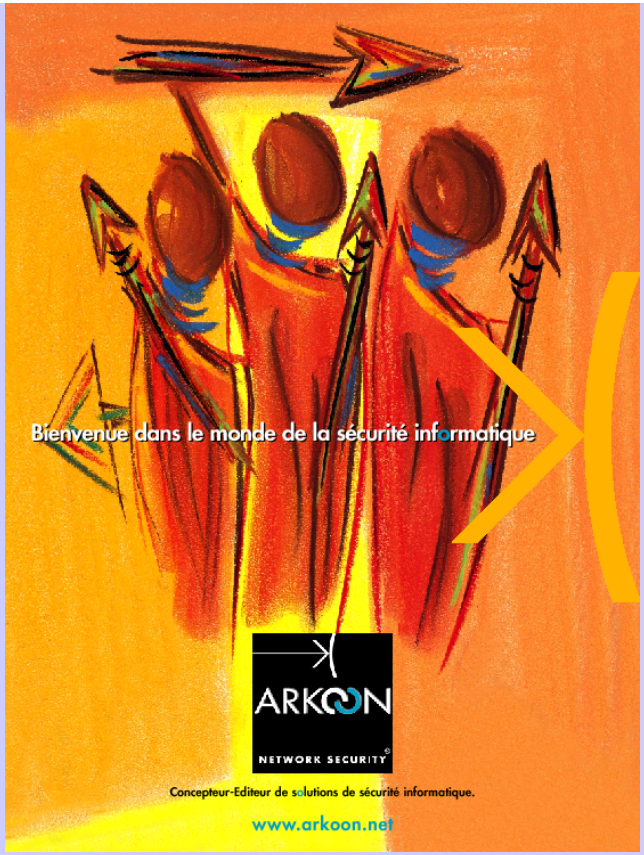
ARKOON NETWORK SECURITY

Technologie Fast
&
Suites Intégrées



Aujourd'hui :

- Concepteur et éditeur de solutions de sécurité pour les grands comptes et les PME-PMI
- SA de 35 personnes au capital de 1,9 M€
- 3 implantations (2 en France et 1 en Italie)

Siège à LYON :

13A, Av. Victor HUGO
69160 LYON TASSIN

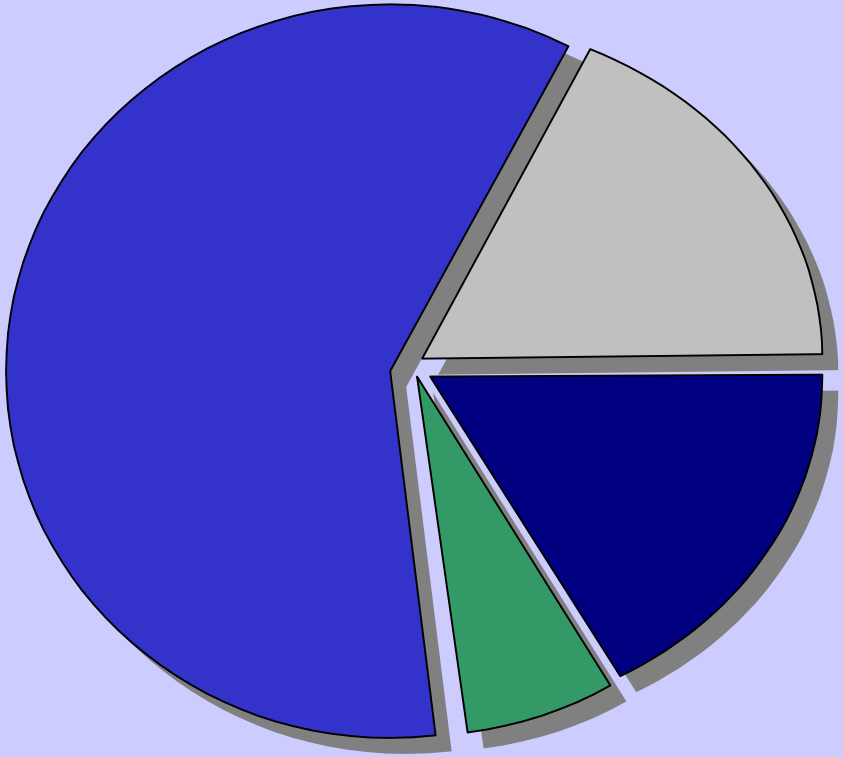
Tél: +33 (0)4 72 53 01 01
Fax: +33 (0)4 72 53 12 60

Agence de PARIS :

6 ter, Rue Denis PAPIN
92600 ASNIERES

Tél: +33 (0)1 49 97 02 12
Fax: +33 (0)1 49 97 02 13

Nos partenaires financiers



THALES
Thomson-CSF

NATEXIS
BANQUES
POPULAIRES

BNP PARIBAS

Arkoon et les institutions gouvernementales

Subventionné par l'ANVAR Développement
sur 2002-2003

Certifications DCSSI Critères commun
Prévue pour le premier semestre 2002

Notre réseau de partenaires

→ Internationaux

→ Nationaux et Régionaux

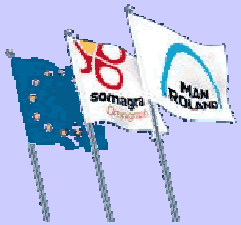
- couverture nationale, régionale de proximité,

