FIELDS

Problématique

- Avis du CERT Renater
  - Basés sur les communications ;
  - Orientés extrusion ;
- Non intrusif
- Forensic réseau

NSM (1/3)

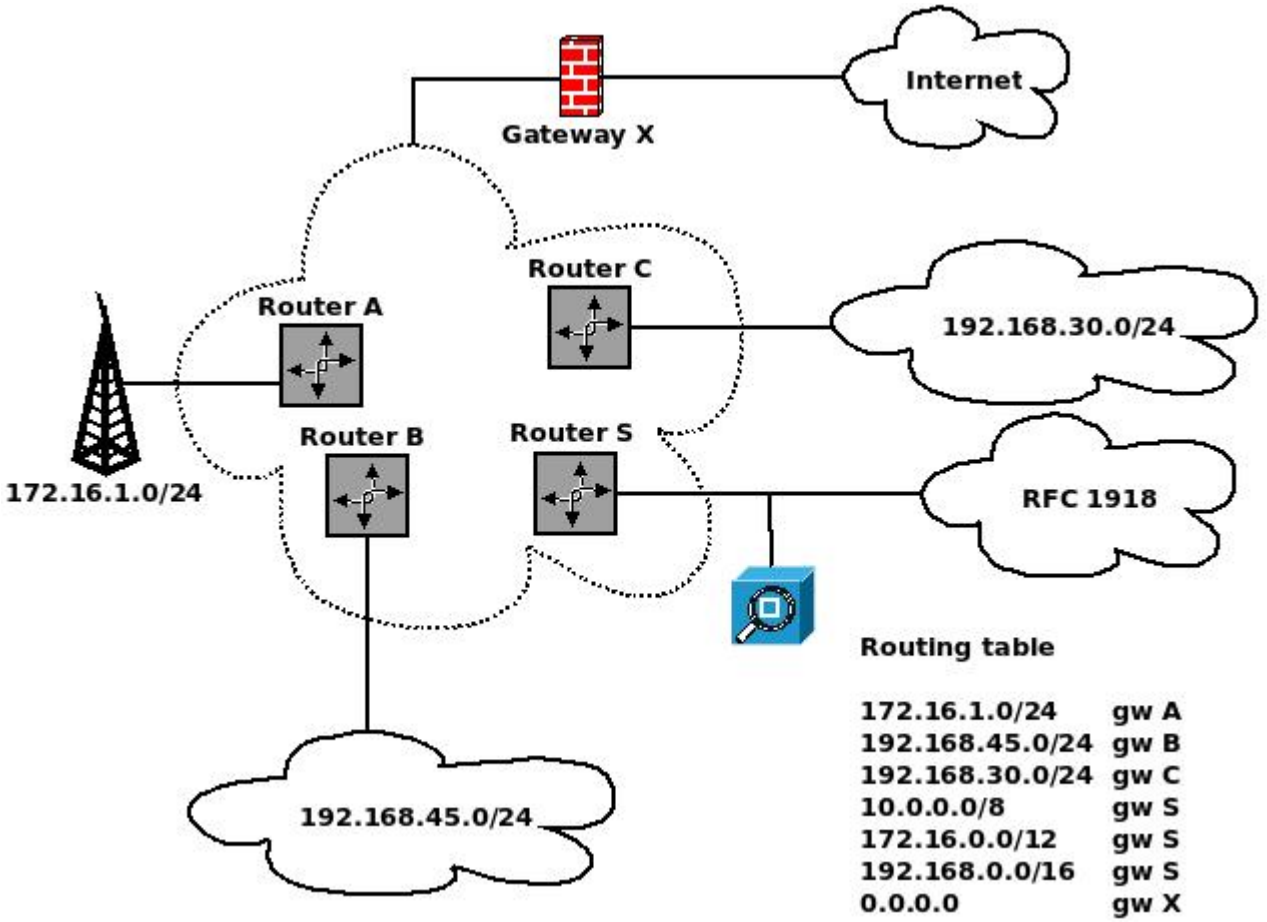
- Network Security Monitoring
- « Un réseau défendable est un réseau sur lequel on voit quelque chose » (Richard Bejlitch)
- Discipline englobant la détection d'intrusion

NSM (2/3)

- Statistiques globales (nombre de paquets TCP)
- Flux réseau (qui a parlé avec qui, quantité de données échangées ...)
- Alertes (NIDS)
- Capture exhaustive (PCAP)

