Contrôle Applicatif

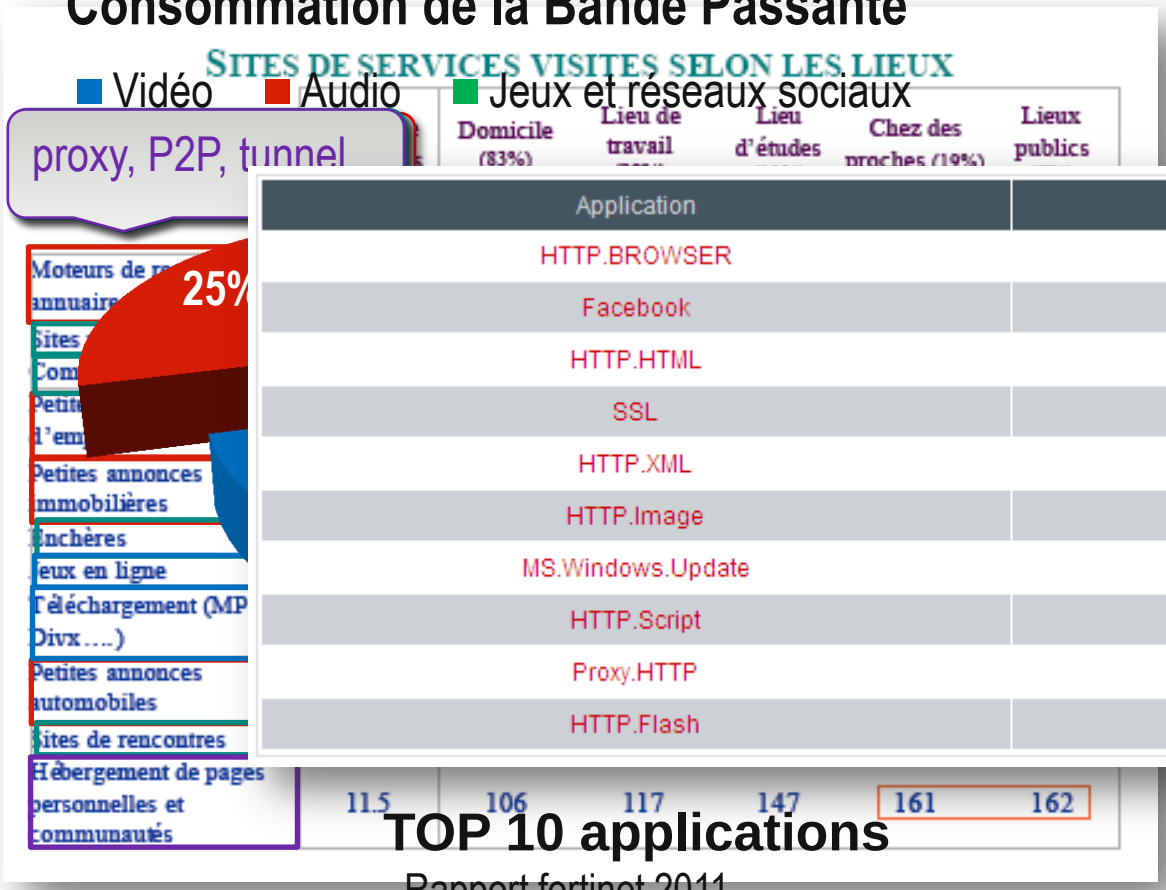
Filtrage multi-couches

Emmanuel RABATAN
Ingénieur Avant Vente Fortinet
erabatan@fortinet.com

Bilan des comportements actuels

Les utilisateurs font plus ou moins ce qu'ils veulent

Consommation de la Bande Passante



Application	Category
HTTP.BROWSER	Web
Facebook	Web
HTTP.HTML	File Transfer
SSL	Network Services
HTTP.XML	File Transfer
HTTP.Image	File Transfer
MS.Windows.Update	System Update
HTTP.Script	File Transfer
Proxy.HTTP	Internet Proxy
HTTP.Flash	File Transfer

TOP 10 applications

- Rapport fortinet 2011 -

nelles
BP
sent les
nde de
Jackson)
nacée
assante

Source IPSOS 2011

Agenda

- La Sécurité Applicative multi-protocoles
- Un focus sur la sécurité des applications web
- Peut être une demo

Evolution des applications

La sécurité autour des applications est obsolète

- Au départ
  - Les applications étaient facilement définies
    - Port ou Protocole
  - Les règles étaient facilement définies
    - Autoriser ou bloquer
    - Le contenu et le comportement sont prévisibles
- Puis vint le Web …

Le parefeu classique sait il contrer les menaces?

