Suivi de connexions sous Linux

Filtrage IP :
interactions avancées avec le suivi de connexions sous Linux

E. Leblond – V. Deffontaines

Suivi de connexions ?

- Filtre de paquets
- Gestion des allers-retours
- Prise en compte de la notion de flux
- Mise en place d'un suivi des “connexions”
- Netfilter (depuis Linux 2.4.0) propose un suivi de connexions : “conntrack” (pour Connection tracking)

Utilisation sous Linux

- filtrage grâce au module STATE :
  - iptables -A FORWARD -m state –state NEW -j ACCEPT
  - iptables -I FORWARD -m state –state ESTABLISHED -j ACCEPT
- Un moyen simple d'autoriser le trafic aller et retour relatif aux connexions dont l'initialisation a été autorisée (par ex: paquets SYN pour TCP)

Dans la vraie vie

- Existence de protocoles non linéaires
  - connexions parallèles
  - ex : ftp, SIP, H323
- On ne peut plus se contenter de vérifier par rapport à un flux existant
- Moyen complémentaire:
  - Passage par un proxy
  - Mise en place d'un support du protocole dans le noyau

Le cas de Netfilter

- Principe :
  - Annonce dans le protocole => connexion parallèle à venir
- Méthode utilisée :
  - Examen des flux primaires (par ex : connexion Ftp port 21)
  - génération d'entrées temporaires (expect)
  - acceptation du paquet par la règle RELATED.

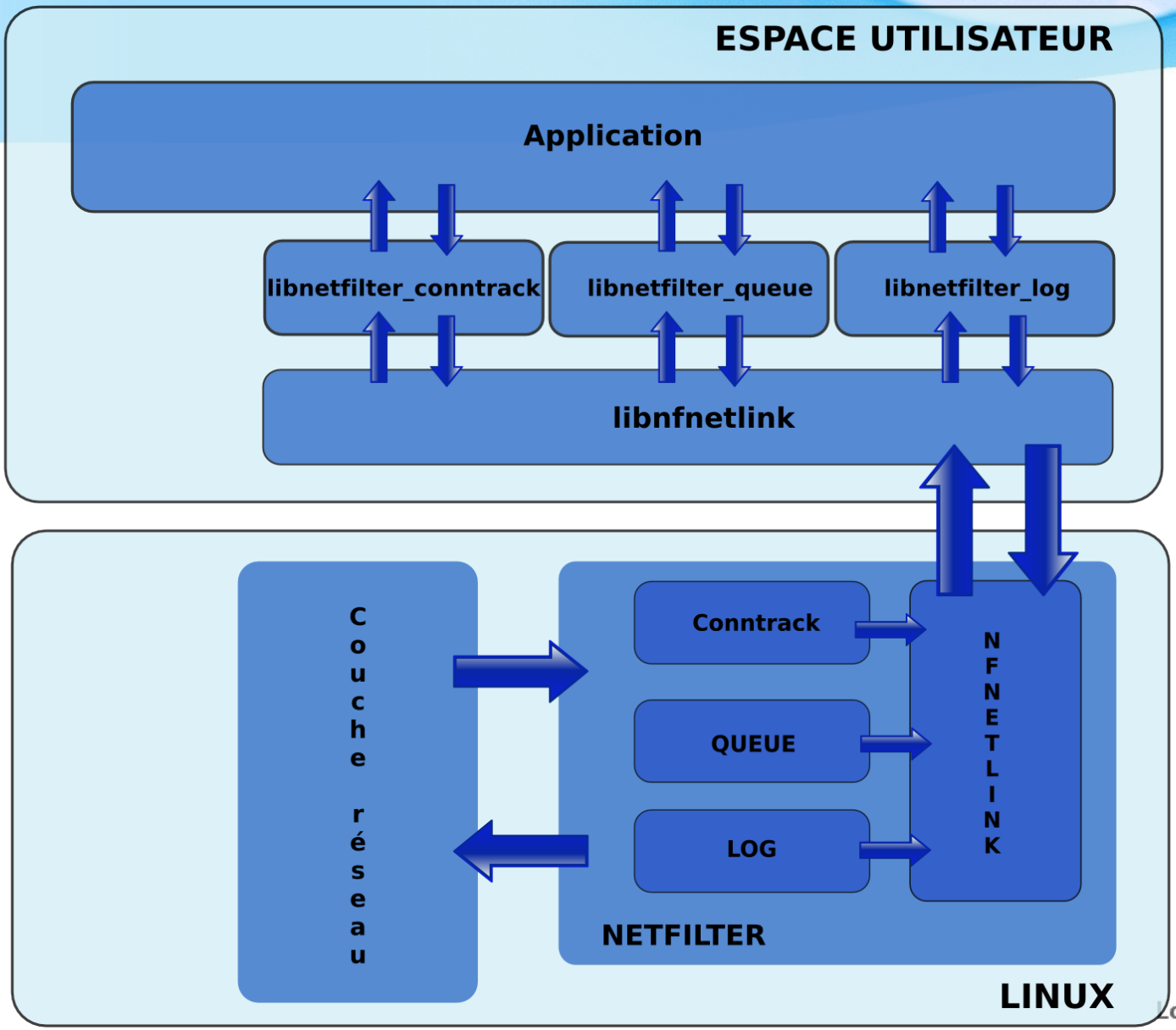
Interactions ?

