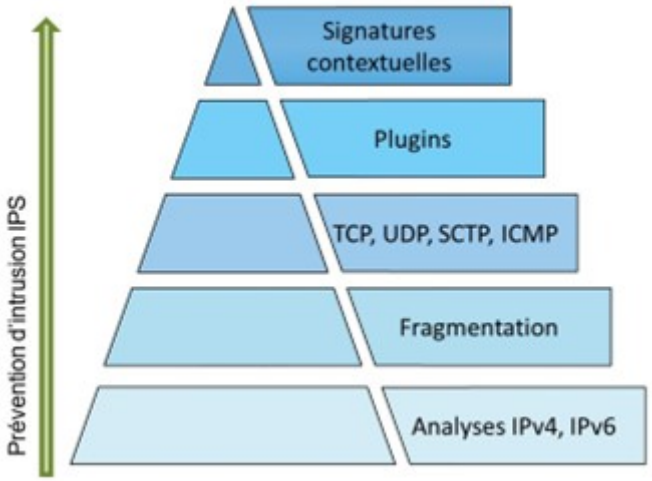
Fiche savoirs : Présentation du moteur de prévention d'intrusion ASQ

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.

Les différents types d'analyses

Un firewall SNS protège le réseau selon trois familles d'analyses :

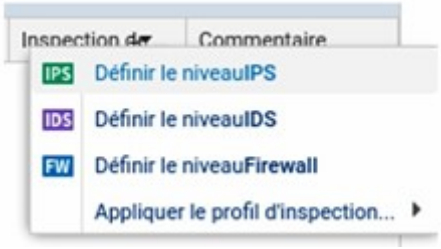
- l'**analyse protocolaire** : elle assure la conformité des flux réseau vis-à-vis des standards de communication (IP, TCP, UDP, ...) ainsi que la conformité aux protocoles applicatifs (HTTP, FTP, ...) grâce aux contrôles appliqués par les contextes applicatifs ;

- l'**analyse statistique** : basée sur des études statistiques du trafic transitant par le firewall, cette analyse détecte des comportements assimilables à du scan de ports, à du SYN flooding, ou encore à des tentatives de DoS (Denial of Service) par maintien de multiples connexions annonçant des petites fenêtres (SockStress) ;
- l'**analyse par signatures contextuelles** : elle vient compléter les contrôles de conformité sur le trafic. Cette analyse permet de se protéger de tentatives d'attaques visant spécifiquement un protocole et une implémentation cliente ou serveur, mais sans toutefois recourir à une inconformité au standard de communication. Elle s'appuie sur des bases de signatures construites par Stormshield, maintenues quotidiennement et mises à disposition sur les serveurs Active Update.

Les niveaux d'inspection de sécurité

Chaque paquet reçu par le pare-feu SNS est soumis à la politique de filtrage. Par défaut, l'analyse **IPS** (Intrusion Prevention System : système de prévention d'intrusion) est appliquée, ce qui signifie que le pare-feu SNS est capable de détecter une anomalie et de bloquer le paquet correspondant.

D'autres niveaux d'inspections peuvent être utilisés, à des fins de tests ou par nécessité ; par exemple si on contacte un serveur ne respectant pas la RFC des protocoles qu'il gère. Ces niveaux sont à sélectionner dans la colonne Inspection de sécurité de la règle de filtrage concernée.



- **IPS : Détecter et bloquer** (choix par défaut). L'ASQ va soumettre le paquet à l'ensemble des couches qu'il est capable d'analyser et le bloquer en cas d'anomalie.
- **IDS : Détecter**. L'ASQ effectue une analyse similaire à l'IPS sauf que le paquet est toujours autorisé. C'est un profil permettant de faire un audit rapide pour une règle de filtrage donnée.
- **Firewall** : Ne pas inspecter. L'ASQ ne va effectuer que très peu d'analyses sur le paquet reçu. Il se comporte comme un simple routeur filtrant.

L'ASQ est composé de 10 configurations (également nommées **profils IPS**). Chacune de ces configurations peut être éditée en fonction des besoins de l'administrateur.
La configuration par défaut, comme indiqué dans le menu **Configuration ⇒ Protection applicative ⇒ Profils d'inspection**, applique les profils **IPS*00 et IPS*01** respectivement aux **connexions entrantes** (paquet dont l'adresse IP source ne fait pas partie d'un réseau protégé) et aux **connexions sortantes** (paquet dont l'adresse IP source fait partie d'un réseau protégé).
Si des flux sains déclenchent des alarmes, il sera sûrement nécessaire de modifier les paramètres de l'ASQ pour ne pas bloquer la production. Dans ce cas, les modifications doivent être faites au plus spécifique. De préférence dans un profil dédié qui sera appliqué sur les règles identifiant précisément le trafic concerné.
Il est alors possible, dans la table de filtrage, de forcer l'utilisation d'un profil ASQ spécifique depuis la colonne **Inspection de sécurité**. Les profils sont ensuite configurables et administrables depuis les menus **Protocoles et Applications et protections** sous **Configuration ⇒ Protection applicative**.
Enfin, par défaut, l'IPS est actif sur toutes les règles de filtrage en mode de **détection automatique du protocole**. Afin de mieux inspecter les flux, il est recommandé de qualifier manuellement le type de protocole si le port utilisé n'est pas standard. L'IPS risquerait de ne pas détecter correctement l'application.

Retour

- Mise en oeuvre de l'UTM Stormshield