- Le réseau de distribution Arkoon compte aujourd'hui plus de 40 partenaires répartis sur le territoire national

Nos références clients

Clients: de grands noms de différents secteurs ont fait confiance à Arkoon dans les domaines tels que : l'aéronautique, la banque, les télécommunications, les collectivités locales, l'industrie agro-alimentaire, pharmaceutiques, pétrolière, l'expertise comptable et financière, l'industrie du plastique, la santé, l'immobilier……

Ministère de l'équipement

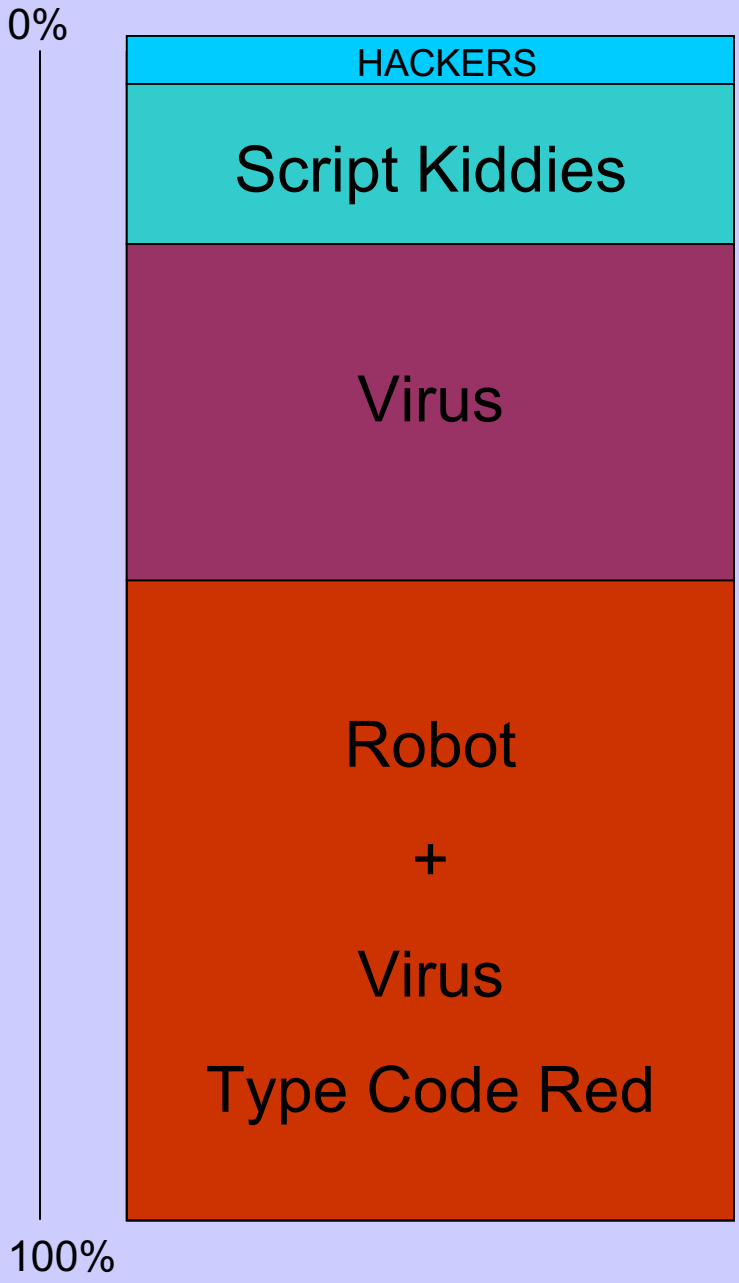


Départ de la réflexion !

- De plus en plus de déni de service par violation de protocole
- Des attaques de grandes envergures sont cachées dans le contenu des requêtes
- Les modèles actuels permettant de travailler au niveau applicatif posent des problèmes de performance (Proxies)

Introduction aux risques de piratage

Par qui est on attaqué ?



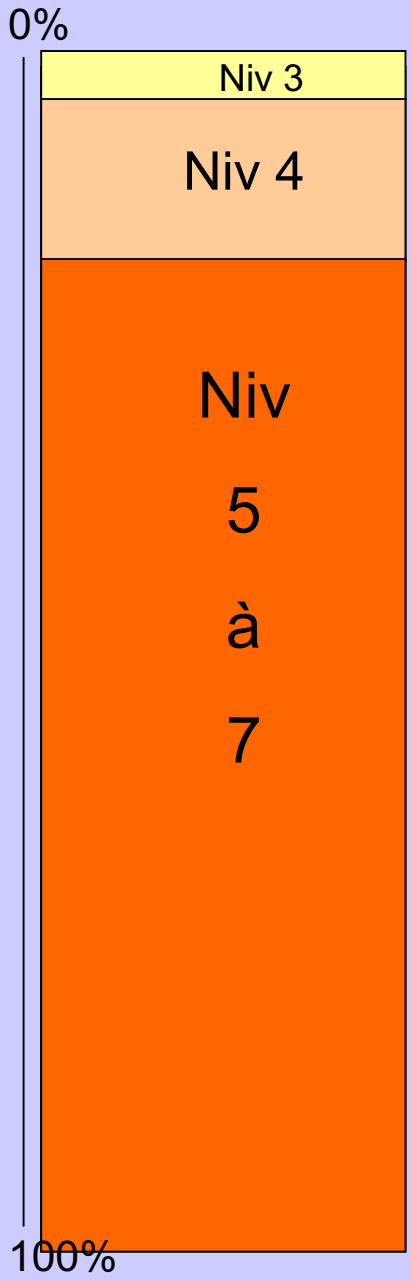
Ils ne s'intéressent qu'aux défi et aux grandes causes … peu de chance de les rencontrer

