



La sécurité périmétrique multi-niveaux

Un white paper de
Daniel Fages CTO
ARKOON Network Security
dfages@arkoon.net

SOMMAIRE

Ce document a pour objectif de décrire les différents types de risques liés à un réseau de communication, de mettre en évidence les limites des moyens de protection traditionnellement mis en œuvre et enfin d'introduire le concept de sécurité multi-niveaux en le comparant avec les autres approches.

1- Introduction – les limites de la protection réseau -	3
2- Classification des attaques	5
Attaques « réseau »	5
Attaques au niveau d'un « protocole applicatif »	5
Attaques au niveau des données transportées par un protocole applicatif (Contenu) ...	5
3- Les différentes techniques de protection.....	6
Filtrage IP à état	6
Détection d'intrusion par Décodage applicatif	6
Détection d'intrusion à base de signatures d'attaques.....	7
Anti-virus.....	9
Synthèse	9
4 L'approche ARKOON	10
Technologie FAST.....	10
Architecture SSA.....	11
FAST In line IDPS	13
Aspect performances	13
Complémentarité avec les autres technologies	13
5 Conclusion	17

Copyright 2003 ARKOON Network Security. Tous droits réservés. Le contenu de cette publication est protégé par copyright. Aucune reproduction même partielle de ce document ne sera autorisée sans autorisation expresse d'ARKOON Network Security.

Marques déposées : ARKOON Network Security, le logo ARKOON, FAST et SSA.

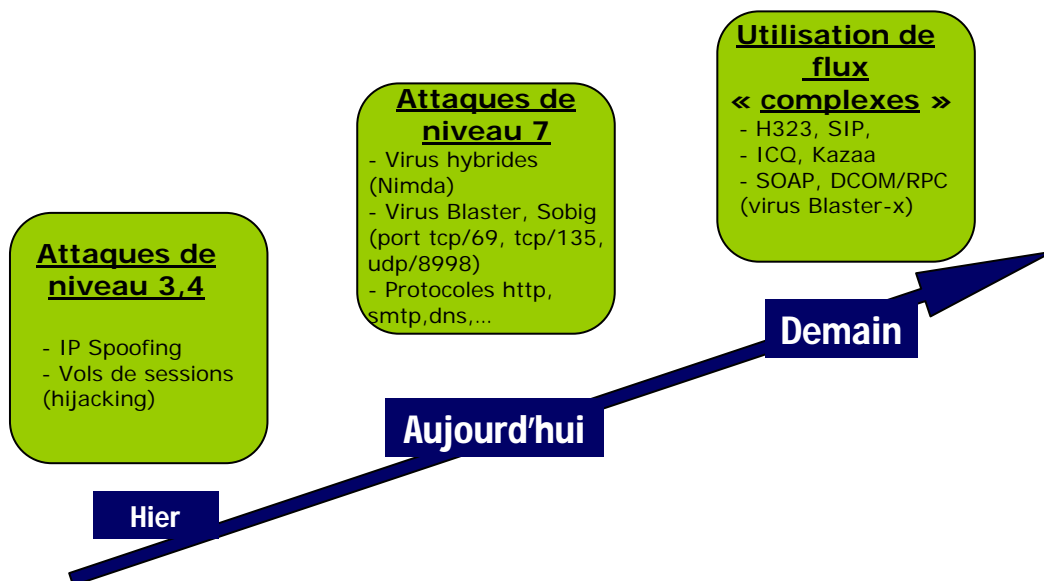
Aucune garantie n'est donnée par l'auteur de cette publication. Celle-ci peut, le cas échéant, contenir des inexactitudes techniques ou des erreurs de typographie.

1- Introduction – les limites de la protection réseau -

Avec la multiplication des échanges interentreprises, l'importance grandissante des actifs immatériels l'augmentation des débits, le développement de la mobilité et le passage à des connexions Internet permanentes, on assiste à une évolution sans précédent du nombre et de la nature des risques auxquels sont exposées les entreprises via leurs réseaux.

Aux menaces « traditionnelles » qui se situent au niveau du réseau de transport lui-même (vol de session, usurpation d'adresse, déni de service...) viennent s'ajouter d'autres menaces :

- celles qui sont liées aux vulnérabilités des très nombreux logiciels de communication (Navigateur Internet, Serveur Web, Serveur DNS, etc...) qui utilisent des protocoles dits applicatifs au dessus du réseau de transport pour communiquer. Par exemple :
 - le protocole HTTP permettant de faire communiquer le navigateur Internet avec le serveur Web
 - le protocole SMTP permettant aux serveurs de messagerie de s'échanger les mails
- celles liées aux contenus qu'il s'agisse des nouveaux virus, vers informatique ou chevaux de Troie.



