

WordPress

- [Procédure ajout site Wordpress](#)

Procédure ajout site Wordpress

Procédure d'ajout de site sur Fortiweb avec profil Wordpress à partir d'un nouveau nom de domaine

Suite à la création d'un nouveau nom de domaine (ici vincennesestivalclub.com), nous avons associé les liens à une IP publique (159.180.242.43)

 chateaudelumieres.com	<input type="checkbox"/>	Domaine	TTL	Type	Cible
 mairie-vincennes.fr	<input type="checkbox"/>	vincennesestivalclub.com.	0	NS	dns100.ovh.net.
 monvincennes.fr	<input type="checkbox"/>	vincennesestivalclub.com.	0	NS	ns100.ovh.net.
 ville-vincennes.fr	<input type="checkbox"/>	vincennesestivalclub.com.	0	A	159.180.242.43
 vincennes-info.com	<input type="checkbox"/>	www.vincennesestivalclub.com.	0	A	159.180.242.43
 vincennes-info.net	<input type="checkbox"/>	ftp.vincennesestivalclub.com.	0	CNAME	vincennesestivalclub.com.
 vincennes-tourisme.fr	<input type="checkbox"/>	vincennesestivalclub.com.	0	SPF	v=spf1 include:mx.ovh.com -all
 vincennes.fr	<input type="checkbox"/>	vincennesestivalclub.com.	0	TXT	"1 www.vincennesestivalclub.com"
 vincenneschateaudelumieres.com	<input type="checkbox"/>	www.vincennesestivalclub.com.	0	TXT	"3 welcome"
 vincennesestivalclub.com					

Cette IP publique est redirigée vers un Virtual Server (VS qui a été configuré sur le fortiweb) via une VIP sur le Firewall.


 VIP 159.180.242.43:443	 Internet_Celeste (port1)	159.180.242.43 (TCP: 443)	192.168.201.236 (TCP: 443)
---	--	---------------------------	----------------------------

Une règle de FW a été créée afin de rediriger la VIP vers le fortiweb :

VincennesEstivalClub vers SP37 (1242)	 all	 VIP 159.180.242.43:443	 always	 HTTPS
---------------------------------------	---	--	--	---

Configuration sur le Fortiweb :

Création d'un nouveau Virtual Server :

 Security Fabric	>	1	VS_192.168.201.239
 User	>	2	VS_192.168.201.238
 Policy	>	3	VS_192.168.201.237
 Server Objects	▼	4	VS_192.168.201.236
Server	▼		
Virtual Server	☆		

Aller dans « Server Objects » puis « Server » et « Virtual Server »

Create New et mettre un nom avec la typologie VS_adresse ip dans la DMZ web

Edit Virtual Server

Name VS_192.168.201.236

OK

Cancel

+ Create New Edit Delete

ID	Use Interface IP	Interface/Virtual IP
1	Disable	vip-VS_192.168.201.236(192.168.201.236/32,::/0)

Cliquer sur « Create New » puis sur « Create »

New Virtual Server item

ID auto

Use Interface IP

Virtual IP

Status

Search

+ Create

vip-VS_192.168.201.237

vip-VS_192.168.201.238

vip-VS_192.168.201.239

vip-VS_192.168.201.236

Renseigner le champ Name de cette manière vip-VS_adresse ip en DMZ web puis l'IP V4 et enfin l'interface port 1

Create Virtual IP

Name

IPv4 Address

IPv6 Address

Interface

- port1
- port2
- port3
- port4
- port5
- port6
- port7
- port8
- port9
- port10

Aller ensuite dans le Server Pool et ajouter le site ainsi que la redirection vers le serveur interne de cette manière :

Dashboard > Network > System > Security Fabric > User > Policy > Server Objects > Server > Server Pool

Edit Server Pool

Name

Protocol HTTP

Type

Single Server/Server Balance

Comments

OK Cancel

+ Create New Edit Delete

ID	IP/Domain/External Connector	Status	Port	HTTP/2	SSL
1	192.168.201.37	Enable	8084	Disable	Disable

Edit Server Pool Rule

ID **1**

Status Enable Disable Maintenance

Server Type IP Domain External connector

IP

Port

Connection Limit ?

Proxy Protocol

HTTP/2

SSL ?

[Show advanced settings](#)

Créer une règle dans le HTTP Content Routing

Edit HTTP Content Routing Policy

Name

Server Pool

Comments

Match Sequence (1)

OK Cancel

+ Create New Edit Delete Insert Move

ID	Match Object	Relationship with Previous Rule	Reverse	Match Condition
1	HTTP Host	AND	Disable	HTTP Host: Match prefix: www.vincennesestivalclub.com

Edit HTTP Content Routing

ID **1**

Match Object
Match against the Host field in the HTTP Request Header.

HTTP Host

The match object begins with the match string.

Reverse

Relationship with Previous Rule AND OR
Choose the relationship with the previous rule. The AND rule sequence.

