

# Mise en œuvre d'un équipement de gestion unifiée des menaces informatiques

## Situation 5 : Configuration et utilisation d'un NIPS/NIDS

Votre responsable vous demande d'approfondir le fonctionnement et la configuration du service NIDS ASQ présent sur les pare-feu UTM Stormshield afin d'améliorer le niveau protection de chaque agence. Votre mission consiste à maîtriser les fondamentaux liés à cet outil puis à implémenter le cahier des charges qui vous a été fourni.

### Généralités

1. Expliquer en quoi un NIPS/NIDS est complémentaire d'un pare-feu stateful traditionnel.
2. Dans le cadre d'un déploiement de ce type de service, quelle architecture proposeriez-vous ? Justifier.
3. Expliquer les avantages et les inconvénients d'avoir un service NIPS installé sur le pare-feu et non sur un équipement dédié à cet usage.

### Cahier des charges

#### A) Simulation d'une attaque ayant pour objectif de rendre le service web indisponible

Il est demandé à un administrateur réseau situé sur le VLAN d'administration d'utiliser les commandes suivantes à destination du serveur web situé en DMZ afin de tester l'efficacité du NIPS/NIDS présent sur le pare-feu :

```
acox@kali:~$ nmap -sS 172.16.X.11
acox@kali:~$ nmap -sU 172.16.X.11
acox@kali:~$ nmap -sV 172.16.X.11
```

4. À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type d'attaque réalisé ainsi que la finalité de chacune de ces commandes.
5. Le NIPS a-t-il été en mesure de détecter et de bloquer cette opération ? Justifier.

Dans un second temps, il est demandé à l'attaquant de réaliser l'opération suivante de son VLAN « Administration » vers l'adresse IP externe du pare-feu d'une autre agence :

```
acox@kali:~$ hping3 --flood -S -p 80 192.36.253.X0
```

6. À l'aide d'une capture de trames réalisée depuis la machine attaquante, définir le type d'attaque réalisé ainsi que la finalité de la commande.
7. Le NIPS a-t-il été en mesure de détecter et de bloquer cette opération ? Votre service web est-il toujours disponible ? Justifier.

#### B) Analyses protocolaires

8. Vérifier que le chiffrement SSL/TLS accepté est « Haut uniquement ».
9. Bloquer les actions de type transfert de zone (AXFR et IXFR) au niveau du protocole DNS.

#### C) Protections applicatives

10. Depuis votre réseau interne, interdire les accès aux boutons « J'aime » ainsi que la possibilité de publier un commentaire sur un mur Facebook.
11. Interdire toute action concernant la plateforme de jeu Steam, et le VPN FrozenWay provenant de votre réseau d'entreprise et lever une alerte mineure lorsque cela se produit.

## Documents

### Document 1 : Qu'est-ce qu'un IDS/IPS ?

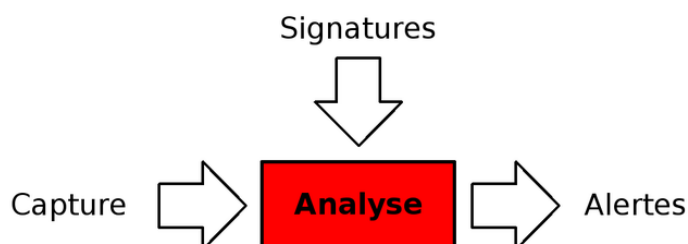
Un système de détection d'intrusion (ou IDS: Intrusion Detection System) est un mécanisme destiné à repérer des activités anormales ou suspectes sur la cible analysée. Il permet ainsi d'avoir une connaissance sur les tentatives réussies comme échouées des intrusions. Un système de prévention des intrusions (IPS) reprend le principe de l'IDS tout en étant capable de bloquer les activités qu'il considère illégitimes.

Il existe deux grandes catégories d'IDS/IPS :

- les HIDS/HIPS (Host Intrusion Detection System) qui sont des outils de sécurité installés sur des hôtes dans le but de détecter des intrusions ou des comportements anormaux sur ces derniers.
- les NIDS/NIPS (Network Intrusion Detection System) qui sont des équipements ou des services à l'écoute sur le réseau destinés à repérer des flux suspects. Les pare-feu UTM Stormshield sont dotés d'un NIDS/NIPS nommé ASQ (Active Security Qualification).

