

Sonde IDS durcie

Pierre Chifflier Arnaud Fontaine

{pierre.chifflier, arnaud.fontaine}@ssi.gouv.fr



25 novembre 2014

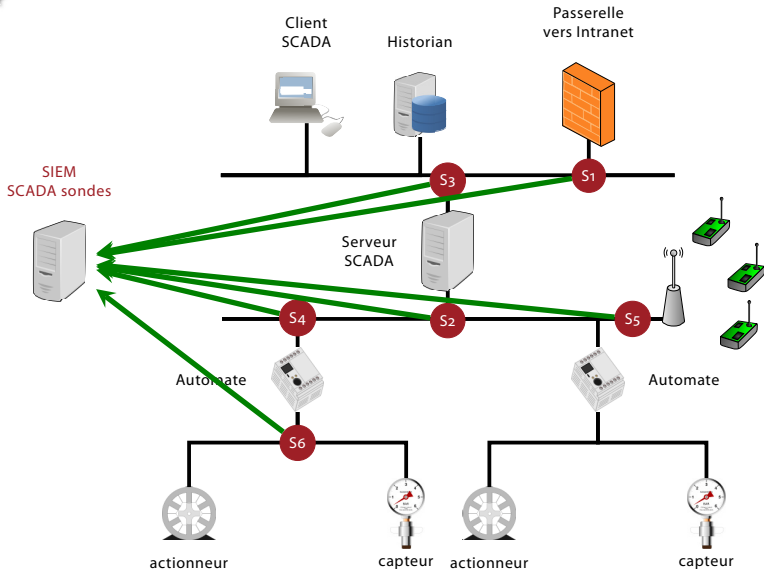


Caractéristiques d'un réseau de supervision de sécurité

- ▶ Collecte d'informations depuis tous les éléments
- ▶ Basé sur des *Intrusion Detection System*
- ▶ Nombreux décodeurs protocolaires
- ▶ Centralisation et analyse

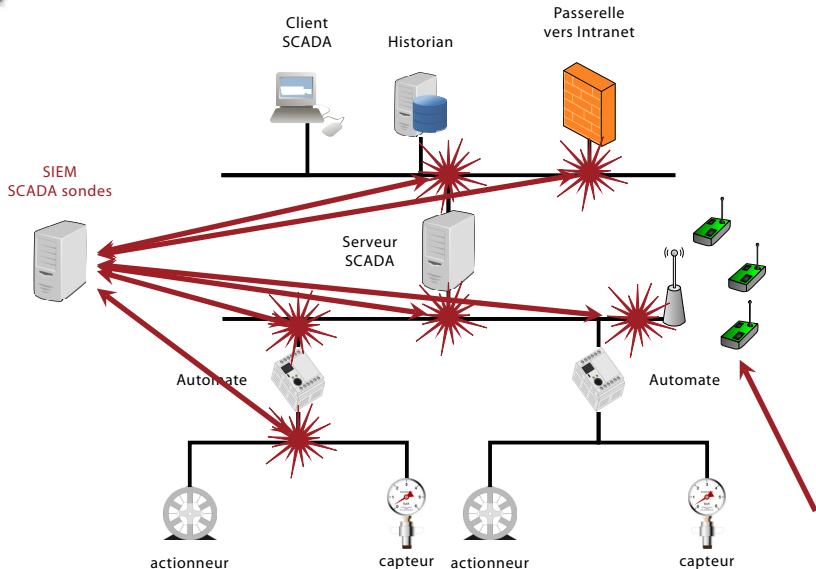


IDS : Où détecter ?





IDS : vu de l'attaquant





IDS pour l'attaquant

- ▶ Éléments identiques
- ▶ Connectés à tous les éléments importants
- ▶ Nombreux décodeurs protocolaires
- ▶ Écrits pour la performance
- ▶ Exposés au trafic réseau

⇒ Cible de choix !