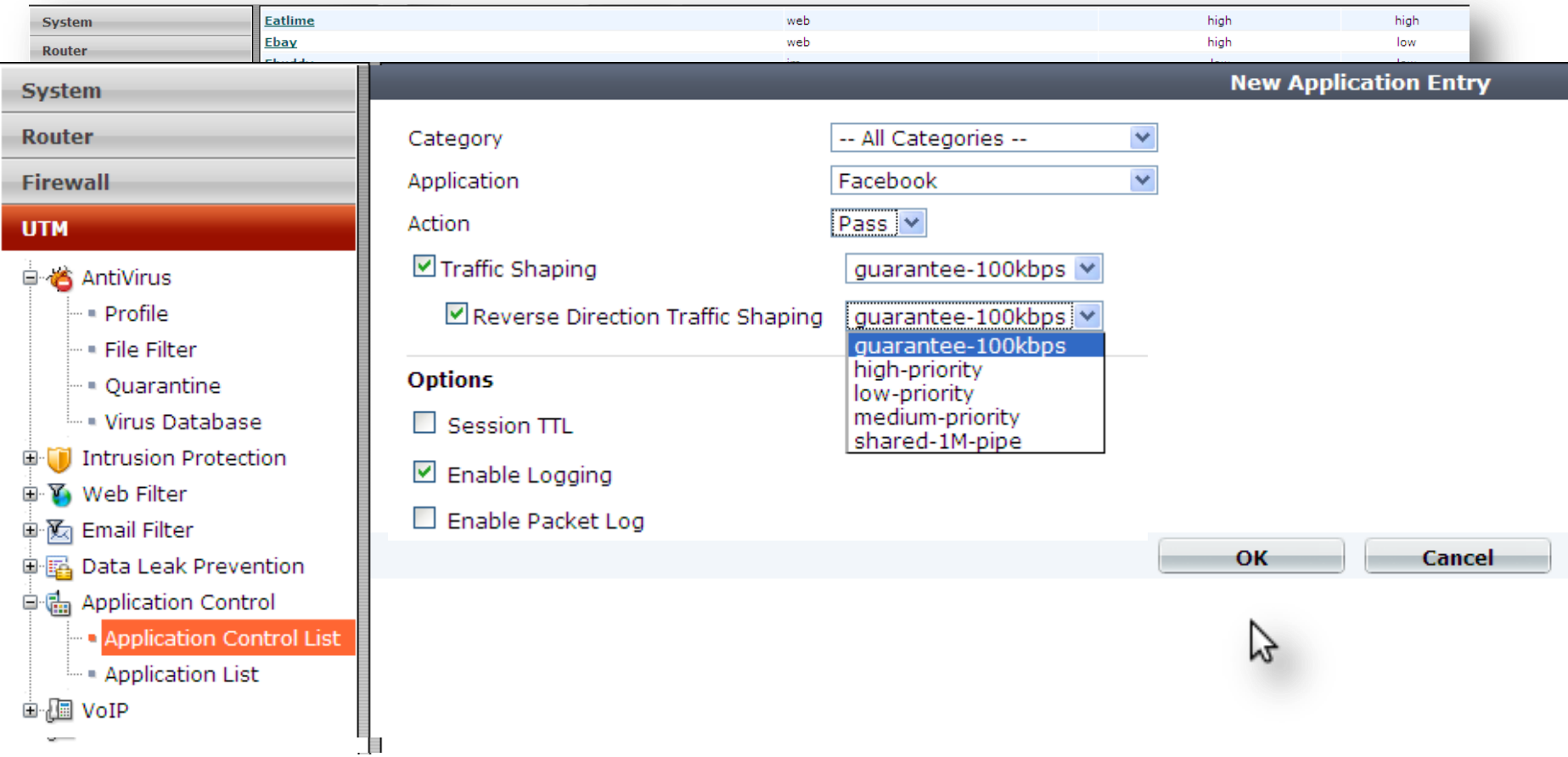
Les applications ont changé

- N'ouvrir qu'une porte ne suffit plus !
  - HTTP : une seule porte (80/tcp) mais plusieurs applications
  - Une application web : plusieurs sous application