NSM (3/3)

- Exemple d'heuristique : le sinkhole IP



Packet Filter (PF)

- Pare-feu issu du monde BSD
- Tables
- Log des paquets au format PCAP
- Proxy applicatifs en userland

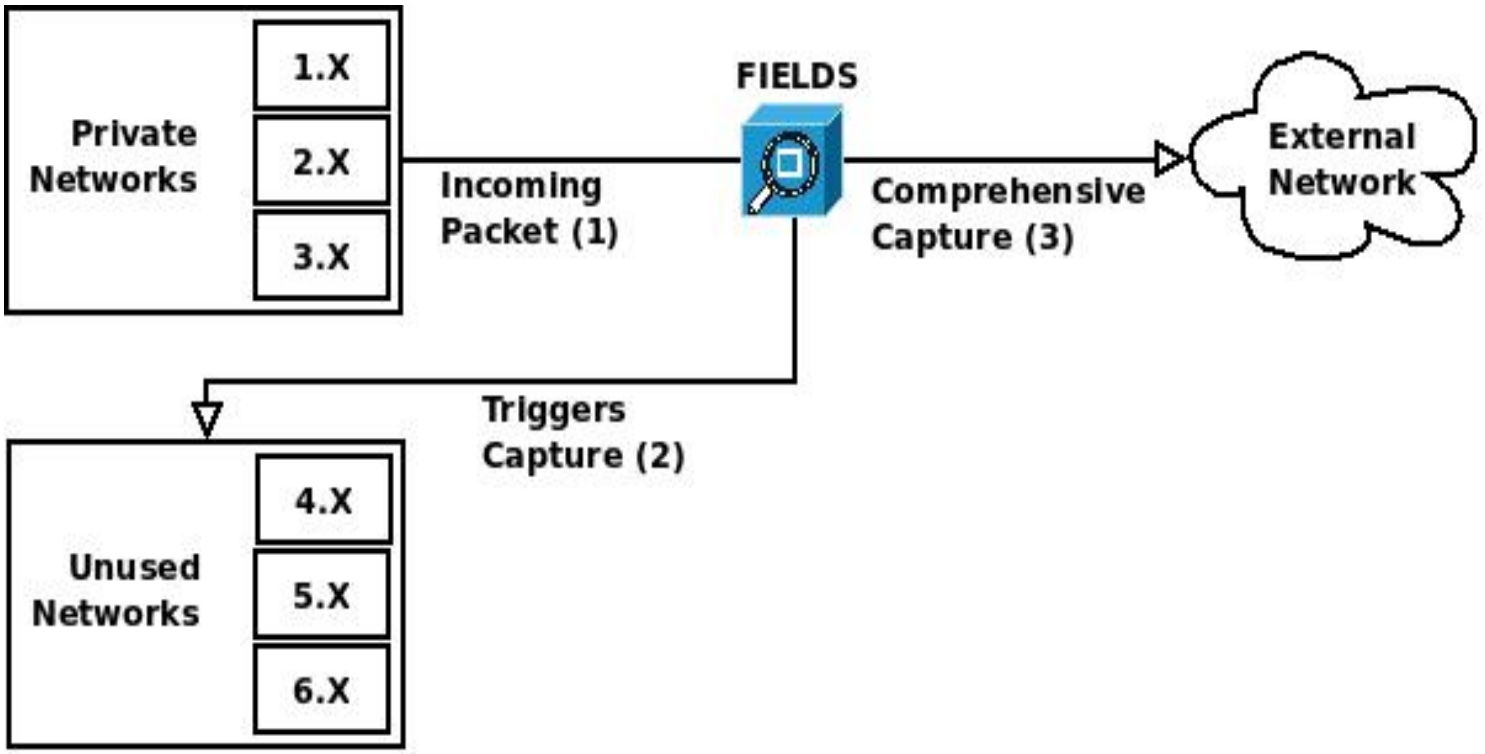
FIELDS (1/3)

- Patch pour PF
  - Ajoute un mot clé « add » à la grammaire du jeu de règles ;
  - Ajout de l'IP source et / ou destination à une table ;

    pass in log on { em0 em1 } from $FEDE to $sinkhole no state add ip src <univ_to_sinkhole>
- Modélisation d'heuristiques

FIELDS (2/3)

- Sinkhole IP :



