

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

■ Vidéo ■ Audio ■ Jeux et réseaux sociaux

SITES DE SERVICES VISITES SELON LES LIEUX

proxy, P2P, tunnel

Domicile (83%) Lieu de travail Lieu d'études Chez des proches (19%) Lieux publics

- Moteurs de recherche
- annuaire
- Sites
- Com
- Petit
- l'em
- Petites annonces immobilières
- enchères
- Jeux en ligne
- Téléchargement (MP Divx ...)
- Petites annonces automobiles
- Sites de rencontres
- Hébergement de pages personnelles et communautés

25%

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 -

Source IPSOS 2011

nelles
BP
sent les
nde de
(Jackson)
enacée
assante

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 ...





Sécurité Appllicative multi-protocoles

Les solutions des parefeux intelligents

en images



System	Eatime	web	high	high
Router	Ebay	web	high	low

New Application Entry

Category: -- All Categories --

Application: Facebook

Action: Pass

Traffic Shaping: guarantee-100kbps

Reverse Direction Traffic Shaping: guarantee-100kbps

Options

Session TTL

Enable Logging

Enable Packet Log

OK Cancel

- System
- Router
- Firewall
- UTM**
 - AntiVirus
 - Profile
 - File Filter
 - Quarantine
 - Virus Database
 - Intrusion Protection
 - Web Filter
 - Email Filter
 - Data Leak Prevention
 - Application Control
 - Application Control List**
 - Application List
 - VoIP

