré l'adresse du MDA (Mail Delivery Agent) de votre réseau et le domaine pour lequel les mails doivent être transférés à votre MDA.

Après configuration de l'appliance avec le configurateur, l'administration à distance de l'appliance se fait par ssh. Un serveur ssh est accessible par toutes les interfaces sur le port 39999/TCP pour l'utilisateur "adminlinux" et son mot de passe "linux".

4.4 Exemple de configuration du système MTA (relais SMTP sécurisé)

Configuration d'une whitelist et d'une blacklist globales

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Le système MTA est composé, entre autres, d'un agent capable de prendre des décisions sur le traitement du courrier entrant. Il peut être nécessaire dans certain cas de placer des expéditeurs en "whitelist" ou "blacklist" globale. Pour cela, il faut éditer les fichiers `"/var/lib/amavis/blacklist_sender"` et `"/var/lib/amavis/whitelist_sender"`.

Ajouter les adresses email des expéditeurs (une par ligne) pour qui les résultats aux différents tests effectués par le système de détection de spam ou de virus n'auront pas d'effet sur la suite du transfert du mail jusqu'à la boîte de réception du destinataire. Il est également possible de spécifier un domaine et ses sous-domaines de cette façon : `".domaineblacklist.fr"`.

Configuration d'une whitelist et d'une blacklist par boîte de réception

En plaçant la configuration suivante dans le fichier de configuration de l'agent Amavisd-new, on va pouvoir définir deux listes (white et black) par boîte de réception :

```
$per_recip_blacklist_sender_lookup_tables = {  
'yves@mondomaine.fr' => read_hash("$MYHOME/yves_sender_blacklist"),  
'sylvie@mondomaine.fr' => read_hash("$MYHOME/sylvie_sender_blacklist"),  
};  
  
$per_recip_whitelist_sender_lookup_tables = {  
'yves@mondomaine.fr' => read_hash("$MYHOME/yves_sender_whitelist"),  
'sylvie@mondomaine.fr' => read_hash("$MYHOME/sylvie_sender_whitelist"),  
};
```

Le courrier bloqué par une blacklist va être considéré comme spam et placé en quarantaine.

Autoriser tout type de courrier sur une boîte de réception

La directive `"*_lovers_maps"` où `"*"` correspond à un des cas suivants :

- spam

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

- banned_files
- bad_header
- virus

permet d'autoriser le courrier ayant été détecté comme un virus, spam ou encore ayant un entête mal formé à être transféré jusqu'à la boîte de réception définie. Cette directive est définie comme ceci :

```
@spam_lovers_maps = (  
    read_hash("$MYHOME/spam_lovers_recip"),  
);
```

Sortir un mail de la quarantaine

La quarantaine contient le courrier déclaré en tant que virus, spam ou mauvais entête. Il existe un fichier par message en quarantaine. Les noms des fichiers sont du type "spam-id.gz".

La commande "amavis-release" permet de re-insérer un mail dans la file d'attente d'envoi sans repasser dans le filtre. Le mail est alors renvoyé à son destinataire.

```
amavisd-release spam-rQ5hkkhKhdi.gz
```

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

5 Désinstallation de TS CE

5.1 Arrêt de la machine virtuelle TS CE

Sous VMware Server/VMware Client

Se connecter au serveur ssh de la machine virtuelle en tant qu'utilisateur "adminlinux" (mot de passe "linux") et faire :

```
su -  
(password "SecureLinux")  
shutdown -h now
```

Ou bien au prompt en tant qu'utilisateur "root" faire :

```
shutdown -h now
```

Fermer la console graphique VMware en faisant *Fichier – Quitter* . La procédure est similaire sous Windows et Linux.

5.2 Désinstaller VMware

Désinstaller VMware Serveur ou VMware Player sous Linux

Sur votre machine hôte, entrez les commandes suivantes :

```
sudo vmware-uninstall.pl  
(Pour VMware server supprimer en plus la console)  
sudo vmware-server-console-uninstall.pl
```

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

Désinstaller VMware Server ou VMware Player sous Windows

Dans le *Panneau de configuration – Ajout/Suppression de programmes* :

- sélectionner VMware Server ou VMware Player
- supprimer
- suivre les instructions à l'écran

	TotalSecure Community Edition	
7 Juillet 2008	Guide de démarrage	

6 Contacts

Pour toute information concernant ce guide, la solution TotalSecure ou le logiciel TotalSecure Community Edition, contactez Wallix au **01 53 42 12 90** ou envoyez un courriel à totalsecure@wallix.com.

Pour bénéficier de nos offres de boîtiers, de support ou d'accompagnement en services professionnels, contactez sales@wallix.com.