AWSUGTW

淺談WAF在AWS的架構

SC Lin@AWSUGTW

2017/07/19

AWSUGTW

SC Lin

- Now:
  - Engineer with focus on public cloud and security.
  - Prepare for AWS Certified DevOps - Professional
- Experiences:
  - System Engineer, PIC
  - Security Engineer, PIC
- AWS Certification:
  - AWS Certified Solutions Architect - Professional
  - AWS Certified Solutions Architect - Associate
  - AWS Certified Developer - Associate
  - AWS Certified SysOps Administrator - Associate

Agenda

- Why WAF? Problems and expectations
- WAF architecture on AWS
- Comparisons
- Demo
- Summary

This is a AWS WAF icon.

Why WAF?

Before Why WAF, What is WAF?

A web application firewall (or WAF) filters, monitors, and blocks HTTP traffic to and from a web application. A WAF is differentiated from a regular firewall in that a WAF is able to filter the content of specific web applications while regular firewalls serve as a safety gate between servers.
- Description of WAF from Wikipedia

A web application firewall (WAF) is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection.
- Description of WAF from OWASP

Why WAF?

Problems and expectations

- OWASP Top 10
- SQL Injection
- XSS
- CVE & NVD
- DDoS
- Compliance

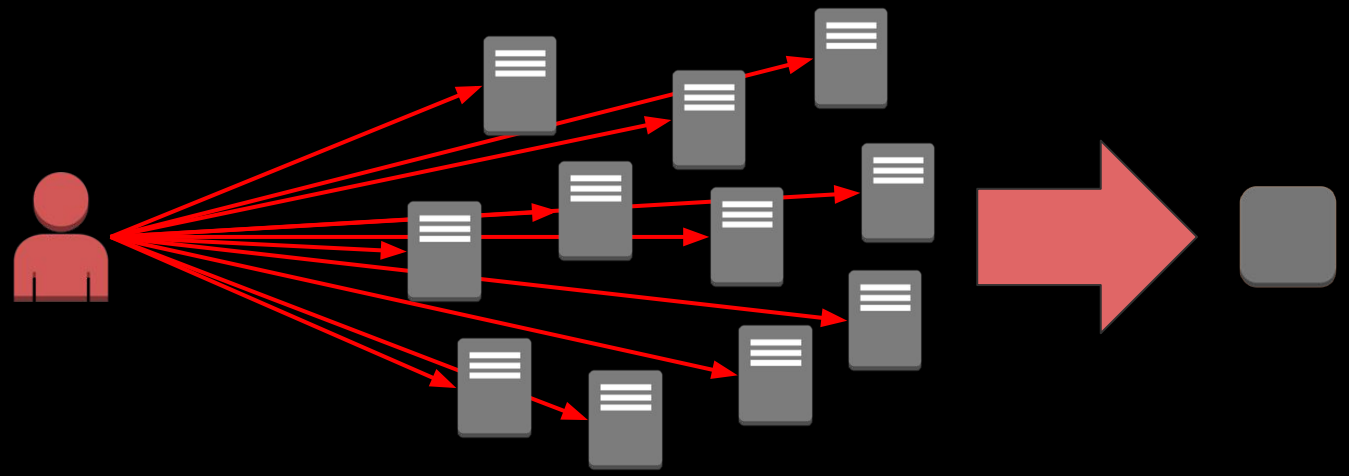
AWSUGTW

Why WAF? - 2017 OWASP Top 10

- **A1-Injection**
- A2-Broken Authentication and Session Management
- **A3-Cross-Site Scripting (XSS)**
- A4-Broken Access Control
- A5-Security Misconfiguration
- A6-Sensitive Data Exposure
- A7-Insufficient Attack Protection
- A8-Cross-Site Request Forgery (CSRF)
- **A9-Using Components with Known Vulnerabilities**
- A10-Underprotected APIs

