3TI
Sécurité des réseaux informatiques
2015-2016

Les firewalls

V.Van den Schrieck

Firewall :

Quoi? Où? Quand? Comment?

Motivations

- Réseau d'entreprise ⟷ Internet
- Internet : Besoin/Menace?
- Protection au niveau des hôtes?

Caractéristiques des FW

- Point de passage unique de l'ensemble des flux de trafic
- Filtrage du trafic en fonction de la politique de sécurité
- Sécurisation du FW

Avantages

- Prévention des intrusions
- Simplification de la gestion de la sécurité
- Point d'observation du trafic
- Politique d'accès sur différents critères (IP, port, applications, identité, horaire, …)
- Hébergement de services supplémentaires (IPS, NAT, IPSec, …)

Types de firewall

- Stateless
- Stateful
- Gateway applicative
- Gateway niveau circuit

Firewall Stateless

Rule	Direction	IP Src	IP Dst	Protocol	Dst port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	r6c5	Any	Deny

Firewall stateless

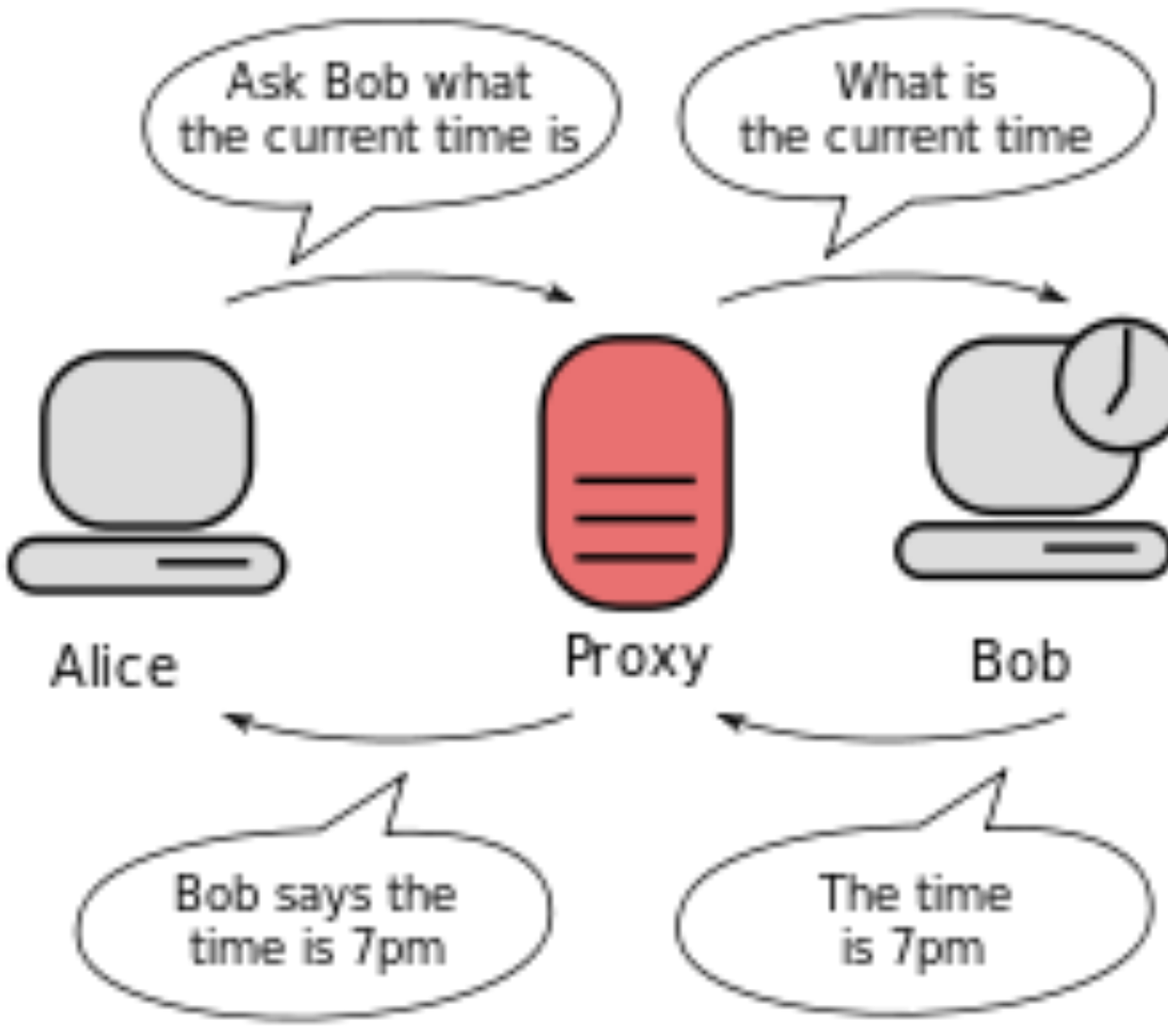
Inconvénients :