Ils utilisent des boites à outils du pirate, ils attaquent les sociétés ou la protection n'est pas importante.
Toute adresse IP sur Internet est soumise à leurs « scan » au moins 1 fois par jour !

Les virus touchent 80 % des entreprises.
Leurs actions vont du simple message à la destruction pure et simple de toutes vos données.
Les nouveaux virus se propagent à la vitesse de l'internet, ils font le tour du monde en quelques heures et personne n'est épargné
Les faiseurs de virus sont de plus en plus nombreux et créatifs.

La grande révolution :
Des robots-virus se disséminent à la vitesse des virus et ensuite utilisent les machines piratées pour attaquer d'autres machines.
Cette technique de démultiplication fait que très rapidement des dizaines de milliers de machines sont corrompues. Ces machines sont attaquées aléatoirement, tous le monde en est la cible de la GE au particulier en passant par les PME, les société comme la votre …...

Quels types d'attaque subissont nous ?



Les attaques utilisant uniquement des failles IP ne représentent plus qu'un pourcentage très faible des attaques actuelles

Le vol de session et autres attaques limitées au niveau 4 sont considérées comme minoritaire.
Les attaques qui mettent en défaut les sessions tracking sont très sophistiquées, elles sont généralement combinées à des attaques applicatives.

Les attaques applicatives sont les plus nombreuses actuellement, elles passent au travers de la plupart des firewalls, elles sont minoritairement manuelles (hacker, script kiddies) et majoritairement automatiques via des robots-virus.
C'est le cas de Code Red qui en quelques jours a pris le contrôle de plus de 10 000 serveurs dans toutes les tailles de société.

De plus en plus les société vont devoir interagir via internet, en s'ouvrant à ses clients/fournisseurs par des portails, en utilisant la messagerie comme véhicule d'ordre et de commandes, elles sont de plus en plus exposées à ces attaques applicatives.

Quels dégâts après un piratage ?

Les attaques utilisant uniquement des failles IP ne représentent plus qu'un pourcentage très faible des attaques actuelles

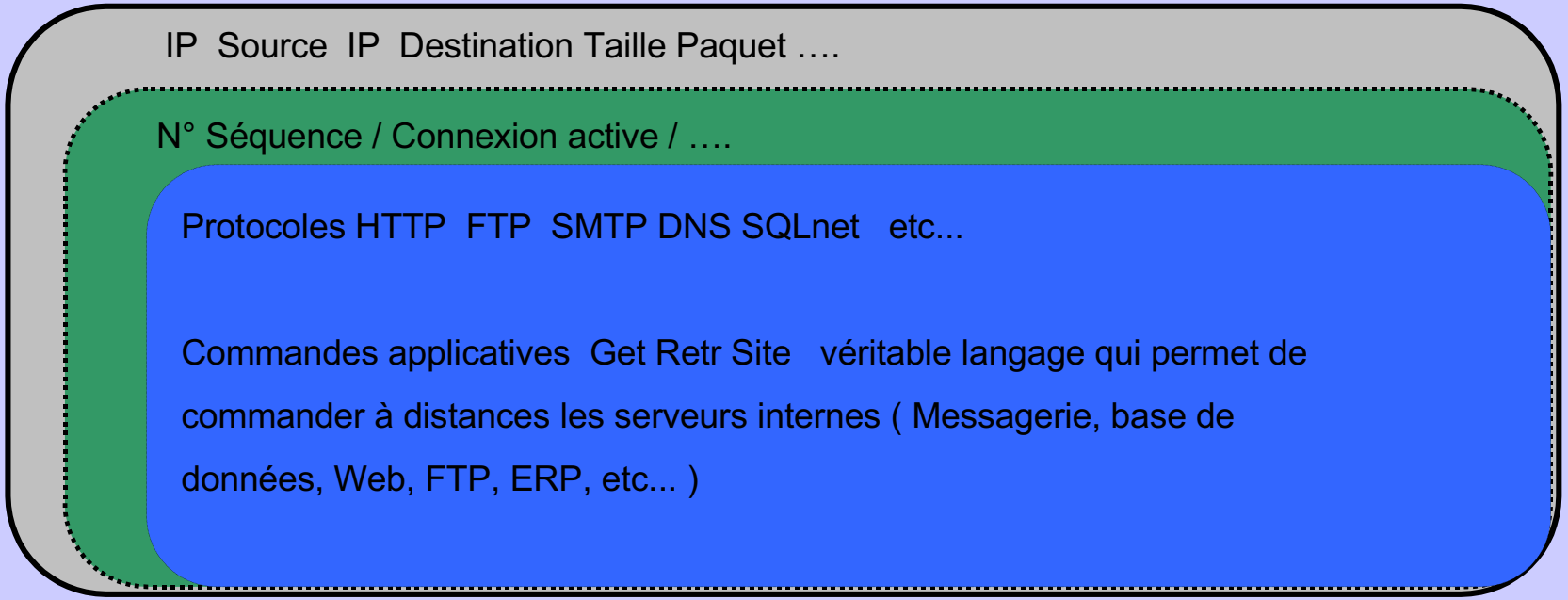
La seule chose à espérer est d'avoir une sauvegarde.
Il faut bien souvent réinstaller les programmes et les données si on tombe sur un virus comme Tchernobyl ou sur un « script kiddies » qui vous plante définitivement un serveur ou une station.

