Bonnes pratiques anti-DDoS

Julien Simon
Principal Technical Evangelist, AWS
julsimon@amazon.fr
@julsimon

amazon web services

Qu’est-ce que le DDoS ?

Distributed **D**enial **O**f **S**ervice

amazon web services

Les attaques sont plus fréquentes et plus massives

La cyberattaque géante aurait été réalisée par de jeunes pirates amateurs

Par Elisa Braun | Mis à jour le 27/10/2016 à 12:19 / Publié le 27/10/2016 à 11:29

Derrière une série d'attaques informatiques très puissantes, un réseau d'objets connectés piratés

Un réseau de caméras de surveillance piratées aurait permis à des pirates de mener des attaques informatiques d'une ampleur sans précédent.

LE MONDE | 26.09.2016 à 11h59 • Mis à jour le 26.09.2016 à 13h41

des organisations ont été victimes d'une attaque DDoS

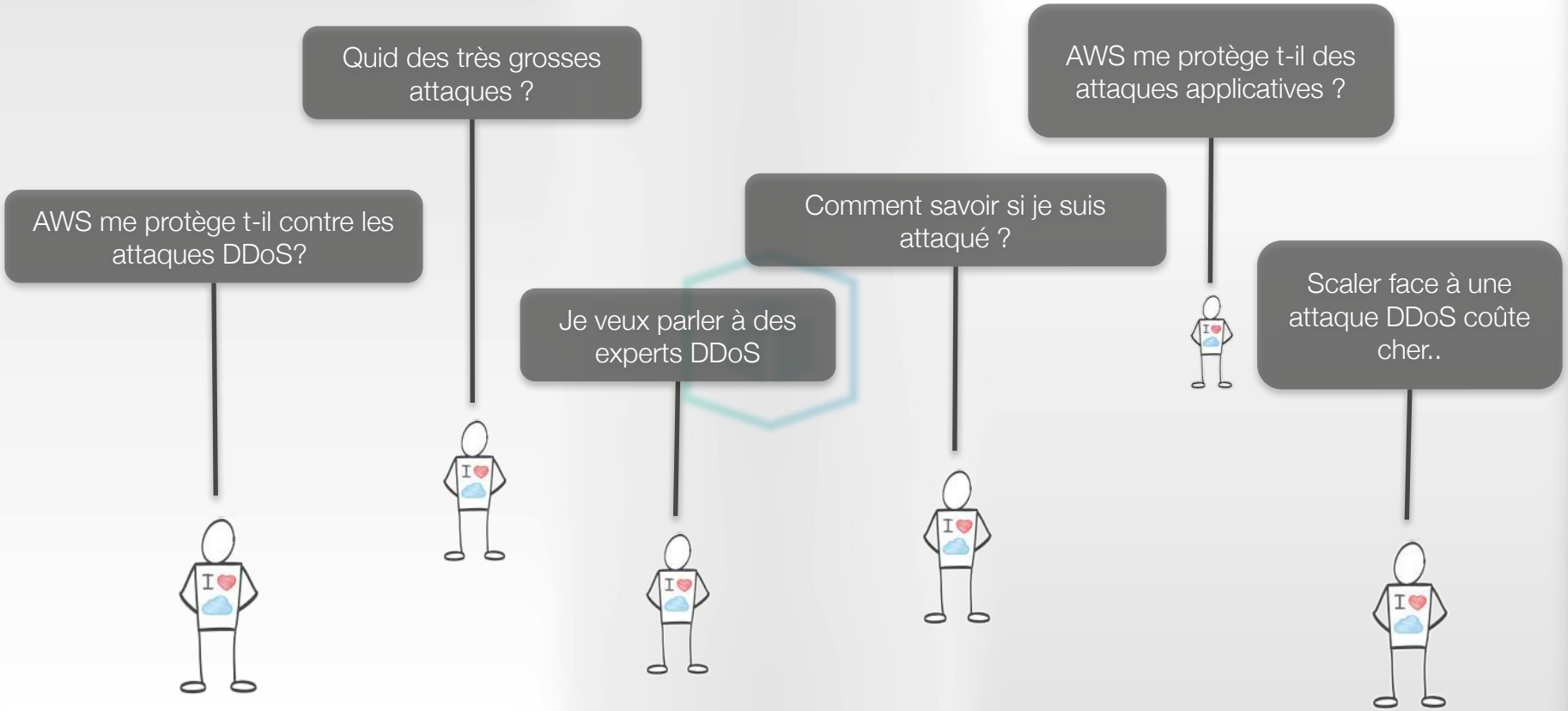
coût horaire moyen d'une attaque DDoS

des attaques durent 30 minutes ou moins

Source : Imperva What DDoS Attacks Really Cost Businesses (n=270)
Source : Imperva Global DDoS Threat Landscape Q2 2015

