FAST In line IDPS
Intrusion Detection and Prevention System

ARKOON Network Security est le **premier constructeur** de solutions de sécurité périmètrique à combiner sur une même appliance les technologies de firewalling et de prévention d'intrusion, avec détection d'intrusion en coupure.

Cette combinaison s'inscrit dans le cadre de l'approche de la sécurité **périmétrique multi-niveaux** adoptée par ARKOON, et vient à la fois compléter le niveau « contenu » en détectant et bloquant les codes malicieux, et renforcer le niveau « protocole applicatif ».

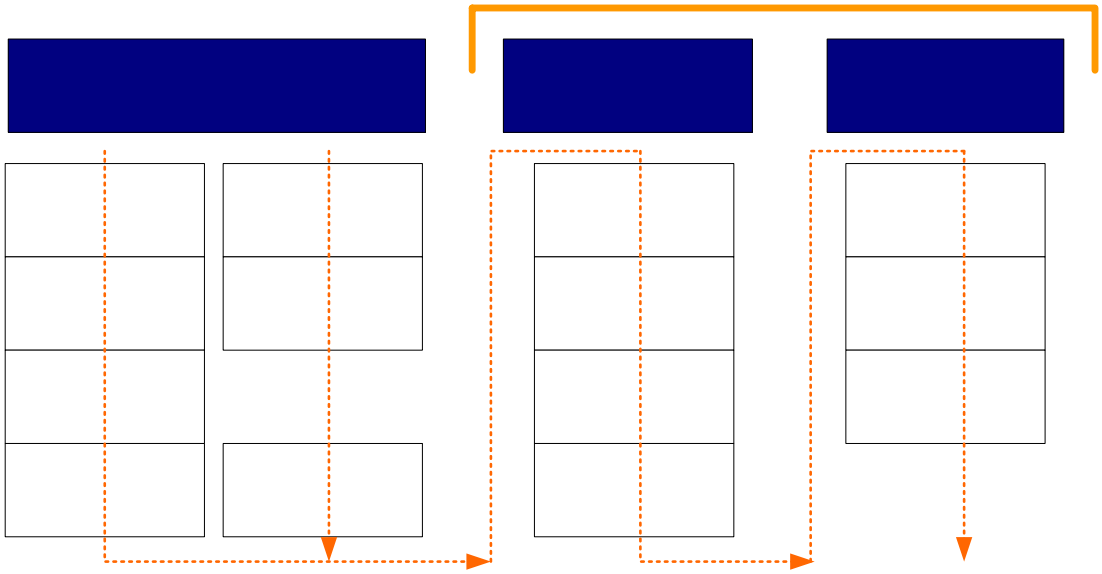
Le module détection d'intrusion en coupure (« Real time IDS ») qui, associé au module IPS pré-existant constitue le « FAST In Line IDPS », est conforme à SSA (**Scalable Security Architecture**) l'architecture d'intégration développée par ARKOON :

- Implémentation « mode noyau »
- Respect des spécifications d'intégration dans SSA
- Intégration dans l'environnement d'administration ARKOON

La conformité à l'architecture SSA permet de garantir le niveau de performance des solutions (mode noyau), leur « scalabilité » (capacité à monter en charge) et leur facilité d'administration (un seul environnement).

Technologie

L'IDPS est la combinaison du décodage applicatif temps réel avec la détection d'intrusion à base de signature utilisée en coupure. L'objet du dispositif de sécurité périmètrique est avant tout de bloquer les attaques. Compte tenu des origines multi-niveaux de ces attaques, **plusieurs méthodes** permettant de les bloquer sont utilisées en cascade.



9 Avril 2004

Performances:

La performance est, avec la génération de fausses alertes, le premier inconvénient des IDS à base de signatures du marché ; ceux-ci ne peuvent d'ailleurs pas être utilisés en coupure pour ces deux raisons.

Dans le « FAST In line IDPS », la comparaison des caractéristiques de la session avec la base de signatures a lieu après le décodage applicatif. La base de signatures ne contient donc que les signatures des attaques qui ne sont pas (ou difficilement) bloquées par le mode stateful inspection, puis par le décodage applicatif temps réel. En particulier, les attaques violant les protocoles (http, dns, smtp..) ou qui ne correspondent pas à l'usage attendu sont bloquées au niveau du décodage applicatif et n'ont pas à être référencées dans la base. Ce dispositif permet de réduire la taille de la base de signatures permettant ainsi une utilisation « à la volée » et en coupure.

