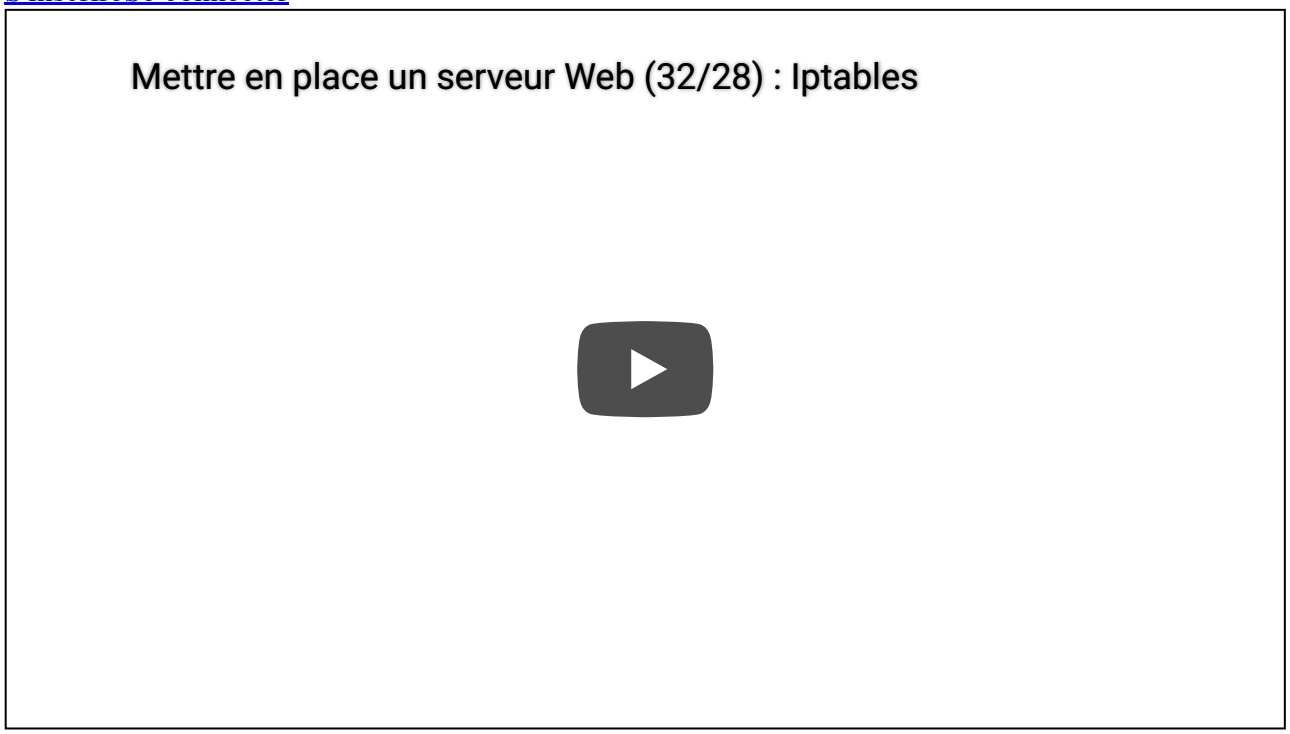


Mettre en place un serveur WebIptables

Télécharger la vidéo

32/28chapitre
ProFTPDufw, Uncomplicated FireWall
Pour débuter
Introduction
04 min
Machine virtuelle avec Virtualbox
08 min
Commandes de bases
29 min
Outils de base
VIM
06 min
SSH
14 min
rsync
20 min
Tâches récurrents, cron
23 min
Shell fish
13 min
Serveur HTTP
Apache

