



IT SYSTEMES

Maitriser / Valoriser / Sécuriser / Automatiser



PURE
EXPERTS



GOODWILL



SAVE TIME
FACTORY



SECURE
EXPERTS

DOCUMENTATION D'EXPLOITATION TECHNIQUE AZURE APPLICATION GATEWAY

Date d'émission : 28/03/2024

Diffusion Du Document

Destinataires	Objet de la diffusion
Direction Nom du client	Frédéric Soulier
Equipe projet Nom du client	Salim Hadid
Equipe commerciale IT-SYSTEMES	Aksel Rouy
Equipe projet IT-SYSTEMES	Marcus Bueno

Suivi des versions / mise à jour du document :

N° version	Etat (1)	Date	Auteur	Objet de la mise à jour
0.1	T		IT-SYSTEMES	Création du document (Template)
0.1	T		IT-SYSTEMES	Rédaction du Document
1			IT-SYSTEMES	VERSION FINALE ET LIVRABLE

(1) T : en cours de modification ; V : Validé

AU SUJET D'IT-SYSTEMES

Depuis plus de 13 ans, IT-SYSTEMES accompagne les entreprises dans leur transformation digitale. Notre capacité à vous accompagner et notre expertise de haut niveau nous ont permis de mettre plus de 2000 entreprises sur les bons rails pour se transformer de manière efficiente.

Disposez d'un temps d'avance a toujours été notre leitmotiv et nous avons la volonté farouche de toujours proposer les meilleures solutions à nos clients.

Pour cela, IT SYSTEMES se transforme pour vous permettre de passer de la transformation digitale à la culture digitale afin de répondre aux enjeux futurs :

- Être à la pointe de l'innovation à des fins stratégiques
- Collaborer avec la DAF pour optimiser l'usage de l'informatique
- Répondre aux besoins métiers et comprendre l'expérience client
- Faire face aux enjeux de sécurité et au manque de compétences IT
- Stopper le cumul des applications et favoriser l'interopérabilité pour mieux travailler.

Pour répondre à ses enjeux, nous avons créé quatre pôles d'excellence offrant conseil et expertise à nos clients. Retrouvez alors nos équipes PURE EXPERT, GOODWILL, SECURE EXPERT et SAVE TIME FACTORY.

Pour plus d'information : Site web - itsystemes.fr / [IT SYSTEMES](#) sur YouTube / [IT Systemes](#) sur LinkedIn.



TABLE DES MATIERES

Section 1 :	Azure Application Gateway	4
1.1.	Introduction.....	4
1.2.	Préparation / prérequis	4
1.3.	Mise en service.....	6
1.3.1.	Création de l'instance Azure Application Gateway	6
1.4.	Paramétrages disponibles	14
1.4.1.	Le menu « Backend Health »	14
1.4.2.	Le menu « Configuration »	15
1.4.3.	Le menu « Health Probe »	16
1.4.4.	Le menu « Monitoring »	16
Section 2 :	Web Application Firewall	17
2.1.	Introduction.....	17
2.2.	Préparation / prérequis	18
2.3.	Mise en place de Web Application Firewall	19

SECTION 1 : AZURE APPLICATION GATEWAY

1.1. INTRODUCTION

Azure Application Gateway est un équilibreur de charge de trafic web permettant de gérer le trafic vers vos applications web au niveau de la couche OSI n°7 « Application ». Les équilibreurs de charge traditionnels fonctionnent au niveau de la couche OSI n°4 de « Transport » (TCP et UDP) et acheminent le trafic en fonction de l'adresse IP et du port sources, vers une adresse IP et un port de destination.

Application Gateway peut prendre des décisions de routage basées sur des attributs supplémentaires d'une requête HTTP, par exemple des en-têtes d'hôte ou le chemin d'un URI. Par exemple, vous pouvez acheminer le trafic en fonction de l'URL entrante.

Une configuration Azure Application Gateway est composée de 5 objets :

- Un écouteur (listener)
 - C'est le point d'entrée d'Azure Application Gateway
 - Une IP publique ou privée associée à un protocole, en général HTTPS
- Des configurations http
 - C'est ici que l'on renseigne le domaine et le certificat SSL/TLS
- Les backends
 - Les services cibles, n'importe quel service accessible via une IP (web app, mais aussi des VM par exemple)
- Des backend pools
 - Les backends que l'on cible avec les mêmes règles de routage peuvent être rassemblés dans un pool commun appelé backend pool
- Une règle (rule) qui permettra d'agréger les 3 objets précédents

Application Gateway existe en deux versions :

- Standard
- Standard V2 :
 - Mise à l'échelle automatique des instances
 - Prise en charge de la gestion des URL de chemin d'accès
 - Zones de redondance
 - Intégration avec AKS ou KV
 - Règles WAF (Web Application Firewall) personnalisées

1.2. PRÉPARATION / PRÉREQUIS

Pour configurer Azure Application Gateway, il faut d'abord préparer les applications à déployer dans un groupe de ressources qui serviront pour établir une infrastructure :

☐ Nom ↑↓

☐  CMSFL-SMTP01-OSdisk-00

☐  nic-CMSFL-SMTP01-00

☐  nic-PRD-SMTP02-VM-00

☐  PRD-SMTP01-VM

☐  PRD-SMTP02-VM

☐  PRD-SMTP02-VM-OSdisk-00

Ici nous avons deux services « VM » qui hébergent un service ADFS :

- Groupe de Ressources : « PRD-Identity-RG »
- Emplacement : France Central
- PRD-SMTP01-VM : ADFS 01
- PRD-SMTP02-VM : ADFS 02
- Abonnement : ITOps-Identity

