

TRIỂN KHAI V2-WAF

MỤC LỤC

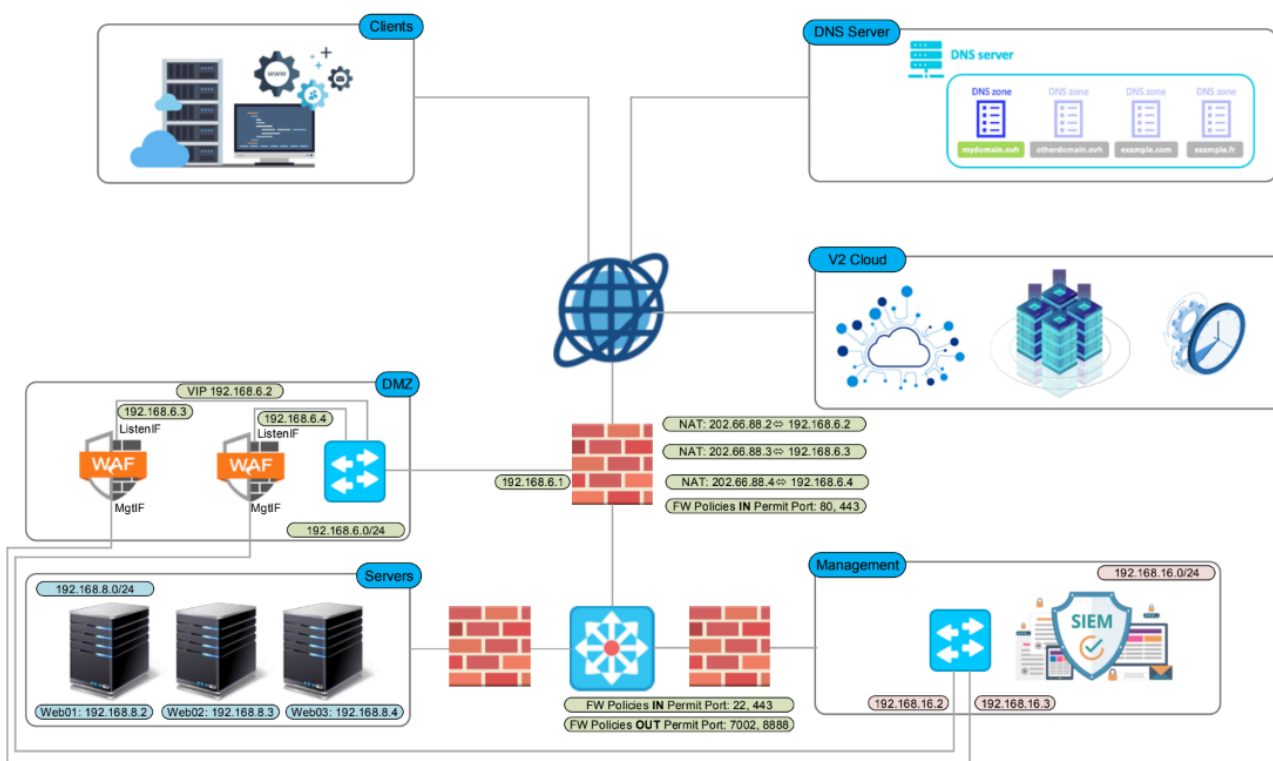
1. Giới thiệu tổng quan về V2-WAF	3
2. Yêu cầu tài nguyên	3
3. Hướng đối tượng doanh nghiệp	4
4. Thực nghiệm V2-WAF trên VMWare Workstation	4
4.1. Mô hình thực nghiệm	4
4.2. Thực hiện cấu hình	5

1. Giới thiệu tổng quan về V2-WAF

Tường lửa ứng dụng web V2-WAF là một giải pháp bảo vệ ứng dụng web trước các cuộc tấn công mạng.

WAF (Web Application Firewall) là một thiết bị phần cứng hoặc phần mềm được cài lên máy chủ có chức năng theo dõi các thông tin sử dụng giao thức http/https giữa trình duyệt của người dùng và máy chủ web.

WAF có chức năng thực thi các chính sách bảo mật dựa trên các dấu hiệu tấn công, các giao thức tiêu chuẩn và các lưu lượng truy cập ứng dụng web bất thường.



