
By fladnaG (Max)
Protecting web applications with FOSS…
Cancel

MyComputer

Media Player

MyDocuments

Internet Explorer

eMail

Trash

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

Who is this?

Address https://federal.network/

FEDERAL GALAXY TOP NEWS ENLIST EXIT

- **Max {fladnaG},**

  Security Architect at **Comect.fr**,

  - French company providing decentralized identity-based solutions called **myDid** (mydid.com)
  - New decentralized tools to create communities, rewards, tickets, open badges and ID wallets through Decentralized Identifiers and Verifiable Credentials (new W3C standards!)

« Would-you like to know more ? » ™
please contact me after the presentation

comect myDid

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

What are we going to talk about?

Address https://github.com/fladna9/protectingwebapp

- What is a reverse proxy?
- What is a WAF (Web application firewall)?
- Example case: what we needed
- Benchmarking solutions
- Adding fail2ban to WAF triggers

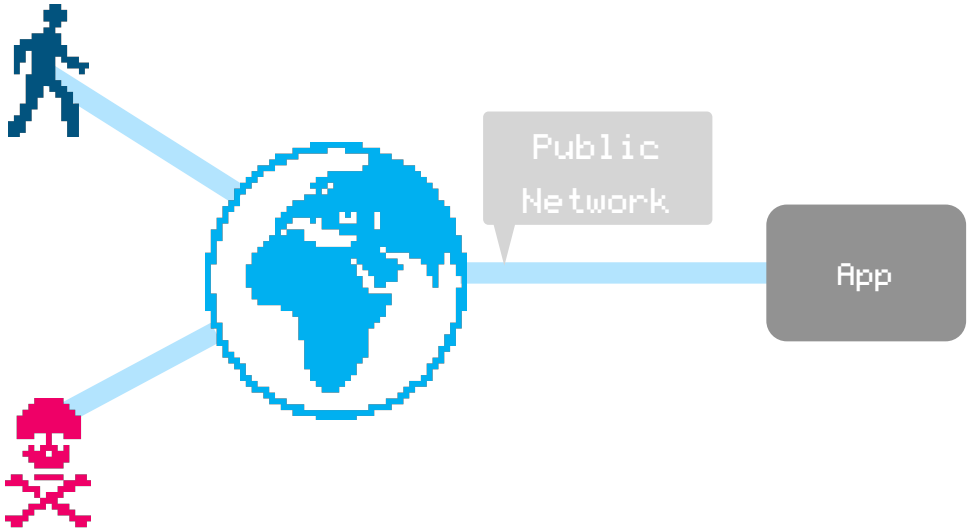
Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

What is a reverse proxy?

What is a reverse proxy?

Let's **not** expose our apps on the interwebs.

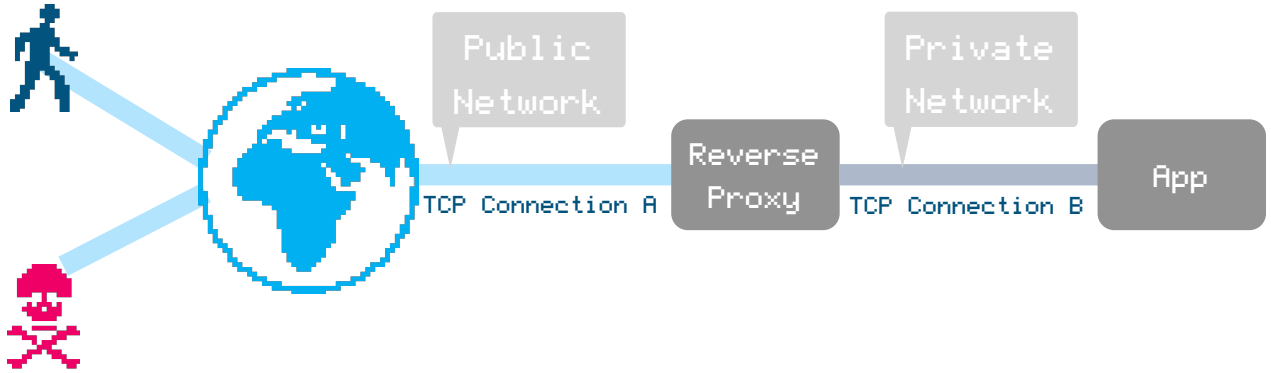
Risks: not easy to load balance or cache, security considerations, SSO authentication…



What is a reverse proxy?

- Allows external users to **indirectly access** instances of apps in a private network.
- Like 'HTTP routing'. But not exactly, as it creates a new TCP connection to your application. Depending on available instances, load, and requested app, the reverse proxy will "route" the request.

NB: A reverse proxy can or cannot be a TCP endpoint (by extension, a TLS endpoint). Transparent reverse proxies are some special kind, and not the kind we're interested in this talk.



What is a reverse proxy?

- On the load balancing side:
  - **Multiple instances** of the same app,
  - **Load balance** by desired metric: CPU load, network usage, load average, etc.

- On the cache side:
  - Since the reverse proxy is "in the middle" of the communication, **easy to cache responses** to users for further use *(but careful about what can be cached, and what can't, with Cache-Control HTTP headers)*.

- On the security side:
  - It **isolates** your web app from internet "background noise",
  - It allows you to keep web apps in **private address space** (that is, in a private network),
  - Wouldn't be a great idea to "check" here, like a customs control point, **attacks from the outside world**?
    Let's talk about that a bit later.

Reverse proxies

- Apache HTTPd Server - Apache Software Foundation (since 1995)
  - FOSS web server
- Nginx (engine X) - Nginx, inc. (since 2004)
  - FOSS web server
- Both are good, both work well as web servers. They can also act as reverse proxies… but some other projects are handling much more as reverse proxy.

HAProxy (High Availability Proxy)

Software Load Balancer & Application Delivery Controller

- Free Open-Source software, using the "community" edition.

- A well-known Reverse Proxy made for heavy loads
  - Load balancing
  - High availability
  - Works at HTTP level or TCP level (for example, reverse-proxying RDP, SSH, IMAP, SMTP, whatever)
  - Used by MANY big companies
    - Go Daddy, GitHub, Bitbucket, Stack Overflow, Reddit, Slack, X/Twitter, Amazon OpsWorks, …
  - 6-8 CPU cores = 200K-500K requests/second

SPOE, SPOA, SPOP

Extend the functionalities of HAProxy with external apps

- SPOE : Stream Processing Offload Engine
  - Filter communicating with external components called SPOA, Stream Processing Offload Agent.
  - Communication between the Engine and the Agent with SPOP, the Stream Processing Offload Protocol (above TCP). It is an in-house binary protocol, still it is Free and Open-Source.

- More info about SPOE, SPOA and SPOP here:
  https://github.com/haproxy/haproxy/blob/master/doc/SPOE.txt

What is a reverse proxy?

Address https://github.com/fladna9/protectingwebapp

What is a web app firewall aka WAF?

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

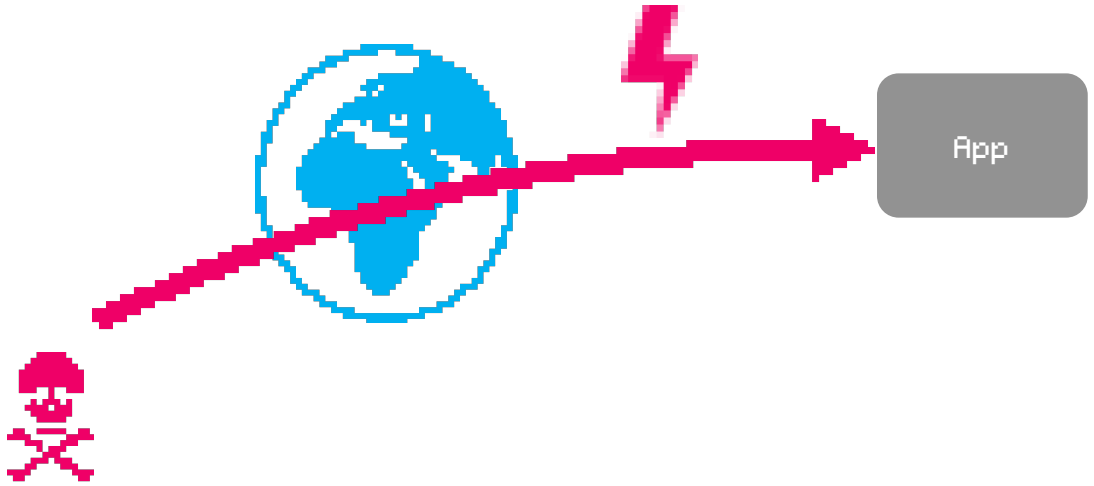
So, what is a WAF?

Last security line of defense before application code

- Rules
  - Can be circumvented obfuscating the attack, if the rules are not updated frequently…
  - They are some good Free open-source rules…
- Protocol enforcement
  - Checking type, length of parameters, headers, POST content, etc.
  - Not too bad, but again, lax rules can be circumvented.
- AI… Closed AI® ChatHQU® high speed cyber-detection
  - That is to say, machine learning. It works… but, as usual with this tech:
    - Hard to train (what is a good/bad request)
    - What happens if there's an attack during learning?
- **NOTHING PREVENTS MORE A WEB ATTACK THAN GOOD CODE.**
  WAF is only a failsafe.

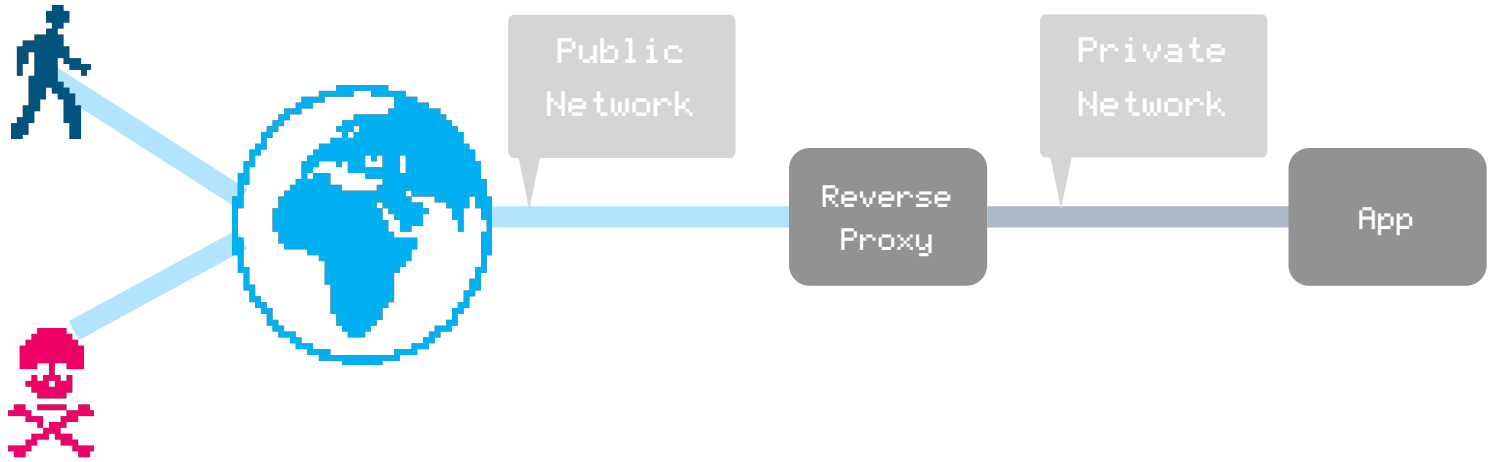
So, what is a WAF?