Que la prise de contrôle à distance soit le fait d'un pirate ou d'un script kiddies travaillant en manuel ou d'un robot virus en automatique, la question est de savoir ce qui est fait :

Votre réseau va souvent devenir un relais de pirate pour d'autres attaques (ce qui ralentit de façon conséquente votre réseau), il va servir de site de stockage pour des contenus frauduleux (jeux et logiciels piratés). Les actions sont souvent pernicieuses, on recherche les informations importantes de votre société (pas seulement R&D) comme les données commerciales ou financières, ensuite elles sont soit modifiés discrètement, soit vendues sur des bourses d'information ou à votre concurrent (sources DST).

COMMENT NOUS PROTEGER ?

TCP/IP :
Que cherchons nous à contrôler ?



Des éléments dans d'autres éléments, le système des poupées russes :

externe = niveau 3 permet de véhiculer le paquet au travers du net

intermédiaire = niveau 4 permet un suivi du transport entre machines

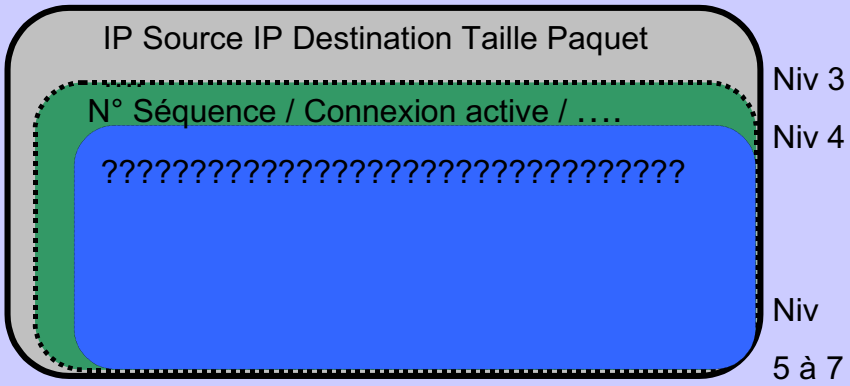
interne = niveau 5 à 7 envoi les commandes vers les applicatifs

Filtrage IP & Session Tracking

Le protocoles de contrôle d'IP (TCP UDP ICMP …) qui permettent à 2 machines de communiquer sont régulièrement transgressés ce qui permet aux pirates d'atteindre leurs cibles.

La création du suivi de session répond à ce besoin de sécuriser le contrôle de la communication entre ordinateurs.

Cette protection est insuffisante car à ce stade de l'analyse on ne sait toujours pas ce que l'on transporte.



Bénéfice : élimine toutes les attaques de niveau 3 & 4 (Hi-jacking, IP spoofing ..)

Inconvénient : ne permet pas de vérifier ce qui est transporté

Utilisation : Ces fonctions ne sont plus suffisantes, elles ne bloquent pas les attaques modernes.

Quels sont les solutions limitées à ces fonctions ?