Face à cette menace que l'on peut qualifier de « multi-niveaux » en se référant aux différentes couches d'un réseau de communication (en simplifiant : réseau, application, contenu) il est indispensable de mettre en place une protection « multi-niveaux » :

- Protection contre les attaques de niveau réseau (pour simplifier, ce que nous appellerons « niveau réseau » dans ce document regroupe les équivalents des couches OSI/3 – réseau – et OSI/4 – transport -)
- Protection contre les attaques qui touchent les protocoles applicatifs (« attaques applicatives »)
- Protection contre les attaques de contenu

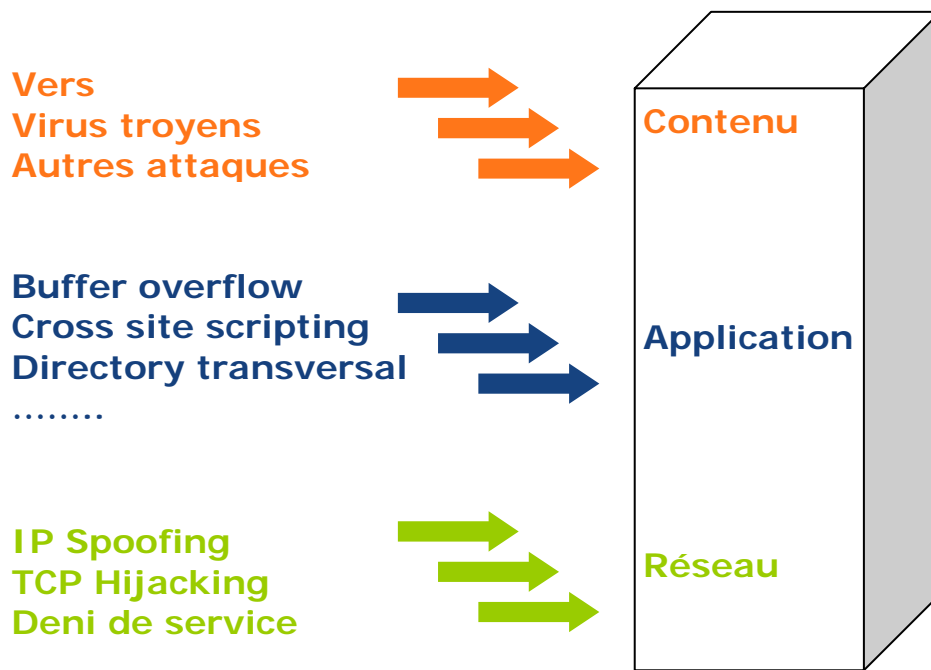
Aujourd'hui plus de 85% des vulnérabilités recensées par les CERTS résident dans les outils de communication, par opposition aux failles découvertes dans les systèmes d'exploitation, notamment les piles TCP/IP de ces systèmes. Les entreprises, quant à elles, ont déployé des solutions qui répondent de manière partielle à ces menaces :

- Firewalls niveau 3/4 (mode stateful) qui agissent au niveau réseau mais n'analysent pas les protocoles de communication inter application
- Sondes IDS (Intrusion Detection System) qui permettent, si l'attaque a été enregistrée dans leur base de données, de la détecter mais pas de la bloquer en temps réel.

Ces solutions, nécessaires, s'avèrent largement insuffisantes car elles ne protègent pas le système d'information contre les attaques qui exploitent les vulnérabilités des logiciels de communication. L'apparition de vers du type Nimda ou Blaster ont mis en évidence ce problème de manière aigüe. En effet Nimda en 2001 puis Blaster lors de l'été 2003 se sont répandus à très grande vitesse alors qu'une grande majorité des entreprises étaient dotées de « firewall ». Ces « firewalls », majoritairement de type « stateful » ne peuvent pas identifier une attaque applicative : ils permettent simplement d'autoriser ou non l'accès à certains « ports » de communication (c'est-à-dire à certaines applications); par exemple :

- Autoriser l'accès au port 80 (http) d'un serveur Web mais pas de détecter une attaque à l'intérieur d'une requête destinée à ce serveur.
- Autoriser l'accès au port 53 (dns) d'un serveur DNS mais pas d'interdire certains types de requête, caractéristiques d'une attaque.

Pour bloquer ce type d'attaque, il est donc indispensable de ne pas se limiter à la protection « réseau » et de disposer de solutions permettant de sécuriser aussi les protocoles applicatifs et le contenu.



2- Classification des attaques

Attaques « réseau »

Ces attaques exploitent des vulnérabilités au niveau des piles IP des systèmes d'exploitation (particulièrement sur les protocoles IP/TCP/UDP) :

- Envoi de paquets avec une entête spécialement formée qui va généralement permettre de lancer une attaque de déni de service.
- IP Spoofing (Usurpation d'adresse) : technique qui consiste à envoyer des paquets IP « construits » en utilisant comme adresse IP source de ces paquets l'adresse IP d'un autre système afin de contourner les mécanismes de filtrage en place.
- TCP Hijacking (Vol de session TCP) : technique qui consiste à insérer des paquets TCP dans une connexion TCP déjà établie afin de contourner les mécanismes de filtrage en place.

Attaques au niveau d'un « protocole applicatif »

Les vulnérabilités au niveau de l'implémentation d'un protocole applicatif (ex : HTTP, FTP, SMTP, etc...) dans un logiciel de communication (serveur web, DNS, serveur de messagerie, base de données, etc...) permettent différents types d'attaques sur le serveur qui héberge l'application concernée : exécution de code, déni de service, accès à des informations sensibles, etc.... Sont particulièrement visés les services http (TCP port 80) et https (TCP port 443) qui sont généralement ouverts sur les réseaux et pour lesquels les équipements de contrôle d'accès ne peuvent pas identifier le trafic malicieux.

