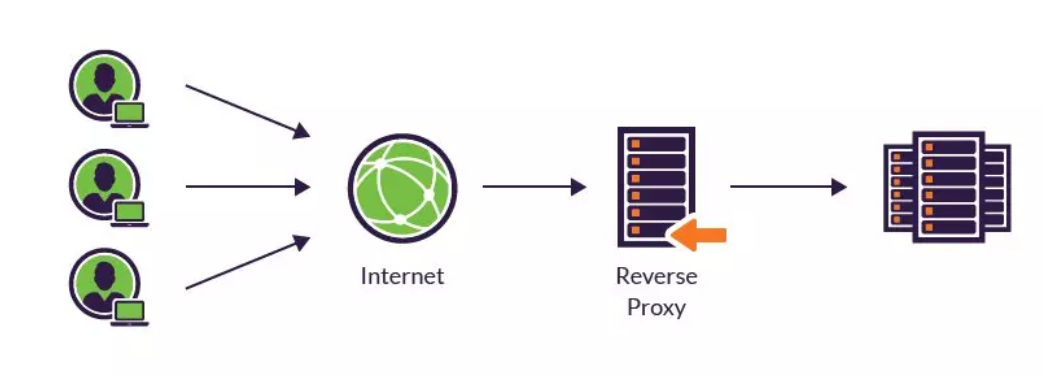
**6. Reverse Proxy & WAF (ModSecurity)**

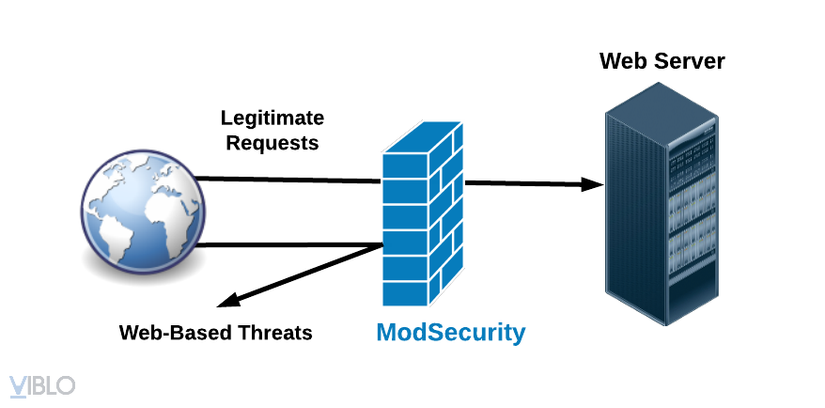
**- Reverse proxy** là một loại proxy server trung gian giữa một máy chủ và các client gửi tới các yêu cầu. Nó kiểm soát yêu cầu của các client, nếu hợp lệ, sẽ luân chuyển đến các server thích ứng. Ưu điểm lớn nhất của việc sử dụng reverse proxy là khả năng quản lý tập trung. Nó giúp kiếm soát mọi request do clieny gửi lên các server được bảo vệ.



* **Bảo mật:** Bằng cách chặn các yêu cầu được gửi đến máy chủ phụ trợ của bạn, reverse proxy server sẽ bảo vệ danh tính của chúng ta và hoạt động như một biện pháp bảo vệ để chống lại các cuộc tấn công bảo mật. Với reverse proxy server thì một trang web hoặc một dịch vụ sẽ không bao giờ tiết lộ địa chỉ IP của các server gốc. Điều này làm cho những cuộc tấn công có thể khó thực hiện.
* **Cân bằng tải:** Đối với một trang web phổ biến thì hàng ngày sẽ có hàng triệu người dùng truy cập và nó có thể không thể xử lý tất cả lưu lượng truy cập đến bằng một máy chủ duy nhất. Vì vậy, trang web nên được phân phối giữa một nhóm các máy chủ khác nhau và tất cả chúng đều xử lý các yêu cầu cho cùng một trang web. Trong trường hợp này, reverse proxy có thể cung cấp giải pháp cân bằng tải sẽ phân phối đồng đều lưu lượng đến giữa các máy chủ khác nhau để ngăn việc một số máy chủ có thể bị quá tải do chịu nhiều yêu cầu cùng lúc. Còn trong trường hợp một máy chủ bị lỗi hoàn toàn thì các máy chủ khác cũng có thể xử lý lưu lượng. Reverse proxy server ở trước các máy chủ phụ trợ của bạn và phân phối các yêu cầu của client trên một nhóm máy chủ theo cách tối đa hóa tốc độ và sử dụng dung lượng trong khi đảm bảo không có máy chủ nào bị quá tải.
* **Tăng tốc độ trang web:** Reverse proxy server có thể nén dữ liệu gửi đến và gửi đi, cũng như lưu vào bộ nhớ cache các nội dung thường xuyên được yêu cầu, cả hai sẽ làm tăng tốc luồng lưu lượng giữa client và server. Ngoài ra nó cũng có thể thực hiện một số tác vụ bổ sung như mã hóa SSL để giảm tải các máy chủ web của bạn, do đó mà hiệu suất cũng được tăng lên.