1.3. MISE EN SERVICE

1.3.1. Création de l'instance Azure Application Gateway

Un second groupe de ressource a été créé un autre abonnement pour la partie connectivité

- Groupe de Ressource : PRD-Connectivity-RG
- Abonnement : ITOps-Connectivity-Prod

1.3.1.1. Basics

1 De base 2 Serveurs frontaux 3 Backends 4 Configuration 5 Étiquettes 6 Vérifier + créer

Une passerelle d'application est un équilibreur de charge du trafic web qui vous permet de gérer le trafic sur votre application web. [En savoir plus sur la passerelle d'application](#)

Détails du projet

Sélectionnez l'abonnement pour gérer les coûts et les ressources déployées. Utilisez les groupes de ressources comme les dossiers pour organiser et gérer toutes vos ressources.

Abonnement * ① ITOps-Connectivity-Prod

Groupe de ressources * ① PRD-Connectivity-RG
[Créer nouveau](#)

Détails de l'instance

Nom de la passerelle * Nom-Applicaiton-Gateway ✓

Région * France Central

Niveau ① Standard V2

Mise à l'échelle automatique ☒ Oui ☐ Non

Nombre d'instances minimal * ① 0

Nombre d'instances maximal 10

Zone de disponibilité * ① Zones 1, 2, 3

HTTP2 ① ☐ Désactivé ☒ Activé

Configurer le réseau virtuel

Réseau virtuel * ① PRD-Connectivity-VNET
[Créer](#)

Sous-réseau * ① Application-Gateway-Subnet (10.128.1.0/24)
[Gérer la configuration du sous-réseau](#)

On choisit le groupe de ressources « RG2 »

- 1- On attribue le nom « PRD-ADFS-AGW » et la région souhaitée « France Central »
- 2- On sélectionne le tier « WAF V2 »
- 3- On sélectionne le VNet « PRD-Connectivity-VNET » && Le sous réseau « Application Gateway Subnet »

1.3.1.2. Frontends

L'onglet « Frontends » permet de définir si l'Azure Application Gateway que l'on crée est publique ou privée.

✓ Basics 2 Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

Traffic enters the application gateway via its frontend IP address(es). An application gateway can use a public IP address, private IP address, or one of each type.

Frontend IP address type ① ☒ Public ☐ Private ☐ Both

Public IP address (New) myIP Add new

On garde ici l'option « Public » puisque c'est via cette adresse que les clients de l'AAG pourront s'y connecter, il est tout à fait possible de changer cette option ultérieurement.

- IP Publique Name : appGwPublicFrontendIpIPv4
- IP : 4.233.16.111

1.3.1.3. Backends

L'onglet « Backends » permet d'ajouter des pools de backends à la configuration. On appelle backends les ressources auxquelles l'AAG peut envoyer du trafic réseau. Ces ressources peuvent être des machines virtuelles, des services d'applications, des adresses IP ou des noms de domaine pleinement qualifiés (FQDN).

✓ Basics ✓ Frontends 3 Backends 4 Configuration 5 Tags 6 Review + create

A backend pool is a collection of resources to which your application gateway can send traffic. A backend pool can contain virtual machines, virtual machine scale sets, app services, IP addresses, or fully qualified domain names (FQDN).

Add a backend pool

Backend pool	Targets
No results	

Il n'y a besoin que d'un seul backend pour le moment, il est possible d'en rajouter plus tard.

Modifier le pool backend ...

Un pool de back-ends est une collection de ressources auxquelles votre passerelle d'application peut envoyer du trafic. Ce pool peut contenir des machines virtuelles, des groupes de machines virtuelles identiques, des adresses IP, des noms de domaine ou un App Service.

Nom

PRD-ADFS-BACKEND

Ajouter un pool backend sans cible

Oui

Non

Cibles de back-end

2 éléments

Type de cible	Cible	
Adresse IP ou nom de domaine complet	10.128.8.13	...
Adresse IP ou nom de domaine complet	10.128.8.14	...
Adresse IP ou nom de domaine comp...		

Règle associée

WAF-ROUTE-POLICY

On appelle cette pool de backends « PRD-ADFS-BACKEND ».

Il est désormais possible de sélectionner le type de cible ainsi que la cible souhaitée.

Il faut sélectionner « Adresse IP ou Nom de Domaine Complet », et ajouter l'adresse ip des ressources créée précédemment « PRD-SMTP01-VM » et « PRD-SMTP02-VM » .

IMPORTANT : On peut sélectionner une cible de type adresse IP ou FQDN, ce qui signifie qu'il est possible d'utiliser une ressource hors Azure comme backend tant qu'elle possède une adresse IP.

App Services

IP address or FQDN

Virtual machine

VMSS

App Services

1.3.1.4. Configuration

Le dernier onglet qui nous intéresse est « Configuration », c'est ici qu'on crée les règles de routage, la section se divise en deux sous-onglets « Listener » et « Backend targets ».



On ajoute la règle de routage côté « Listener » :

WAF-ROUTE-POLICY

PRD-ADFS-AGW

Configurez une règle de routage pour envoyer le trafic à partir d'une adresse IP de front-end donnée à une cible de back-end spécifiée. Une règle doit contenir un écouteur et au moins une cible.

Nom de la règle

WAF-ROUTE-POLICY

Priorité *



1

* Écouteur * Cibles de back-end

Un écouteur « écoute » le trafic utilisant un protocole spécifié sur une adresse IP et un port donnés. Si les critères de l'écouteur sont remplis, la passerelle d'application applique cette règle de routage. ⓘ

Écouteur *

PRD-ADFS-FRONT

PRD-ADFS-FRONT ...