Why WAF? - DDoS

DDoS



Why WAF? - Compliance

Compliance

- PCI DSS 3.2 requirement 6.6 choice 2

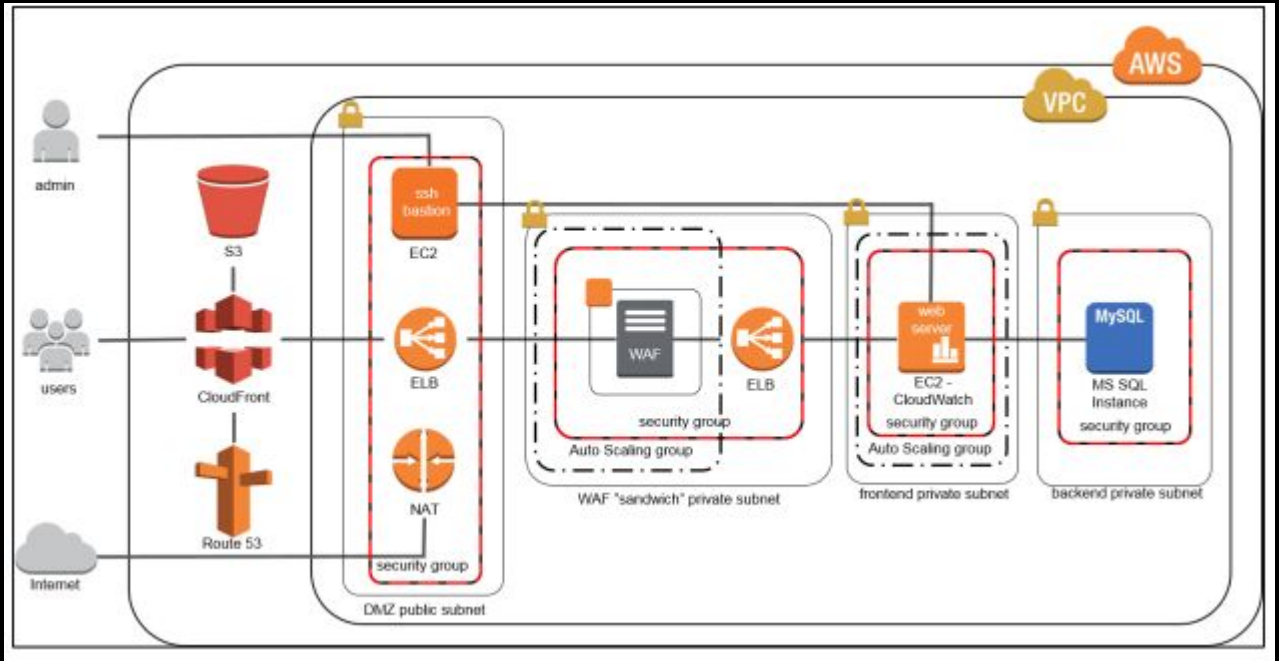
“Installing an automated technical solution that detects and prevents web-based attacks (**for example, a web-application firewall**) in front of public-facing web applications, to continually check all traffic.”

- Don’t worry, most of the solutions can help you meet PCI DSS.
- AWS WAF service is already certified by PCI DSS.
  - check here “https://aws.amazon.com/tw/compliance/services-in-scope/”