Les attaquants cherchent à atteindre un des objectifs suivants :

- Déni de service,
- Prise de contrôle d'un système avec des droits administrateur,
- Accès à des données de l'entreprise,
- Installation d'un cheval de Troie pour accéder aux applications.

On peut distinguer deux types d'attaques qui exploitent les vulnérabilités au niveau d'un protocole applicatif :

- Attaques qui ne respectent pas le protocole applicatif, qui enfreignent les règles liées à ce protocole ou qui se caractérisent par un usage « anormal » de celui-ci,
- Attaques qui respectent le protocole applicatif et qui ne peuvent donc pas être détectées par l'analyse protocolaire.

Attaques au niveau des données transportées par un protocole applicatif (Contenu)

Les données transportées par le protocole applicatif (on parle aussi de Contenu) peuvent constituer une menace pour l'intégrité du système qui les reçoit.

Parmi les attaques qui utilisent le contenu, on peut dénombrer notamment :

- Les codes malicieux (Virus, Ver, Applet Java, ...),
- L'exécution de scripts (type CGI) sur un serveur Web,
- Le spam.

3- Les différentes techniques de protection

Chacune des techniques de protection présentées ci-dessous, n'agit que sur un des niveaux (réseau, applicatif, contenu) :

Filtrage IP à état

Cette technique « de base » est généralement implémentée sous le nom générique de « **Firewall** ». En effet, elle consiste à autoriser ou non les demandes de connexions selon une liste de règles (issues de la politique de sécurité) définies par l'administrateur ; ces règles se basent au minimum sur les adresses IP et les ports (TCP/UDP) de la demande de connexion. Une fois la connexion autorisée, le moteur basé sur cette technique autorise également les paquets appartenant à cette connexion. Il utilise une « table de connexions actives » (table des connexions « connues » par le moteur de filtrage) pour s'assurer qu'un paquet qui désire entrer sur le réseau interne de l'entreprise protégée fait bien partie d'une connexion sortante précédemment établie ou est une demande de connexion, expressément autorisée par l'administrateur.

Les moteurs mettant en œuvre cette technique réalisent généralement un ensemble de contrôles sur les entêtes des paquets pour s'assurer que les protocoles de niveau Réseau (IP) et Transport (TCP, UDP, ICMP, ...) sont bien respectés par les paquets inspectés.

- Avantages : technique efficace contre les attaques réseau, technique performante car elle permet de traiter des flux importants
- Limitations : protège uniquement contre les attaques de niveau « réseau ».

Prévention d'intrusion par Décodage applicatif

Cette technique consiste à analyser les paquets circulant sur un réseau dans le but de « décoder » le protocole applicatif utilisé :

- Contrôle de conformité de la communication aux standards (on parle ici de RFC) du protocole applicatif.
- Contrôle de l'utilisation faite du protocole

Elle permet de dissocier dans une même communication les différents éléments du protocole (commande, paramètres, données, etc...), ce qui permet, comme nous le verrons ensuite, de la combiner avec une technologie de détection d'intrusion à base de signatures d'attaques applicatives contextuelles.

Elle permet de bloquer les attaques visant à exploiter une vulnérabilité applicative qui utilise le protocole applicatif en dérogeant au RFC, à un usage « normal » de celui-ci, ou à des règles fixées par l'administrateur de sécurité : par exemple, limitation des commandes utilisées ou longueur des paramètres admis.

Un phénomène relativement récent complexifie cette approche, c'est l'augmentation sensible des protocoles dits « encapsulés », c'est à dire les protocoles applicatifs qui utilisent un autre protocole pour leur transport. Par exemple, les protocoles de Peer-to-peer (ex : Kazaa, Gnutella, ...) sont transportés à l'intérieur du protocole HTTP. Les systèmes de décodage applicatif doivent donc être suffisamment sophistiqués et performants pour détecter et décoder les protocoles encapsulés.

- **Avantages**: technique proactive, elle permet de bloquer des attaques non connues simplement car elles dérogent aux RFC ou aux règles. Elle ne nécessite pas le maintien d'une base de signatures d'attaques.
- **Limitations**: technique efficace seulement sur les protocoles analysés (difficulté d'analyser tous les protocoles). Elle ne permet pas de détecter attaques qui respectent le protocole.

Différentes implémentations de la technique détection d'intrusion par décodage applicatif :

Il existe deux types d'implémentations possibles :

La technologie « proxy » (ou relais) qui consiste à créer deux communications IP distinctes, l'une entre le client et le proxy, l'autre entre le proxy et le serveur, le proxy analysant le protocole applicatif utilisé. Cette technologie a l'avantage d'apporter une grande souplesse à l'analyse applicative ; elle pose par contre de gros problèmes de performance dès que les flux deviennent importants.

Il existe deux catégories de produits qui implémentent la technologie Proxy, l'un et l'autre peuvent être qualifiés de « Firewall Applicatif » mais leur utilisation est différente.