PRD-ADFS-AGW

Nom de l'écouteur ⓘ

PRD-ADFS-FRONT

Adresse IP du front-end * ⓘ

Publique

Protocole ⓘ

☐ HTTP ☒ HTTPS

Port * ⓘ

443

Sélectionner un certificat

☐ Créer ☒ Sélectionner un groupe existant

Certificat *

Wildcard

☐ Renouveler ou modifier le certificat sélectionné

☐ Activer le profil SSL ⓘ

Règle associée

WAF-ROUTE-POLICY

Type d'écouteur ⓘ

☒ De base ☐ Plusieurs sites

Pages d'erreurs personnalisées

Afficher les pages d'erreur personnalisées pour différents codes de réponse générés par Application Gateway. Cette section vous permet de configurer des pages d'erreurs spécifiques à l'écouteur.

[En savoir plus ⓘ](#)

Passerelle incorrecte - 502

Entrer une URL de fichier HTML

Interdit - 403

Entrer une URL de fichier HTML

[Afficher plus de codes d'état](#)

On nomme cette règle ainsi que l'écouteur (PRD-ADFS-FRONT).

Puis, nous allons choisir le protocole HTTPS qui utilisera le port 443 et nous allons ajouter le Certificat pour le site Front dans notre cas « * cms-fl.com » et le lien de l'app « fsfl.cms-fl.com ».

IMPORTANT : L'option « Error page URL » permet d'ajouter des pages d'erreur pour les codes 403 (Forbidden / Interdit) et 502 (Bad gateway / Mauvaise passerelle).

Type d'écouteur ⓘ

☒ De base ☐ Plusieurs sites

Pages d'erreurs personnalisées

Afficher les pages d'erreur personnalisées pour différents codes de réponse générés par Application Gateway. Cette section vous permet de configurer des pages d'erreurs spécifiques à l'écouteur.

[En savoir plus](#)

Passerelle incorrecte - 502

Entrer une URL de fichier HTML

Interdit - 403

Entrer une URL de fichier HTML

[Afficher plus de codes d'état](#)

On configure maintenant la partie « Backend targets » :

WAF-ROUTE-POLICY

PRD-ADFS-AGW

Configurez une règle de routage pour envoyer le trafic à partir d'une adresse IP de front-end donnée à une cible de back-end spécifiée. Une règle doit contenir un écouteur et au moins une cible.

Nom de la règle

WAF-ROUTE-POLICY

Priorité * ⓘ

1

*Écouteur *Cibles de back-end

Choisissez un pool de back-ends auquel cette règle d'acheminement envoie le trafic. Vous devez également spécifier un jeu de paramètres du back-end définissant le comportement de la règle de routage.

Type de cible

☒ Pool principal ☐ Redirection

Cible de back-end * ⓘ

PRD-ADFS-BACKEND

Paramètres du back-end * ⓘ

PROB-ADFS

Deux options sont disponibles, le routage vers un des backends (backend pool) ou vers une URL donnée (redirection).

On sélectionne la cible backend précédemment créée « PRD-ADFS-BACKEND ».

Il est aussi nécessaire de déclarer des paramètres (PROB-ADFS).

Nom des paramètres du back-end

PROB-ADFS

Protocole de back-end

☐ HTTP ☒ HTTPS

Port principal *

443

Le certificat du serveur principal est émis par une autorité de certification connue

☐ Oui ☒ Non

Charger le certificat d'autorité de certification racine

i Vous devez charger le certificat racine (.CER) du serveur principal sur le paramètre du serveur principal si une autorité de certification privée a émis ce certificat ou si celui-ci est auto-généré. Ce certificat racine permet à votre passerelle applicative d'effectuer la validation de chaîne de certificats.

- Pour extraire le certificat racine du serveur principal, suivez le [guide de résolution des problèmes](#).
- Vous pouvez également créer vos propres certificats de serveur et autorité de certification racine. [Découvrez plus d'informations](#).

Certificat

adfs2

[+ Ajouter un certificat](#)

Paramètres supplémentaires

Affinité basée sur les cookies ⓘ

☒ Activer ☐ Désactiver

Nom du cookie d'affinité

ApplicationGatewayAffinity

Drainage des connexions ⓘ

☐ Activer ☒ Désactiver

Délai d'expiration de la demande (secondes) * ⓘ

20

Remplacer le chemin backend ⓘ

/

Nom de l'hôte

Par défaut, la passerelle applicative envoie le même en-tête d'hôte HTTP au backend qu'il reçoit du client. Si votre application/service principal nécessite une valeur d'hôte spécifique, vous pouvez la remplacer à l'aide de ce paramètre.

Remplacer par le nouveau nom d'hôte

☒ Oui ☐ Non

i Si le service principal est un service Azure multi-locataires tel que App Services, Functions ou Portal Apps, nous vous recommandons d'utiliser [Méthode de domaine personnalisé](#), au lieu de remplacer le nom d'hôte. L'utilisation d'un nom d'hôte de remplacement avec des domaines par défaut (azurewebsites.net, azuremicroservices.io, etc.) est une bonne solution uniquement pour les tests et les opérations de base.

Nom de l'hôte

Par défaut, la passerelle applicative envoie le même en-tête d'hôte HTTP au backend qu'il reçoit du client. Si votre application/service principal nécessite une valeur d'hôte spécifique, vous pouvez la remplacer à l'aide de ce paramètre.