Sécurité Applicative multi-protocoles

Les solutions des parefeux intelligents

en images



Les solutions des parefeux intelligents

en images

Memory

Log Type: Application Control Log

1 / 2 Column Settings Raw Clear All Filters

Quelque soit le port

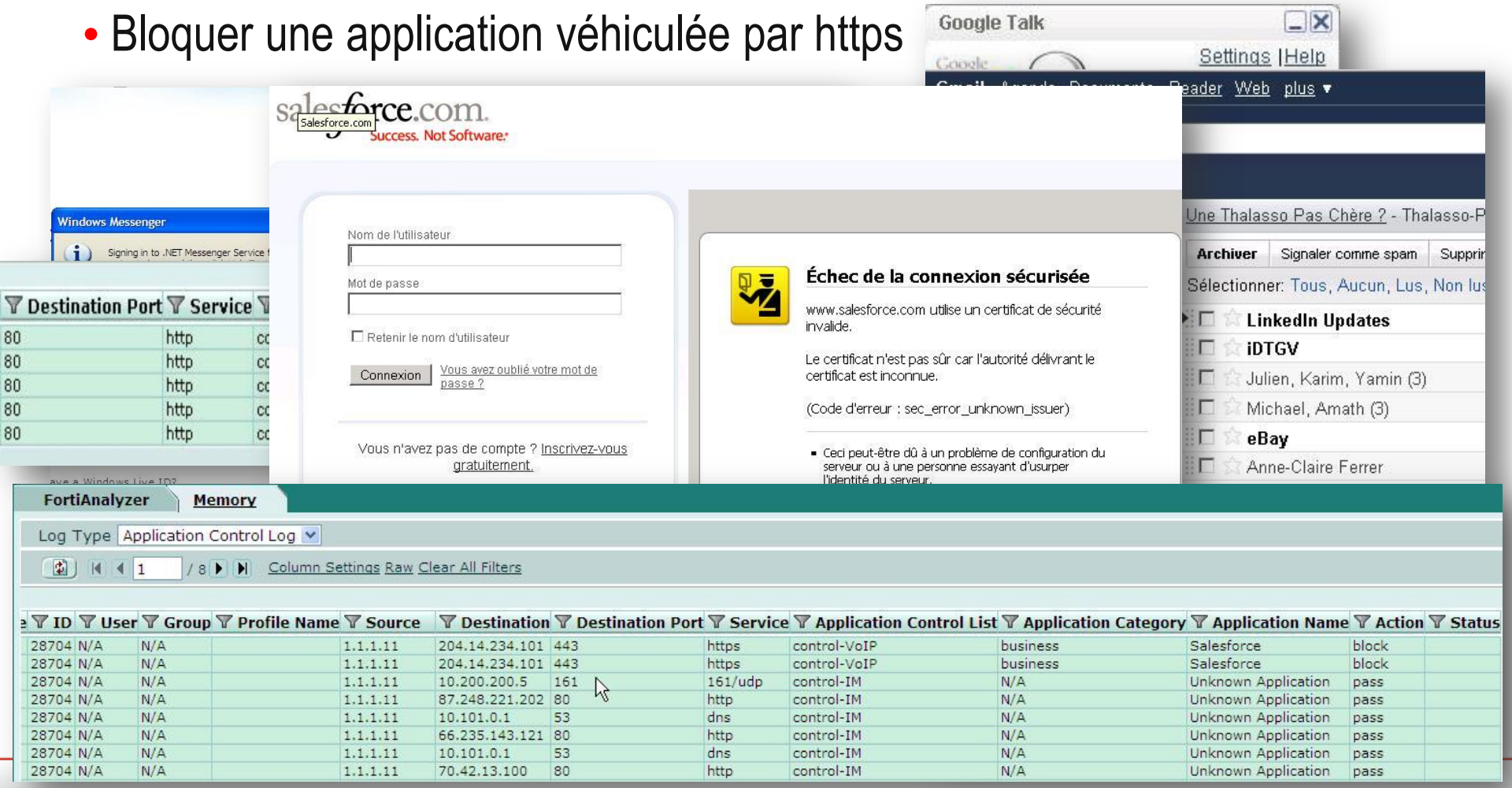
Bloquer SKYPE

#	Time	Source	Destination	Destination Port	Service	Appli	ontrol List	Application Category	Application	Actio
1	09:54:33	66.249.91.18	10.162.1.93	2937	2937/tcp	applic on control		web-mail	Gmail	block
2	09:53:54	66.249.91.18	10.162.1.93	2936	2936/tcp	application control		web-mail	Gmail	block
3	09:51:19	10.162.1.93	217.141.212.231	16467	16467/udp	application control		p2p	Skype	block
4	09:51:13	10.162.1.93	122.218.216.158	6087	6087/udp	application control		p2p	Skype	block
5	09:51:13	10.162.1.93	189.32.154.78	38872	38872/udp	application control		p2p	Skype	block
6	09:51:13	10.162.1.93	76.87.10.90	64620	64620/udp	application control		p2p	Skype	block
7	09:51:13	10.162.1.93	85.219.59.35	55084	55084/udp	application control		p2p	Skype	block
8	09:51:13	10.162.1.93	68.3.121.208	44015	44015/udp	application control		p2p	Skype	block
9	09:51:13	10.162.1.93	96.3.78.211	61678	61678/udp	application control		p2p	Skype	block
10	09:51:13	10.162.1.93	72.208.5.178	18087	18087/udp	application control		p2p	Skype	block
11	09:51:13	10.162.1.93	70.225.38.241	59711	59711/udp	application control		p2p	Skype	block
12	09:51:13	10.162.1.93	24.7.238.219	16585	16585/udp	application control		p2p	Skype	block
13	09:51:13	10.162.1.93	129.59.34.26	52778	52778/udp	application control		p2p	Skype	block
14	09:51:13	10.162.1.93	74.12.67.34	42517	42517/udp	application control		p2p	Skype	block
15	09:51:13	10.162.1.93	64.30.91.128	19041	19041/udp	application control		p2p	Skype	block
16	09:51:13	10.162.1.93	86.14.39.177	33089	33089/udp	application control		p2p	Skype	block
17	09:51:13	10.162.1.93	190.157.193.38	24953	24953/udp	application control		p2p	Skype	block
18	09:51:13	10.162.1.93	89.143.91.144	11277	11277/udp	application control		p2p	Skype	block
19	09:51:11	10.162.1.93	82.242.3.21	443	https	application control		p2p	Skype	block
20	09:50:47	10.162.1.93	82.253.83.223	52593	52593/udp	application control		p2p	Skype	block
21	09:50:38	10.162.1.93	79.133.20.43	31240	31240/udp	application control		p2p	Skype	block
22	09:50:17	10.162.1.93	203.145.202.133	25936	25936/udp	application control		p2p	Skype	block
23	09:50:17	10.162.1.93	210.139.161.146	12050	12050/udp	application control		p2p	Skype	block
24	09:50:17	10.162.1.93	58.159.66.39	28214	28214/udp	application control		p2p	Skype	block
25	09:50:17	10.162.1.93	219.75.236.66	33251	33251/udp	application control		p2p	Skype	block
26	09:50:17	10.162.1.93	89.169.7.140	42269	42269/udp	application control		p2p	Skype	block
27	09:50:17	10.162.1.93	69.87.133.173	42576	42576/udp	application control		p2p	Skype	block
28	09:50:17	10.162.1.93	71.145.161.186	18448	18448/udp	application control		p2p	Skype	block
29	09:50:17	10.162.1.93	75.181.110.35	7477	7477/udp	application control		p2p	Skype	block
30	09:50:17	10.162.1.93	74.130.50.105	13794	13794/udp	application control		p2p	Skype	block
31	09:50:17	10.162.1.93	75.186.97.83	12121	12121/udp	application control		p2p	Skype	block
32	09:50:17	10.162.1.93	209.161.228.6	45674	45674/udp	application control		p2p	Skype	block

Les solutions des parefeux intelligents

en images

- Plus de 1500 applications détectées !
- Bloquer une application véhiculée par https



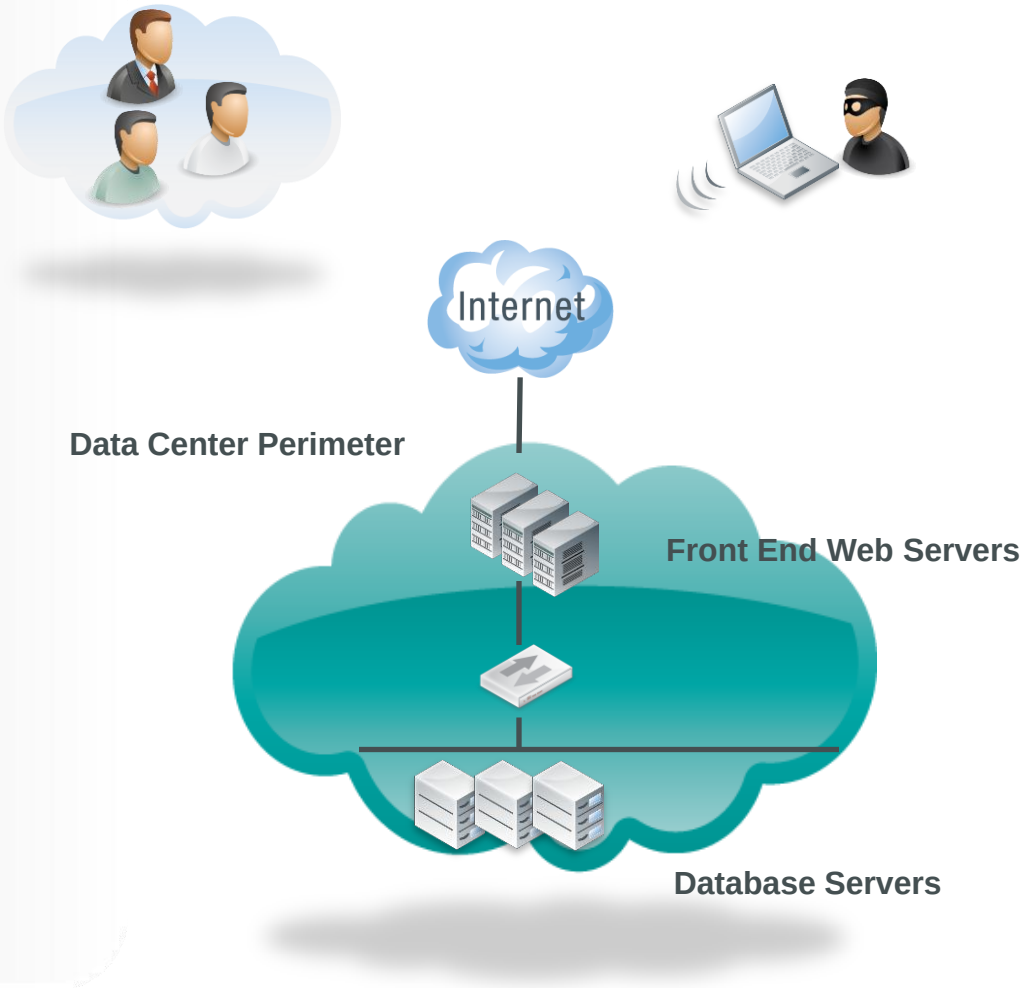
ID	User	Group	Profile Name	Source	Destination	Destination Port	Service	Application Control List	Application Category	Application Name	Action	Status
28704	N/A	N/A		1.1.1.11	204.14.234.101	443	https	control-VoIP	business	Salesforce	block	
28704	N/A	N/A		1.1.1.11	204.14.234.101	443	https	control-VoIP	business	Salesforce	block	
28704	N/A	N/A		1.1.1.11	10.200.200.5	161	161/udp	control-IM	N/A	Unknown Application	pass	
28704	N/A	N/A		1.1.1.11	87.248.221.202	80	http	control-IM	N/A	Unknown Application	pass	
28704	N/A	N/A		1.1.1.11	10.101.0.1	53	dns	control-IM	N/A	Unknown Application	pass	
28704	N/A	N/A		1.1.1.11	66.235.143.121	80	http	control-IM	N/A	Unknown Application	pass	
28704	N/A	N/A		1.1.1.11	10.101.0.1	53	dns	control-IM	N/A	Unknown Application	pass	
28704	N/A	N/A		1.1.1.11	70.42.13.100	80	http	control-IM	N/A	Unknown Application	pass	