WAF architecture on AWS

WAF architecture on AWS - AWS best practice

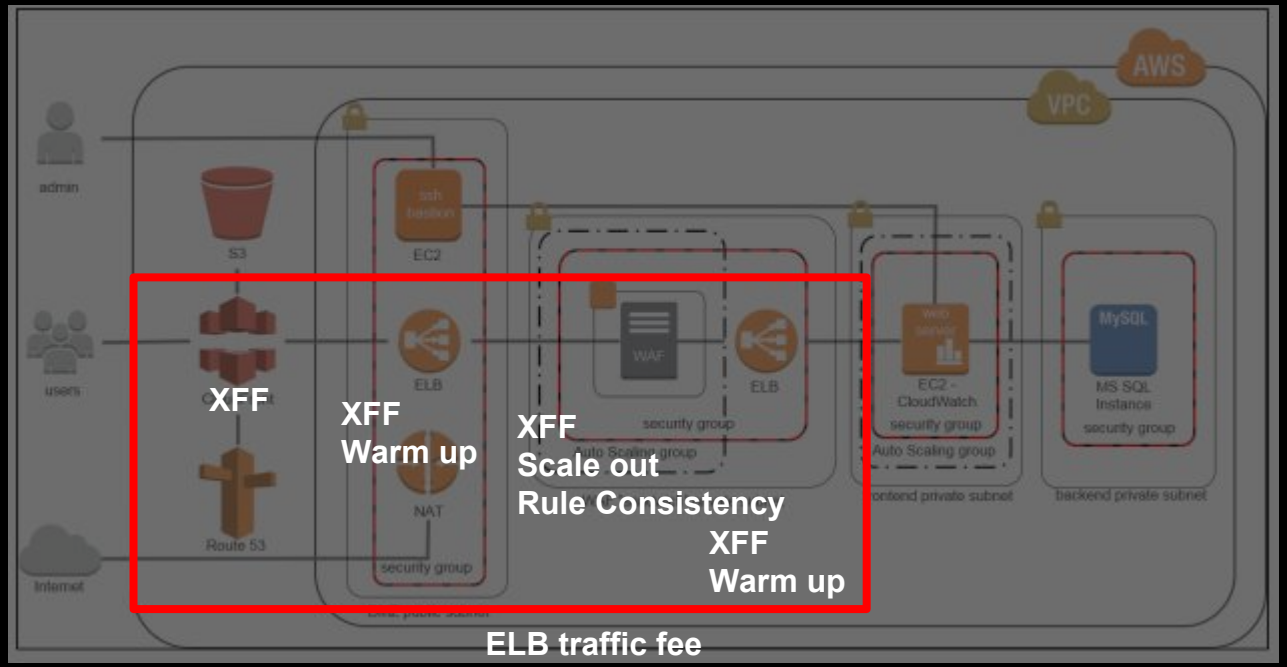
AWS best practice



Reference: AWS Best Practices for DDoS Resiliency (June 2015)

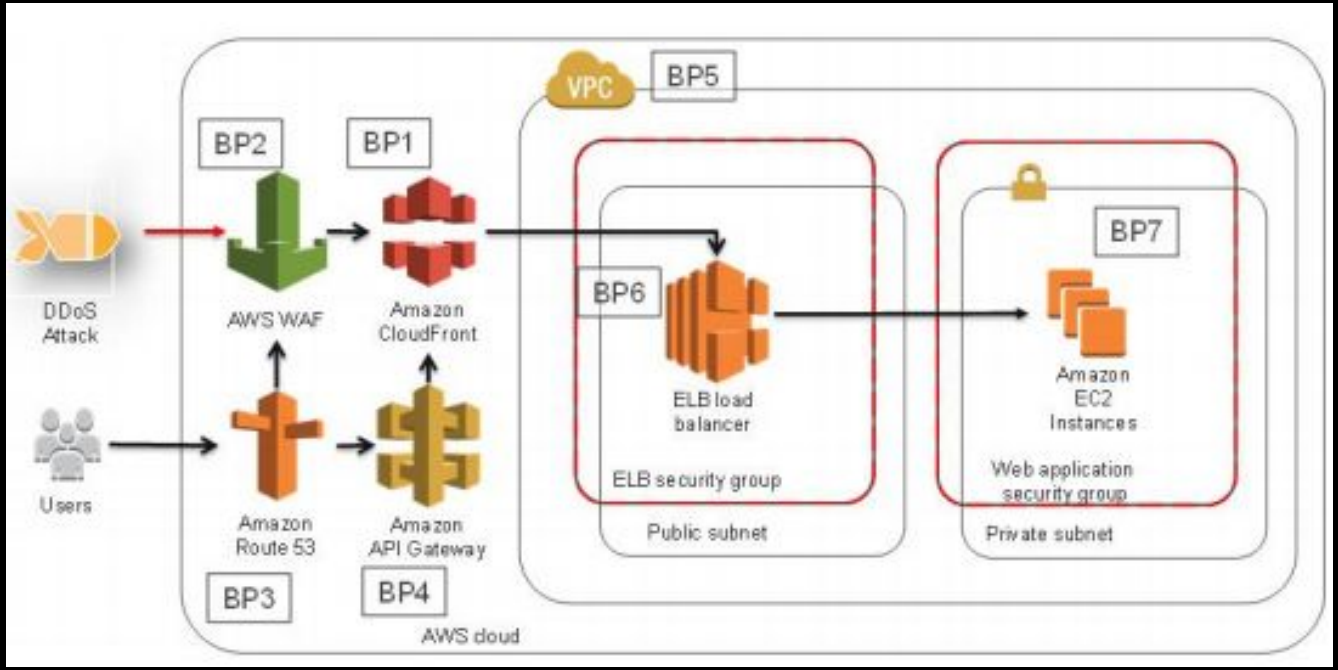
WAF architecture on AWS - Traditional architecture