- À sa sortie, Netfilter ne permet pas d'interaction de l'administrateur avec le suivi de connexions
- Possibilité de lister les connexions par :
  - /proc/net/ip_conntrack
- Insuffisant
- Dangereux : la lecture du fichier bloque le conntrack

Problématiques

- Problèmatiques :
  - Conntrack sans interaction
  - Complexification des protocoles
- Solution :
  - Offrir une infrastructure permettant la manipulation du conntrack

2.6.14 : Nouvelle architecture



libnetfilter_conntrack

- Lister les connexions :
  - conntrack -L
- Supprimer une connexion :
  - conntrack -D -p tcp –orig-sport 1234 –orig-dport 80
- Modifier une connexion
  - Coordonnées IP
  - Timeout
  - Flags : fixed_timeout, ...

libnetfilter_conntrack

- Travail sur la table “expect”
  - Lister les “expect”
  - Modifier
  - Créér
- Création d'”expect”
  - Détecter les connexions parallèles en espace utilisateur
  - Créér les “expects” depuis ce programme

Suivi des événements

- Possibilité de suivre les événements :
  - conntrack -E
- Gestion de l'activité au fur et à mesure
  - Stockage de l'activité
  - Volumétrie par connexion
  - Scripting ?

Un manque d'outils

- Problème :
  - Mise à disposition de bibliothèque en C
  - D'un outil “primaire” : conntrack
- Solution :
  - Développement d'une bibliothèque de haut-niveau en python
  - Développement d'une interface web de gestion

pynetfilter_conntrack

- Objectif :
  - fournir une abstraction à la bibliothèque C difficile à prendre en main
  - Permettre à un administrateur d'écrire des scripts de gestion
- Méthode :
  - Utilisation de ctypes pour lier C et python
  - Création d'objets python de haut niveau

Exemple de code

```
from pynetfilter_conntrack import NetfilterConntrack, CONNTRACK
nf = NetfilterConntrack(CONNTRACK)
table = nf.create_table()
filter_table = table.filter(6,orig_dst_port=22)
filter_table.display()
for entry in filter_table:
    nf.delete_conntrack(entry)
```

