How to Configure Multi-Hop Log Forwarding with rsyslog from Kali Linux to Splunk via Ubuntu

Submitted by: Faizanullah Syed
Use Case: Centralized Log Collection in SOC using rsyslog
Systems Used:

- **Kali Linux** (Log Source)
- **Ubuntu Server** (Intermediate Forwarder)
- **Enterprise Server** (Log Collector)

✅ Objective

To configure centralized log forwarding where logs are sent:

Kali Linux (Client) → Ubuntu Server (Forwarder) → Enterprise Server (Collector)

This method is essential in Security Operations Centers (SOCs) where intermediate forwarders are used to centralize logs before sending them to SIEMs or log analysis tools.

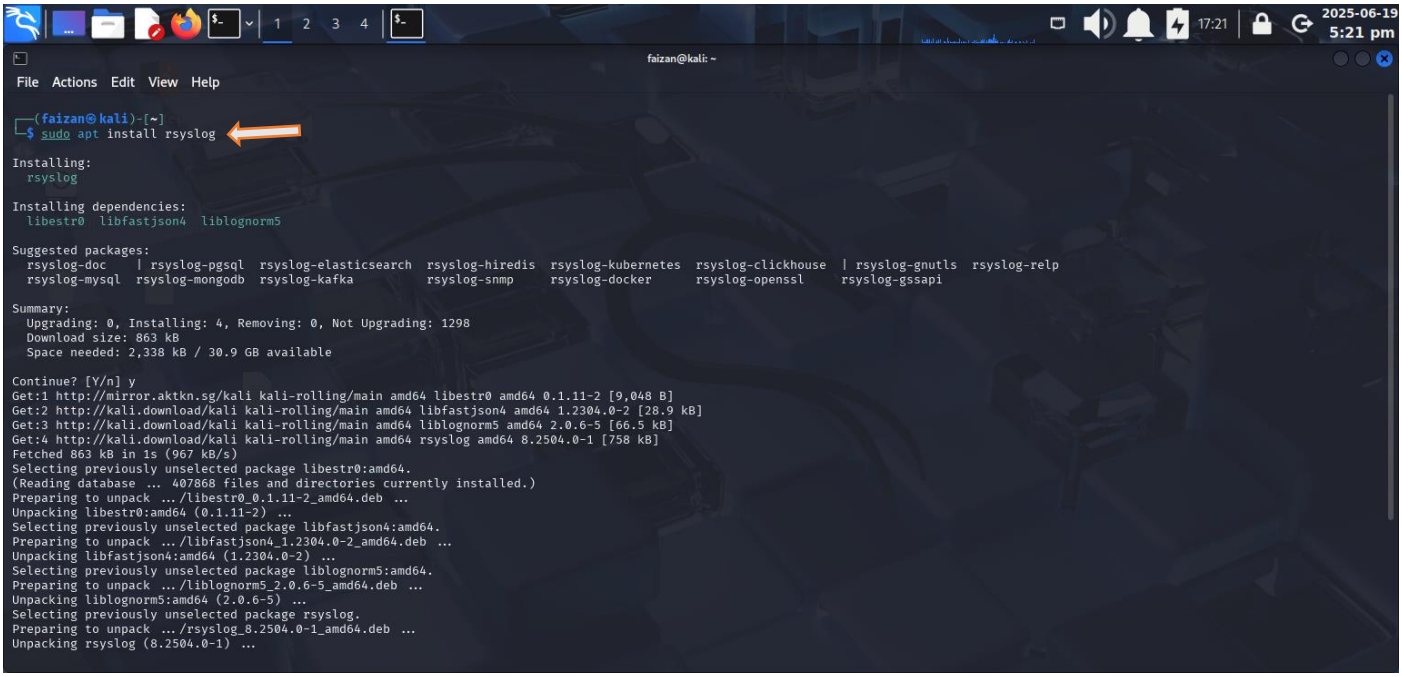
Implementation Steps:

🔹 Step 1: Install `rsyslog` on All Machines

Run the following on **Kali**, **Ubuntu**, and **Enterprise Server**:

sudo apt update

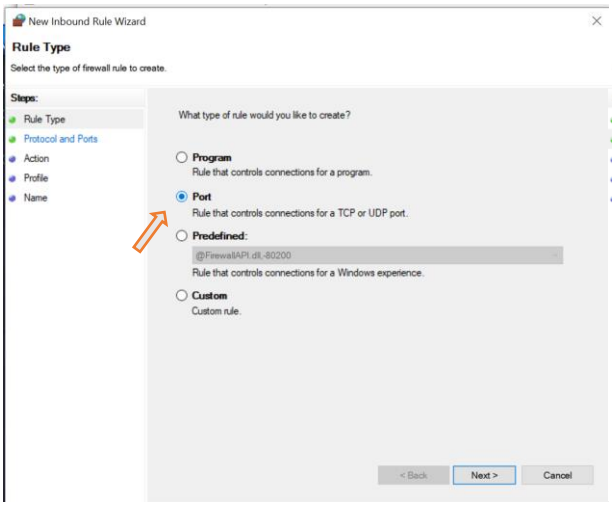
apt install rsyslog sudo

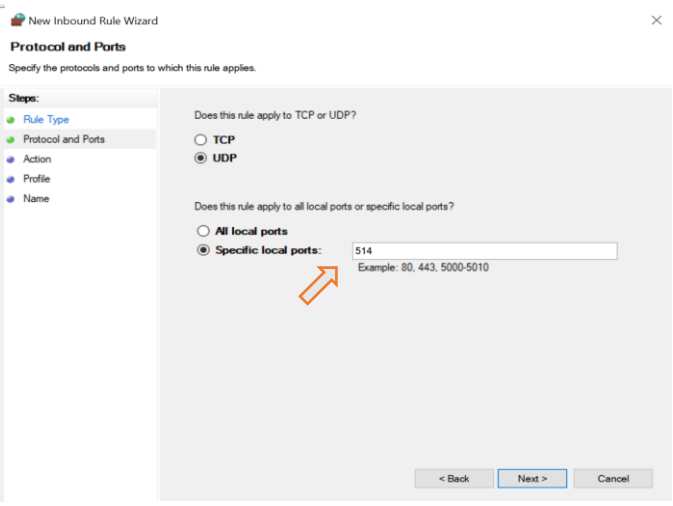


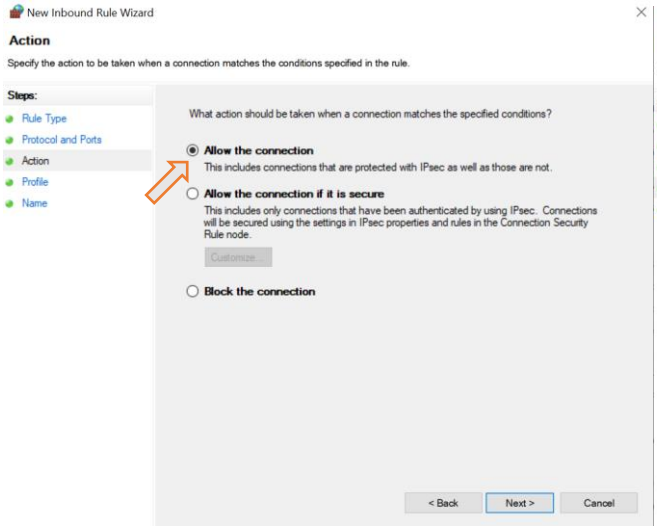
Step 2: Configure Enterprise Server to Receive Logs

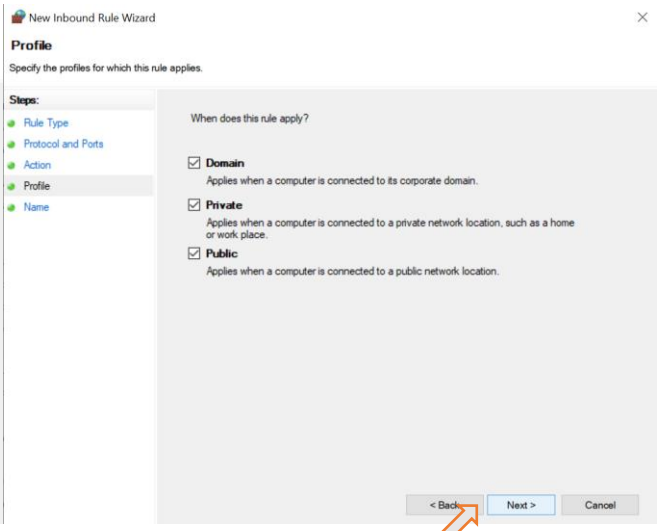
On the **Enterprise Server** :