2. Yêu cầu tài nguyên

Yêu cầu tài nguyên hệ thống để triển khai V2-WAF phụ thuộc vào số lượng trang web cần bảo vệ, cụ thể như sau:

Websites	CPU/VCPU	RAM	HDD
Websites < 5	8	32	100G
5 ≤ Websites < 10	12	64	300G
10 ≤ Websites < 20	16	128	500G
20 ≤ Websites < 30	24	256	1T
Websites ≥ 30	32	512	2T

3. Hướng đối tượng doanh nghiệp

Triển khai cho doanh nghiệp ở hồ sơ cấp độ 2

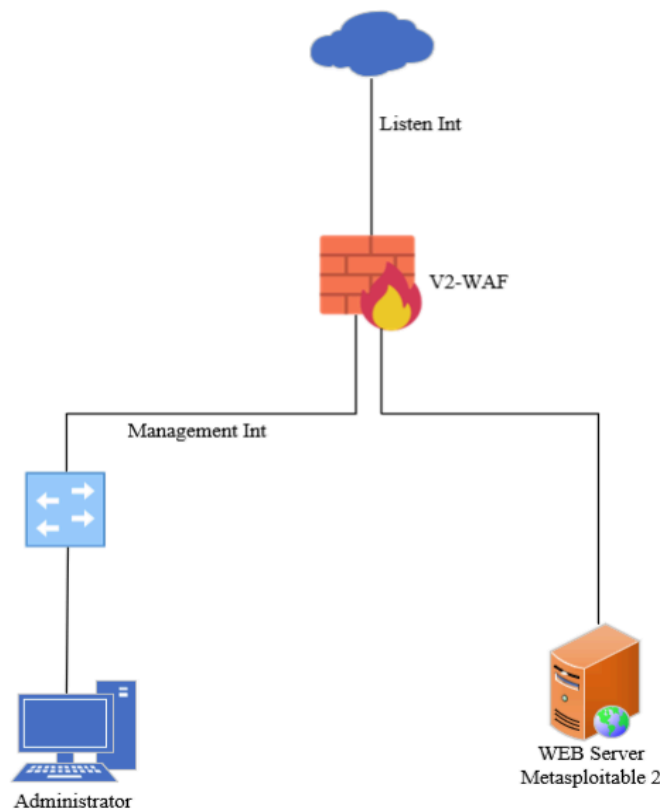
Cấp độ 2

Xử lý thông tin riêng, cá nhân; Hệ thống cung cấp DVCTT cấp ≤ 2 ; không thuộc DMDV kinh doanh có ĐK; xử lý thông riêng, cn < 10.000 người sử dụng; cơ sở hạ tầng thông tin phục vụ hoạt động của một CQTC

Doanh nghiệp đăng ký dùng miễn phí trong 1 tháng tối đa 90 ngày (nếu cần license liên hệ về website ... để được hỗ trợ)

4. Thực nghiệm V2-WAF trên VMWare Workstation

4.1. Mô hình thực nghiệm



Mô hình bao gồm:

- Máy Web Server hệ điều hành Windows Server 2016, cài đặt Metasploitable 2
- Máy Windows 7 ...
- Tường lửa V2-WAF

Phân hoạch địa chỉ IP

	Địa chỉ IP	Subnet Mask	Default Gateway	Preferred DNS
--	------------	-------------	-----------------	---------------

