

Debian Lenny - Shoreline Firewall

Debian GNU/Linux



Matthieu Vogelweith
22 janvier 2009

Résumé

Ce document a été rédigé en LaTeX en utilisant l'excellent Vim sous Debian GNU/Linux. Il est disponible aux formats [XHTML](#) et [PDF](#). Les sources LaTeX sont disponibles ici : [L^AT_EX](#)

Licence

Copyright ©2009 Matthieu VOGELWEITH <matthieu@vogelweith.com>.

Vous avez le droit de copier, distribuer et/ou modifier ce document selon les termes de la GNU Free Documentation License, Version 1.3 ou ultérieure publiée par la Free Software Foundation ; avec aucune section inaltérable, aucun texte de première page de couverture, et aucun texte de dernière page de couverture. Une copie de la licence est disponible dans la page [GNU Free Documentation License](#).

Table des matières

Table des matières	3
1 Firewall Basic	4
1.1 Présentation - Shorewall	4
1.2 Configuration générale	4
1.3 Définition des interfaces et des zones	4
1.4 Règles par défaut	5
1.5 Personnalisation des règles de filtrage	5
1.6 Quelques tests	5
2 Configuration avancée	6
2.1 Limitation des connexions SSH	6
2.2 Intégration OpenVPN	6
3 Références	7

Chapitre 1

Firewall Basic

1.1 Présentation - Shorewall

- Netfilter / Iptables
- Création du firewall simple

1.2 Configuration générale

Précaution d'usage :

```
ADMINISABSENTMINDED=Yes
```

Verbosité des journaux :

```
LOGRATE=10/minute  
LOGBURST=5
```

1.3 Définition des interfaces et des zones

- Fichiers par défaut avec les en-têtes pour `/etc/shorewall/interfaces` et `/etc/shorewall/zones`

```
# cp /usr/share/doc/shorewall-common/default-config/zones /etc/shorewall/  
# cp /usr/share/doc/shorewall-common/default-config/interfaces /etc/shorewall/
```

- Dans `/etc/shorewall/zones`

```
net    ipv4
```

- Dans `/etc/shorewall/interface`

```
net    eth0
```

1.4 Règles par défaut

- Fichier par défaut avec les en-têtes pour /etc/shorewall/policy

```
# cp /usr/share/doc/shorewall-common/default-config/policy /etc/shorewall/
```

- Dans /etc/shorewall/policy

```
fw      all      ACCEPT
all     all      DROP      info
```

1.5 Personnalisation des règles de filtrage

```
# cp /usr/share/doc/shorewall-common/default-config/rules /etc/shorewall/
```

- Dans /etc/shorewall/rules

```
# Ping
Ping/ACCEPT      all      fw

# SSH
SSH/ACCEPT      all      fw
```

1.6 Quelques tests

```
# aptitude install nmap
```

```
# nmap xx.xx.xx.xx
```

Chapitre 2

Configuration avancée

2.1 Limitation des connexions SSH

- Dans `/usr/share/shorewall/macro.SSHLIMIT` :

#ACTION	SOURCE	DEST	PROTO	DEST	SOURCE	RATE	USER/
#		PORT(S)	PORT(S)	LIMIT	GROUP		
PARAM	-	-	tcp	22	-	3/min:3	

- Dans `/etc/shorewall/rules` :

SSHLIMIT/ACCEPT	all	\$FW
-----------------	-----	------

2.2 Intégration OpenVPN

Chapitre 3

Références

- [1] Site officiel du projet debian. www.debian.org.
- [2] La page debian security. www.debian.org/security/.
- [3] Shoreline firewall. www.shorewall.net.