

ĐƠN VỊ TÀI TRỢ VÀNG

ĐƠN VỊ TÀI TRỢ BẠC

ĐƠN VỊ TỔ CHỨC



**InterData**  
UNLIMITED CONNECTIONS



**123** HOST

**VNG CLOUD**




**SePay**



# LARAVEL LIVE VIETNAM 2024



HO CHI MINH CITY

 13:00 - 17/08/2024

 **TÒA NHÀ THÔNG TẤN XÃ**

116-118 NGUYỄN THỊ MINH KHAI, PHƯỜNG VÕ THỊ SÁU, QUẬN 3, TP. HCM

# Anti-DDoS cho hệ thống vừa & nhỏ

## ~ Tư duy phòng thủ ~

Đức Đỗ - Software Engineer

# Giới thiệu

- Cựu Software Engineer @ CellphoneS.
- Software Engineer @ Zalo, VNG.
- Đam mê máy tính, yêu lập trình.
- Cùng nhau chia sẻ, cùng nhau phát triển.



**Lý do tại sao có chủ đề này ?!!**

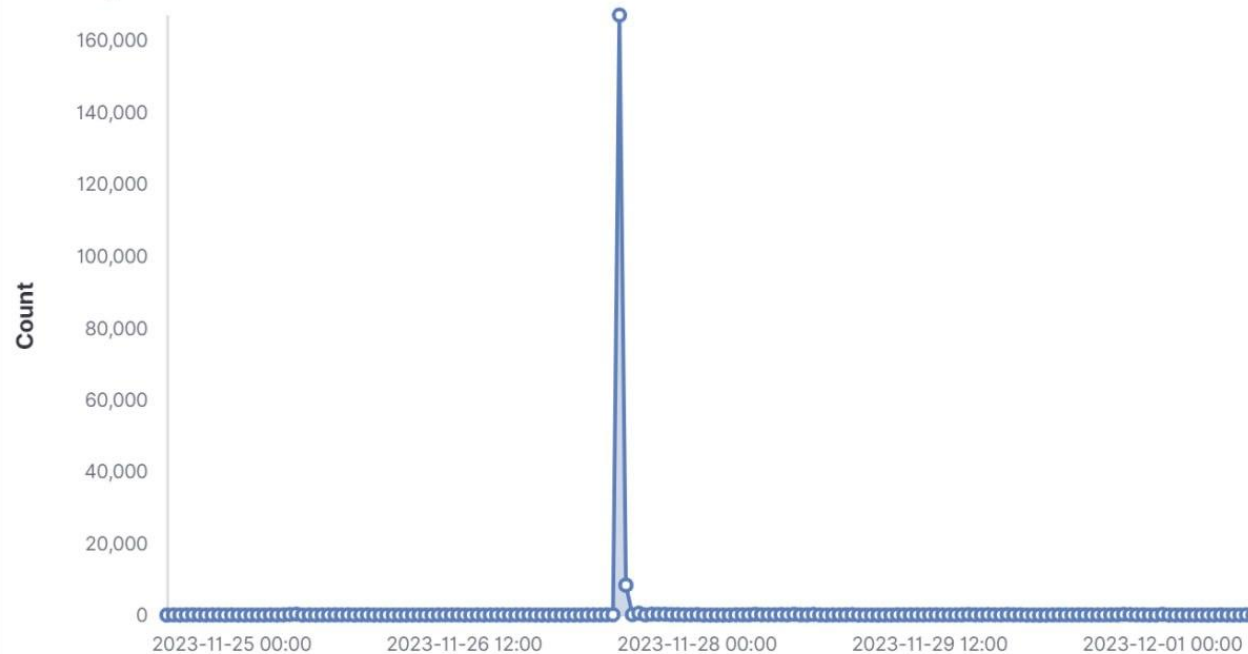




request\_host: cellphones.com.vn ×

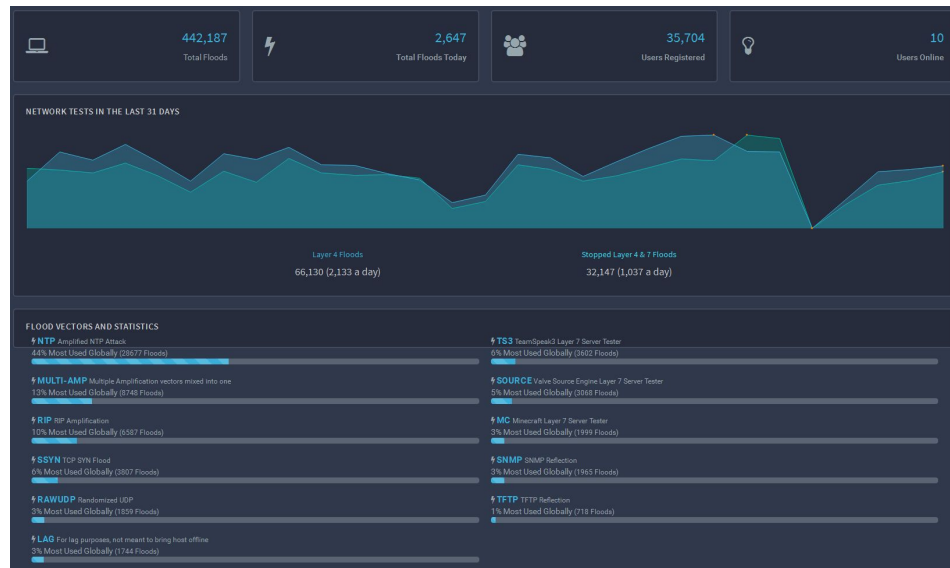
+ Add filter

### Total Requests to WAF



## Our Pricing

1 Month Basic	Bronze Lifetime	Gold Lifetime	Green Lifetime	Business Lifetime
<b>5.00€</b> /month	<b>22.00€</b> Lifetime	<b>50.00€</b> Lifetime	<b>60.00€</b> Lifetime	<b>90.00€</b> lifetime
1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +	1 Concurrent +
300 seconds boot time	600 seconds boot time	1200 seconds boot time	1800 seconds boot time	3600 seconds boot time
125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity	125Gbps total network capacity
Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools	Resolvers & Tools
24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support	24/7 Dedicated Support
<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>	<a href="#">Order Now</a>



Không còn là các công cụ Private. Các dịch vụ DDoS, những năm gần đây đã thay đổi sang loại hình dịch vụ mua bán công khai.