Sécurité des Applications WEB

La complexité des applications web

L'enjeu est différent

- La famille des applications web regroupe entre autres les outils générateurs de business ainsi que les applications e-commerce.
- Les applications sont pensées pour délivrer du contenu de manière efficace
- Hélàs ces applications ne sont pas développées avec le soucis de la sécurité:
  - Les applis sont faciles à exploiter
  - Des informations critiques sont exposées
  - Des attaques peuvent pirater des applis web critiques



Pourquoi des parefeux WEB applicatifs (WAF) ?

- Les Applications sont plus critiques que jamais
- Mais…
  - 49% des applications web sont sujettes aux attaques par des robots
  - 80%-96% sont vulnérables aux attaques ciblées et manuelles
  - 99% des applis web ne respectent pas les normes PCI DSS
  - La plupart des techniques d'exploitations de vulnérabilités ne sont pas adressées par les parefeux intelligents:
    - Cross-site scripting
    - SQL injection
    - Information Leakage
- Implications :
  - Pertes financières
  - Poursuites judiciaires sur le chef d'établissement
  - Impact sur l'image de la compagnie

SECURITY dark READING
Protect The Business Enable Access

Breach Exposes Data Of 3.5 Million Teachers And Employees In Texas

WIRED **Citi Credit Card Data Breached for 200,000 Customers**

Visa, Amex cuts ties with CardSystems
Payment processor left 40 million accounts vulnerable to hackers

MSNBC

Sony PlayStation suffers massive data breach

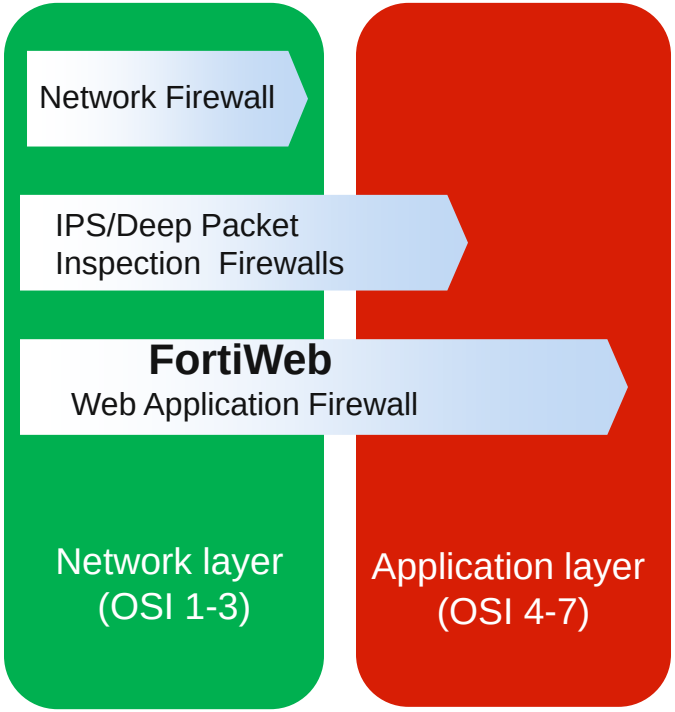
REUTERS

*Source – Web Application Security Consortium (WASC)

J'ai déjà un parefeu et un IPS, pourquoi ai-je besoin d'un WAF?

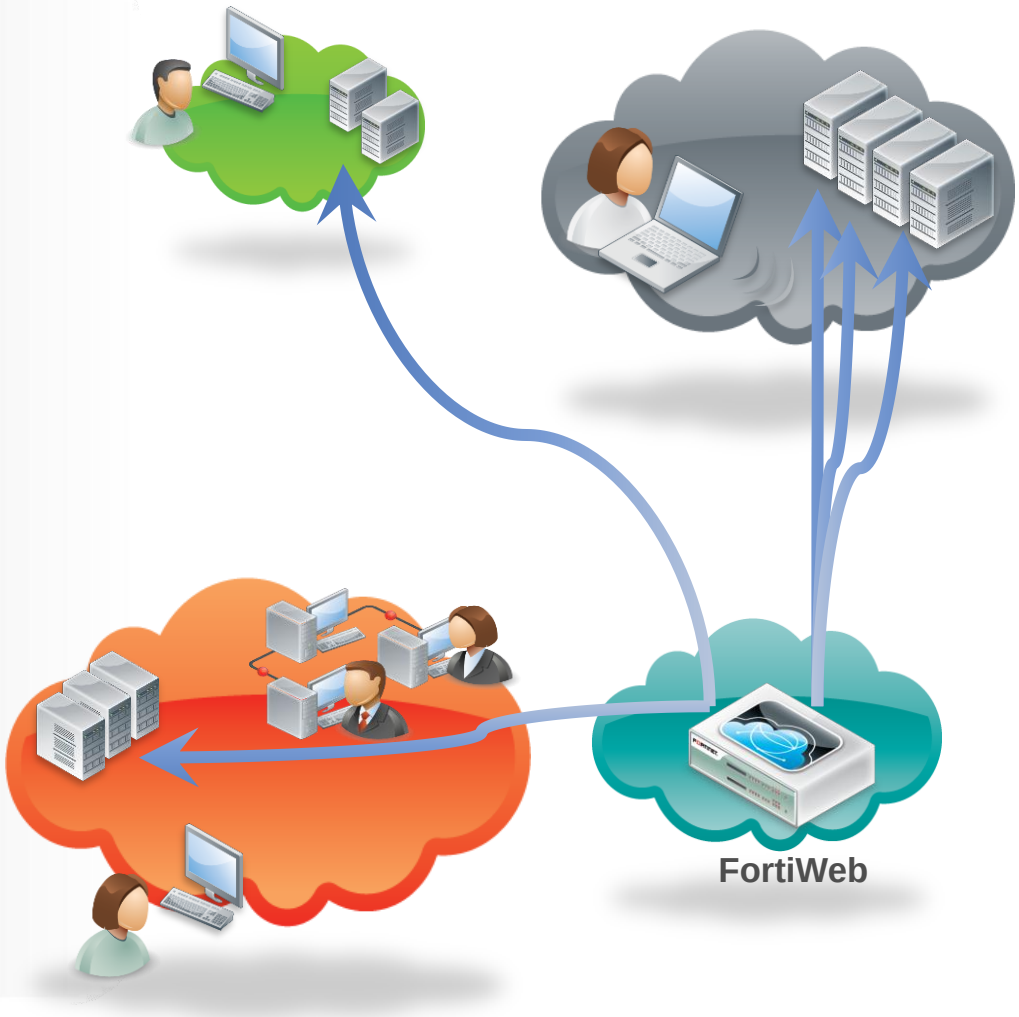
- Les parefeux détectent les attaques réseaux et les protocoles
  - Inspection de l'IP, du port et du protocole
- Les IPS détectent les signatures connues uniquement
  - Les évasions de signatures sont possibles
  - Aucune protection du trafic chiffré SSL
  - Aucune compréhension du protocole HTTP (headers, paramètres, etc)
  - Aucune conscience de l'application
  - Aucune conscience de l'utilisateur