Without reverse proxy nor WAF



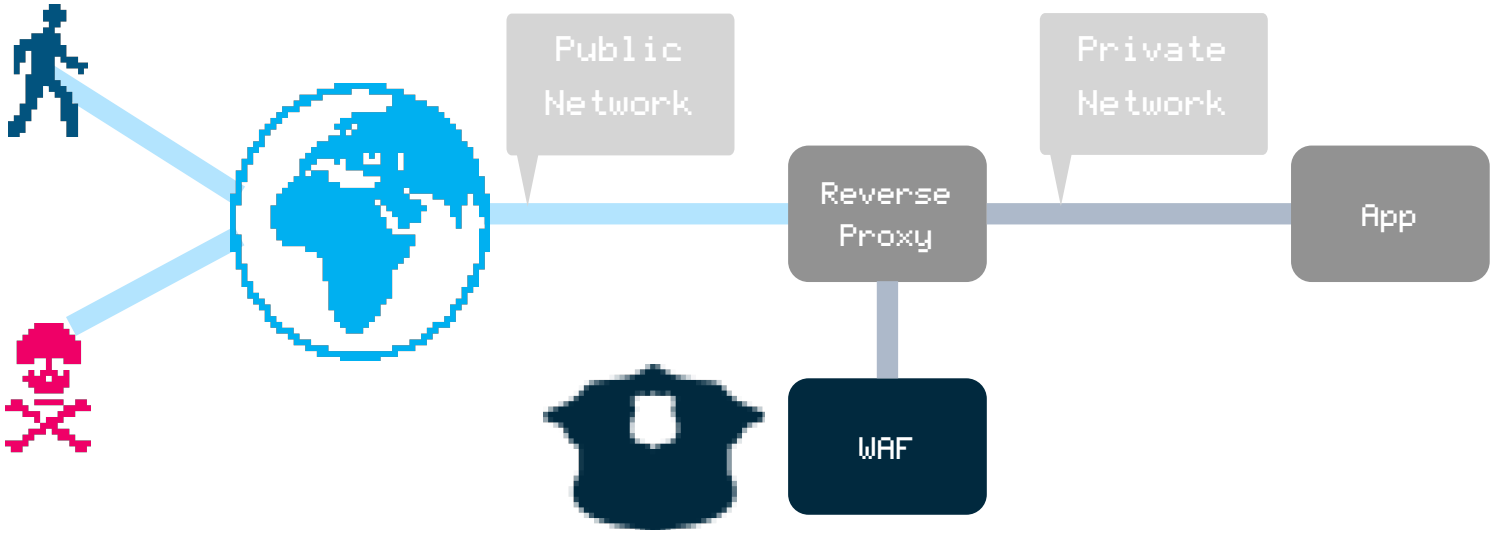
So, what is a WAF?

With a reverse proxy but without WAF



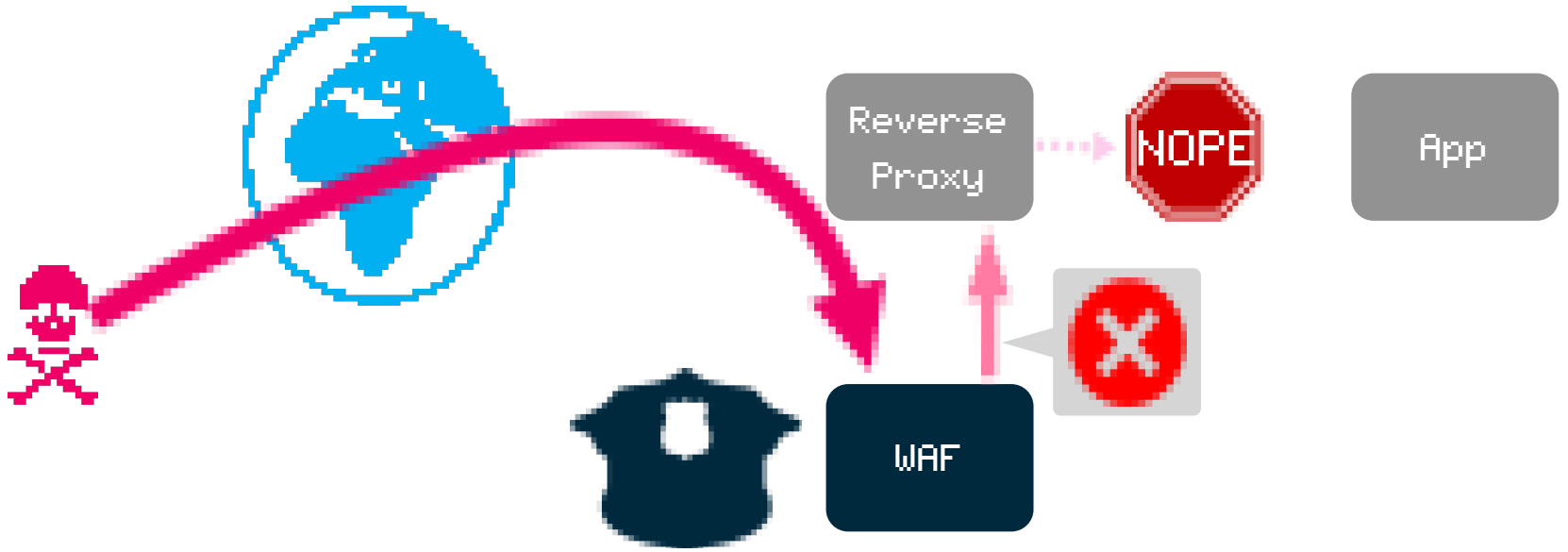
So, what is a WAF?

With a reverse proxy and WAF



So, what is a WAF?

With a reverse proxy and WAF



So, what is a WAF?

Things to consider

- One good rule to put in the reverse proxy is:
  `if [[ -z "$WAF" ]]; then exit 403; fi`
  Or: block if WAF not responding

- The WAF is then a Single Point of Failure (SPoF).
  - So you need a resilient one.
  - And multiple instances of it.

- Stress testing a Reverse Proxy + WAF solution is interesting, as it may show that some solutions are not suited for heavy loads…

What WAF?

Solutions

- Of course big names are here
  - Imperva, Cisco, ^Forti.*$, Stormshield, IBM…
  - Costs a lot, I have no money.
  - Compatibility with HAProxy depending on vendor.

- Cloudflare
  - Well known reverse proxy + WAF in the clouds® as a service
  - Not so expensive, but…
  - … Hello NSA / PRISM / Cloud Act / whatever -_-'

What WAF?

OWASP CoreRuleSet (CRS)

CRS

- Free open-source rules!
- Generic attack detection rules!
  - Many rules for many attack types *(SQLi, XSS, LFI/RFI/Path traversal, PHPi etc.)*
- Heavily maintained <3
- Sometimes false positives…
  - …but can be “patched” with custom whitelists.
- Not perfect but should detect and block most generic attacks.

What WAF?

FOSS CRS engine solutions that can be SPOA-ed

- **OWASP Mod_security2 (mod_security3 is not SPOA-compatible yet)**
  Old and well-known FOSS WAF engine
  Initially developed by Trustwave, now by OWASP
  - Active development for mod_security2
  - No longer in active development for the SPOA part
  - C lang
  - Compilation needed (**and OH BOY THIS IS NOT EASY**)
  - Compatible with OWASP CoreRuleSet version **3**

- **OWASP Coraza (means Armor/Breastplate in español)**
  *Brand new FOSS WAF engine to replace mod_security**
  - Active development (both the project and SPOA part)
  - Go lang
  - Compilation needed (and this one is so easy, thanks Golang!)
  - Compatible with OWASP CoreRuleSet version **4**

Bench tool

Address https://github.com/fladna9/protectingwebapp

Benchmark tool

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

Let's benchmark, but with wut?

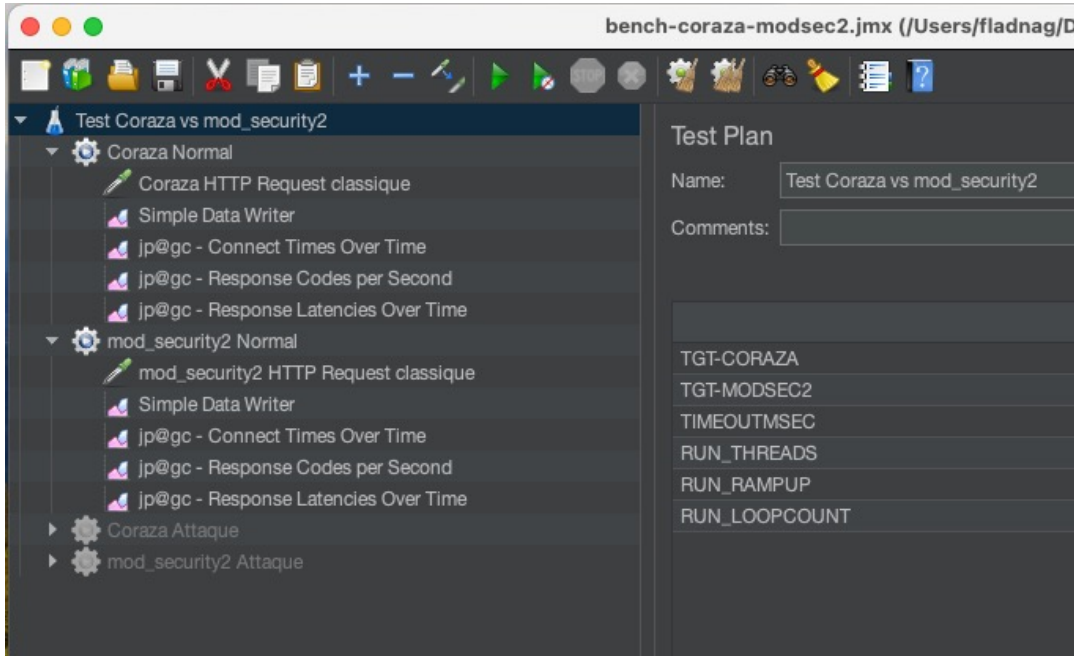
Autonomous Platform & Remote Operations (AP&RO)

- 2 devices 1 case
  - OpenWRT WiFi 6 router w Gigabit Ethernet
    - ARM 1.2Ghz (4 cores)
    - 512 MB RAM DDR3L
  - Mini server
    - AMD Ryzen 5 5500U (6 cores, 12 threads)
    - 64GB RAM DDR4
    - 2TB SATA SSD
    - Proxmox Virtual Environment 8
- With a screen, small keyboard, 100W power.
- If you don't speak no French:
  AP&RO = Apéro = Aperitif ;)
  I'm a self-certified AP&RO specialist :D

Let's benchmark, but with wut?

Stress test tool : Apache JMeter

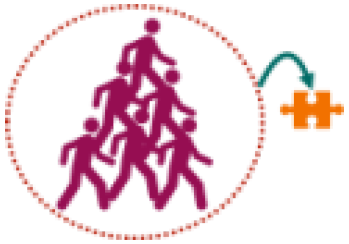
- IDE to configure.
- CLI to run, deployable to a server.
- Automagically generates results, graphs, etc.
- Easy to use.



Let's benchmark, but with wut?

Stress test parameters

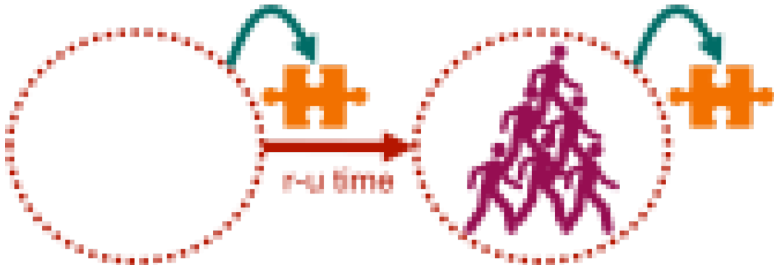
- Same tests on all platforms : **1 000 000 requests in a small period of time.**
- App is a simple HTML file running on Apache2, like a standard website.
- All VMs configured the same : **2 cores, 4GB RAM.**
- Let's start with recommended configuration for each, then we'll experiment.
- Multiple runs to lessen statistical errors.
- Since its all on a local network : **timeout is 1 second.**



Threads

Simultaneous users

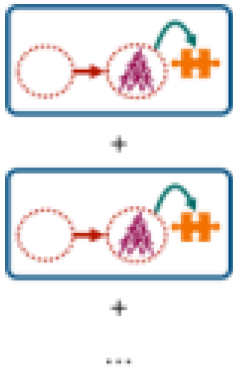
Here: 1 000 users



Ramp-up time

From 0 to 1 000 users

Here: 10 seconds



Loop count

How many iterations

Here: 1 000 loops

Benchmarks! Benchmarks! Benchmarks! Benchmarks! Benchmarks! Benchmarks! Benchmarks! Benchmarks!