# Mô hình OSI 7 Layer Network





# 7 Layers of the OSI Model

## 7. Application

- End User layer
- HTTP, FTP, IRC, SSH, DNS

## 6. Presentation

- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

## 5. Session

- Synch & send to port
- API's, Sockets, WinSock

## 4. Transport

- End-to-end connections
- TCP, UDP

## 3. Network

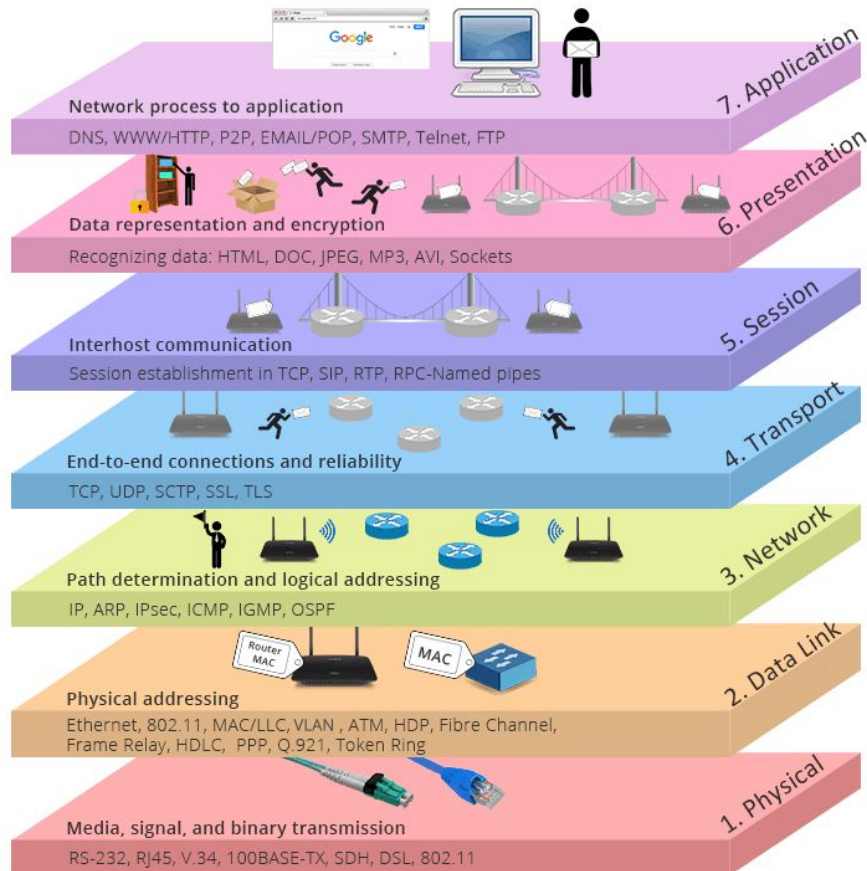
- Packets
- IP, ICMP, IPSec, IGMP

## 2. Data Link

- Frames
- Ethernet, PPP, Switch, Bridge

## 1. Physical

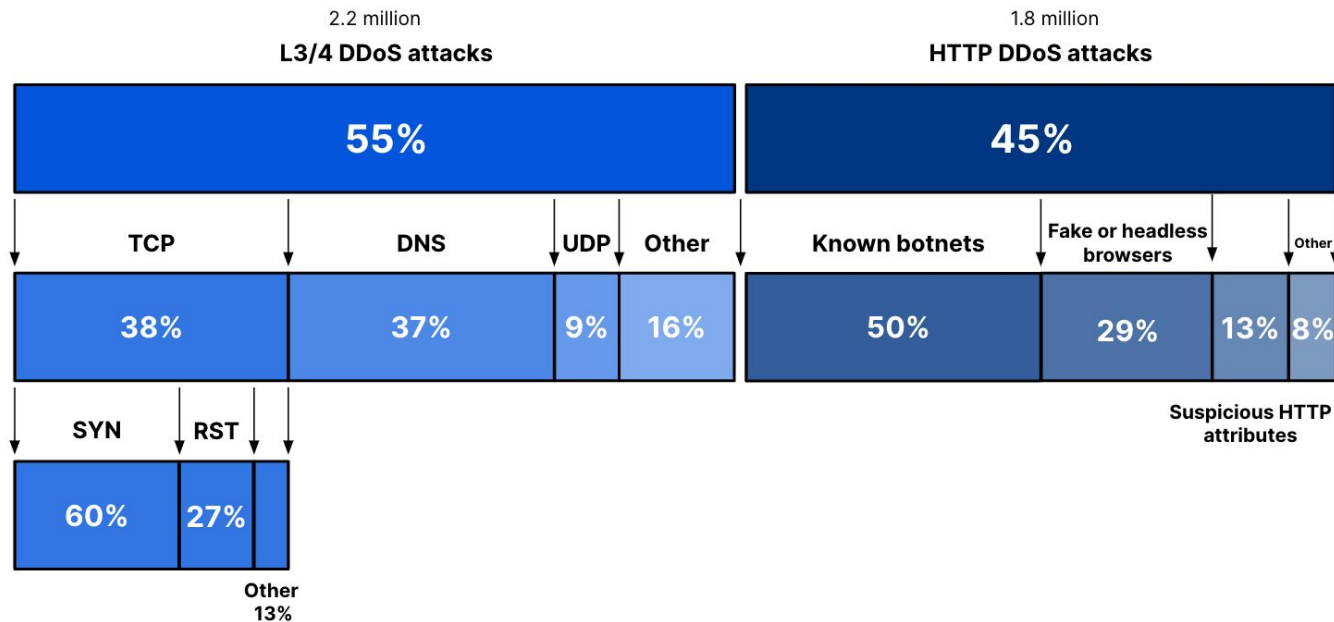
- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters





