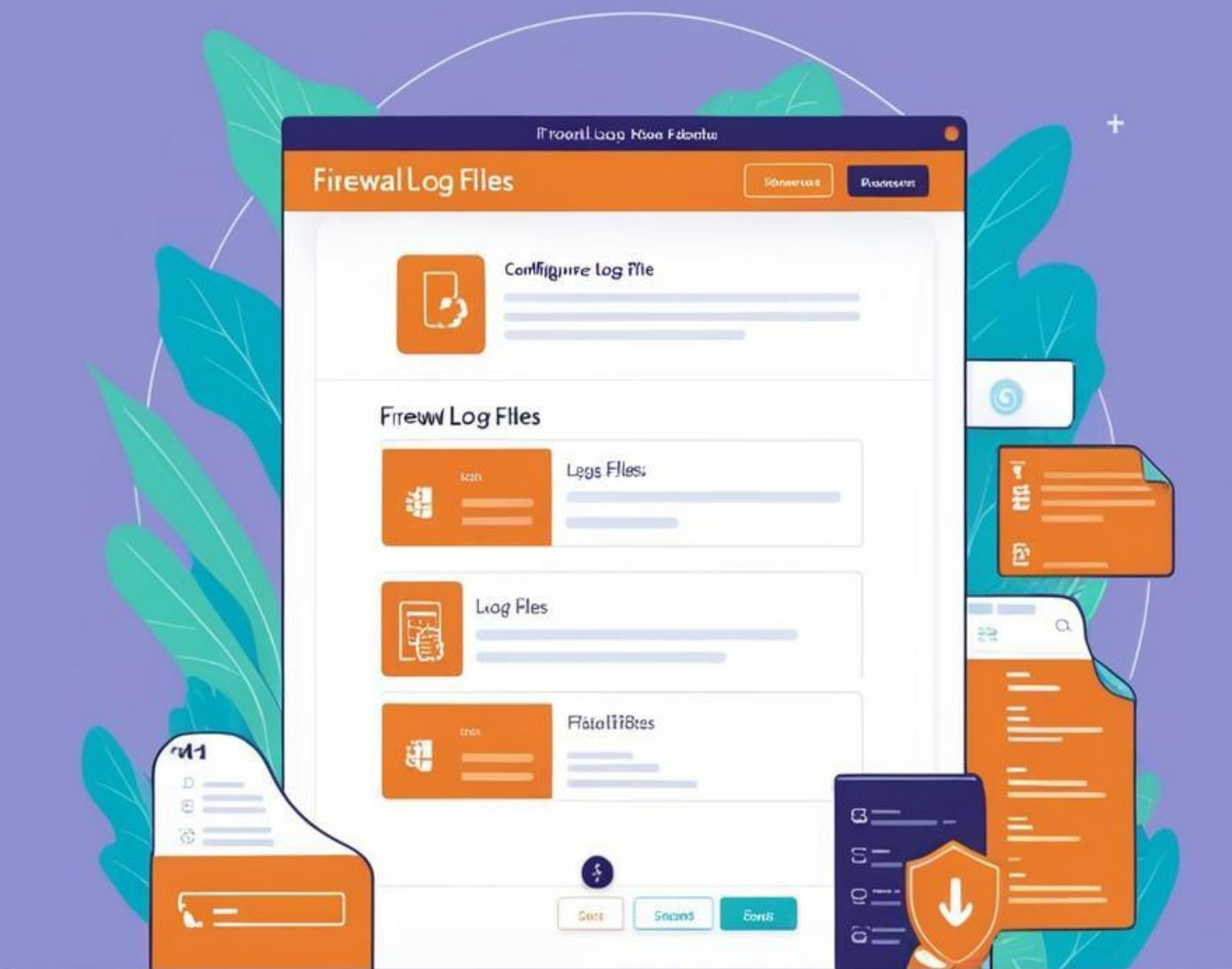


Configuración de los Ficheros log del cortafuego



Ivana Sánchez Pérez

Introducción

Los archivos de log del cortafuegos son registros detallados de las actividades que ocurren en el cortafuegos. Estos registros son esenciales para la seguridad y el monitoreo de la red, ya que permiten a los administradores identificar y analizar posibles amenazas o intrusiones.