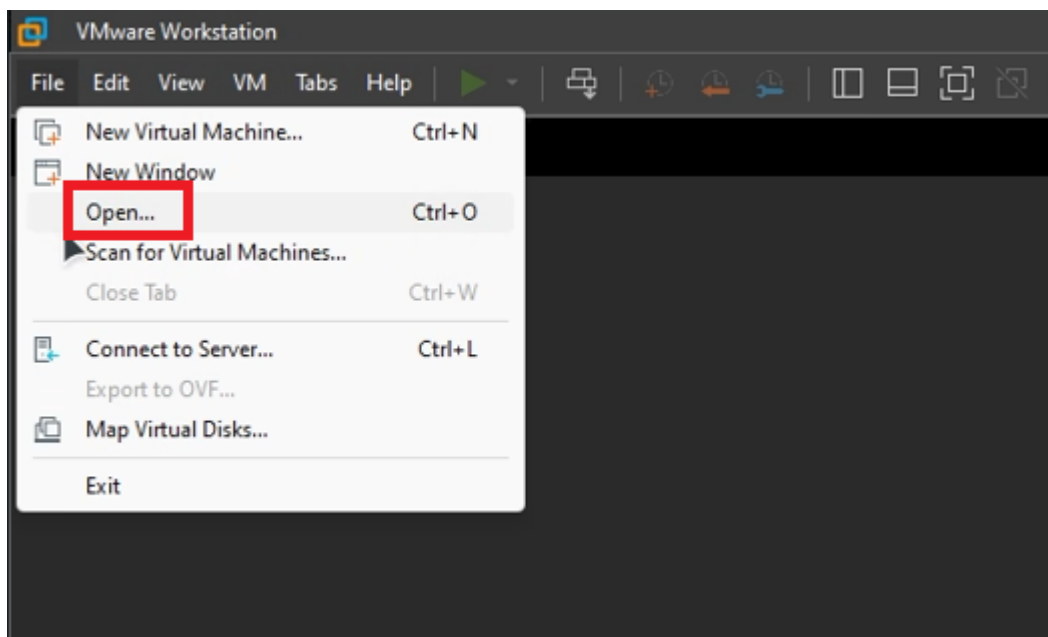
Web Server	192.168.100.100	255.255.255.0	192.168.100.1	192.168.100.100
Windows 7	192.168.100.101	255.255.255.0	192.168.100.1	192.168.100.100
V2-WAF	192.168.100.103	255.255.255.0	192.168.100.1	192.168.100.100

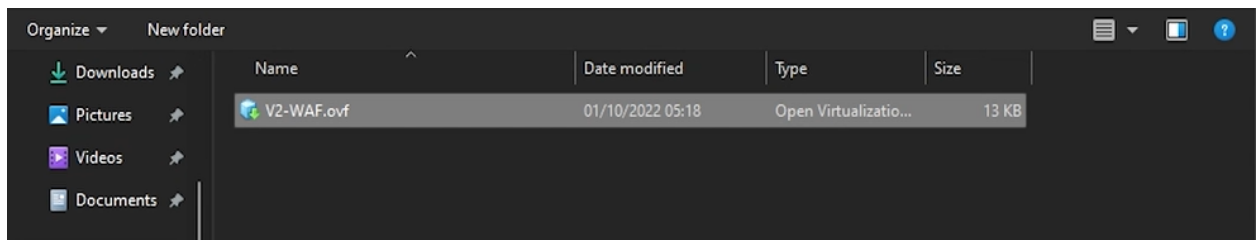
Yêu cầu cấu hình các máy ảo trong VMWare Workstation

	Web Server	Windows 7	V2-WAF
RAM	8GB	2GB	16GB
Disk space	500GB	500GB	500GB
CPU cores	...	...	...
Processor speed	2.3 GHz or more	2.3 GHz or more	2.3 GHz or more

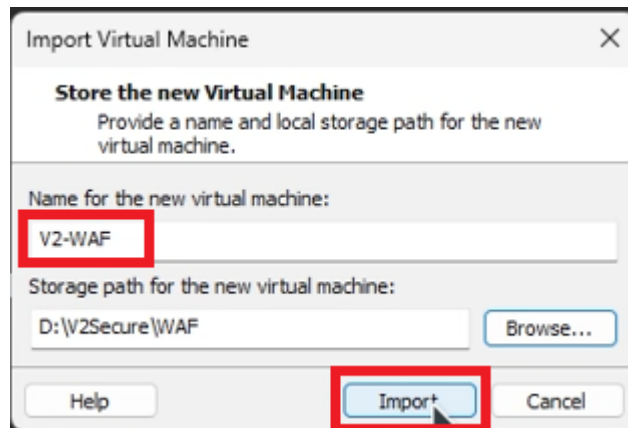
4.2. Thực hiện cấu hình

Vào giao diện của VMware, chọn file -> open và chọn đường dẫn đến file V2-WAF (.ovf) được đóng gói sẵn