Architecture système sécurisée

- ▶ Architecture générique
- ▶ Protection de la sonde
- ▶ Protection du réseau de supervision
- ▶ Cloisonnement des rôles
- ▶ Limitation et suppression de privilèges

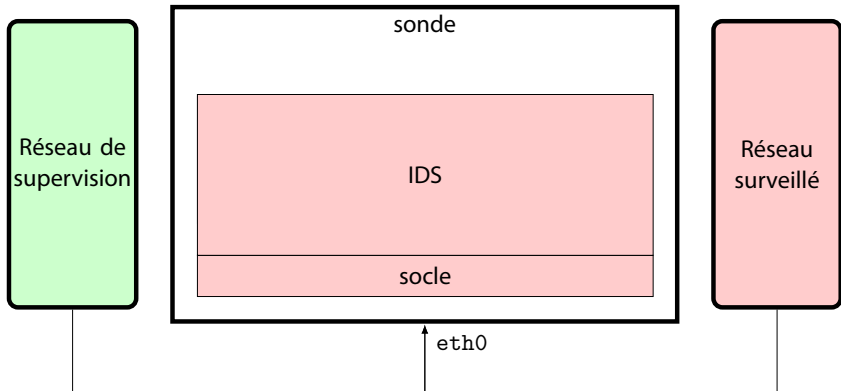


Définition des rôles

- 1 IDS
- 2 Administrateur de l'IDS
- 3 Audit
- 4 Administrateur système
- 5 Système



Sonde : état initial



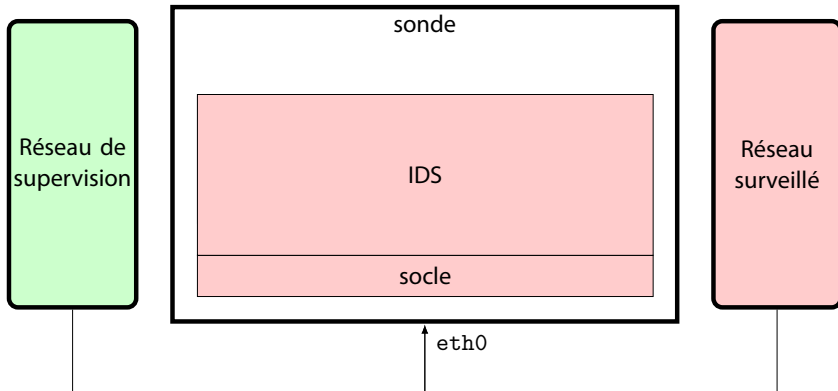


Cloisonnement réseau

- ▶ Séparation des réseaux
 - ▶ Supervision
 - ▶ Réseau surveillé
 - ▶ Administration
- ▶ Utilisation d'un ou plusieurs canaux IPsec

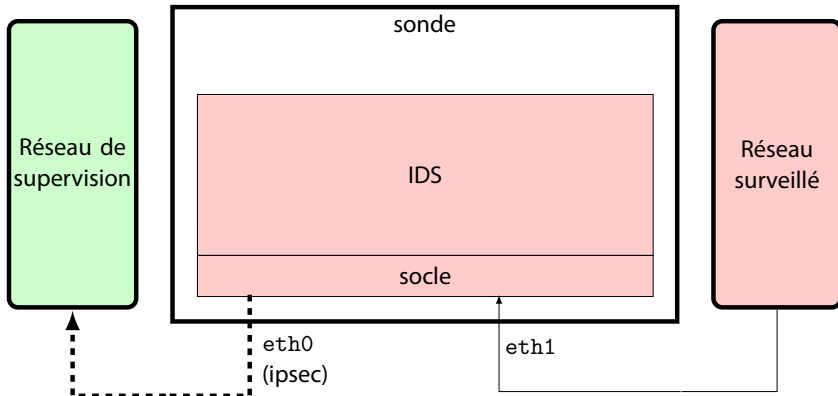


Sonde : état initial





Étape 1 : séparation des réseaux





Durcissement du socle et du noyau

- ▶ Réduction des droits administrateur
- ▶ Suppression des fonctions inutiles
- ▶ Rendre immuable la sonde
- ▶ Empêche/complique l'exécution de code
- ▶ ...
- ▶ Note : complique la mise à jour