Créer une Policy dans « Policy » puis « Server Policy »

Dashboard	>	+ Create New Edit Delete Search Q							
Network	>								
System	>								
Security Fabric	>								
User	>								
Policy	>								
Server Policy	☆	#	Policy Name	Virtual Server	VIP	Port	Protocol	Deployment Mode	Web Protection Profile
		1	VS_HTTP	VS_192.168.201.238	192.168.201.238/32	port1	HTTP	HTTP Content Routing	Profile_Vincennes
		2	VS_HTTPS_PROD	VS_192.168.201.239	192.168.201.239/32	port1	HTTP,HTTPS	HTTP Content Routing	Profile_Vincennes
		3	VS_HTTPS_PREPROD	VS_192.168.201.237	192.168.201.237/32	port1	HTTP,HTTPS	HTTP Content Routing	Profile_Vincennes
		4	VS_estival_club	VS_192.168.201.236	192.168.201.236/32	port1	HTTP,HTTPS	HTTP Content Routing	Profile_Vincennes+Wordpress

Edit Policy

Name

Network Configuration

Deployment Mode

Virtual Server

HTTP Content Routing ⓘ

+ Create New Edit Delete Move Search Q				
#	HTTP Content Routing Policy	Server Pool	Default	Inherit Web Protection Profile
1	ESTIVAL	https_vincennesestivalclub.com	No	Yes

Match Once ⓘ

Protected Hostnames ⓘ

Client Real IP ⓘ

HTTP Service

HTTPS Service

HTTP/3 Service

HTTP/2

Certificate Type

Let's Encrypt

Certificate Intermediate Group

[Advanced SSL settings](#)

Redirect HTTP to HTTPS ⓘ

Redirect Naked Domain ⓘ

Application Delivery

Proxy Protocol

Retry On ⓘ

Scripting

Scripting

Security Configuration

Monitor Mode 

Syn Cookie

Web Protection Profile 

Allow List  


Replacement Message 

URL Case Sensitivity

Log Config

Enable Traffic Log

One Click GSLB Server

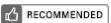
One Click GSLB Server 

+ Machine Learning

Tags

Comments  0/999 (bytes)

Il faut au préalable créer une « Web protection Profile » de cette manière :

	#	Name	Client Management	Signatures
	Predefined 10			
	1	Inline Standard Protection 	Enable	Standard Protection
	2	Inline Extended Protection	Enable	Extended Protection
	3	Inline Alert Only	Enable	Alert Only
	4	Inline Exchange 2013	Enable	Exchange 2013
	5	Inline Exchange 2016	Enable	Exchange 2016
	6	Inline Exchange 2019	Enable	Exchange 2019
	7	Inline SharePoint 2013	Enable	SharePoint 2013
	8	Inline SharePoint 2016	Enable	SharePoint 2016
	9	Inline WordPress	Enable	WordPress
	10	Inline Drupal	Enable	Drupal
	User Defined 2			
	11	Profile_Vincennes	Enable	Signatures_Vincennes
	12	Profile_Vincennes+Wordpress	Enable	WordPress

Inline Protection Profile

Edit Inline Protection Profile

Name

Standard Protection

Client Management

Signatures



To enable signature detection for API applications, you must first ensure that signature detection is enabled in the relevant application.

HTTP Protocol Constraints

X-Forwarded-For

Cookie

Cookie Security Policy

Advanced Protection

Custom Policy

CSRF Protection

HTTP Header Security

Man in the Browser Protection

URL Encryption Policy

Link Cloaking Policy

SQL/XSS Syntax Based Detection

Data Loss Prevention

Data Loss Prevention

Création du lien Wordpress dans le module X-forwarded-For :

Aller dans « Server Objects » puis X-Forwarded-For

[Dashboard](#) > [+ Create New](#) [Edit](#) [Delete](#)

#	Name	Add X-Forwarded-For
1	wordpress	Disable

- Dashboard >
- Network >
- System >
- Security Fabric >
- User >
- Policy >
- Server Objects** >
 - Server >
 - Protected Hostnames
 - Service
 - Certificates >
 - SSL Ciphers
 - Global >
 - X-Forwarded-For** ☆

Edit X-Forwarded-For Rule

Name

Add X-Forwarded-For

IP Location to Add

Add Source Port ⓘ

Add X-Forwarded-Port ⓘ

Add X-Real-IP ⓘ

Add X-Forwarded-Proto ⓘ

Delete Previous XFF Headers

Merge Previous XFF Headers

Use X-Header to Identify Original Client's IP

IP Location in X-Header

Block Using Original Client's IP ⓘ

Block Using Full Scan ⓘ IP Reputation

Dans la Policy du VS_estival_club se trouve la partie Certificat

Certificate Type

Let's Encrypt

Certificate Intermediate Group

La configuration de ce dernier s'effectue via le menu « Server Objects » puis « Certificates » et « Let's Encrypt »