Les routeurs avancés,

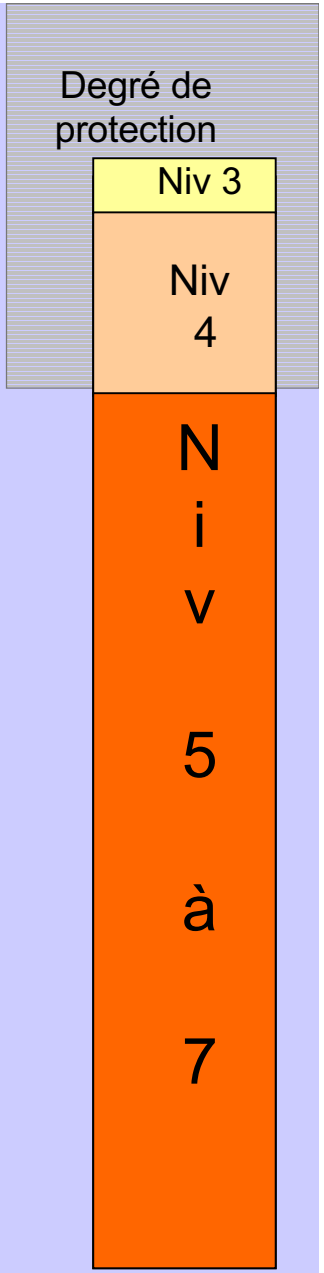
les firewalls niv 3&4

Netasq,

Netscreen,

SonicWall,

Watchguard, etc …

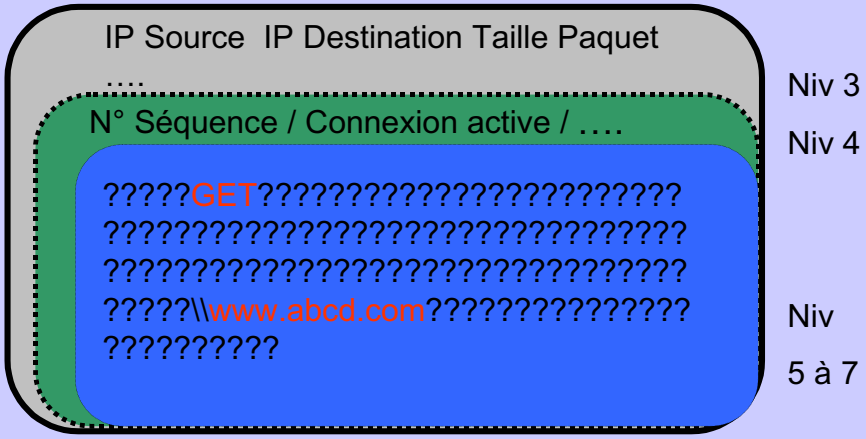


Filtrage IP & Applicatif

Les nouvelles attaques respectent les règles de sécurité des niveaux 3 & 4, elles portent directement sur les applications (Bases de données, serveurs Web, messageries).

Le filtrage applicatif recherche des éléments précis sur le même principe que les signatures anti-virus.

Cette protection est insuffisante car elle ne bloque que certains éléments connus et elle peut être leurrée par la présence de fausses commandes.



Bénéfice : élimine certaines attaques applicatives répertoriées.

Inconvénient : c'est un contrôle par sondage et pas un contrôle global et exhaustif du contenu

Utilisation : c'est le mode de protection le plus répandu, il n'est pas étanche au regard des attaques les plus répandues.

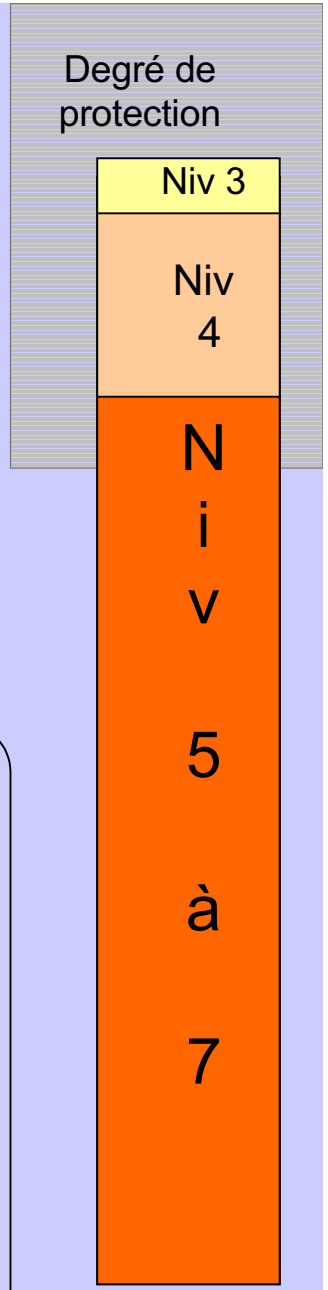
Quels sont les solutions limitées à ces fonctions ?

Les firewalls niveau 7

Checkpoint F1 & VPN1

Cisco Pix Matra Mwall

N.B. : certains de ces firewalls peuvent aussi travailler en mode proxy.



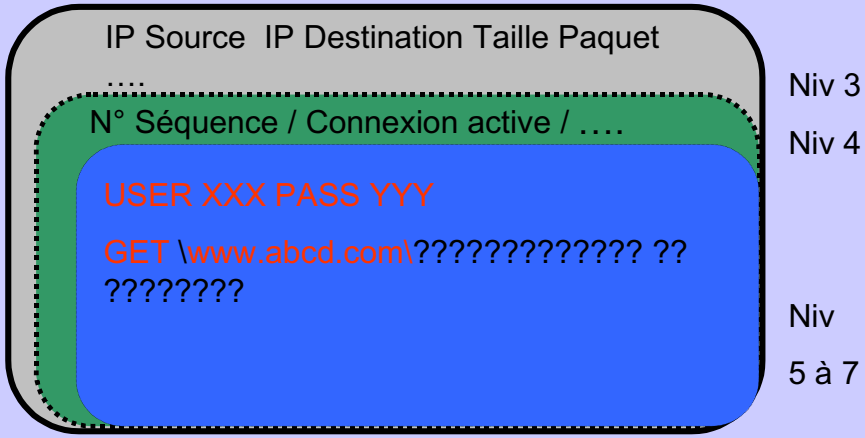
Filtrage IP & PROXY

Les proxy marchent sur un principe de reformulation. Ils se substituent au serveur distant pour répondre au demandeur et reformulent ensuite vers le serveur.