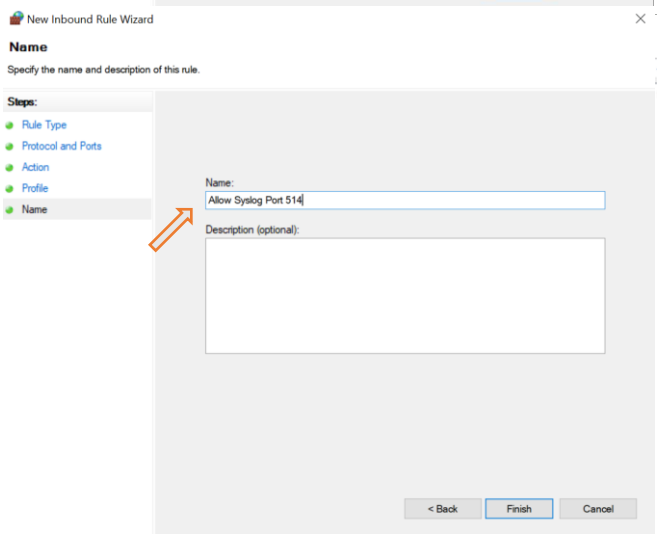
1) First need to create inbound rule in windows firewall & network protection where Splunk Enterprise server installed.