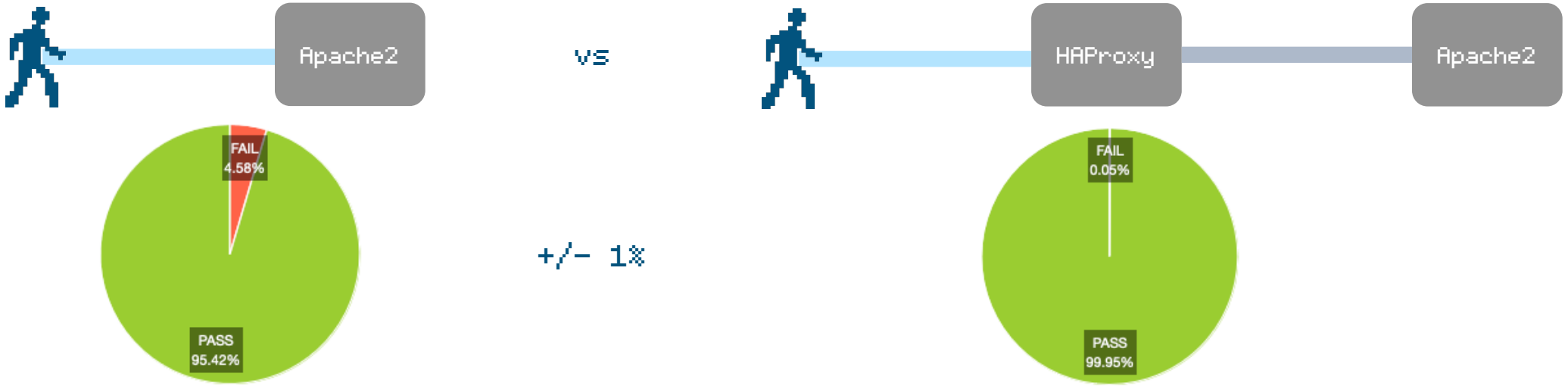
Address https://github.com/fladna9/protectingwebapp

Benchmarks! Benchmarks! Benchmarks!

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

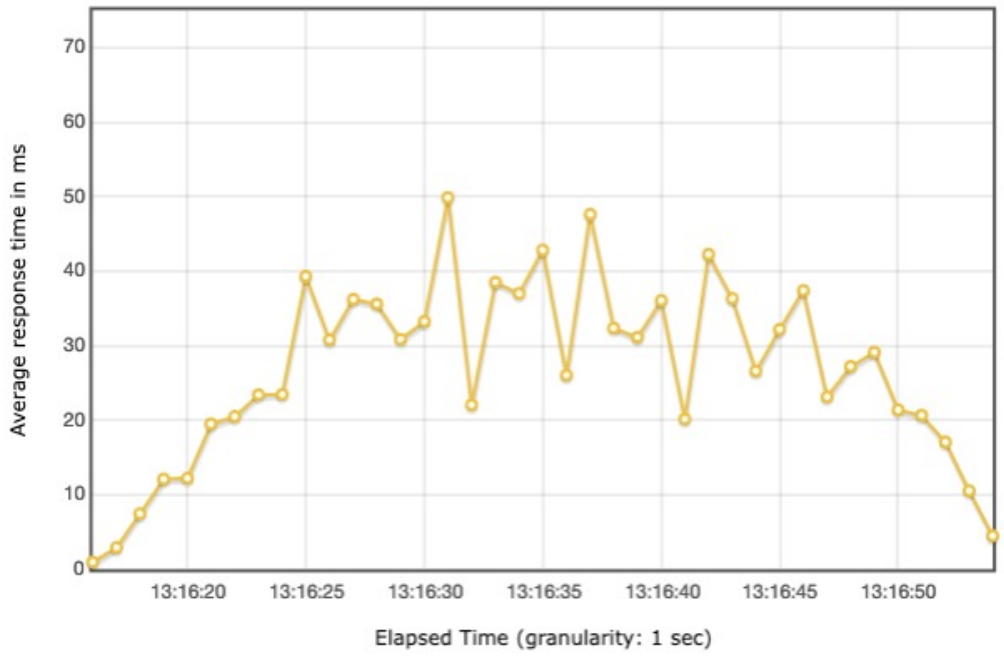
Let's benchmark!

Run 1 - Bare Apache2 vs HAProxy in front of Apache2 (no WAF)



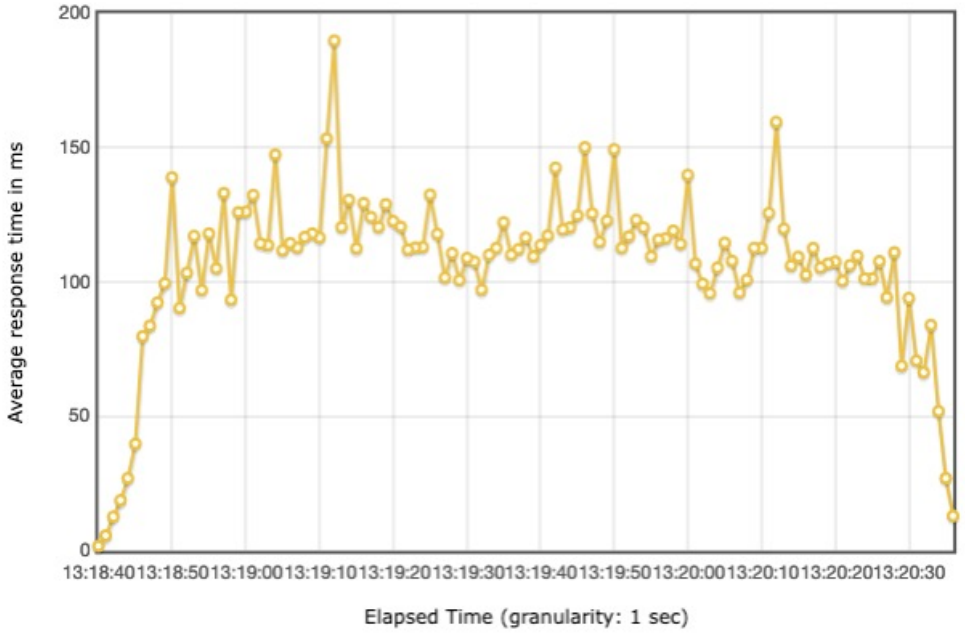
Let's benchmark!

Response time



Apache2

40 seconds

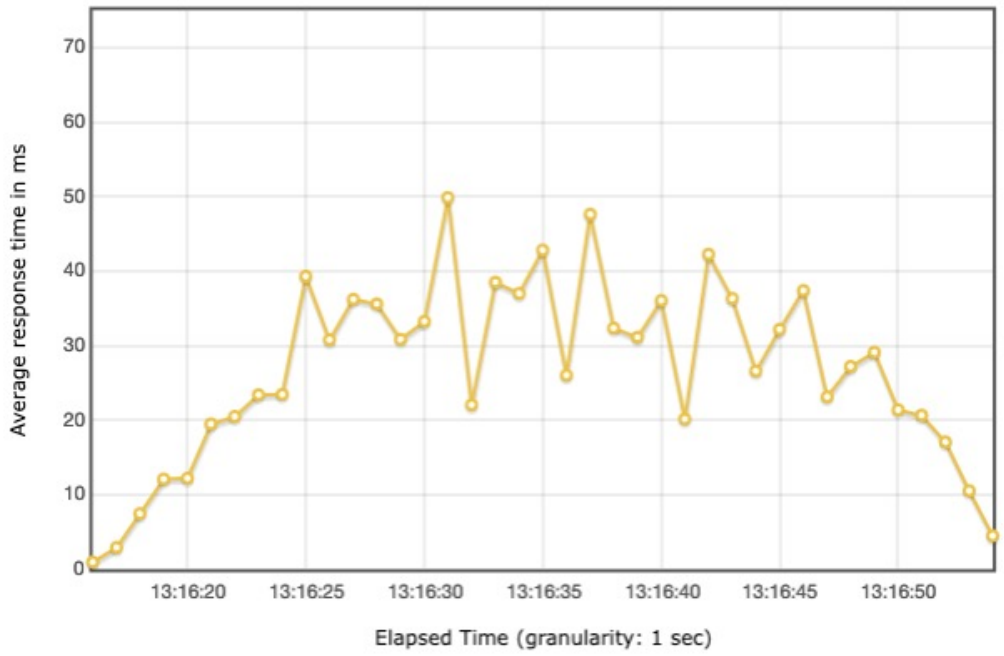


HAProxy

120 seconds

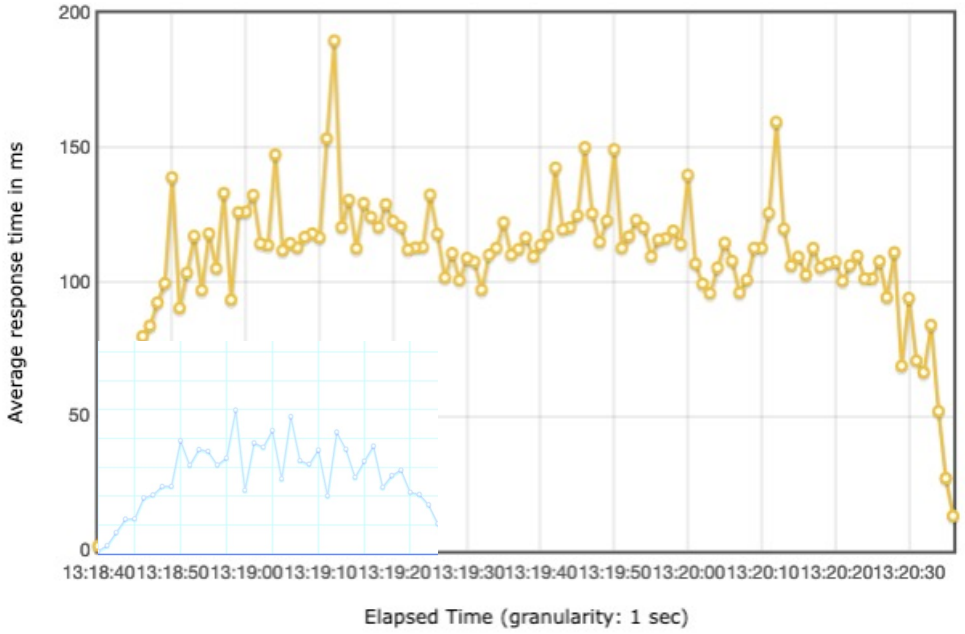
Let's benchmark!