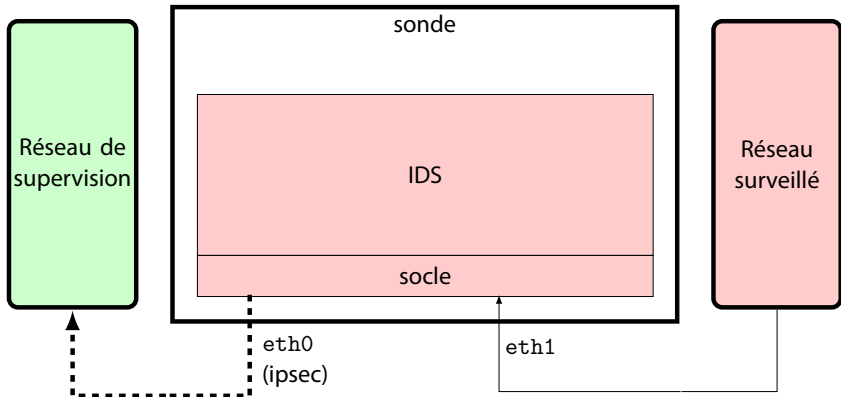
Patch grsec/PaX

- ▶ Espace d'adressage aléatoire
- ▶ Pages mémoire en lecture seule
- ▶ $W \oplus X$
- ▶ Restrictions
 - ▶ visibilité
 - ▶ interdiction du *debug*
 - ▶ ...
- ▶ Points de montage en lecture seule (irréversible)



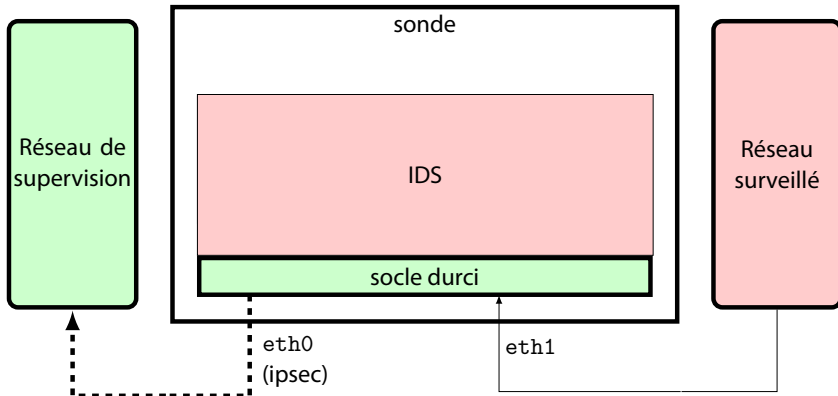


Étape 1 : séparation des réseaux





Étape 2 : durcissement du socle





Cloisonnement

Principes

- ▶ Isolation des IDS entre eux
- ▶ Isolation des IDS et du socle
- ▶ Suppression de l'accès au matériel



Mise en œuvre

- ▶ Utilisation des *Linux Containers* (LXC)
- ▶ Réduction des privilèges
- ▶ Duplication des flux réseau par un *bridge*

