



FAST360

1. **Qu'est ce que FAST in line IDPS**
2. **Technologie**
3. **Arguments clés**



1. Qu'est ce que FAST in line IDPS ?

FAST in line IDPS est une extension de la technologie **FAST** capable de détecter et neutraliser des attaques applicatives avec ou sans violation protocolaire en tenant compte du contexte des connexions.

FAST in line IDPS (Intrusion Detection and Prevention System) est la combinaison de **FAST** (IPS capable d'identifier et de bloquer les violations protocolaires) et d'un IDS (Intrusion Detection System à base de signatures) en coupure. Les deux technologies fonctionnent ensemble pour déterminer le contexte d'une connexion, détecter une attaque ou un comportement dangereux et agir en temps réel.

2. La Technologie FAST in line IDPS

Limites des IDS Classiques

Les IDS à base de signatures présentent plusieurs inconvénients qui limitent leur déploiement dans un réseau :

1. Performances limitées

Lors d'une analyse IDS standard, la comparaison systématique de l'ensemble des signatures stockées avec le contenu de la connexion contrôlée exige des ressources considérables ce qui crée inévitablement un goulot d'étranglement.

2. Fausses alertes

Une fausse alerte (ou faux positif) se produit lorsqu'une attaque est détectée à tort dans une session ou un protocole. En effet, une même signature (souvent une chaîne de caractère) n'a pas la même signification suivant le contexte de la session ou le protocole. Une chaîne de caractère, si elle ne tient pas compte de ce contexte peut se retrouver dans une session sans pour autant signifier qu'il s'agit bien d'une attaque.

Avantages de la technologie FAST in line IDPS

Le module FAST in line IDPS détecte et empêche les intrusions. Une base de données de signatures **contextuelle** identifie et bloque les attaques non détectées par le contrôle de conformité protocolaire FAST.

1. Optimisation de la performance

- La base de signatures contient uniquement les signatures d'attaques qui ne peuvent pas être bloquées de manière fiable par le module de décodage et contrôle applicatif FAST. La taille de la base de signatures est réduite.
- La base de signature est « **contextualisée** » : les signatures sont indexées en fonction de l'état protocolaire dans lequel elles constituent une attaque. Pour un protocole donné et dans un état applicatif donné, seules les signatures qui sont synonymes d'attaque sont recherchées.
- L'utilisation de l'algorithme Boyer-Moore accélère la recherche dans la totalité de la base et l'implémentation en mode noyau du module IDPS garantit un traitement rapide des paquets.

2. Élimination des faux positifs

- En utilisant une base de signatures contextuelle, l'IDPS compare uniquement les signatures qui correspondent à l'état protocolaire d'une connexion et réduit considérablement les risques de faux positifs.
- Chaque analyse est pondérée à l'aide de la correspondance WPM (*Weighted Pattern Matching*, exclusivité développée par ARKOON) qui identifie une attaque en recoupant la détection de plusieurs signatures pondérées.
- Les signatures sont regroupées par profil en fonction de la configuration de l'environnement à protéger (type de serveur, systèmes, OS, etc...). Ce mécanisme (exclusivité développée par ARKOON) permet de balayer uniquement les signatures correspondant à l'environnement protégé.

3. Les arguments clés

1. Une technologie innovante et unique

Parce qu'elle est une extension de **FAST** ; parce qu'elle est intégrée ; parce qu'elle gère le contexte de la connexion ; **FAST in line IDPS** est la seule technologie de filtrage qui analyse, détecte et neutralise tous types d'attaques applicatives. Elle ne peut formellement être assimilée à aucune autre technologie du marché.

2. Une pertinence d'analyse optimisée

FAST in line IDPS est capable de définir au plus juste le contexte d'analyse. Grâce à l'utilisation de jeux de signatures contextuels, à la définition de profils et à la technologie WPM, **FAST in line IDPS** diminue très fortement le risque de « faux positifs »

3. Une performance de filtrage préservée

L'intégration de la technologie dans le noyau d'ARKOON, l'optimisation de la base de signature permettent à **FAST in line IDPS** de soutenir les excellentes performances de filtrage des équipements ARKOON (l'impact de l'IDPS sur la performance réseau est inférieur à 10%).

4. Une base de signatures optimisée

La technologie FAST in line IDPS, de par sa capacité à détecter des signatures comportementales sur les protocoles applicatifs http et https, permet de bloquer les applications non productives ou potentiellement intrusives comme les messageries instantanées, les applications P2P ou encore les flux Skype.