Remplacer par le nouveau nom d'hôte

☒ Oui ☐ Non

i Si le service principal est un service Azure multi-locataires tel que App Services, Functions ou Portal Apps, nous vous recommandons d'utiliser [Méthode de domaine personnalisé](#), au lieu de remplacer le nom d'hôte. L'utilisation d'un nom d'hôte de remplacement avec des domaines par défaut (azurewebsites.net, azuremicroservices.io, etc.) est une bonne solution uniquement pour les tests et les opérations de base.

Remplacement du nom d'hôte

- ☐ Choisir un nom d'hôte à partir d'une cible de back-end
☒ Remplacer par un nom de domaine spécifique

Nom de l'hôte *

fsfl.cms-fl.com

Utiliser une sonde personnalisée ⓘ

☒ Oui ☐ Non

Sonde personnalisée *

fsfl.cms-fl.com

On attribue un nom au paramétrage, le protocole ciblé est https pour le service (backend port : 443).

Nous devons aussi ajouter un certificat d'autorité de certification racine pour valider l'authentification au format « .CER »

Il faut accepter le paramètre « Host Name » et choisir l'option « Remplacer par un nom de domaine Spécifique » qui permet de sélectionner un nom d'hôte depuis les cibles backend (backend target).

Create application gateway ...

✓ Basics ✓ Frontends ✓ Backends **4 Configuration** 5 Tags 6 Review + create

Create routing rules that link your frontend(s) and backend(s). You can also add more backend pools, add a second frontend IP configuration if you haven't already, or edit previous configurations.

Frontends

+ Add a frontend IP

Public: (new) myIP

Routing rules

+ Add a routing rule

rule1

Manage Backend settings

Backend pools

+ Add a backend pool

amethyst1back

Il ne reste alors plus qu'à déployer l'AAG.

Nom	Type	Emplacement
prdvaflog-6b97189f-3abc-4318-95c6-de82c47745cf	Rubrique système Event Grid	France Central
prdvaflog	Compte de stockage	France Central
PRD-WAF-POLICY	Stratégie WAF Application Gateway	France Central
PRD-PALOMGMT-GW	Table de routage	France Central
PRD-Connectivity-VNET	Réseau virtuel	France Central
PRD-ADFS-IP	Adresse IP publique	France Central
PRD-ADFS-AWG	Passerelle d'application	France Central
logspaceappgateway	Espace de travail Log Analytics	France Central

1.3.1.5. Test de la configuration

Pour tester la configuration on récupère l'adresse IP dans le tableau de bord :

Réseau/sous-réseau virtuel : [PRD-Connectivity-VNET/Application-Gateway-Subnet](#)

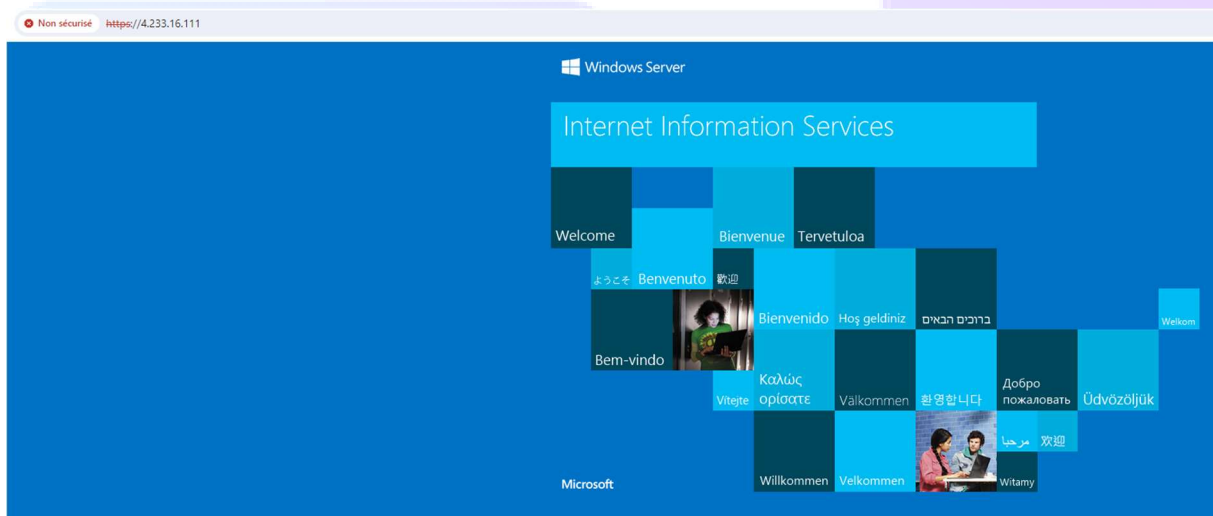
Adresses IP publiques fro... : [4.233.16.111 \(PRD-ADFS-IP\)](#)

Adresses IP privées front... : -

Niveau : WAF V2

Zone de disponibilité : 1, 2, 3

On clique tout simplement sur le lien qui nous emmène sur la page de l'application.



1.4. PARAMÉTRAGES DISPONIBLES

1.4.1. Le menu « Backend Health »

Ce menu permet de récupérer le statut des différents backend déclarés dans les pools.

