Tasks

1- install splunk

2- install forwarder

3- configure Domain Controller

4- install Xampp Web app server

5- install Pfsense firewall

6- install Suricata IPS/IDS

6- configure DVWA vulnerable Web app on xampp

7- configure securityMod WAF To detect web app attacks

8- write rule in splunk to generate alert

9- detect Active Directory Attacks

splunk install

1- Download Splunk

2- sudo dpkg -i splunk.deb

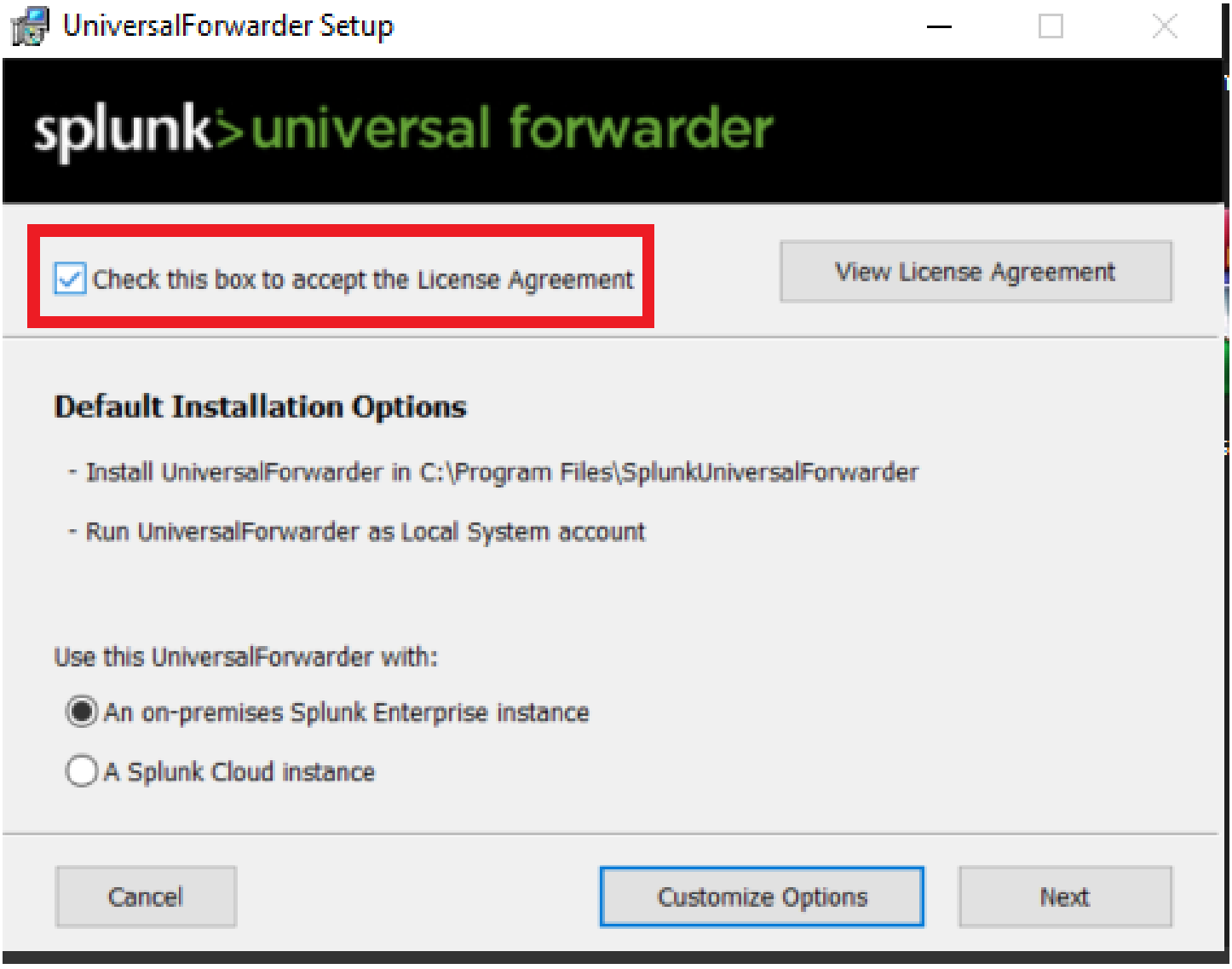
3- sudo /opt/splunk/bin/splunk start --accept-license

4- sudo /opt/splunk/bin/splunk enable boot-start

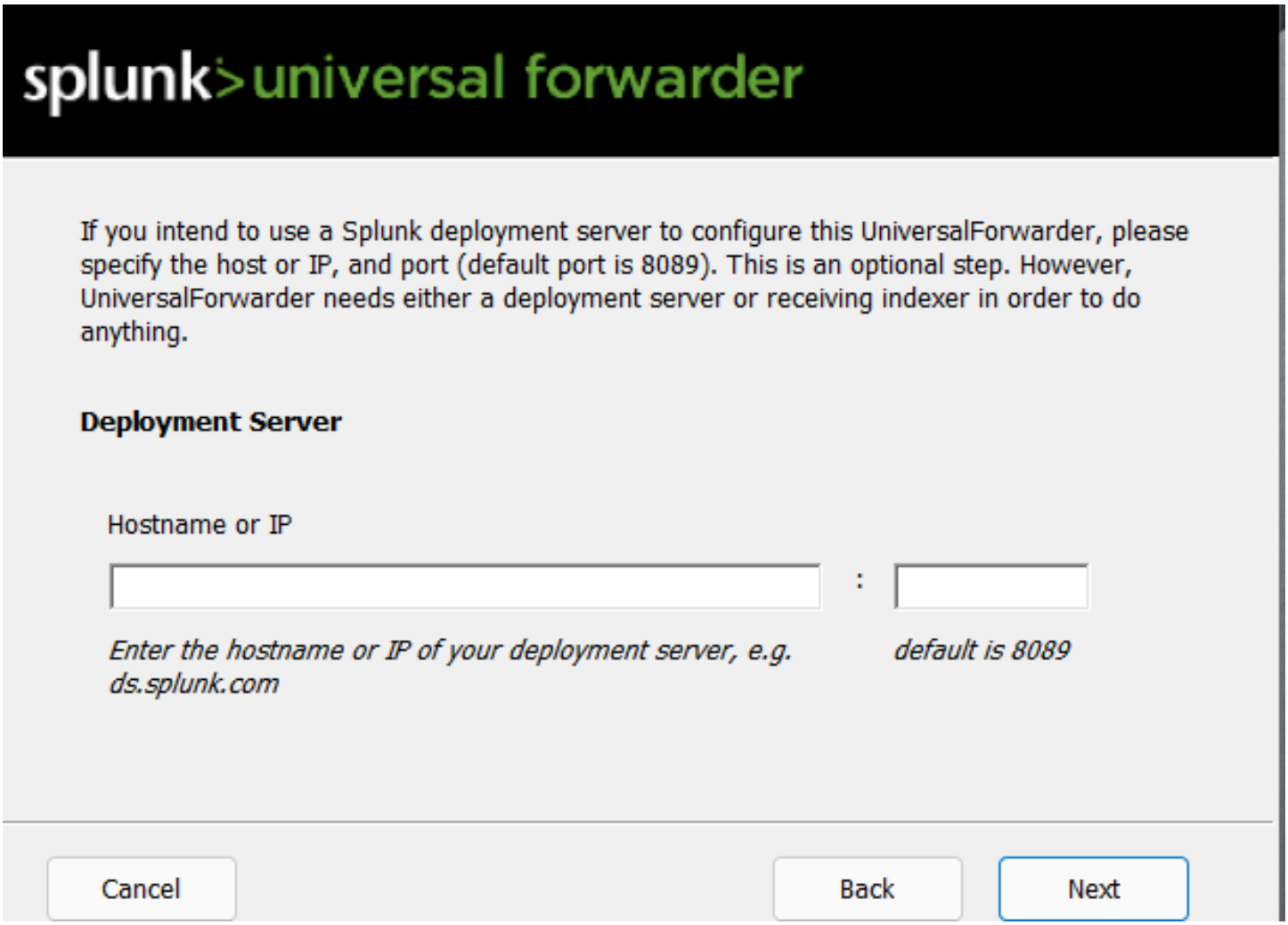
you can access splunk via web browser
http://127.0.0.1:8000

install forwarder

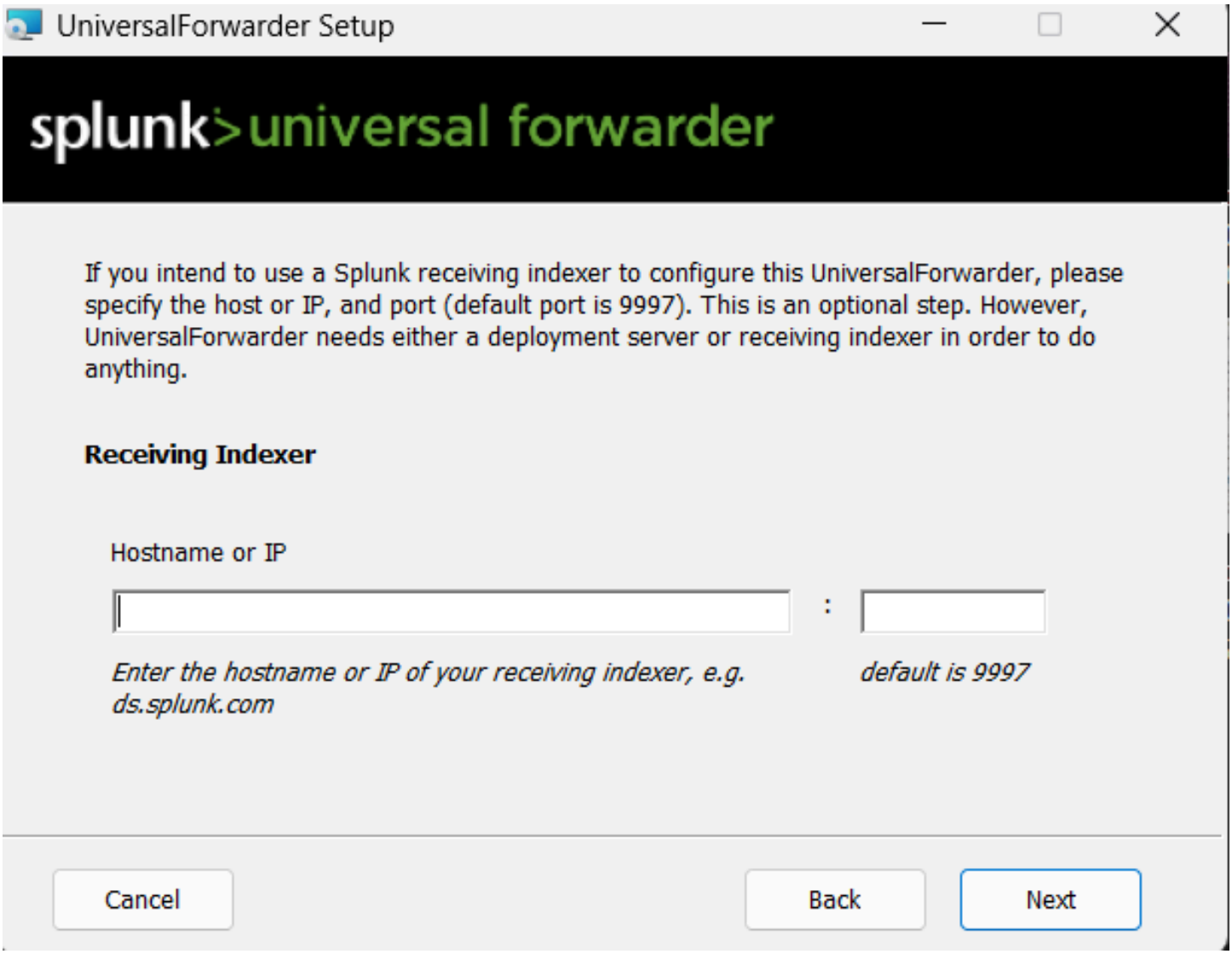
Download [Forwarder]



Add Splunk Machine IP Address And Default Port Like ==> 192.168.1.20:8089



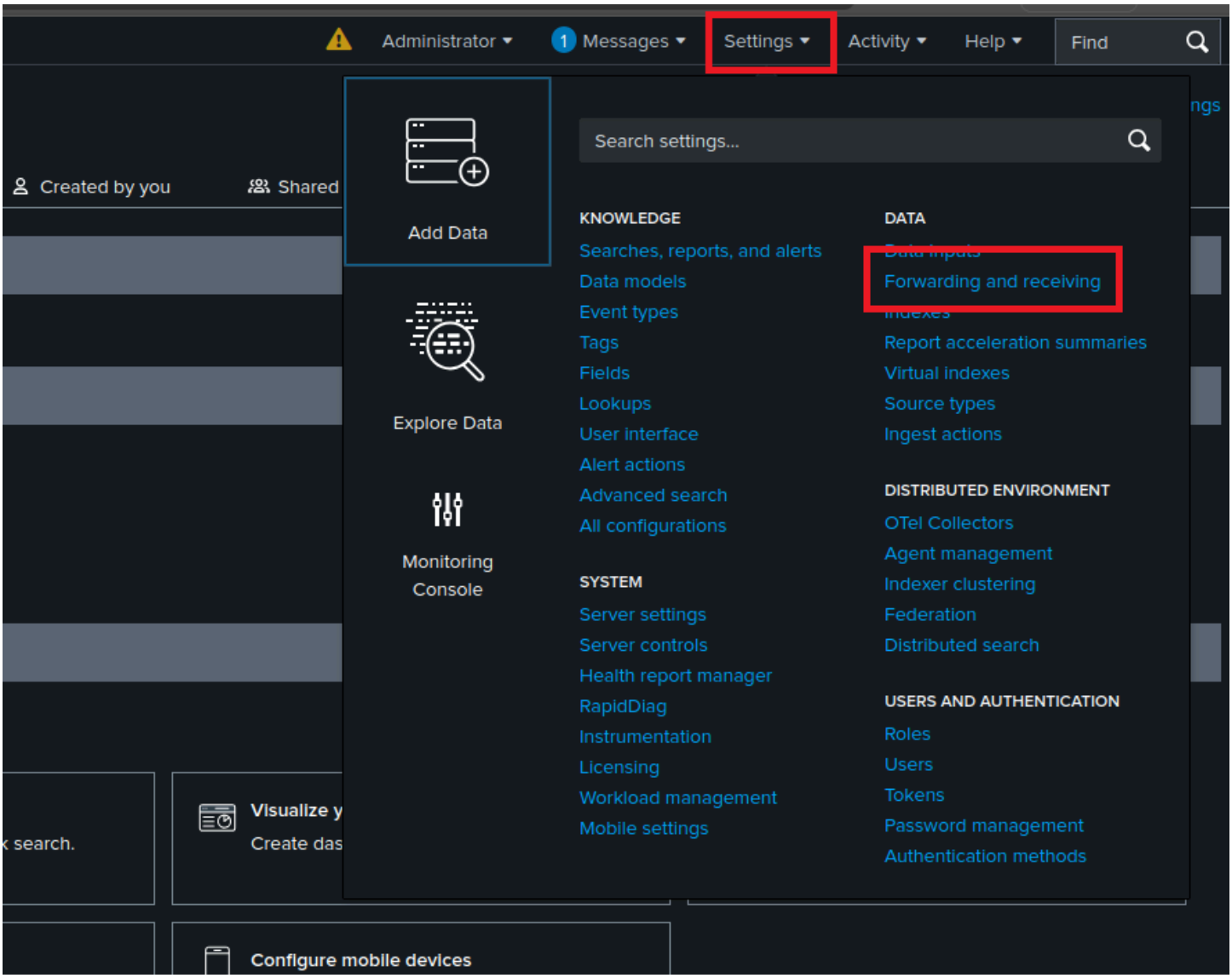
Add Splunk Machine IP Address And Default Port Like ==> 192.168.1.20:9997

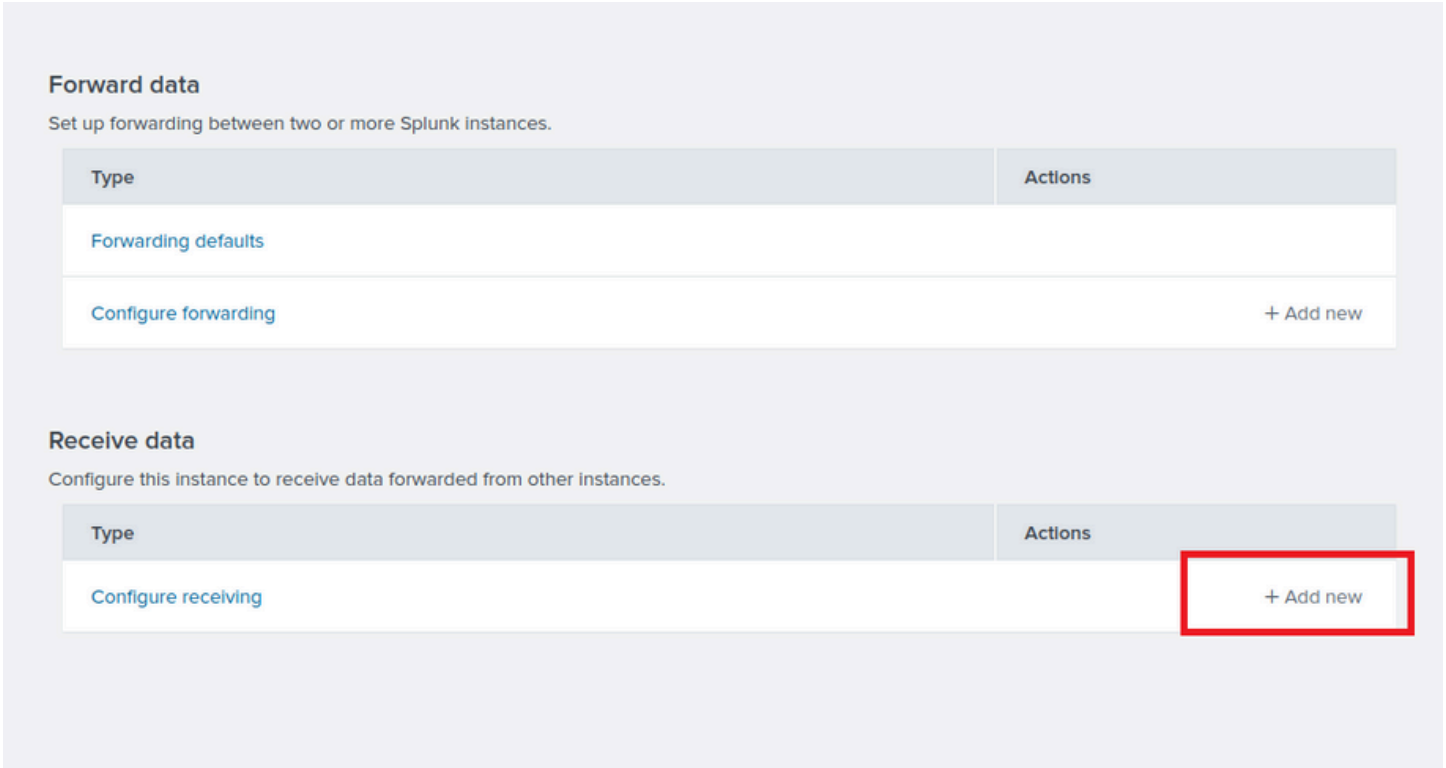


Configure Receiving In Splunk

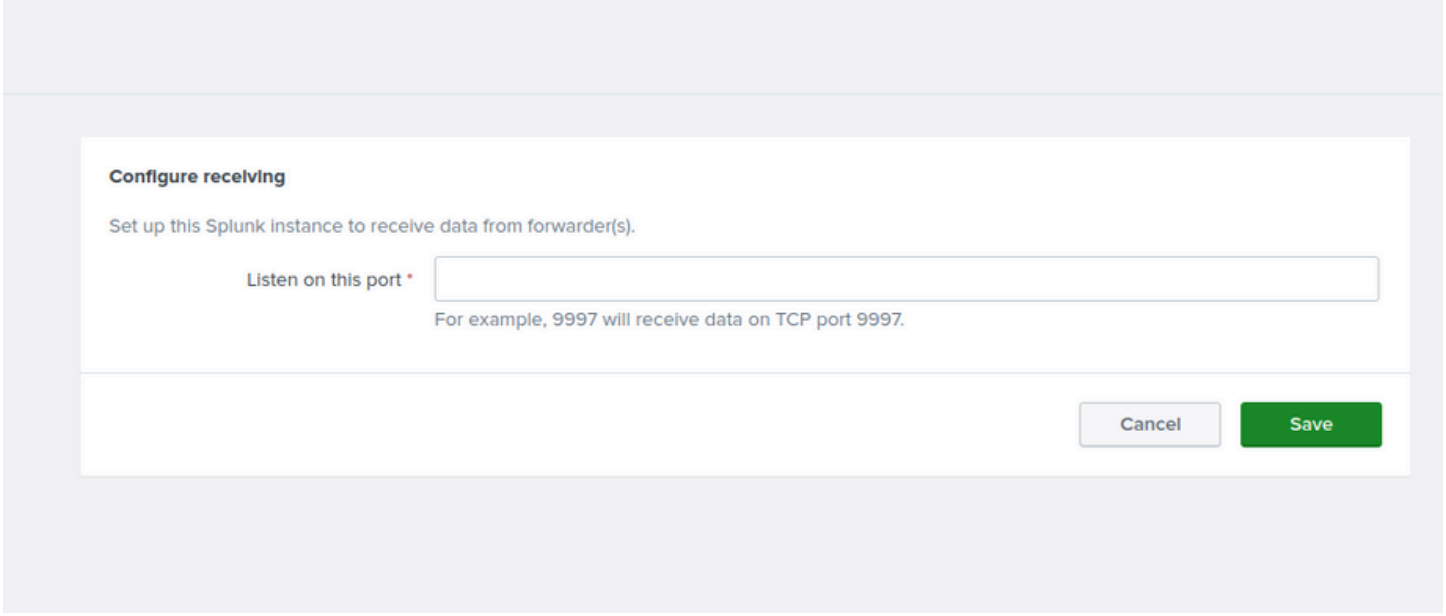
Note:

Make sure allow traffic through Firewall port 8089, 9997 on Windows Machine And Linux Machine

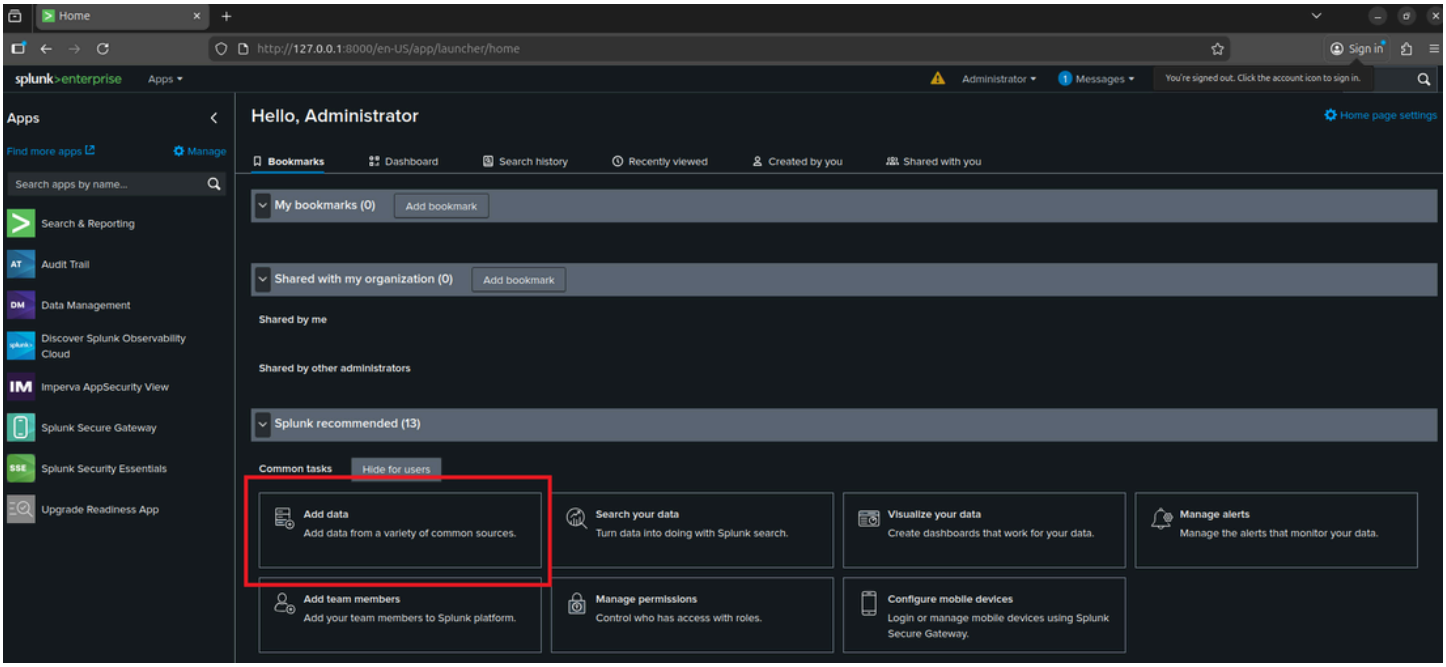


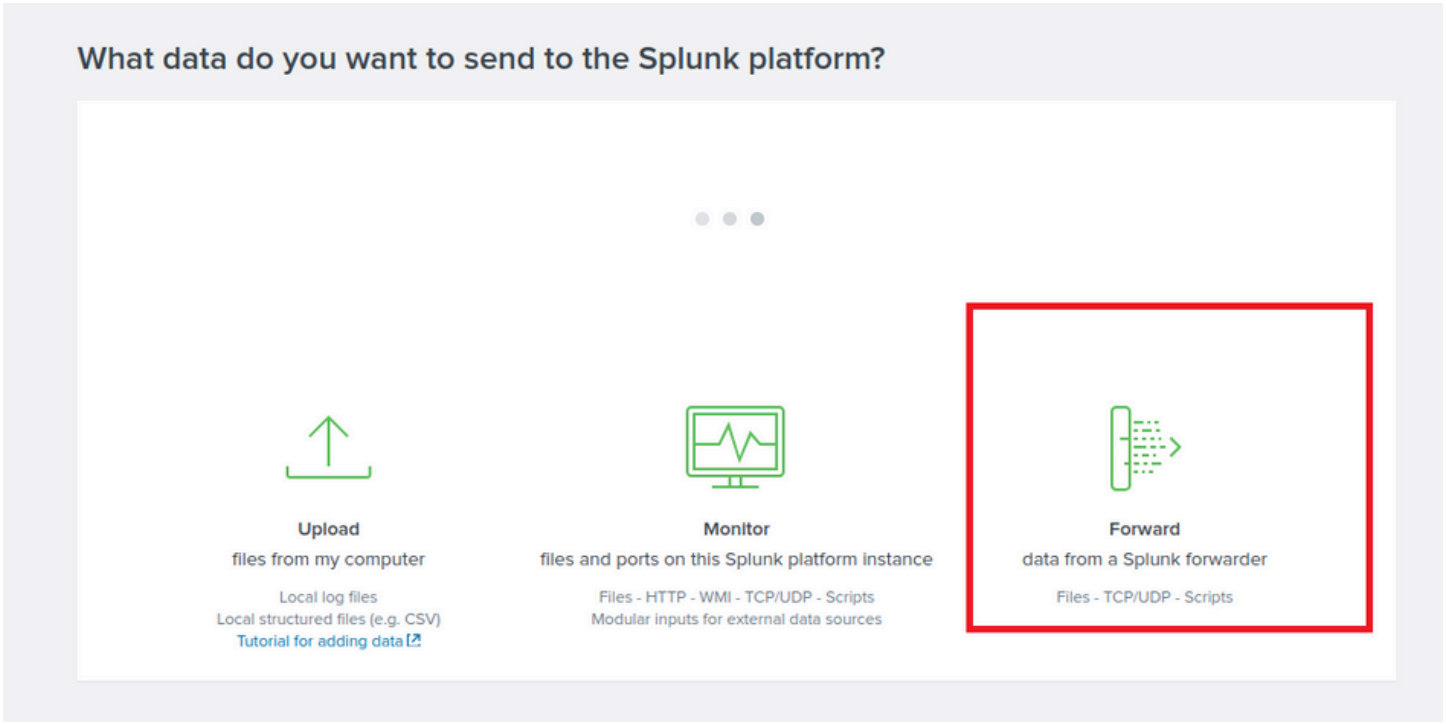


Write Default Port 9997



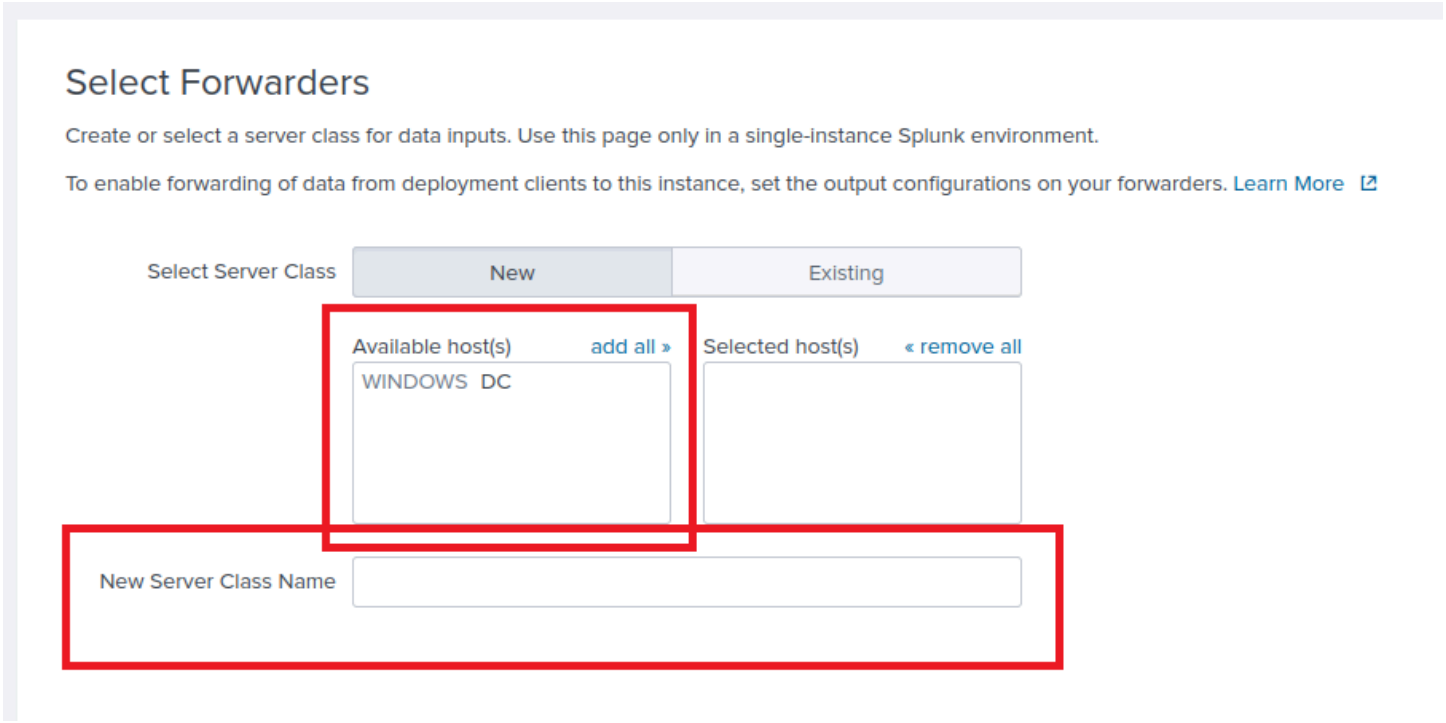
Add Date In Splunk

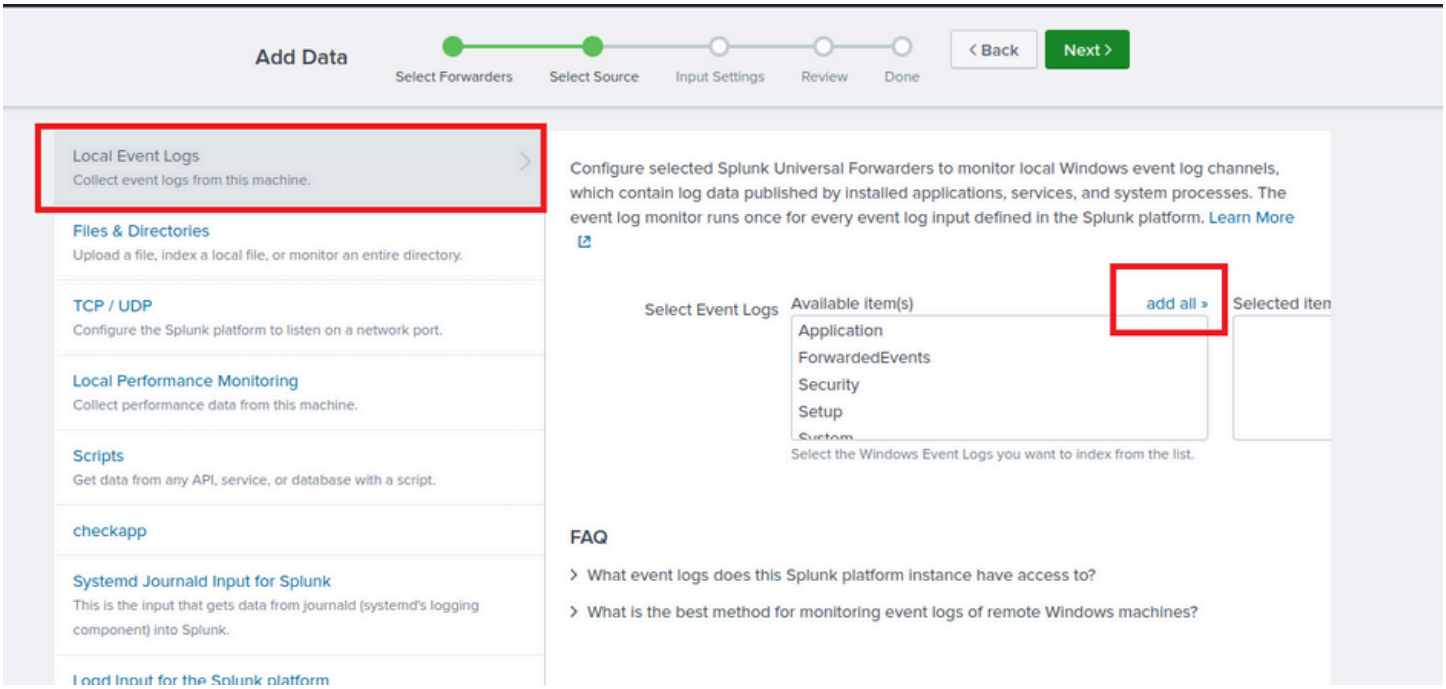


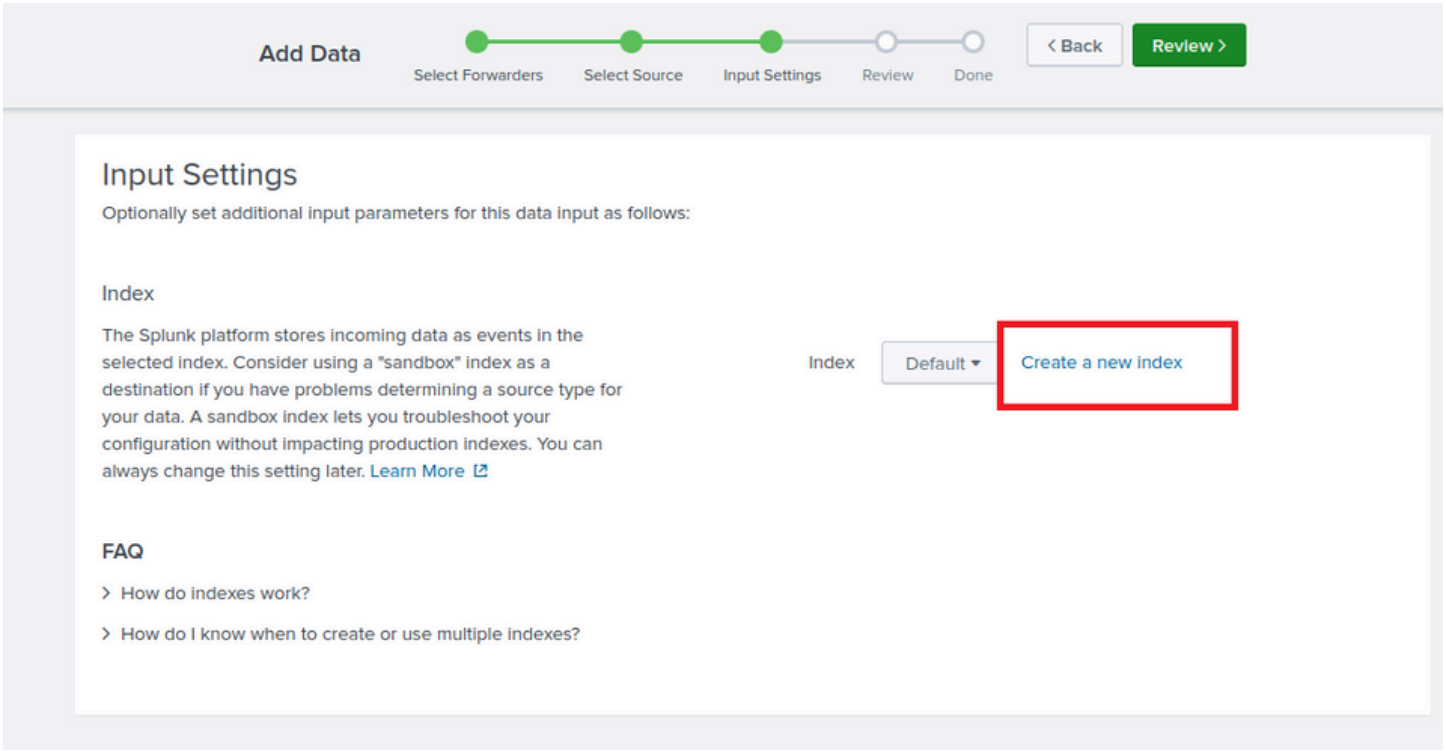


1- Select host from Available Host

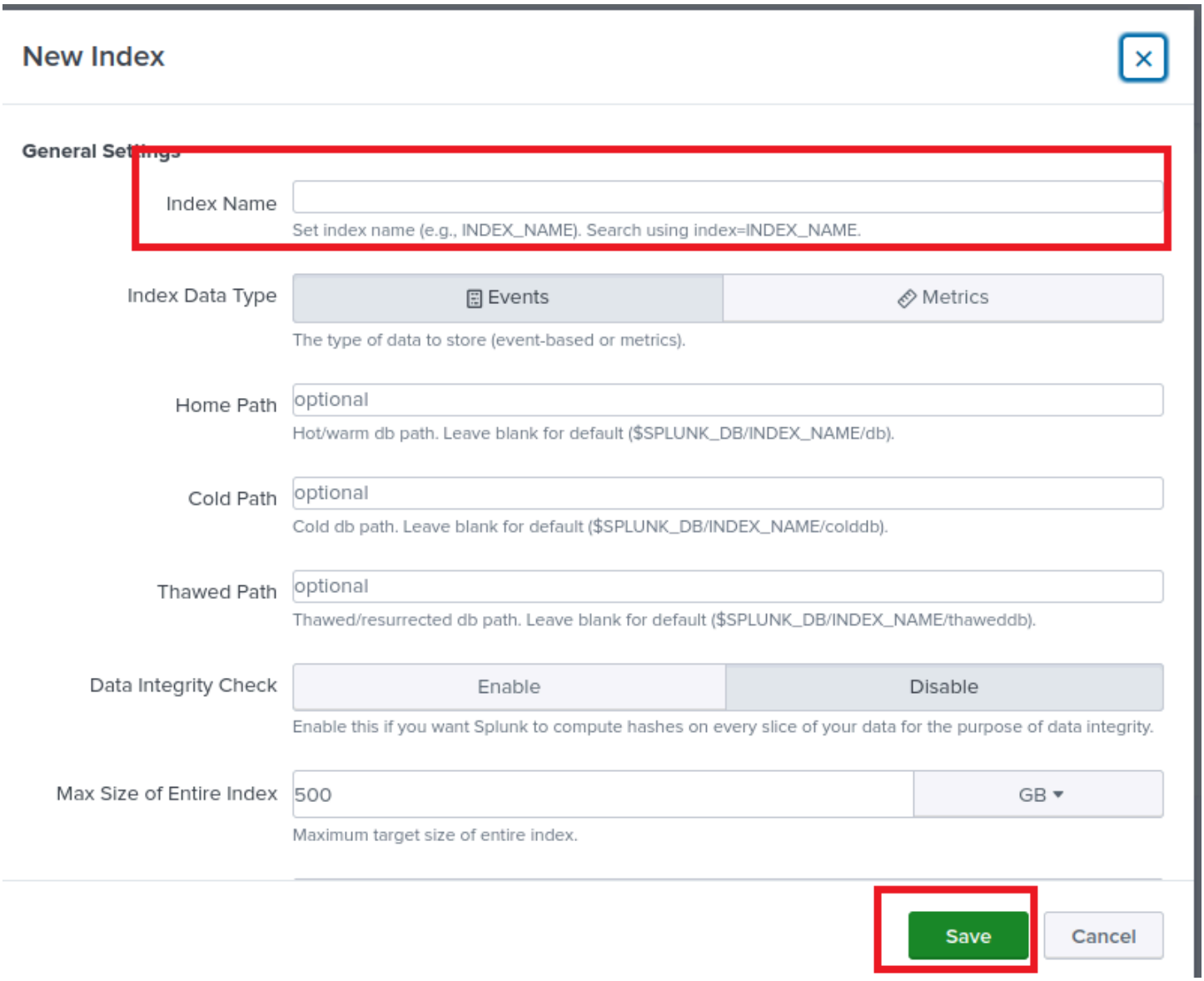
2- Add A New Host Name







Create New Index Name PC-01



After Create It Choose It And Click Rivew And Done

Install And Configure Sysmon:

Download Sysmon

Download Configuration File

Copy Configuration file to Sysmon Directory

Open PowerShell OR CMD As Administrator

Command:

Sysmon64.exe -accepteula -i sysmonconfig.xml

Send Sysmon Logs To Splunk

Go To This Path ==>
C:\ProgramFiles\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

Open Inputs.conf file And Add this

[WinEventLog://Microsoft-Windows-Sysmon/Operational]

disabled = false

renderXml = true

source = XmlWinEventLog:Microsoft-Windows-Sysmon/Operational

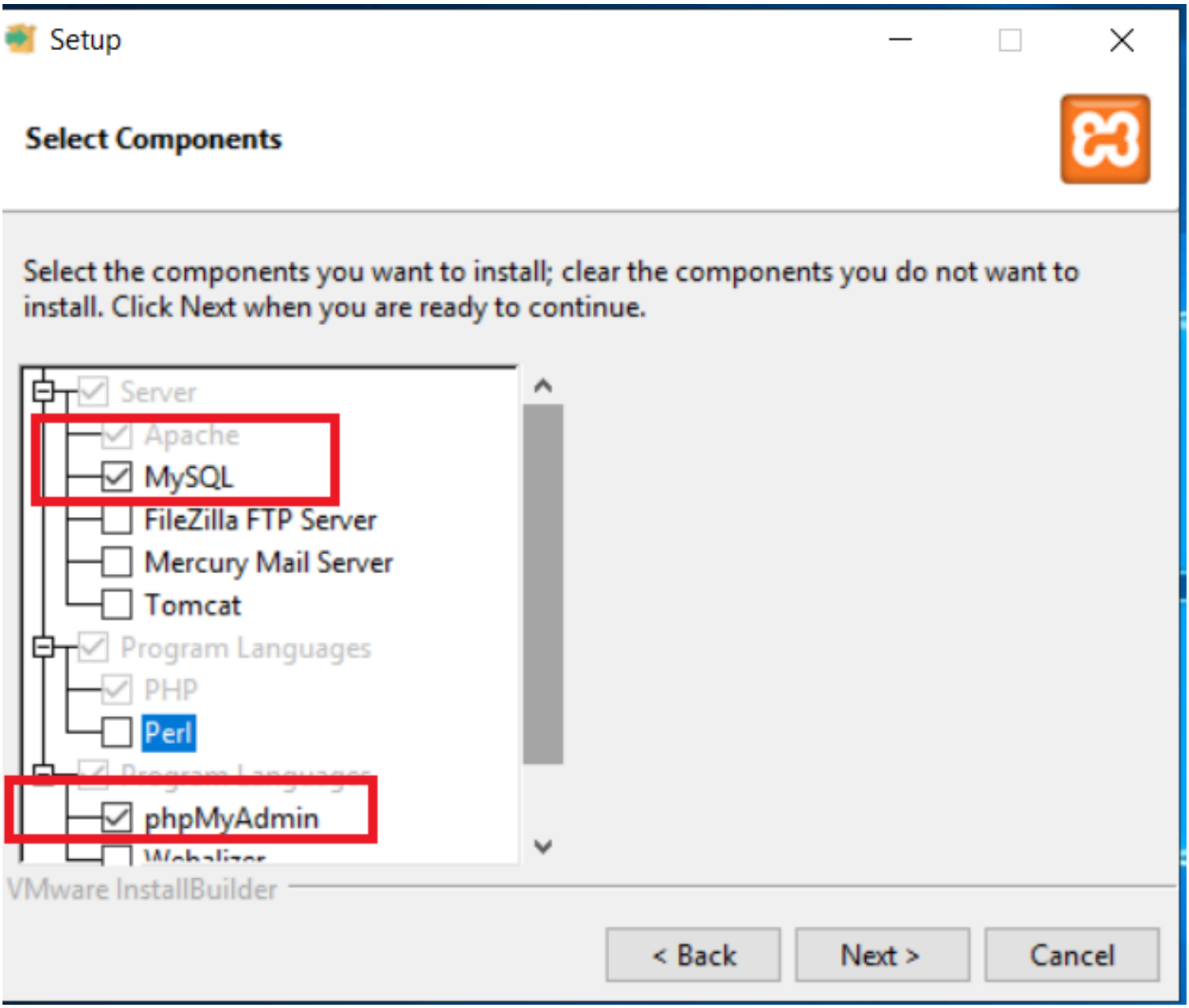
index = PC-01

Install Xampp Server On windows Server To Configure DVWA Lab

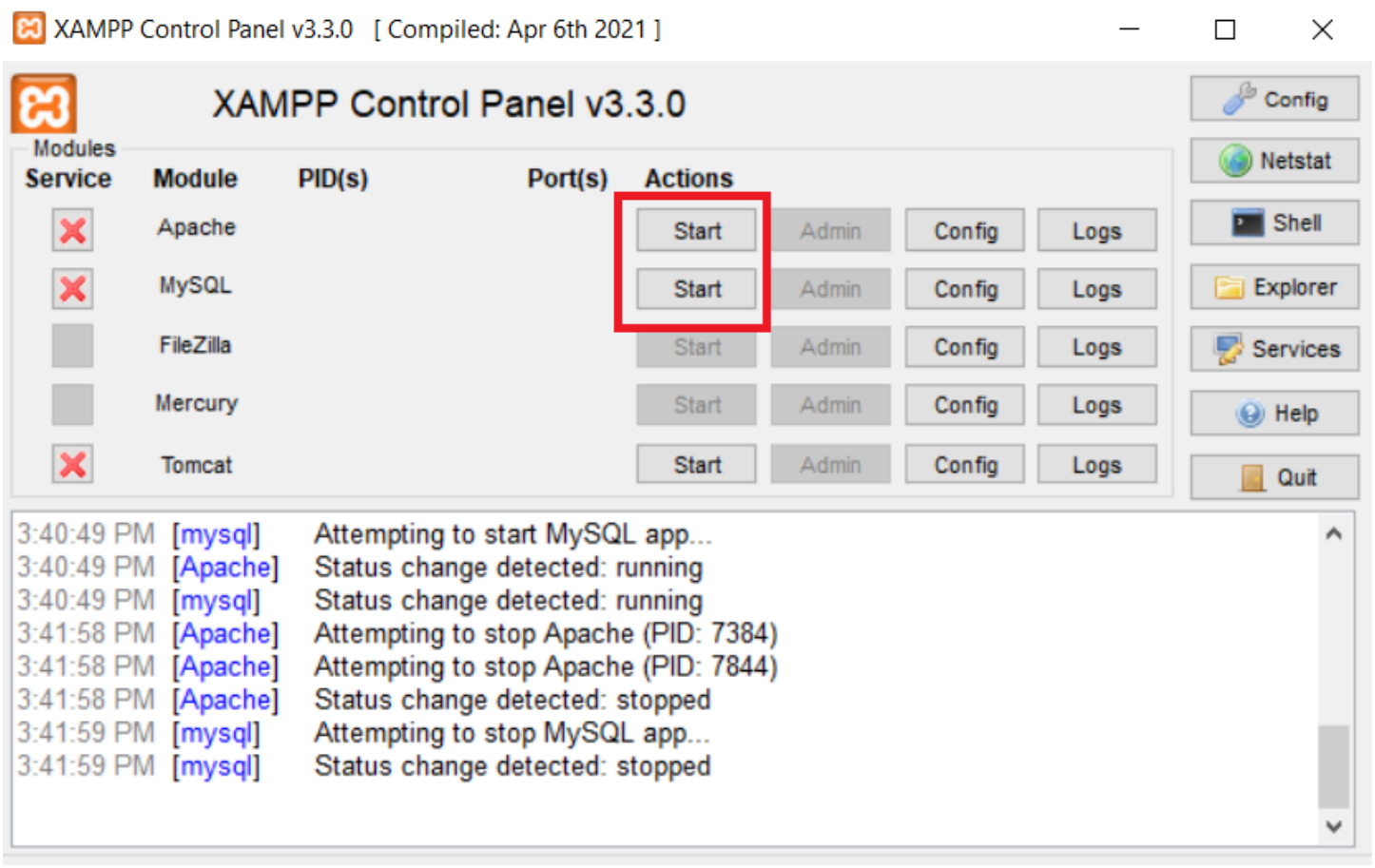
Download Xampp

Installation Process Like As Any exe File Click Next Next...BlaBlaBla

Note: Make Sure Choose this Options



When Installation Complete Successfully Open App You will Show This, Click Start On Apache And MySQL



Configure DVWA Vulnerable Web App

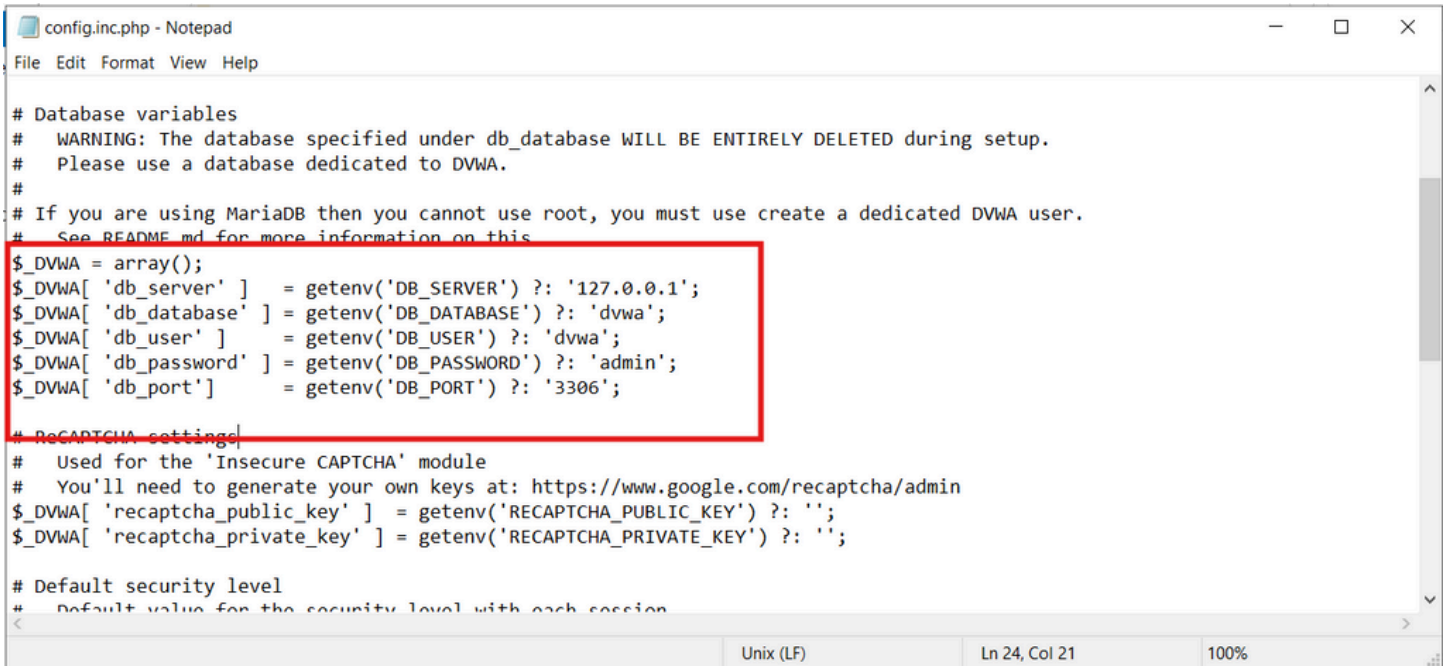
Download DVWA

After Download It Extract File And Rename It dvwa And Copy To This Path ==> C:\xampp\htdocs

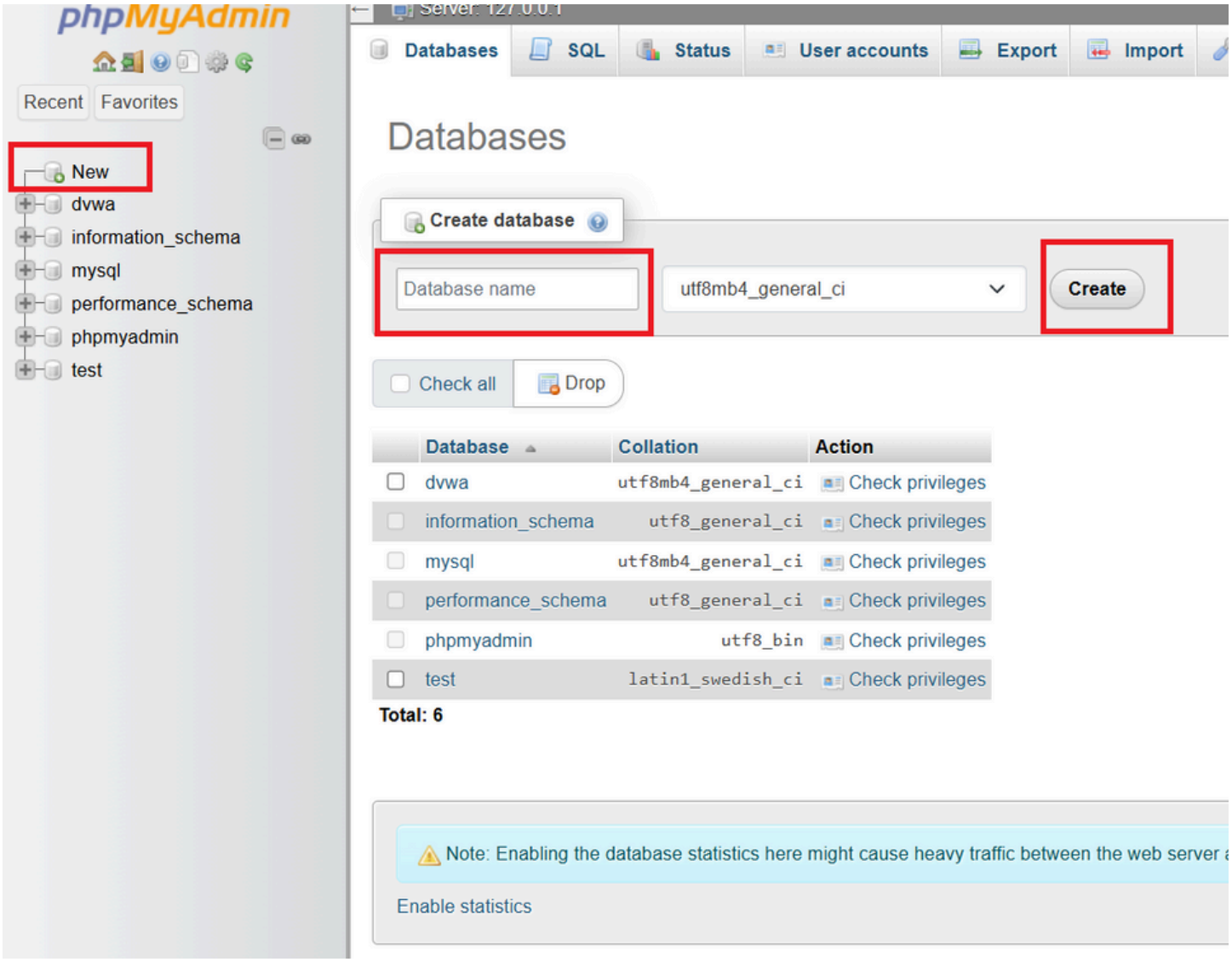
now you need edit dvwa configuration file from this path ==> C:\xampp\htdocs\dvwa\config

you can see file name config.inc.php.dist rename it config.inc.php and open file

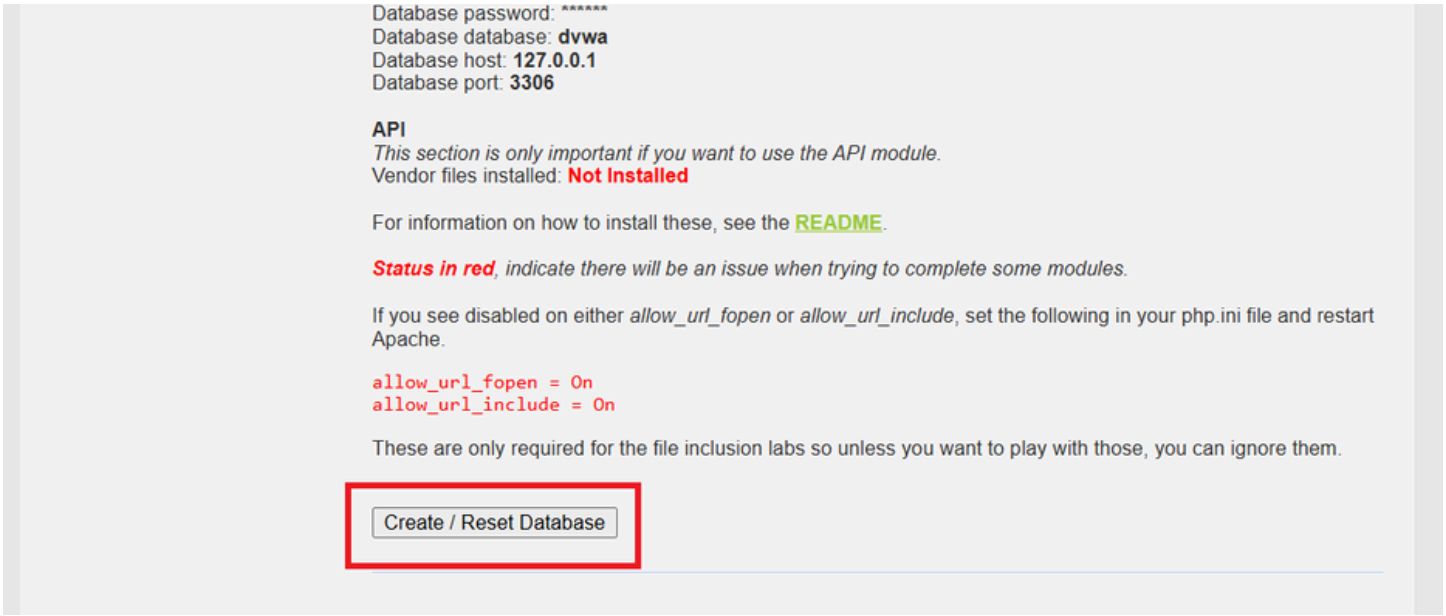
Add username and password you will use it to login



now we will configure Database open http://127.0.0.1/phpmyadmin/ in your browser to create dvwa Database