¿Qué es un archivo de log del cortafuegos?

Un archivo de log del cortafuegos es un documento que registra todas las conexiones y actividades que pasan a través del cortafuegos. Estos registros pueden incluir información como:

- Direcciones IP de origen y destino
- Puertos utilizados
- Protocolos empleados
- Horarios de las conexiones
- Acciones tomadas por el cortafuegos (permitir, denegar, bloquear)

Importancia de los archivos de log del cortafuegos

1. **Monitoreo de la seguridad:** Los archivos de log permiten a los administradores monitorear las actividades de la red y detectar comportamientos sospechosos o no autorizados.
2. **Análisis de incidentes:** En caso de una brecha de seguridad, los archivos de log pueden ayudar a identificar cómo ocurrió el incidente y qué secciones de la red fueron afectadas.
3. **Cumplimiento y auditoría:** Los registros de cortafuegos son cruciales para cumplir con regulaciones y estándares de seguridad, así como para realizar auditorías internas y externas.
4. **Optimización del rendimiento:** Analizando los logs, los administradores pueden identificar patrones de tráfico y ajustar las políticas del cortafuegos para mejorar el rendimiento de la red.

Ejemplos de herramientas y sistemas de log

- **iptables:** Utilizado en sistemas Linux para configurar y gestionar reglas de cortafuegos.
- **Firewall-1 de Check Point:** Incorpora un módulo de inspección con estado (stateful inspection) que registra todas las actividades en el cortafuegos.

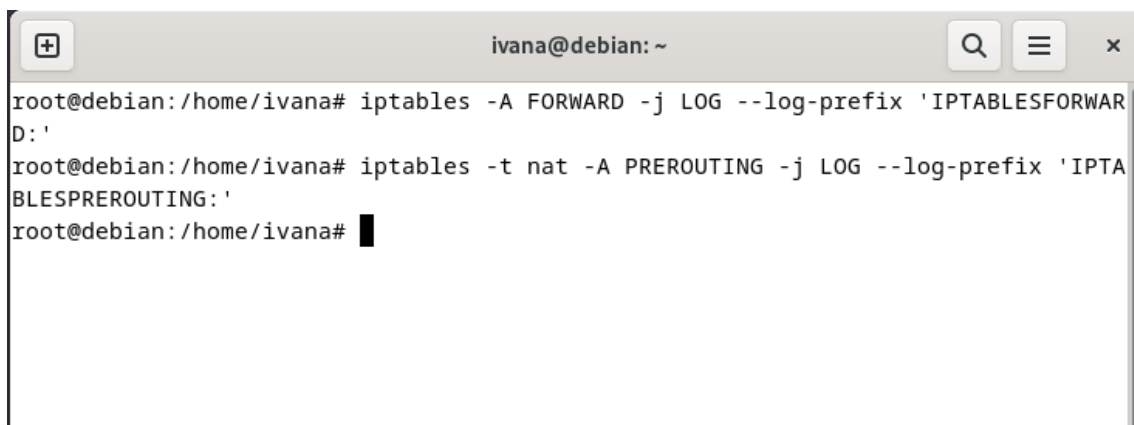
- **Cisco ASA:** Un cortafuegos de hardware que proporciona registros detallados de todas las conexiones y actividades.
- **ELK Stack (Elasticsearch, Logstash, Kibana):** Una herramienta popular para la recolección, almacenamiento y visualización de logs de cortafuegos.

Conclusión

Los archivos de log del cortafuegos son una herramienta fundamental para la seguridad de la red. Permiten a los administradores monitorear, analizar y optimizar el rendimiento del cortafuegos, así como cumplir con regulaciones y realizar auditorías.