amazon web services

Ce que nos clients nous demandent



Agenda

Types d'attaques DDoS

Difficultés à gérer les attaques DDoS

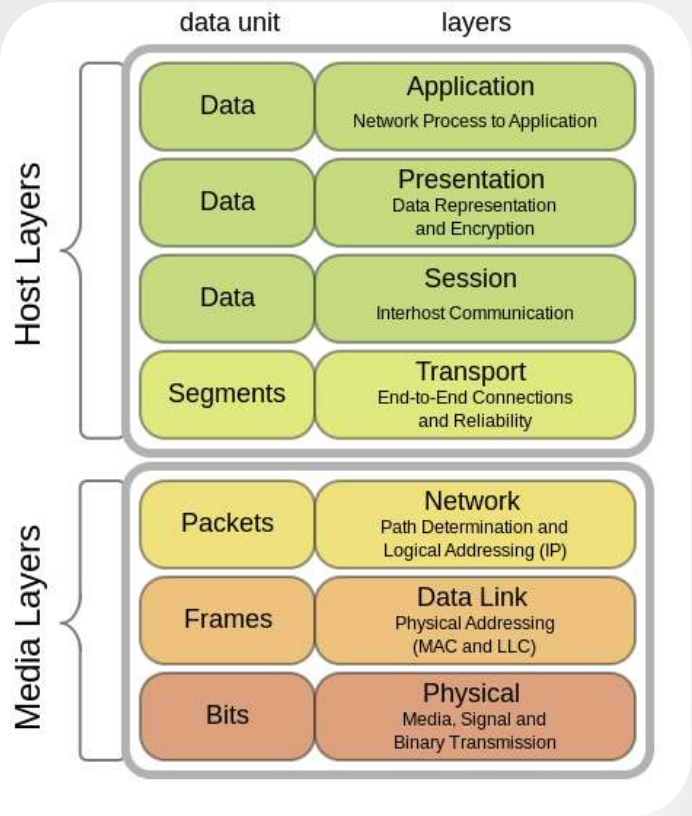
Bonnes pratiques de résilience

Services AWS utiles contre le DDoS

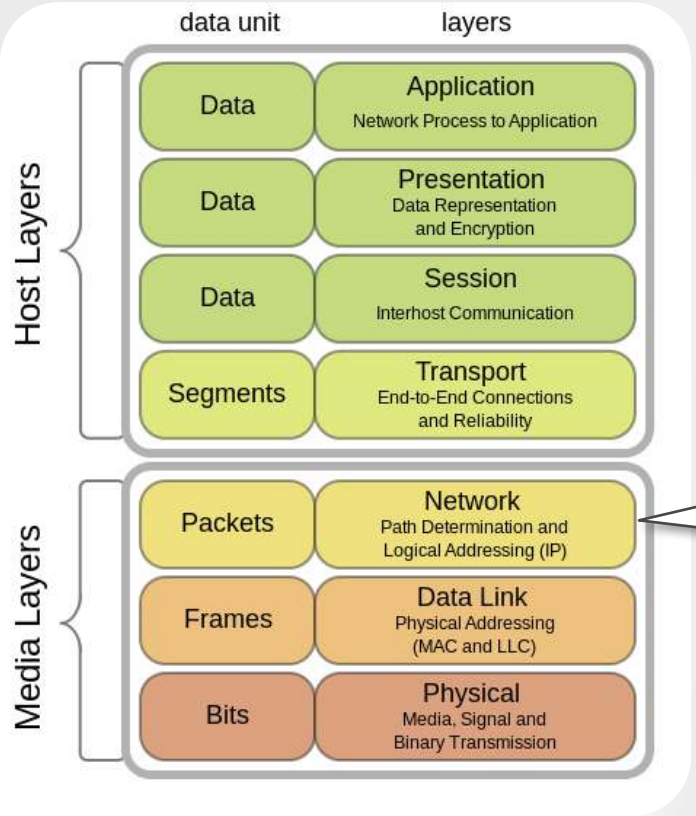
Questions et réponses

Types d’attaques DDoS

Types d’attaques DDoS



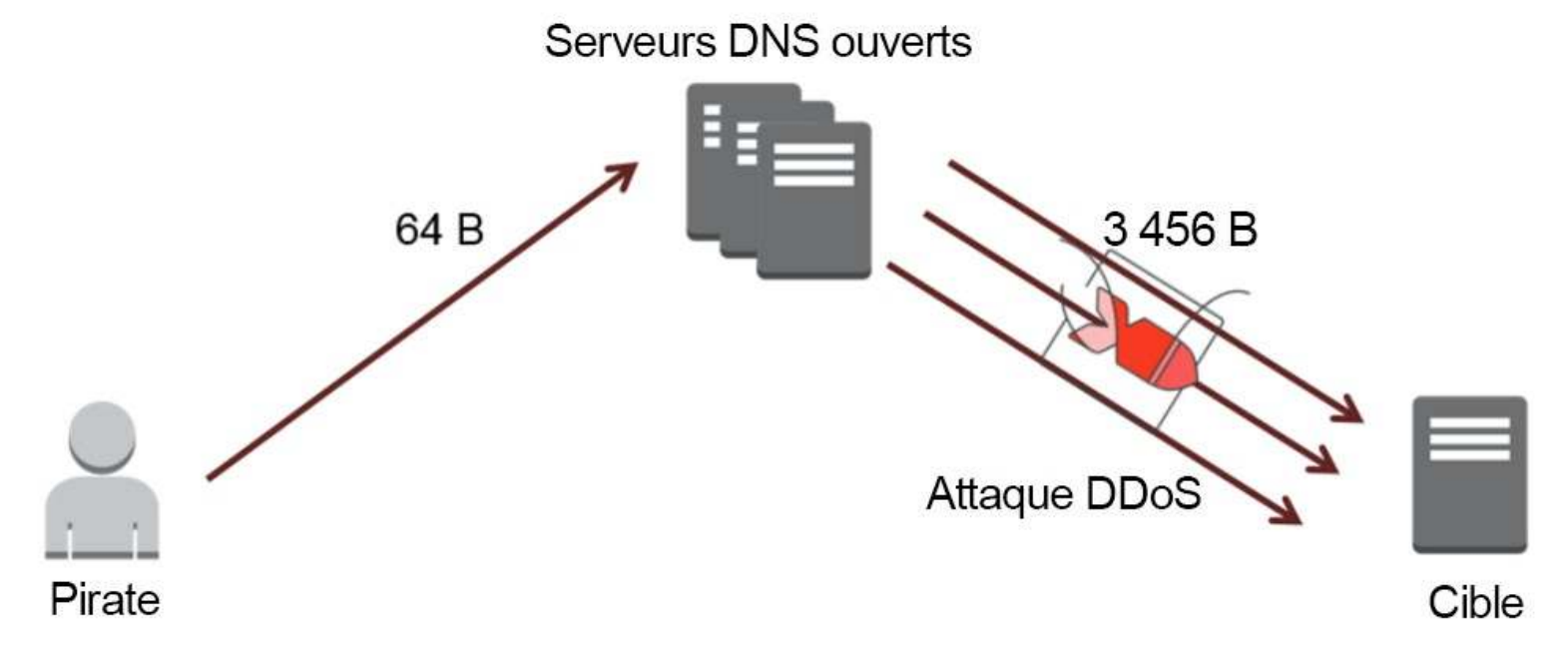
Types d’attaques DDoS



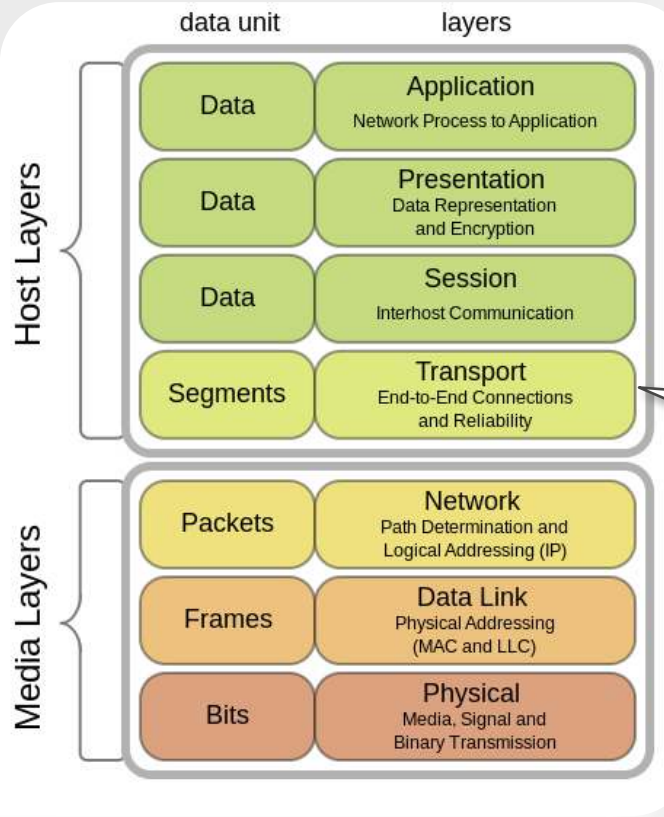
L3 : attaques volumétriques

Encombrer les réseaux en les inondant de plus de trafic qu’ils ne peuvent gérer (exemple: attaques par amplification)