Les solutions des parefeux intelligents en images

Memory

Log Type Application Control Log

1 / 2 Column Settings Raw Clear All Filters

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

Quelque soit le port

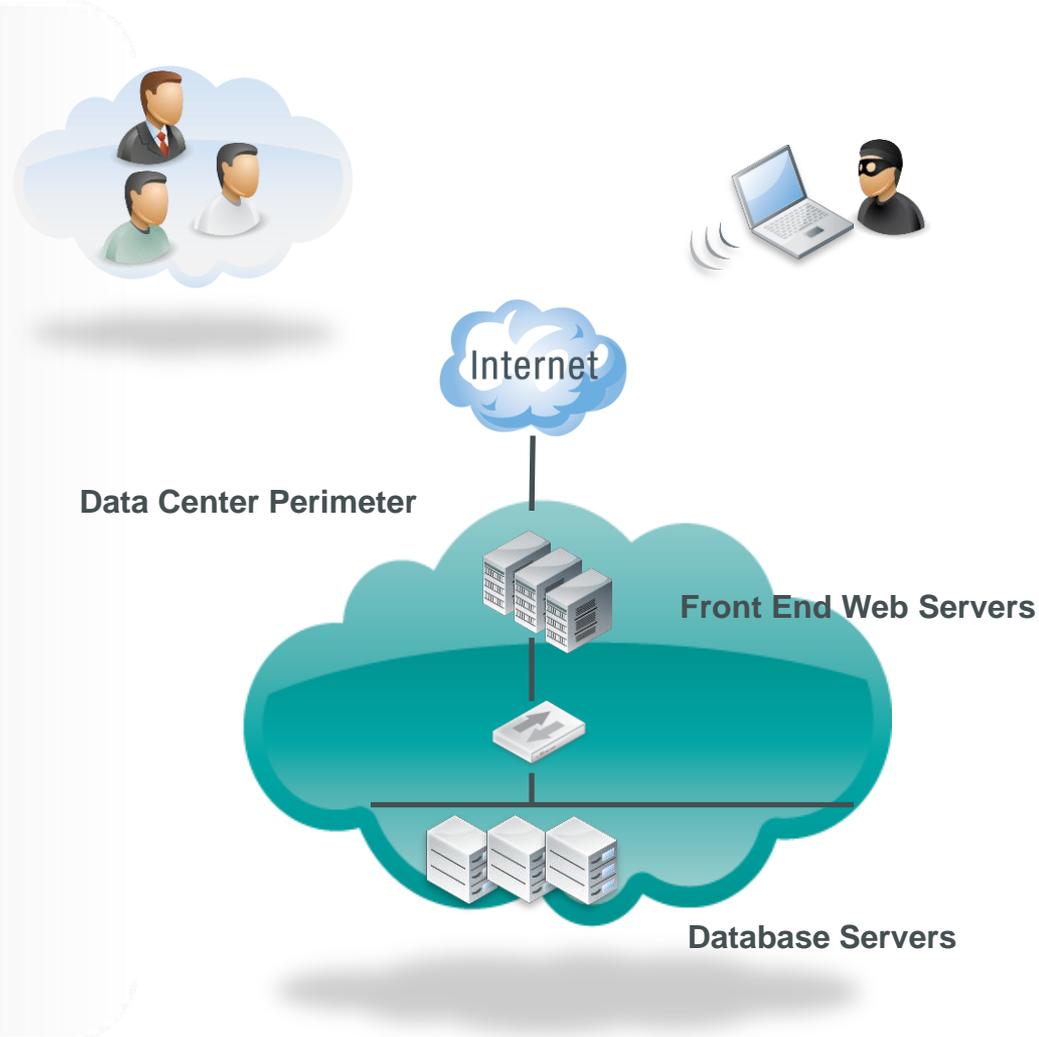
Bloquer SKYPE

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
- Hélas 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



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



Sony PlayStation suffers massive data breach

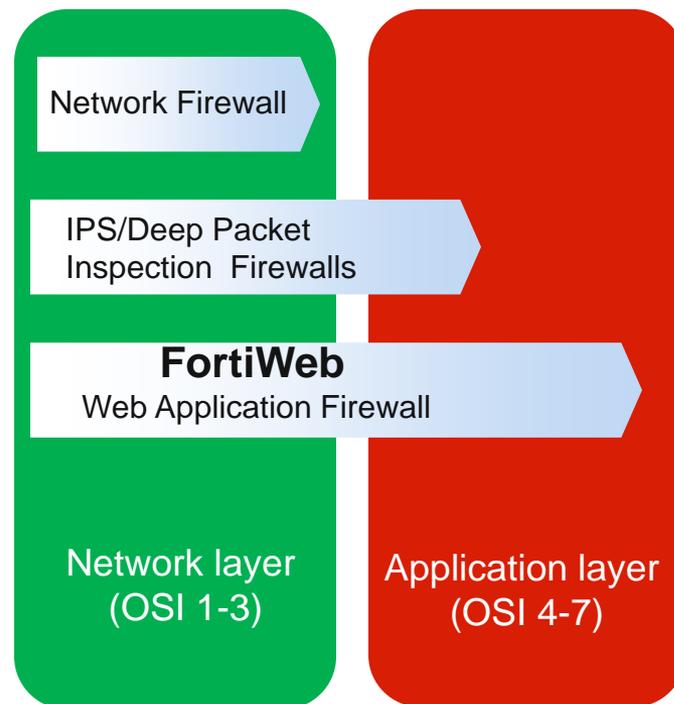


*Source – Web Application Security Consortium (WASC)

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

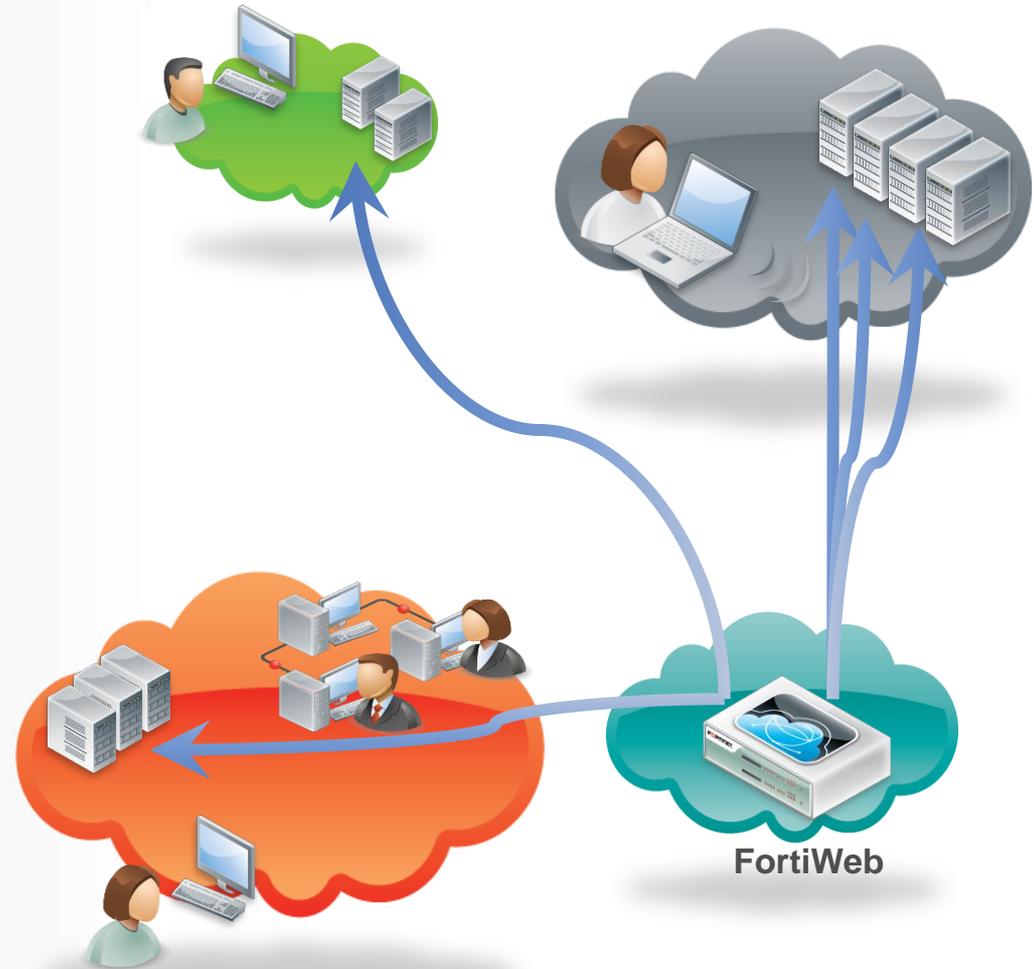
Seuls les WAF peuvent détecter et bloquer des attaques spécifiques au web!