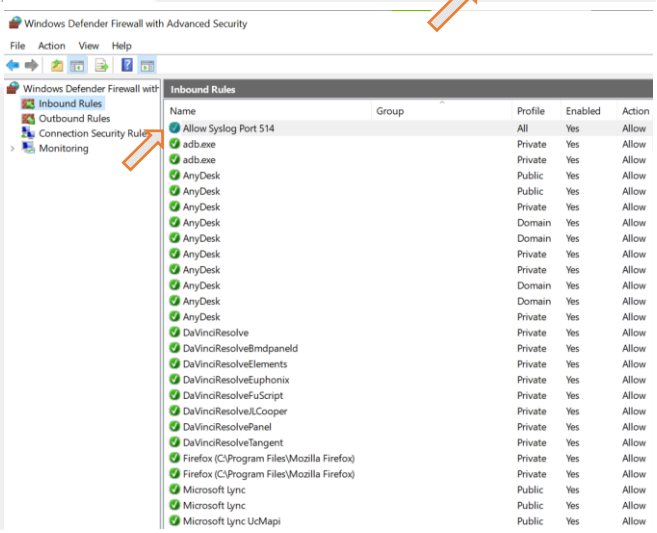






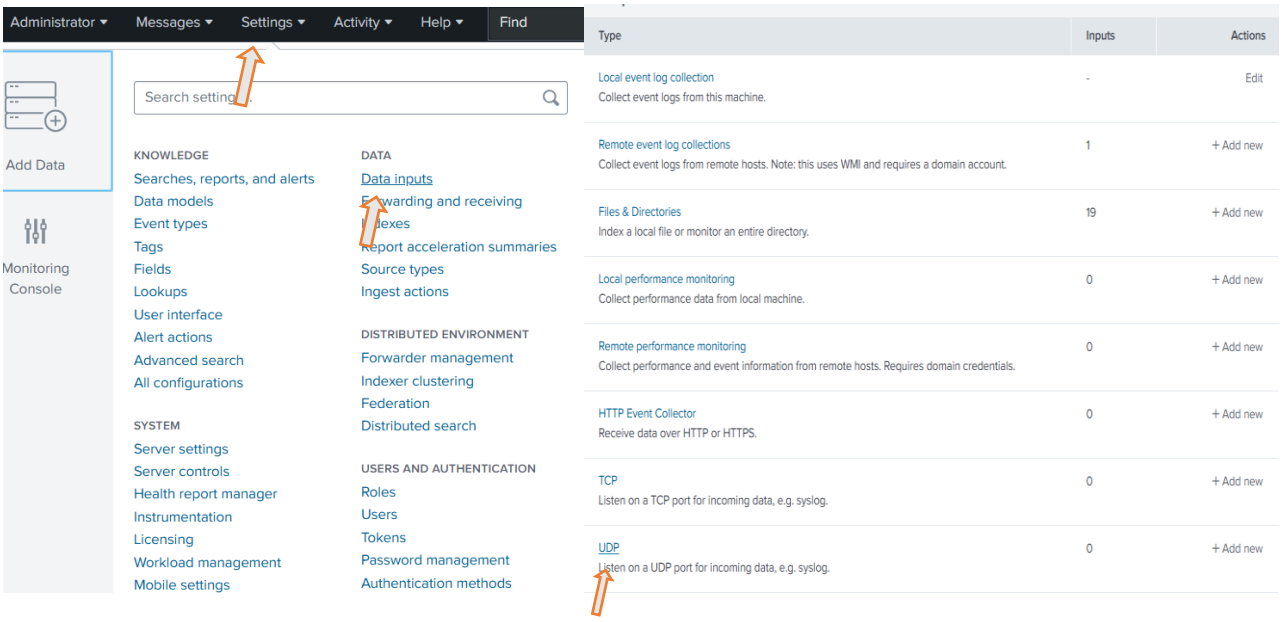


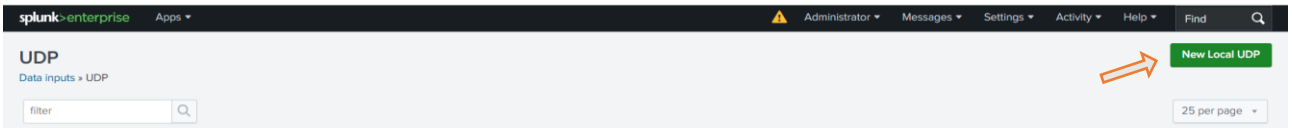


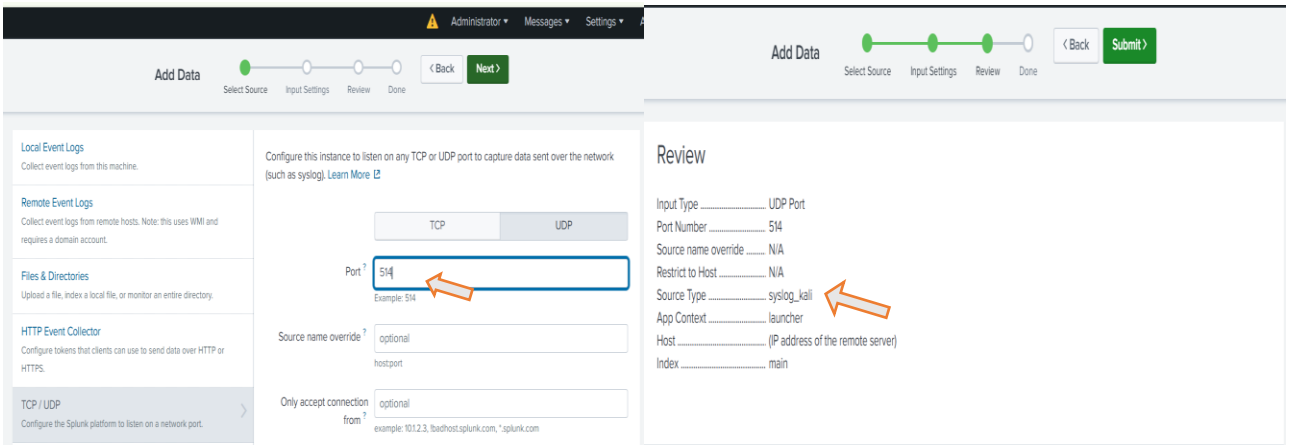


2) Configured splunk Enterprise server settings to listen a port UDP:514.