- Spoofing d'adresses IP
- Attaques par source routine
- Attaques par petits fragments

Firewall Stateful

- Fonctionnalité supplémentaire : Filtrer sur base de l'état de la connexion TCP
- Que faut-il pour faire ça?

Gateway applicative / Proxy



http://en.wikipedia.org/wiki/Proxy_server

Principes du Proxy

- Point de terminaison des connexions TCP
- Nécessité d'implémenter le protocole applicatif concerné
- Relai applicatif : Reçoit la requête, effectue des opérations (filtrage, authentification,…), puis retransmet la requête à la destination originale

Types de proxy

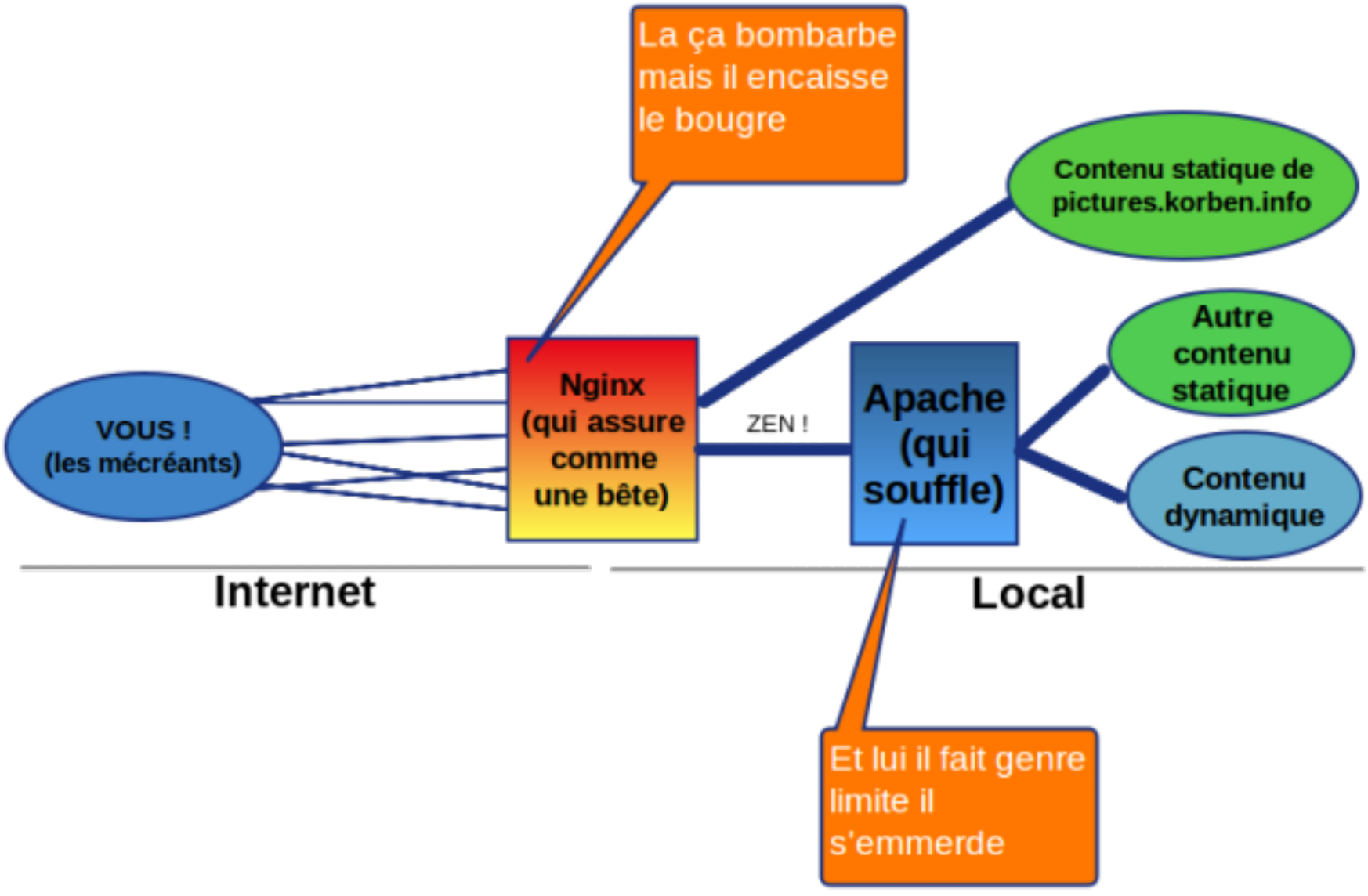
Proxy HTTP :