De plus, dans une recherche de performances, le module de comparaison à la base de signature « Real Time IDS » a été développé, comme le moteur FAST, en mode noyau (c'est à dire au cœur du système d'exploitation), ce qui garanti le faible temps de traitement des paquets.

L'activation de la fonction « Real Time IDS » avec une base de plus de 650 signatures engendre une dégradation des performances du réseau de moins de 20% en comparaison à une situation où seul le décodage applicatif (IPS) est activé. Compte tenu des performances du décodage applicatif (17.000 requêtes http/s), cette dégradation reste largement compatible avec une utilisation en coupure.

Elimination des faux-positifs :

Un inconvénient majeur des IDS est la génération de fausses alertes « faux-positif » liées à la reconnaissance de la signature de l'attaque dans une session ou un protocole pour lequel cette signature n'est pas une attaque. Si, dans le cas d'un IDS, la génération de faux-positif est un véritable inconvénient elle est inacceptable lorsqu'il s'agit d'un dispositif en coupure.

Pour éliminer ce risque ARKOON a mis en place trois mécanismes complémentaires :

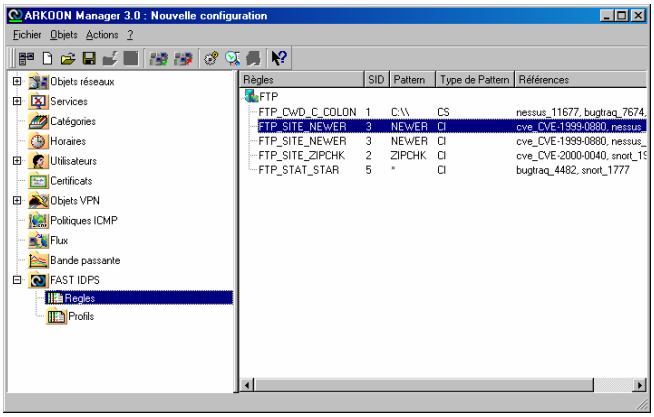
- La base de signature est « **contextualisée** » (on peut aussi parler de signatures « à état » ou de « stateful signature »). A chaque signature est affectée le contexte dans lequel cette signature est effectivement une attaque, à contrario toute détection de cette signature dans un autre contexte ne sera pas considérée comme une attaque.

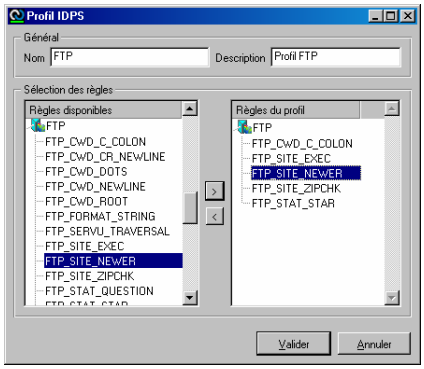
- Chaque signature est pondérée, il s'agit là d'une technique originale développée par ARKOON est appelée **WPM** pour « Weighted Pattern Matching ». Ce mécanisme permet d'identifier une attaque et de la bloquer en corrélant des événements caractérisés par des signatures pondérées.

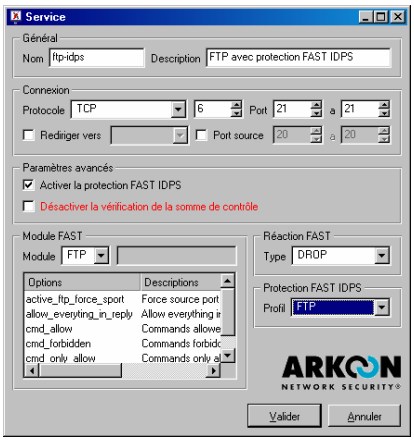
- Les signatures sont regroupées par profil en fonction des configurations de l'environnement à protéger. Il existe par exemple, un profil http Apache, un profil IIS, un profil PHP, un profil Solaris, un profil Windows NT4,…. Ce mécanisme de gestion de profil original développé par ARKOON permet de ne rechercher dans le flux que les signatures d'attaque concernant l'environnement protégé. A la configuration, l'administrateur définit le ou les profils à utiliser, qui seront appelés par les règles de flux.