Attaque volumétrique par amplification DNS



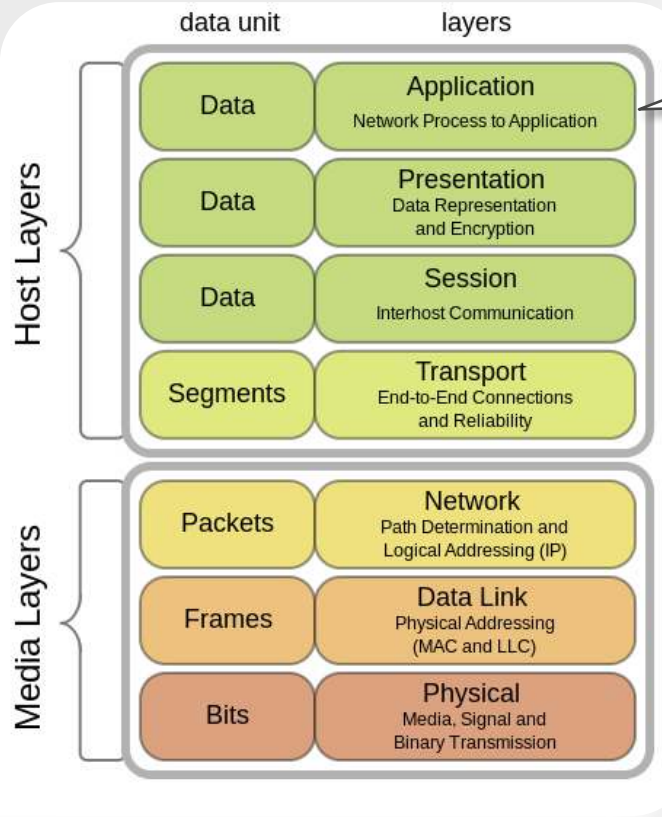
Types d'attaques DDoS



L4 : attaques par épuisement de ressources

Exploiter les protocoles pour stresser les *firewalls*, les *load balancers*, etc.
(exemple: TCP Syn Flood)

Types d’attaques DDoS



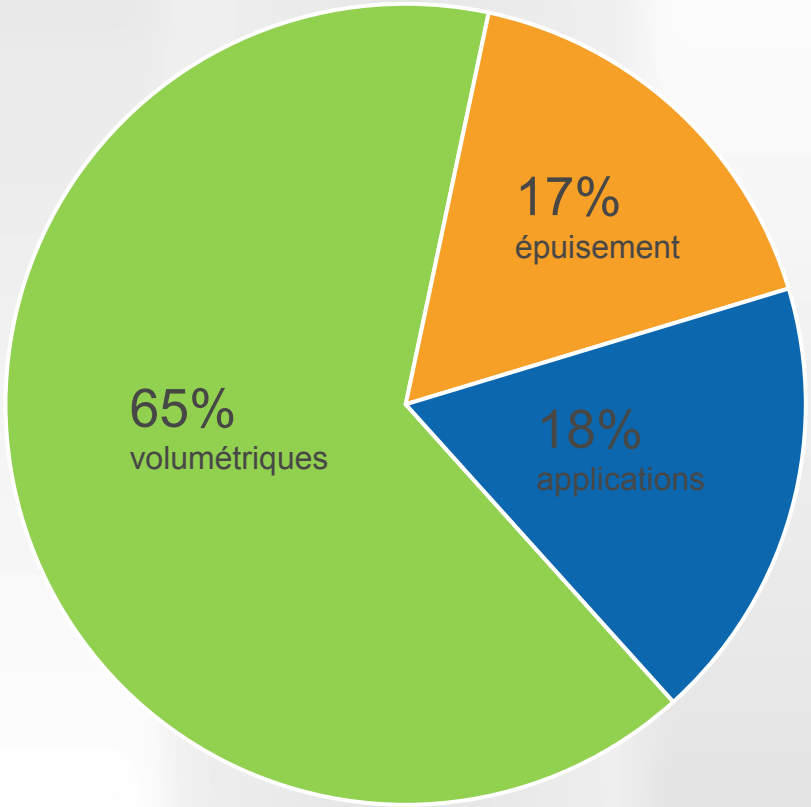
L7 : attaques applicatives

Utiliser des requêtes malicieuses pour contourner la mitigation et épuiser les ressources de l’application (exemple : HTTP GET, DNS flood)

Attaques contre une application web (niveau 7)

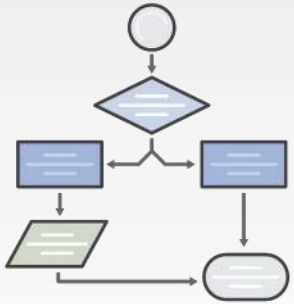
https://en.wikipedia.org/wiki/Slowloris_(computer_security)

Typologies des attaques DDoS



Difficulté à gérer les attaques DDoS

Difficultés à mettre en place la protection



Configuration complexe

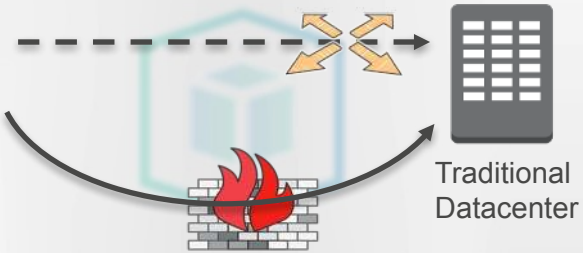
Capacity planning de la bande passante

Modification de l'architecture de l'application

Coût

Difficultés à activer la protection

Besoin d'impliquer l'opérateur



Reroutage du trafic vers une destination de nettoyage, potentiellement avec un augmentation de latence

Le temps, c'est de l'argent !

