Mise en place d'un IDS/IPS avec Suricata

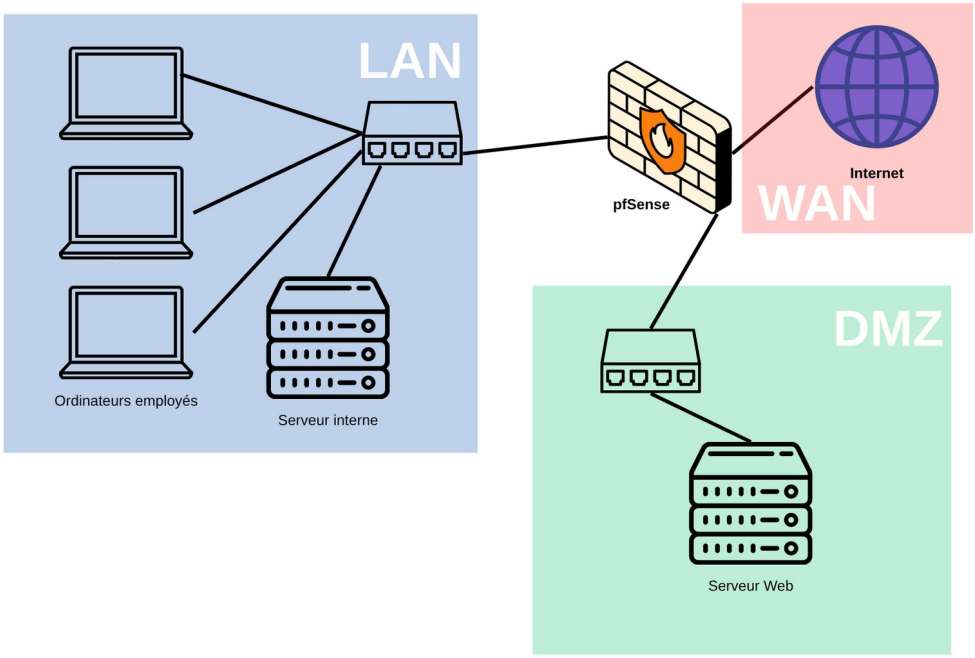
Contexte

Lors du précédent TP, vous avez sécurisé l'infrastructure en mettant en place une DMZ afin d'isoler le serveur Web accessible depuis Internet.

Cette nouvelle architecture améliore la sécurité, mais elle ne permet pas de détecter ou de bloquer les attaques visant les services publiés.

Le RSSI souhaite désormais renforcer la sécurité en déployant un **système de détection et de prévention d'intrusion (IDS/IPS)** sur le pare-feu pfSense.

Vous allez installer Suricata, configurer des règles de détection puis vérifier son fonctionnement en réalisant différentes attaques de test.



L'architecture réseau est identique à celle obtenue à la fin du TP précédent.

Partie 1 - Installation de Suricata

Depuis l'interface Web de pfSense :

- Installer le package Suricata.
- Vérifier que l'installation est terminée.
- Ouvrir le menu Services > Suricata.

1. Quel est le rôle d'un IDS ?
2. Quel est le rôle d'un IPS ?
3. Quelle est la différence entre un IDS et un IPS ?

4. Pourquoi installer Suricata directement sur le pare-feu ?

Partie 2 - Configuration de Suricata

Créer une nouvelle instance Suricata sur l'interface : WAN

Configurer :

- Interface : **WAN**
- Activer **Suricata**
- Activer le mode **IPS**
- Activer le mode **Promiscuous**
- Activer la **journalisation**

Télécharger ensuite les règles proposées par défaut. Mettre à jour les règles. Démarrer Suricata.

Le service est-il démarré ?

Les règles sont-elles correctement téléchargées ?

Combien de règles sont actives ?

Partie 3 - Activation des catégories de règles

Toutes les règles ne sont pas nécessaires. Activer uniquement les catégories suivantes :

- Emerging Scan
- Emerging Malware
- Emerging Web Server
- Emerging Attack Response

Appliquer la configuration. Redémarrer Suricata.

Pourquoi n'active-t-on pas toutes les règles ?

Quels problèmes peuvent apparaître lorsqu'un trop grand nombre de règles est activé ?

Partie 4 - Détection d'une attaque

Depuis le poste Windows, effectuer plusieurs tests :

- Scanner les ports du serveur Web avec Nmap.
- Réaliser plusieurs connexions HTTP.
- Effectuer plusieurs tentatives de connexion SSH vers le serveur.

Observer ensuite :

Services > Suricata > Alerts

Compléter le tableau suivant.

Heure	Adresse source	Adresse destination	Signature détectée	Action

Quelle attaque a été détectée ?

Quelle règle a déclenché l'alerte ?

L'attaque a-t-elle été bloquée ou simplement détectée ?

Partie 5 - Passage en mode IPS

Modifier la configuration afin que Suricata fonctionne en véritable IPS. Redémarrer le service.

Relancer le scan Nmap.

Le scan fonctionne-t-il encore ?

Les paquets sont-ils bloqués ?

Comment le vérifier ?

Partie 6 - Analyse des journaux

Ouvrir : Services > Suricata > Logs

Puis : Status > System Logs

Compléter le tableau.

Élément observé	Résultat
Adresse IP attaquante	
Adresse IP cible	
Signature	
Action réalisée	
Date	

Quelle différence observez-vous entre les journaux du Firewall et ceux de Suricata ?

Pourquoi est-il intéressant de conserver les deux ?

Partie 7 - Test de faux positif

Certaines signatures peuvent bloquer un trafic légitime. Choisir une règle ayant généré une alerte. La désactiver. Redémarrer Suricata. Relancer le même test.

Le trafic est-il désormais autorisé ?

Quels sont les risques de désactiver une règle ?

Partie 8 - Conclusion

Compléter le tableau.

Solution	Avantages	Inconvénients
Firewall uniquement		
Firewall + IDS		
Firewall + IPS		

1. Quel est le rôle de Suricata ?
2. Pourquoi un pare-feu ne suffit-il pas à protéger un réseau ?
3. Dans quels cas est-il préférable d'utiliser le mode IDS ?
4. Dans quels cas est-il préférable d'utiliser le mode IPS ?
5. Pourquoi est-il indispensable de surveiller régulièrement les alertes générées ?