Forwarding via iptables and rsyslog

This procedure is intends for forwarding logs from a variety of end machines to XpoLog SysLog listener, using a Linux proxy server that is responsible for forwarding all traffic which has been forwarded to the relevant listener.

We will use this method when there is no direct access from the end machines to the XpoLog server. and a mediating machine is needed

Procedure

1. Configure TCP\UDP Listener on the your XpoLog machine.
2. Using rsyslog configuration for defining the logs which I would like to transfer to the proxy.

- With root user, edit the /etc/rsyslog.conf file.
- Create the following configuration:

  $ModLoad imfile
  $InputFileName File_Path
  $InputFileTag TAG
  $InputFileStateFile STATE
  $InputFileSeverity SEVERITY
  $InputFileFacility FACILITY
  $InputRunFileMonitor
  FACILITY.* @@PROXY_SERVER:PROXY_PORT

  Note - '@' is used for UDP and '@@' for TCP.
- Set the default syslog configuration within this file as marks.

  #$FileOwner syslog
  #$FileGroup adm
  #$FileCreateMode 0640
  #$DirCreateMode 0755
  #$Umask 0022
  #$PrivDropToUser syslog
  #$PrivDropToGroup syslog
- Reload the rsyslog service with /etc/init.d/rsyslog restart

3. Open ssh window directly to the Linux machine which serves you as a proxy and configure the iptables rules with the following commands:

- Allowing IP forwarding in your server - sysctl net.ipv4.ip_forward=1
- ```
  iptables -F
  iptables -t nat -F
  iptables -X
  ```
- Define a TCP\UDP rule which will forward all the traffic which is sent to the port of the proxy to the XpoLog machine, via the port which XpoLog listens to:

```
iptables -t nat -A PREROUTING -p tcp --dport Listen_Port_Proxy -j DNAT --to-destination
XpoLog_IP:XpoLog_Listener_Port
```

- Using command for MASQUERADE the traffic.

```
iptables -t nat -A POSTROUTING -j MASQUERADE
```

- Reload the firewall of the proxy server
  ufw reload
```