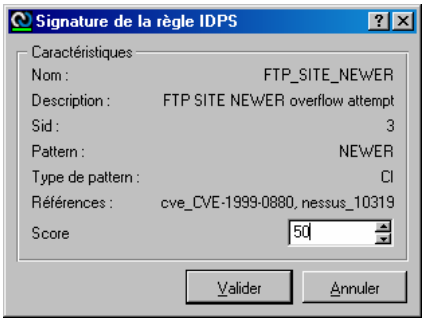
Administration

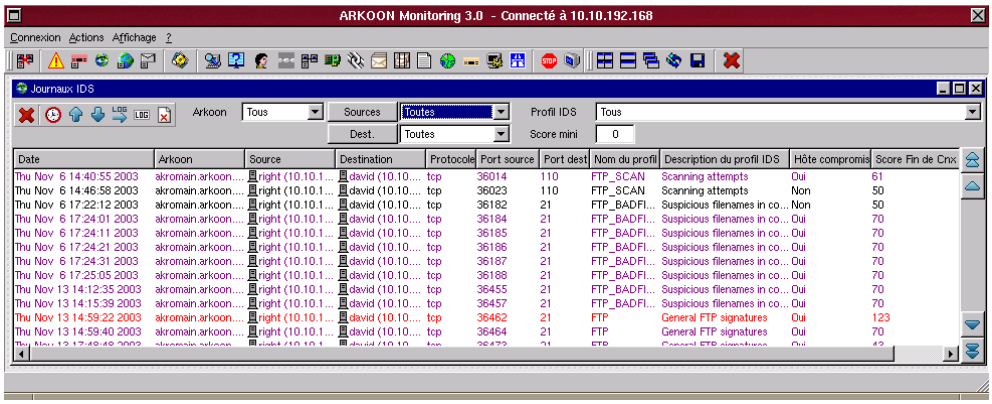
Les outils d'administration de « FAST In Line IDPS » sont intégrés à l'environnement d'administration d'ARKOON.











La base de signature utilise le même canal de mise à jour authentifié par certificat et sécurisé que les mises à jour des bases anti-virus et des logiciels des équipements de la gamme ARKOON.
L'équipe de veille d'ARKOON, **AK Security Watcher** collecte en permanence les informations relatives aux différentes attaques, identifie celles qui doivent être insérées dans la base et, le cas échéant, les ajoutes à la base de signatures après avoir déterminé le contexte applicatif associé.

Bénéfices clients

Le FAST In line IDPS renforce le niveau de protection offert par les appliances de sécurité multi-niveaux d'ARKOON en permettant de bloquer des attaques qui ne violeraient pas les protocoles inter application ou l'usage attendu de ceux-ci. C'est le cas en particulier des scripts (CGI, Java, PHP…) malicieux qui ne sont pas non plus détectables par un anti-virus. Il fournit également une deuxième méthode pour les attaques qui peuvent être bloquées au niveau décodage applicatif à condition que les règles de paramétrage appropriées aient bien été mise en place.

Exemples :

Attaques	Protection	Valeur ajoutée de FAST In line IDPS
Attaques de type : - Directory traversal - Cross site scripting	Ces attaques sont bloquées par le décodage applicatif (FAST) si l'administrateur l'a explicitement configuré pour bloquer les requêtes correspondantes.	Détectées et bloquées au niveau de la comparaison avec la base de signatures.
Attaque par des scripts serveurs (CGI, PHP, ASP, Java…)	Ne sont pas bloquées par le décodage applicatif	Détectées et bloquées au niveau de la comparaison avec la base de signatures.
NIMDA (Ver)	Bloqué par le décodage applicatif : Une taille maximum d'URL est autorisée (correspond à l'usage attendu) Des mots sont interdits dans l'URL Bloqué par l'anti-virus lorsque transféré par mail ou http	Détectées et bloquées au niveau de la comparaison avec la base de signatures
BLASTER (Ver)	Bloqué par la fonction de filtrage IP	Détecté et bloqué au niveau de la comparaison avec la base de signatures

L'environnement d'administration proposé par ARKOON permet de gérer de manière simple et cohérente l'ensemble des mécanismes de protection permettant la mise en place d'une véritable sécurité multi-niveaux.

ARKOON NETWORK SECURITY®

Siège social : 13A avenue Victor Hugo 69160 Lyon Tassin

Agence Paris : 15 bis rue Ernest Renan 92136 Issy les Moulineaux

Tel : 33 04 72 53 01 01 Fax : 33 04 72 12 60

Email : info@arkoon.net http://www.arkoon.net