Mise en place du WAF : Web Application Scanner

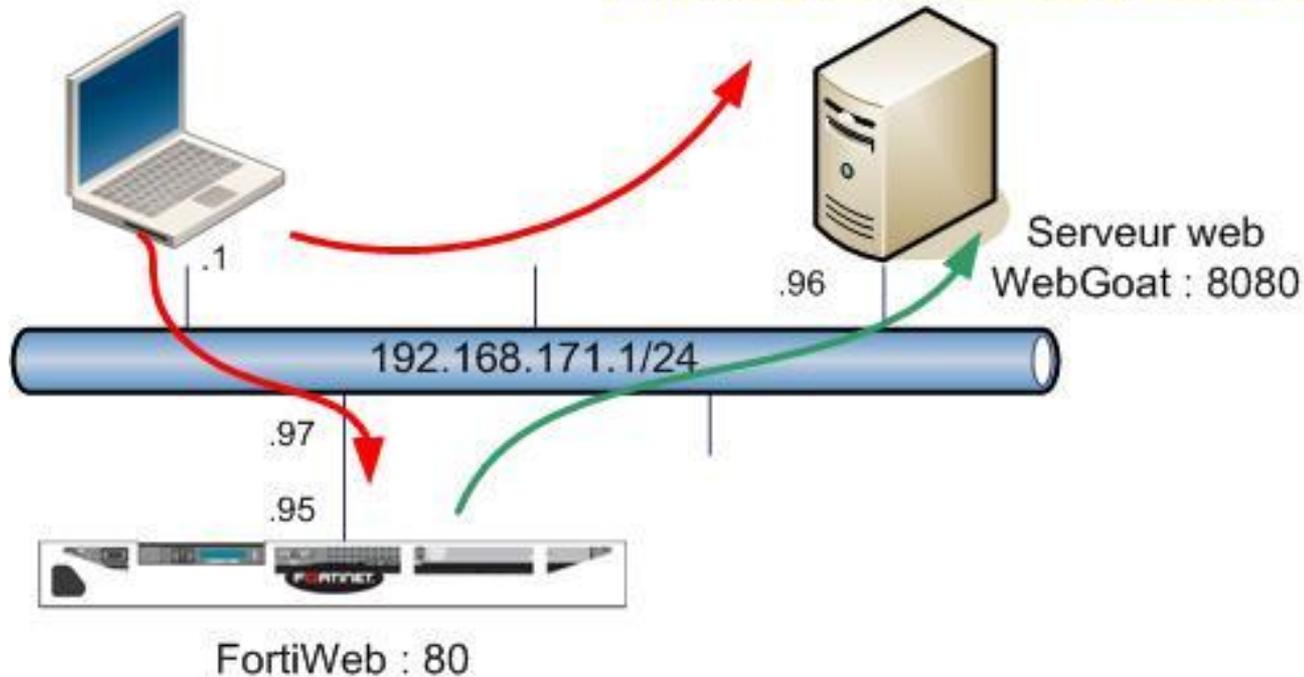


- Scanne facilement les applications web pour déterminer les vulnérabilités
 - Vulnérabilités Classiques
 - SQL Injection
 - Cross Site Scripting
 - Source code disclosure
 - OS Commanding
- Modes Enhanced/Basic
- Options d'Authentification
- **DEMO**