- Usages?
- Explicite ou transparent
- Apache, Squid, nginx, …
- Proxy public

Types de proxy

- Proxy = Protection du client
- Reverse proxy = Protection du serveur
  - Objectifs?

Reverse proxy : Exemple



http://korben.info/configurer-nginx-reverse-proxy.html

Types de proxy

Proxies FTP, Mail, DNS :

- Usages?

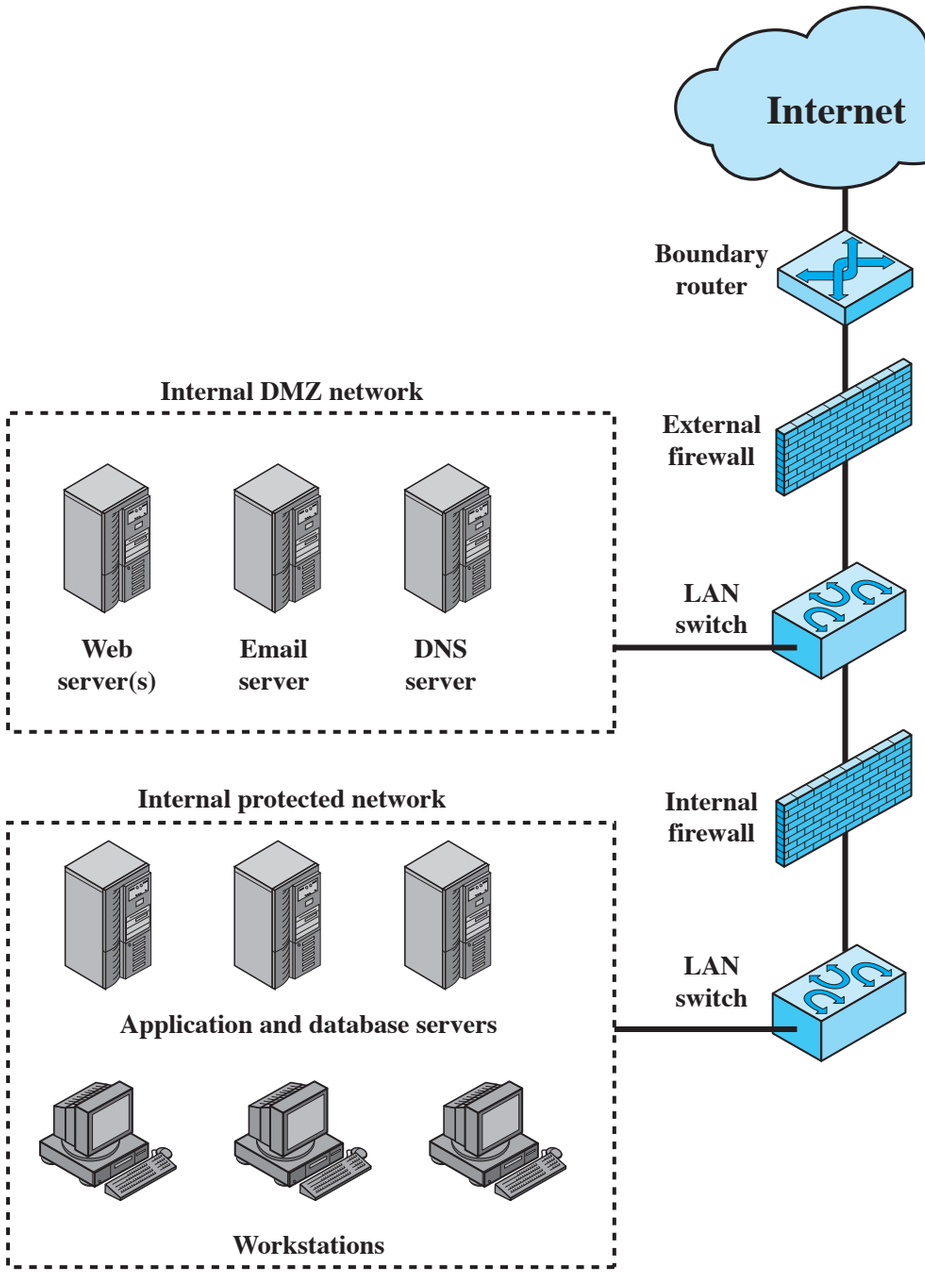
Gateway niveau circuit

- Proxy au niveau transport
  - Objectif?
  - SOCKS

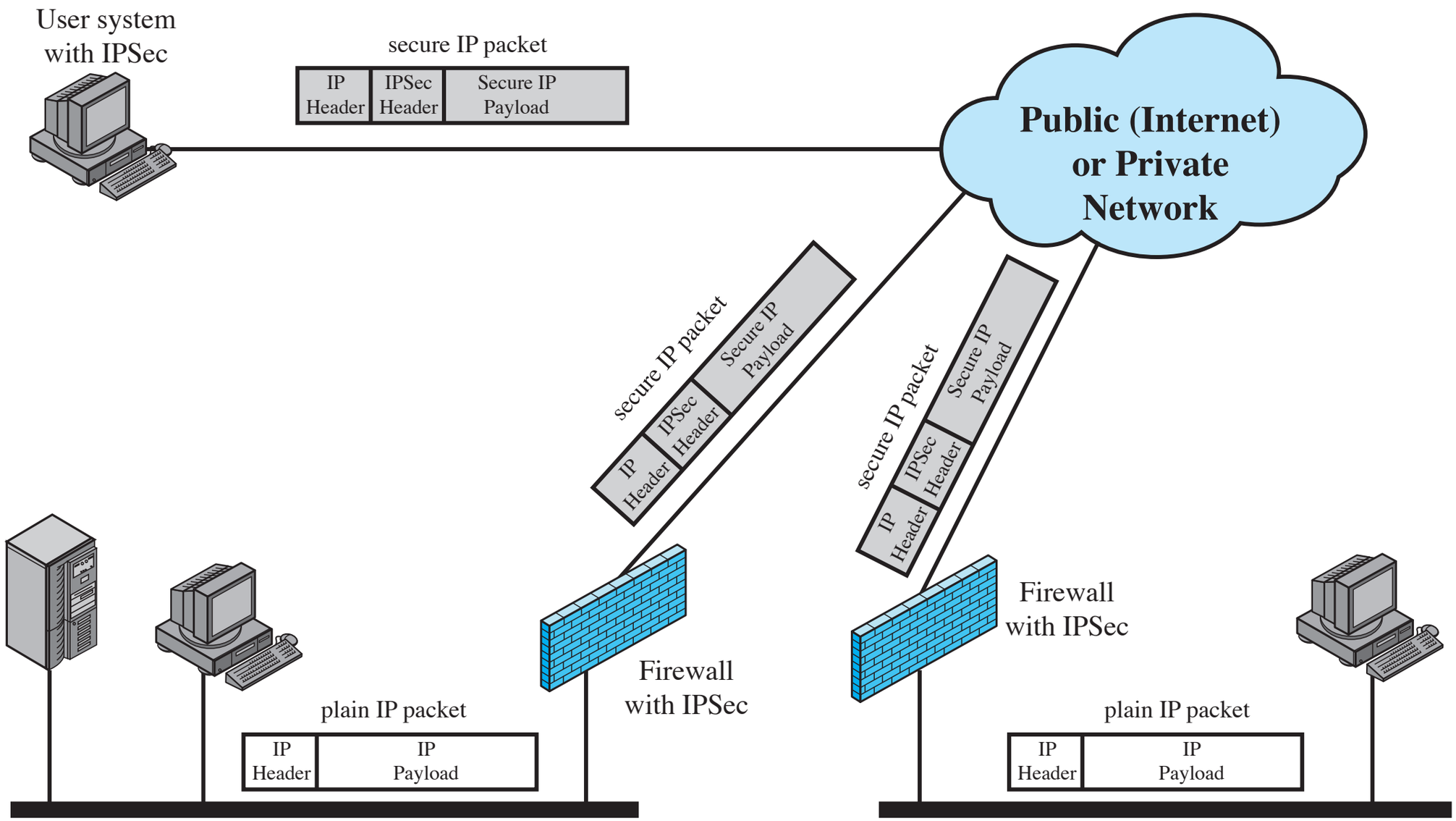
Sur quelle machine installer un FW?