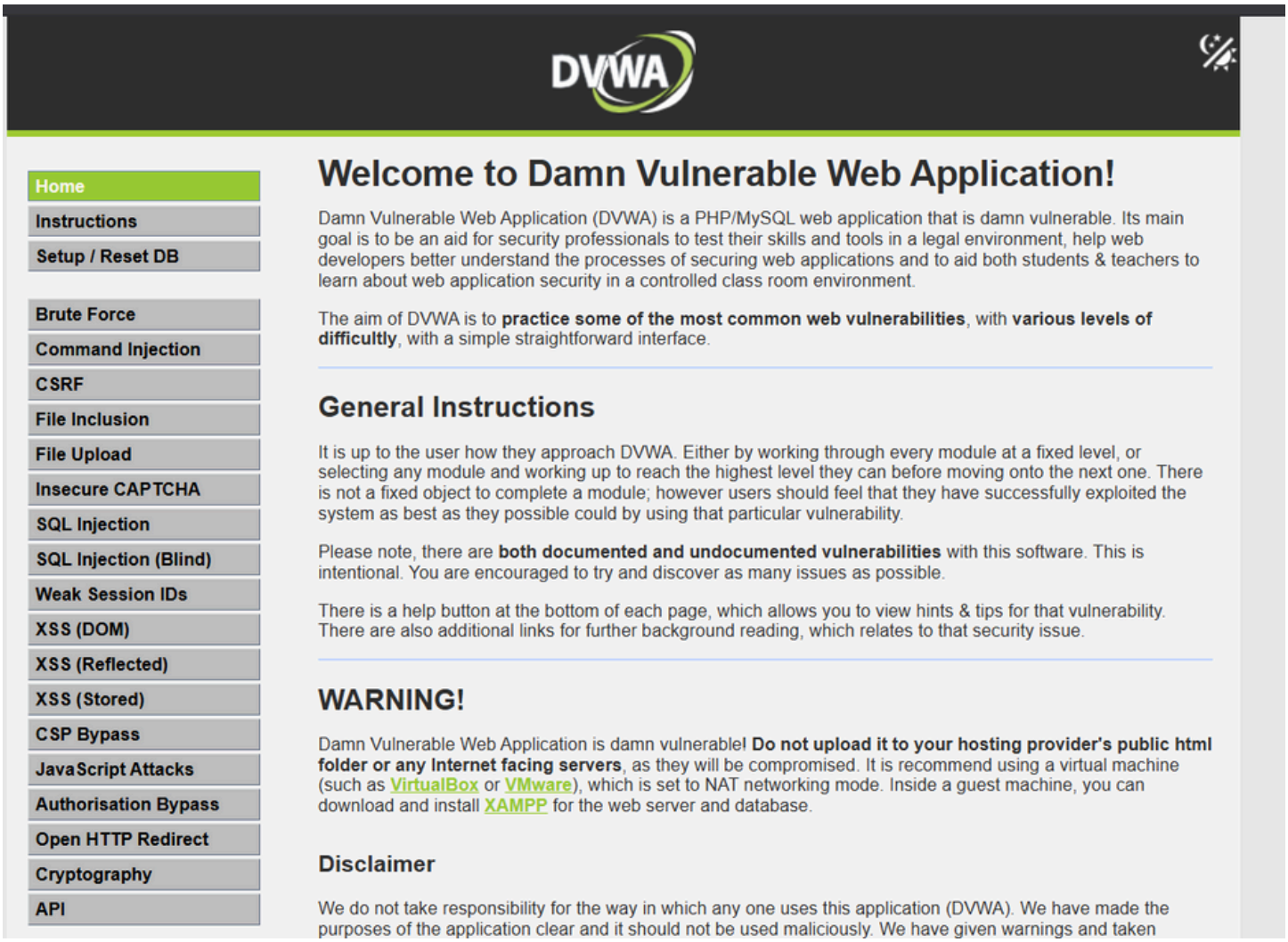


Now Open dvwa in your browser http://127.0.0.1/dvwa/ And scroll Down And click Create / Reset Database



Now Refresh browser and login via this credential admin:password

Congratulations



now create a new index in splunk name webapp to send logs add this configuration in inputs.conf >> C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

[monitor://C:\xampp\apache\logs\access.log]

sourcetype = apache:access

index = webapp

disabled = false

[monitor://C:\xampp\apache\logs\error.log]

sourcetype = apache:error

index = webapp

disabled = false

install WAF

download mod security WAF from here

unzip file and copy mob_security2.so to >> C:\xampp\apache\modules

create config file name modsecurity.conf in >> C:\xampp\apache\conf and add this settings

SecAuditLog "C:/xampp/apache/logs/modsec_audit.log"

SecDebugLog "C:/xampp/apache/logs/modsec_debug.log"

SecRuleEngine DetectionOnly

SecRequestBodyAccess On

SecAuditEngine On

SecAuditLogParts ABC

Note: We will use the WAF here to capture the request body, and we will not rely on the default rules because we want to try writing custom rules by hand and generate alert

now create a new index in splunk name waf to send logs to splunk add this configuration in inputs.conf >> C:\Program Files\SplunkUniversalForwarder\etc\apps\SplunkUniversalForwarder\local

[monitor://C:/xampp/apache/logs/modsec_audit.log]

disabled = false

index = waf

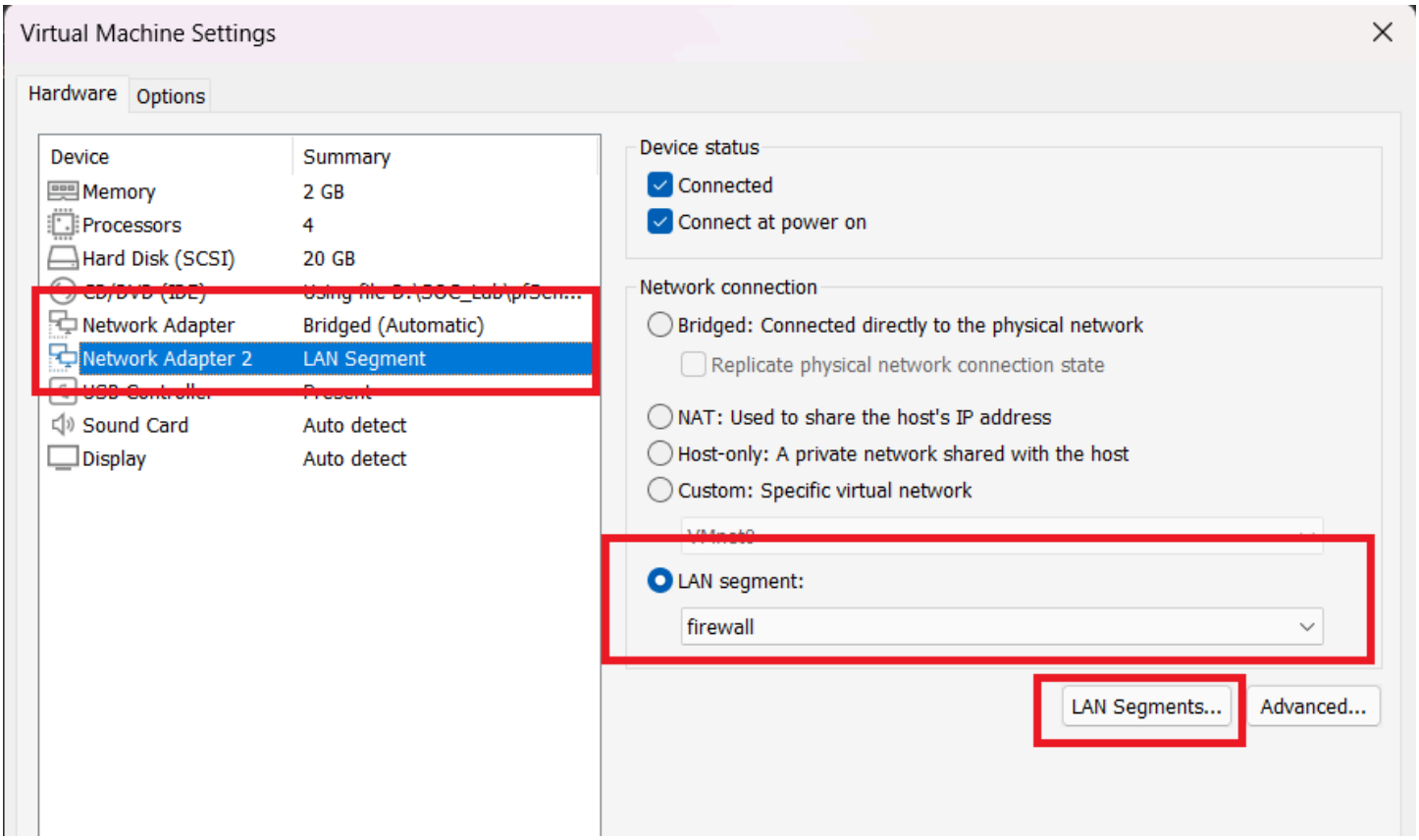
sourcetype = modsecurity:json

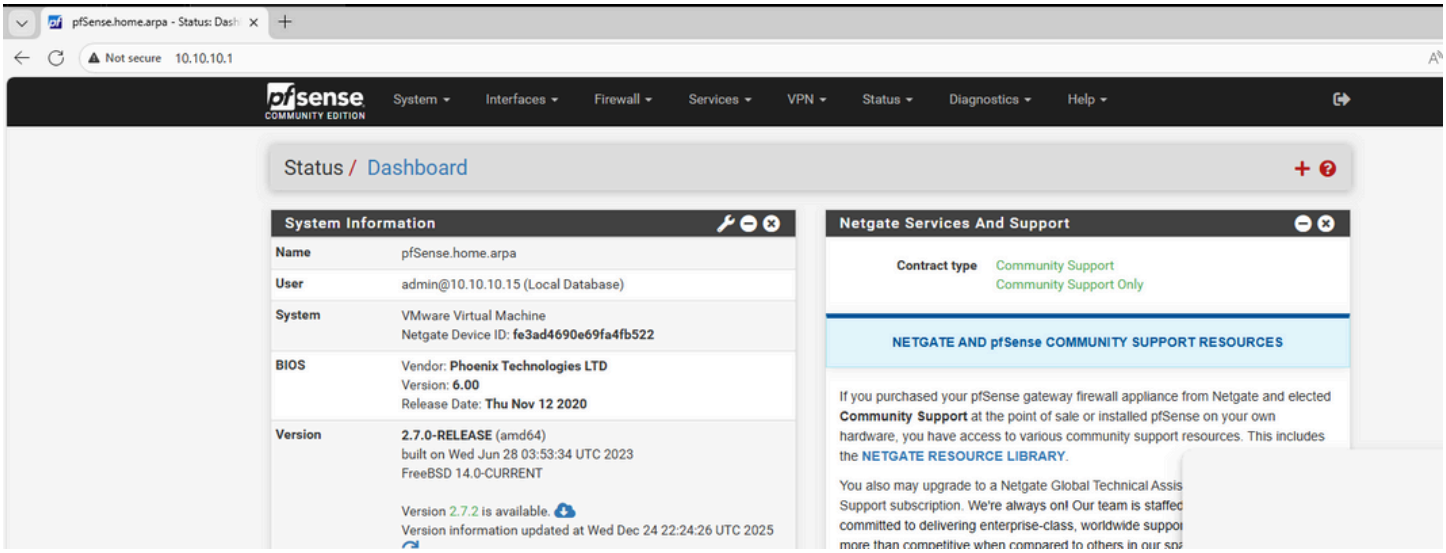
Install pfsense FW

download pfsense

install it in VMware

create a 2 network card (LAN, Bridge) Ip some thing like 10.10.10.1/24 WAN 192.168.1.0/24 after installation complete access Pfsense from any Machine in NAT card via web browser by pfsense ip 10.10.10.1

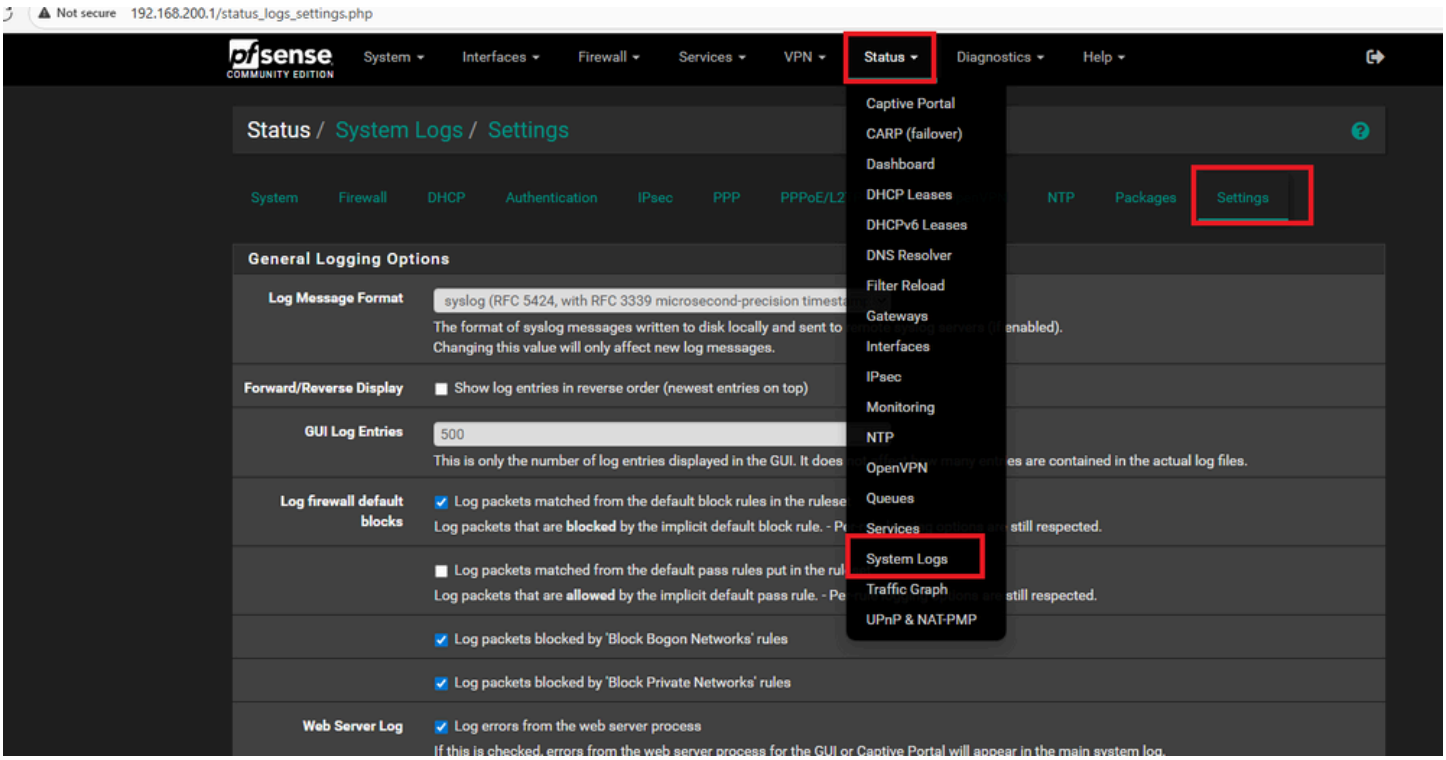




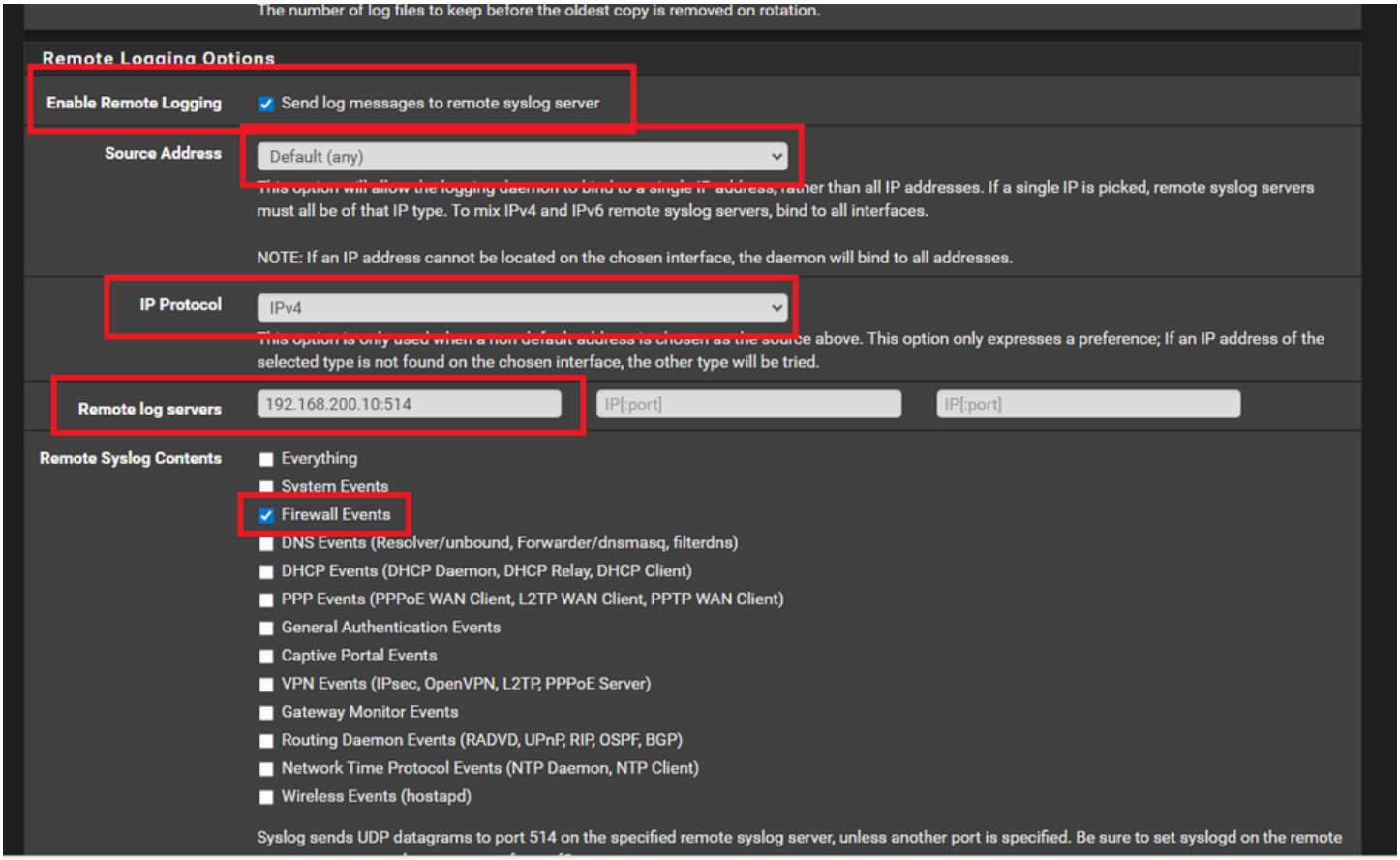
require check update from Tab >> System >> update