Seuls les WAF peuvent détecter et bloquer des attaques spécifiques au web!

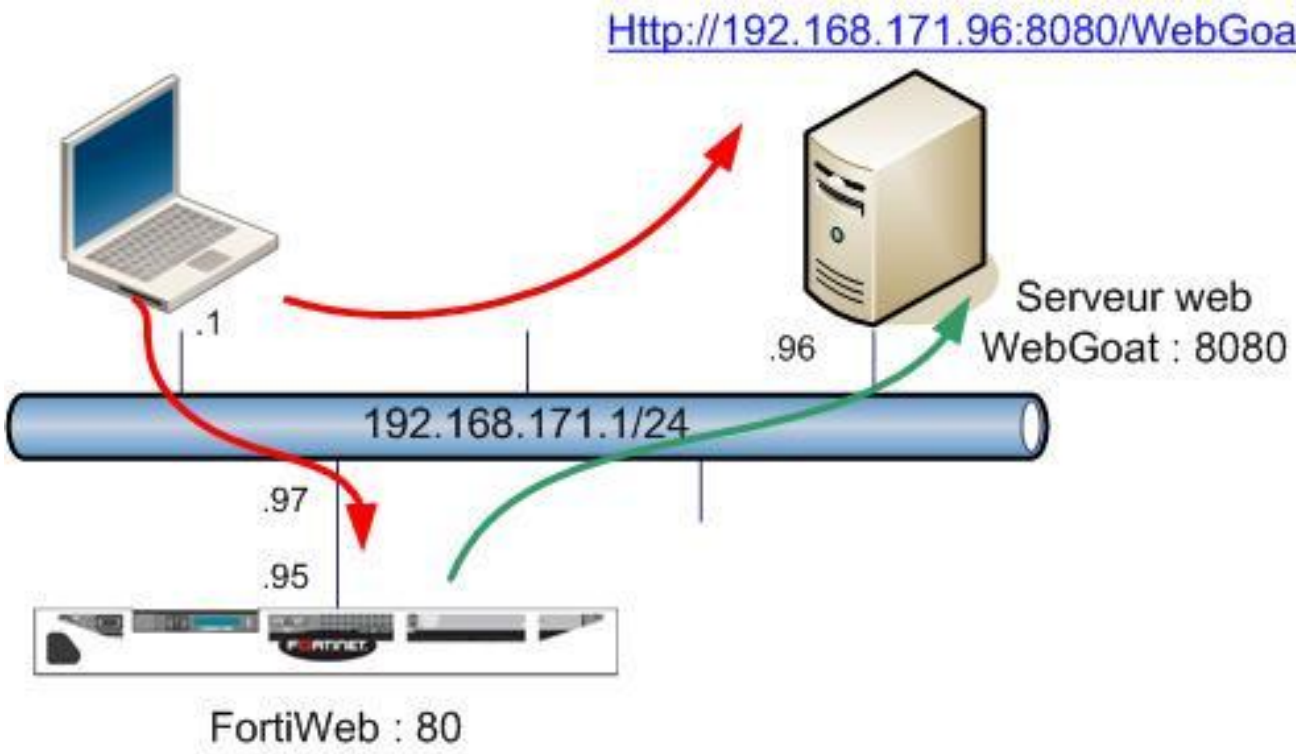


Mise en place du WAF : Web Application Scanner

- Scanne facilement les applications web pour déterminer les vulnérabilités
  - Vulnérabilités Classiques
  - SQL Injection
  - Cross Site Scripting
  - Source code disclosure
  - OS Commanding
- Modes Enhanced/Basic
- Options d'Authentification
- DEMO