FIELDS (3/3)

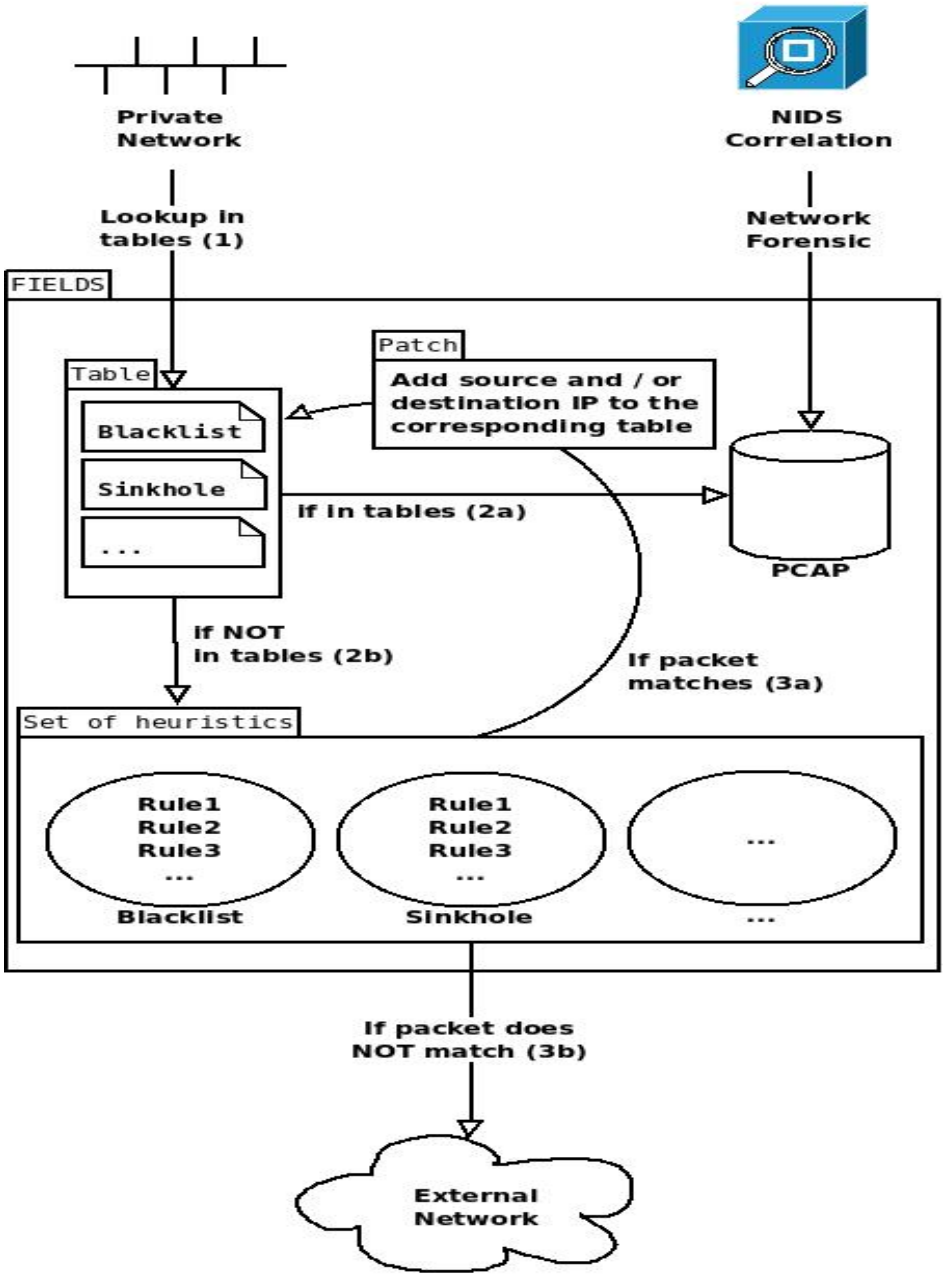
pass in log on { em0 em1 } from $FEDE to $sinkhole no state add ip src <univ_to_sinkhole>