Demo Scanner

[Http://192.168.171.96:8080/WebGoat/attack](http://192.168.171.96:8080/WebGoat/attack)



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 fausses positives – Le trafic qui ne correspond pas à la liste est rejeté
- => auto-apprentissage nécessaire !

http://216.2.15.65:8012/WebGoat/attack?screen=2003&menu=1600

File Edit View Favorites Tools Help

Favorites Bypass Client Side JavaScript Validation

OWASP WebGoat V5.2 < Hints > Show Params Show Cookies

Introduction
General
Access Control Flaws
AJAX Security
Authentication Flaws
Buffer Overflows
Code Quality
Concurrency
Cross-Site Scripting (XSS)
Denial of Service
Improper Error Handling
Injection Flaws
Insecure Communication
Insecure Configuration
Insecure Storage
Parameter Tampering

[Exploit Hidden Fields](#)
[Exploit Unchecked Email](#)
[Bypass Client Side JavaScript Validation](#)

Session Management Flaws
Web Services
Admin Functions
Challenge

Solution Videos This website performs bypass validation. For this exercise, you will need to bypass client side validation and send the website **7 validators at the same time.**

Field1: exactly three lowercase characters
abc

Field2: exactly three digits (^[0-9]{3}\$)
123

Field3: letters, numbers, and space only (^[a-zA-Z0-9]+\$)
abc 123 ABC

Field4: enumeration of numbers (^(one|two|three|four|five|six|seven|eight|nine|ten)\$)
seven

Field5: simple zip code (^\\d{5}\$)
90210

Field6: zip with optional dash four (^\\d{5}(-\\d{4})?\$)
90210-1111

Field7: US phone number with or without extension (^\\d{3}-\\d{3}-\\d{4}(-\\d{4})?\$)
901-604-4882

Auto-apprentissage efficace

Auto Learn Report

webgoat

- 192.168.171.100
 - WebGoat
 - attack
 - admin

Refresh Generate Config Generate PDF

Overview Attacks Visits Pa

Edit URL Page

Overview Table

Refresh Generate Config Generate PDF

Overview Attacks Visits Parameters Cookies

Edit Parameter

Name: start

Type: Unknown

MinLen: Unknown

MaxLen: Email

AverageLen: Uri

Set MaxLen: Number

Required: String

Address: Date and Time

Phone

Makeup or Code

Credit Card Number

US Zip Code

US State Name

Canadian Post Code

Canadian Province Name

Country Name

China Post Code

US SSN

Canadian Sin

Level 1 Password

Level 2 Password

OK

Parameter Table

Name	Type	TypeMatch	MinLen	MaxLen	AverageLen	Required	Set	Custom
start	String	100%	13	13	13	1.9%		<input type="checkbox"/>
Screen	Makeup or Code	61.2%	1	48	12	90.7%		<input type="checkbox"/>
menu	Makeup or Code	63.3%	1	46	11	90.7%		<input type="checkbox"/>
show	String	100%	7	7	7	1.9%		<input type="checkbox"/>
action	String	100%	6	6	6	3.7%		<input type="checkbox"/>

<< < 1 > >>

Parameters from URL Replacer

Name	Type	TypeMatch	MinLen	MaxLen	AverageLen	Required
------	------	-----------	--------	--------	------------	----------

Ajustement des empreintes formulaires effectuées pendant l'auto-apprentissage

Ajustement du p des a

Ajusteme blanch

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

Information Disclosure

Alert High [Please Select...]

All / None

Statistics Pages Revealed

SQL Errors Leakage

IIS Errors Leakage

Zope Information Leakage

CF Information Leakage

PHP Information Leakage

ISA Server Existence Revealed

MS Doc Properties Leakage

Directory Listing

ASP/JSP Source Code Leakage

PHP Source Code Leakage

CF Source Code Leakage

IIS Default Location

Application Not Available

Weblogic Info Disclosure

File Or Dir Names Leakage

HTTP Return Code 4XX

HTTP Return Code 5XX

HTTP Header Leakage

Remote File Inclusion

Alert High [Please Select...]