- Bastion
- Firewall sur un hôte
  - Serveur
  - PC

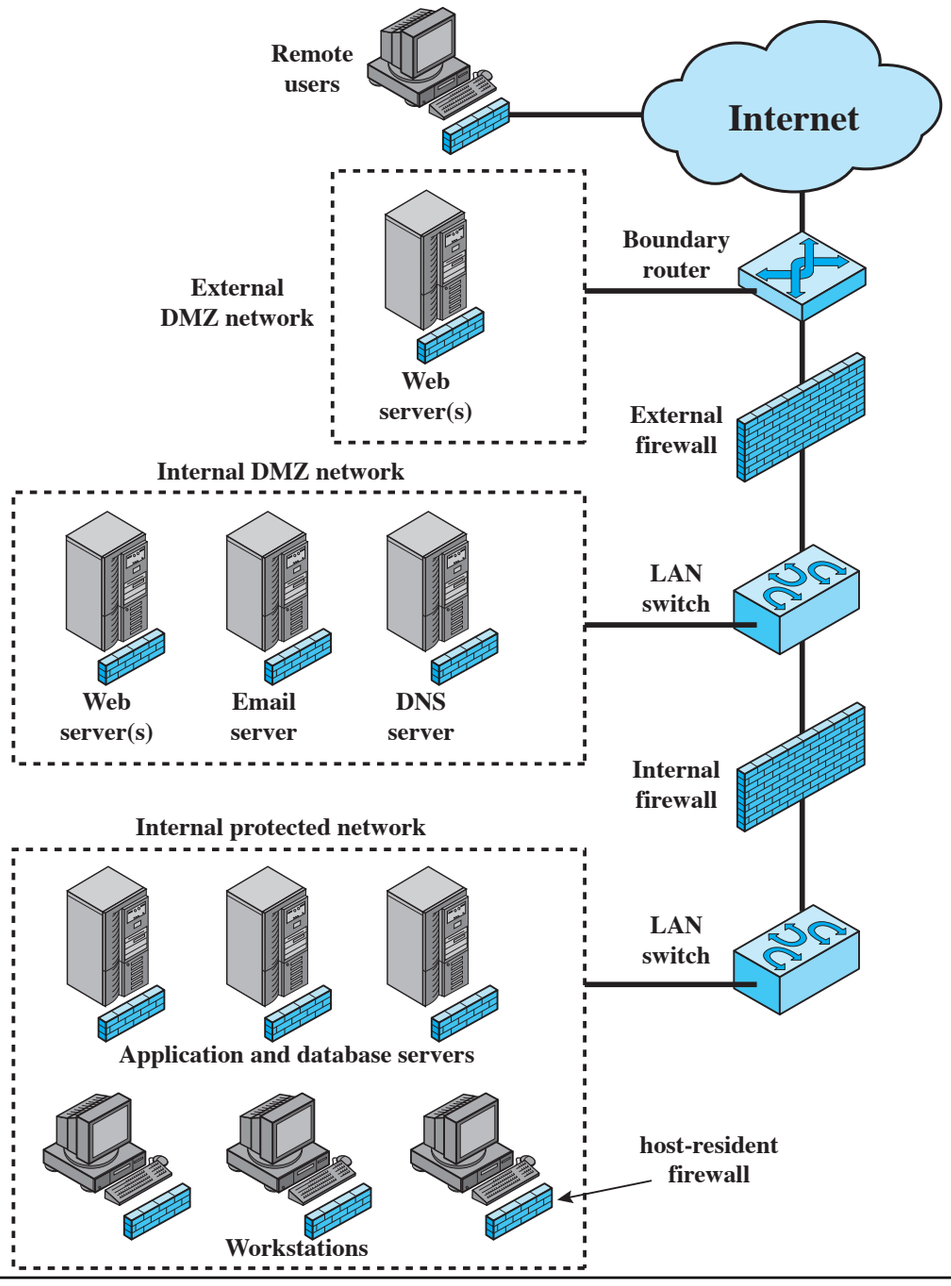
Architecture des FWs



Architecture des FW



Architecture des FW



Synthèse des architectures

- FW sur les hôtes
- Router-FW
- Bastion unique en ligne
- Bastion unique en T
- Double bastion en ligne