Response time



Apache2

40 seconds



HAProxy

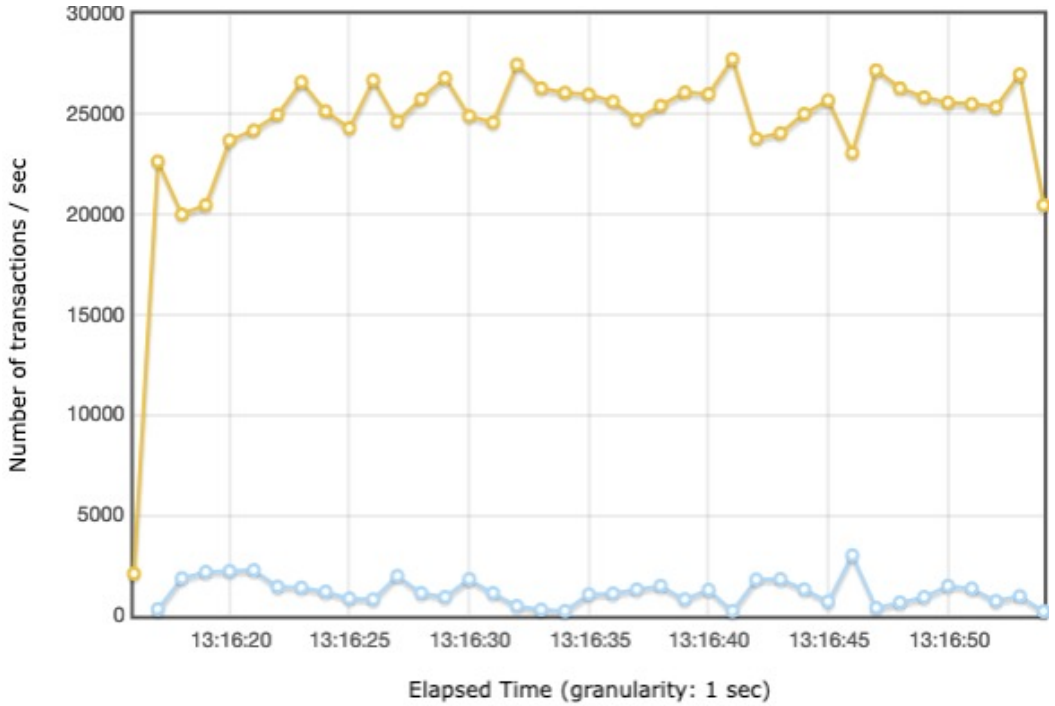
120 seconds

Benchmarking 1 - Apache2 vs HAProxy

Address https://github.com/fladna9/protectingwebapp

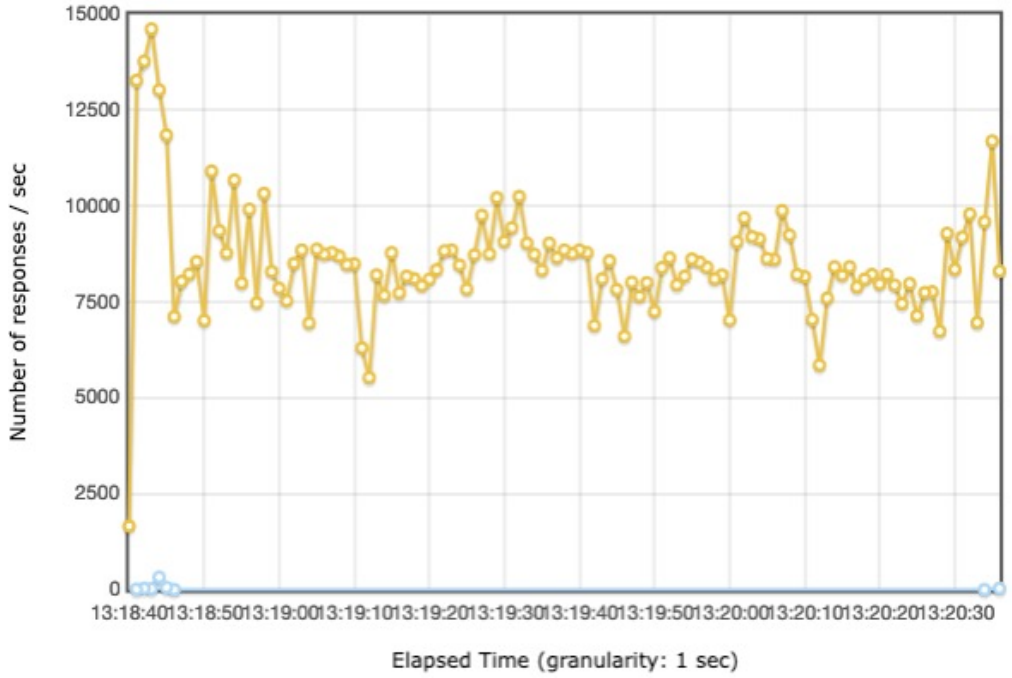
Let's benchmark!

Response type - yellow is OK



Apache2

40 seconds



HAProxy

120 seconds

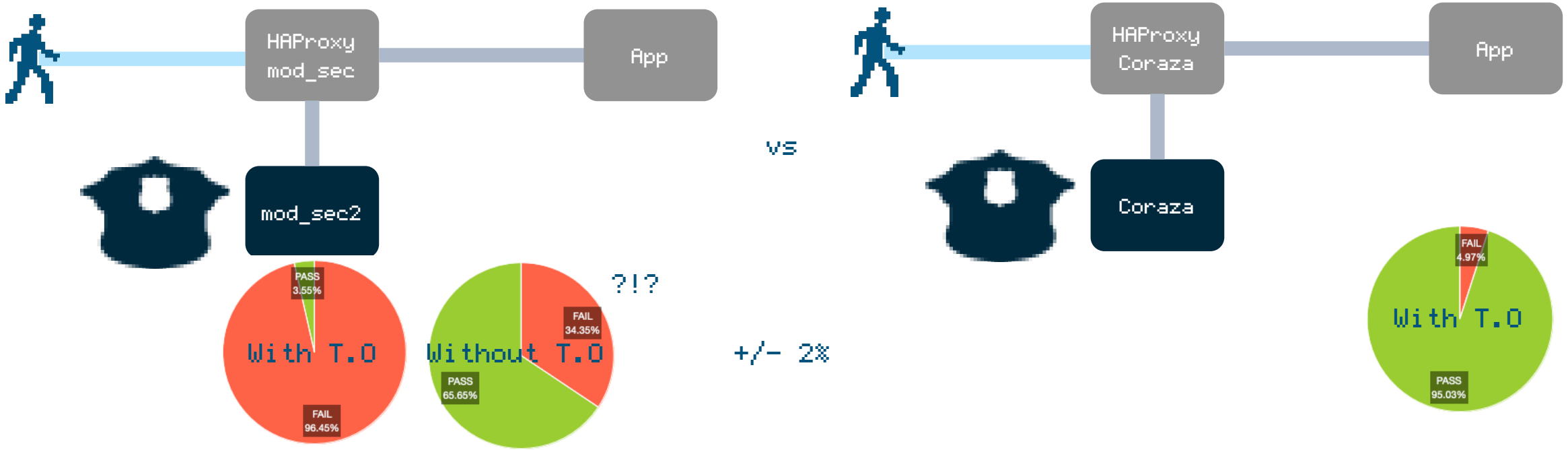
Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

Benchmarking 2 - mod_security2 vs Coraza - editor config.

Address https://github.com/fladna9/protectingwebapp

Let's benchmark!

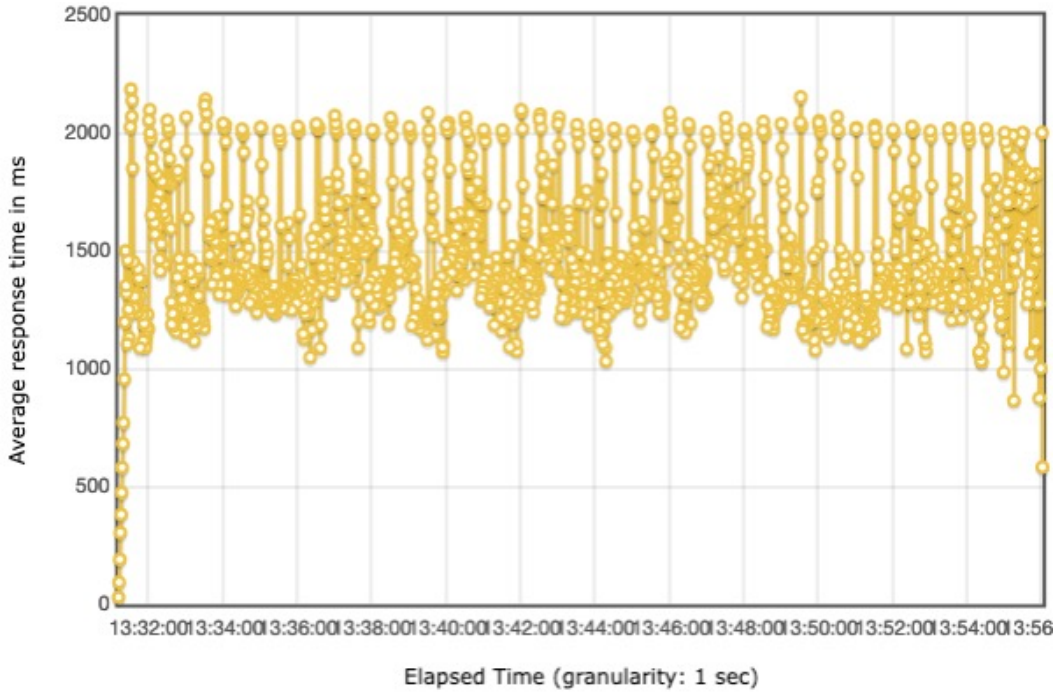
Run 2 - HAProxy+mod_sec2 vs HAProxy+Coraza - editor config.



Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

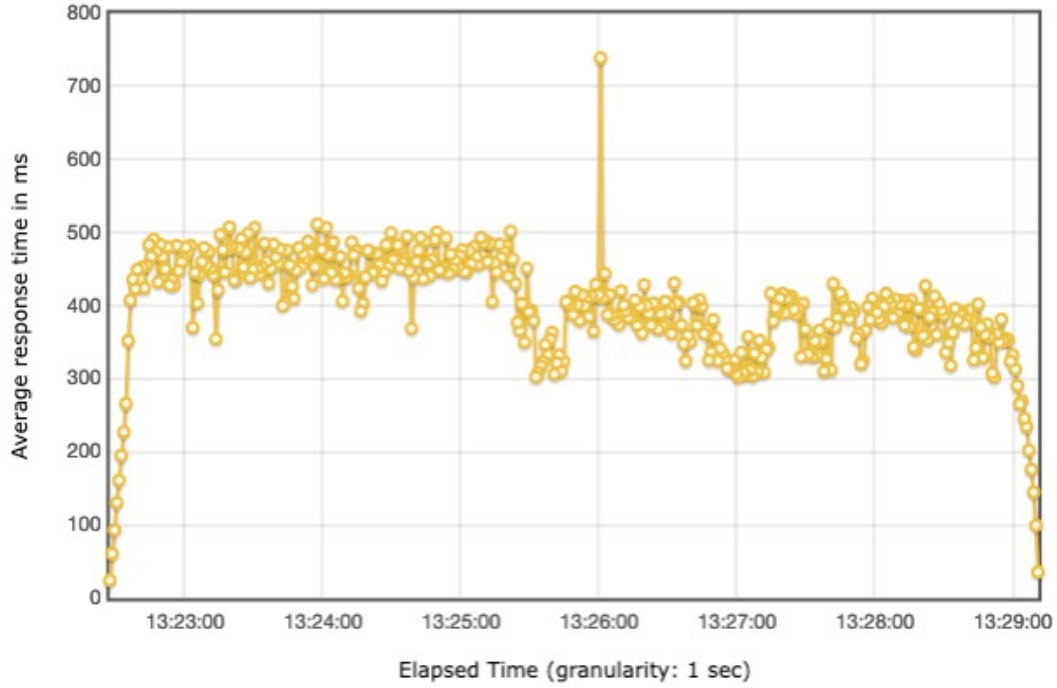
Let's benchmark!