- **Firewall à base de Proxies** : Analyse des protocoles applicatifs pour lesquels l'éditeur a développé le proxy (un proxy par protocole). Permet de réaliser des traitements complexes dans le proxy, très consommateur de ressource, pose des problèmes de performance dès que les flux deviennent importants.
- **« Reverse proxy »** : les reverse-proxies sont dédiés aux protocoles HTTP et HTTPS et protègent les sites web contre les attaques en provenance de l'Internet. La plus part d'entre eux proposent d'assurer les fonctions d'accélération SSL (via un processeur spécialisé) déchargeant ainsi le serveur Web de cette tâche et permettant de réaliser l'analyse applicative sur le flux HTTPS.

L'analyse applicative « temps réel » qui s'appuie sur une seule communication IP, le flux étant recomposé et analysé « à la volée ». Son principal avantage étant sa capacité à traiter en temps réel des flux importants.

- **Produits qui implémentent l'analyse applicative « temps réel »**
Dans ces produits, également qualifiés de Firewalls Applicatifs, l'analyse applicative n'est plus faite dans une application qui s'exécute au-dessus du système d'exploitation (comme dans le cas des proxies), mais directement dans le noyau du système d'exploitation, au plus près du matériel. Cette différence est importante car elle permet d'assurer des performances de premier ordre même dans le cas de flux haut débit.

La produits implémentant les fonctions de décodage applicatifs temps réel sont qualifiés d'IPS : Intrusion Prevention System

Détection d'intrusion à base de signatures d'attaques

La technique de détection d'intrusion avec base de signatures d'attaques consiste à rechercher des « signatures » (une suite de caractères caractérisant une attaque) dans toutes les communications qui passent sur le réseau. Elle permet de détecter des

attaques applicatives même si elles respectent les standards des protocoles applicatifs, en cela elle est complémentaire au décodage applicatif. Elle suppose de maintenir et de mettre à jour une base de signatures d'attaques, le délai de mise à jour de cette base sur les équipements qui utilisent cette technologie étant primordial pour l'intérêt de cette technique.

Cette technique peut utiliser une base de signatures contextuelles (on parle aussi de « stateful signatures ») ; par signature contextuelle, on entend une signature qui prend en charge le contexte applicatif : cela permettra, par exemple, de ne rechercher les URLs connues comme étant malicieuses que dans les URLs des requêtes HTTP, alors que, avec une base de signatures non contextuelles, on rechercherait cette URL dans toute la communication. L'intérêt est à la fois de diminuer de manière importante le risque de fausse alerte (ou « false positive »), inhérent à cette technique, et d'améliorer les performances en facilitant le travail de comparaison.

- Avantages : permet théoriquement de détecter tout type d'attaque si celle-ci est répertoriée dans la base
- Limitations : technologie réactive, nécessite la mise à jour d'une base de signatures d'attaques. Risque de fausse alerte dans le cas d'une base importante.

Il existe deux types d'implémentation la technique de détection d'intrusion à base de signature d'attaque.

- **Sonde IDS (Intrusion Detection System)** : C'est un équipement « passif » qui écoute les paquets circulant sur le réseau. Généralement, ces produits utilisent une technique de détection d'intrusion avec base de signatures d'attaques, qui consiste à rechercher des « signatures » (une suite de caractères caractérisant une attaque) dans toutes les communications transitant sur le réseau surveillé.

L'intérêt de ces solutions est de détecter les attaques applicatives puisque la recherche de signatures d'attaque se fait sur la totalité du paquet (y compris le corps du paquet).

Il s'agit par contre d'une analyse à posteriori, l'attaque étant déjà passée lorsque la sonde IDS la détecte et met en œuvre une contre-mesure.

Les problèmes issus de l'utilisation de cette technologie sont :

- le nombre important de fausses alertes
- le volume des traces d'audit à analyser

- **L'IDS Temps réel en coupure**: Il s'agit d'utiliser la technique de détection d'intrusion à base de signature d'attaque en résolvant les problèmes inhérents à celle-ci : limitation de l'impact sur la performance du réseau et élimination des fausses alertes qui sont évidemment incompatibles avec un dispositif en coupure.

Pour pouvoir utiliser cette technologie ARKOON la combine avec le décodage applicatif pour que seules les attaques indétectables par le décodage soient répertoriées dans la base. Cette combinaison associée à l'utilisation d'une base de signature contextuelle et à un système de scoring des signatures facilite considérablement le travail de comparaison offrant des performances satisfaisantes et éliminant les risques de fausses alertes.

Anti-virus

Un autre élément majeur dans la « boîte à outils » du responsable sécurité est la technique des anti-virus en ligne, qui consiste à rechercher dans un fichier la présence d'un virus à l'aide d'une base de signatures de virus. Avant Internet, la propagation des virus se limitait à l'infection des disquettes insérées dans le lecteur de la machine infectée ; mais depuis l'utilisation massive d'Internet, les virus se sont « mutés » en vers et utilisent Internet et les réseaux comme mode de propagation (notamment par mails et via serveurs Web). Il est donc devenu nécessaire d'analyser les échanges pour s'assurer de la non présence de virus dans les fichiers échangés. Aujourd'hui, les produits s'attachent principalement à l'analyse des flux mails (SMTP, POP3) et web (HTTP, FTP) ; demain, il sera nécessaire d'analyser également les autres types d'échanges (File-Sharing, Instant-Messaging, Travail collaboratif, etc...)