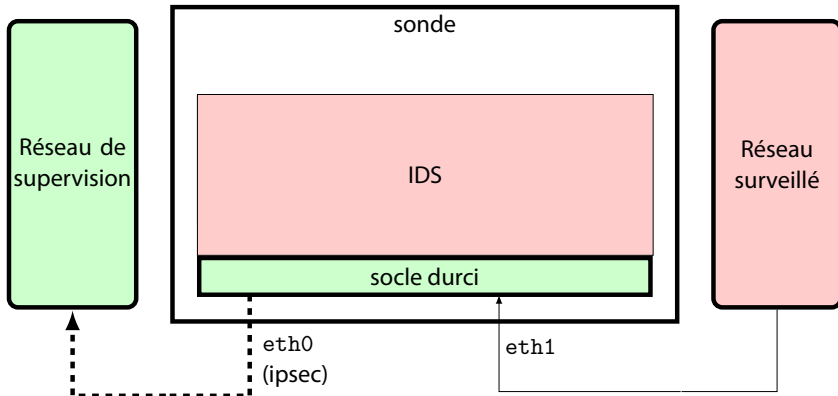


IDS

- ▶ Système en lecture seule
- ▶ Configuration figée
- ▶ Extension du principe $W \oplus X$ aux fichiers

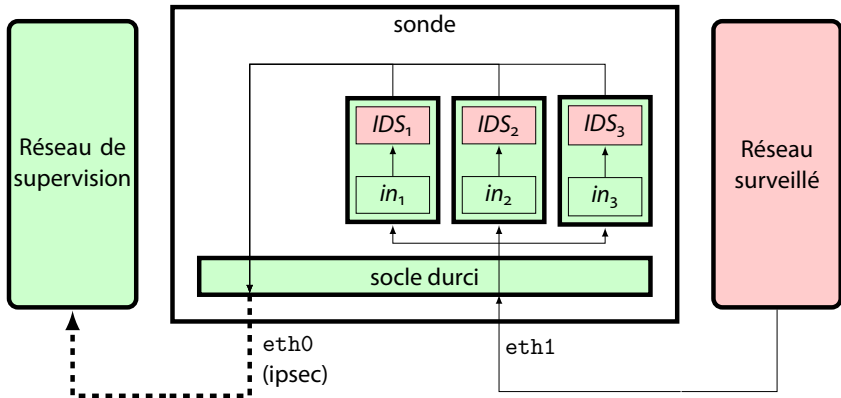


Étape 2 : durcissement du socle





Étape 3 : cloisonnement des IDS



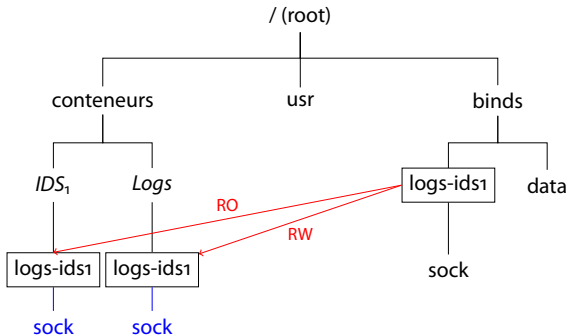


Journalisation

- ▶ Émission des alertes par les IDS
- ▶ Interdiction des modifications par l'IDS
- ▶ Rôle administrateur IDS : pas d'accès aux journaux
- ▶ Intégrité des journaux
- ▶ Centralisation des alertes, envoi vers le réseau de supervision



Isolation des données

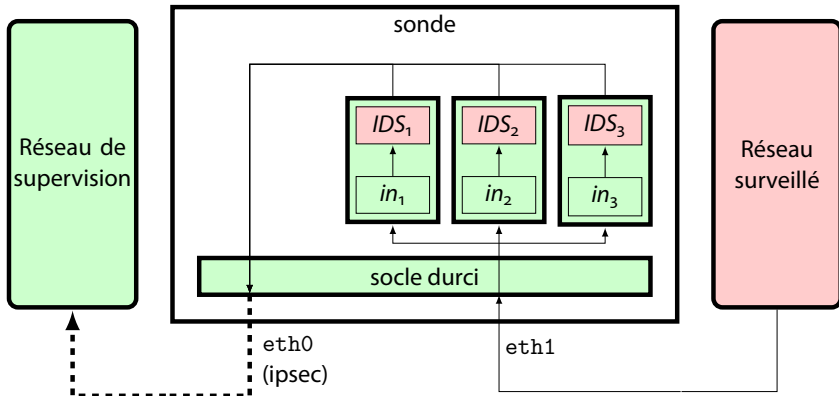


- ▶ Utilisation de la virtualisation
 - ▶ Partage de la racine
 - ▶ Répertoires spécifiques par conteneurs