pass in quick log on { em0 em1 } from <univ_to_sinkhole> to any no state

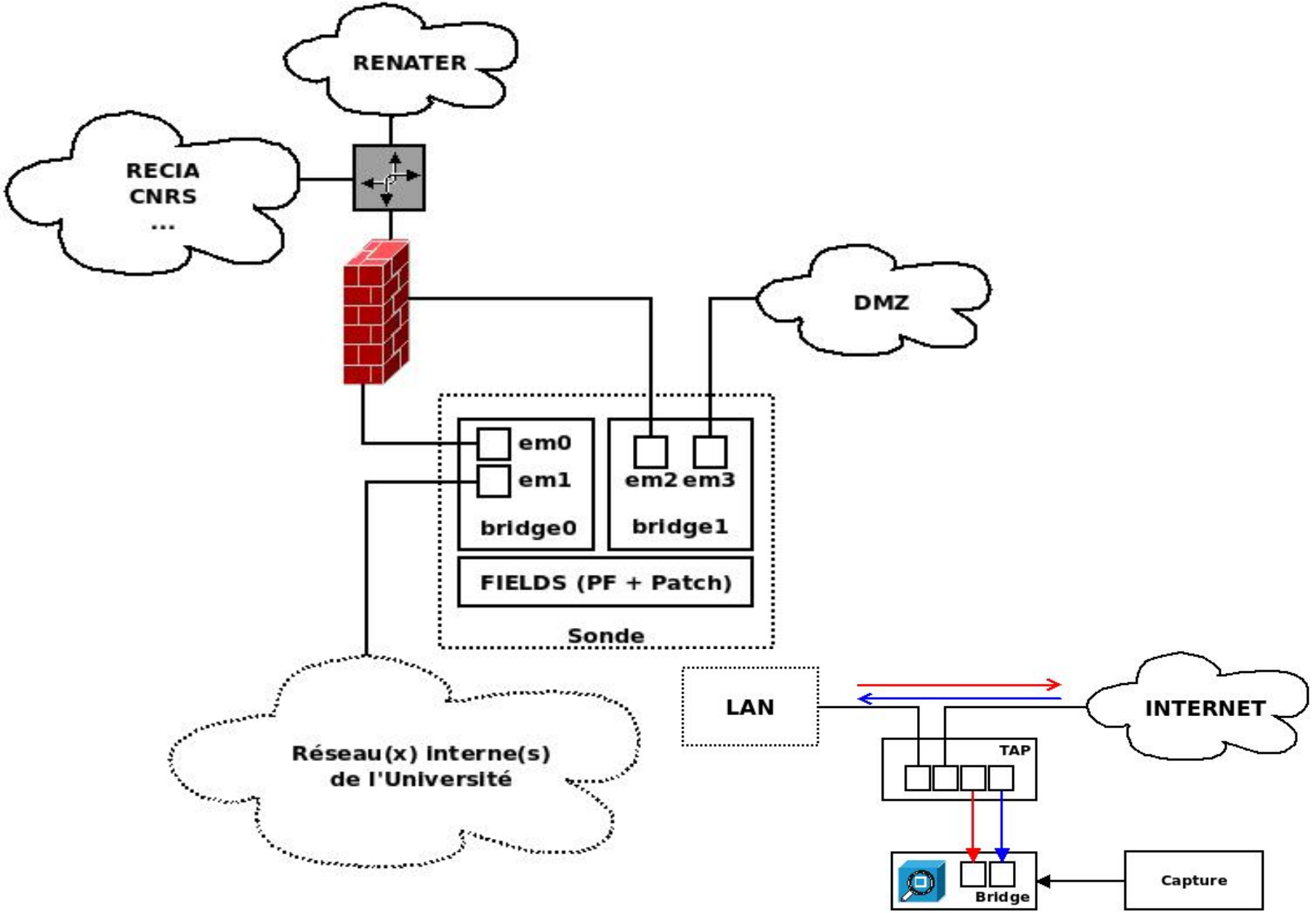
pass in quick log on { em0 em1 } from any to <univ_to_sinkhole> no state

pass quick on { em0 em1 } from $FEDE to $FEDE no state

Architecture de FIELDS



Expérimentation



Résultats

Heuristiques	Nombre d'IP	Infecté	Configuration	Non confirmé	Formaté
Blacklist	10	90 %	0 %	10 %	0 %
Bruteforce	0	0 %	0 %	0 %	0 %
Sinkhole IP	163	22 %	11 %	32 %	35 %
Sinkhole DNS	45	82 %	0 %	18 %	0 %
Sinkhole Windows	44	64 %	15 %	21 %	0 %