Traditional architecture - problems



WAF architecture on AWS - AWS best practices

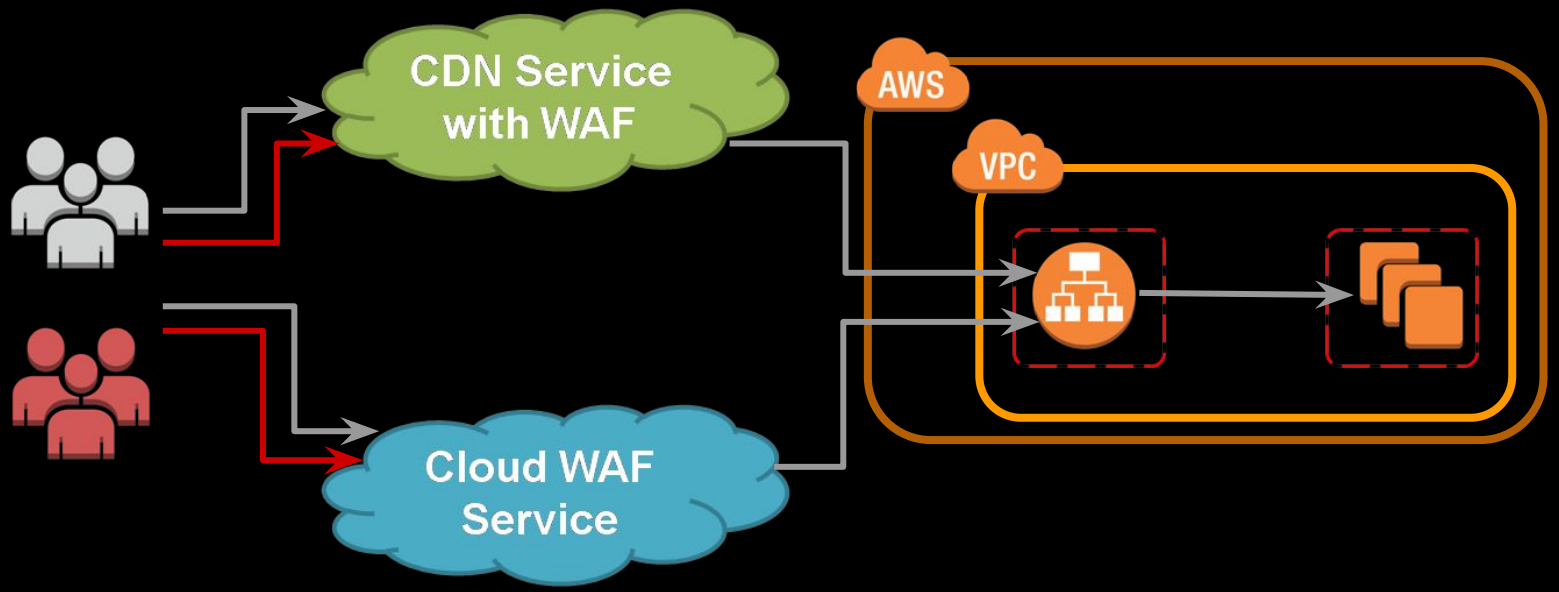
AWS best practice



Reference: AWS Best Practices for DDoS Resiliency (June 2016)