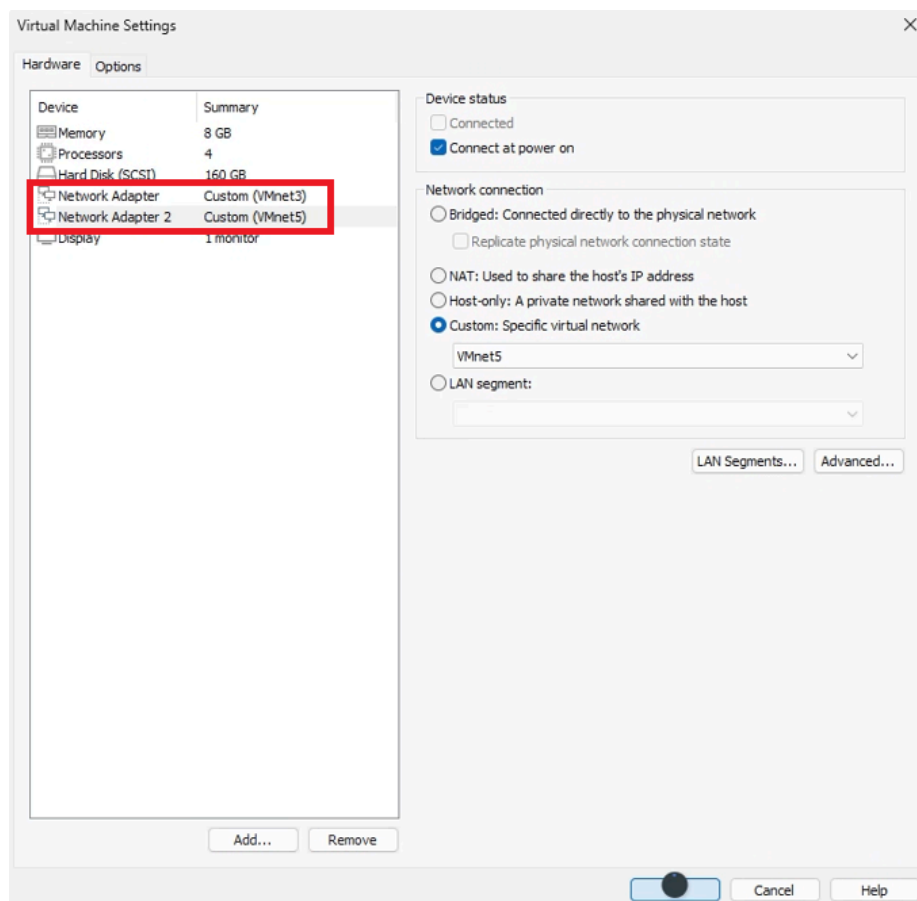




Đặt tên cho máy ảo là và chọn đường dẫn để máy



Sau khi import V2-WAF vào VMware chúng ta sẽ tiến hành add thêm card mạng vào máy ảo



Bước 2: Thiết lập card mạng cho máy V2-WAF

Cấu hình 2 card mạng cho WAF (1 card VMnet 5 cho Listen IP, 1 card VMnet 3 cho Management IP)

Sau khi chạy máy ảo V2-WAF, đăng nhập với tài khoản mặc định là admin/admin, chọn số 2 để thay đổi IP

```
#####
# WELCOME TO WAF-V2 SYSTEM #
#####
WAFV2 login: admin
Password:
-----WAF-V2 SYSTEM CONFIGURATION-----
:
: 0) Assign Interface          9) Logger Service          :
: 1) Interface Information    10) Database Service       :
: 2) Set IP Management & Name server  11) Detection Service      :
: 3) System Time             12) DDoS Defence           :
: 4) System Information       13) Listener Service      :
: 5) WAF Status              14) Ping host              :
: 6) Expert login            15) Reboot system         :
: 7) Restart WebService      16) Halt system           :
: 8) WAF Service             17) Logout (SSH only)     :
:
+-----+
Enter an option: 2_
```

Hệ thống sẽ hiển thị IP của 2 card mạng, chọn "yes" để tiến hành thay đổi

Note: Do set card Vmnet (mạng LAN) nên dãy IP, Netmask, Gateway là do chúng ta tự set

```
Current Interface Information
-----ManagementIF-----
IPADDRESS: 192.168.2.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.2.1
-----ListenIF-----
IPADDRESS: 192.168.1.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.1.1
-----
Would you like to change Management IP address? yes or no: yes
New ip address: _
```