- Avantages : seule technologie viable pour identifier les codes malicieux.
- Limitations : technologie réactive, nécessite la mise à jour d'une base de signatures de virus. Risque lié aux performances, dans son utilisation en ligne, si l'implémentation de la technique n'est pas bien faite.

Synthèse

Tableau : Technologies / niveau de protection

Protection	Réseau	Protocole Applicatif		Contenu
		Non respect protocole	Respect protocole	
Filtrage IP à état	Oui			
Décodage applicatif		Oui		
Base signature d'attaques		Oui	Oui	
Antivirus				Oui

Tableau : produits / Technologies

Technologies	Filtrage IP	Décodage applicatif	Base signatures	Antivirus
Firewall « stateful »	X			
Firewall applicatif : Proxy / Reverse-Proxy		X		
Firewall applicatif « temps réel »		X		
Sonde IDS			X	
IDS en coupure			X	
Gateway Anti-virus en ligne				X

Comme le montre les tableaux de synthèse ci-dessus, il est nécessaire de combiner les différentes techniques existantes afin de disposer d'une architecture de sécurité périmétrique qui saura répondre aux différentes menaces qui pèsent sur le système d'information de l'entreprise en agissant sur les différents niveaux des flux de communication.

4 L'approche ARKOON

Face à ces différentes menaces (réseau, applicatif, contenu), ARKOON a développé le concept de sécurité multi-niveaux pour offrir une protection périmétrique complète à ses clients.

Résultat d'investissement en Recherche et Développement très important depuis plus de 3 ans, ARKOON propose aujourd'hui une technologie exclusive qui s'appuie sur :

- L'architecture d'intégration logicielle SSA (Scalable Security Architecture)
- La technologie de filtrage applicatif temps réel FAST (Fast Applicative Shield Technology)

Les principaux bénéfices de la technologie ARKOON sont de permettre :

1°) d'intégrer les différentes techniques de protection pour qu'elles agissent de manière complémentaire suivant les 3 niveaux.

2°) d'offrir un niveau de performance élevé qui permet le fonctionnement combiné des fonctions de sécurité sans dégrader les performances du réseau (pas de goulot d'étranglement): analyse des protocoles applicatifs, analyse niveau transport en mode stateful, détection virale, comparaison à une base de signature.

La technologie FAST

Développée par ARKOON depuis l'année 2000, la technologie FAST est la première technologie de filtrage temps réel qui combine les techniques employées dans le filtrage IP à état (stateful) et le décodage applicatif. Elle permet de bloquer à la fois les attaques « réseau » et les attaques qui ne respectent pas les protocoles applicatifs.

Le décodage applicatif s'appuie sur une technique d'analyse des flux au niveau des protocoles de communication inter application (HTTP, FTP, SMTP, POP3, H323, DNS...) :

Contrôle de conformité aux RFC

Permet de détecter des attaques de type ne respectent pas les RFC :

- Redirection, interception d'appel, DoS... sur protocoles VoIP (H323,SIP) :
- Import de cheval de Troie par introduction de données binaires dans les en tête http

Contrôle de l'utilisation (normale) du protocole

- Détection des protocoles type P2P encapsulés pour se protéger des attaques et les contrôler (instant messaging, file sharing)
- Directory transversal qui, permette à un hacker de prendre la main sur un site web en utilisant des requêtes « anormales » dans l'URL.
- Buffer overflow par utilisation d'URL très longue.

Limitation de la capacité des requêtes applicatives à transporter des données malicieuses