# Distribution of DDoS attack types

2024 Q2



## DDoS threat report for 2024 Q2 - CloudFlare

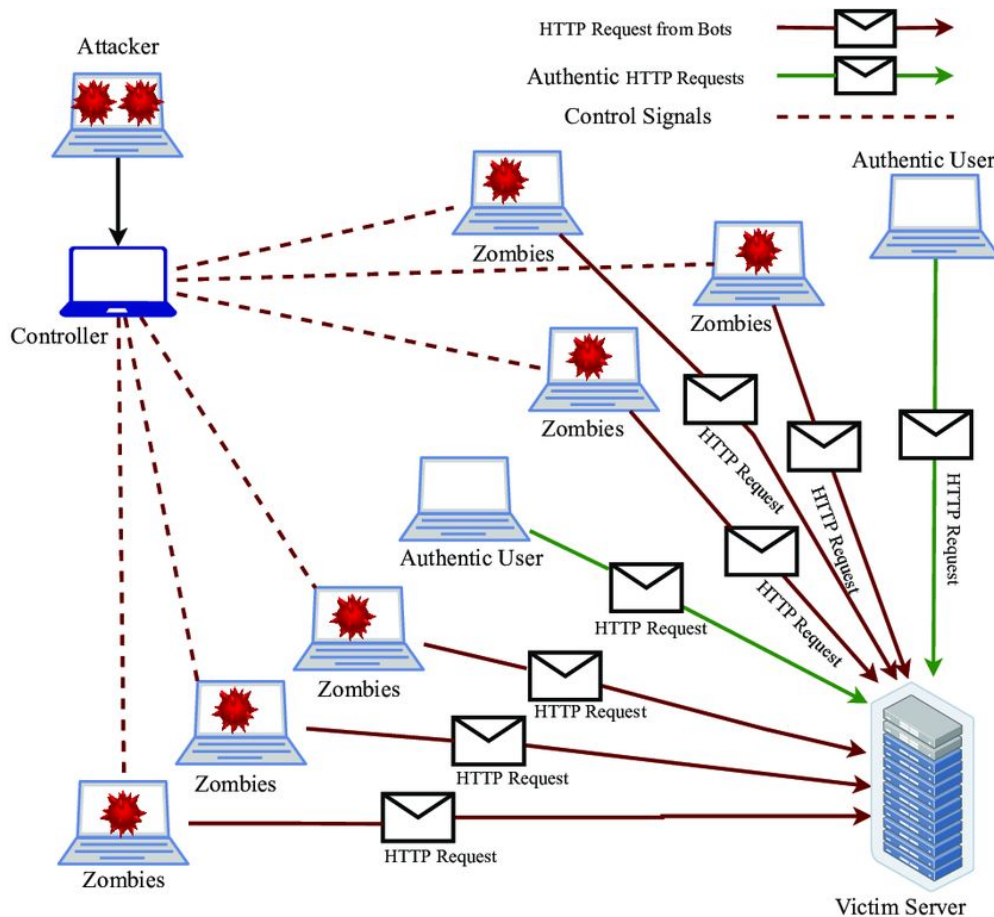
Overall, the number of DDoS attacks in Q2 decreased by 11% quarter-over-quarter, but **increased 20% year-over-year**.