Sau khi nhập IP Management mới tiếp tục chọn "yes" thay đổi IP Listen

Note: Do set card Vmnet (mạng LAN) nên dãy IP, Netmask, Gateway là do chúng ta tự set

```

Current Interface Information
-----ManagementIF-----
IPADDRESS: 192.168.2.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.2.1
-----ListenIF-----
IPADDRESS: 192.168.1.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.1.1
-----

Would you like to change Management IP address? yes or no: yes
New ip address: 10.10.1.100
New netmask: 255.255.255.0
New gateway: 10.10.1.1
New Name Server: 8.8.8.8
Would you like to change Listen IP address? yes or no: yes
New ip address: _

```

Chọn “no” để không thay đổi IPv6

```

Current Interface Information
-----ManagementIF-----
IPADDRESS: 192.168.2.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.2.1
-----ListenIF-----
IPADDRESS: 192.168.1.149
NETMASK: 255.255.255.0
GATEWAY: 192.168.1.1
-----

Would you like to change Management IP address? yes or no: yes
New ip address: 10.10.1.100
New netmask: 255.255.255.0
New gateway: 10.10.1.1
New Name Server: 8.8.8.8
Would you like to change Listen IP address? yes or no: yes
New ip address: 10.10.2.100
New netmask: 255.255.255.0
New gateway: 10.10.2.1
Would you like to setup IPv6 for Listen IF? yes or no: no

```

Sau khi nhập xong tất cả chúng ta sẽ chọn “yes” để khởi động lại

```

Apply configuration requires Restarting System!!! Would you like to apply configuration? yes or no: yes

```

Chọn 1 để xem các cấu hình card mạng đã thiết lập


```
Current Interface Information

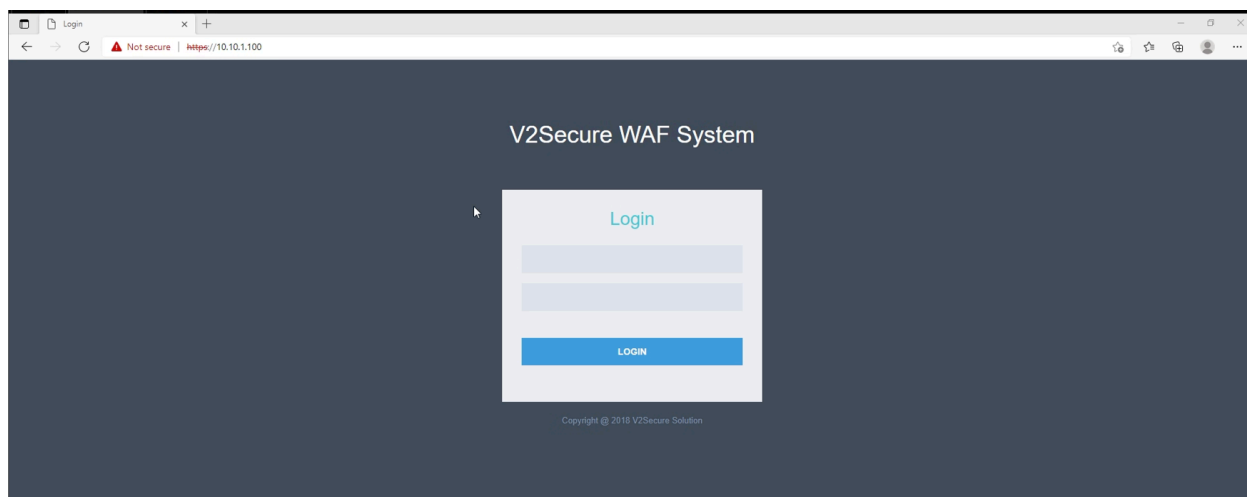
MANAGEMENT INTERFACE
Name ens160
Status UP
MAC address 08:0c:29:75:69:8e
IPv4 address 10.10.1.100

LISTEN INTERFACE
Name ens192
Status UP
MAC address 08:0c:29:75:69:98
IPv4 address 10.10.2.100

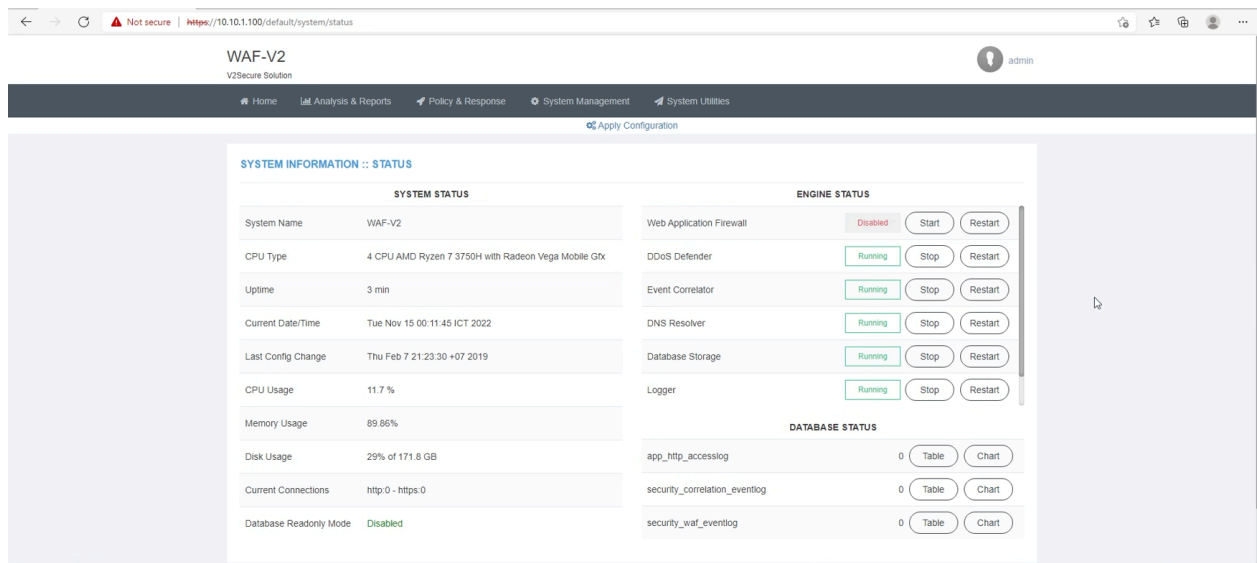
-----V2-WAF SYSTEM CONFIGURATION-----
:
: 0) Assign Interface                      9) Logger Service                      :
: 1) Interfaces Information                10) Database Service                   :
: 2) Set IP Management & Name server       11) Detection Service                 :
: 3) System Time                          12) DDoS Defence                      :
: 4) System Information                    13) Listener Service                  :
: 5) WAF Status                           14) Ping host                         :
: 6) Expert login                         15) Reboot system                     :
: 7) Restart WebService                    16) Halt system                       :
: 8) WAF Service                           17) Logout (SSH only)                 :
:
-----
```