Configuración de los archivos log

- 1- Agregamos las reglas de iptables para registrar paquetes y almacenarlas en el archivo logs con:
 - `sudo iptables -A FORWARD -j LOG --log-prefix 'IPTABLESFORWARD: '`
 - `sudo iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING: '`

A terminal window titled 'ivana@debian: ~' showing the execution of two iptables commands. The first command is 'iptables -A FORWARD -j LOG --log-prefix 'IPTABLESFORWARD: '' and the second is 'iptables -t nat -A PREROUTING -j LOG --log-prefix 'IPTABLESPREROUTING: ''.

Con las reglas anteriores no se han añadido reglas en las cadenas INPUT o OUTPUT, que son esenciales para registrar tráfico entrante o saliente directamente relacionado con nuestro sistema. Por lo que procedo a ajustar y completar la configuración.

A terminal window titled 'ivana@debian: ~' showing the execution of two additional iptables commands. The first is 'iptables -A INPUT -j LOG --log-prefix 'IPTABLES INPUT:' --log-level 4' and the second is 'iptables -A OUTPUT -j LOG --log-prefix 'IPTABLES OUTPUT:' --log-level 4'.

```
ivana@debian: ~  
root@debian:/home/ivana# sudo iptables -L -n -v  
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination LOG flags 0 level 4 prefix "IPTABLES INPUT:"  
4 298 LOG 0 -- * * 0.0.0.0/0 0.0.0.0/0  
  
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination  
  
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)  
pkts bytes target prot opt in out source destination LOG flags 0 level 4 prefix "IPTABLES OUTPUT:"  
4 298 LOG 0 -- * * 0.0.0.0/0 0.0.0.0/0  
root@debian:/home/ivana#
```

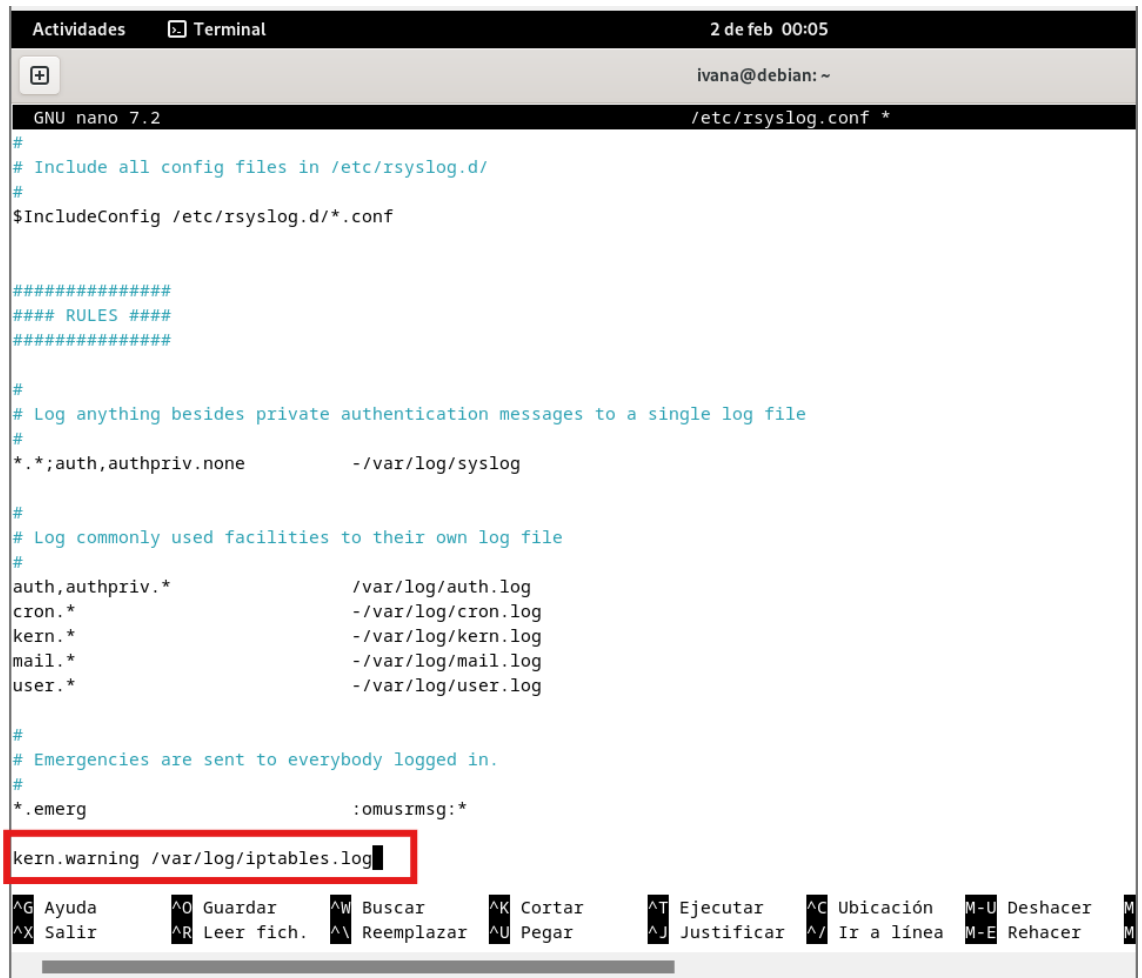
Explicación:

- -A FORWARD: Agrega una regla a la cadena FORWARD.
- -t nat -A PREROUTING: Agrega una regla en la tabla NAT antes de reenviar paquetes.
- -j LOG: Indica que los paquetes deben ser registrados en los logs.
- --log-prefix: Agrega un prefijo a los registros para identificarlos fácilmente.

2- Configuramos el sistema de logs. Para ello primero instalamos e iniciamos el sistema rsyslog.

```
ivana@debian: ~  
Created symlink /etc/systemd/system/multi-user.target.wants/rsyslog.service  
ib/systemd/system/rsyslog.service.  
Procesando disparadores para libc-bin (2.36-9+deb12u9) ...  
Procesando disparadores para man-db (2.11.2-2) ...  
root@debian:/home/ivana# sudo systemctl enable rsyslog  
root@debian:/home/ivana# sudo systemctl start rsyslog  
root@debian:/home/ivana# sudo systemctl status rsyslog  
● rsyslog.service - System Logging Service  
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: en  
   Active: active (running) since Sat 2025-02-01 23:53:24 CET; 57s ago  
TriggeredBy: ● syslog.socket  
   Docs: man:rsyslogd(8)  
         man:rsyslog.conf(5)  
         https://www.rsyslog.com/doc/  
 Main PID: 3494 (rsyslogd)  
   Tasks: 4 (limit: 3490)  
  Memory: 1.3M  
    CPU: 12ms  
   CGroup: /system.slice/rsyslog.service  
           └─3494 /usr/sbin/rsyslogd -n -iNONE  
  
feb 01 23:53:24 debian systemd[1]: Starting rsyslog.service - System Logging  
feb 01 23:53:24 debian rsyslogd[3494]: imuxsock: Acquired UNIX socket '/run/  
feb 01 23:53:24 debian systemd[1]: Started rsyslog.service - System Logging
```