40 min
Nginx
30 min
PHP
PHP, Module Apache
20 min
PHP FPM pour Apache
20 min
PHP FPM pour Nginx
20 min
NodeJS
NodeJS et Nginx
17 min
Base de données
MySQL
15 min
Redis
08 min
Emails
postfix, envoie seulement
10 min
HTTPS
Apache, Let's Encrypt
05 min
Nginx, Let's Encrypt
31 min
FTP
ProFTPD
14 min
Sécurité
Iptables
18 min
ufw, Uncomplicated FireWall
13 min
Fail2ban
20 min
Nginx : Se protéger des attaques Flood
21 min
Pour le confort
Pimp my shell, Zsh & Tmux
30 min
Déploiement
Capistrano
45 min
Capistrano : Déployer Rails avec Puma / Nginx
28 min
Ansible
56 min
Tutoriels Mettre en place un serveur Web Iptables
Il y a 4 ans

Par défaut notre serveur peut communiquer librement avec internet. Si un service est mal configuré il pourrait alors être accessible depuis l'extérieur, ce qui n'est évidemment pas une bonne chose. La solution pour remédier

au problème est d'utiliser un parefeu afin de ne laisser ouvert qu'un nombre limité de port. Heureusement pour nous linux dispose d'un système de pare feu intégré : IpTables.

Pour ajouter des règles à IpTables il suffit de taper la commande `iptables` suivie de ce qu'on veut lui faire faire. Nous allons créer un fichier de script afin de regrouper toutes les règles pour ne pas avoir à les retaper à chaque fois. Ce fichier va dépendre de votre configuration mais voici un exemple (si vous avez besoin de plus de détails sur ce que font ces règles, utilisez explainshell.com).

```
#!/bin/sh

# On vide les règles déjà existantes
iptables -t filter -F
iptables -t filter -X

# On refuse toutes les connexions
iptables -t filter -P INPUT DROP
iptables -t filter -P FORWARD DROP
iptables -t filter -P OUTPUT DROP
echo "On interdit tout"

# On autorise les connexions déjà établie
iptables -A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
iptables -A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# On autorise le loop-back (localhost)
iptables -t filter -A INPUT -i lo -j ACCEPT
iptables -t filter -A OUTPUT -o lo -j ACCEPT

# On autorise le ping
iptables -t filter -A INPUT -p icmp -j ACCEPT
iptables -t filter -A OUTPUT -p icmp -j ACCEPT

# On autorise le SSH (à adapter suivant votre cas)
iptables -t filter -A INPUT -p tcp --dport 5896 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 5896 -j ACCEPT

# Si on a un serveur DNS
iptables -t filter -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 53 -j ACCEPT
iptables -t filter -A INPUT -p udp --dport 53 -j ACCEPT

# NTP (pour avoir un serveur à l'heure)
iptables -t filter -A OUTPUT -p udp --dport 123 -j ACCEPT

# HTTP
iptables -t filter -A OUTPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 80 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 443 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 8443 -j ACCEPT

# FTP
iptables -t filter -A OUTPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 20 -j ACCEPT
iptables -t filter -A INPUT -p tcp --dport 21 -j ACCEPT
iptables -t filter -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

# MAIL
## SMTP
iptables -t filter -A INPUT -p tcp --dport 25 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 25 -j ACCEPT
```

```
## POP3
iptables -t filter -A INPUT -p tcp --dport 110 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 110 -j ACCEPT
## IMAP
iptables -t filter -A INPUT -p tcp --dport 143 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 143 -j ACCEPT
echo "trafic IMAP sur le port 143 autorisé"
## POP3S
iptables -t filter -A INPUT -p tcp --dport 995 -j ACCEPT
iptables -t filter -A OUTPUT -p tcp --dport 995 -j ACCEPT
```

On va placer ce fichier dans le dossier contenant les scripts de démarrage `/etc/init.d/parefeu`. On va ensuite le rendre éxécutable et demander à notre machine de l'éxécuter au démarrage (Si vous n'êtes pas sûr de vos règles, vous pouvez éxécuter le fichier une fois, si vous vous enfermez dehors vour pourrez redémarrer la machine pour "oublier" les règles)

```
sudo chmod +x /etc/init.d/parefeu
sudo update-rc.d parefeu defaults
```

Et voila le tour est joué !