Bénéfice : élimine certains ordres du protocole

Inconvénient : Cette technique est plus tournée compréhension et reformulation que recherche d'attaque.

Utilisation : De moins en moins utilisé car trop lourd et trop contraignant



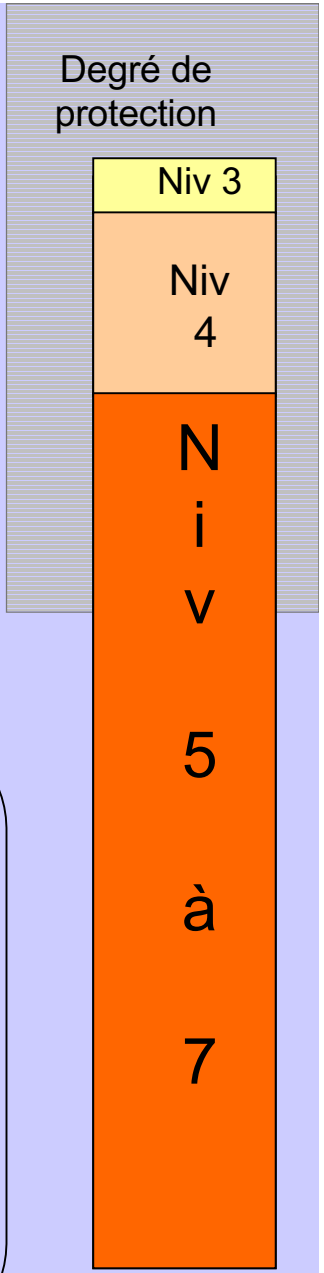
Quels sont les solutions limitées à ces fonctions ?

Les firewalls proxy

Axent Raptor,

Bull Netwall,

Matra Mwall …



Un nouveau modèle : la technologie « FAST » d'ARKOON

F ast

A pplicative

S hield

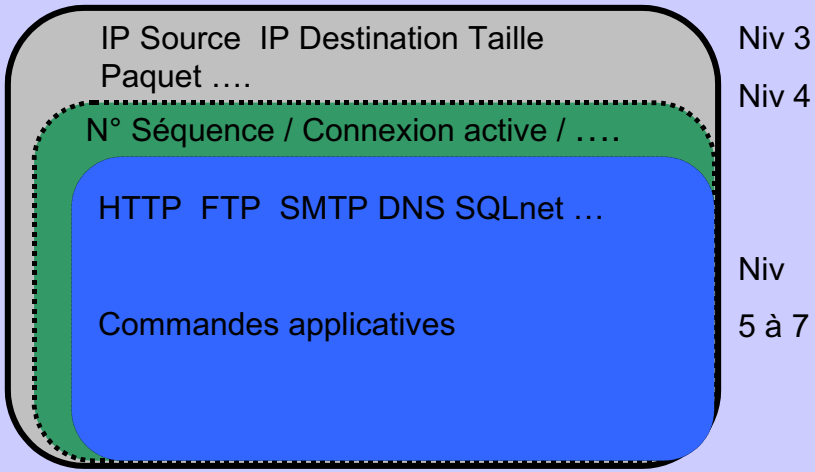
T echnology

SUIVI DE SESSION IP & APPLICATIVE

Les serveurs applicatifs (messageries, publics, base de données …) ont systématiquement des failles qui permet de corrompre, il faut donc filtrer les ordres leur parvenant pour éliminer ceux qui sont incorrects ou dangereux.

Le suivi de session applicatif impose le respect du protocole applicatif. Il impose le suivi des différents états du protocoles, de sa syntaxe et de sa grammaire.

Cette protection va jusqu'à permettre de bloquer de façon certaine les commandes applicatives pour protéger les serveurs.



Bénéfice : Permet un contrôle total des flux par une compréhension de l'intégralité de ce qui est transporté.

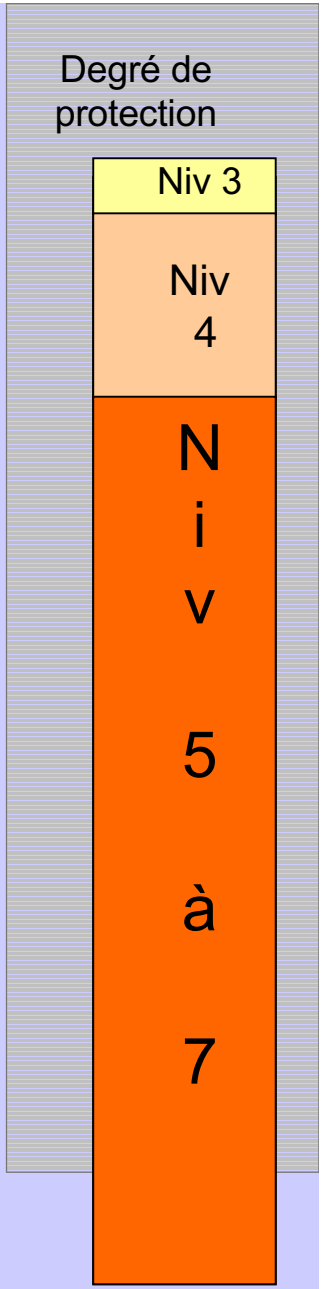
Inconvénient : à vous de nous le dire !