- ▶ Diodes logicielles
 - ▶ *socket* Unix
 - ▶ tube nommé (*FIFO*)
 - ▶ point de (re-)montage

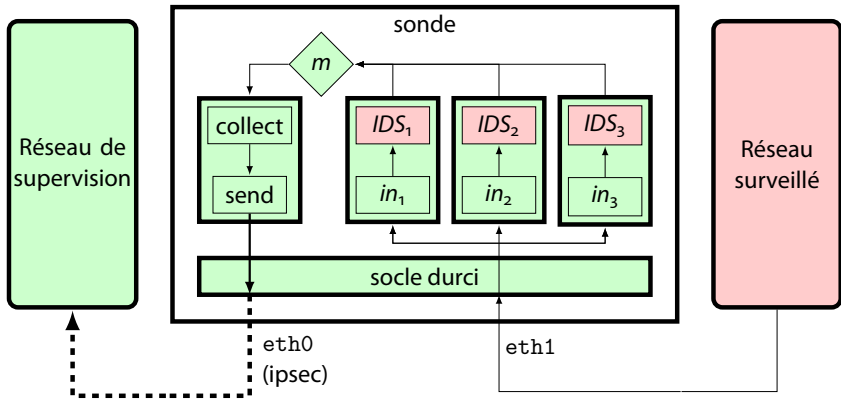


Étape 3 : cloisonnement des IDS





Étape 4 : cloisonnement des journaux





TAP physique

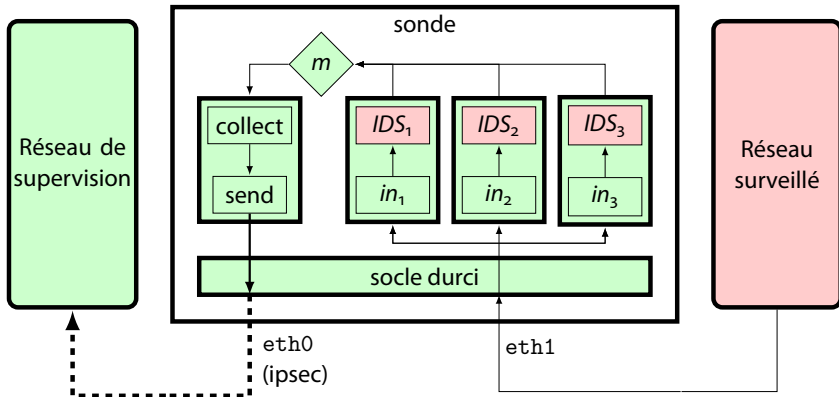
- ▶ Diode
- ▶ Coût additionnel
- ▶ Interface unique