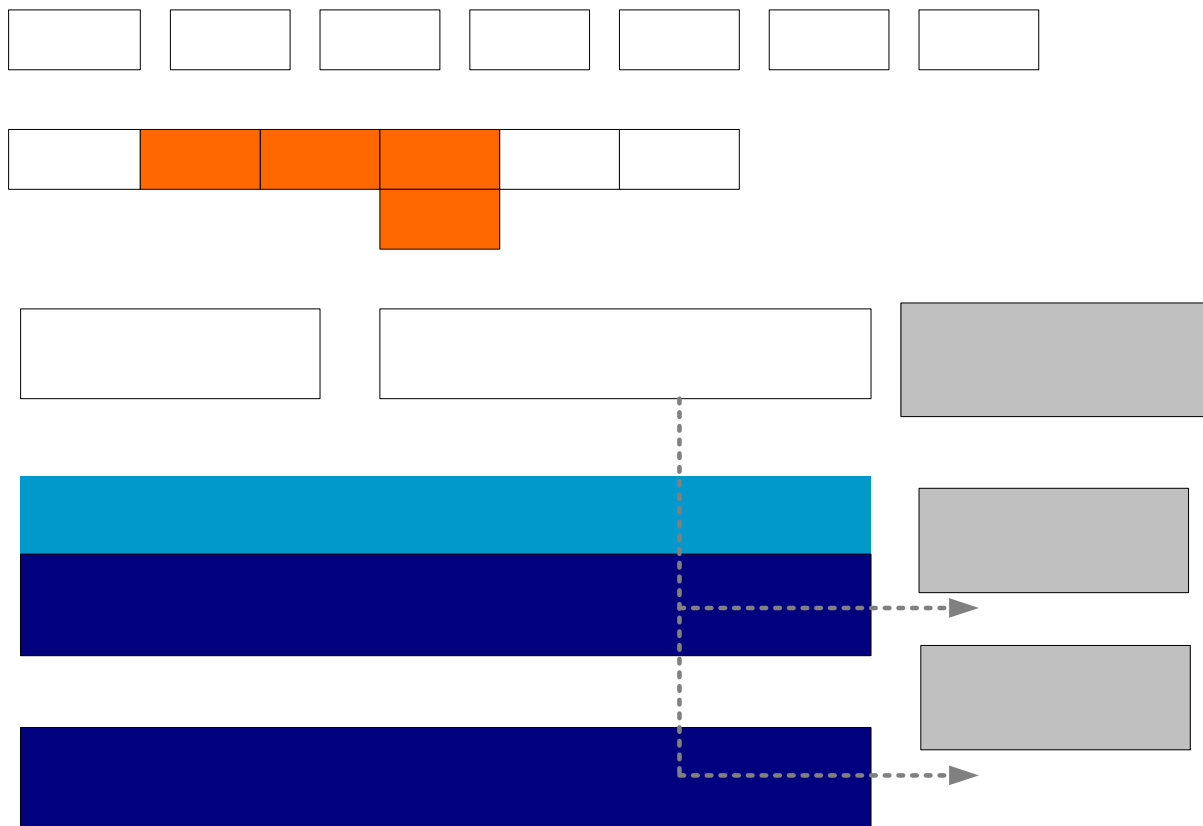
Protection contre

- Attaques de type cross site scripting qui permette au hacker de se substituer à un utilisateur dans la relation avec un site web en lui volant ses paramètres d'identification. Cette attaque est lancée en introduisant un script caché dans une requête http
- Attaques lancées en insérant des données malicieuses dans un URL

Contrôle des opérations par mise en place de règles sur les protocoles

- Limitation/Interdiction des commandes (ex : Interdiction de la commande 'Site' sur le protocole FTP).
- Limitation de la taille des commandes/paramètres (ex : Limitation de la taille des requêtes http).
- Etc....

Principe de fonctionnement de FAST illustré sur un exemple concernant un flux http



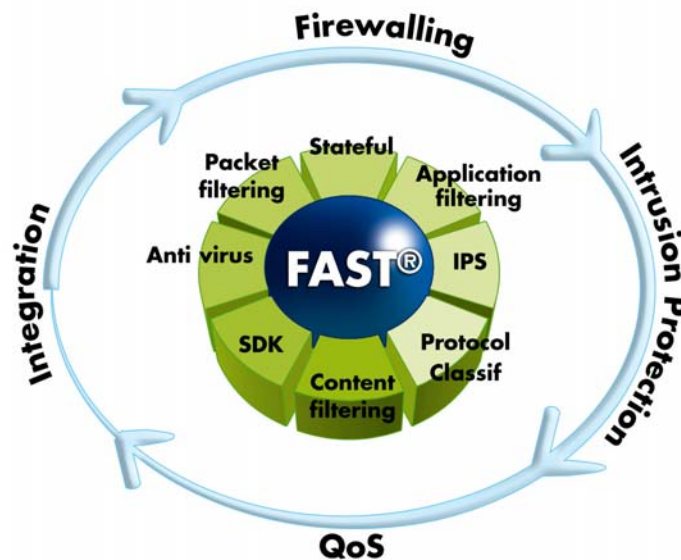
1°) Réception des paquets

GET /Dev/RE base/../../../../

2°) Défragmentation / ré

Architecture SSA

La « Scalable Security Architecture (SSA) » est une architecture logicielle qui permet d'intégrer différents services de sécurité tout en garantissant un haut niveau de performance. Dans le cadre de SSA les services de sécurité sont implémentés sous la forme de composants entièrement développés en mode noyau (« Kernel Space ») et qui s'exécutent à l'intérieur d'un système d'exploitation sécurisé. Il s'agit d'une architecture modulaire dans laquelle les modules communiquent directement avec les drivers sans traverser les couches réseau et système de l'O.S. Ce modèle évite aux modules FAST® d'être interrompus par des processus non critiques et offre une performance exceptionnelle.



L'architecture SSA permet à Arkoon et à ses partenaires de construire des solutions à haut niveau de sécurité capables de supporter des applications « critiques » nécessitant des niveaux de performance élevés à la fois en terme de flux (plusieurs Gb/s) et de type d'utilisation (requêtes http ou DNS, nombre de messages, etc....). La mesure de ces performances a fait l'objet de benchmarks qui permettent de dimensionner précisément les solutions tirant parti de l'architecture de sécurité FAST®.