Y posteriormente editamos el archivo de configuración de rsyslog para asegurarnos que el sistema almacene los registros en un archivo separado. Hacemos un `sudo nano /etc/rsyslog.conf` y le añadimos la línea `kern.warning /var/log/iptables.log` al final del mismo. Esta línea nos indica que los mensajes de nivel “warning” generados por el kernel se guardaran en el archivo `iptables.log`.



```
Actividades Terminal 2 de feb 00:05
ivana@debian: ~
GNU nano 7.2 /etc/rsyslog.conf *
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf

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

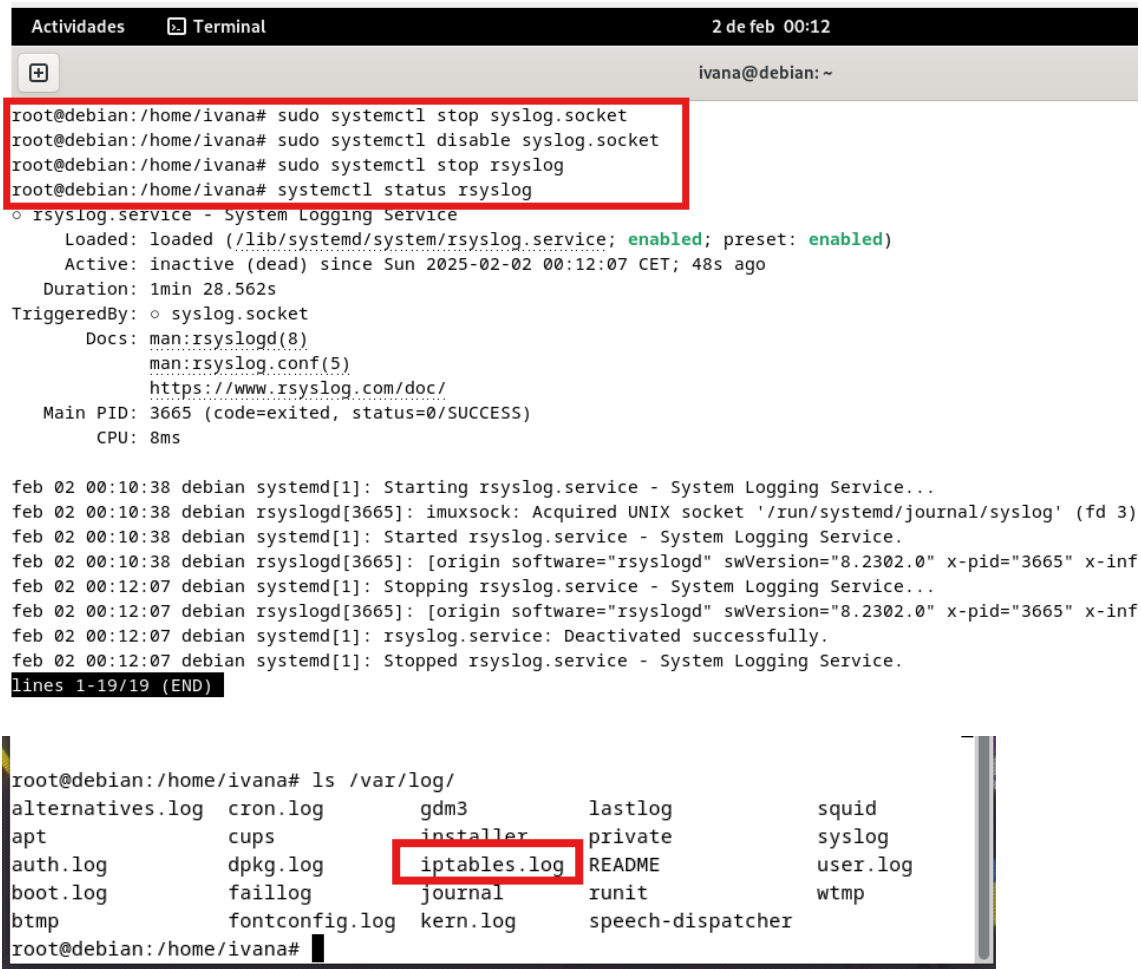
#
# Log anything besides private authentication messages to a single log file
#
*. *;auth,authpriv.none -/var/log/syslog

#
# 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 :omusmsg:*

kern.warning /var/log/iptables.log
^G Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación M-U Deshacer M
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^/ Ir a línea M-E Rehacer M
```