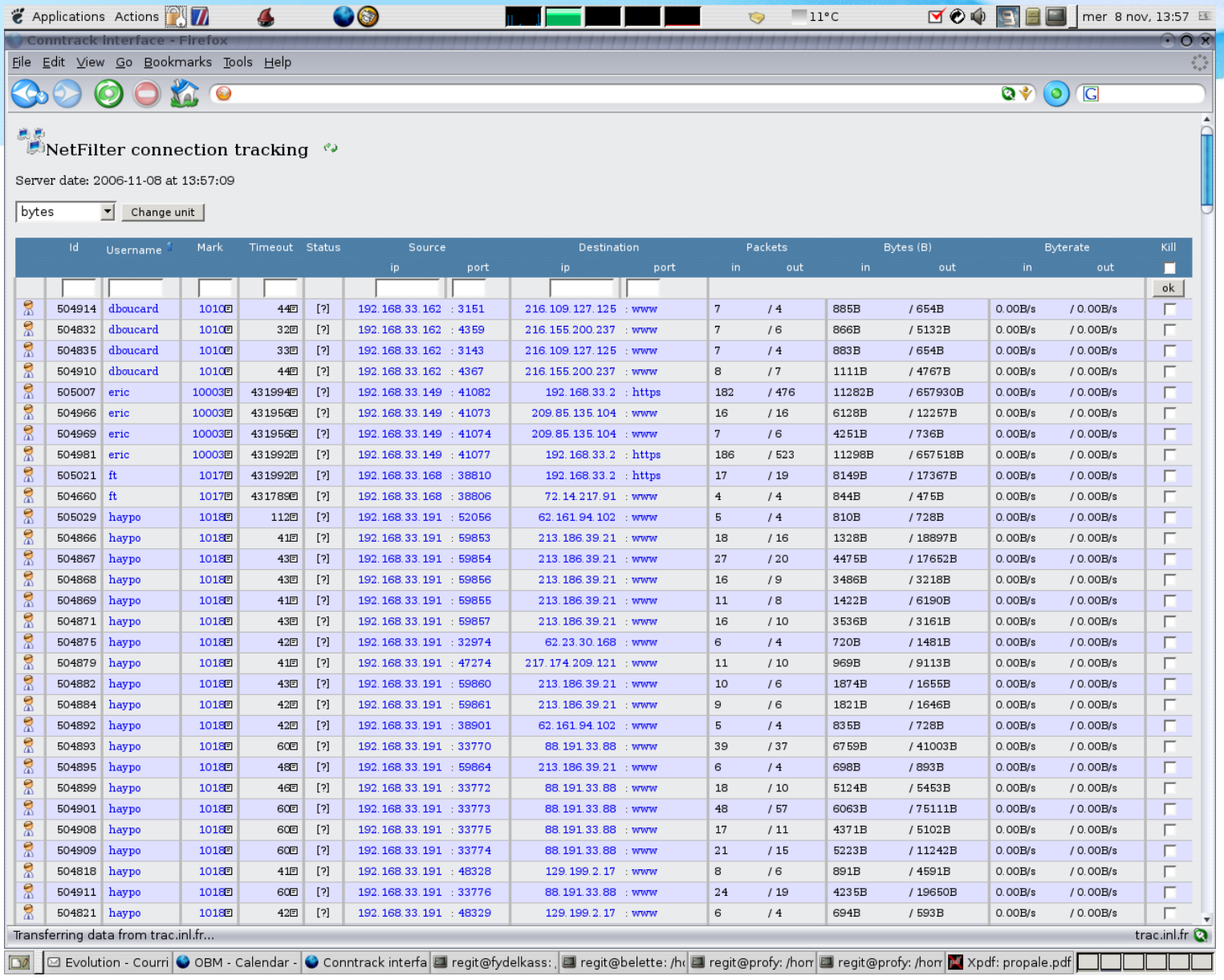
conntrack.py

- Une surcouche à pynetfilter_conntrack :
  - même niveau de fonctionnalités
  - couche d'abstraction supplémentaire (itération)
- Liste :
  - conntrack.py list
- Suppression :
  - conntrack.py delete -p tcp –orig-src-port 22

pyctd

- Serveur XML-RPC
- Mise à disposition des commandes :
  - Listing
  - Modification
  - Suppression