# Phòng thủ



# Layer 7: Application Layer



# Làm sao để nhận biết cuộc tấn công ?!

```
top - 07:06:38 up 2 min, 2 users, load average: 896.33, 299.64, 106.77
Tasks: 285 total, 10 running, 275 sleeping, 0 stopped, 0 zombie
Cpu(s): 52.6%us, 17.5%sy, 0.3%ni, 27.3%id, 0.6%wa, 0.0%st, 1.7%si, 0.0%sw
Mem: 5959496k total, 5205164k used, 754332k free, 166100k buffers
Swap: 3071992k total, 0k used, 3071992k free, 1122664k cached
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
3380	apache	20	0	3705m	75m	4500	S	10.7	1.3	0:12.96	/usr/sbin/httpd
3725	apache	20	0	3706m	79m	4568	S	10.0	1.4	0:12.95	/usr/sbin/httpd
2109	apache	20	0	3867m	76m	4508	S	9.7	1.3	0:13.94	/usr/sbin/httpd
2113	apache	20	0	3706m	77m	4556	S	9.7	1.3	0:14.44	/usr/sbin/httpd
3726	apache	20	0	3706m	75m	4572	S	9.6	1.3	0:12.12	/usr/sbin/httpd
2117	apache	20	0	3706m	82m	4544	S	9.5	1.4	0:14.38	/usr/sbin/httpd
3729	apache	20	0	3705m	72m	4600	S	9.4	1.3	0:12.67	/usr/sbin/httpd

```
1 [|||||] 100.0% Tasks: 50, 250 thr; 4 running
2 [|||||] 100.0% Load average: 97.86 55.14 31.89
3 [|||||] 100.0% Uptime: 39 days, 02:31:47
4 [|||||] 100.0%
Mem 2.52G/7.75G
Swap 285M/4.79G
```

PID	USER	PRI	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	Command
934	mongod	20	0	4472M	1783M	37584	S	386	22.5	274h	/usr/bin/mongod --config /etc/mongo
1701592	root	20	0	11.5G	301M	51184	S	10.0	3.8	1:11.12	node /var/apps/test2/chanlebank-sel
1701856	mongod	20	0	4472M	1783M	37584	R	6.6	22.5	0:08.33	/usr/bin/mongod --config /etc/mongo
1701874	mongod	20	0	4472M	1783M	37584	R	5.3	22.5	0:08.47	/usr/bin/mongod --config /etc/mongo
1701712	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.60	/usr/bin/mongod --config /etc/mongo
1701737	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.72	/usr/bin/mongod --config /etc/mongo
1701857	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.39	/usr/bin/mongod --config /etc/mongo
1701689	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:12.75	/usr/bin/mongod --config /etc/mongo
1701776	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.47	/usr/bin/mongod --config /etc/mongo
1701818	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.52	/usr/bin/mongod --config /etc/mongo
1701640	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:09.88	/usr/bin/mongod --config /etc/mongo
1701869	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.34	/usr/bin/mongod --config /etc/mongo
1701860	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.35	/usr/bin/mongod --config /etc/mongo
1701872	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.34	/usr/bin/mongod --config /etc/mongo
1701704	mongod	20	0	4472M	1783M	37584	R	4.6	22.5	0:08.62	/usr/bin/mongod --config /etc/mongo
1701741	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:08.60	/usr/bin/mongod --config /etc/mongo
1701685	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:16.86	/usr/bin/mongod --config /etc/mongo
1701748	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:09.16	/usr/bin/mongod --config /etc/mongo
1701865	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:08.29	/usr/bin/mongod --config /etc/mongo
1701654	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:08.91	/usr/bin/mongod --config /etc/mongo
1701771	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:08.91	/usr/bin/mongod --config /etc/mongo
1701785	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:09.64	/usr/bin/mongod --config /etc/mongo
1701862	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:08.35	/usr/bin/mongod --config /etc/mongo
1701734	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:10.89	/usr/bin/mongod --config /etc/mongo
1701666	mongod	20	0	4472M	1783M	37584	R	4.0	22.5	0:12.33	/usr/bin/mongod --config /etc/mongo

F1 Help F2 Setup F3 Search F4 Filter F5 Tree F6 Sort By F7 Nice F8 Nice F9 Kill F10 Quit

- CPU 100%, load average vượt quá số lượng Core CPU.
- Các process liên quan đến Webservice (httpd - Apache, php-fpm - Nginx) sử dụng full 100% CPU







# Phân tích tấn công tại Layer 7

- Các IP tấn công phải là IP thật (Có thể là Proxy, Sock, ...)
- Số lượng IP này có hạn, tùy vào tài chính của kẻ tấn công.
- IP access thường là IP nước ngoài.
- Truy cập vào 1 URI, với các ký tự vô nghĩa ở phía sau
- Các IP này không hề tải các static resource (css, js...)

**Tư duy phòng thủ số 1:**

**Rate Limit để giảm thiểu tác hại của DDoS.**