- Double bastion en T
- FW distribué

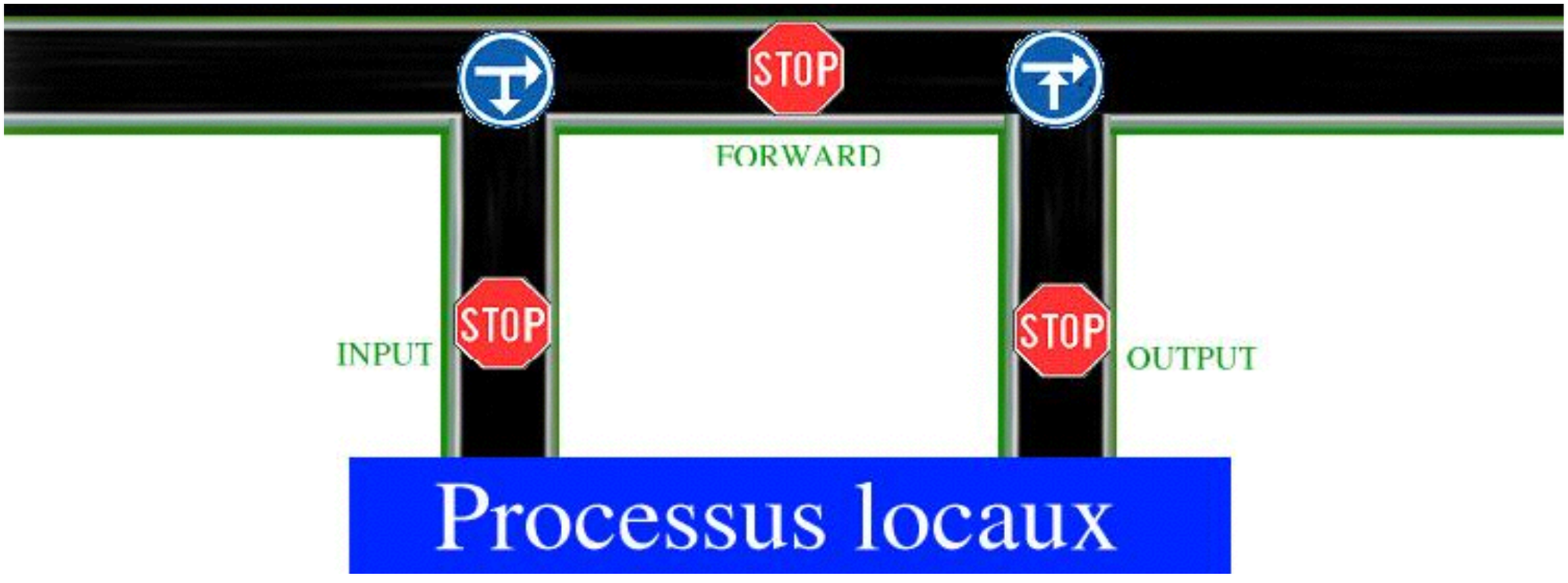
Case Study : iptables

```
iptables -A INPUT  -s 192.168.0.0/24  -p tcp --dport 80 -j REJECT
```

```
iptables –A PREROUTING –t nat –p tcp –i eth0 –d 14.15.16.21
        –dport 5900 –j DNAT –to 192.168.0.2:5900
```