Serveur (pool principal)	↑↓	État	↑↓	Port (paramètre b... ↑↓	Protocole	↑↓	Détails	Action
10.128.8.13 (PRD-ADFS-BACKE...		🟢 Sain		443 (PROB-ADFS)	Https		Success. Received 404 status code	
10.128.8.14 (PRD-ADFS-BACKE...		🟢 Sain		443 (PROB-ADFS)	Https		Success. Received 404 status code	

Si une des Web apps est stoppée :

Search backend health			
Server (backend pool)	Port (Backend setting)	Status	Details
amethysteweb1.azurewebsites.net (amethyste1back)	80 (settings1)	🟢 Healthy	Success
amethysteweb2.azurewebsites.net (amethyste1back)	80 (settings1)	🔴 Unhealthy	Received invalid status code in the backend :

1.4.2. Le menu « Configuration »

Ce menu permet de modifier les réglages comme le nombre d'instances, le SKU (Unité de gestion des stocks) ou le tier :

Enregistrer Ignorer Commentaires

Niveau * ⓘ
WAF V2

Type de capacité
☒ Mise à l'échelle automatique ☐ Manuel

Nombre d'instances minimal * ⓘ
0

Nombre d'instances maximal * ⓘ
4

HTTP2 *
Désactivé **Activé**



1.4.3. Le menu « Health Probe »

Il permet de déclarer des sondes personnalisées, c'est utile avec certains backend, l'assistant de déploiement en créer une à la suite de la configuration :

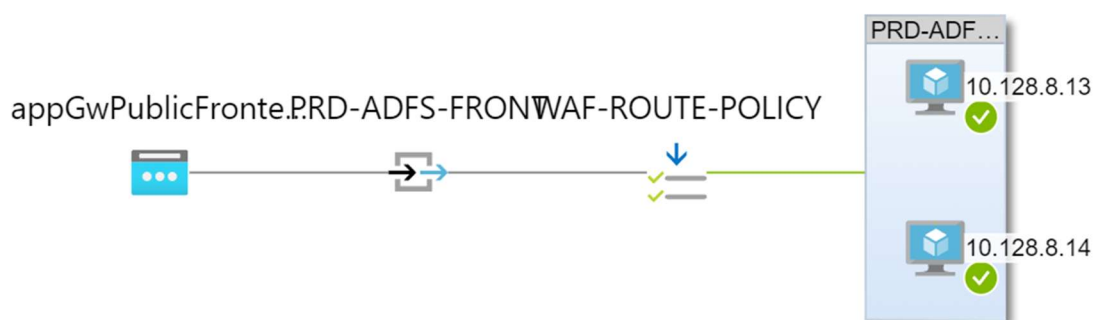
fsfl.cms-fl.com

PRD-ADFS-AGW

Nom	fsfl.cms-fl.com
Protocole *	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Choisir le nom d'hôte dans les paramètres du back-end	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Choisir un port à partir des paramètres du back-end	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Chemin * ⓘ	<input type="text" value="/"/>
Intervalle (secondes) * ⓘ	<input type="text" value="30"/>
Délai d'expiration (secondes) * ⓘ	<input type="text" value="30"/>
Seuil de défaillance sur le plan de l'intégrité * ⓘ	<input type="text" value="3"/>
Utiliser des conditions de correspondance de sonde ⓘ	<input checked="" type="radio"/> Oui <input type="radio"/> Non
Correspondance du code d'état de réponse HTTP * ⓘ	<input type="text" value="200-499"/>
Correspondance du corps de réponse HTTP ⓘ	<input type="text"/>
Paramètres du back-end ⓘ	<input type="text" value="PRD-ADFS"/>

1.4.4. Le menu « Monitoring »

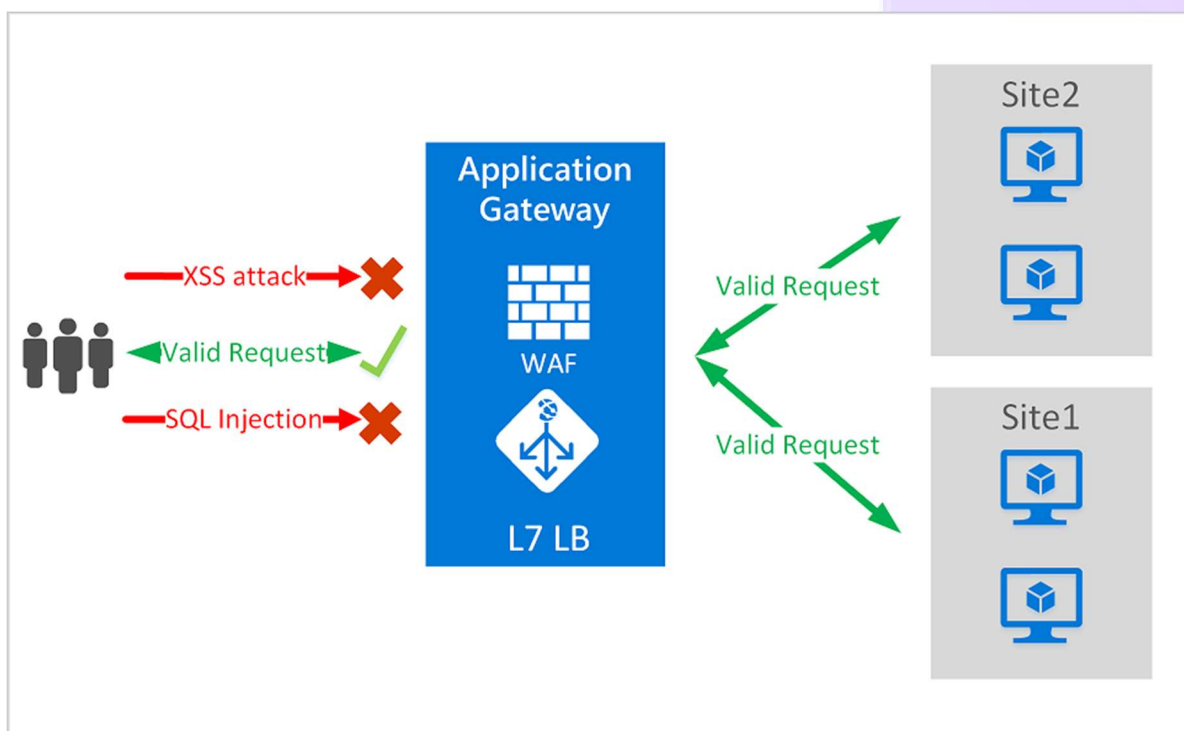
Il offre un état des lieux de la configuration déployée, c'est utile pour avoir une vue globale.