Reiniciamos y verificamos el servicio



```
Actividades Terminal 2 de feb 00:12
ivana@debian: ~

root@debian:/home/ivana# sudo systemctl stop syslog.socket
root@debian:/home/ivana# sudo systemctl disable syslog.socket
root@debian:/home/ivana# sudo systemctl stop rsyslog
root@debian:/home/ivana# systemctl status rsyslog
○ rsyslog.service - System Logging Service
   Loaded: loaded (/lib/systemd/system/rsyslog.service; enabled; preset: enabled)
   Active: inactive (dead) since Sun 2025-02-02 00:12:07 CET; 48s ago
   Duration: 1min 28.562s
   TriggeredBy: ○ syslog.socket
   Docs: man:rsyslogd(8)
         man:rsyslog.conf(5)
         https://www.rsyslog.com/doc/
   Main PID: 3665 (code=exited, status=0/SUCCESS)
   CPU: 8ms

feb 02 00:10:38 debian systemd[1]: Starting rsyslog.service - System Logging Service...
feb 02 00:10:38 debian rsyslogd[3665]: imuxsock: Acquired UNIX socket '/run/systemd/journal/syslog' (fd 3)
feb 02 00:10:38 debian systemd[1]: Started rsyslog.service - System Logging Service.
feb 02 00:10:38 debian rsyslogd[3665]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="3665" x-inf
feb 02 00:12:07 debian systemd[1]: Stopping rsyslog.service - System Logging Service...
feb 02 00:12:07 debian rsyslogd[3665]: [origin software="rsyslogd" swVersion="8.2302.0" x-pid="3665" x-inf
feb 02 00:12:07 debian systemd[1]: rsyslog.service: Deactivated successfully.
feb 02 00:12:07 debian systemd[1]: Stopped rsyslog.service - System Logging Service.
lines 1-19/19 (END)

root@debian:/home/ivana# ls /var/log/
alternatives.log  cron.log      gdm3          lastlog       squid
apt               cups          installer     private       syslog
auth.log          dpkg.log      iptables.log  README        user.log
boot.log          faillog       journal       runit         wtmp
btmtp             fontconfig.log kern.log      speech-dispatcher
root@debian:/home/ivana#
```

Verificamos que los logs se están generando. Si no lo vemos inmediatamente, generamos el tráfico para que iptables tenga algo que registrar. Y ahora ya podemos verificar que iptables está registrando con el comando `sudo tail -f /var/log/iptables.log`. También lo podemos ver con un `cat /var/log/iptables.log`


```
ivana@de
root@debian:/home/ivana# ping -c 4 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=116 time=28.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=116 time=15.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=116 time=15.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=116 time=45.0 ms

--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3017ms
rtt min/avg/max/mdev = 15.616/26.279/44.988/12.062 ms
root@debian:/home/ivana# cat /var/log/iptables.log
```