Bonne pratiques de résilience

Livre blanc : bonnes pratiques pour la résilience DDoS

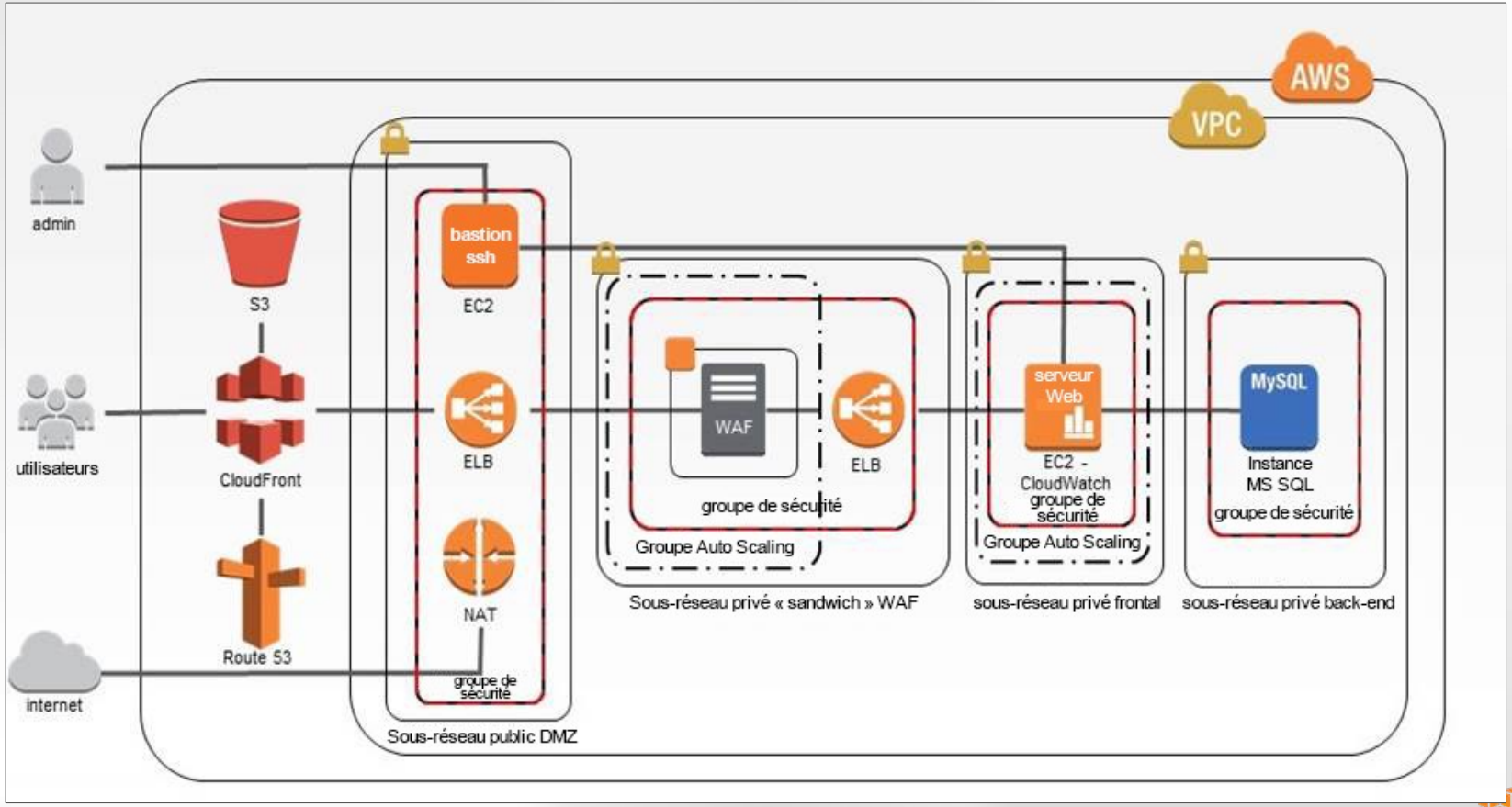
https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

Mis à jour en Juin 2016.

Ce sont aussi des bonnes pratiques de haute disponibilité et de performance.

Lecture fortement conseillée ☺

Architecture résiliente DDoS



Quelques bonnes pratiques

Réduisez la surface d'attaque

Préparez la mise à l'échelle pour absorber l'attaque

Etudiez le comportement de votre plate-forme

Surveillez vos flux VPC

Utilisez les services gérés pour contrer les attaques en amont

Réduisez la surface d'attaque

Concevez votre application en tenant compte de la surface d'attaque potentielle

- Réduisez le nombre de points d'entrée par Internet
- Séparez le trafic et l'infra des différents services
- Autorisez explicitement les utilisateurs et le trafic

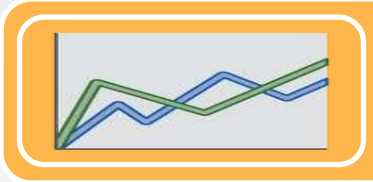
Mécanismes pour réduire la surface d'attaque

- Application Load Balancers
- Instances distinctes dans des sous-réseaux différents
- Adresses IP élastiques (réassignables et non contiguës)
- Security Groups, ACL réseau

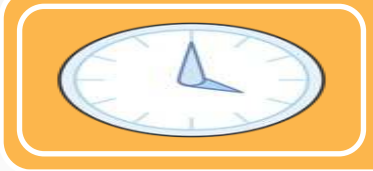
https://aws.amazon.com/fr/blogs/security/how-to-help-prepare-for-ddos-attacks-by-reducing-your-attack-surface/

Préparez la mise à l'échelle pour absorber l'attaque

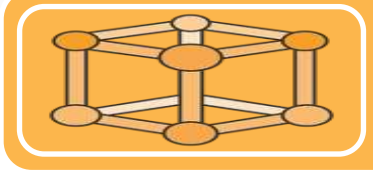
Disperser l'attaque sur une zone plus étendue



Obliger les attaquants à déployer beaucoup plus de ressources pour faire monter l'attaque d'un cran



Vous laisser le temps d'analyser l'attaque DDoS et d'y répondre

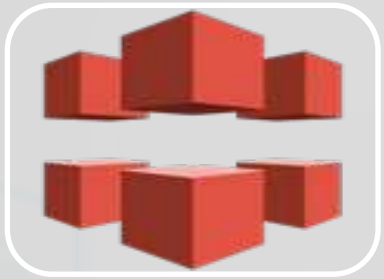


Fournir une couche supplémentaire de redondance pour les autres scénarios de défaillance

