Le mode transport IPSec face à netfilter un autre “cheval de Troie”?

Yoann ALLAIN

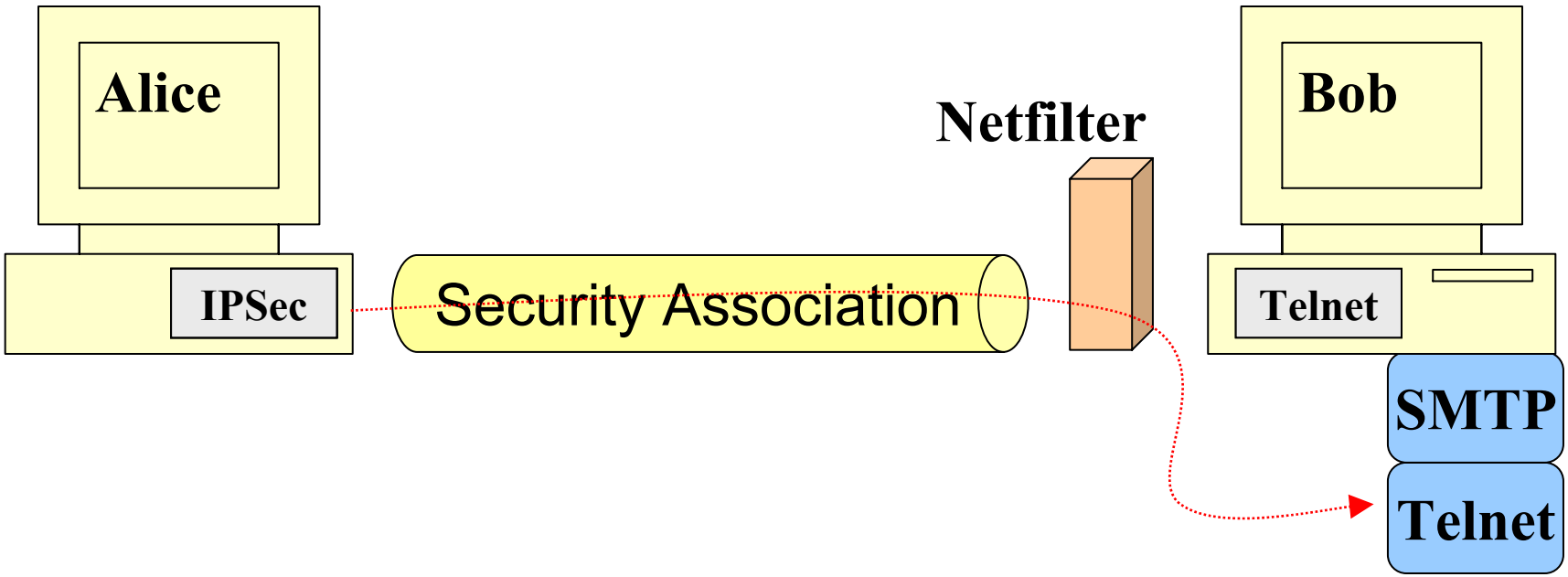
Stagiaire au Security Lab
Encadrants : Olivier Courtay et Nicolas Prigent