Ce service repose sur 3 phases :

1. La capture.
2. L'analyse à partir d'une base de signatures, des RFC<sup>1</sup>, de règles applicatives.
3. Les alertes et le blocage potentiel.<sup>2</sup>



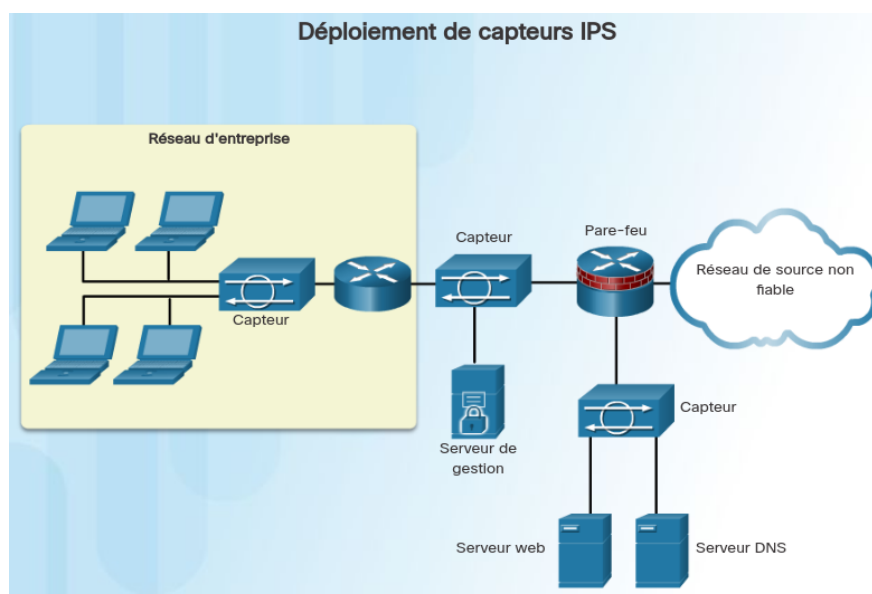
La pertinence du placement d'un système NIDS/NIPS sur un réseau est fondamentale, car il doit capturer un maximum de trafic réseau à des fins d'analyse. Plusieurs architectures existent et peuvent être pertinentes. Chacune a ses avantages et ses inconvénients :

- L'IDS/IPS est placé sur le ou les pare-feu de l'entreprise. Les pare-feu sont souvent des équipements pertinents, car ce sont eux qui autorisent ou bloquent la transmission de flux entre les réseaux.
- L'IDS/IPS peut se placer de manière transparente en mode pont sur l'interconnexion principale entre des réseaux afin de jouer son rôle de façon efficace. Les pare-feu Stormshield peuvent d'ailleurs être utilisés à cette fin.
- L'IDS/IPS est connecté sur un port du commutateur en miroir et récupère ainsi les flux émanant des autres ports.

1 Les requests for comments (RFC) sont une série numérotée de documents officiels décrivant les aspects et spécifications techniques d'Internet et des protocoles associés.

2 Sources : Wikipédia ainsi que le blog sio57.info.

Voici un exemple de schéma décrivant une topologie pour déployer un NIDS/NIPS.



**Source : Formation Cisco CyberOps**

Sur les pare-feu Stormshield, le NIPS est activé par défaut. Cela renforce donc naturellement la sécurité car même en cas d'autorisation globale dans la table de filtrage de l'équipement, ce dernier inspecte et bloque les flux qu'il juge potentiellement dangereux. Bien évidemment, ce service peut générer des faux positifs. Dans le cadre d'un NIPS, les faux positifs sont des flux légitimes que le boîtier a bloqué estimant qu'ils étaient suspects. Suite aux remontées de terrain, les mises à jour (fix) permettent de minimiser les faux positifs et améliore la pertinence des alertes remontées.

Ce dernier est donc extrêmement complémentaire des autres solutions de sécurité mises en œuvre dans l'entreprise. Sur les pare-feu SNS, il est primordial, sauf cas particuliers, de le laisser activé. Dans le cas contraire, il est possible de basculer en mode IDS ou en mode pare-feu simple (c'est-à-dire filtrage couches 3 et 4).