Bước 3: Đăng nhập vào giao diện UI

Mở trình duyệt (có cùng dãy mạng, cùng card Vmnet với card ManagementIF của V2-WAF) và nhập địa chỉ IP management của máy V2-WAF vào <https://10.10.1.100>, chọn nâng cao -> Tiếp tục truy cập



Đăng nhập admin/admin



=> Giao diện UI của hệ thống V2-WAF

Sau đó, ta thu được thông tin trạng thái hệ thống:

- Thông tin trạng thái hoạt động của hệ thống

SYSTEM INFORMATION :: STATUS	
SYSTEM STATUS	
System Name	WAF-V2
CPU Type	4 CPU AMD Ryzen 7 3750H with Radeon Vega Mobile Gfx
Uptime	3 min
Current Date/Time	Tue Nov 15 00:11:45 ICT 2022
Last Config Change	Thu Feb 7 21:23:30 +07 2019
CPU Usage	11.7 %
Memory Usage	89.86%
Disk Usage	29% of 171.8 GB
Current Connections	http:0 - https:0
Database Readonly Mode	Disabled

- Thông tin trạng thái dịch vụ

ENGINE STATUS			
Web Application Firewall	Disabled	Start	Restart
DDoS Defender	Running	Stop	Restart
Event Correlator	Running	Stop	Restart
DNS Resolver	Running	Stop	Restart
Database Storage	Running	Stop	Restart
Logger	Running	Stop	Restart

- Thông tin về số lượng Log

DATABASE STATUS			
app_http_accesslog	0	Table	Chart
security_correlation_eventlog	0	Table	Chart
security_waf_eventlog	0	Table	Chart

Phần tiếp theo (Part 2) sẽ tìm hiểu về các function cơ bản và nâng cao của V2-WAF (to be continue)