Préparez la mise à l'échelle pour absorber l'attaque

Activer *Enhanced Networking* sur EC2

Utiliser *Application Load Balancing* et *Auto Scaling*



Déployer plusieurs points de présence à l'aide d'Amazon CloudFront

Etudiez le comportement normal

Comprenez et utilisez comme référence les niveaux d'utilisation attendus

Utilisez ces données pour identifier les niveaux ou comportements anormaux

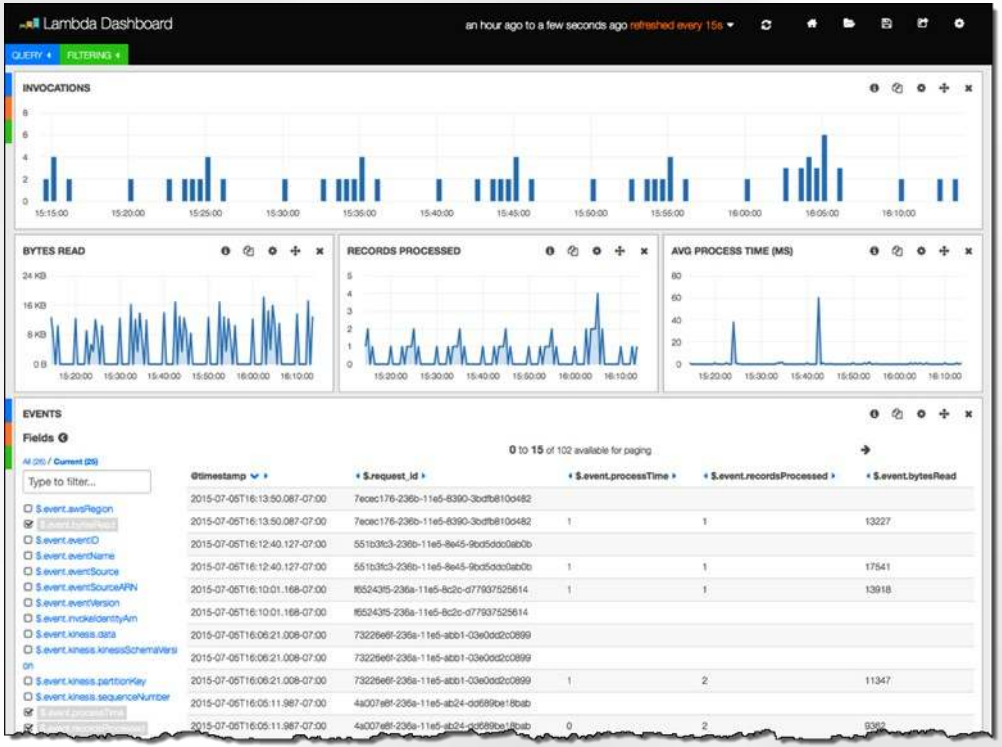
Détectez les attaquants qui scrutent ou testent votre application

Faites des tests de charge et corrigez les points chauds

Métriques CloudWatch à surveiller

Thème	Métrique	Description
Auto Scaling	GroupMaxSize	Taille maximale du groupe Auto Scaling.
Facturation AWS	EstimatedCharges	Frais estimés pour votre utilisation des services AWS.
Amazon CloudFront	Requêtes	Nombre de demandes pour l'ensemble des requêtes HTTP/S.
Amazon CloudFront	TotalErrorRate	Pourcentage de toutes les demandes pour lesquelles le code d'état HTTP est 4xx ou 5xx.
Amazon EC2	CPUUtilization	Pourcentage d'unités de calcul EC2 allouées actuellement utilisées.
Amazon EC2	NetworkIn	Nombre d'octets reçus par l'instance sur toutes les interfaces réseau.
Amazon EC2	StatusCheckFailed	Combinaison de StatusCheckFailed_Instance et StatusCheckFailed_System qui établit si l'une ou l'autre des vérifications de l'état a échoué.
ELB	RequestCount	Nombre de demandes terminées qui ont été reçues et acheminées vers les instances enregistrées.
ELB	Latence	Temps écoulé, en secondes, entre le moment où la demande quitte l'équilibreur de charge et où elle reçoit une réponse.
ELB	HTTPCode_ELB_4xx HTTPCode_ELB_5xx	Nombre de codes d'erreur HTTP 4XX ou 5XX générés par l'équilibreur de charge.
ELB	BackendConnectionErrors	Nombre de connexions ayant échoué.
ELB	SpilloverCount	Nombre de demandes qui ont été rejetées en raison de la file d'attente qui était pleine.
Amazon Route 53	HealthCheckStatus	Etat du point de terminaison de la vérification de l'état.

Surveillez vos flux VPC



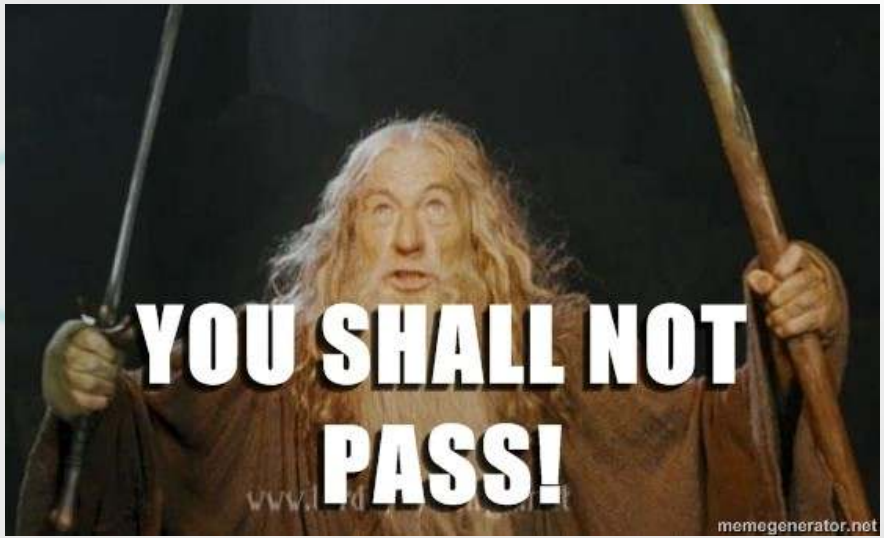
https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/
https://aws.amazon.com/blogs/aws/cloudwatch-logs-subscription-consumer-elasticsearch-kibana-dashboards/

amazon web services

Services AWS utiles contre le DDoS

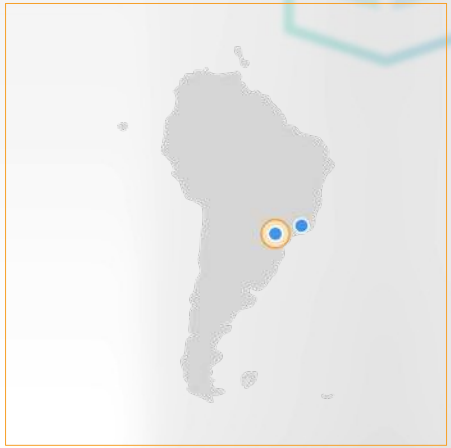
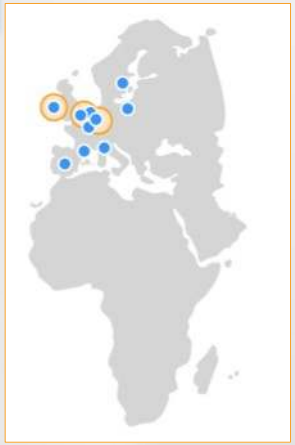
Utilisez les services gérés en amont de votre plate-forme