Response time without timeout



mod_security2

about 5 minutes

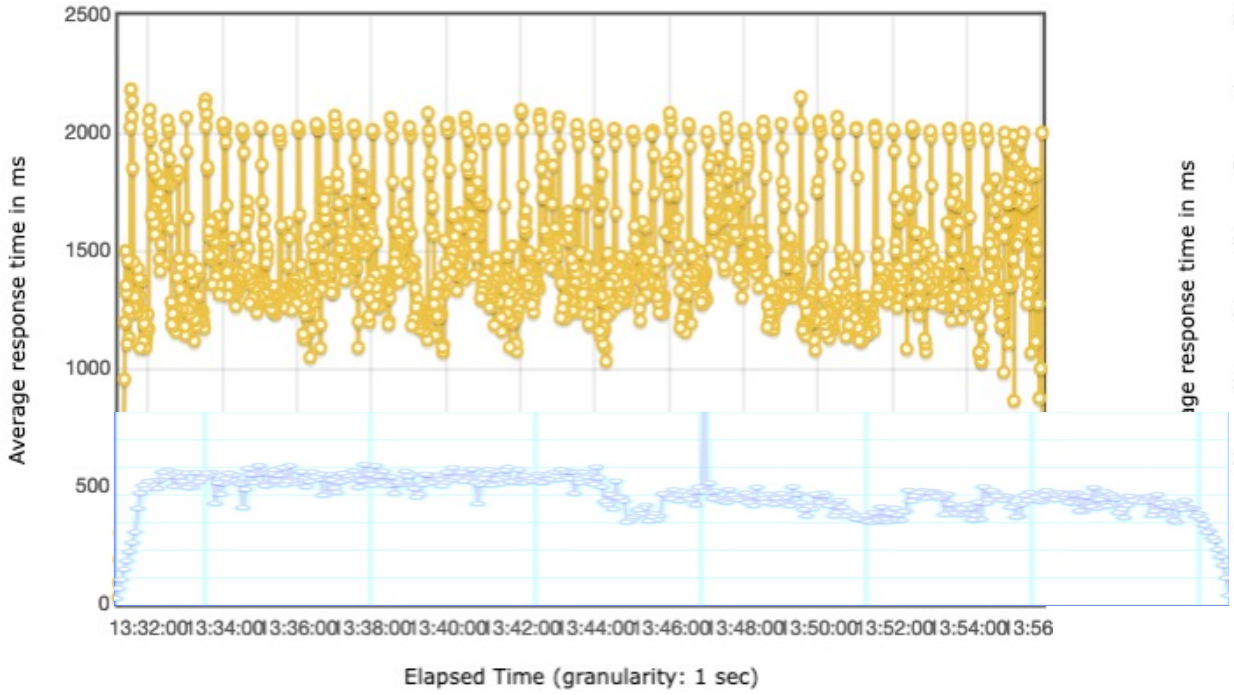


Coraza

about 7 minutes

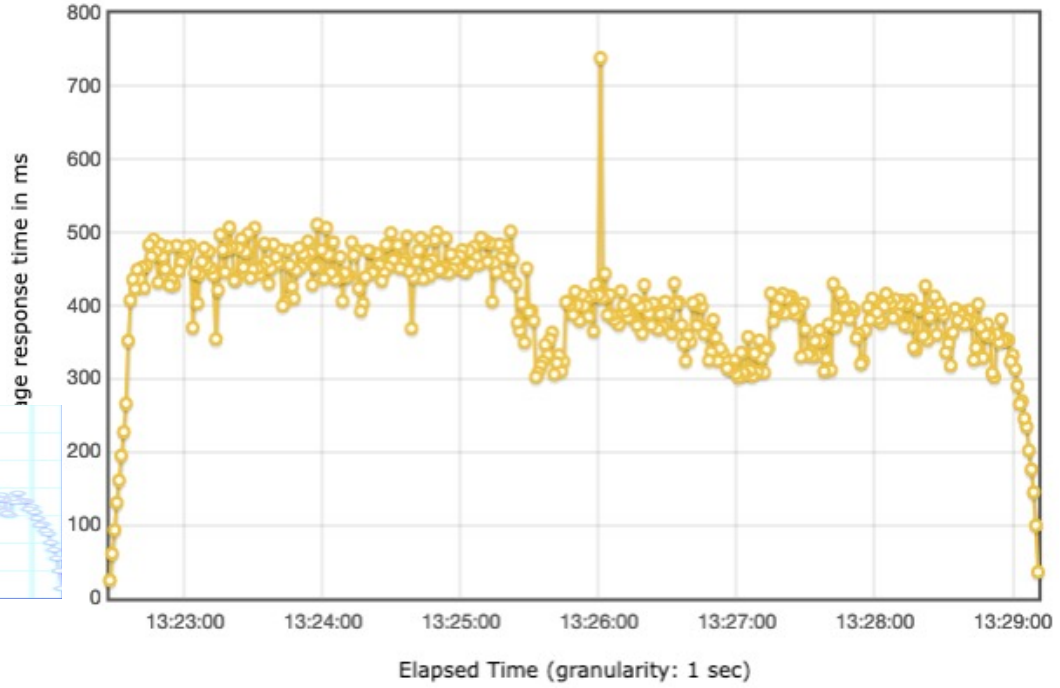
Let's benchmark!

Response time without timeout



mod_security2

about 5 minutes

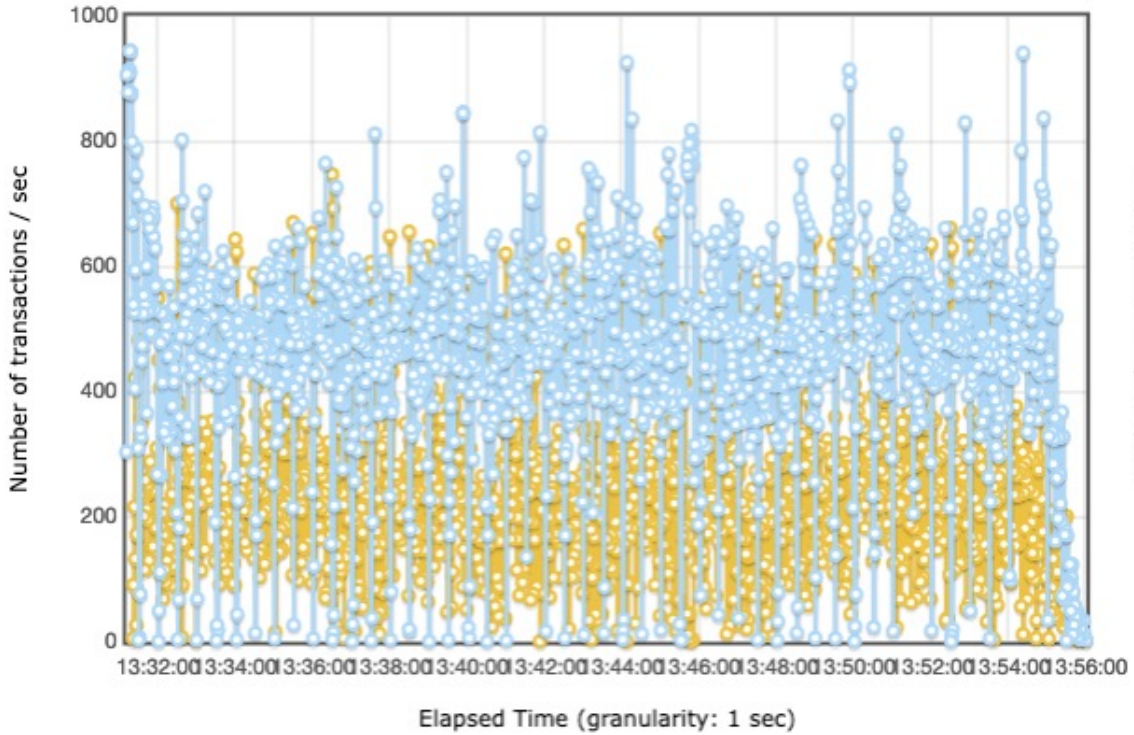


Coraza

about 7 minutes

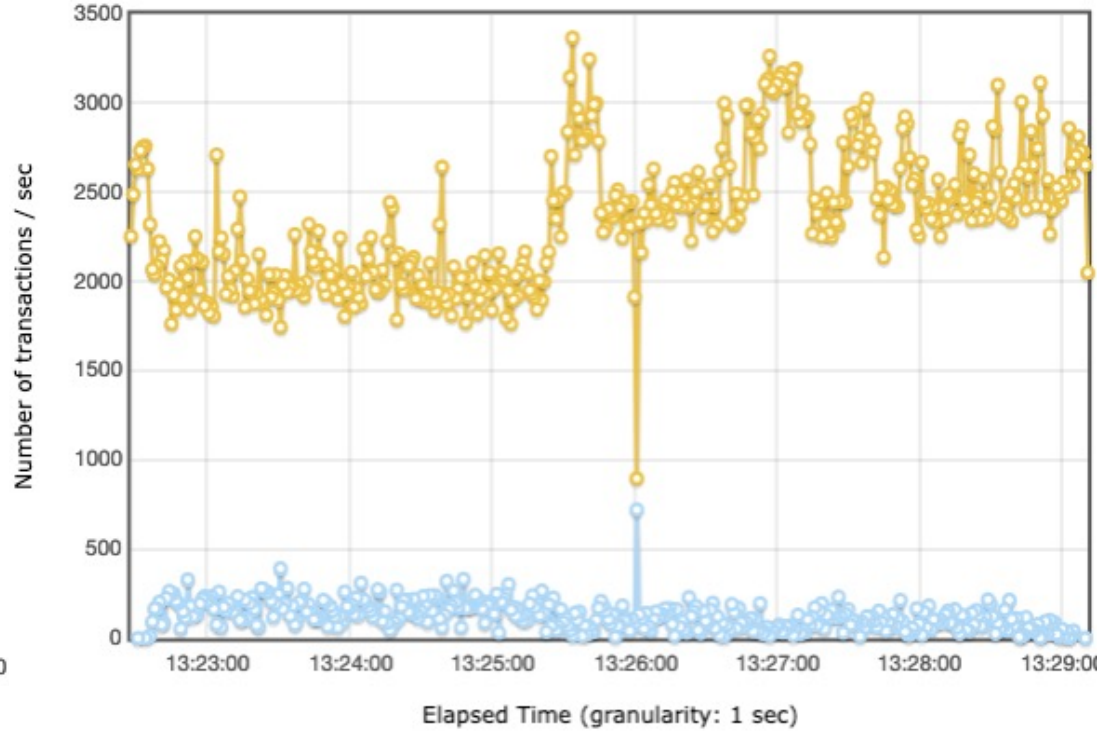
Let's benchmark!

Response type without timeout - yellow is OK



mod_security2 (Blue is OK, *dunno why it changed*)

about 5 minutes

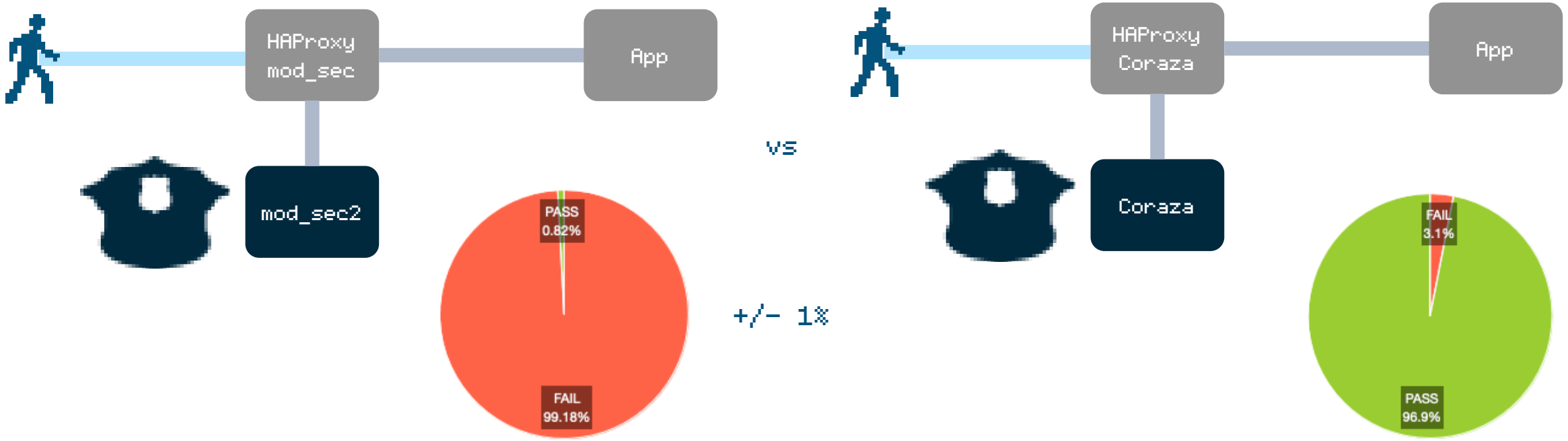


Coraza (yellow is OK)

about 7 minutes

Let's benchmark!

Run 3 - HAProxy+mod_sec2 vs HAProxy+Coraza - fixed config.

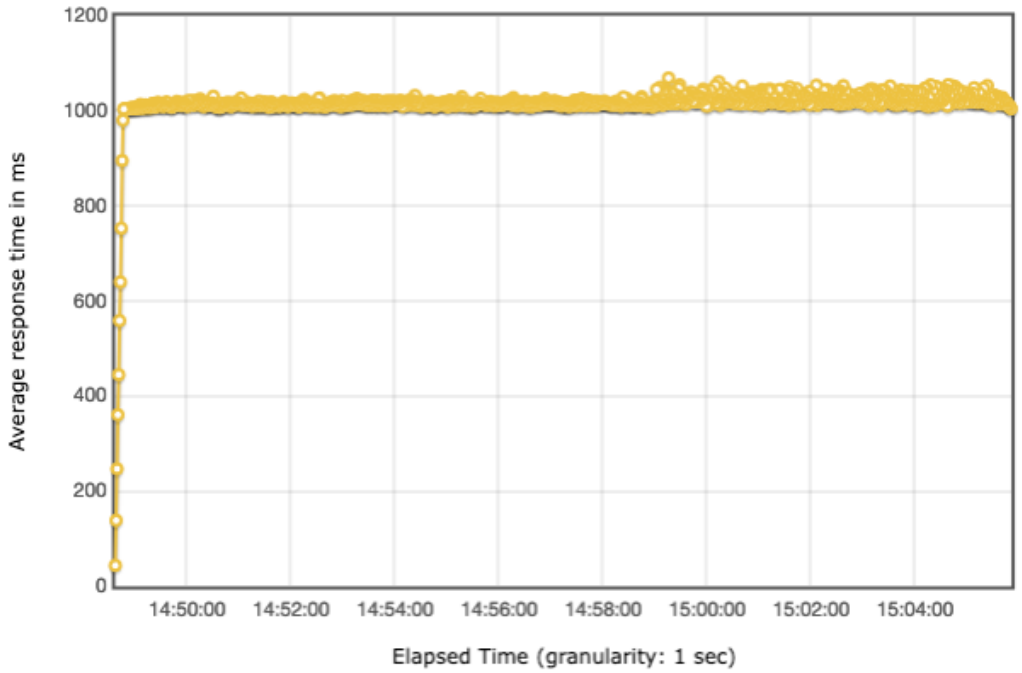


Benchmarking 3 - mod_security2 vs Coraza - fixed config.