```

http {
    geo $is_vn {
        default 0;
        VN 1;
    }

    map $is_vn$http_x_forwarded_for$http_x_real_ip $limit_req_zone {
        "~1.+.+." 5r/s;
        "~0.+.+." 2r/s;
        default "";
    }

    limit_req_zone $binary_remote_addr zone=rate_limit_zone:10m
    rate=$limit_req_zone;

    server {
        location / {
            limit_req zone=rate_limit_zone burst=10 nodelay;
            proxy_pass http://backend;
        }
    }
}

```

## Nginx

If incoming requests match...

Field	Operator	Value	
URI Path	equals	/	And Or

e.g. /content

Expression Preview

[Edit expression](#)

```
(http.request.uri.path eq "/" )
```

With the same characteristics...

IP

When rate exceeds...

Requests (required)	Period (required)
50	10 seconds

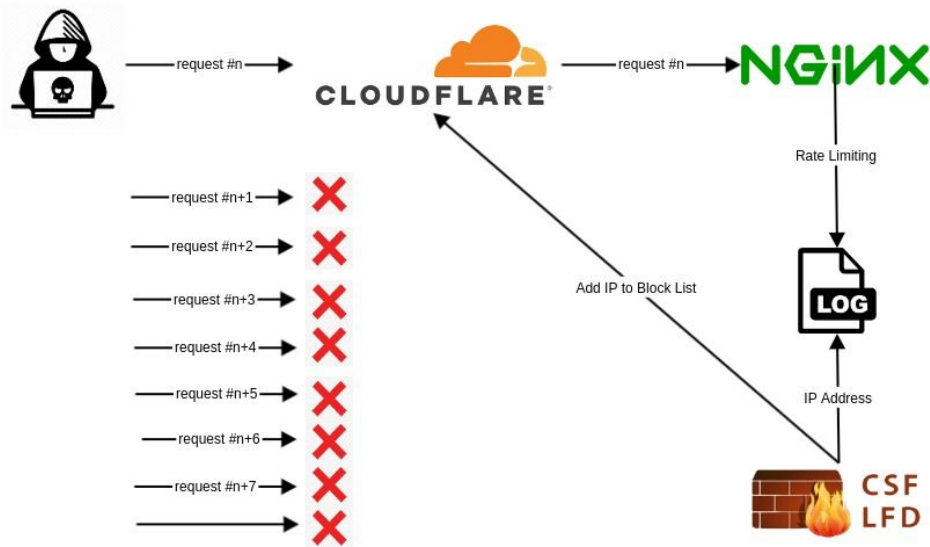
Then take action...

Choose action	With response type	With response code
Block	Custom HTML	429

## CloudFlare



# Kết hợp giữa Rate Limit và CSF Firewall, IPTables



- Khi áp dụng Rate Limit, nếu tần suất IP tái phạm quá 3 lần
- => Block !!!



# Tư duy phòng thủ số 2:



**Rate Limit**



**Challenges**



[← Back](#)

Edit rule [Custom rules](#)

Rule name (required)

Challenge Captcha

Give your rule a descriptive name.

When incoming requests match...

Field	Operator	Value	
Country	is not in	Vietnam	×
		e.g. GB	
And			
Known Bots	equals	<input type="checkbox"/>	×

Expression Preview

[Edit expression](#)