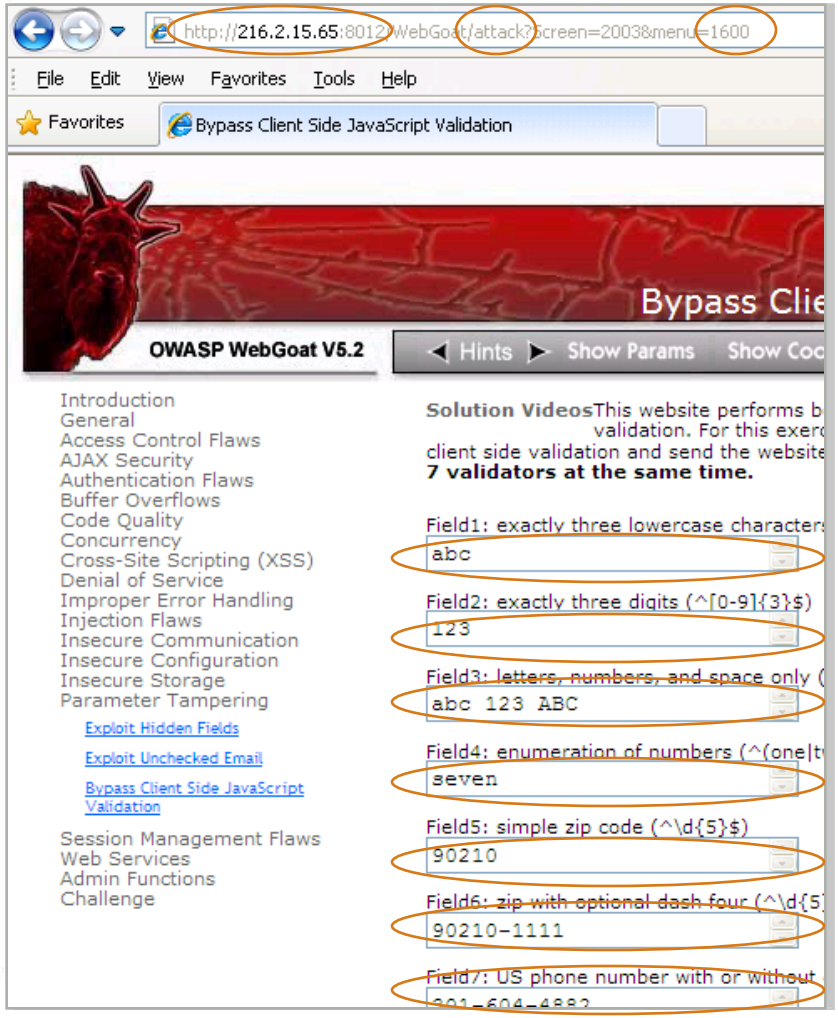
Demo Scanner



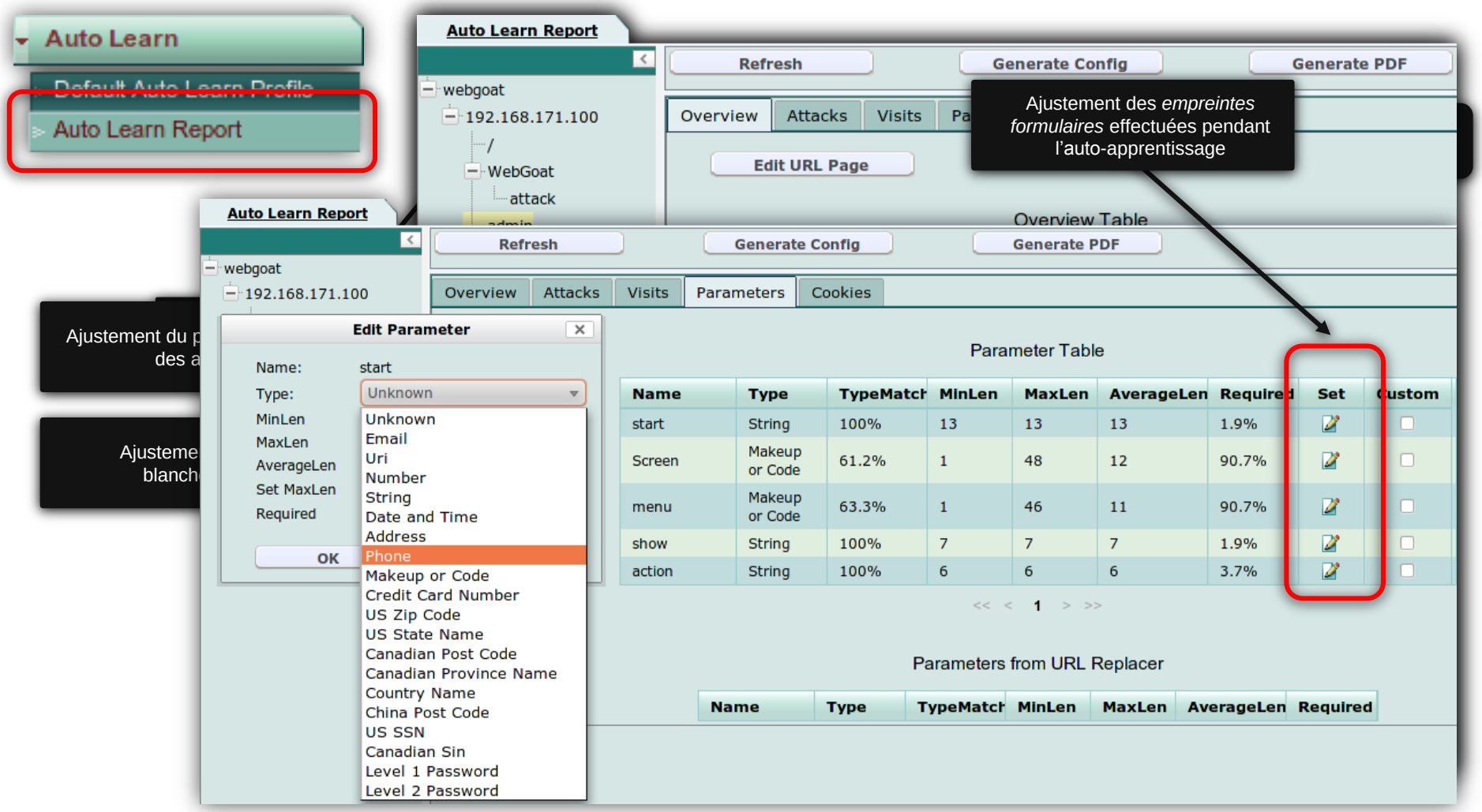
Problématiques autour de la sécurité WAF

- Les Admins doivent manuellement définir :
  - Chaque URL, dossier, parametre, longueur de champs et type
  - Expressions régulières pour le contenu dynamique, JavaScript, XML, etc
- Constamment mettre à jour cette liste
- Fort taux de falses positives – Le trafic qui ne correspond pas à la liste est rejeté

=> auto-apprentissage nécessaire !