Case Study : iptables

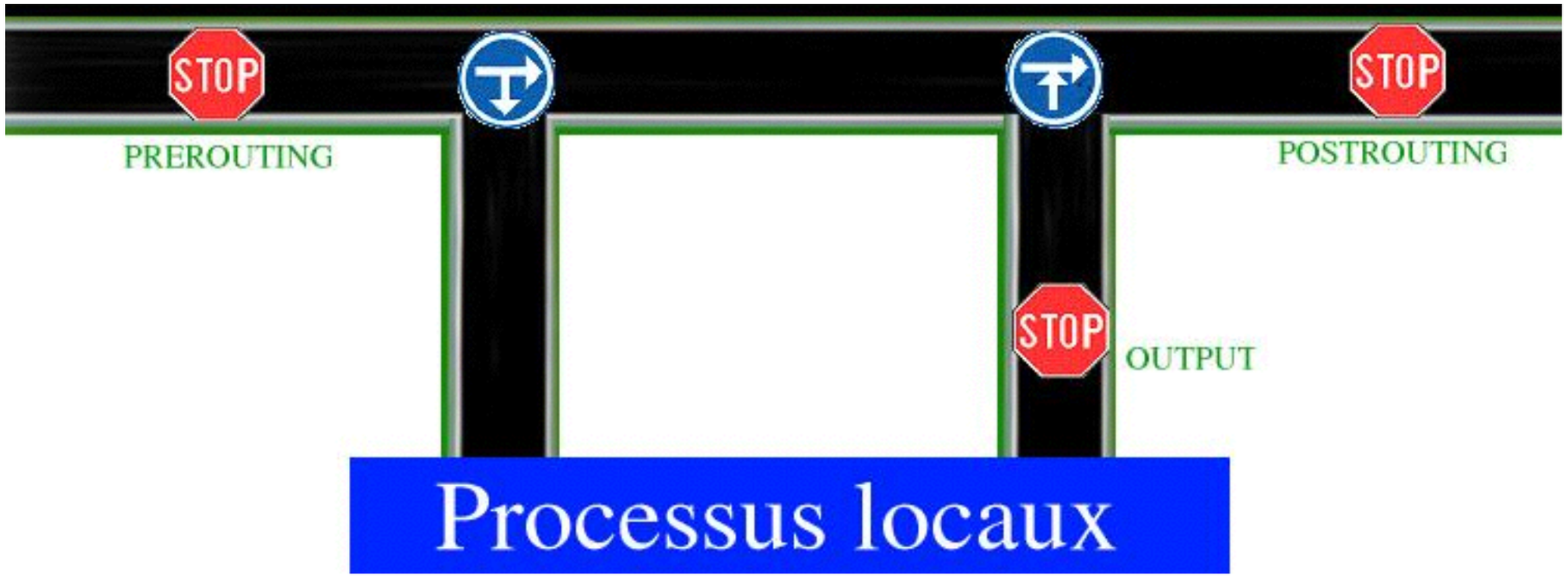
Filtrage :



Olivier Allard-Jacquin : http://olivieraj.free.fr/fr/linux/information/firewall/fw-03-04.html (26/10)

Case Study : iptables

NAT :



Olivier Allard-Jacquin : http://olivieraj.free.fr/fr/linux/information/firewall/fw-03-04.html (26/10)