SECTION 2 : WEB APPLICATION FIREWALL

2.1. INTRODUCTION

De nombreuses configurations sont disponibles après le déploiement d'Azure Application Gateway, une des plus intéressantes est Azure Web Application Firewall (WAF), un service intégré à AAG et dont il est dépendant. Il occupe une fonction de pare-feu et dispose de règles destinées à protéger un site de diverses attaques comme l'injection de code SQL, ou l'exploitation de failles de sécurité inter-sites.



Il est possible de le configurer selon deux modes :

- Detection Mode
 - WAF surveille et logue mais ne bloque rien
- Prevention Mode
 - WAF surveille et logue, mais il peut aussi bloquer une requête si une anomalie est détectée

Etant donné que ce service est intégré à Azure Application Gateway, on se situe encore sur la couche n°7 « Application » du modèle OSI, par conséquent, la protection se fait uniquement au niveau des applications Web contre les attaques entrantes http/HTTPS.

IMPORTANT : Malgré les ressemblances entre Azure WAF et Azure Firewall, ces deux services se distinguent. Azure WAF est une fonctionnalité d'AAG protégeant des attaques entrantes http/HTTPS, Azure Firewall est un stand-alone protégeant toutes les ressources intégrées dans le VNET sur d'autres protocoles (RDP, SSH, FTP, HTTPS...) en entrée comme en sortie.

2.2. PRÉPARATION / PRÉREQUIS

En se basant sur le déploiement précédemment réalisé, il est tout à fait possible d'activer l'option dans la sélection du « Tier » :

Instance details

Application gateway name *

Region * France Central

Tier ⓘ Standard V2

Enable autoscaling

Minimum instance count * ⓘ

Maximum instance count

Cependant il est aussi possible de modifier le « Tier » dans le menu configuration :

Accueil > Groupes de ressources > PRD-Connectivity-RG > PRD-ADFS-AGW

PRD-ADFS-AGW | Configuration ☆ ...

Passerelle d'application

Rechercher « Enregistrer Ignorer Commentaires

Vue d'ensemble

Journal d'activité

Contrôle d'accès (IAM)

Étiquettes

Diagnostiquer et résoudre les problèmes

Paramètres

Configuration

Pare-feu d'applications web

Pools principaux

Niveau * ⓘ WAF V2

Type de capacité

Mise à l'échelle automatique Manuel

Nombre d'instances minimal * ⓘ 0

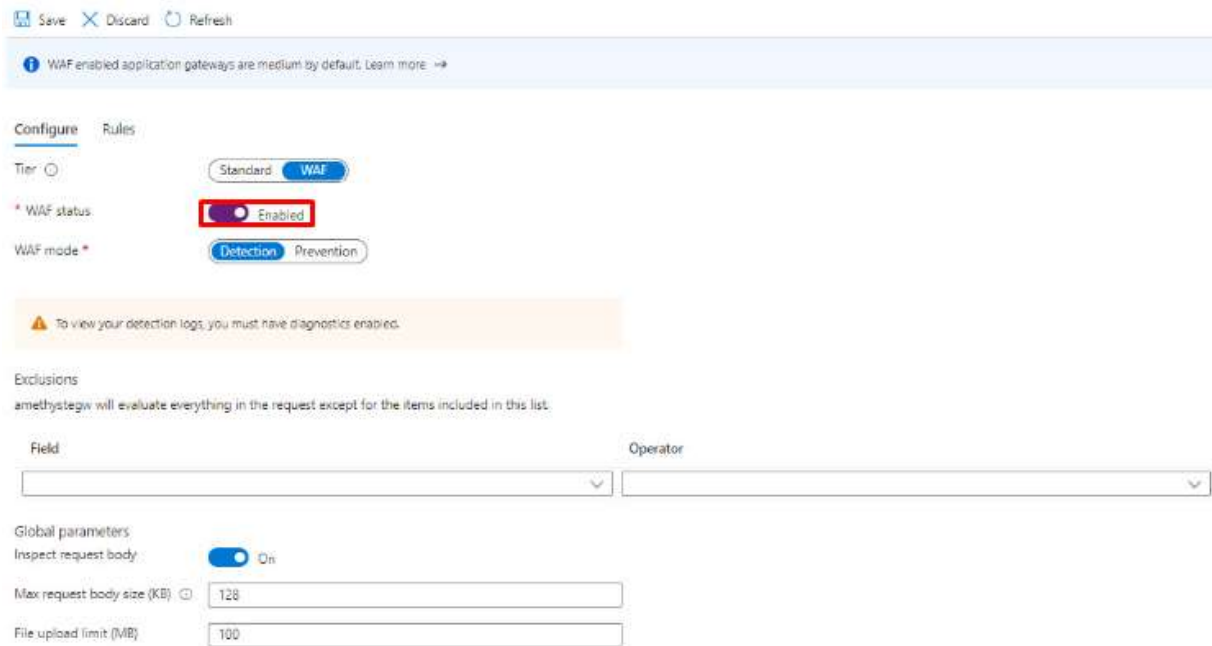
Nombre d'instances maximal * ⓘ 4

HTTP2 * Désactivé Activé

IMPORTANT : WAF n'est pas compatible avec le SKU size small.