- Amazon CloudFront
- Amazon API Gateway
- AWS WAF
- AWS Shield



Amazon CloudFront

- 68 points de présence dans le monde
- Servez votre contenu statique et dynamique au plus près de vos utilisateurs
- Compliquez la tâche des attaquants en les éloignant de votre infrastructure AWS

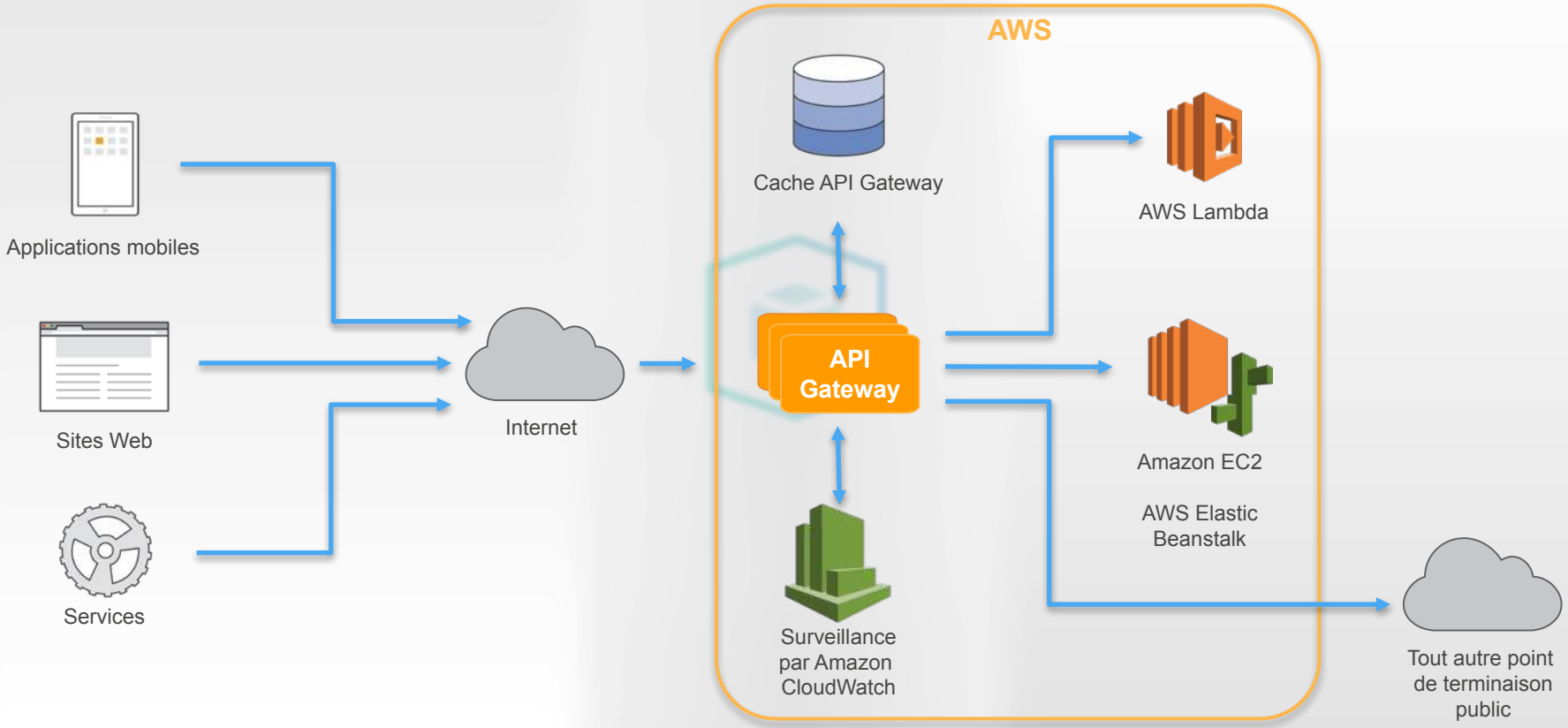

https://aws.amazon.com/cloudfront/

Amazon API Gateway

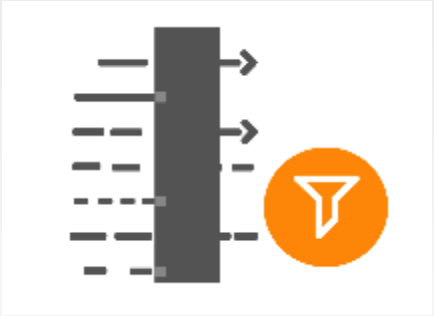
- API Gateway est un service géré qui vous permet de déployer des API REST
- Il supporte les opérations suivantes :
  - Authentification de l'utilisateur
  - Limitations des demandes (*throttling*)
  - Mise en cache des réponses
- Ces opérations vous permettent de protéger les ressources situées en aval (notamment les instances EC2)

https://aws.amazon.com/apigateway/

Trafic vers Amazon API Gateway



AWS Web Application Firewall (WAF)