Notes: add all VM machine in LAN Network add statice Ip Range 192.168.200.0/24 Subnet 255.255.255.0 Default Gateway firewall Ip like 192.168.200.1

now send logs to splunk

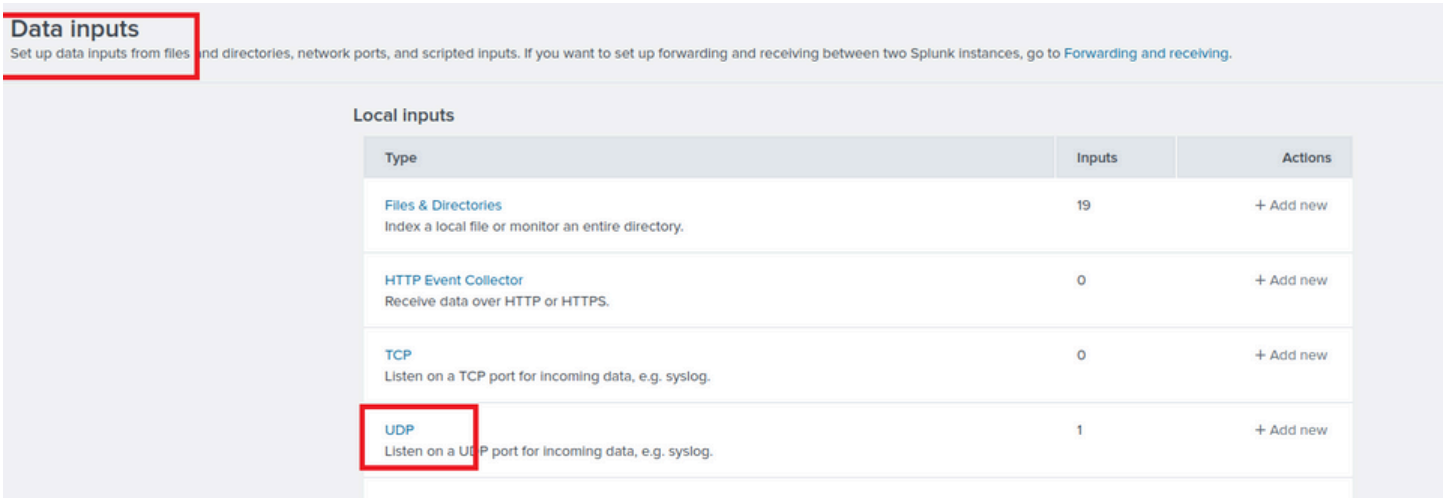


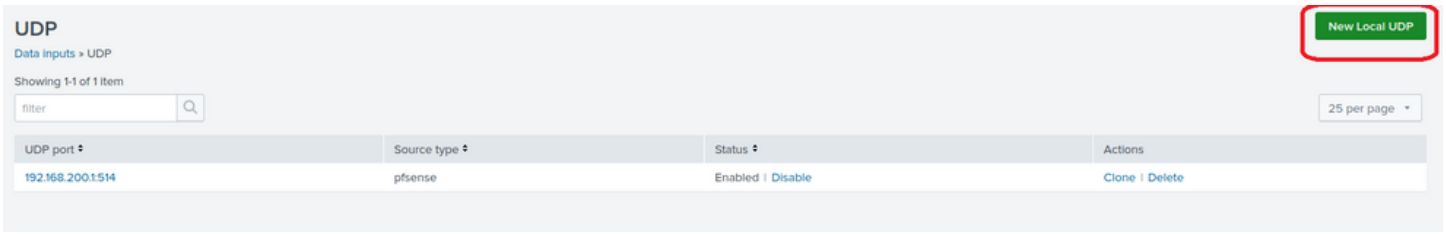
scroll down to

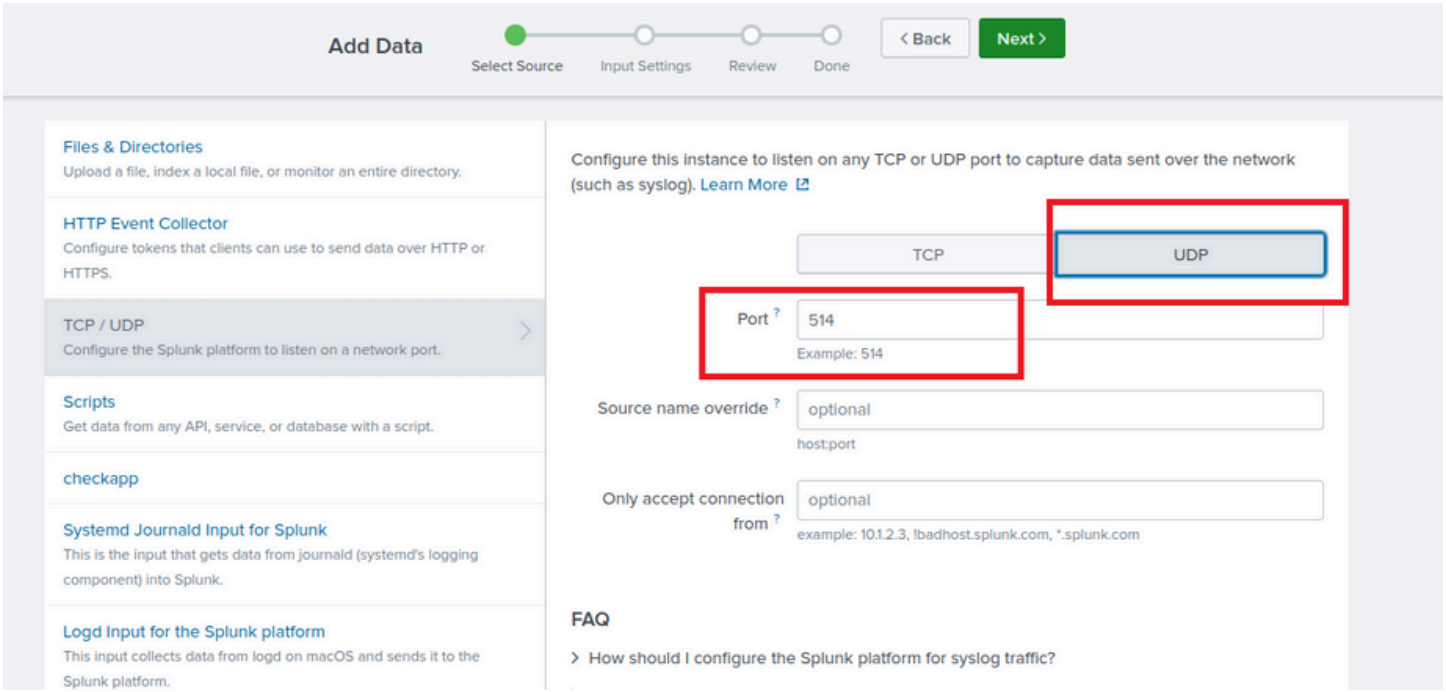


and click save

now configure receiving in splunk >> settings >> data inputs >> UDP

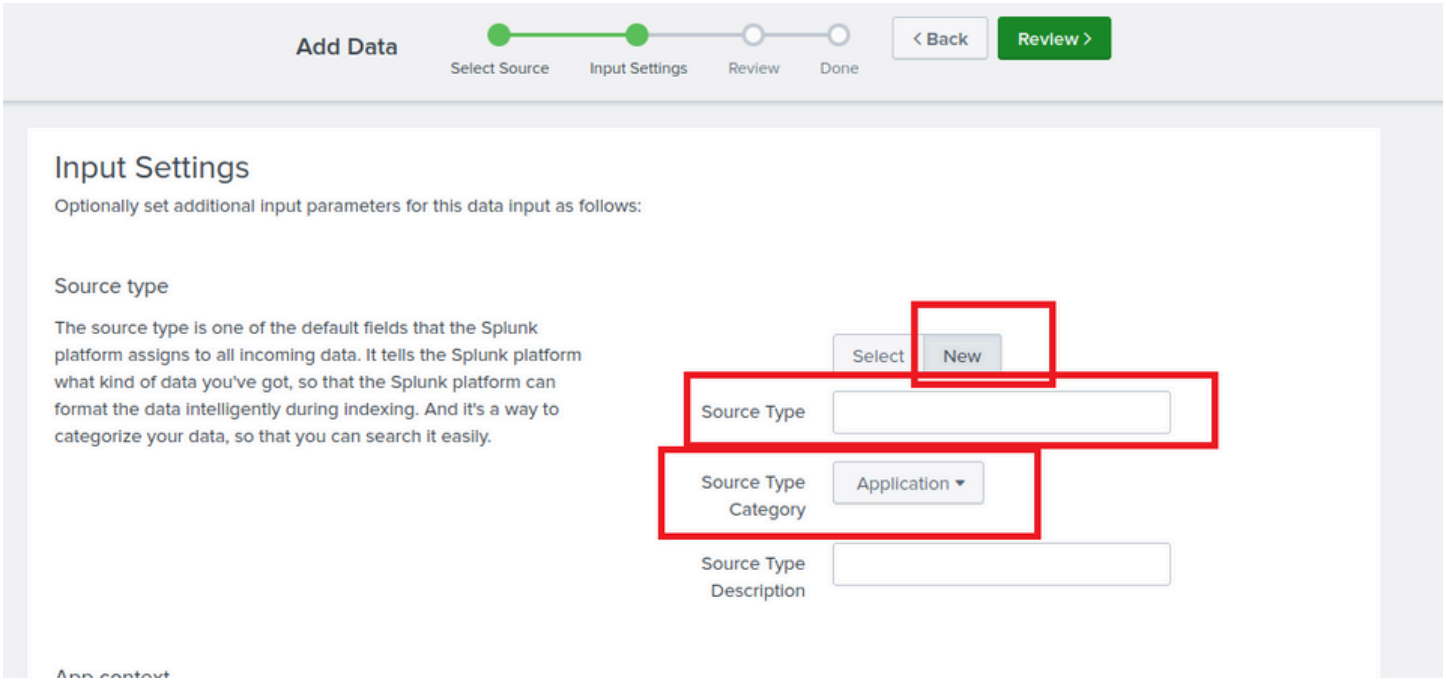




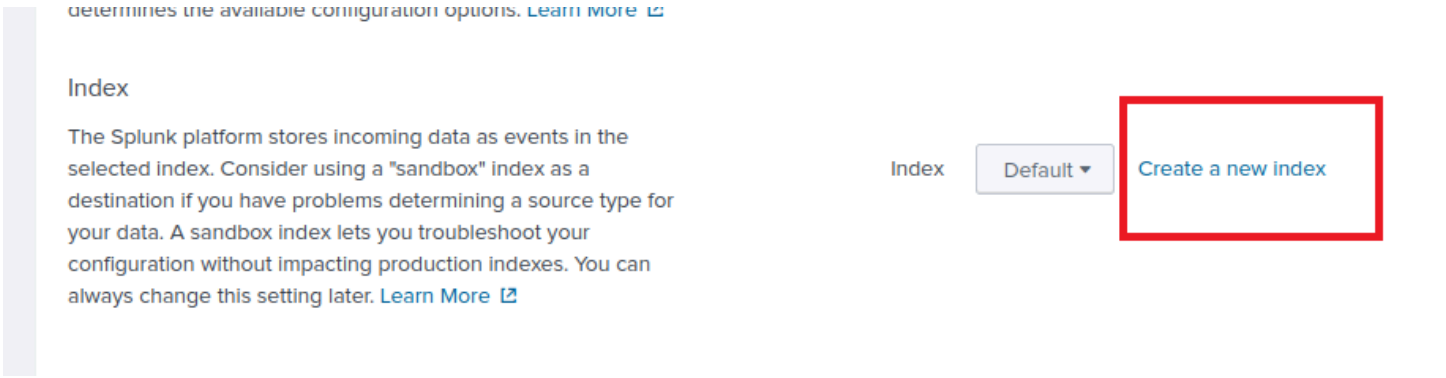


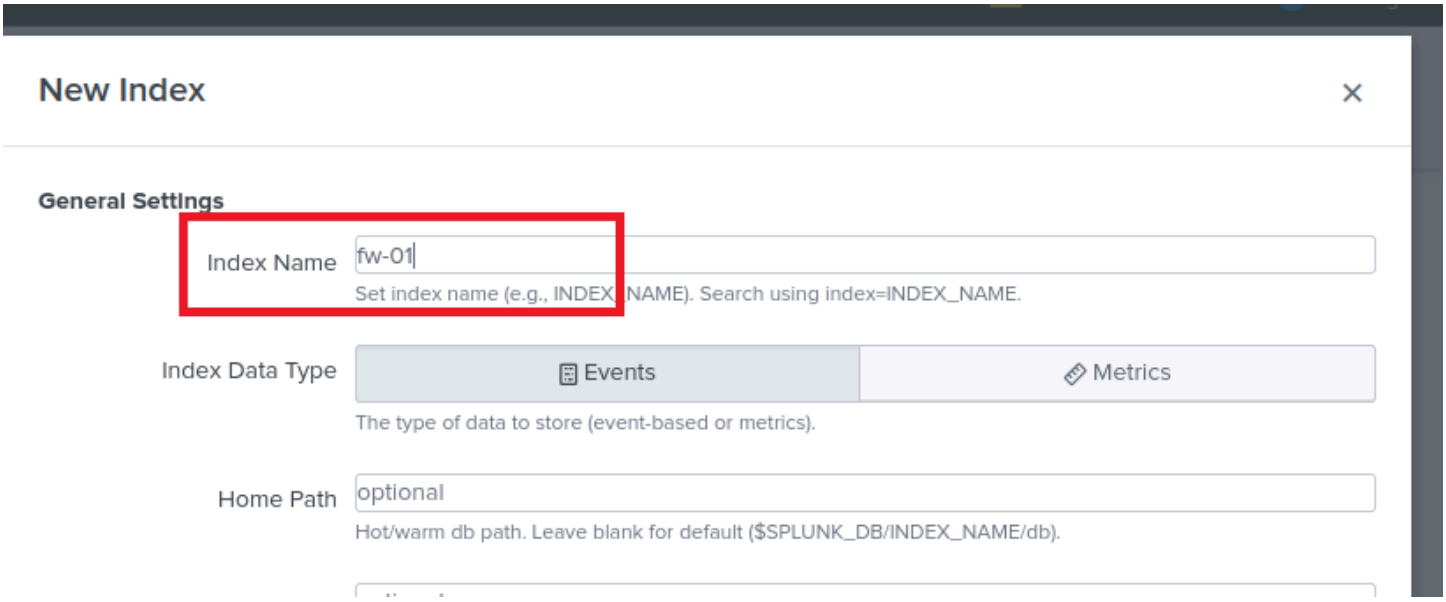
and click next

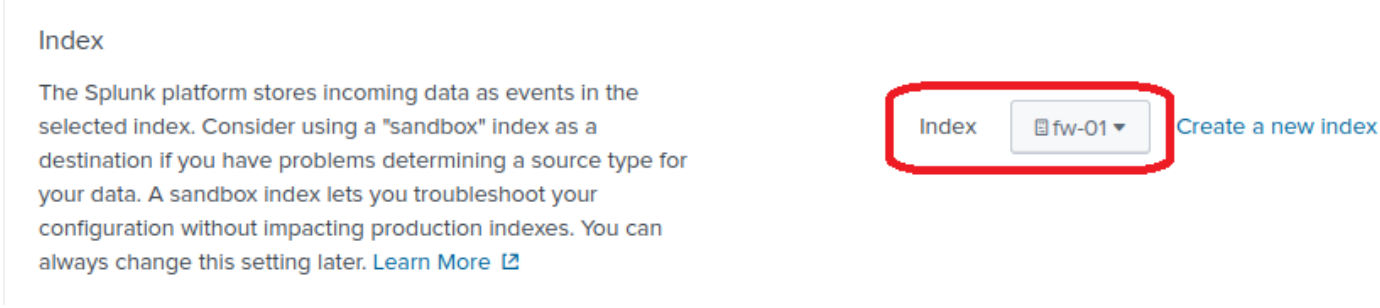
source Type pfsense



scroll down to

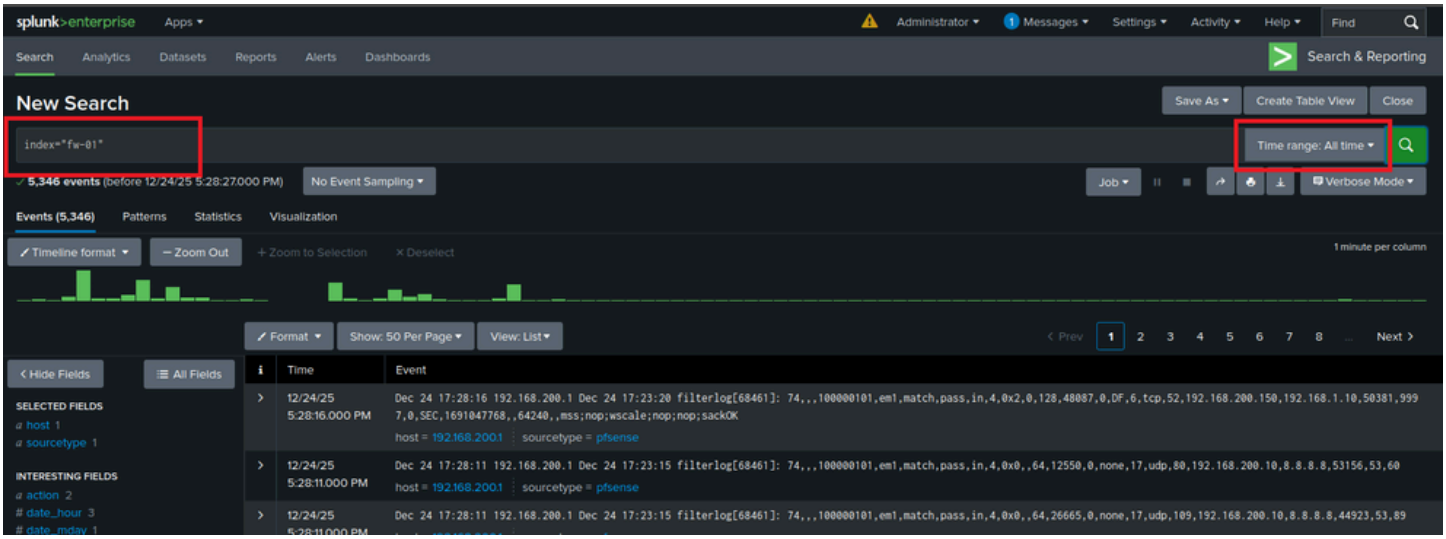