Utilisation : c'est le présent et l'avenir de la guerre contre le piratage.

Quels sont les solutions présentant ces fonctionnalités ?

Aujourd'hui ARKOON est le seul éditeur possédant ce niveau de protection.

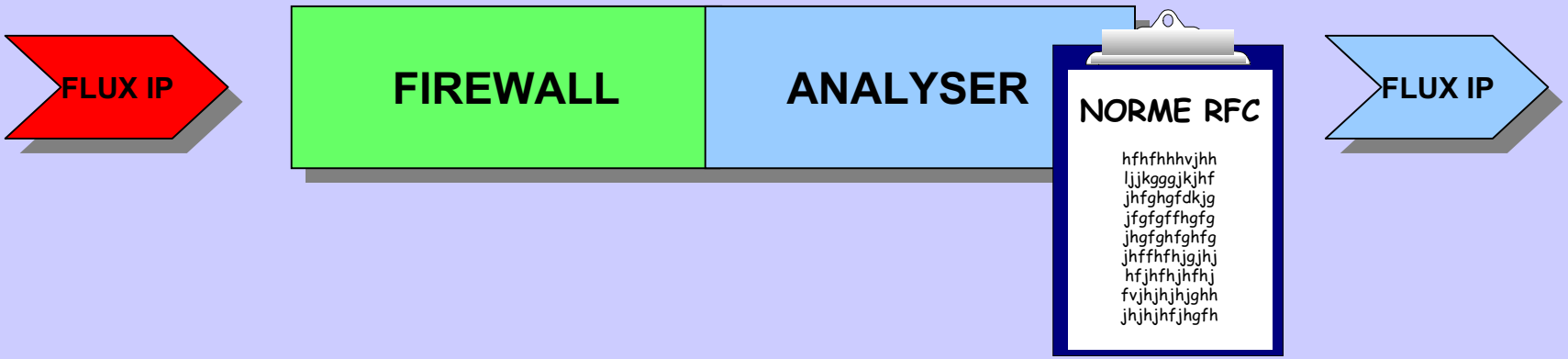
La technologie FAST vise le plus haut niveau de sécurité existant car il a été conçu pour contrer les attaques les plus modernes.



Technologie « FAST » d'ARKOON

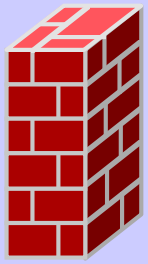
FIREWALL Classique:

FIREWALL / ANALYSER « ARKOON »:

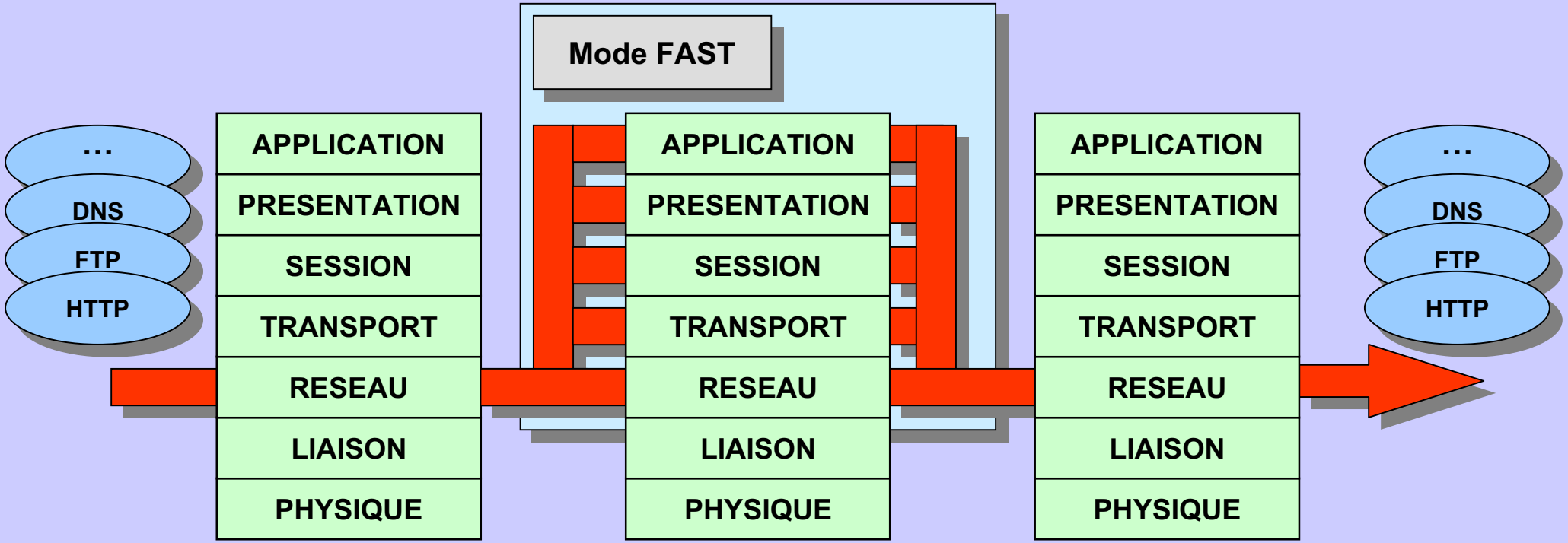


Technologie « FAST » d'ARKOON

- Très Bonne Sécurité
- Reconstitution Applicative Complète (niv 7)