Filtrage du trafic web à l'aide de règles

Blocage des requêtes malicieuses

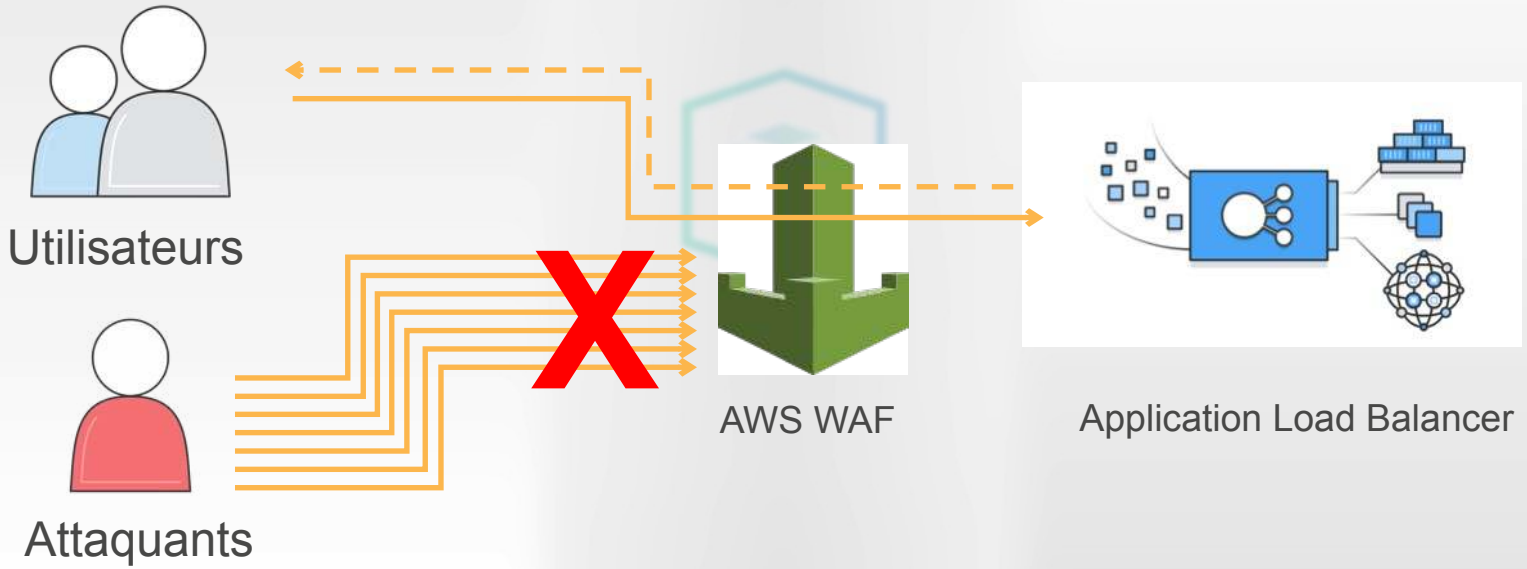
Monitoring

- WAF vous permet de bloquer le trafic web suspect ou indésirable
- Plusieurs modèles de règles pré-définies (blocage d'IP, injection SQL, etc.)
- WAF est intégré avec CloudFront et Application Load Balancer

https://aws.amazon.com/waf/

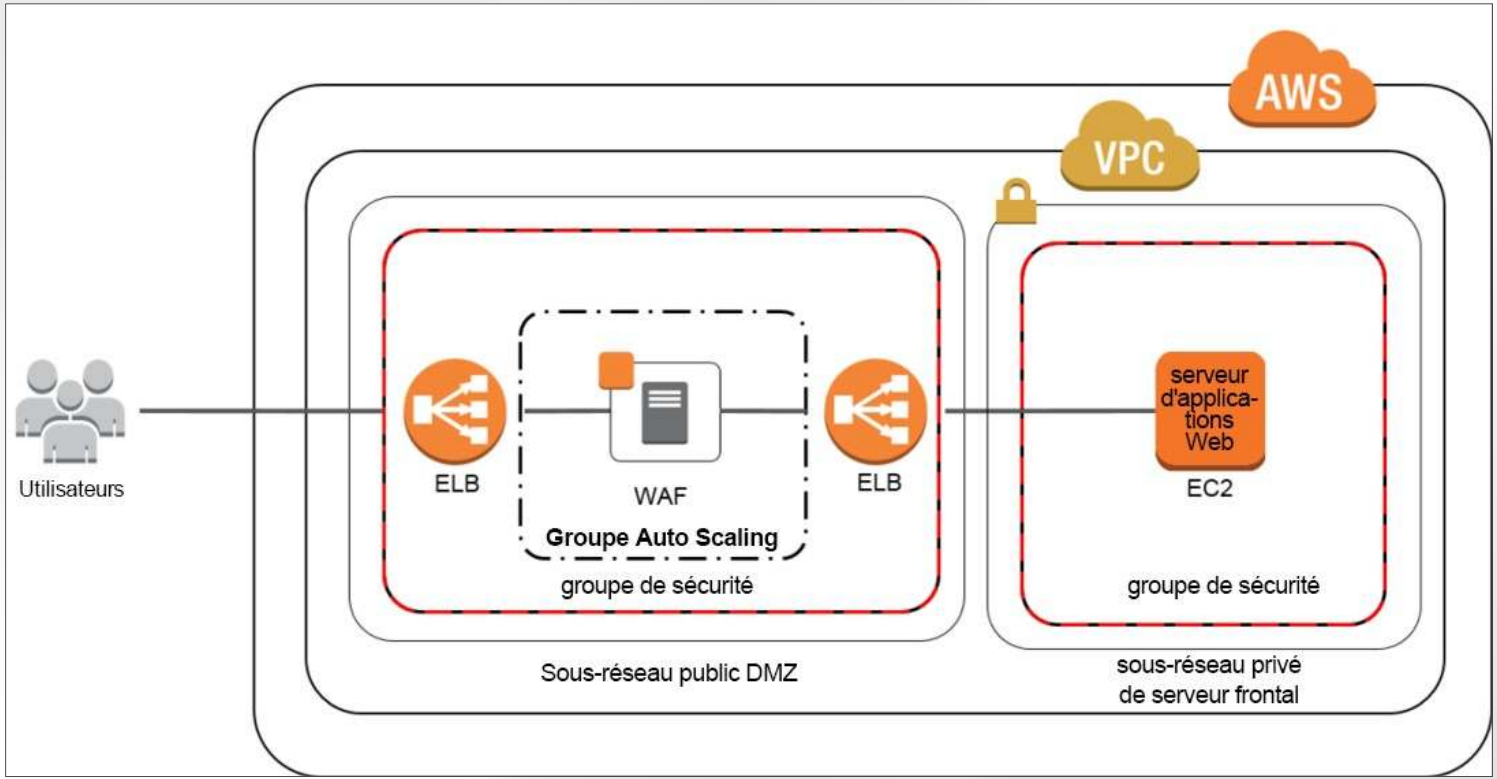
amazon web services

AWS WAF avec Application Load Balancer



https://aws.amazon.com/fr/about-aws/whats-new/2016/12/AWS-WAF-now-available-on-Application-Load-Balancer/

Protégez vos ressources avec un WAF tiers
Architecture « WAF sandwich »



Quelques solutions partenaires

Consultez la section Sécurité d'AWS Marketplace pour plus d'informations
https://aws.amazon.com/marketplace

AWS Shield

Protection Standard

Disponible pour TOUS les clients AWS, sans aucun coût supplémentaire

Protection Avancée

Service payant proposant des fonctionnalités et des protections supplémentaires

AWS Shield Standard

Protection couches 3/4

- ✓ Detection & mitigation automatiques
- ✓ Protection contre les attaques les plus courantes (SYN/UDP Floods, attaques par réflexion, etc.)
- ✓ Intégré aux services AWS

Ajoutez AWS WAF pour une protection applicative

Protection couches 3/4

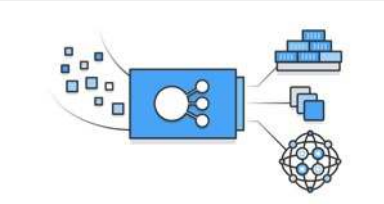
- ✓ Detection & mitigation automatiques
- ✓ Protection contre les attaques les plus courantes (SYN/UDP Floods, attaques par réflexion, etc.)
- ✓ Intégré aux services AWS

