

Introduction à packet filter

le pare-feu *BSD

Adrien Kunysz

Free Softwares Users Group Arlon

réunion du 10 février 2007

Qu'est-ce que pf ?

- système de pare-feu
- libre (licence BSD)
- NAT
- système de priorités
- routeur redondant
- répartition de charge

Historique

- OpenBSD utilisait IPFilter de Darren Reed

Historique

- OpenBSD utilisait IPFilter de Darren Reed
- Darren Reed retire l'autorisation aux développeurs d'OpenBSD de modifier IPFilter

Historique

- OpenBSD utilisait IPFilter de Darren Reed
- Darren Reed retire l'autorisation aux développeurs d'OpenBSD de modifier IPFilter
- Daniel Hartmeier réécrit un nouveau pare-feu pour OpenBSD 3.0 (2002)

Historique

- OpenBSD utilisait IPFilter de Darren Reed
- Darren Reed retire l'autorisation aux développeurs d'OpenBSD de modifier IPFilter
- Daniel Hartmeier réécrit un nouveau pare-feu pour OpenBSD 3.0 (2002)
- 3.1 : authpf
- 3.3 : random-id
- 3.4 : détection passive d'OS
- 3.5 : CARP et pfsync
- 3.7 : max-src-conn
- 4.1 : hoststated, tables timeout

Systèmes d'exploitation intégrant pf

- OpenBSD
- FreeBSD (depuis juin 2004)
- NetBSD (depuis juillet 2004)
- DragonFlyBSD (depuis la version 1.1 ?)

Utilisation

- un fichier de configuration (pf.conf)
- gestion du pare-feu (pfctl)
- logging (pflogd)
- programmes annexes (authpf, pftop, ...)

- (dés)activer pf (-e, -d)
- (re)charger des règles (-f)
- mettre à jour une table (-T)
- afficher les connexions, les règles, ... (-s)
- tuer une connexion (-k)

- une ligne par règle
- une règle est composée d'un motif et d'une action
- le motif détermine à quels paquets/connexions seront appliqués l'action

```
block in quick on $ext_if from $evilnet
pass in quick on $ext_if proto tcp to \
$webserver port www flags S/SA keep state
block in on $ext_if all
```

- traduction d'adresse
- redirection de trafic

```
nat on $ext_if from $lan to !$lan -> ($ext_if)
rdr on $ext_if proto tcp to port www -> \
{ $webserver1, $webserver2 } round-robin
```

- les macros permettent de rendre les règles plus claires
- les tables permettent de modifier les hôtes auxquels s'appliquent certaines règles
- les ancrés permettent de charger des règles dynamiquement (pfctl -a)

```
lan="192.168/16"  
ext_if="tun0"  
table <blacklist> file /etc/blacklist  
anchor spam
```

authpf

- permet de rajouter des règles lorsqu'un utilisateur se connecte
- pseudo shell qui charge des règles sur l'ancre « authpf/* »
- déchargement des règles lorsque l'utilisateur se déconnecte

- chaque règle peut logger les paquets qui y correspondent
- les paquets sont envoyés sur une interface pflog
- le daemon pflogd lis l'interface et écrit les paquets dans les logs au format tcpdump