Settings → Data inputs → UDP → New local UDP







Step 3: Configure Kali Linux machine to forward log to Receive Logs

On the **kali linux machine** :

1. Open the config file:

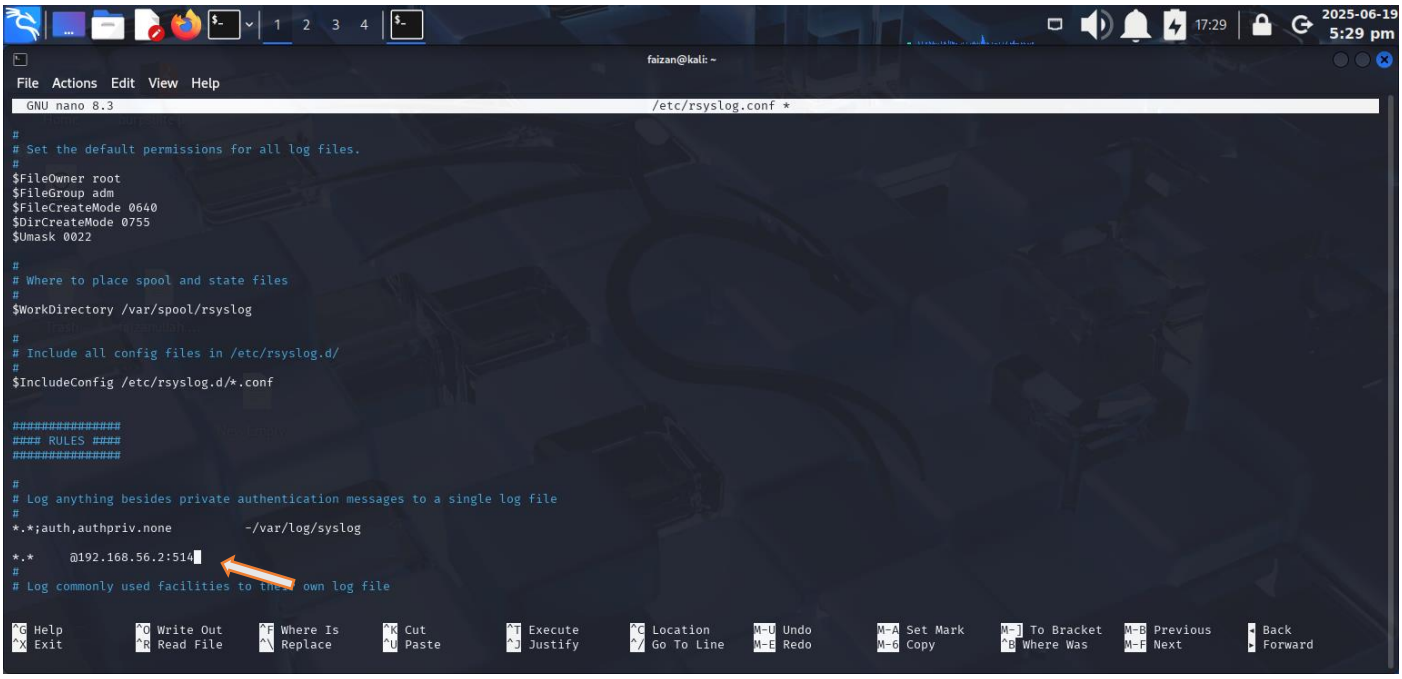
sudo nano /etc/rsyslog.conf

2. Add this line to forward logs to the Enterprise Server:

. @<ENTERPRISE_SERVER_IP>:514

3.Save and restart:

sudo systemctl restart rsyslog



4. Check rsyslog Status: # sudo Systemctl status rsyslog.

Step 4: Configure Ubuntu (Intermediate) to Forward Logs to Enterprise

On the **Ubuntu Server** (Intermediate):

```
splunk_uf@splunkufserver: ~
splunk_uf@splunkufserver:~$ sudo apt install rsyslog
[sudo] password for splunk_uf:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
rsyslog is already the newest version (8.2312.0-3ubuntu9.1).
rsyslog set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 1 not upgraded.
splunk_uf@splunkufserver:~$
```