Address https://github.com/fladna9/protectingwebapp

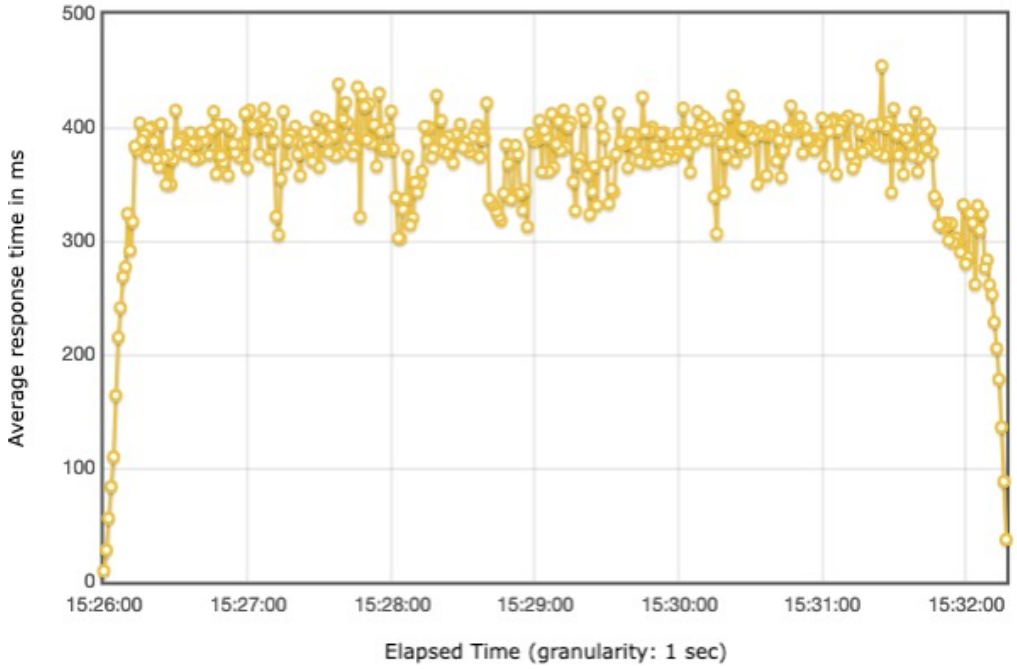
Let's benchmark!

Response time



mod_security2

about 5 minutes



Coraza

about 6 minutes

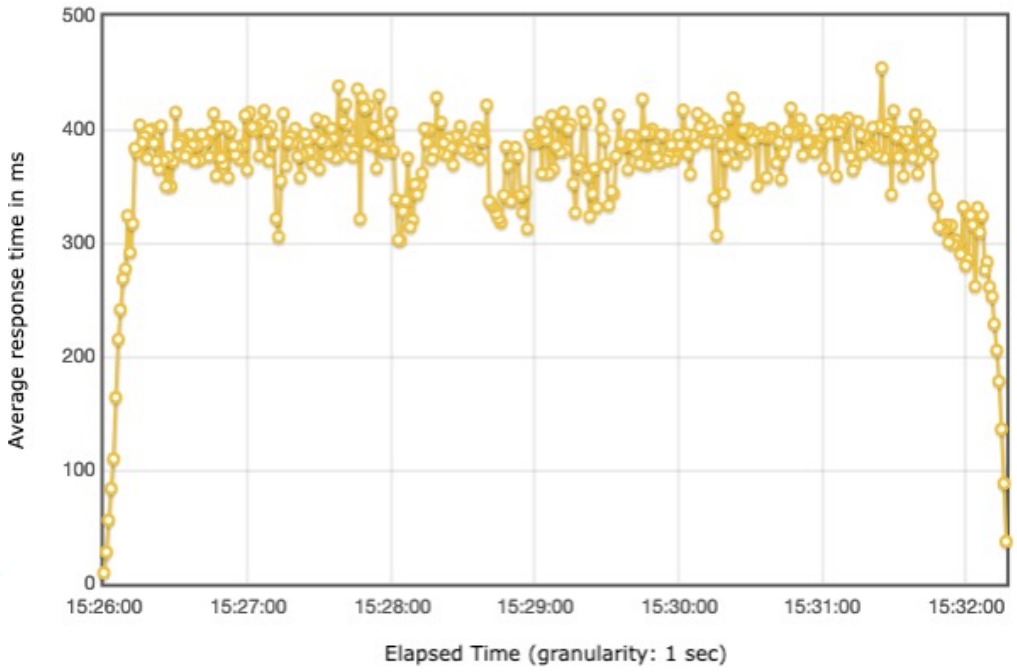
Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

Let's benchmark!

Response time

mod_security2

about 5 minutes

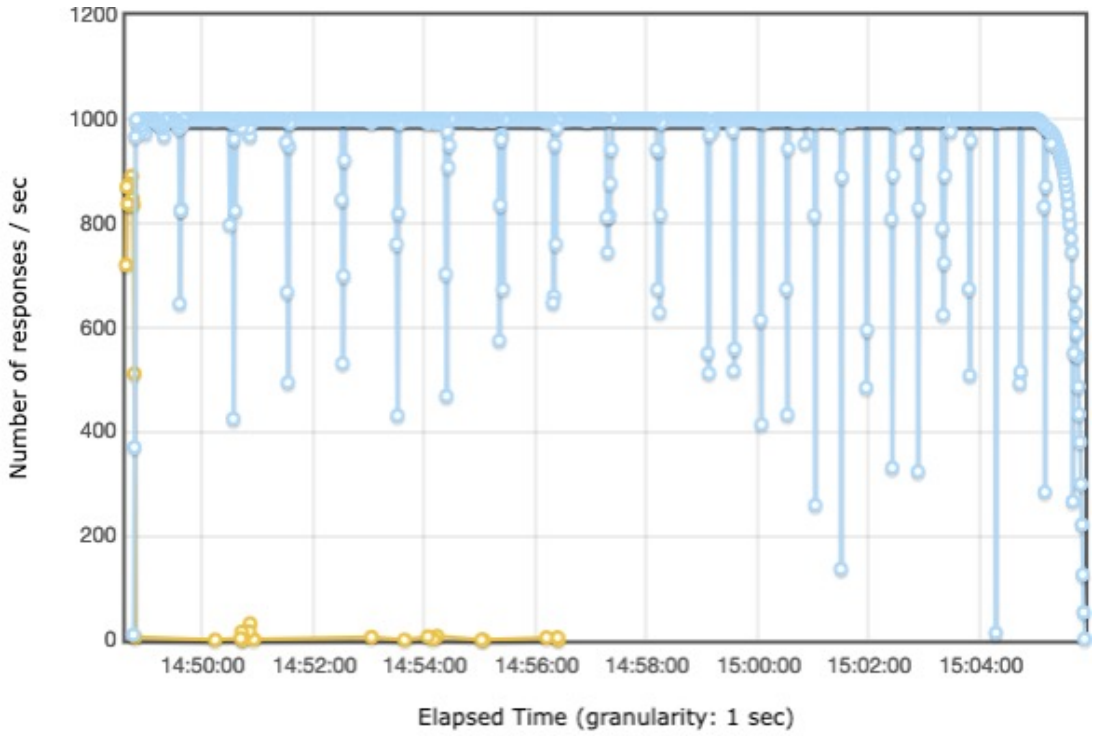


Coraza

about 6 minutes

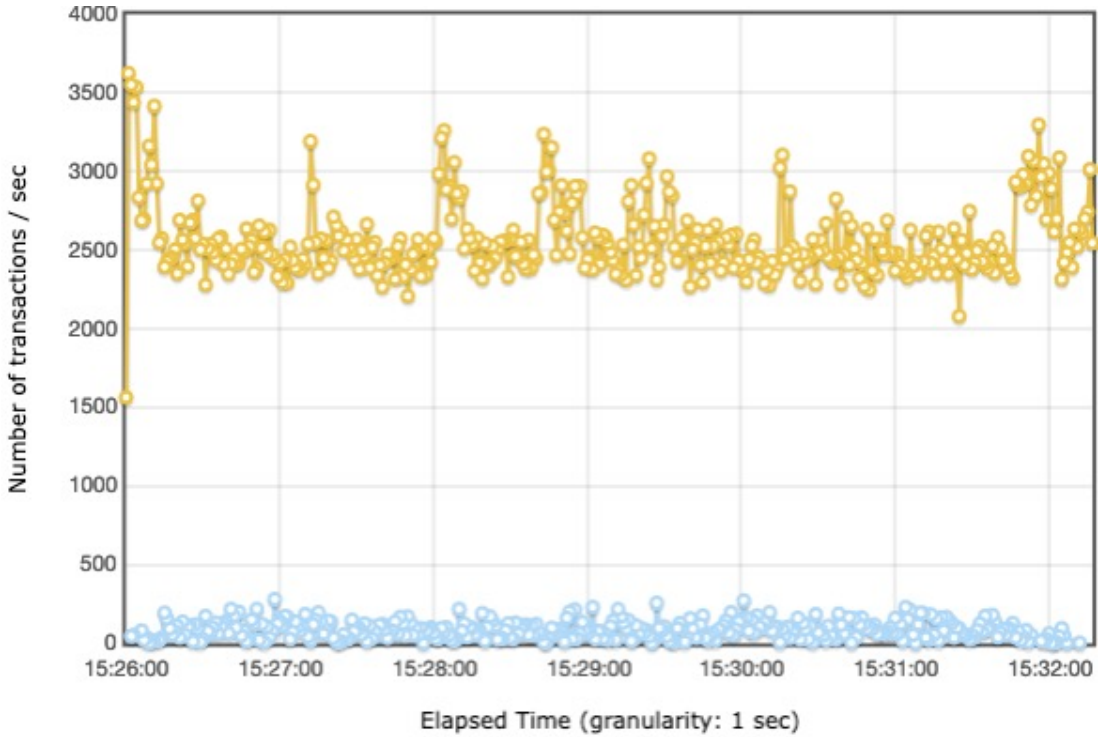
Let's benchmark!