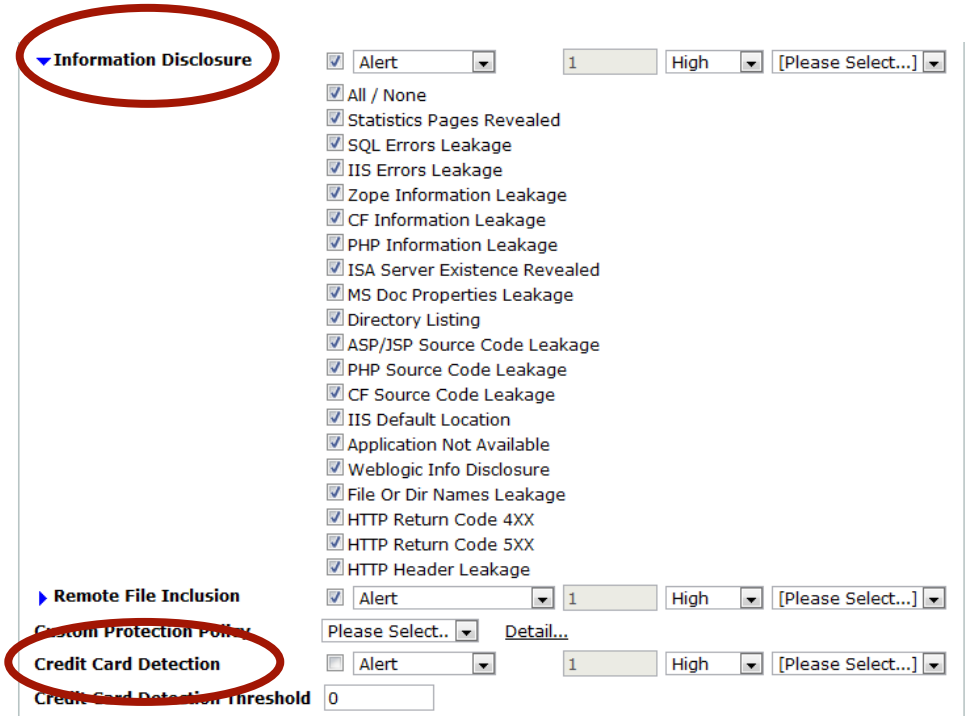


Auto-apprentissage efficace



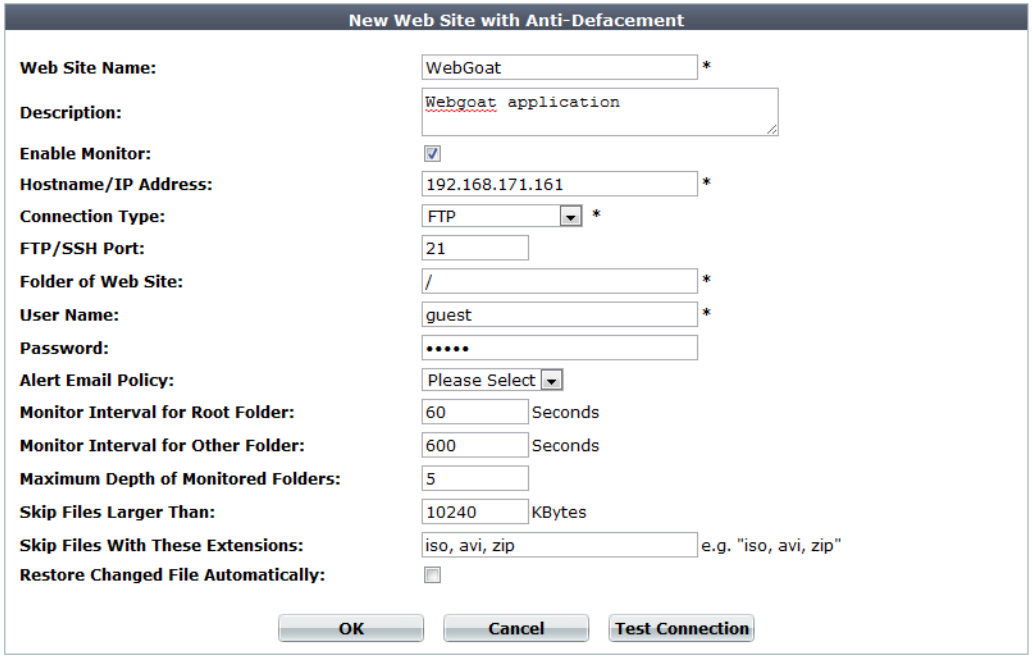
Les techniques de protection WAF
Data Leak Prevention

- Le trafic de sortie est vérifié protégeant contre:
  - Fuite d'Information
  - Vol ou détournement de Carte de Crédit



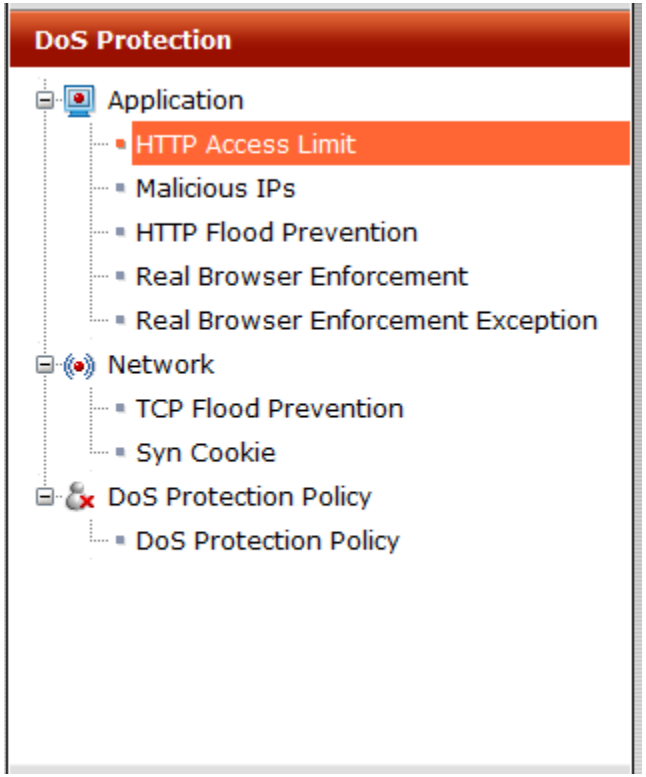
Les techniques de protection WAF
Web Site anti-defacement

- Surveille les fichiers sources de l'application régulièrement
- Au moment de la modification, le WAF génère :
  - Une alerte
  - Une restauration automatique