```
(not ip.geoip.country in {"VN"}) and not cf.client.bot)
```

Then take action...

Choose action

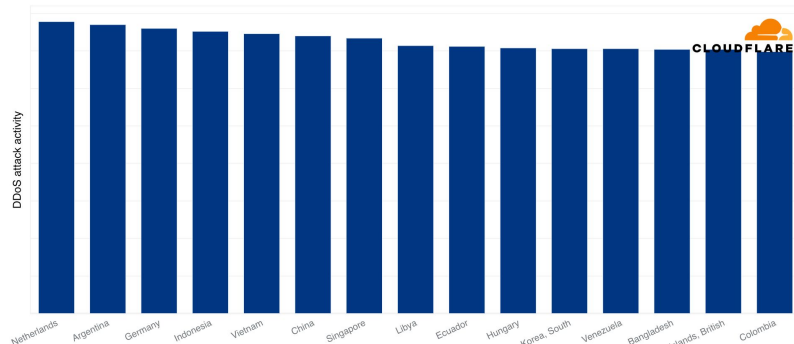
JS Challenge

Presents a JavaScript challenge to the client making the request

Top sources of DDoS attacks

Application-layer

2024 Q2



15 largest sources of DDoS attacks in 2024 Q2

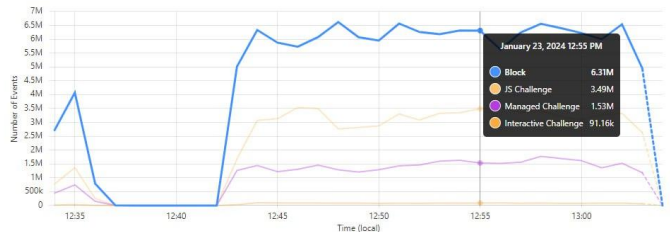
[Add filter](#)

Live Previous 30 minutesLive updating

Events summary [About Firewall Events](#)

Action Host Country ASN IP Path ...

Total	Block	JS Challenge	Managed Challenge	Interactive Challenge
237.25M	135.47M	68.2M	31.76M	1.82M



# Challenge các truy cập ngoài VN



Laravel Vietnam

LARAVEL LIVE  
VIETNAM 2024

#### Configure Super Bot Fight Mode

Super Bot Fight Mode identifies traffic that may be automated. For each request, Cloudflare characterizes a request as automated, likely automated, and likely human. This can be used to isolate bot requests.

##### Definitely automated

Definitely automated traffic typically consists of bad bots. Select an action for this traffic.

Block ▼

##### Likely automated

Likely automated traffic can include bad bots, along with other traffic. Select an action for this traffic.

Managed Challenge ▼

##### Verified bots

Verified bots are unique good bot identities validated by Cloudflare. Select an action for verified bots for this traffic.

Allow ▼

- **Definitely automated:** Các bot đã được xác nhận là hoàn toàn tự động hoá, phần lớn là bot spam hoặc bot crawl dữ liệu từ các công cụ ít phổ biến, loại này là nên chặn hẳn.
- **Likely automated:** Là danh sách các bot mà CloudFlare cho là nó vẫn tự động nhưng có thể mức độ phổ biến về nguy hiểm sẽ ít hơn.
- **Verified bot:** Các bot mà CloudFlare xác nhận là đã được xác nhận, ít hoặc không gây ảnh hưởng đến website. Danh sách này sẽ bao gồm bot của Google, Microsoft, Amazon Bot, GPT Bot,...



# Tư duy phòng thủ số 3:

**Hệ thống của bạn phải đủ khỏe**

...

**Ít nhất là 5 phút !!!**



# Tối ưu kiến trúc hệ thống



## Combo "Tân thủ" cho Junior Dev

Full Combo "Tân thủ" cho ae Junior Dev nâng cao kỹ năng coding của mình. Bộ comb...



## Combo "Khởi nghiệp" không ngại công nghệ

Full Combo "Khởi nghiệp" không ngại công nghệ cho ae Junior Dev nâng cao kỹ năng...