1. Open the config file:
sudo nano /etc/rsyslog.conf

2. Add this line to forward logs to the Enterprise Server:
. @<ENTERPRISE_SERVER_IP>:514

3.Save and restart:
sudo systemctl restart rsyslog

```
splunk_uf@splunkufserver: ~
  GNU nano 7.2                    /etc/rsyslog.conf *
#
$FileOwner syslog
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022
$PrivDropToUser syslog
$PrivDropToGroup syslog

#
# Where to place spool and state files
#
$WorkDirectory /var/spool/rsyslog

#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.*     @192.168.100.5:514

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

4. Check rsyslog Status: # sudo Systemctl status rsyslog

```
splunk_uf@splunkufserver: ~
● rsyslog.service - System Logging Service
     Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; preset: >
     Active: active (running) since Thu 2025-06-19 17:04:50 UTC; 4h 39min left
TriggeredBy: ● syslog.socket
       Docs: man:rsyslogd(8)
             man:rsyslog.conf(5)
             https://www.rsyslog.com/doc/
    Process: 762 ExecStartPre=/usr/lib/rsyslog/reload-apparmor-profile (code=ex>
   Main PID: 828 (rsyslogd)
      Tasks: 4 (limit: 2246)
     Memory: 4.0M (peak: 5.1M)
        CPU: 568ms
     CGroup: /system.slice/rsyslog.service
             └─828 /usr/sbin/rsyslogd -n -iNONE

Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' r>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd/udp: socket 7: sendto() err>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd: socket 7: error 101 sendin>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' s>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' r>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd/udp: socket 7: sendto() err>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: omfwd: socket 7: error 101 sendin>
Jun 19 17:08:02 splunkufserver rsyslogd[828]: action 'action-8-builtin:omfwd' s>
lines 1-23
```

Step 5: Configure Kali Linux to Send Logs to Ubuntu

On the **Kali Linux** system:

- Add this line to forward logs to the Ubuntu Forwarder in ***/etc/rsyslog.conf*** file .

```
faizan@kali: ~
File  Actions  Edit  View  Help
GNU nano 8.3                    /etc/rsyslog.conf

###############
#### RULES ####
###############

#
# Log anything besides private authentication messages to a single log file
#
*.*;auth,authpriv.none          -/var/log/syslog

#*.*    @192.168.XX.X:514

*.*     @192.168.100.6:514
# Log commonly used facilities to their own log file

auth,authpriv.*                 /var/log/auth.log
cron.*                          -/var/log/cron.log
kern.*                          -/var/log/kern.log
mail.*                          -/var/log/mail.log
user.*                          -/var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg                         :omusrmsg:*