frontend PHP



Id	Username	Mark	Timeout	Status	Source ip	Source port	Destination ip	Destination port	Packets in	Packets out	Bytes (B) in	Bytes (B) out	Byterate in	Byterate out	Kill
															ok
504914	dboucard	1010	44	[?]	192.168.33.162	3151	216.109.127.125	www	7	/ 4	885B	/ 654B	0.00B/s	/ 0.00B/s	
504832	dboucard	1010	32	[?]	192.168.33.162	4359	216.155.200.237	www	7	/ 6	866B	/ 5132B	0.00B/s	/ 0.00B/s	
504835	dboucard	1010	33	[?]	192.168.33.162	3143	216.109.127.125	www	7	/ 4	883B	/ 654B	0.00B/s	/ 0.00B/s	
504910	dboucard	1010	44	[?]	192.168.33.162	4367	216.155.200.237	www	8	/ 7	1111B	/ 4767B	0.00B/s	/ 0.00B/s	
505007	eric	10003	431994	[?]	192.168.33.149	41082	192.168.33.2	https	182	/ 476	11282B	/ 657930B	0.00B/s	/ 0.00B/s	
504966	eric	10003	431956	[?]	192.168.33.149	41073	209.85.135.104	www	16	/ 16	6128B	/ 12257B	0.00B/s	/ 0.00B/s	
504969	eric	10003	431956	[?]	192.168.33.149	41074	209.85.135.104	www	7	/ 6	4251B	/ 736B	0.00B/s	/ 0.00B/s	
504981	eric	10003	431992	[?]	192.168.33.149	41077	192.168.33.2	https	186	/ 523	11298B	/ 657518B	0.00B/s	/ 0.00B/s	
505021	ft	1017	431992	[?]	192.168.33.168	38810	192.168.33.2	https	17	/ 19	8149B	/ 17367B	0.00B/s	/ 0.00B/s	
504660	ft	1017	431789	[?]	192.168.33.168	38806	72.14.217.91	www	4	/ 4	844B	/ 475B	0.00B/s	/ 0.00B/s	
505029	haypo	1018	112	[?]	192.168.33.191	52056	62.161.94.102	www	5	/ 4	810B	/ 728B	0.00B/s	/ 0.00B/s	
504866	haypo	1018	41	[?]	192.168.33.191	59853	213.186.39.21	www	18	/ 16	1328B	/ 18897B	0.00B/s	/ 0.00B/s	
504867	haypo	1018	43	[?]	192.168.33.191	59854	213.186.39.21	www	27	/ 20	4475B	/ 17652B	0.00B/s	/ 0.00B/s	
504868	haypo	1018	43	[?]	192.168.33.191	59856	213.186.39.21	www	16	/ 9	3486B	/ 3218B	0.00B/s	/ 0.00B/s	
504869	haypo	1018	41	[?]	192.168.33.191	59855	213.186.39.21	www	11	/ 8	1422B	/ 6190B	0.00B/s	/ 0.00B/s	
504871	haypo	1018	43	[?]	192.168.33.191	59857	213.186.39.21	www	16	/ 10	3536B	/ 3161B	0.00B/s	/ 0.00B/s	
504875	haypo	1018	42	[?]	192.168.33.191	32974	62.23.30.168	www	6	/ 4	720B	/ 1481B	0.00B/s	/ 0.00B/s	
504879	haypo	1018	41	[?]	192.168.33.191	47274	217.174.209.121	www	11	/ 10	969B	/ 9113B	0.00B/s	/ 0.00B/s	
504882	haypo	1018	43	[?]	192.168.33.191	59860	213.186.39.21	www	10	/ 6	1874B	/ 1655B	0.00B/s	/ 0.00B/s	
504884	haypo	1018	42	[?]	192.168.33.191	59861	213.186.39.21	www	9	/ 6	1821B	/ 1646B	0.00B/s	/ 0.00B/s	
504892	haypo	1018	42	[?]	192.168.33.191	38901	62.161.94.102	www	5	/ 4	835B	/ 728B	0.00B/s	/ 0.00B/s	
504893	haypo	1018	60	[?]	192.168.33.191	33770	88.191.33.88	www	39	/ 37	6759B	/ 41003B	0.00B/s	/ 0.00B/s	
504895	haypo	1018	48	[?]	192.168.33.191	59864	213.186.39.21	www	6	/ 4	698B	/ 893B	0.00B/s	/ 0.00B/s	
504899	haypo	1018	46	[?]	192.168.33.191	33772	88.191.33.88	www	18	/ 10	5124B	/ 5453B	0.00B/s	/ 0.00B/s	
504901	haypo	1018	60	[?]	192.168.33.191	33773	88.191.33.88	www	48	/ 57	6063B	/ 75111B	0.00B/s	/ 0.00B/s	
504908	haypo	1018	60	[?]	192.168.33.191	33775	88.191.33.88	www	17	/ 11	4371B	/ 5102B	0.00B/s	/ 0.00B/s	
504909	haypo	1018	60	[?]	192.168.33.191	33774	88.191.33.88	www	21	/ 15	5223B	/ 11242B	0.00B/s	/ 0.00B/s	
504818	haypo	1018	41	[?]	192.168.33.191	48328	129.199.2.17	www	8	/ 6	891B	/ 4591B	0.00B/s	/ 0.00B/s	
504911	haypo	1018	60	[?]	192.168.33.191	33776	88.191.33.88	www	24	/ 19	4235B	/ 19650B	0.00B/s	/ 0.00B/s	
504821	haypo	1018	42	[?]	192.168.33.191	48329	129.199.2.17	www	6	/ 4	694B	/ 593B	0.00B/s	/ 0.00B/s	

Réplication du conntrack

- ct-sync :
  - Réplication au niveau noyau
  - Développement plus ou moins arrété
- Conntrackd :
  - En mode utilisateur
  - Basé sur libnetfilter_conntrack
  - Actif

Conclusion

- libnetfilter_conntrack :
  - Une infrastructure puissante
  - Des utilisations intéressantes : conntrackd
- pynetfilter_conntrack :
  - Une interface de choix pour l'administrateur avancé
- pyctd :
  - Un outil pour l'administrateur

Questions ?

- libnetfilter_conntack : http://www.netfilter.org/
- pynetfilter_conntrack, pyctd : http://software.inl.fr/
- INL : http://www.inl.fr/