## MySQL cho người đi làm - Các chiến lược tối ưu MySQL cơ bản

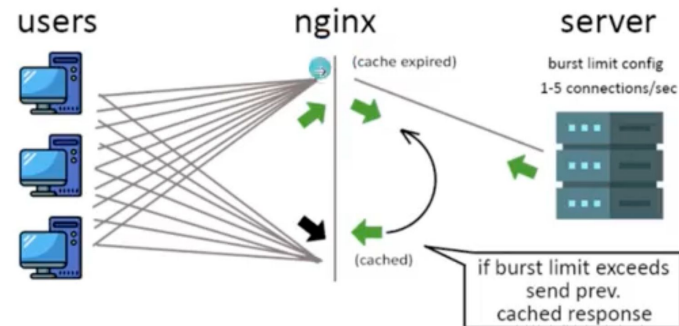
Giới thiệu Ebook: MySQL cho Người Đi Làm - Các Chiến Lược Tối Ưu MySQL Cơ Bản. Bạn...



## Combo 2 cuốn OOP và Thiết kế

Combo 2 cuốn "OOP cho người đi làm" và "Thiết kế hướng nghiệp vụ với Laravel" ch...



# Hãy sử dụng cache nếu có thể



# Layer 3/4: Network Layer

## Network-layer and SSL/TLS DDoS attack protection

Rulesets managed by Cloudflare that automatically mitigate SSL/TLS-based and Network-layer DDoS attacks such as SYN floods and UDP reflection attacks. **Network-layer DDoS attack protection protects all Cloudflare customers,** but only Magic Transit and Spectrum customers on an Enterprise plan can customize the managed ruleset.

Name	Description
 SSL/TLS DDoS attack protection	Automatic mitigation of SSL/TLS based DDoS attacks and encryption-based attacks such as DDoS attacks, SSL exhaustion floods, and SSL negotiation attacks.
 Network-layer DDoS attack protection	Automatic mitigation of network-layer DDoS attacks such as ACK floods, SYN-ACK amplification attacks, UDP attacks, ICMP attacks and DDoS attacks launched by botnets such as Mirai.

[Help](#) ▶



# Sử dụng IPTables, CSF Firewall

- Chặn toàn bộ truy cập từ bên ngoài.
- Chỉ mở những Port thực sự cần thiết.
- Chỉ cho phép IP của CloudFlare đi vào port 80 và 443.
  - <https://www.cloudflare.com/ips/>
- Port SSH (22):
  - Nên đổi sang port private.
  - Mở chế độ login bằng SSH Key.
  - Nếu có thể, hãy allow duy nhất IP cố định của cá nhân bạn!



# Tổng kết

- Rate Limit để giảm thiểu tác hại của DDoS.
  - Chia để trị bao giờ cũng hiệu quả.
- Block, Challenge các yếu tố nguy hiểm đến hệ thống.
- Hệ thống của bạn phải đủ khỏe ... ít nhất 5 phút.

**Cảnh báo & phát hiện dấu hiệu tấn công, càng sớm càng tốt !!!**



**Luôn có ý thức trong việc  
nâng cao kiến thức về an toàn thông tin**



# UNG CLOUD



# Q & A



ĐƠN VỊ TÀI TRỢ VÀNG

ĐƠN VỊ TÀI TRỢ BẠC

ĐƠN VỊ TỔ CHỨC



**InterData**  
UNLIMITED CONNECTIONS



**HOST**

**VNG CLOUD**




**SePay**



# LARAVEL LIVE VIETNAM 2024



**HO CHI MINH CITY**

 13:00 - 17/08/2024

 **TÒA NHÀ THÔNG TẤN XÃ**

116-118 NGUYỄN THỊ MINH KHAI, PHƯỜNG VÕ THỊ SÁU, QUẬN 3, TP. HCM