^G Help   ^O Write Out  ^F Where Is  ^K Cut   ^T Execute  ^C Location  M-U Undo   M-A Set Mark  M-] To Bracket  M-B Previous  ^← Back
^X Exit   ^R Read File  ^\ Replace   ^U Paste ^J Justify  ^/ Go To Line M-E Redo   M-6 Copy    ^B Where Was    M-F Next      ^→ Forward
```

Save and restart: # sudo systemctl restart rsyslog.

◈ Step 6: Configure Splunk Universal Forwarder to Monitor and Forward `/var/log/syslog`

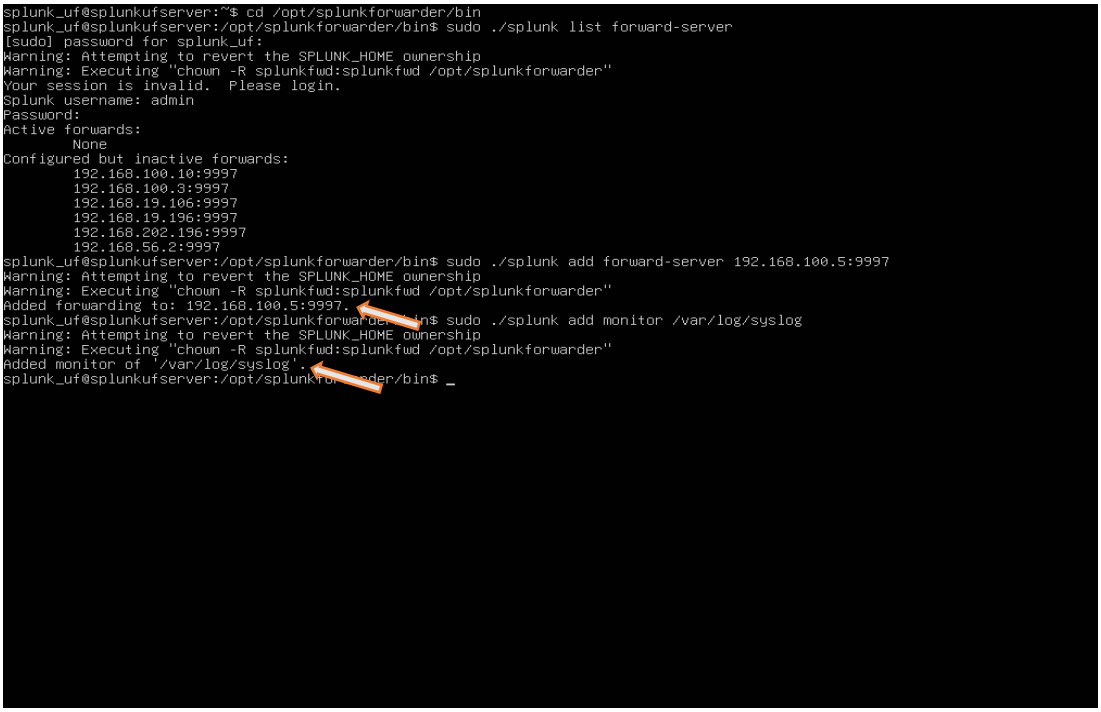
To forward logs from your Ubuntu system to a Splunk Enterprise server, follow these commands using the **Splunk Universal Forwarder (UF)**.

1. **Check Current Forward Servers:**
   # sudo ./splunk list forward-server

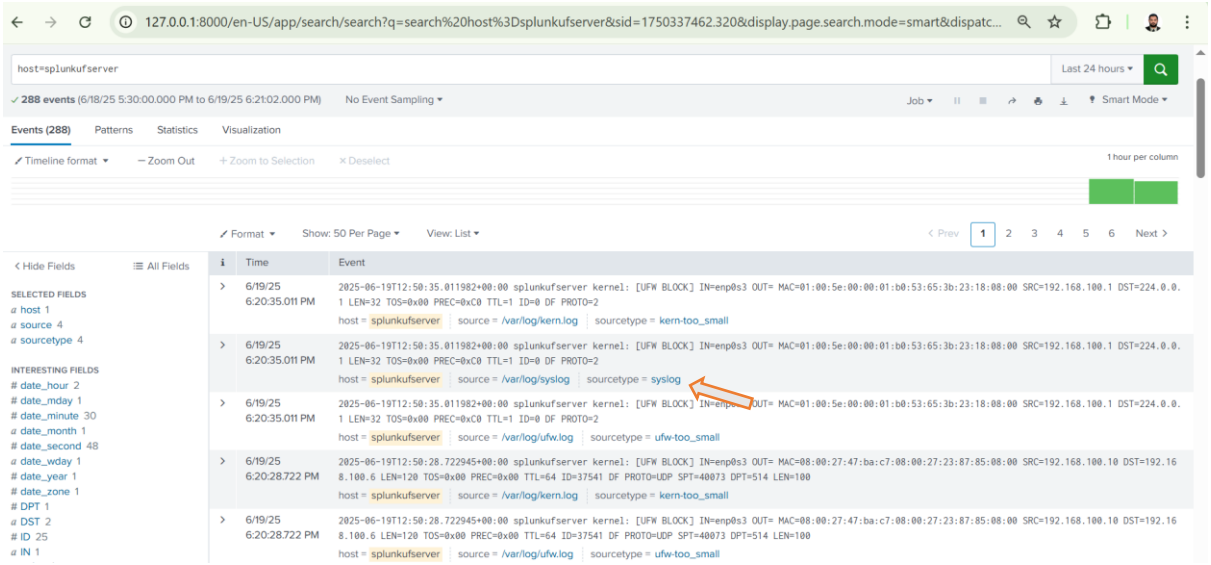
It shows both:

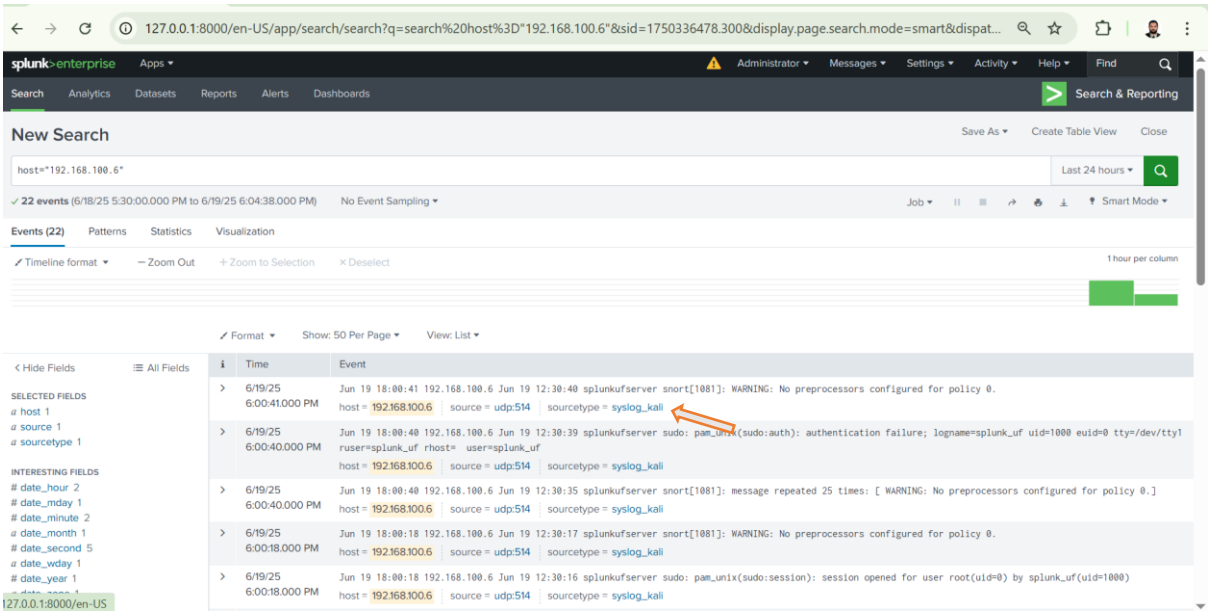
- **Active Forwards**: Working forwarder IPs
- **Inactive Forwards**: Configured but not working

2. **Add a Forward Server (Enterprise Splunk Server)**
   #sudo ./splunk add forward-server 192.168.100.5:9997
   Output confirms: Added forwarding to: 192.168.100.5:9997
3. **Add Monitor for** /var/log/syslog
   #sudo ./splunk add monitor /var/log/syslog
   Output: Added monitor of '/var/log/syslog'.



```
splunk_uf@splunkufserver:~$ cd /opt/splunkforwarder/bin
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk list forward-server
[sudo] password for splunk_uf:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: admin
Password:
Active forwards:
        None
Configured but inactive forwards:
        192.168.100.10:9997
        192.168.100.3:9997
        192.168.19.106:9997
        192.168.19.196:9997
        192.168.202.196:9997
        192.168.56.2:9997
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk add forward-server 192.168.100.5:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added forwarding to: 192.168.100.5:9997.
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ sudo ./splunk add monitor /var/log/syslog
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Added monitor of '/var/log/syslog'.
splunk_uf@splunkufserver:/opt/splunkforwarder/bin$ _
```





✅ Result

You now have:

- ✅ Logs generated on **Kali Linux**
- ✅ Forwarded to **Ubuntu**
- ✅ Finally relayed to **Enterprise Server**

All via secure and structured `rsyslog` configurations.