Sur la base de SSA, les solutions de sécurité multi-niveaux Firewall/IPS d'ARKOON combinent les différentes technologies:

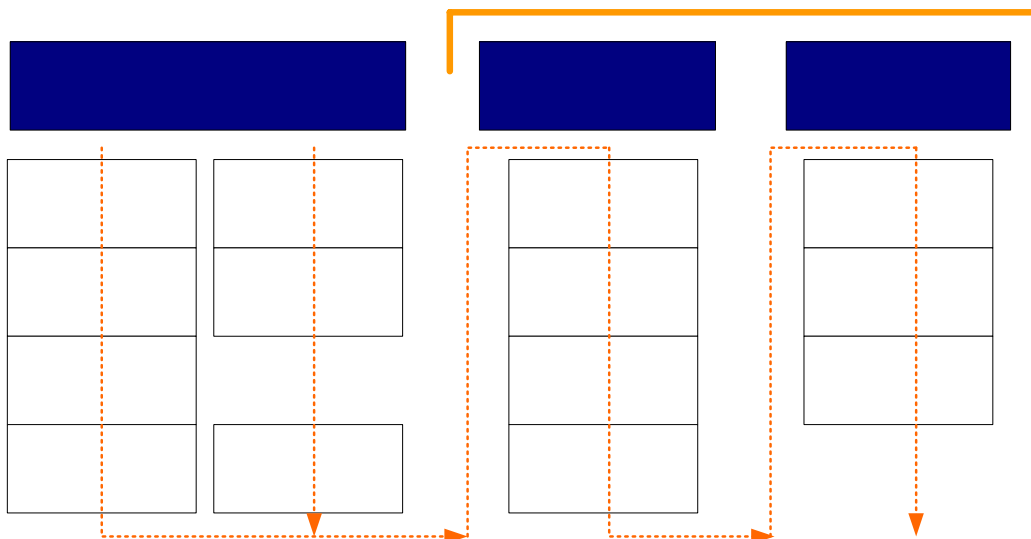
- Filtrage IP à état : Moteur stateful (niveau 3 & 4)
- Prévention d'intrusion par Décodage applicatif [FAST]
 - Contrôle de conformité aux RFC et des règles protocolaires,
 - Contrôle de l'utilisation des protocoles applicatifs,
 - Plus de 20 protocoles supportés : HTTP, FTP, SMTP, POP3, IMAP4, DNS, H323, ...
- Détection d'intrusion en coupure à base de signatures contextuelles [R.T IDS]
- Gateway antivirus : Intégration d'un antivirus permettant l'éradication virale à la volée dans les flux HTTP, SMTP, POP3

Bénéfices de l'architecture SSA

- **Evolutivité** : SSA est une architecture « ouverte » Elle permet, via la mise à disposition d'un kit de développement et l'utilisation d'API, d'ajouter des composants de sécurité :
 - Module de décodage d'un protocole applicatif propriétaire
 - Utilisation d'un moteur d'analyse anti-virus alternatif
 - Connexion à un nouveau type de serveur de filtrage d'URLs
 - Création d'un nouveau mode d'administration/supervision
 - Etc....
- **Performances** : La technologie FAST et l'architecture SSA rendent possible la conception de solution de sécurité haute performance même en implémentant des fonctions réputées très consommatrices de ressources comme le décodage applicatif, la détection d'intrusion à base de signature en ligne ou encore l'éradication virale en ligne.
- **Administrabilité** : Outre la combinaison des différentes techniques de protection pour bâtir une solution de sécurité multi niveaux, l'architecture SSA permet de définir un environnement d'administration unique permettant de gérer l'ensemble des fonctions de sécurité en cohérence par rapport à la politique de sécurité.

FAST In line IDPS – «Intrusion Detection and Prevention System» -

Le FAST In line IDPS est la combinaison du décodage applicatif avec la détection d'intrusion à base de signatures contextuelles l'ensemble fonctionnant en temps réel. Cette combinaison permet en effet de limiter la taille de base de signature aux seules signatures d'attaques qui sont indétectables par décodage applicatif limitant la consommation de ressources associées et permettant ainsi d'utiliser cette technique en coupure sans dégrader les performances.



Avec l'adjonction de la technologie de détection d'intrusion à base de signature d'attaque au moteur d'analyse (décodage applicatif) ARKOON offre aujourd'hui les premières appliances de sécurité périmétriques réellement multiniveaux du marché combinant firewall, prévention d'intrusion, détection d'intrusion et antivirus en ligne.

Aspect performances

La capacité d'une technologie ou d'un composant de sécurité à assurer sa fonction dans des conditions d'utilisation pour lesquelles les volumes d'échanges sont importants est un facteur essentiel.

En ce qui concerne le filtrage applicatif les solutions à base de proxy offrent du point de vue fonctionnel une solution pertinente. Elles s'avèrent néanmoins extrêmement coûteuses dès qu'il s'agit de traiter des volumes de flux important avec un niveau de performance acceptable. Des tests de performance démontrent que l'implémentation de la technologie FAST de décodage applicatif en mode « analyse temps réel » présente des performances 100 fois plus rapide qu'une implémentation de type « proxy ».

La détection d'intrusion en coupure quand à elle présente des contraintes liées à l'utilisation en temps réel. L'implémentation du FAST in line IDPS ARKOON a utilisé les principes suivants :

- Utilisation en complément des niveaux firewall stateful et décodage applicatif,
- Tirer partie de la vitesse du moteur d'analyse FAST,
- Disposer d'une base de signatures suffisante et évolutive pour détecter et bloquer de manière certaine les attaques connues.
- Mettre en œuvre la technique de comparaison à la base de signature en mode contextuel (stateful) pour limiter le nombre de fausses alertes (false positive) et optimiser le traitement.