2.3. MISE EN PLACE DE WEB APPLICATION FIREWALL

On active le service Web Application Firewall :



Save Discard Refresh

WAF enabled application gateways are medium by default. Learn more →

Configure Rules

Tier ☐ Standard ☒ WAF

* WAF status ☒ Enabled

WAF mode * ☒ Detection ☐ Prevention

⚠ To view your detection logs, you must have diagnostics enabled.

Exclusions
amethystegw will evaluate everything in the request except for the items included in this list.

Field Operator

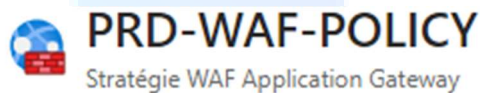
Global parameters

Inspect request body ☒ On

Max request body size (KB) 128

File upload limit (MiB) 100

IMPORTANT : WAF V2 Cree une ressource Azure a part entire



Sur cette ressource nous allons avoir 4 menu lier a la configuration :

Paramètres

- Paramètres de stratégie
- Règles managées
- Règles personnalisées
- Passerelles applicatives associées
- Données sensibles
- Propriétés
- Verrous

Supervision

1. Regles Manager
2. Regles personnalisées
3. Regles de donner Sensibles (Pour Nettoyage des Jounaux)

Le premier menu « Regles manager » laisse apparaître les « Rule set ». Azure Application Gateway supporte OWASP 3.2 a 3.0.0 (Open Worldwide Application Security Project¹) qui sont des ensembles de règles permettant de se prémunir contre les risques de sécurité les plus critiques dans les applications web.

Ensembles de règles managés Exclusions

Un ensemble de règles préconfiguré est activé par défaut. Cet ensemble de règles protège votre application web contre les menaces courantes définies dans le top 10 des catégories établies par OWASP. L'ensemble de règles par défaut est gén

Attribuer + Ajouter des exclusions Actualiser | Activer Désactiver Changer l'action

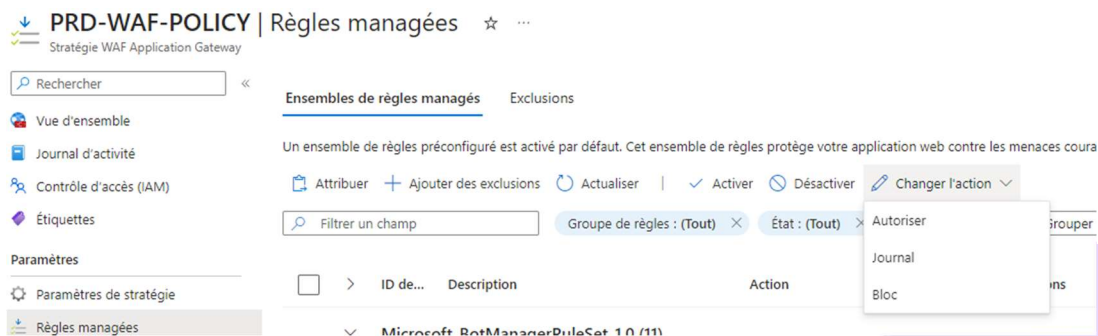
Filter un champ Groupe de règles : (Tout) État : (Tout) Action : (Tout) Grouper par Ensemble de ...

ID de...	Description	Action	État	Exclusions	Groupe de règles	Ensemble de règles
Microsoft_BotManagerRuleSet_1.0 (11)						
100100	Malicious bots detected by threat intelligence	Bloc	Enabled		BadBots	Microsoft_BotManagerRuleSet_1.0
100200	Malicious bots that have falsified their identity	Bloc	Enabled		BadBots	Microsoft_BotManagerRuleSet_1.0
200100	Search engine crawlers	Autoriser	Enabled		GoodBots	Microsoft_BotManagerRuleSet_1.0
200200	Unverified search engine crawlers	Journal	Enabled		GoodBots	Microsoft_BotManagerRuleSet_1.0
300100	Unspecified identity	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300200	Tools and frameworks for web crawling and attack	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300300	General purpose HTTP clients and SDKs	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300400	Service agents	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300500	Site health monitoring services	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300600	Unknown bots detected by threat intelligence	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
300700	Other bots	Journal	Enabled		UnknownBots	Microsoft_BotManagerRuleSet_1.0
OWASP_3.2 (186)						
200002	Failed to Parse Request Body.	Score d'anomalie	Enabled		General	OWASP_3.2
200003	Multipart Request Body Strict Validation.	Score d'anomalie	Enabled		General	OWASP_3.2
200004	Possible Multipart Unmatched Boundary.	Score d'anomalie	Enabled		General	OWASP_3.2
911100	Method is not allowed by policy	Score d'anomalie	Enabled		REQUEST-911-METHOD-ENFORCEMENT	OWASP_3.2
913100	Found User-Agent associated with security scann	Score d'anomalie	Enabled		REQUEST-913-SCANNER-DETECTION	OWASP_3.2
913101	Found User-Agent associated with scripting/gene	Score d'anomalie	Enabled		REQUEST-913-SCANNER-DETECTION	OWASP_3.2
913102	Found User-Agent associated with web crawler/b	Score d'anomalie	Enabled		REQUEST-913-SCANNER-DETECTION	OWASP_3.2