Please Select.. [Detail...](#)

Credit Card Detection

Alert High [Please Select...]

Credit Card Detection Threshold

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

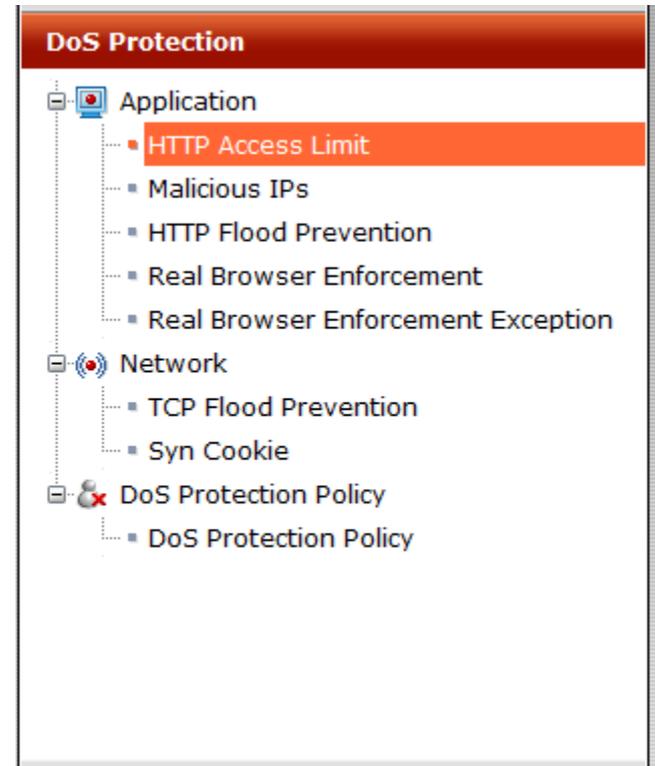
New Web Site with Anti-Defacement

Web Site Name:	<input type="text" value="WebGoat"/> *
Description:	<input type="text" value="Webgoat application"/>
Enable Monitor:	<input checked="" type="checkbox"/>
Hostname/IP Address:	<input type="text" value="192.168.171.161"/> *
Connection Type:	<input type="text" value="FTP"/> *
FTP/SSH Port:	<input type="text" value="21"/>
Folder of Web Site:	<input type="text" value="/"/> *
User Name:	<input type="text" value="guest"/> *
Password:	<input type="password" value="*****"/>
Alert Email Policy:	<input type="text" value="Please Select"/>
Monitor Interval for Root Folder:	<input type="text" value="60"/> Seconds
Monitor Interval for Other Folder:	<input type="text" value="600"/> Seconds
Maximum Depth of Monitored Folders:	<input type="text" value="5"/>
Skip Files Larger Than:	<input type="text" value="10240"/> KBytes
Skip Files With These Extensions:	<input type="text" value="iso, avi, zip"/> e.g. "iso, avi, zip"
Restore Changed File Automatically:	<input type="checkbox"/>

Les techniques de protection WAF

DOS Protection

- Analyse les requêtes provenant de différents utilisateurs selon différentes caractéristiques 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

The image displays the Fortinet WAF configuration interface. On the left, a sidebar lists various protection techniques under the 'Web Protection' category:

- Parameter Validation Rule
- Page Access Rule
- Server Protection Rule
- Start Pages
- URL Access Policy
- IP List
- Brute Force Login
- Robot Control
- Allow Request Method
- Hidden Fields Protection
- URL Rewriting Policy
- HTTP Protocol Constraints
- Authentication Policy
- File Upload Restriction
- Web Protection Profile

On the right, the 'New Inline Protection Profile' dialog box is open, showing configuration options for a new profile named 'Example':