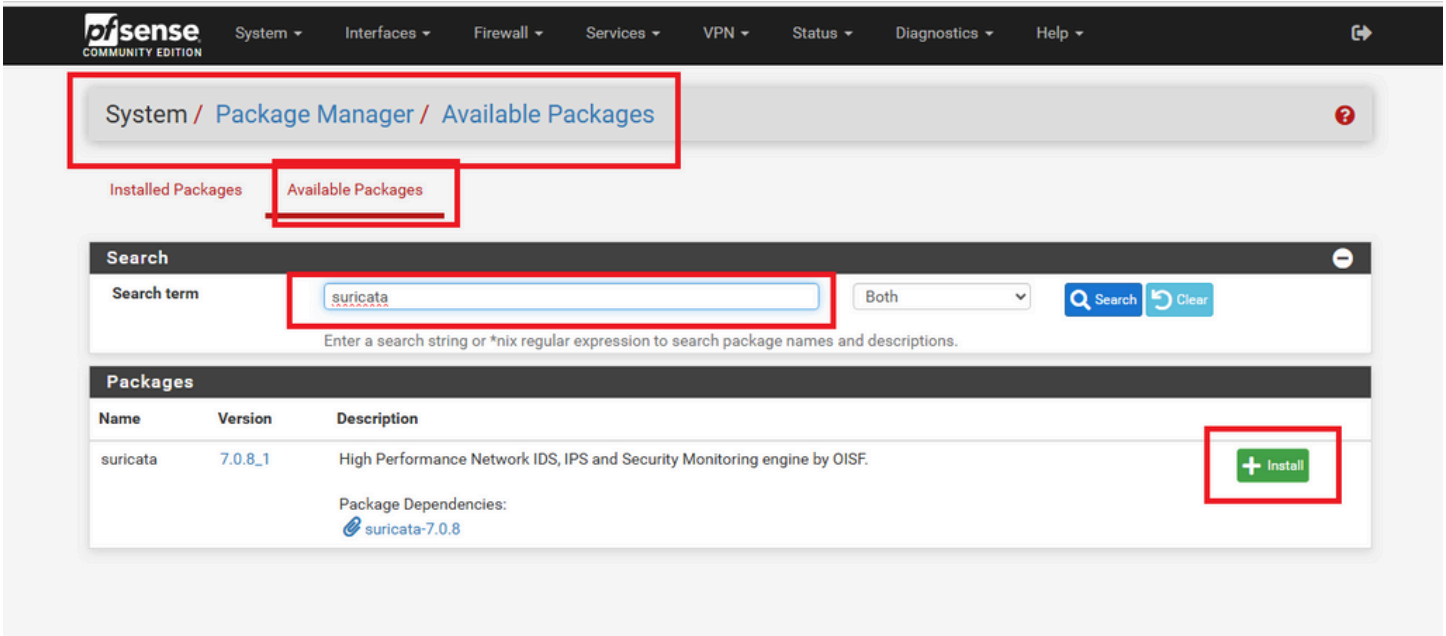
click Review >> submit

check logs send succefuly



Install Suricata IPS/IDS System

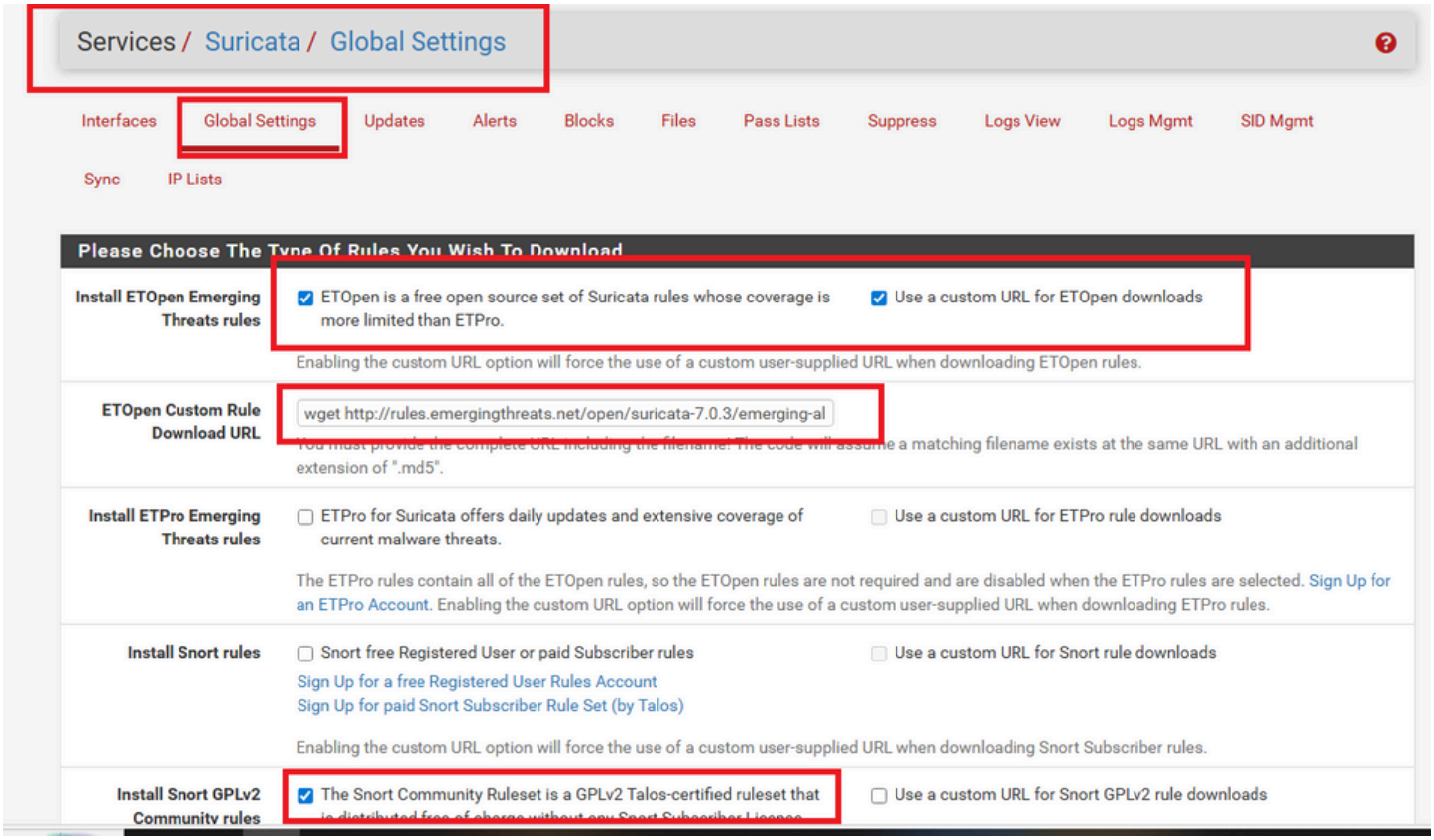
from pfsense web GUI >> System >> Package Manger

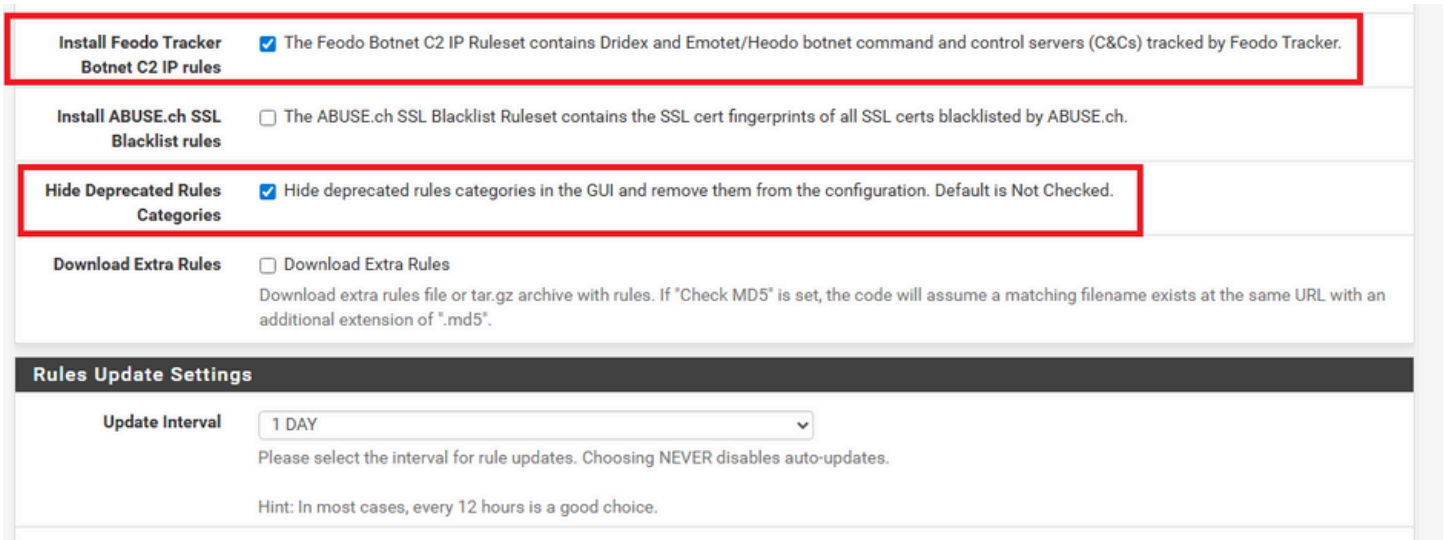


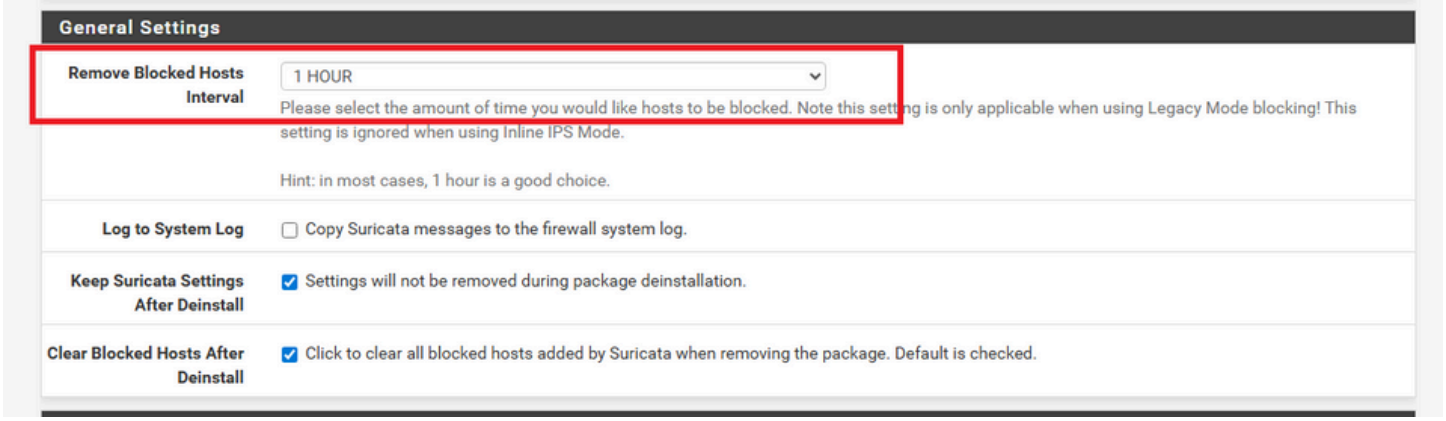
after installation complete go to suricat from >>Services >> Suricata >> Global Settings

to do some configuration

Link in First image >> **wget http://rules.emergingthreats.net/open/suricata-7.0.3/emerging-all.rules.tar.gz**

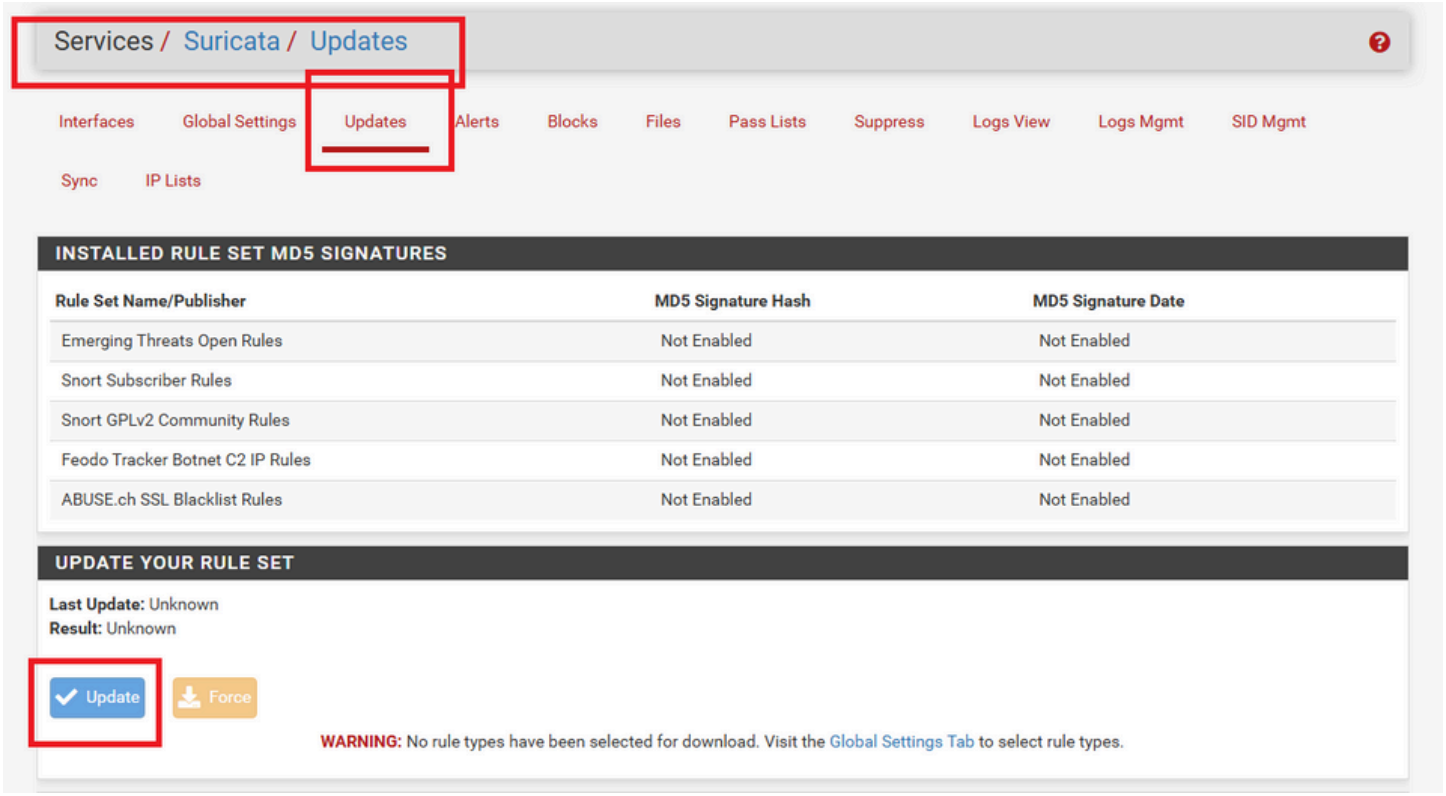






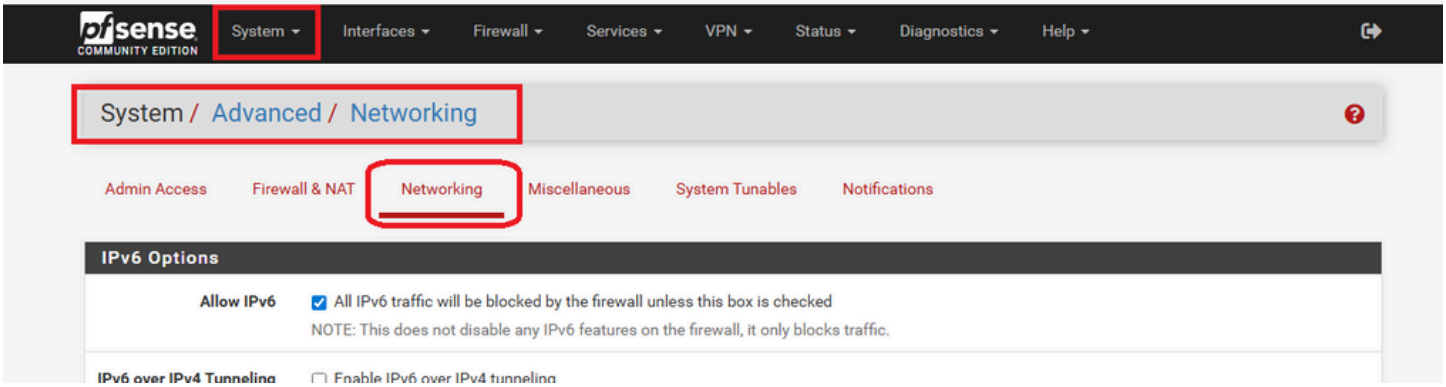
Click save and go to >> services >> Suricata >> update

