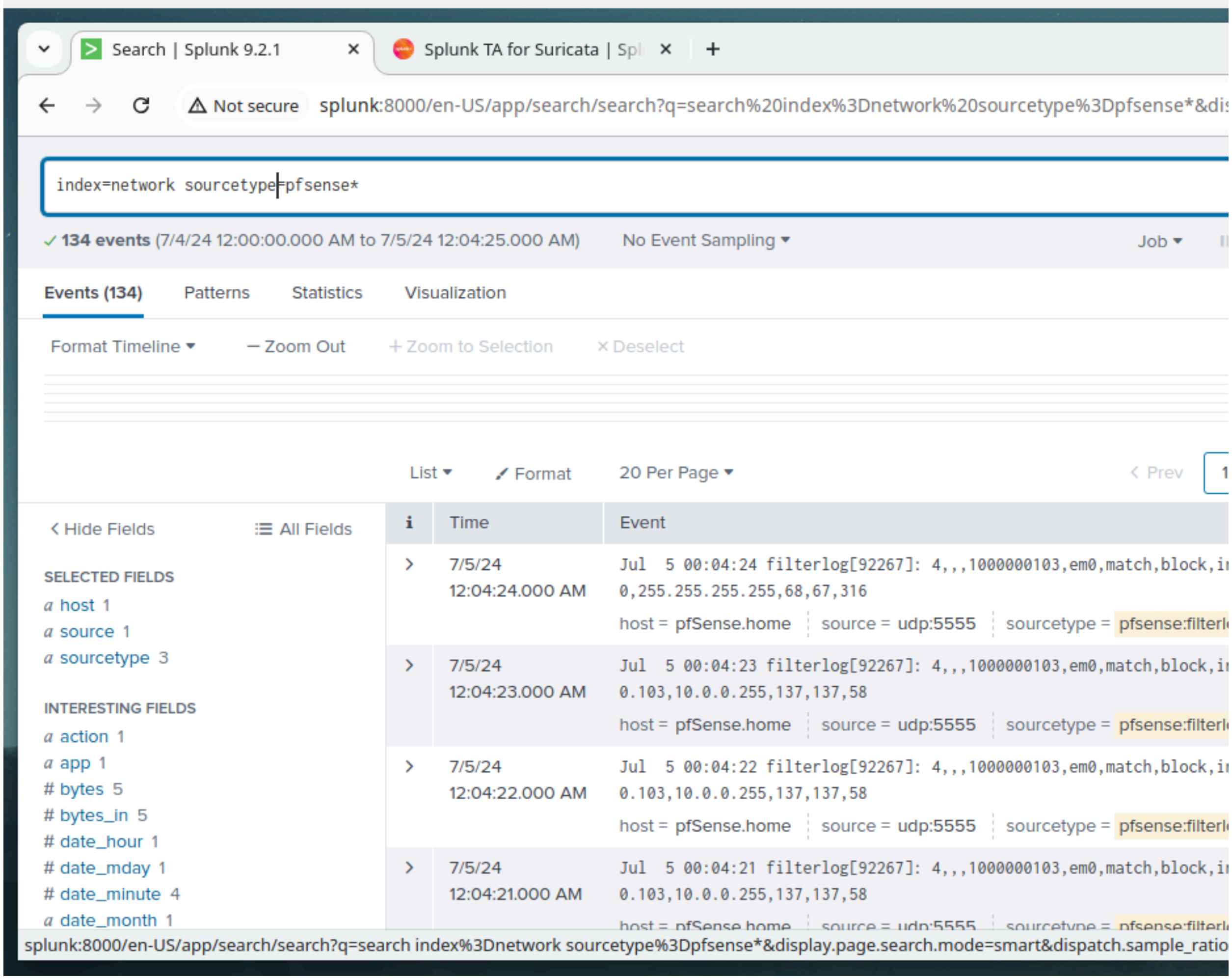
2. Network hardening, taking pfsense logs and suricata logs to send to splunk server for analysis and management.

Input the data (pfsense logs to splunk) via splunk settings of UDP port of 5555 then we set this for remote logging on pfsense system logs

Installing apps to help manage suricata and pfsense logs

https://splunkbase.splunk.com/app/1621
https://splunkbase.splunk.com/app/1527
https://splunkbase.splunk.com/app/2760

Use Splunk's searching feature



splunk:8000/en-US/app/search/search?q=search%20index%3Dnetwork%20sourcetype%3Dpfsense*&dis

```
index=network sourcetype=pfsense*
```