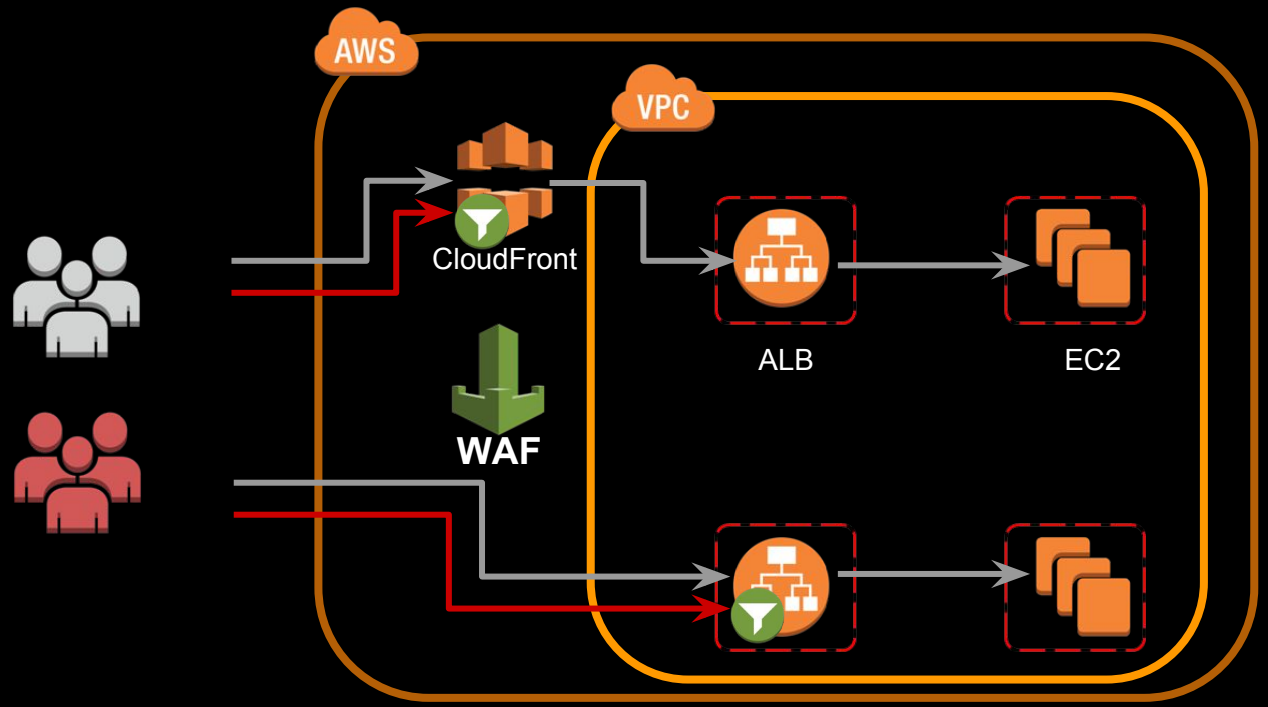
WAF architecture on AWS - Cloud service

Architecture working with cloud service



WAF architecture on AWS - AWS WAF

Architecture - AWS WAF



Comparisons

Comparisons - Meet OWASP

Traditional architecture

1. 使用高度自行客製化的rule。
2. 使用品牌產品自帶的rule。

Working with cloud service

1. 上限和下限完全取於服務供應商

Working with AWS WAF

1. AWS WAF請參考Use AWS WAF to Mitigate OWASP’s Top 10 Web Application Vulnerabilities

Comparisons - Meet compliance

Traditional architecture

1. 調整rule的彈性大，對於服務供應商的依賴性小。
2. 品牌產品能產出Compliance report，減少對應稽核的負擔。

Working with cloud service

1. 上限和下限完全取於服務供應商的服務 內容。

Working with AWS WAF

1. AWS WAF底層直接符合PCI，但是Rule的產出與改善... 是使用者的責任。
   (AWS shared responsibility model)

Comparisons - Maintain & automation

Traditional architecture

1. 學習的時間成本，需要維運者有較高的技術 /溝通能力。
2. 複雜的架構，管理複雜度必然增加。
3. 難以自動化，須熟悉特定廠商的 API/Command。

Working with cloud service

1. 架構單純，維運難度較低。
2. 難以自動化，須熟悉特定廠商的 API/Command。

Working with AWS WAF

1. 架構單純，維運難度較低。
2. 學習一套API打天下。

Comparisons - Pricing

Traditional architecture

1. 養機器 = 貴
2. 專業的維運 = 貴
3. 使用知名品牌 = 貴
   (License fee $1~3 hourly)