Response type - yellow is OK



mod_security2

about 5 minutes

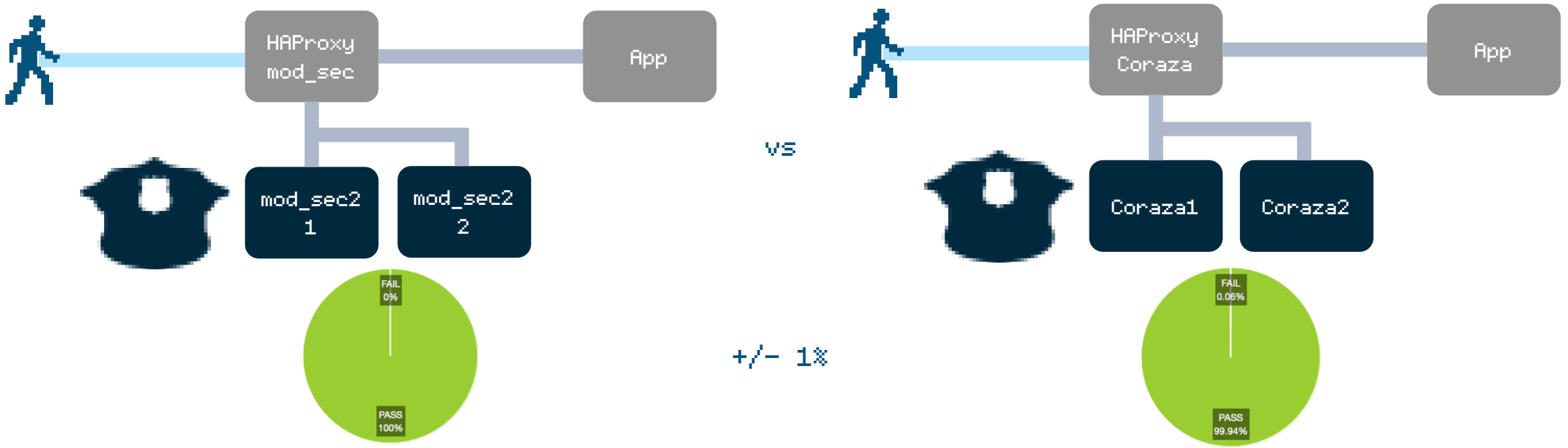


Coraza

about 6 minutes

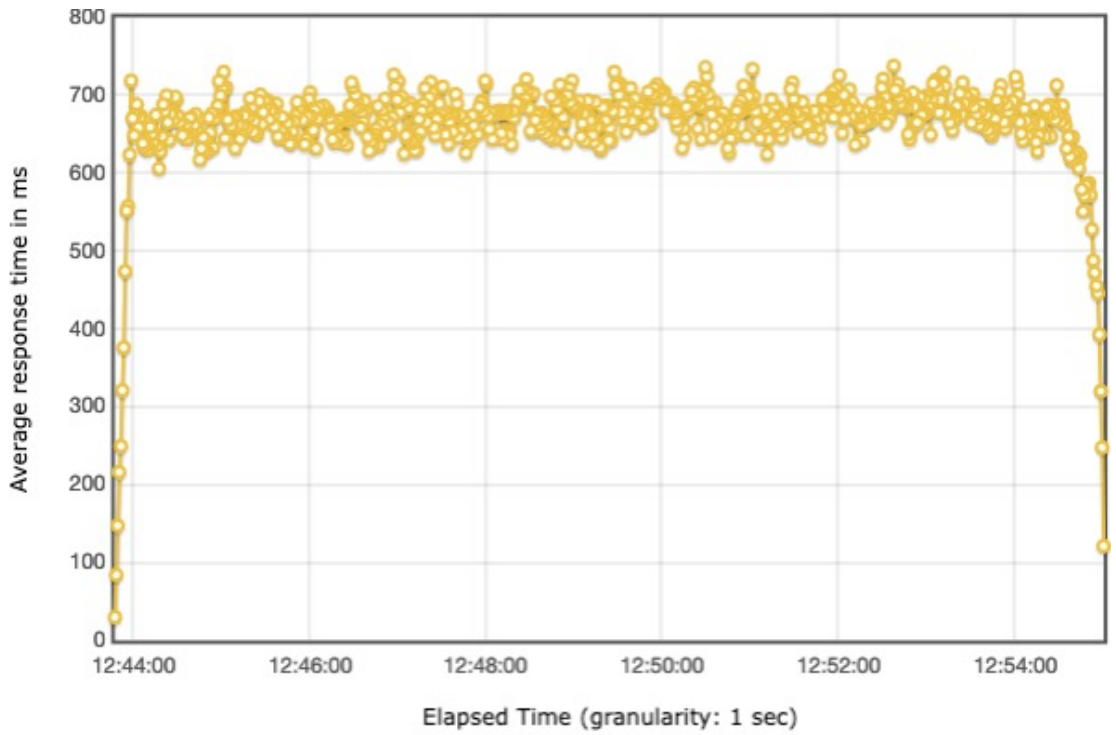
Let's benchmark!

Run 4 - HAProxy+mod_sec2 vs HAProxy+Coraza - fixed config. + LB



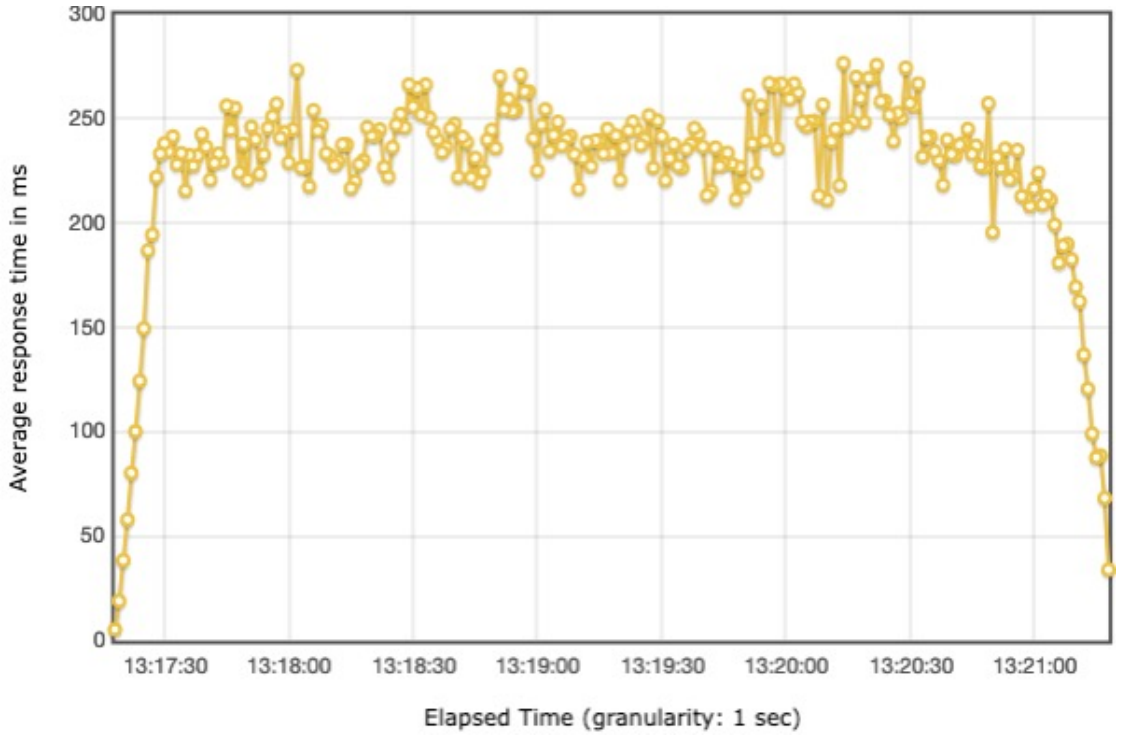
Let's benchmark!

Response time



mod_security2

about 12 minutes

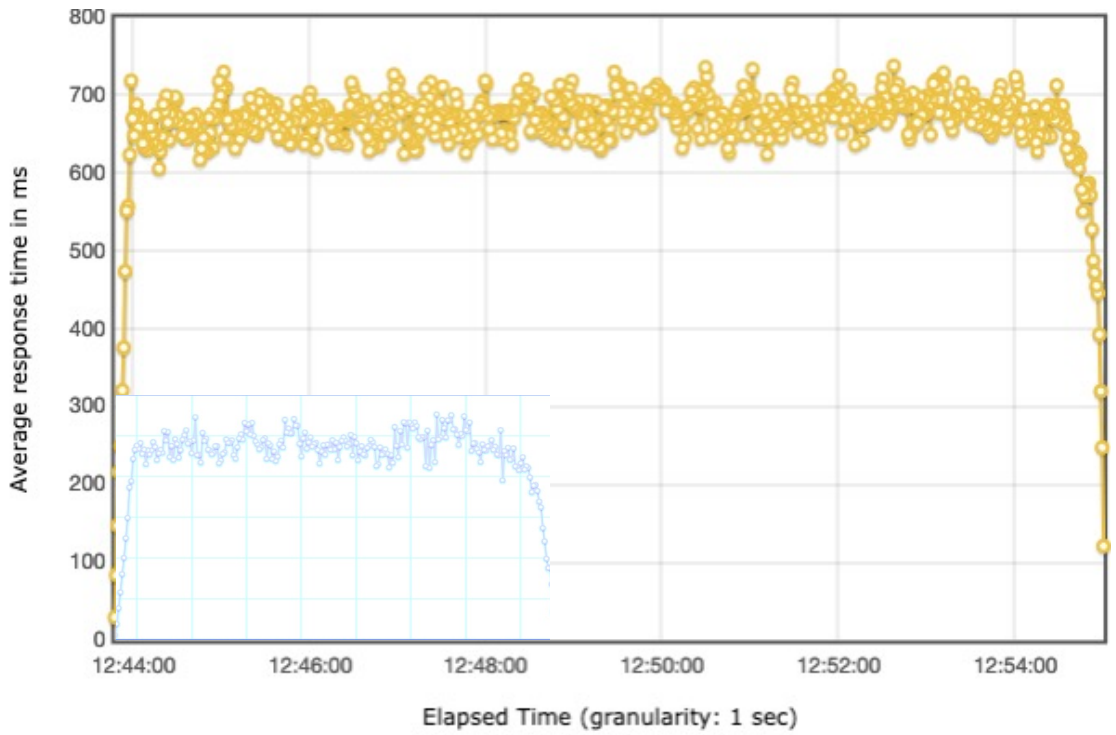


Coraza

about 5 minutes

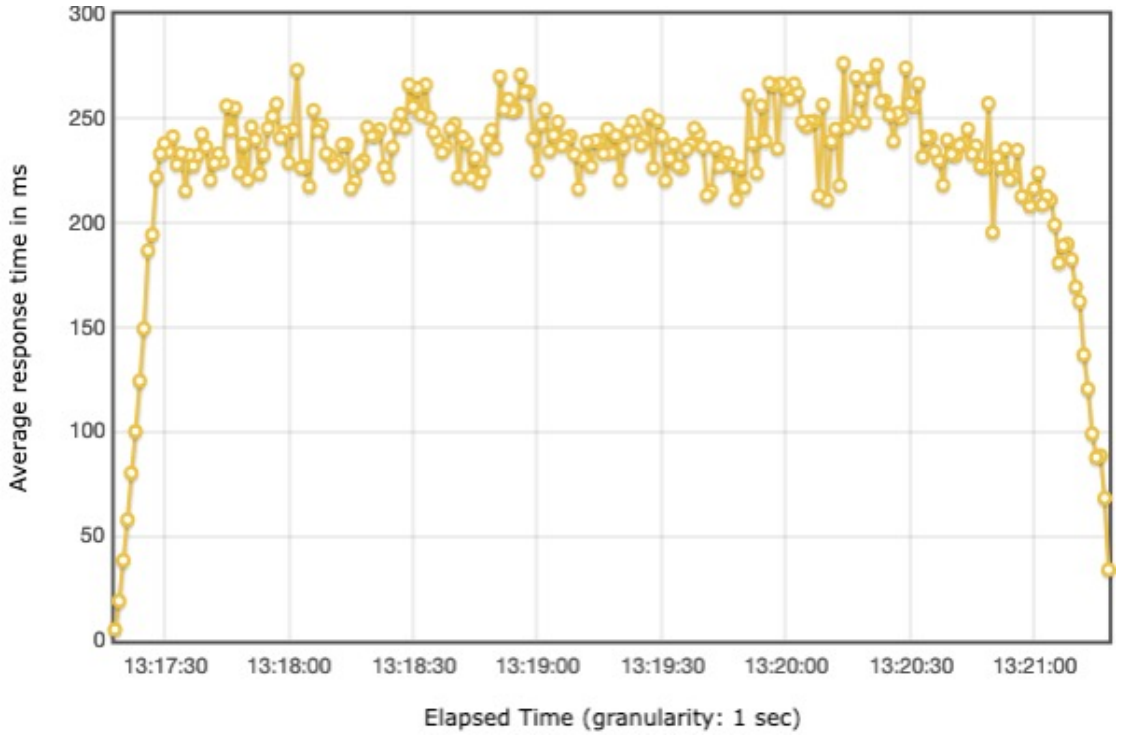
Let's benchmark!