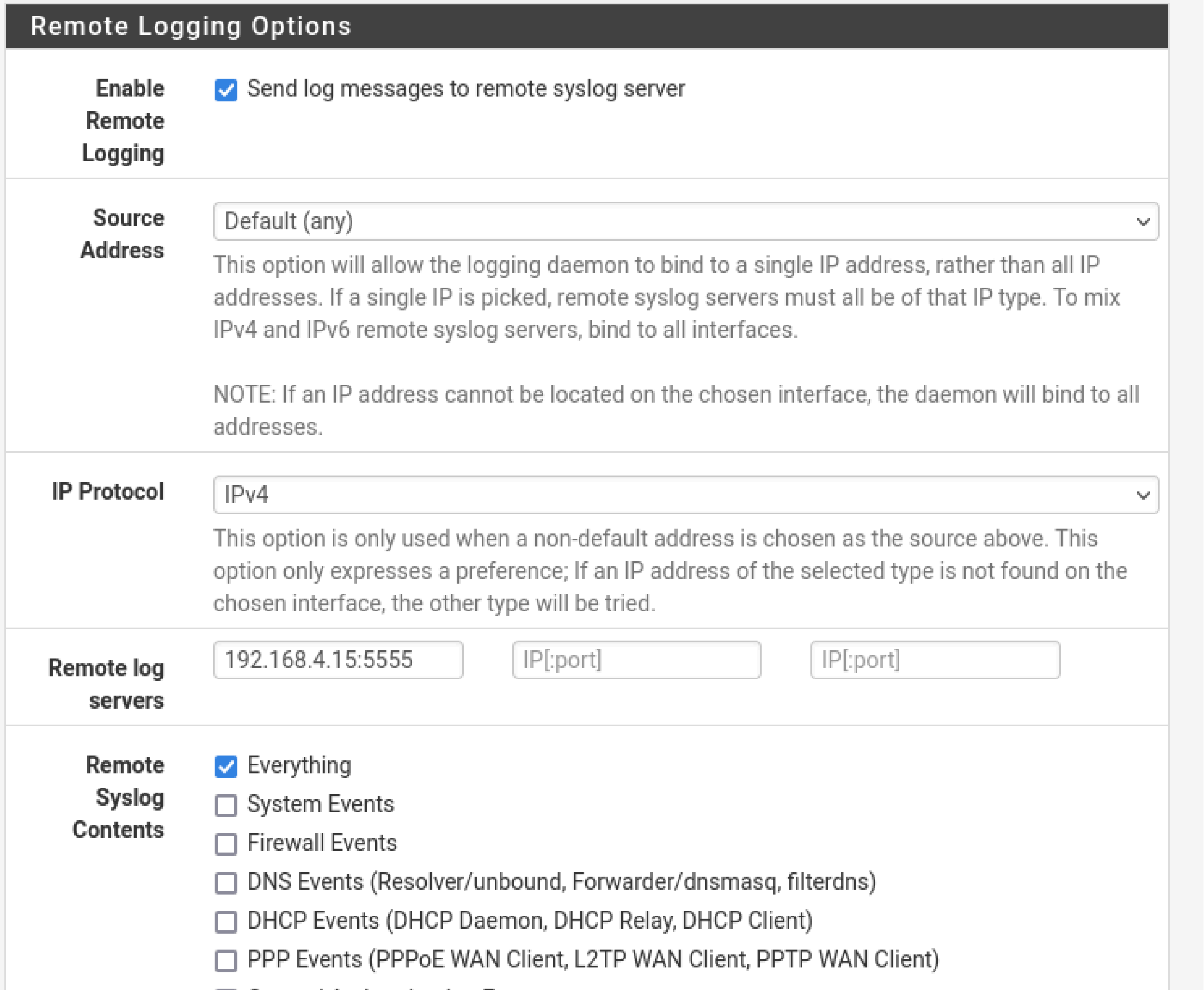
✓ 134 events (7/4/24 12:00:00.000 AM to 7/5/24 12:04:25.000 AM)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 3

INTERESTING FIELDS
a action 1
a app 1
# bytes 5
# bytes_in 5
# date_hour 1
# date_mday 1
# date_minute 4
a date_month 1

Time	Event
7/5/24 12:04:24.000 AM	Jul 5 00:04:24 filterlog[92267]: 4,,,1000000103,em0,match,block,i 0,255.255.255.255,68,67,316 host = pfSense.home source = udp:5555 sourcetype = pfsense:filterl
7/5/24 12:04:23.000 AM	Jul 5 00:04:23 filterlog[92267]: 4,,,1000000103,em0,match,block,i 0.103,10.0.0.255,137,137,58 host = pfSense.home source = udp:5555 sourcetype = pfsense:filterl
7/5/24 12:04:22.000 AM	Jul 5 00:04:22 filterlog[92267]: 4,,,1000000103,em0,match,block,i 0.103,10.0.0.255,137,137,58 host = pfSense.home source = udp:5555 sourcetype = pfsense:filterl
7/5/24 12:04:21.000 AM	Jul 5 00:04:21 filterlog[92267]: 4,,,1000000103,em0,match,block,i 0.103,10.0.0.255,137,137,58 host = pfSense.home source = udp:5555 sourcetype = pfsense:filterl

splunk:8000/en-US/app/search/search?q=search index%3Dnetwork sourcetype%3Dpfsense*&display.page.search.mode=smart&dispatch.sample_ratio



Remote Logging Options

Enable Remote Logging: ☑ Send log messages to remote syslog server

Source Address: Default (any)

This option will allow the logging daemon to bind to a single IP address, rather than all IP addresses. If a single IP is picked, remote syslog servers must all be of that IP type. To mix IPv4 and IPv6 remote syslog servers, bind to all interfaces.

NOTE: If an IP address cannot be located on the chosen interface, the daemon will bind to all addresses.

IP Protocol: IPv4

This option is only used when a non-default address is chosen as the source above. This option only expresses a preference; If an IP address of the selected type is not found on the chosen interface, the other type will be tried.

Remote log servers: 192.168.4.15:5555 | IP[:port] | IP[:port]

Remote Syslog Contents:
- ☑ Everything
- □ System Events
- □ Firewall Events
- □ DNS Events (Resolver/unbound, Forwarder/dnsmasq, filterdns)
- □ DHCP Events (DHCP Daemon, DHCP Relay, DHCP Client)
- □ PPP Events (PPPoE WAN Client, L2TP WAN Client, PPTP WAN Client)

pfsense system logs will go into the “network” index on splunk server

TODO: Set up pfsense’s suricata to have a splunk universal forwarder to send suricata logs to the splunk server.