Working with cloud service

1. 不需搭配CDN的專業Cloud WAF，假如包含professional service的話價格必然貴。
2. 搭配CDN的類型必須先購買 CDN服務，再購買 WAF模組。

Working with AWS WAF

1. AWS WAF有較低的起始費用，同時也支援 CF & ALB來賦予使用者選擇架構的彈性。
   ($5 per web ACL, $1 per rule, $0.60 per million requests)

Demo

Demo

SQL Injection Protect

XSS Protect

Rate based rule

CVE 2017-5638: Strust2

Summary

Summary

1. 把WAF套進架構不是問題，如何Tuning rule才是問題。
2. 對應適合的場景/能力，使用適合架構。
3. 程式有洞就要補... 不要推給資安設備!
4. 如果有用CloudFront/ALB的，
   馬上試試看AWS WAF能幫你攔到多少東西!

Wishlist

透明的SQLinj, XSS規則清單。

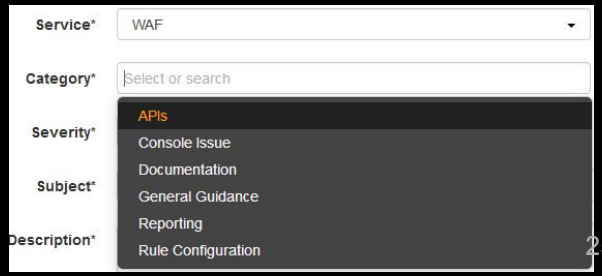
~~String match支援**Regular Expression**~~
(Oct 16, 2017 update “AWS WAF Now Supports Regular Expressions” https://goo.gl/kCdfgq)

Rate-based rule的**取樣單位是5分鐘**，希望可以自由讓使用者調整。

Log只能看到**最近3小時**，最好能夠儲存log到S3/Cloudwatch Logs。

Rules per web ACL只能有**10條**...

更多的Feature…
(Support case分類居然沒有feature request...)



References

- AWS Security Blog
  https://aws.amazon.com/blogs/security/
- AWS WAF Developer Guide
  http://docs.aws.amazon.com/waf/latest/developerguide/waf-chapter.html
- AWS WAF Preconfigured Rules & Tutorials
  https:
- //aws.amazon.com/waf/preconfiguredrules/AWS Security Whitepaper
  https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- AWS Security Best Practices
  https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf
- Overview of AWS Security - Network Security
  https://d0.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf
- AWS Best Practices for DDoS Resiliency Whitepaper
  https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf


thank you
danke
謝謝
ngiyabonga
شكراً جزيلاً
teşekkür ederim
gracias
спасибо
рахмат
Баярлалаа
bedankt
dziękuję
obrigado
merci
go raibh maith agat
sukriya
kop khun krap
grazie
arigatô
takk
dakujem
merci
terima kasih
감사합니다
ありがとう
ευχαριστώ
tapadh leat
mauruuru
hvala
sagolun
taiku
mochchakkeram
dank je
blagodaram
faafetai lava
kiitos
dankie
dhanyavad
köszönöm
gràcie
bayarlalaa
enkosi
nanni
nandri
vinaka
спасибі
misaotra
matondo
paldies
grazzi
mahalo
spas
mersi
kia ora
barka
welalin
tack
хвала
asante
manana
obrigada
murakoze
tenki
djiere dieuf
tau
akun
dankon
aciù
дякую
mamnun
chnorakaloutioun
gràcies
sulpáy
sobodi
dèkuji
mèsi
didi madloba
najis tuke
kam sah hamnida
তোমাকে ধন্যবাদ
rahmat
tanemirt
rahmet
diolch
dhanyavadagalu
shukriya
merce
мерси
trugarez
xiexie