Protection couche 7

- ✓ AWS WAF
- ✓ Self-service & paiement à l'usage

AWS Shield Advanced

Disponible sur…



Application Load Balancer

Elastic Load Balancer

Amazon CloudFront

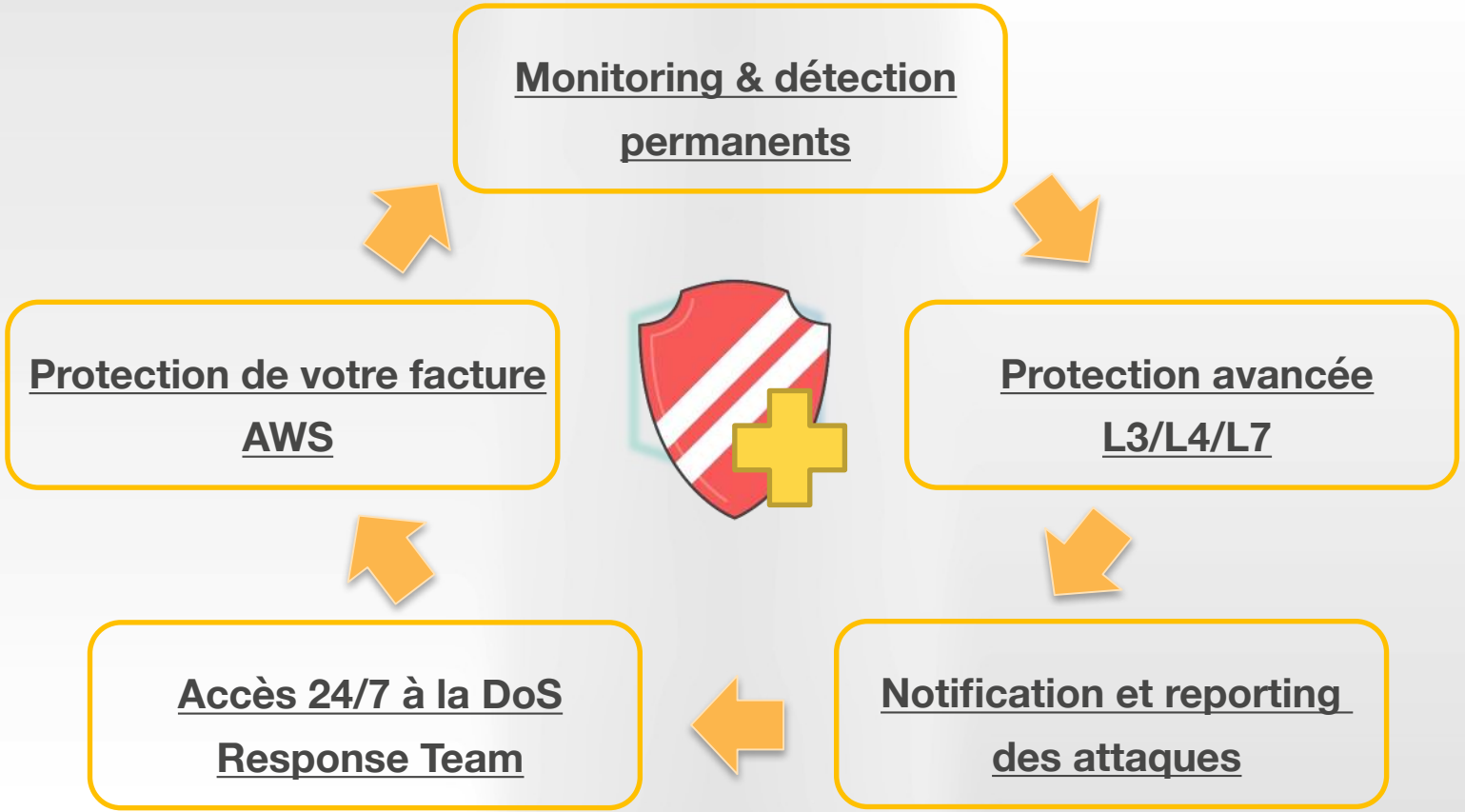
Amazon Route 53

AWS Shield Advanced

Disponible dans les régions suivantes

US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2
EU (Ireland)	eu-west-1
Asia Pacific (Tokyo)	ap-northeast-1

AWS Shield Advanced



AWS Shield : tarification

Protection Standard

- Pas d'engagement
- Pas de coût additionnel

Protection Avancée

- Abonnement d'un an
- Coût fixe mensuel : $3,000
- Coût de transfert de données

	$ par GB	
	CloudFront	**ELB**
Premiers 100 To	$0.025	0.050
400 To suivants	$0.020	0.040
500 To suivants	$0.015	0.030
4 Po suivants	$0.010	Contactez nous
Au delà de 5 Po	Contactez nous	Contactez nous

AWS Shield: comment choisir

Protection Standard

Se protéger contre les attaques DDoS les plus courantes.

Accéder à des outils et des bonnes pratiques vous permettant de construire une architecture résiliente.

Protection Avancée

Pour une protection accrue contre des attaques plus puissantes et plus sophistiquées, y compris au niveau 7 (AWS WAF inclus).

Visibilité, reporting, protection de votre facture, accès aux experts DDoS.

N’hésitez pas à nous contacter !

Equipe de compte

- Votre gestionnaire de compte défend votre cause
- Les architectes de solutions possèdent une grande expertise

Niveaux de support recommandés

- **Professionnel** – Support par téléphone/chat/ e-mail, délai de réponse d'1 heure
- **Entreprise** – Délai de réponse de 15 min, gestionnaire technique de compte dédié, notification proactive

Ressources complémentaires

Blog sécurité AWS
https://aws.amazon.com/blogs/security/

Livre blanc : Bonnes pratiques pour la résilience DDoS
https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf

AWS re:Invent 2016: NEW LAUNCH! AWS Shield—A Managed DDoS Protection Service (SAC322)
https://www.youtube.com/watch?v=R06GDQBbtRU

AWS re:Invent 2016: Mitigating DDoS Attacks on AWS: Five Vectors and Four Use Cases (SEC310)
https://www.youtube.com/watch?v=w9fSW6qMktA

Merci !

Julien Simon
Principal Technical Evangelist, AWS
julsimon@amazon.fr
@julsimon

Lundi
- Bonnes pratiques d'authentification avec AWS IAM
- Chiffrez vos données avec AWS

Mardi
- Fireside chat avec Matthieu Bouthors et Julien Simon
- Re:Invent update 1

Mercredi
- Deep dive : Amazon Virtual Private Cloud
- Bonnes pratiques anti-DDoS

Jeudi
- Re:Invent update 2
- Gérez les incidents de sécurité avec AWS CloudTrail

Vendredi
- Automatisez vos audits de sécurité avec Amazon Inspector
- Bonnes pratiques de sécurité sur AWS