TAP logique

- ▶ Diode, si le socle est intègre
- ▶ Pas de coût (€)
- ▶ Duplication possible

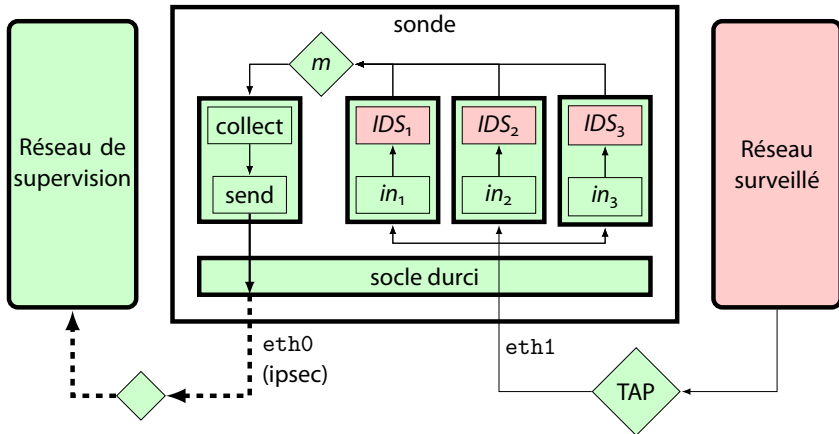


Étape 4 : cloisonnement des journaux





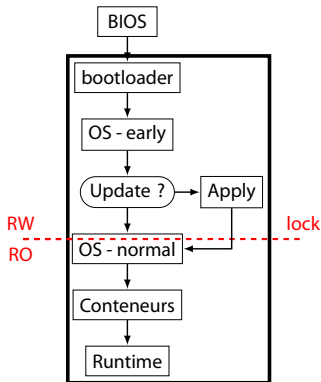
Sonde durcie





Mises à jour

- ▶ Zone de confiance (sans interactions)
- ▶ Verrouillage du système
- ▶ Modifications du socle interdites





Le cas des systèmes industriels

- ▶ Fortes contraintes
 - ▶ Protocoles peu analysés
 - ▶ Très sensibles à la latence
 - ▶ Nombreux points de collecte
 - ▶ Contraintes physiques (espace) et mécaniques
- ▶ Équipements traditionnels inadaptés
- ▶ Faible trafic réseau



Challenge

- ▶ Construire une sonde basée sur l'architecture proposée
- ▶ Utiliser un matériel peu encombrant
- ▶ Réduire le coût
- ▶ Conserver des performances acceptables



Base commune

- ▶ Boîtier Mirabox
 - ▶ SoC ARM (Armada 370), mono-cœur à 1,2 GHz
 - ▶ 1 Go de RAM, 2 interfaces Gbit
- ▶ Debian unstable
 - ▶ Noyau Linux 3.16.3
 - ▶ Suricata 2.0

Sonde durcie

- ▶ Patch grsecurity du noyau, toutes protections activées
- ▶ TAP logique (*bridge* + interface réseau virtuelle)
- ▶ 1 LXC contenant l'IDS
- ▶ 1 LXC pour collecter les alertes



Configuration de l'IDS

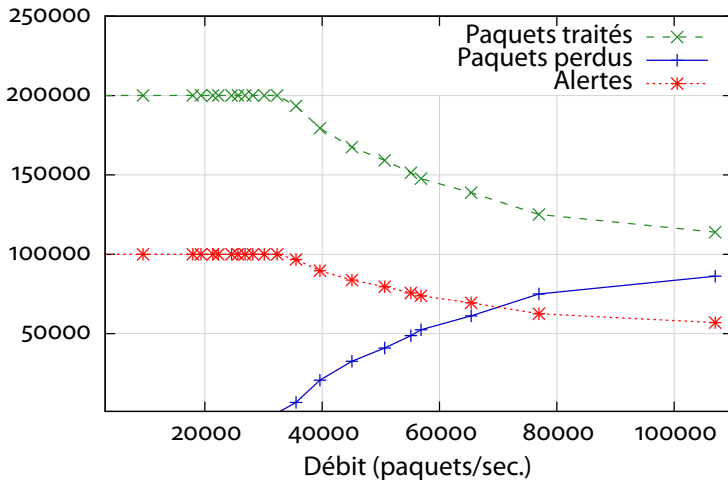
- ▶ Règles Modbus
 - ▶ Génération d'une alerte par transaction Modbus
- ▶ Alertes fastlog
 - ▶ tube nommé (*FIFO*) dans le cas de la sonde durcie