Analizamos los registros. Cada línea en el log contiene información clave

```
Actividades Terminal 2 de feb 14:22
ivana@debian: ~
2025-02-02T14:14:57.512061+01:00 debian kernel: [ 1084.530897] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=90.68.206.60 DST=10.0.2.15 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=242 PROTO=UDP SPT=123 DPT=45719 LEN=56
2025-02-02T14:15:29.689450+01:00 debian kernel: [ 1116.703733] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=90.68.206.60 LEN=76 TOS=0x18
PREC=0xA0 TTL=64 ID=35177 DF PROTO=UDP SPT=35186 DPT=123 LEN=56
2025-02-02T14:15:29.877837+01:00 debian kernel: [ 1116.890989] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=90.68.206.60 DST=10.0.2.15 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=243 PROTO=UDP SPT=123 DPT=35186 LEN=56
2025-02-02T14:15:55.346730+01:00 debian kernel: [ 1142.333662] hrtimer: interrupt took 34846049 ns
2025-02-02T14:16:01.937283+01:00 debian kernel: [ 1148.950683] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=90.68.206.60 LEN=76 TOS=0x18
PREC=0xA0 TTL=64 ID=40434 DF PROTO=UDP SPT=38870 DPT=123 LEN=56
2025-02-02T14:16:03.733523+01:00 debian kernel: [ 1150.746871] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=8.8.8.8 LEN=84 TOS=0x00 PREC
=0x00 TTL=64 ID=38283 DF PROTO=ICMP TYPE=8 CODE=0 ID=2662 SEQ=1
2025-02-02T14:16:03.778116+01:00 debian kernel: [ 1150.775595] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=8.8.8.8 DST=10.0.2.15 LEN=84 TOS=0x00 PREC=0x00 TTL=116 ID=244 PROTO=ICMP TYPE=0 CODE=0 ID=2662 SEQ=1
2025-02-02T14:16:04.736115+01:00 debian kernel: [ 1151.750040] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=8.8.8.8 LEN=84 TOS=0x00 PREC
=0x00 TTL=64 ID=38284 DF PROTO=ICMP TYPE=8 CODE=0 ID=2662 SEQ=2
2025-02-02T14:16:04.752074+01:00 debian kernel: [ 1151.765724] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=8.8.8.8 DST=10.0.2.15 LEN=84 TOS=0x00 PREC=0x00 TTL=116 ID=245 PROTO=ICMP TYPE=0 CODE=0 ID=2662 SEQ=2
2025-02-02T14:16:05.740175+01:00 debian kernel: [ 1152.753158] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=8.8.8.8 LEN=84 TOS=0x00 PREC
=0x00 TTL=64 ID=38322 DF PROTO=ICMP TYPE=8 CODE=0 ID=2662 SEQ=3
2025-02-02T14:16:05.756060+01:00 debian kernel: [ 1152.768755] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=8.8.8.8 DST=10.0.2.15 LEN=84 TOS=0x00 PREC=0x00 TTL=116 ID=246 PROTO=ICMP TYPE=0 CODE=0 ID=2662 SEQ=3
2025-02-02T14:16:06.752097+01:00 debian kernel: [ 1153.764670] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=8.8.8.8 LEN=84 TOS=0x00 PREC
=0x00 TTL=64 ID=38394 DF PROTO=ICMP TYPE=8 CODE=0 ID=2662 SEQ=4
2025-02-02T14:16:06.796348+01:00 debian kernel: [ 1153.809126] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=8.8.8.8 DST=10.0.2.15 LEN=84 TOS=0x00 PREC=0x00 TTL=116 ID=247 PROTO=ICMP TYPE=0 CODE=0 ID=2662 SEQ=4
2025-02-02T14:16:17.188607+01:00 debian kernel: [ 1164.197911] IPTABLES OUTPUT:IN= OUT=enp0s3 SRC=10.0.2.15 DST=90.68.206.60 LEN=76 TOS=0x18
PREC=0xA0 TTL=64 ID=42183 DF PROTO=UDP SPT=38870 DPT=123 LEN=56
2025-02-02T14:16:17.396567+01:00 debian kernel: [ 1164.405834] IPTABLES INPUT:IN=enp0s3 OUT= MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00 S
RC=90.68.206.60 DST=10.0.2.15 LEN=76 TOS=0x00 PREC=0x00 TTL=64 ID=248 PROTO=UDP SPT=123 DPT=38870 LEN=56
root@debian:/home/ivana#
```

Explicación de los datos registrados:

1. **Fecha y hora** → 2025-02-02 14:14:57
2. **Nombre del equipo** → debian
3. **Código del log del kernel** → kernel:
4. **Prefijo personalizado** → [IPTABLES INPUT]
5. **Interfaces de red** → IN=enp0s3

6. **Direcciones MAC** → OUT
=MAC=08:00:27:3a:49:2f:52:54:00:12:35:02:08:00
7. **Dirección IP de origen** → SRC=90.68.206.60
8. **Dirección IP de destino** → DST=10.0.2.15
9. **Longitud del paquete** → LEN=76
10. **Tipo de servicio (ToS)** → TOS=0x00 PREC=0x00
11. **Tiempo de vida (TTL)** → TTL=64
12. **ID de reensamblaje** → ID=242
13. **Protocolo de transporte** → PROTO=UDP
14. **Puerto de origen** → SPT=123
15. **Puerto de destino** → DPT=45719 LEN=56