Technologies utilisées dans cette vidéo

SSH

Auteur

Grafikart

---

8 Commentaires

Pseudo

Email

Votre commentaire...

Envoyer

ZerefGG Il y a environ un an - Répondre

C'est normal d'utiliser --dport pour les connexions sortantes? ex: iptables -t filter -A OUTPUT -p tcp --dport 5896 -j ACCEPT

c'est quoi la difference si je met --sport?

Cordialement

Kandjhur Il y a 2 ans - Répondre

Bonjour, merci pour cette série de tutos sur Linux. J'ai suivi IPTables et les règles ont bloqué le 'apt-get'. Les sources du sources.list n'étaient plus disponibles. Après recherches, j'ai ajouté deux règles (tcp/udp) sur l'INPUT des sources port 80 (--sport). Cela fonctionne, mais est-ce une bonne manière de faire ? D'autres ont-ils eu ce cas ?

Gael Il y a 3 ans - Répondre

Super entrée en matière dans la sécurisation de notre cher petit serveur ! Je consulte en parallèle les tutoriels sur Docker, quelqu'un aurait-il réussi à faire cohabiter des iptables en mode "whitelist" comme présenté dans ce tutoriel tout en permettant à des containers Docker de fonctionner correctement ?

mzkd Il y a 3 ans - Répondre

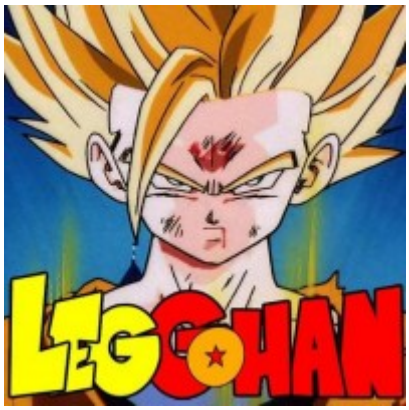
BTW: chez OVH, si vous avez un VPS/dédié, il ya quelques règles à ajouter pour permettre le monitoring SLA chez eux (permet aux techniciens de la maison d'accèder aux historiques système). Veulliez consulter ce lien : http://guide.ovh.com/firewall

crips Il y a 3 ans - Répondre

Merci pour touts tes supers tutos. Une petite question, si on a suivi tout le tuto à la lettre, comment faire pour désactiver et effacer le fichier parefeu? Et en même temps désactiver toutes les règles mises en place dans ce fichier. Merci d'avance.

webly Il y a 4 ans - Répondre

bonjour il faut mettre une en-tête a ton fichier merci pour tout grafikart ;)



LegGohan Il y a 3 ans - Répondre

Effectivement, sinon Debian sort une erreur missing LSB tags and overrides.

J'ai donc pour ma part ajouté

BEGIN INIT INFO

Provides: parefeu

Required-Start: $network $remote_fs $syslog

Required-Stop: $network $remote_fs $syslog

Default-Start: 2 3 4 5

Default-Stop: 0 1 6

Short-Description: parefeu

Description: parefeu

END INIT INFO

juste après #!/bin/sh

girioal Il y a 4 ans - Répondre

Très bonne entrée en matière !

Après avoir appris sur Internet quoi de plus normal que de partager à son tour ? Passionné par le web depuis un peu plus de 14 ans maintenant j'aime partager mes compétences et mes découvertes avec les personnes qui ont cette même passion pour le web

Mes derniers tweets
Un peu de culture générale aujourd'hui avec la découverte de l'algorithme boyer-moore-horspool https://t.co/i6HI4YBLEn
Je propose une nouvelle unité en CSS : le pw / ph. Pour "parent width", cela fonctionnerait comme le vw / vh mais b… https://t.co/OGF4IH8Pvb
Mise à jour d'un vieux tutoriel sur la création d'un système de ScrollSpy en JavaScript en se basant cette fois-ci… https://t.co/hjbFdQY8BP

- Me contacter
- Par email
- Tchat
- Chaine youtube
- A propos
- Politique de confidentialité