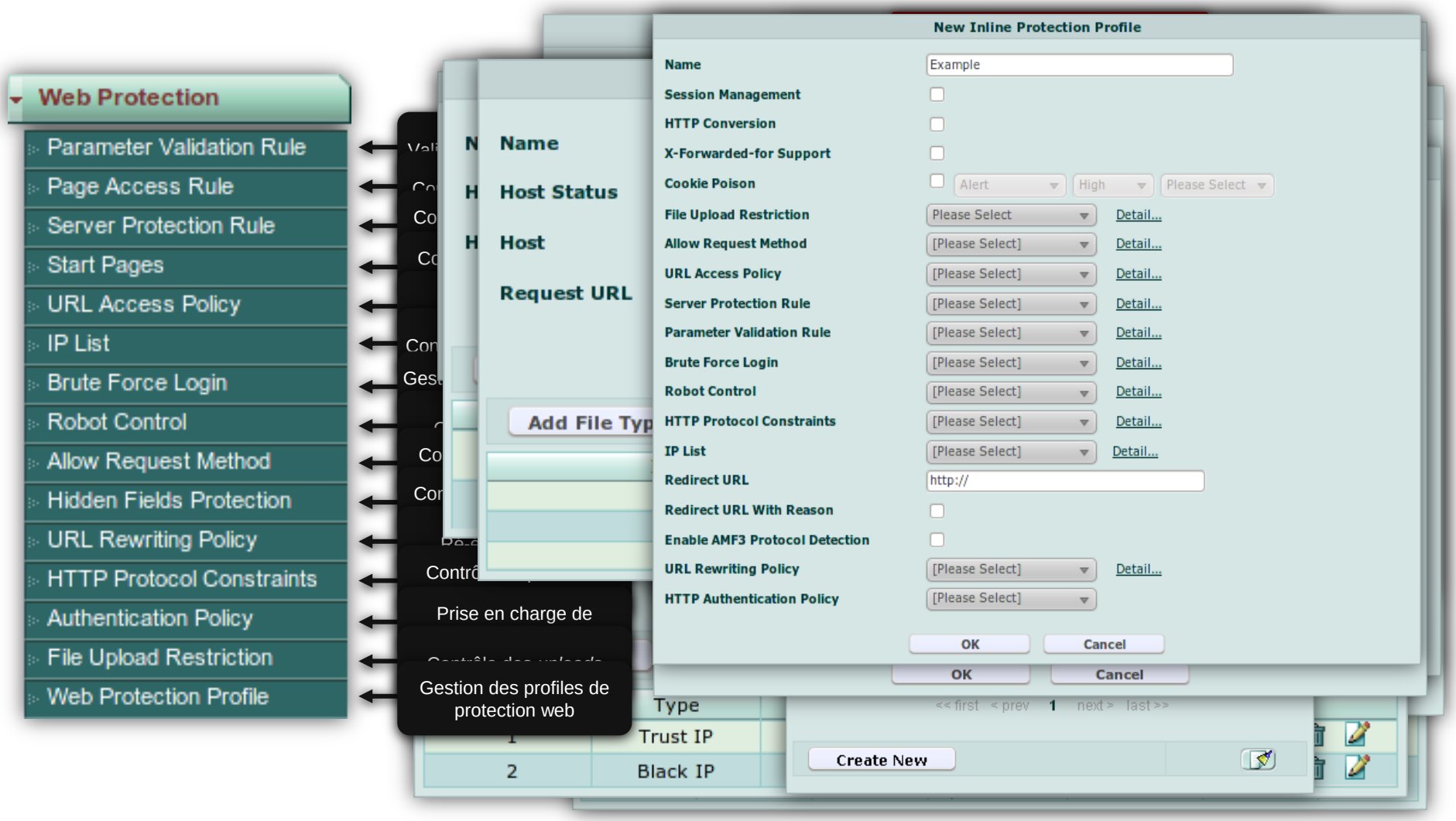
Les techniques de protection WAF
DOS Protection

- Analyse les requêtes provenant de différents utilisateurs selon différentes caratéristiques telles que l'IP ou les cookies
- Couche Applicative
  - HTTP Access Limit - *Limits the amount of HTTP requests per second from a certain IP*
  - Malicious IPs - *Limits the number of TCP connections with the same session cookie*
  - HTTP Flood Prevention - *Limits the number of HTTP requests per second with the same session cookie*
  - Real Browser Enforcement - *Sets the number of HTTP requests per TCP connection, per second, to a specific URL before FortiWeb issues a script to the client to validate whether this is a real browser or an automated tool*
- Couche réseau
  - TCP Flood Prevention - *Limits the number of TCP connections from the same source IP address*
  - SYN Cookie – Protège contre les attaques SYN flood

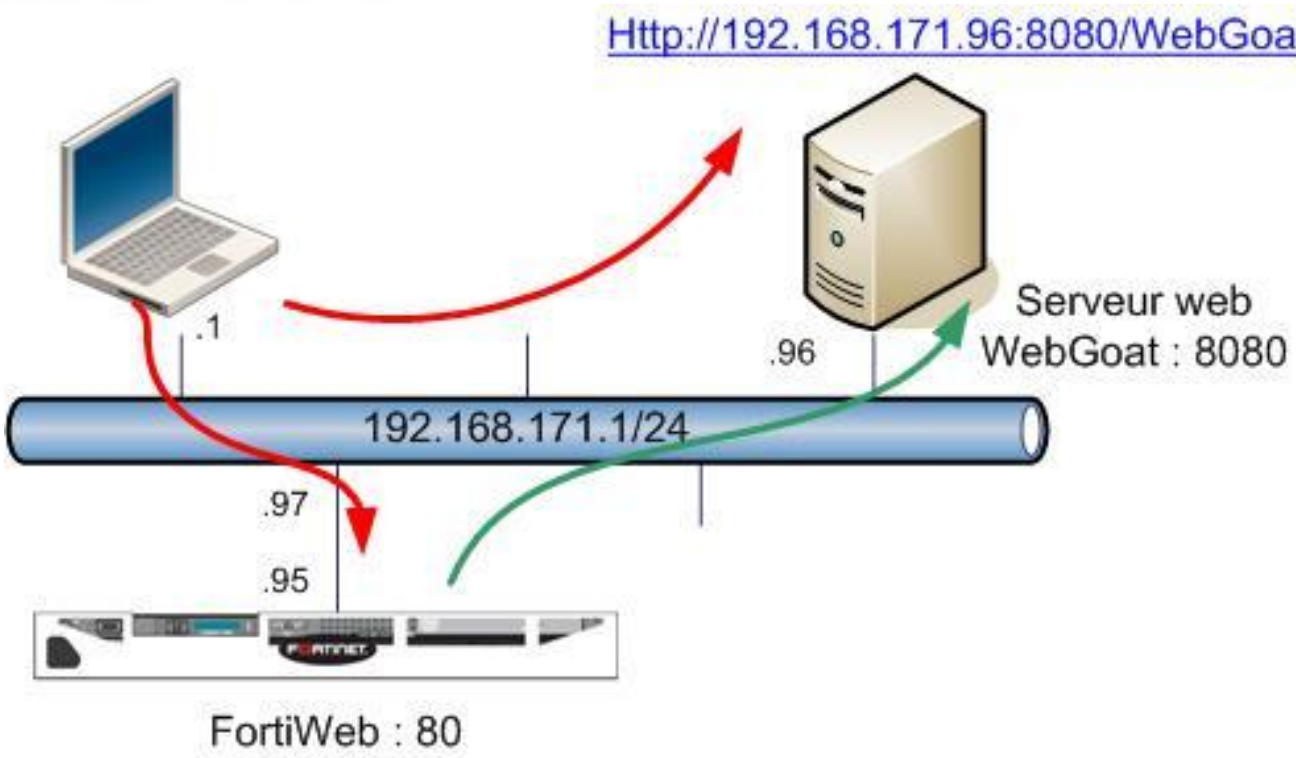


Les techniques de protection WAF

Mécanismes de la sécurité WEB



Demo XSS


Http://192.168.171.96:8080/WebGoat/attack
.1
.96
Serveur web
WebGoat : 8080
192.168.171.1/24
.97
.95
FortiWeb : 80

Merci.