Sur chaque règle, vous avez la possibilité de configurer 4 modes. Ils sont visibles sur le bouton Changer l'action :

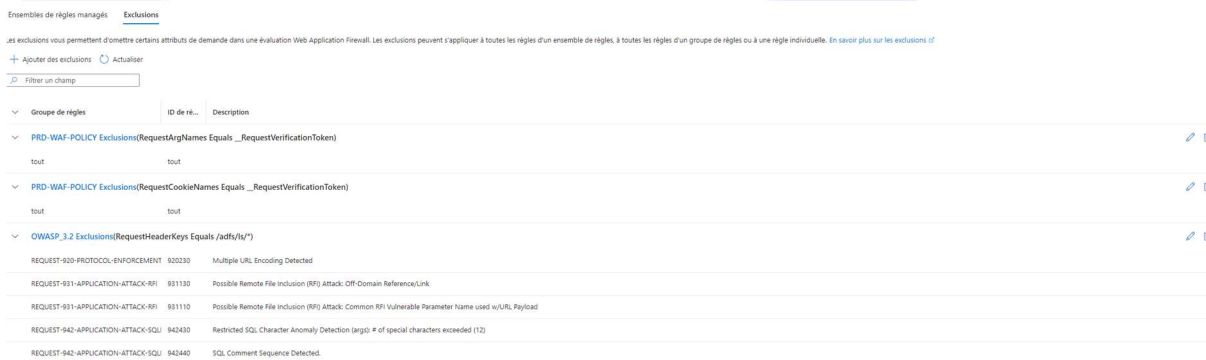
- Autoriser (Disponibles sur les règles anti BOTs)
- Journal
- Bloc
- Score d'anomalie

¹ L'OWASP est une organisation à but non lucratif créée dans le but de sensibiliser les développeurs quant aux risques les plus courants des applications web.



IMPORTANT : Par défaut, toutes les règles sont appliquées en mode « Score d'anomalie », pour éviter les faux positifs passer les règles bloquantes en « journal » cela permet de donner accès aux services tout en enregistrant l'événement sur les Logs

Sur l'onglet « Exclusion » nous pouvons ajouter des règles d'exclusion pour chaque règle OWASP. Ses règles sont disponibles pour exclure les microservices de l'application web



Les règles personnalisées vous permettent de créer vos propres règles évaluées pour chaque requête passant par le pare-feu d'applications Web (WAF). Ces règles ont une priorité plus élevée que les autres règles des ensembles de règles gérés. Les règles personnalisées contiennent un nom de règle, une priorité de règle et un tableau des conditions de correspondance. Si ces conditions sont remplies, une action est entreprise (pour autoriser, bloquer ou consigner). Si une règle personnalisée est déclenchée et qu'une action d'autorisation ou de blocage est effectuée, aucune autre règle personnalisée ou gérée n'est évaluée. Les règles personnalisées peuvent être activées/désactivées à la demande.

Par exemple, vous pouvez bloquer toutes les demandes à partir d'une adresse IP de la plage 192.168.5.0/24. Dans cette règle, l'opérateur est `IPMatch`, `matchValues` correspond à la plage d'adresses IP (192.168.5.0/24) et l'action consiste à bloquer le trafic. Vous définissez également le nom, la priorité et l'état d'activation de la règle.

Les règles personnalisées prennent en charge l'utilisation de la logique de composition pour établir des règles plus avancées répondant à vos besoins de sécurité. Par exemple, vous pouvez utiliser deux règles personnalisées pour créer la logique suivante ((`rule1:Condition 1 et rule1:Condition 2`) ou `rule2:Condition 3`). Cet exemple signifie que si Condition 1 et Condition 2 sont remplies, ou si Condition 3 est remplie, le pare-feu d'applications web doit effectuer l'action spécifiée dans la règle personnalisée.

Différentes conditions de correspondance au sein de la même règle sont toujours composées à l'aide de **et**. Par exemple, bloquer le trafic à partir d'une adresse IP spécifique, et seulement si un certain navigateur est utilisé.

Si vous voulez utiliser **ou** entre deux conditions différentes, ces conditions doivent se trouver dans des règles différentes. Par exemple, bloquer le trafic à partir d'une adresse IP spécifique, ou seulement si un certain navigateur est utilisé.

Les expressions régulières sont également prises en charge dans les règles personnalisées, comme dans les ensembles de règles CRS. Pour plus de détails, voir les exemples 3 et 5 dans Créer et utiliser des règles de pare-feu d'applications web personnalisées.

IMPORTANT : Le nombre maximal de règles personnalisées WAF est de 100.

IMPORTANT : Les règles de redirection appliquées au niveau de la passerelle applicative ignorent les règles personnalisées WAF

Vous pouvez créer des règles personnalisées pour répondre aux besoins exacts de vos applications et stratégies de sécurité. À présent, vous pouvez restreindre l'accès à vos applications web par pays ou par région. Comme avec toutes les règles personnalisées, cette logique peut être composée d'autres règles pour répondre aux besoins de votre application.

Pour créer une règle personnalisée de filtrage géographique dans le Portail Azure, sélectionnez Zone géographique comme type de correspondance, puis le pays/la région que vous souhaitez autoriser ou bloquer à partir de votre application. Lorsque vous créez des règles de filtrage géographique avec Azure PowerShell ou Azure Resource Manager, utilisez la variable `match RemoteAddr` et l'opérateur `Geomatch`