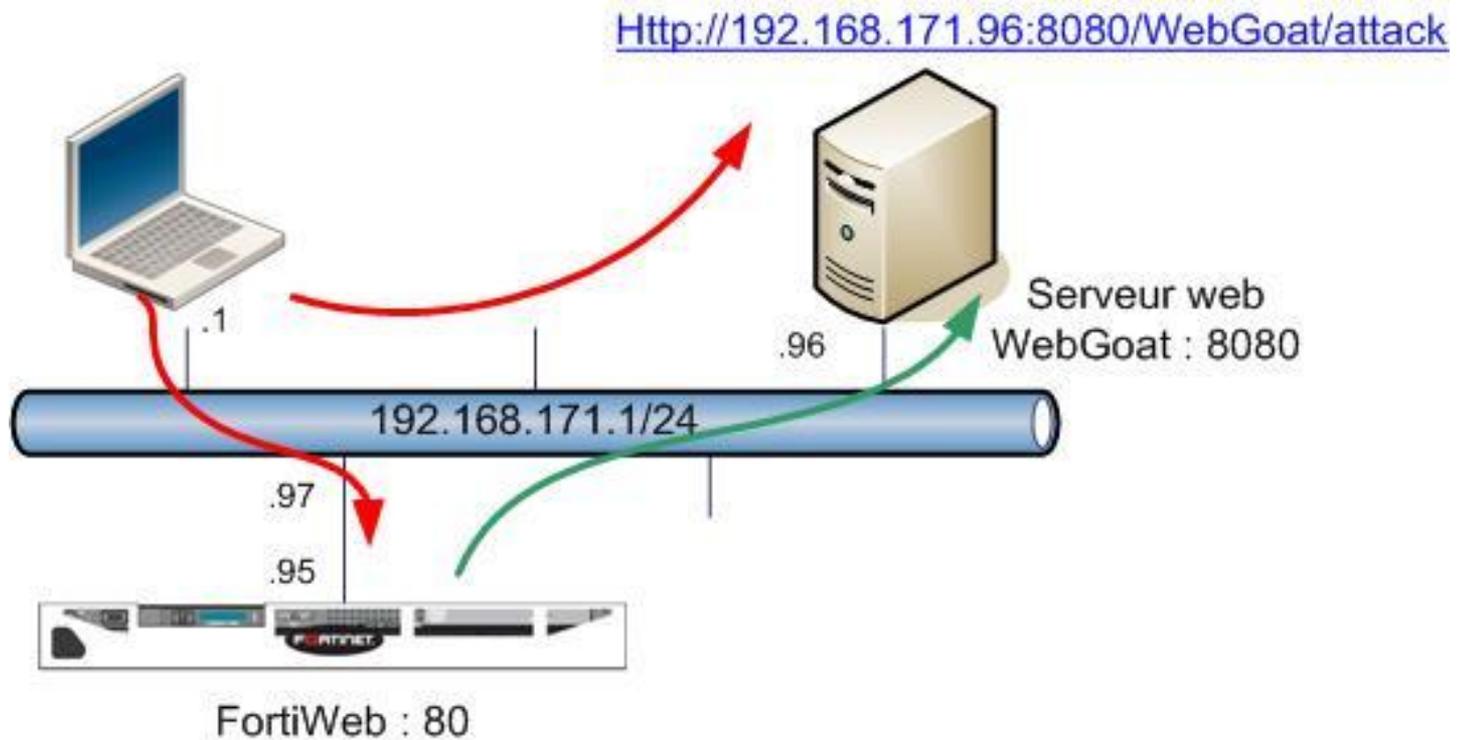
- Name:** Example
- Session Management:**
- HTTP Conversion:**
- X-Forwarded-for Support:**
- Cookie Poison:** Alert | High | Please Select
- File Upload Restriction:** Please Select | Detail...
- Allow Request Method:** [Please Select] | Detail...
- URL Access Policy:** [Please Select] | Detail...
- Server Protection Rule:** [Please Select] | Detail...
- Parameter Validation Rule:** [Please Select] | Detail...
- Brute Force Login:** [Please Select] | Detail...
- Robot Control:** [Please Select] | Detail...
- HTTP Protocol Constraints:** [Please Select] | Detail...
- IP List:** [Please Select] | Detail...
- Redirect URL:** http://
- Redirect URL With Reason:**
- Enable AMF3 Protocol Detection:**
- URL Rewriting Policy:** [Please Select] | Detail...
- HTTP Authentication Policy:** [Please Select]

At the bottom of the dialog, there are 'OK' and 'Cancel' buttons. Below the dialog, a table shows the profile configuration:

Type	Trust IP
1	Trust IP
2	Black IP

A 'Create New' button is visible at the bottom right of the interface.

Demo XSS





Merci.