Protéger les communications

Les outils de Linux 2.6

OUTIL	FONCTION
IPSec	Chiffrement
Netfilter / Iptables	Filtrage

Le problème

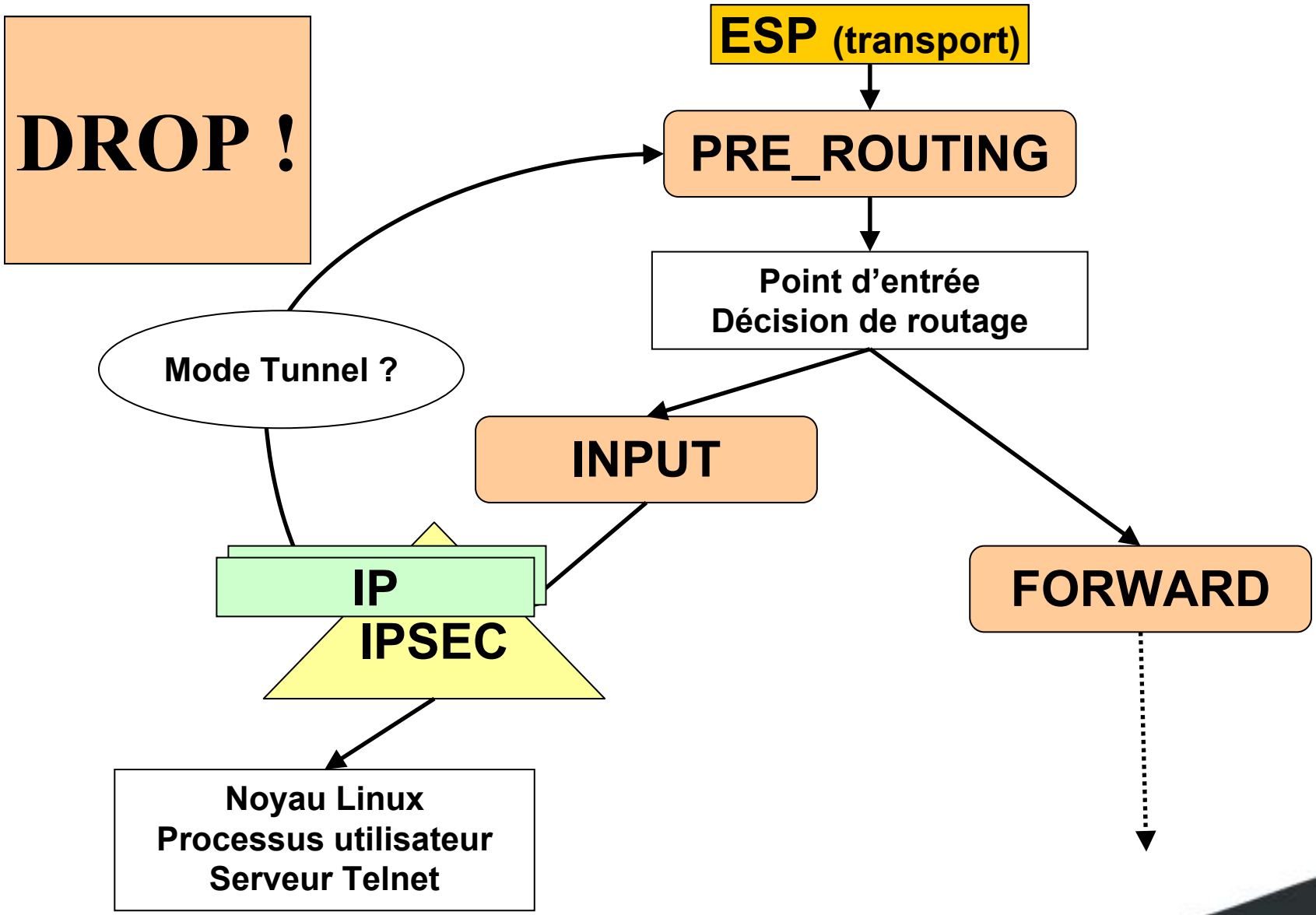


1. Bob: 2 serveurs
2. spdadd ip_alice ip_bob[25] tcp -P in ipsec esp/tranport//require;
3. iptables –A INPUT –p tcp –dport 23 –j DROP
4. Alice peut-elle atteindre le serveur Telnet ?

=> OUI !

Pourquoi ?

Petit tour dans la stack IP Linux



Des solutions ?

- Filtrage simple par IPSec, mais pas de suivi de connexion possible :

```
spdadd ip_alice ip_bob[25] tcp -P in ipsec
                        esp/transport//require;
spdadd ip_alice ip_bob          any -P in discard;
```

- Patch du noyau mais problèmes liés au NAT.
  Imitation du mode tunnel ?
  Non conseillé par les développeurs du noyau.

- Utiliser le mode tunnel tout le temps ?
  Pose des problèmes de sécurité et de performances.

Association Netfilter/IPSec risquée sans connaissance de leurs limitations

Questions ?

yoann.allain@thomson.net