- Très Bonnes Performances
- Simple à mettre en Oeuvre
- Contrôle au Niveau 3/4



Technologie « FAST » d'ARKOON

- Firewall « niveau 7 applicatif »
  - « **Session Tracking** » suivi des sessions (tables connexions actives)
  - Vérification couche **OSI/3** (IP) et couche **OSI/4** TCP/UDP/ICMP (Normes RFC)
- Analyseur de protocoles applicatifs TCP/IP
  - Vérification « à la lettre » du respect des protocoles applicatifs (HTTP, FTP, SMTP, POP3, NNTP, DNS, IMAP4, RTSP, H323, Netbios) en fonction des normes RFC
  - **Filtrage dynamique complet au niveau applicatif** avec reconstitution de la trame et analyse de l'intégralité du message
- Règles protocolaires
  - Permet d'interdire certaines commandes d'un protocole (ex: la commande « site » du protocole FTP qui exécute une commande à distance sur un serveur)
  - Règles protocolaires applicatives **Sans Proxy**
- Analyseur modulaire
  - Capable d'intégrer un protocole TCP/IP Propriétaire ou nouveau

Technologie « FAST » d'ARKOON

- Administration unique et centralisée
  - Une seule machine pour tous les modules **ARKOON**
  - ARKOON « **Maître** » au siège et « **Esclave** » sur les sites distants
- Mise à jour à distance
  - Cryptage SSL V3 128 Bits
- Hardware et OS sécurisé
  - O.S. de base sur **noyau linux simplifié** (30 Mo) sécurisé et en clair
  - Carte PCMCIA pour l'O.S. et le Logiciel (Boîtier Rackable)
  - HA – Haute Disponibilité (ARKOON Redondant)
- Performances élevées
  - Analyse applicative en **mode noyau** et non en mode utilisateur
  - **Optimisation** du noyau linux et Processeur > 700 Mhz
  - Validation de la Solution **ARKOON** jusqu'à **100Mb/s** entre deux réseaux
  - **ARKOON GigaBit** disponible.

La gamme Arkoon

- Secure Yellow
- Secure Green
- Secure Blue
- Secure Purple

Principaux éléments des Suites **ARKOON**

- **ARKOON Routeur**
- **ARKOON FireWall niveau 3 & 4**
- **ARKOON FAST Applicatif**
- **ARKOON Relais SMTP Anti-virus**
- **ARKOON Proxy Cache + Anti-virus**
- **ARKOON VPN**
- **ARKOON Services Balancing**
- **ARKOON Gestion bande passante**
- **ARKOON Haute disponibilité**
- **ARKOON Admin & Monitoring**

La Suite **ARKOON**

- **ARKOON Fonction routeur**
  - RNIS (avec option carte RNIS intégrée)
  - ADSL
  - CABLE

- **ARKOON FireWall 3&4 / FAST Applicatif**

Filtrage de paquets avancé

Session Tracking (« statefull inspection »)

Translation d‘ Adresse et de Port

La Suite **ARKOON**

- **ARKOON Proxy**

PROXY CACHE HTTP/FTP

– PROXY CACHE pour **augmenter les performances** des flux HTTP et FTP

– Authentification des utilisateurs (NT, LDAP, Radius)

FILTRAGE URL et mots clés

– Filtrage d'URL par « Black List » à thème (sexe, violence, loisirs, etc ..)

– Filtrage du contenu par « mots clés »

- **ARKOON Administration & Monitoring**

– Télé-administration

– Administration Maître-Esclave dans les multi sites

La Suite **ARKOON**

- **ARKOON Antivirus**

Mise à jour quotidienne en **Automatique**

– Sur le serveur **ARKOON** avec certificat SSL V3

Performance

– Librairie intégrée dans le code ARKOON

- **ARKOON VPN**

Sécurité à la norme IPSEC:

– Avec Cryptage (Clés **triple DES 168 bits**)

– Authentification (Clés MD5 et SHA1)

– Échange de Clés utilisant le protocole **IKE**

La Suite **ARKOON**

- **ARKOON** ***Services Balancing***
- **ARKOON** ***Gestion bande passante***

La Suite **ARKOON**

- **ARKOON** ***Haute disponibilité***
- **ARKOON** ***Gigabit***

ARKOON NETWORK SECURITY

Vos contacts:

Directeur R&D
Daniel FAGES dfages@arkoon.net

PDG
Frédéric ROBERT frobert@arkoon.net