Response time



mod_security2

about 12 minutes

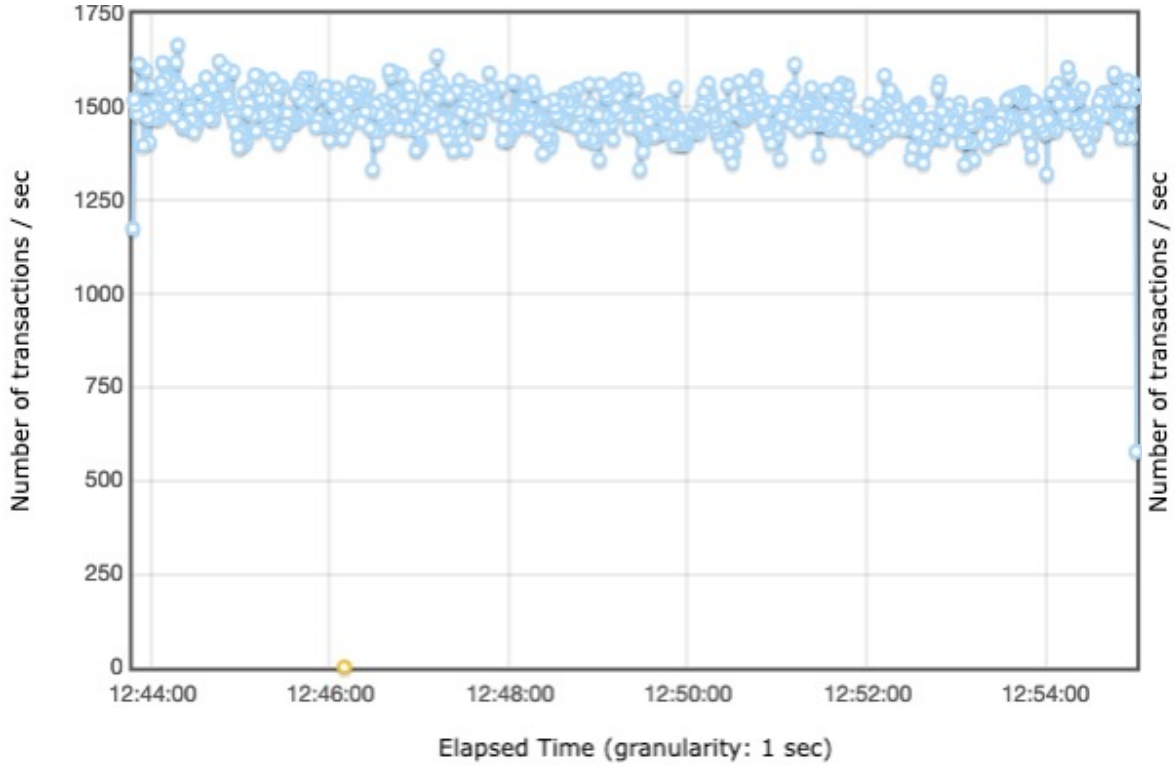


Coraza

about 5 minutes

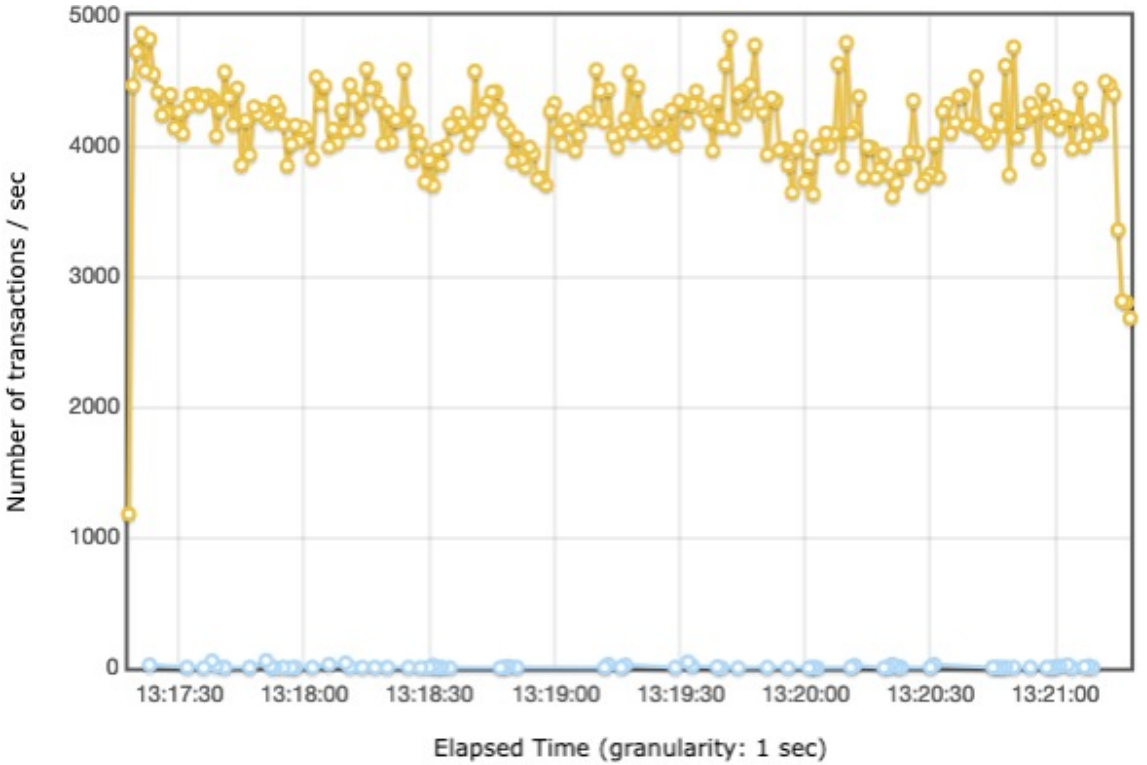
Let's benchmark!

Response type - yellow is OK



mod_security2

about 12 minutes



Coraza

about 5 minutes

Which solution we chose?

HAProxy + Coraza

- Not much errors, even on heavy loads
- Fast response, even on heavy loads
- Easy build/updates

- The future of FOSS WAFs? Coraza!

- Careful: even though we are using it, and it seems stable enough, the GitHub repository for Coraza still mark the SPOA as **EXPERIMENTAL.**

- Let's go a bit further.

What is a reverse proxy?

Address https://github.com/fladna9/protectingwebapp

HAProxy + Coraza + fail2ban = 

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37

HAProxy + Coraza + Fail2ban

Let's ban an IP for some time after an attempted injection

- Blocking with WAF is great. But let's ban "curious" IPs.

- fail2ban: Host-based Intrusion Prevention System (HIPS) based on log parsing.

- Installing fail2ban on HAProxy
  ```
  # sudo apt install fail2ban
  ```

- Important: let's not forget to whitelist ourselves.
  - Editing /etc/fail2ban/jail.local on the ignoreip line.

HAProxy + Coraza + Fail2ban

Let's ban an IP for some time after an attempted injection

- What do we need in HAProxy logs? Source IP, source port, and the fact that Coraza denied the request.

- Configure HAProxy to log WAF action (in frontend section)
  - log-format "%ci:%cp\ [%t]\ %ft\ %b/%s\ %Th/%Ti/%TR/%Tq/%Tw/%Tc/%Tr/%Tt\ %ST\ %B\ %CC\ %CS\ %tsc\ %ac/%fc/%bc/%sc/%rc\ %sq/%bq\ %hr\ %hs\ %{+Q}r\ %ID\ wafaction:%[var(txn.coraza.action)]\ wafruleid:%[var(txn.coraza.ruleid)]\ wafstatus:%[var(txn.coraza.status)]\ wafdata:%[var(txn.coraza.data)]"

- Then, a log line will look like:
  - 57361:Sep 16 07:33:14 reverseproxy1 haproxy[145765]: 1.2.3.4:42000 [16/Sep/2024:07:33:13.917] web-http~ web-http/<NOSRV> 119/97/2/218/-1/-1/-1/218 403 72 - - PR-- 3/3/0/0/0 0/0 "GET /.env HTTP/1.1" 68750185-f340-417e-b9b8-286f03307ae6 wafaction:deny wafruleid:949110 wafstatus:0 wafdata:-

HAProxy + Coraza + Fail2ban

Let's ban an IP for some time after an attempted injection

- Create a filter for fail2ban for HAProxy custom log: /etc/fail2ban/filter.d/haproxy-coraza.conf

```
[INCLUDES]
before = common.conf
[Definition]
_daemon = haproxy
failregex = ^.* (\S+) (\S+)\[(\d+)\]: <HOST>:(\d+) \[(.*)\] (\S*) (\S*) \S+ (\d+) .* \"(.*)\" (\S*)
wafaction:deny wafruleid:(\d+)
ignoreregex =
```

- In fail2ban, <HOST> is a shortcut for IPv4, IPv6 or domain name.
  It means (?::::f{4,6}:)?(?P<host>\S+)

Address https://github.com/fladna9/protectingwebapp

HAProxy + Coraza + Fail2ban

Let's ban an IP for some time after an attempted injection

- Create a jail for web attacks

```
[haproxy-coraza-immediate]
enabled = true
filter  = haproxy-coraza
logpath = /var/log/haproxy.log
bantime = X1
findtime = Y1
maxRetry = Z1

[haproxy-coraza-long]
enabled = true
filter  = haproxy-coraza
logpath = /var/log/haproxy.log
bantime = X2
findtime = Y2
maxRetry = Z2
```

HAProxy + Coraza + Fail2ban

Let's ban an IP for some time after an attempted injection

- Check banned Ips with
  # fail2ban-client get haproxy-coraza-immediate banned

  or

  # fail2ban-client get haproxy-coraza-long banned

Notepad - closing words and thanks.txt

File Edit Search

CLOSING WORDS

+ You can find this presentation, HOWTOs and tutorials on **https://github.com/fladna9/protectingwebapp**
+ I'll be happy to discuss with you about experiences you have on these software ;)

SPECIAL THANKS TO

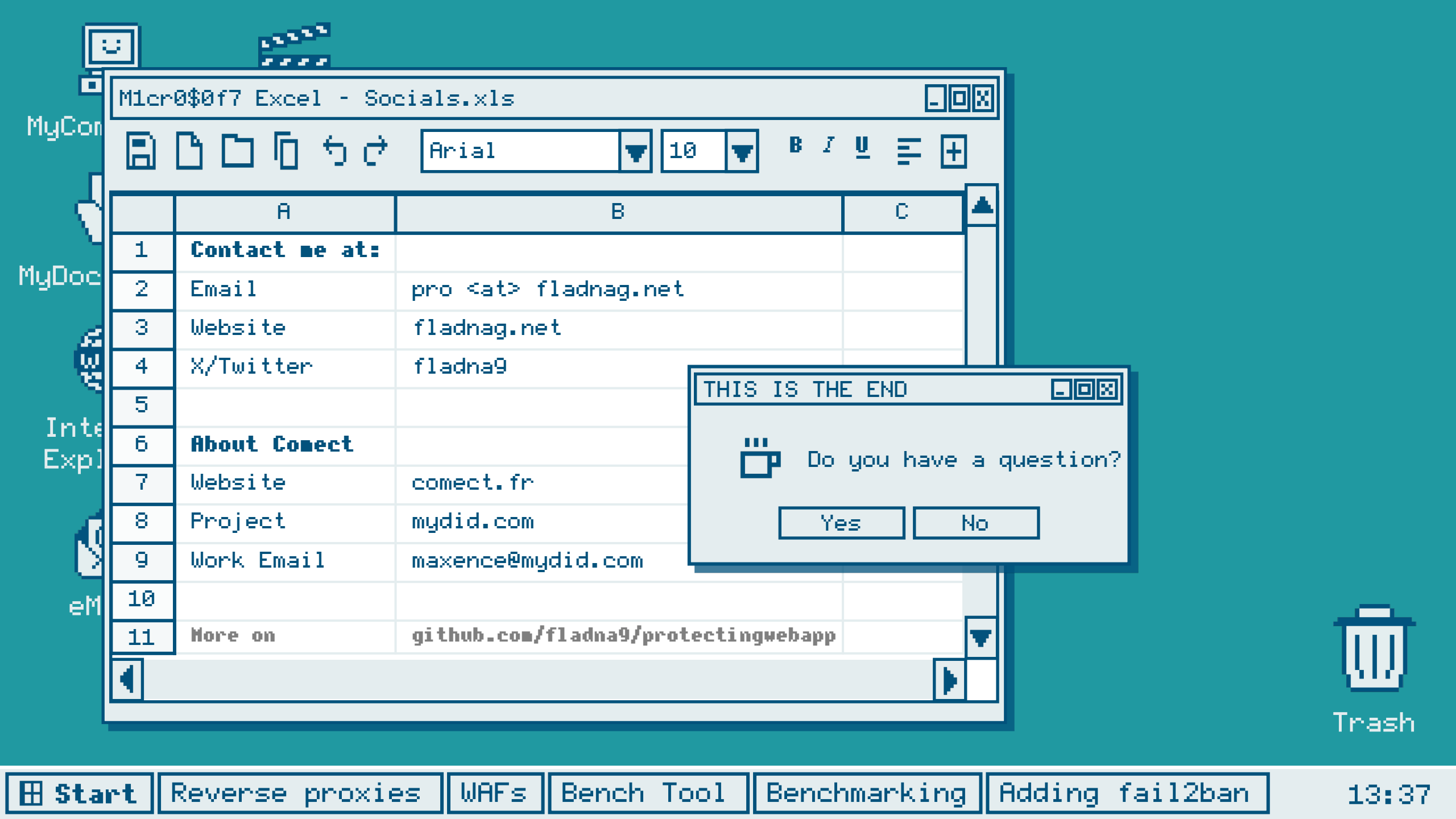
+ **You**, for listening,
+ **Frédéric MARTIN**, CEO of Comect, for his trust and advices,
+ **Friends** for reading/correcting/improving this presentation.

LAST BUT NOT LEAST

+ **BALCCON TEAM for this wonderful event, love you** 

Trash

Start | Reverse proxies | WAFs | Bench Tool | Benchmarking | Adding fail2ban | 13:37


M1cr0$0f7 Excel - Socials.xls
Arial
10
A
B
C
1 Contact me at:
2 Email pro <at> fladnag.net
3 Website fladnag.net
4 X/Twitter fladna9
5
6 About Comect
7 Website comect.fr
8 Project mydid.com
9 Work Email maxence@mydid.com
10
11 More on github.com/fladna9/protectingwebapp
THIS IS THE END
Do you have a question?
Yes
No
Trash
Start
Reverse proxies
WAFs
Bench Tool
Benchmarking
Adding fail2ban
13:37

;)

Your talk ran into a problem and needs to stop.

42% complete

For more information about this issue and possible fixes, visit
https://github.com/fladna9/protectingwebapp

If you call a support person, give them this info:

Stop code: PRESENTATION_ENDED