to apply rule and configuration

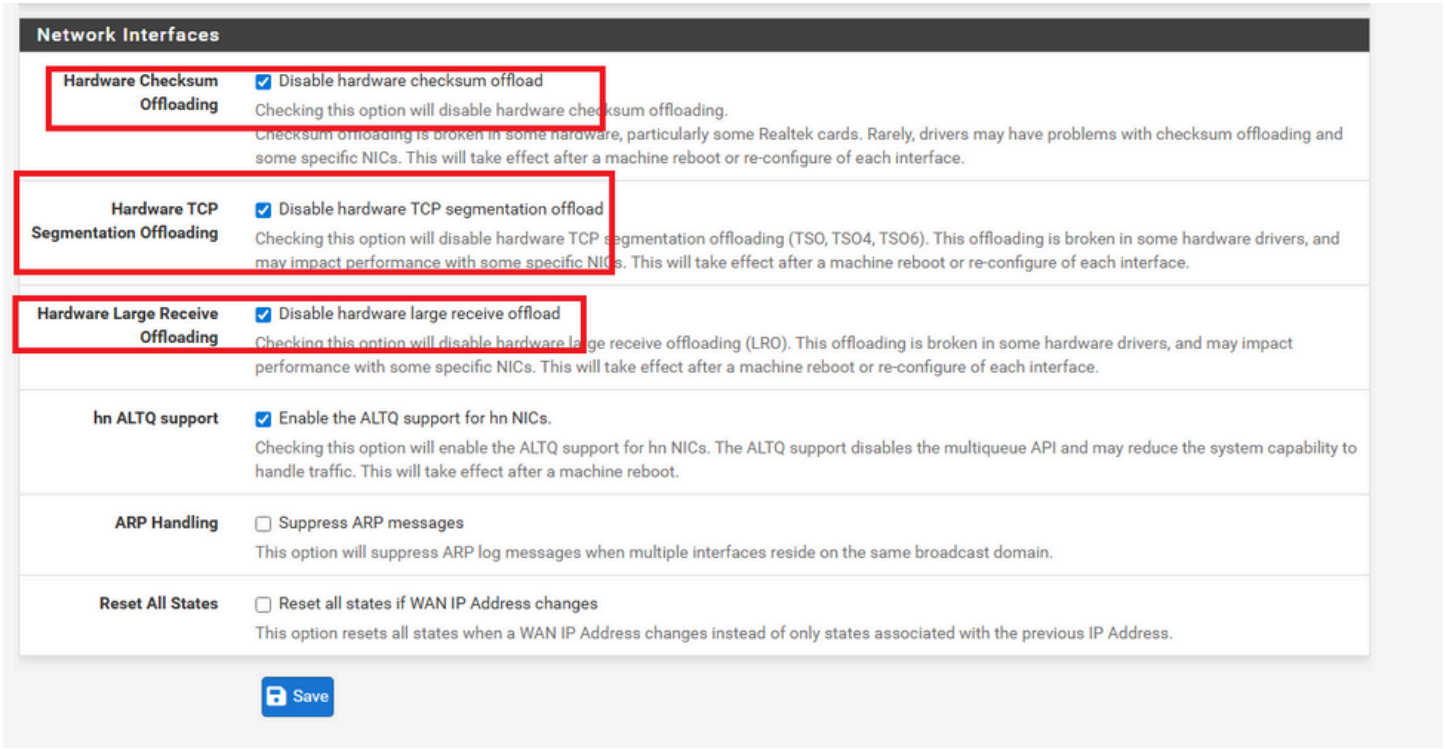


Now go to >> System >> Advanced >> Networking

to enable suricate got on Raw Traffic without any edit from firewall

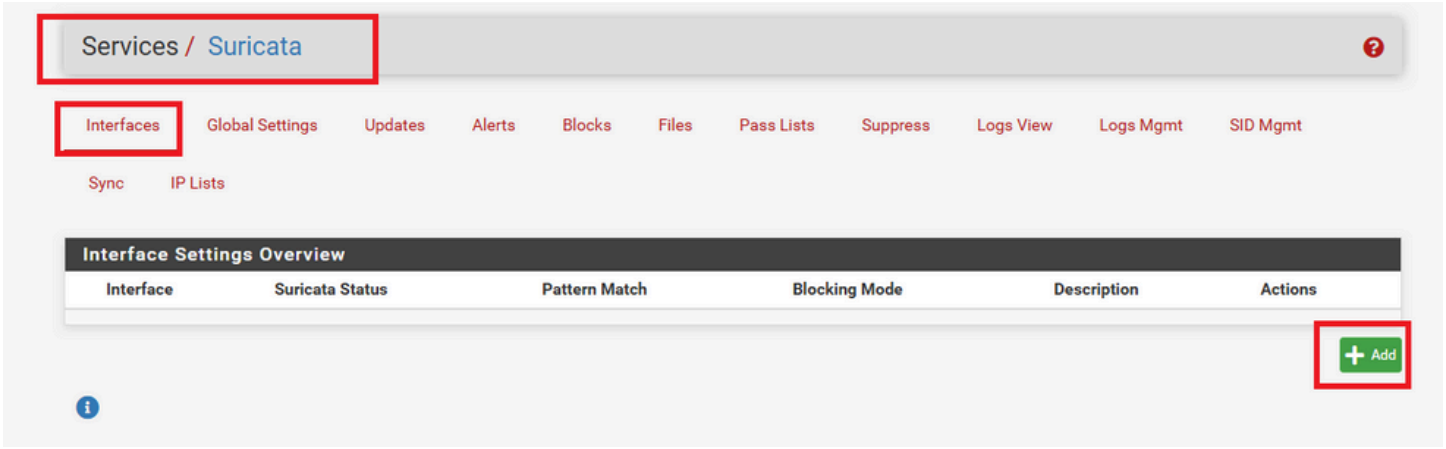


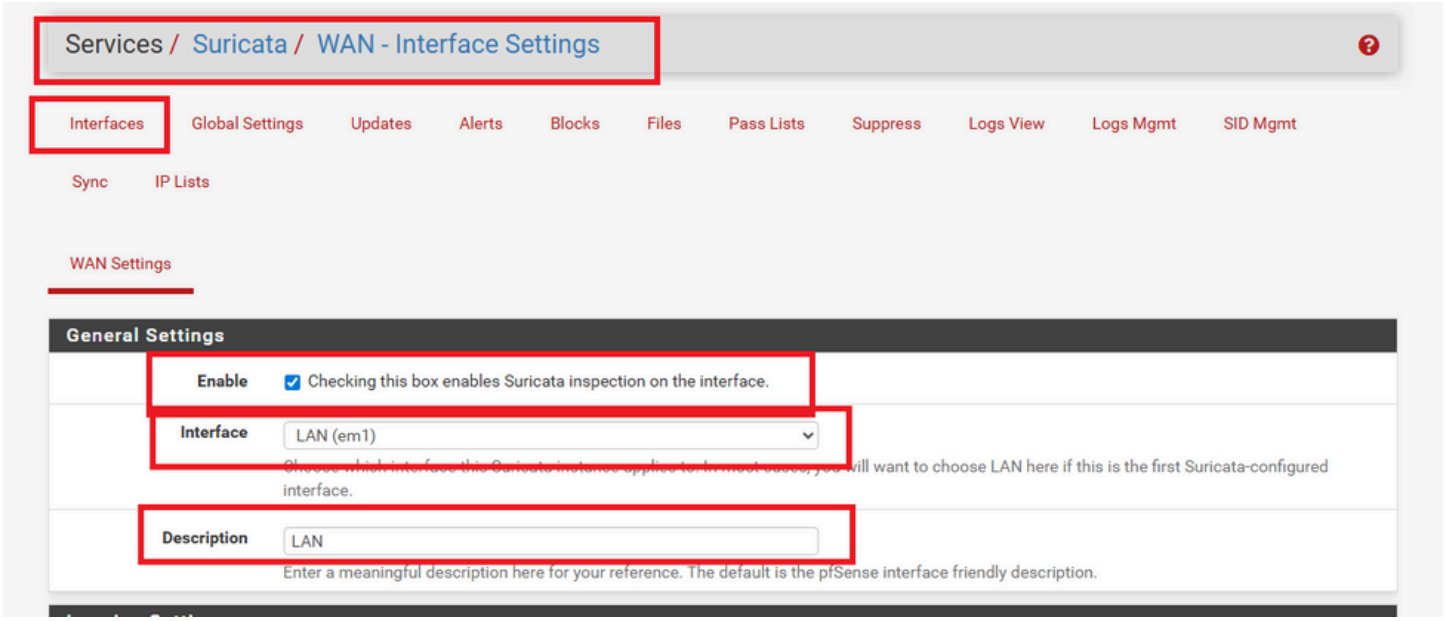
scroll down to



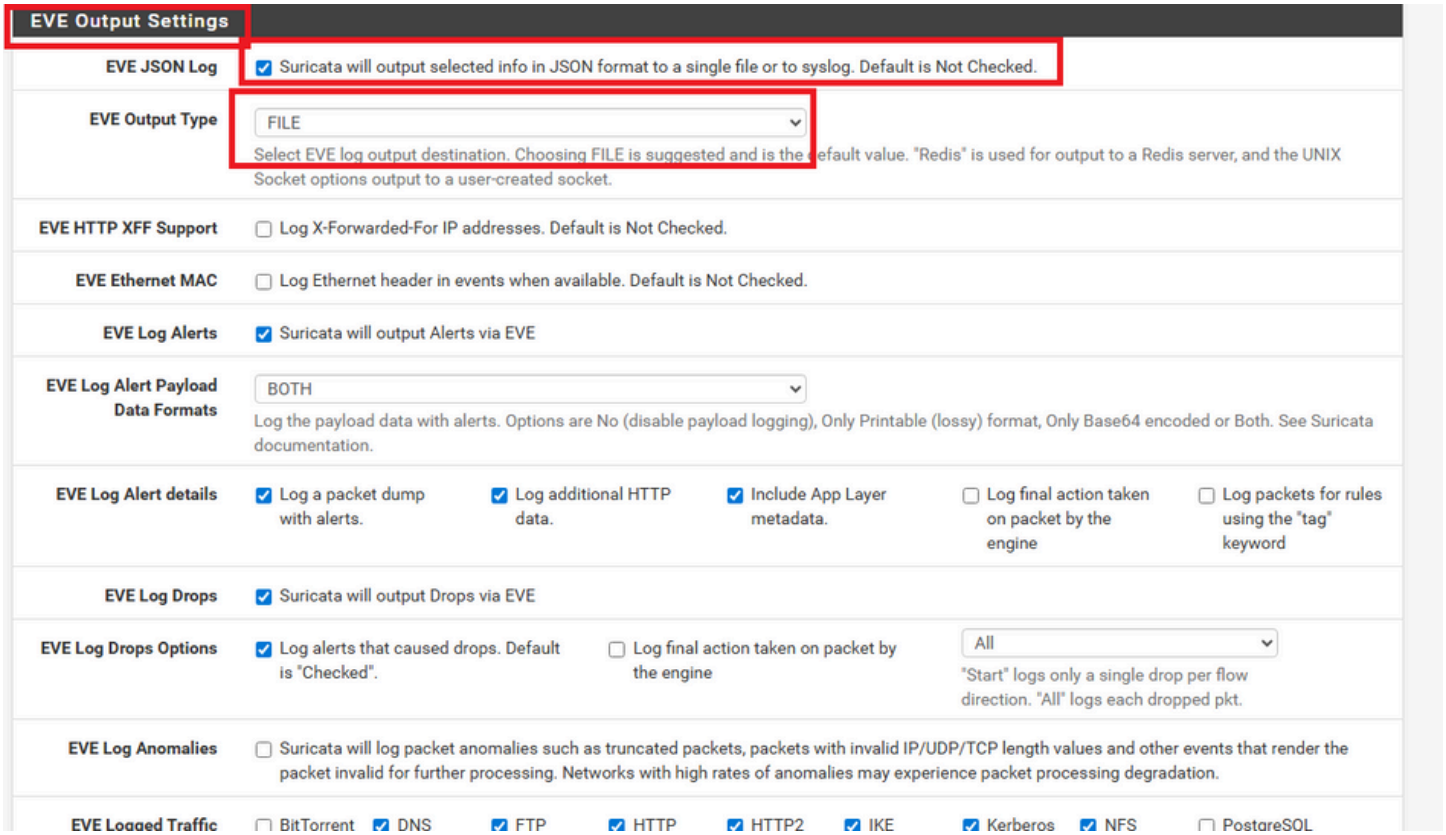
Click save and go to >> Services >> Suricata >> Interfaces

to allow this configuration in specific interface

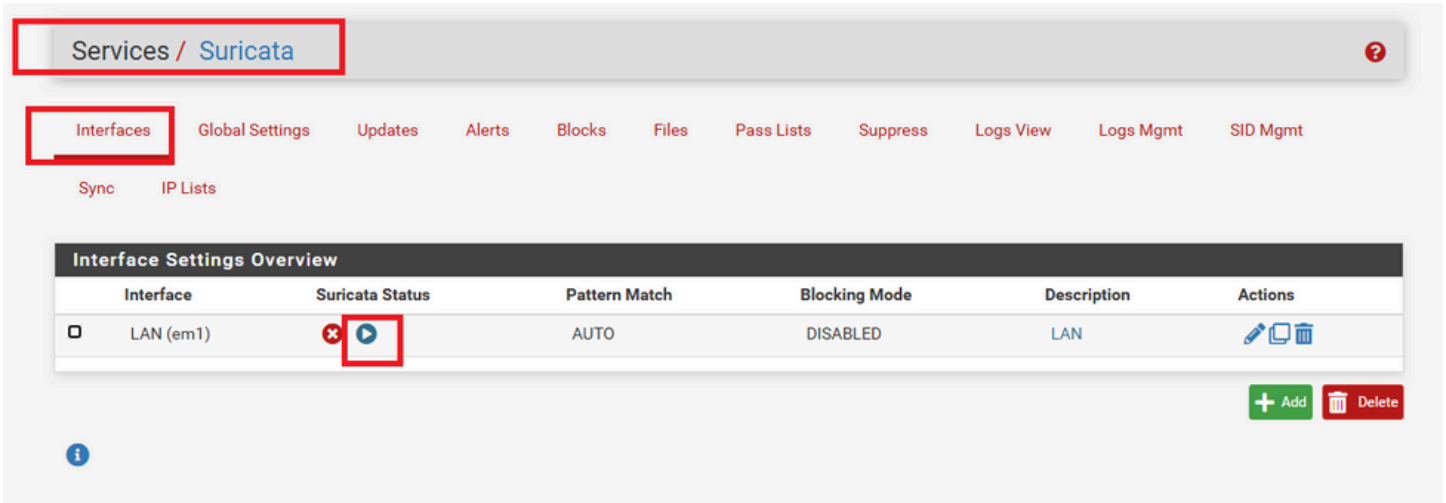




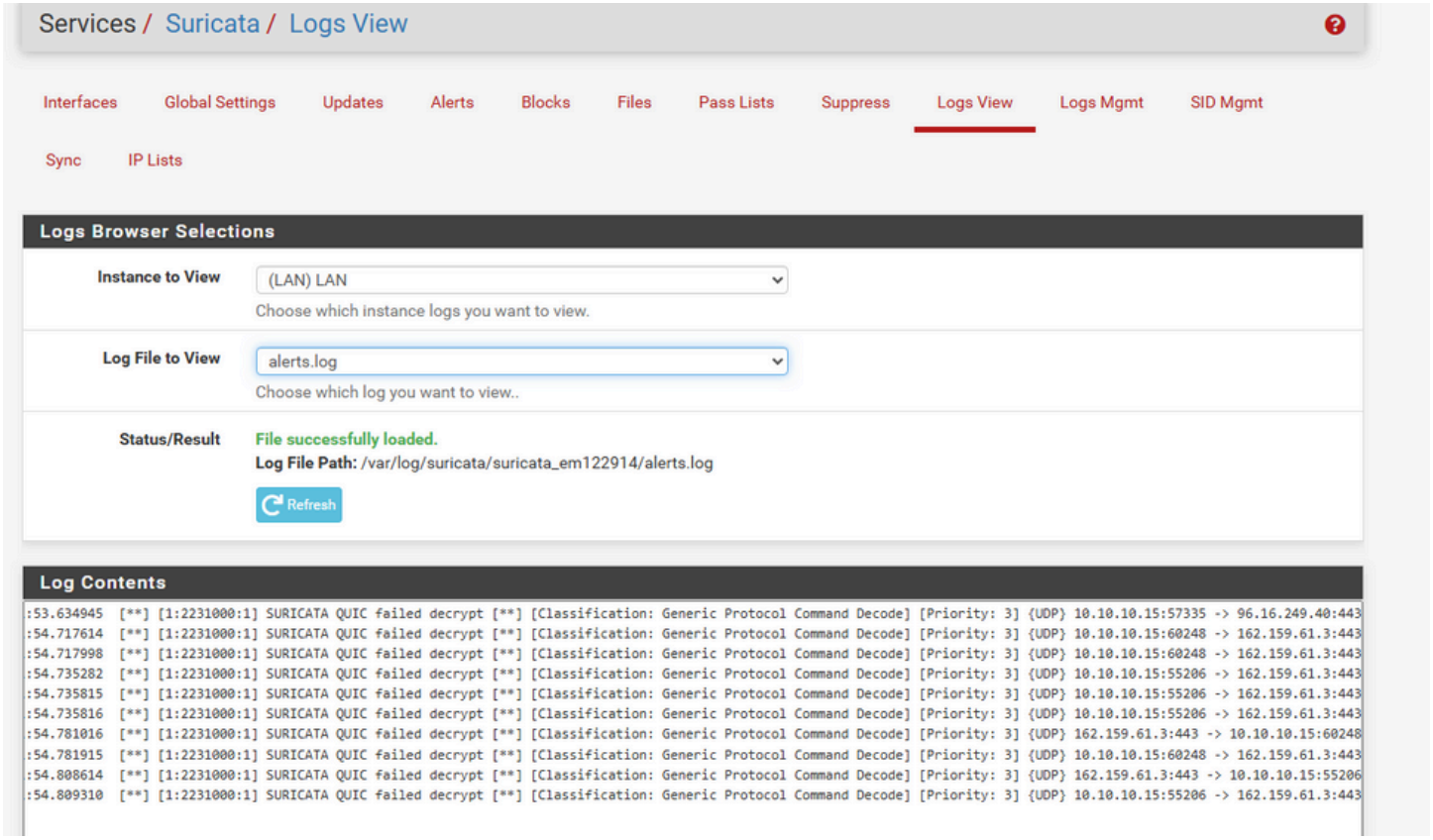
scroll down to



Click save and go to check logs gerated successfluy

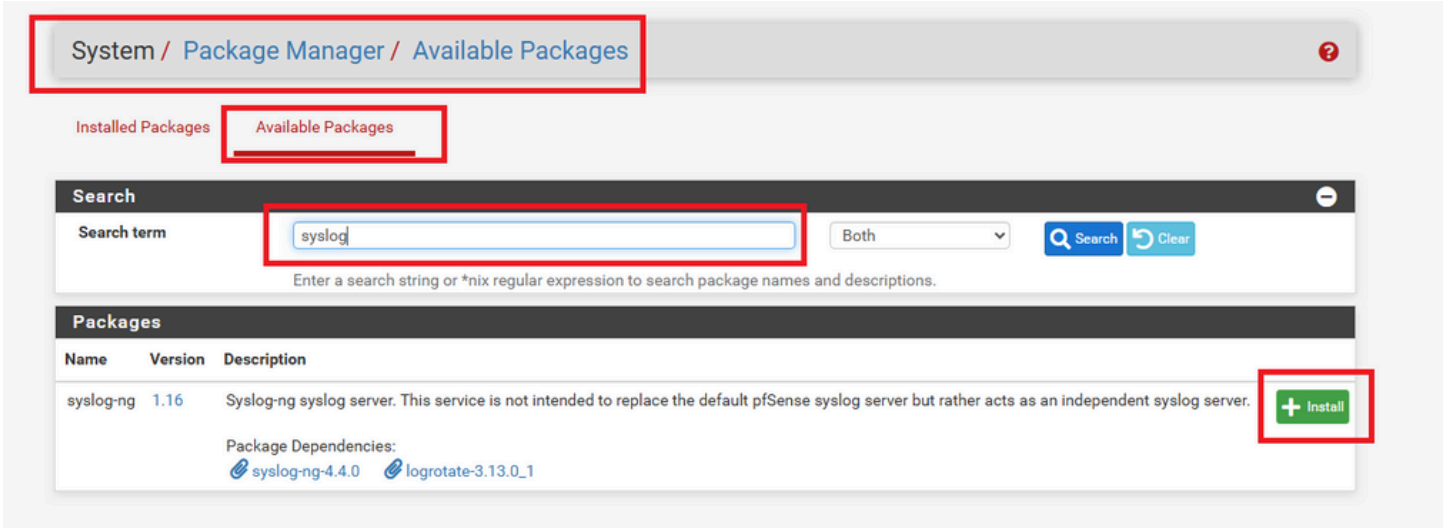


go to this url to make suricata genrate alert >> http://testmyids.com

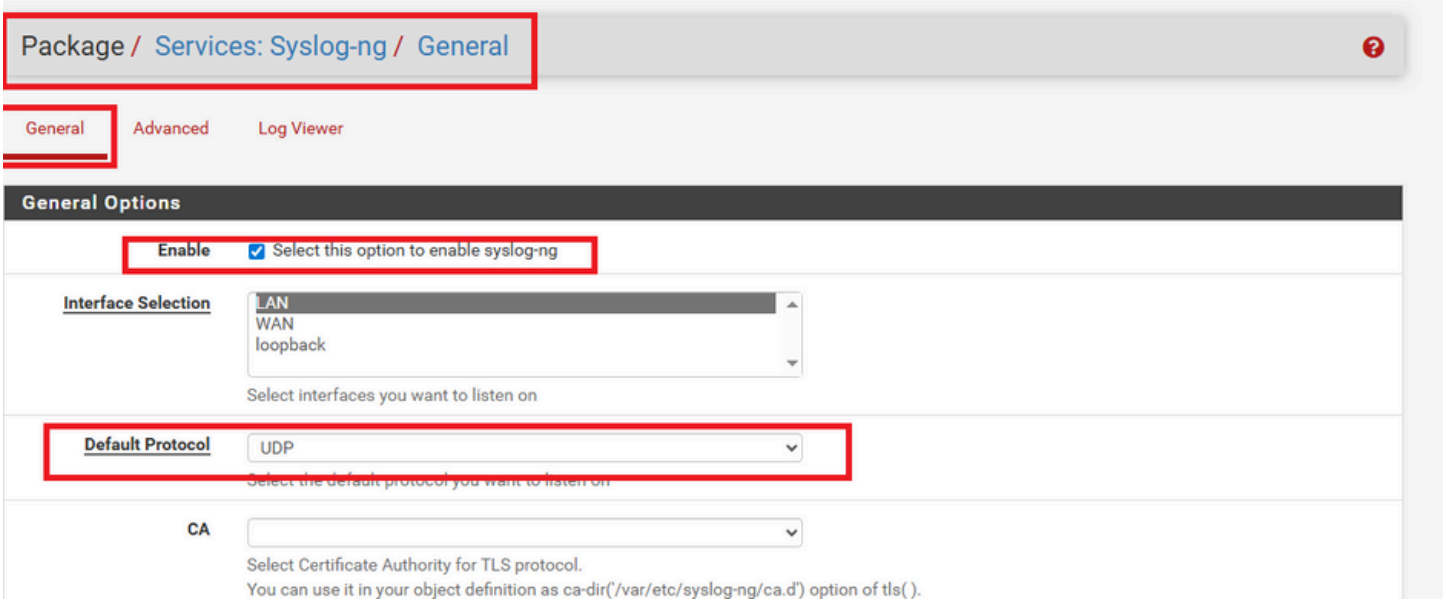


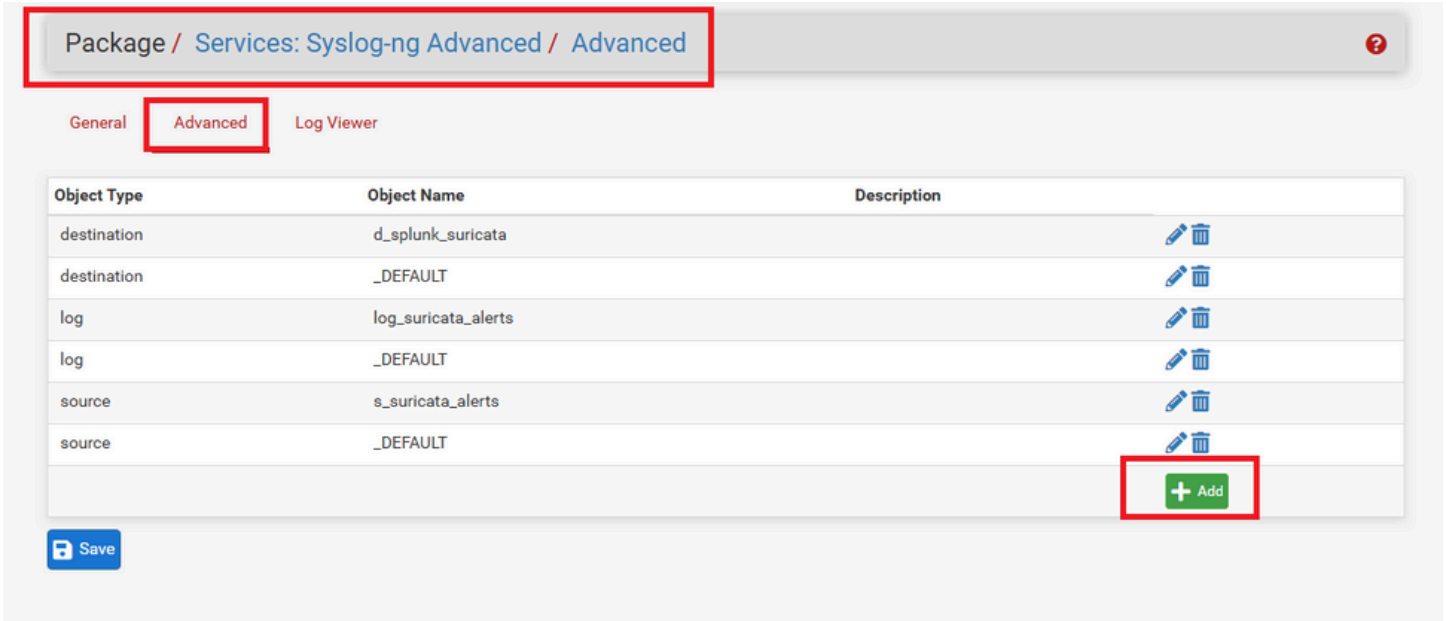
now lets go to send logs to splunk

install Syslog-ng From package manger to send logs



go to >> services >> syslog-ng





now we will create three object to send logs to splunk

1- monitor file

object name: s_suricata_alerts

object type: Source

object Parameters:

