Activité : Mise en oeuvre du filtrage applicatif

Ressources

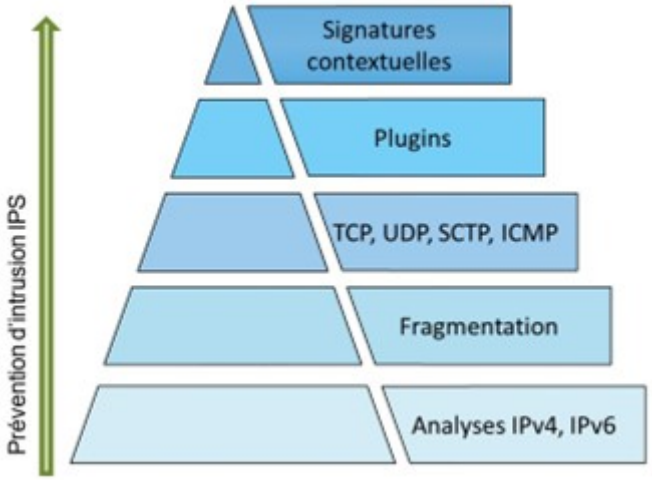
Aidez-vous des fiches suivantes :

- Fiche 8 – Filtrage applicatif

Rappel sur le moteur de prévention d'intrusion ASQ

Les équipements Stormshield Network Security sont équipés nativement d'un module de prévention d'intrusion nommé **ASQ (Active Security Qualification)**. Chaque paquet reçu par le pare-feu SNS sera soumis à un ensemble d'analyses à commencer par la **vérification du protocole IP**.

Le rôle principal de l'ASQ est de s'assurer de la **conformité du paquet** par rapport aux protocoles utilisés de la **couche IP** jusqu'à la **couche applicative** (grâce aux **plugins**) et aux **signatures contextuelles** (ou Patterns).



C'est également l'ASQ qui est en charge de **filtrer les flux** et d'appliquer une **opération de NAT** si nécessaire.

Le système de prévention d'intrusion

Le système de prévention d'intrusion ou **IPS (Intrusion Prevention System)** :

- **détecte et bloque** les tentatives d'attaques des applicatifs
- grâce à des **analyses contextuelles et comportementales**
- complétées par une **identification par signatures**.

Cette association présente deux **bénéfices majeurs** :

- permettre de réaliser un **traitement préventif** sur toutes les couches de communication (du réseau à l'application) fournissant ainsi une réelle **protection 0-day** ;
- l'usage des contextes applicatifs **limite le nombre de signatures à examiner** et réduit ainsi les risques de faux positifs tout en **optimisant les temps de traitements** pour procurer des performances optimales.

Les signatures utilisées par le moteur de prévention d'intrusion SNS sont construites pour :

- **détecter des attaques identifiables**
- mais également leurs **variantes potentielles**. À titre d'exemple, la signature contextuelle sur une injection SQL par une commande SELECT (http:url:decoded:95) permet de contrer plus de 1 540 variantes d'attaques.

En plus de maintenir un espace de stockage contenu, cette technique permet d'optimiser les temps de traitement et propose une protection contre de futures attaques basées sur les mêmes principes.

La mise à jour des bases de signatures du moteur de prévention Stormshield Network Security est assurée indépendamment de la mise à jour du firmware pour garantir une actualisation périodique et automatique afin de rester constamment protégé contre les nouvelles attaques. Cette fonctionnalité de mise à jour automatique se nomme **Active Update** ; elle permet également d'ajouter de nouveaux contextes pour intégrer de nouvelles catégories de signatures contextuelles.

Retour

- Mise en oeuvre de l'UTM Stormshield