**- Mod Security** là một module tường lửa có thể tích hợp với các Web Application Server (máy chủ ứng dụng web) như Apache, IIS, Nginx cho phép phân tích và ghi nhật ký các luồng dữ liệu HTTP/S.Với sự đóng góp từ dự án ModSecurity Core Rule Set của tổ chức OWASP đã giúp ModSecurity trở nên mạnh mẽ và linh động hơn trong việc phân tích các hành vi có nguy cơ xâm hại an ninh ứng dụng web.

Mod Security đứng trước Web Server, làm nhiệm vụ như một firewall để kiểm soát truy cập vào ra Web Server. Các thông tin đi từ bên ngoài vào và bên trong ra sẽ được kiểm soát chặt chẽ để tránh những thông tin có thể gây hại cho Web Server hay là việc rò rỉ các thông tin đặc biệt từ Web Server đến Client.



Ở đây ta sẽ cấu hình Reverse Proxy và cài đặt ModSecurity cho server sử dụng **nginx**.

- Cài đặt các gói cần thiết :

|  |
| --- |
| sudo apt install tcpdump git wget libssl-dev zlib1g-dev gcc make build-essential autoconf automake libtool libcurl4-openssl-dev liblua5.3-dev libfuzzy-dev ssdeep gettext pkg-config libpcre3 libpcre3-dev libxml2 libxml2-dev libcurl4 libgeoip-dev libyajl-dev doxygen -y |

- Viết file cấu hình **nginx.conf** :

|  |
| --- |
| user nginx;  worker\_processes auto;  pid /var/run/nginx.pid;  include /etc/nginx/modules-enabled/\*.conf;  load\_module /etc/nginx/modules/ngx\_http\_modsecurity\_module.so;  events {  worker\_connections 1024;  }  http {    include /etc/nginx/conf.d/\*.conf;  server {  listen 80;  modsecurity on;  modsecurity\_rules\_file /etc/nginx/modsec/main.conf;  location / {  proxy\_set\_header Cookie $http\_cookie;  proxy\_pass http://localhost:3000;  }  }  } |

- Copy file config tới nginx:

|  |
| --- |
| sudo cp nginx.conf /etc/nginx/nginx.conf |

- Cài đặt **ModSecurity** sử dụng file shell script viết sẵn :

|  |
| --- |
| #!/bin/bash  cd /opt  git clone https://github.com/SpiderLabs/ModSecurity.git  cd ModSecurity/  git submodule init  git submodule update  ./build.sh  ./configure  make  make install  cd /opt/  git clone https://github.com/SpiderLabs/ModSecurity-nginx.git  NGINX\_VERSION="nginx-"`nginx -v 2>&1 | cut -d "/" -f 2`  NGINX\_VERSION\_TAR\_GZ="nginx-"`nginx -v 2>&1 | cut -d "/" -f 2`".tar.gz"  wget http://nginx.org/download/$NGINX\_VERSION\_TAR\_GZ  tar -xzvf $NGINX\_VERSION\_TAR\_GZ  cd $NGINX\_VERSION  #NGINX\_CONF\_ARG=`nginx -V 2>&1 | awk -F "configure arguments:" '{print $2}' | tr -d "\n"`" #--add-dynamic-module=../ModSecurity-nginx"  #echo $NGINX\_CONF\_ARG | ./configure  ./configure --with-compat --add-dynamic-module=../ModSecurity-nginx  make modules  mkdir /etc/nginx/modules  cp objs/ngx\_http\_modsecurity\_module.so /etc/nginx/modules  # Pull core rules setup of OSWAP  cd /opt  git clone https://github.com/coreruleset/coreruleset modsecurity-crs  cd modsecurity-crs/  mv crs-setup.conf.example crs-setup.conf  mv rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf.example rules/REQUEST-900-EXCLUSION-RULES-BEFORE-CRS.conf  cd /opt  mv modsecurity-crs /usr/local/  mkdir -p /etc/nginx/modsec  cp ModSecurity/unicode.mapping /etc/nginx/modsec  cp ModSecurity/modsecurity.conf-recommended /etc/nginx/modsec  cd /etc/nginx/modsec  sed 's/DetectionOnly/On/' modsecurity.conf-recommended > modsecurity.conf  echo "Include /etc/nginx/modsec/modsecurity.conf  Include /usr/local/modsecurity-crs/crs-setup.conf  Include /usr/local/modsecurity-crs/rules/\*.conf  " > main.conf |

Sau khi cài đặt hoàn tất, thử kiểm tra với https://my-website/?id=1 and 'c'='c' ta được:

Graphical user interface, text, application, email

Description automatically generated