A titre d'exemple, voici un extrait des performances mesurées sur une appliance ARKOON de type A 5000 :

- **Throughput : 1,7 Gbits/s** - Cette mesure caractérise la qualité du moteur de « Filtrage IP à état », et par conséquent la performance de la protection au niveau réseau.
- **Nombre de sessions TCP : 25000 /s** – IDEM
- **Nombre de requêtes HTTP : 17000 /s** – Mesure la performance du moteur de « Décodage applicatif » en temps réel FAST.

Complémentarité avec les autres technologies :

Sonde IDS

Si les sondes IDS et les solutions de sécurité périmétriques ARKOON utilisent la même technique de détection d'intrusion à base de signatures d'attaques, elles sont complémentaires et répondent à des besoins différents : pas non plus en concurrence frontale. En effet, elles ne sont pas utilisées de la même façon

- Situées « en coupure » les solutions ARKOON sont des équipements actifs, elles utilisent la technique de détection d'intrusion à base de signatures d'attaques combinée avec le décodage applicatif pour faire de la détection et prévention d'intrusion en temps réel. Ce mode d'utilisation nécessite de garantir les performances pour ne pas ralentir le flux et de limiter au maximum le nombre de « faux positif » (détection d'une attaque dans un flux n'en contenant pas) pour éviter de couper la communication de manière intempestive. Pour ces raisons les solutions ARKOON s'appuie sur une base de signatures réduite par rapport à ce que proposerait une sondes IDS.
- De leur côté, les sondes IDS sont des équipements passifs qui écoutent le trafic réseau sans être en coupure. Elles stockent en général beaucoup de données (paquets issus du réseau) afin de retrouver à posteriori l'environnement d'une attaque, cette fonction n'est pas remplie par la solution de sécurité périmétrique pour des questions de performance.

Reverse-Proxy

Si les solutions de sécurité périmétrique ARKOON et les reverse-proxies sont parfois tous les deux qualifiés de « firewall applicatif », il s'agit en fait de produits différents et plus complémentaires que non concurrents :

- Les reverse-proxies sont limitées aux protocoles HTTP et HTTPS. Ils proposent des fonctions avancées tels que l'accélération SSL, l'authentification des utilisateurs, l'accélération du transport des données (cache, compression, ...). Ils sont généralement utilisés combinés avec un Firewall pour protéger un site web. Etant dédiés aux protocoles HTTP/HTTPS et fonctionnement en mode « proxy », les reverse-proxies sont capables de réaliser des **opérations de filtrage au niveau de l'application elle-même** : interdire l'accès à une partie de l'arborescence web, ou n'autoriser le passage que du flux attendu par l'application par exemple. Si les flux sont importants le mode Proxy utilisé dans ces produits sera gourmand en ressources machine.
- Les solutions de sécurité ARKOON réalise **des opérations de filtrage au niveau des protocoles applicatifs** (par opposition à l'applicatif lui-même), elles sont multi protocoles (donc non limitées à HTTP/HTTPS) et permettent de bloquer les attaques concernant des protocoles aussi divers qu'http, DNS, H323 ou SNMP. Les appliances de sécurité ARKOON sont utilisées pour segmenter les différentes parties d'un réseau en autant de zone de sécurité et n'autoriser que le trafic, quelque soit le protocole utilisé, conforme aux règles, protocoles ou usage attendu Elles ne supportent pas, par contre, les fonctions avancées de filtrage au niveau de l'application web elle-même pas plus que les fonctions d'accélération web proposées par les reverse proxies. Les solutions de sécurité ARKOON utilisant la technique de décodage applicatif

temps réel supportent des débits beaucoup plus importants que les reverse-proxies (technologie FAST).

Anti-virus sur poste de travail

L'antivirus en ligne et l'antivirus sur les postes de travail ne sont pas antagonistes. En effet :

- L'utilisation de moteur anti-virus d'éditeur différent sur la solution de sécurité périmétrique et sur les postes de travail permet d'augmenter le niveau de sécurité (Possibilité qu'une signature de virus soit fournie par un éditeur mais pas par l'autre)
- Une défaillance d'un des deux types d'antivirus est toujours possible
- L'utilisation d'un antivirus sur la solution de sécurité périmétrique permet de libérer de la ressource sur les serveurs internes (particulièrement les serveurs de mail) qui n'auront pas à traiter les messages vérolés
- Un virus peut entrer sur le réseau sans passer par la solution de sécurité périmétrique (disquette, connexion Internet sauvage via modem, ...)

5 Conclusion

La menace évolue rapidement. Face à la multiplication et la sophistication des nouvelles attaques, les entreprises ont montré qu'elles n'étaient que très partiellement protégées et que bien souvent leurs systèmes de protection étaient mal administrés.

La sécurité des réseaux est une problématique multi-niveaux qui ne peut se régler qu'en combinant différentes technologies dans le cadre d'une architecture susceptible de procurer le niveau de performance attendu et la capacité à évoluer en intégrant de nouvelles fonctions de sécurité capables de s'exécuter en ligne.

Nous pensons que l'avenir des solutions de sécurité périmétrique passe par cette combinaison dans le but de toujours améliorer le compromis sécurité/performances.