{

wildcard-file(

base-dir("/var/log/suricata/suricata_em153486")

filename-pattern("*")

recursive(yes)

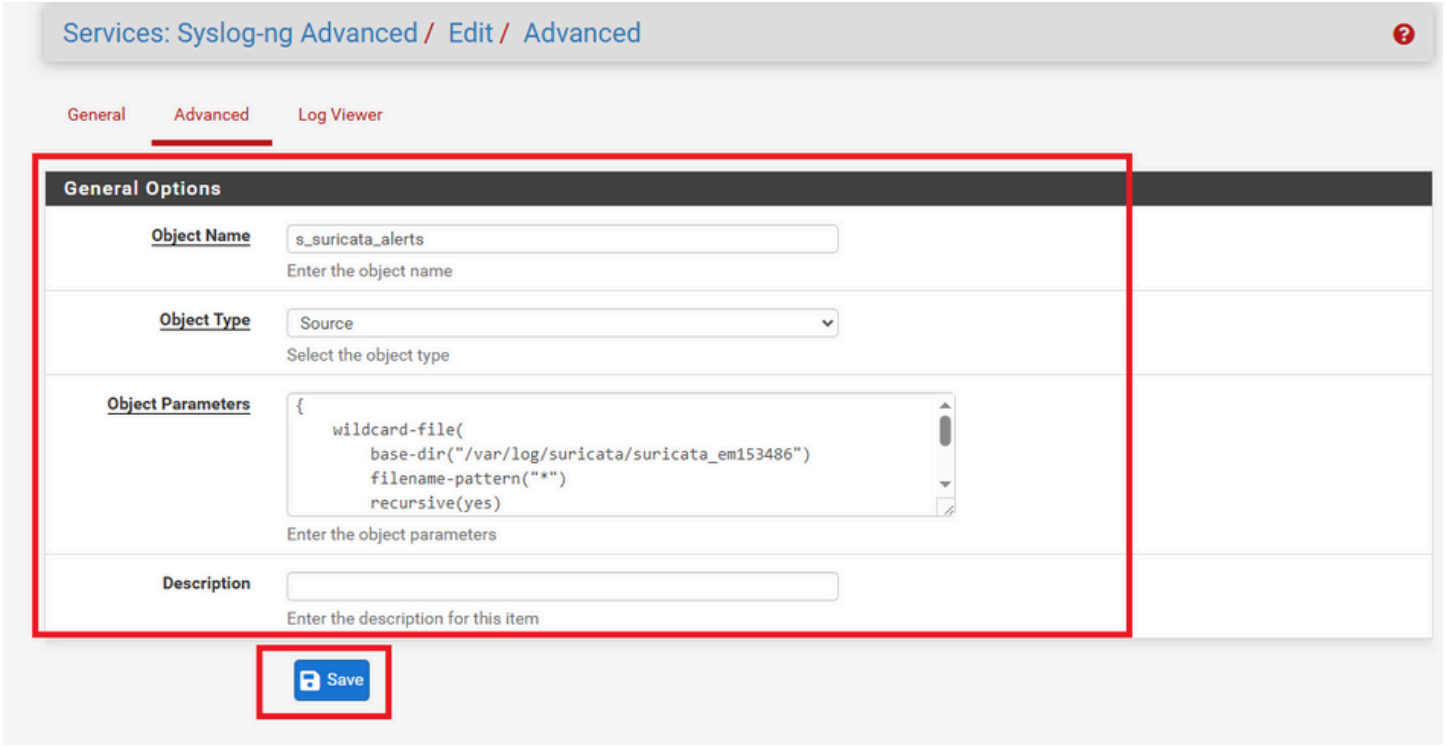
follow-freq(1)

flags(no-parse)

program-override("suricata")

);

};



and click save

2- create socket

object name: d_splunk_suricata

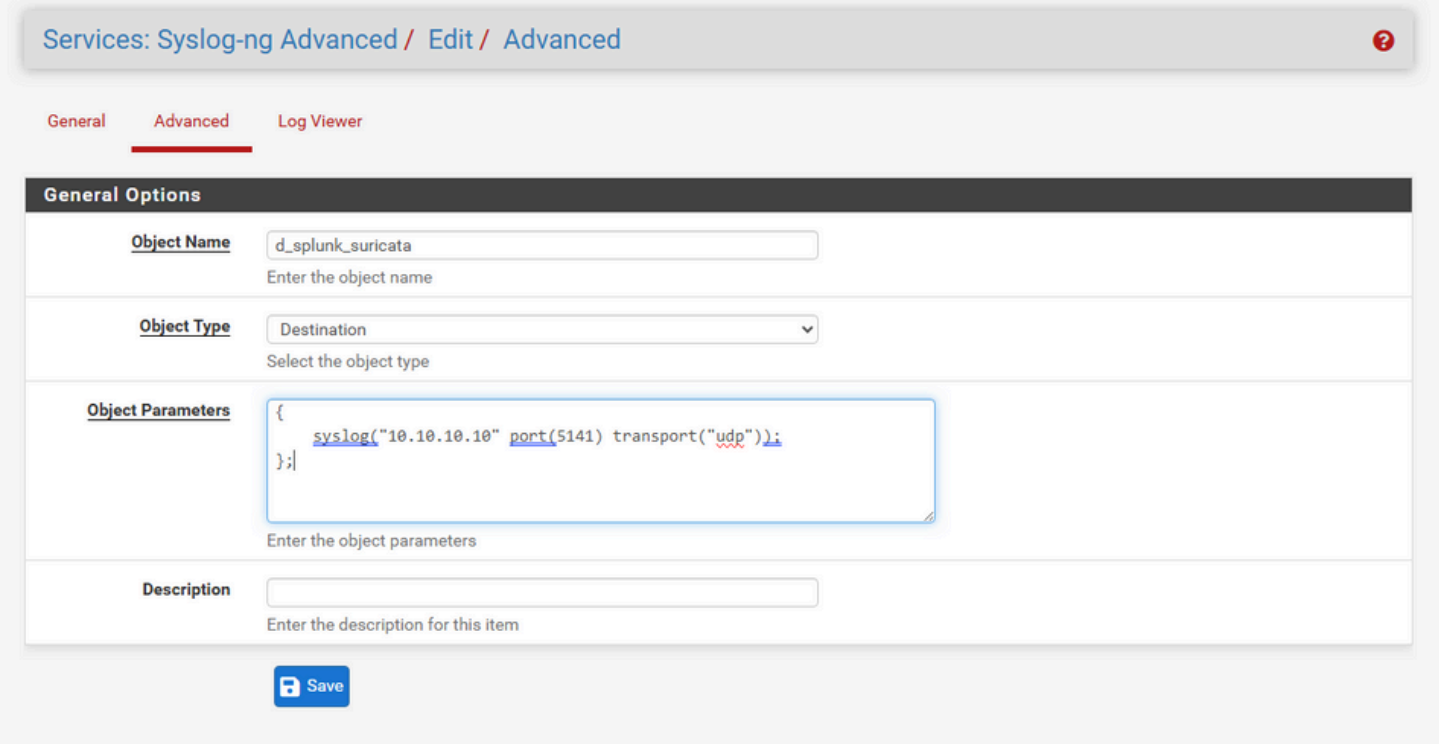
object type: destination

object Parameters:

{

syslog("splunk-ip" port(5141) transport("udp"));

};



and click save

3- forward logs

object name: log_suricata_alerts

object type: Logs

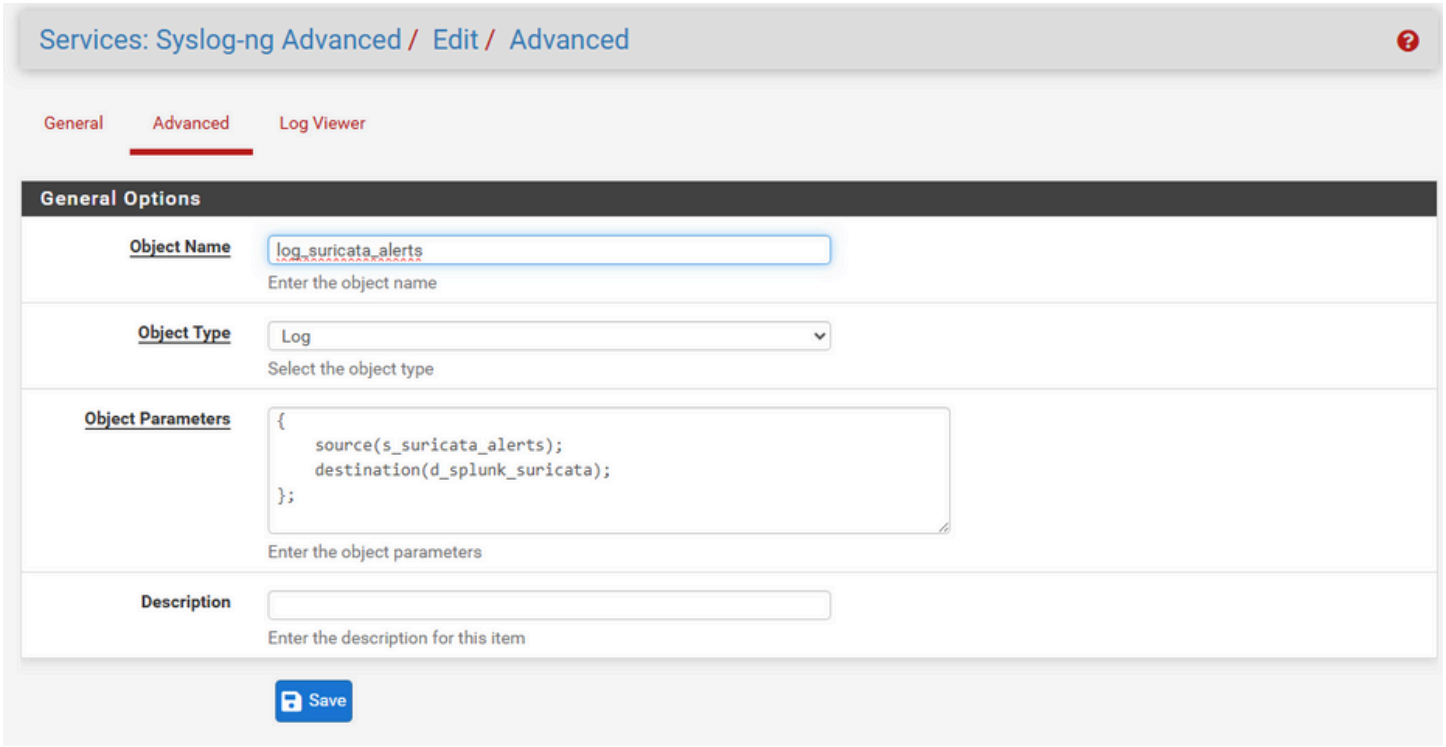
object Parameters:

{

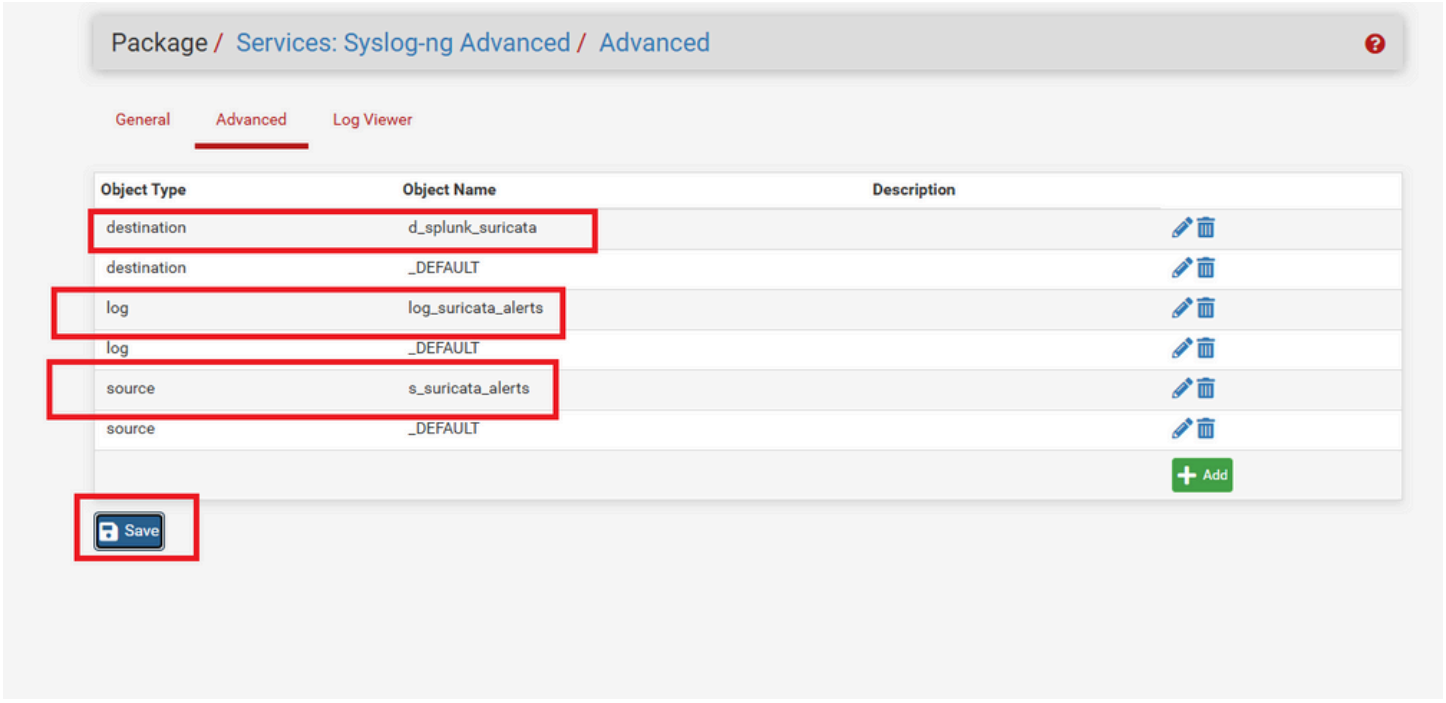
source(s_suricata_alerts);

destination(d_splunk_suricata);

};



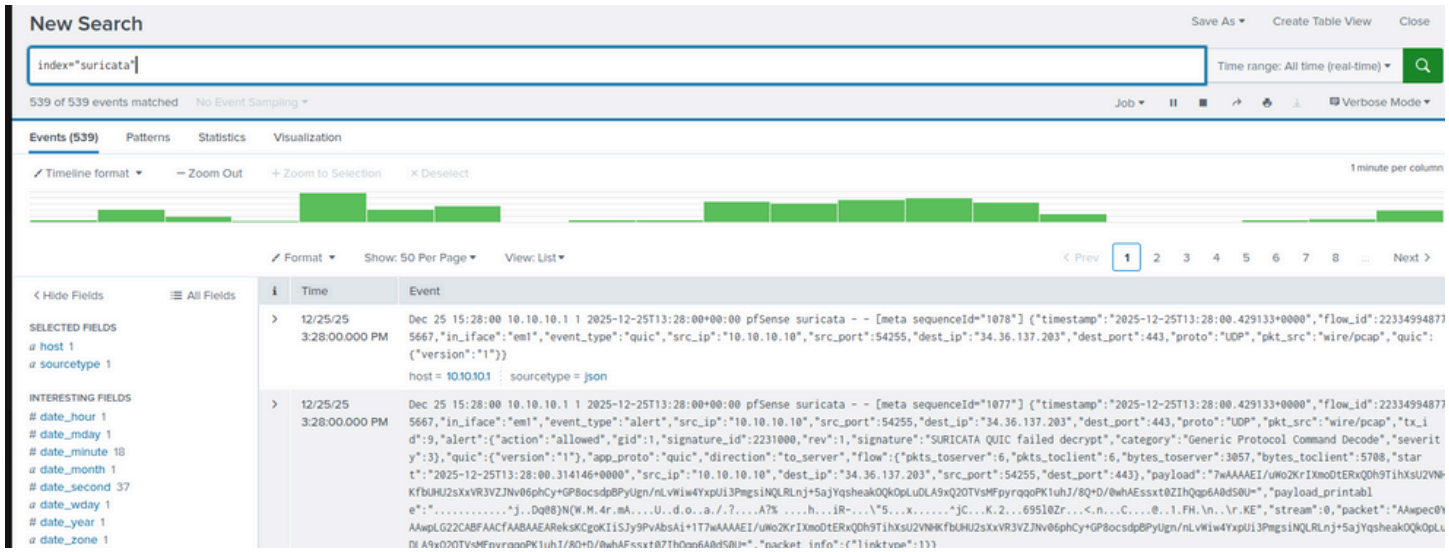
and click save



configure splunk forward and make sure port is 5141 source type json and create new index suricata

go to this url to make suricata genrate alert >> http://testmyids.com

check logs send successfuly to splunk


New Search
Save As
Create Table View
Close
index="suricata"
Time range: All time (real-time)
539 of 539 events matched
No Event Sampling
Job
Verbose Mode
Events (539)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 minute per column
Format
Show: 50 Per Page
View: List
Prev
1
2
3
4
5
6
7
8
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a sourcetype 1
INTERESTING FIELDS
date_hour 1
date_mday 1
date_minute 18
a date_month 1
date_second 37
a date_wday 1
date_year 1
a date_zone 1
Time
Event
12/25/25
3:28:00.000 PM
Dec 25 15:28:00 10.10.10.1 1 2025-12-25T13:28:00+00:00 pfSense suricata - - [meta sequenceId="1078"] {"timestamp":"2025-12-25T13:28:00.429133+0000","flow_id":22334994877
5667,"in_iface":"em1","event_type":"quic","src_ip":"10.10.10.10","src_port":54255,"dest_ip":"34.36.137.203","dest_port":443,"proto":"UDP","pkt_src":"wire/pcap","quic":
{"version":"1"}}
host = 10.10.10.1
sourcetype = json
12/25/25
3:28:00.000 PM
Dec 25 15:28:00 10.10.10.1 1 2025-12-25T13:28:00+00:00 pfSense suricata - - [meta sequenceId="1077"] {"timestamp":"2025-12-25T13:28:00.429133+0000","flow_id":22334994877
5667,"in_iface":"em1","event_type":"alert","src_ip":"10.10.10.10","src_port":54255,"dest_ip":"34.36.137.203","dest_port":443,"proto":"UDP","pkt_src":"wire/pcap","tx_i
d":9,"alert":{"action":"allowed","gid":1,"signature_id":2231000,"rev":1,"signature":"SURICATA QUIC failed decrypt","category":"Generic Protocol Command Decode","severit
y":3},"quic":{"version":"1"},"app_proto":"quic","direction":"to_server","flow":{"pkts_toserver":6,"pkts_toclient":6,"bytes_toserver":3057,"bytes_toclient":5708,"star
t":"2025-12-25T13:28:00.314146+0000","src_ip":"10.10.10.10","dest_ip":"34.36.137.203","src_port":54255,"dest_port":443},"payload":"7wAAAAEI/uWo2KrIXmoOtERxQDh9TihXsU2VNH
KfbUHU2sXxVR3VZJNv06phCy+GP8ocsdpBPyUgn/nLvWiw4YxpUi3PmgsiNQLRLnj+5ajYqsheakOQkOpLuDLA9xQ2OTVsMFpyrqqoPK1uhJ/8Q+D/0whAEssxt0ZIhQqp6A0dS0U=","payload_printabl
e":".............^j..Dq08}N(W.M.4r.mA....U..d.o..a./.?....A?% ....h...iR-...\"5...x......^jC...K.2...69510Zr...<.n...C....@..1.FH.\n..\r.KE","stream":0,"packet":"AAwpec0
AAwpLG22CABFAACfAABAAEAReksKCgoKIiSJy9PvAbsAi+1T7wAAAAEI/uWo2KrIXmoOtERxQDh9TihXsU2VNHKfbUHU2sXxVR3VZJNv06phCy+GP8ocsdpBPyUgn/nLvWiw4YxpUi3PmgsiNQLRLnj+5ajYqsheakOQkOpLu
DLA9xQ2OTVsMFpyrqoPK1uhJ/8Q+D/0whAEssxt0ZIhQqp6A0dS0U=","packet_info":{"linktype":113}