Mesure des performances

- ▶ 200 000 paquets de trafic réel d'un système industriel
 - ▶ 100 000 transactions Modbus
- ▶ Rejeu de la capture à différents débits

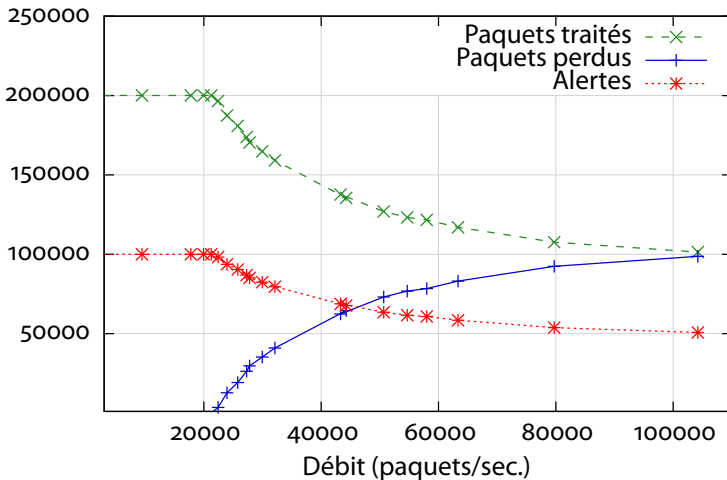


Résultats (sonde témoin)



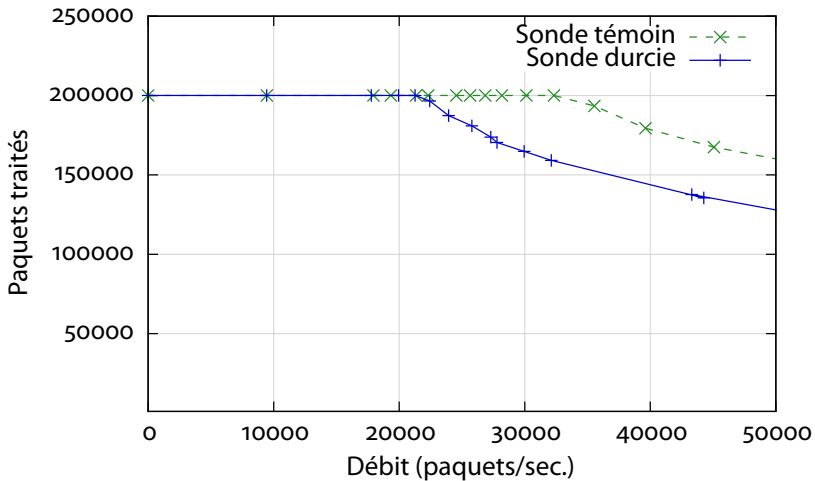


Résultats (sonde durcie)





Résultats





Sonde témoin vs sonde durcie

- ▶ Débit maximum **sans perte**
 - ▶ sonde témoin : 32 500 paquets/sec.
 - ▶ sonde durcie : 21 500 paquets/sec.
- ▶ Impact global du durcissement : environ 33 %

Impact relatif de chaque mesure

- ▶ TAP *logique* : environ 60 %
- ▶ Diode de collecte (*FIFO*) : environ 15 %
- ▶ grsecurity/PaX : environ 13 %
- ▶ Virtualisation LXC : environ 12 %



Conclusion

- ▶ Architecture « de référence »
 - ▶ Défense en profondeur
 - ▶ Protections à l'état de l'art
 - ▶ Réutilisation encouragée
- ▶ Preuve de concept fonctionnelle
- ▶ Performances acceptables
 - ▶ Contexte défavorable
 - ▶ Borne supérieure sur l'impact du durcissement
- ▶ Points d'amélioration
 - ▶ Intégrité du démarrage
 - ▶ Tester avec d'autres IDS
- ▶ *Quid* de la qualité des IDS ?