

For Context, there were a set of firewalls with exactly the same configuration and output as below but only this firewall cannot send the logs to the designated syslog server. Seems the configuration is not taking effect.

Log Forwarding Profile (Read Only)

Name: Panorama_Logging_PRD

Description:

NAME	LOG TYPE	FILTER	FORWARD METHOD	BUILT-IN ACTIONS
Traffic_logs	traffic	All Logs	<ul style="list-style-type: none"> Panorama SysLog [REDACTED] 	
Threat_logs	threat	All Logs	<ul style="list-style-type: none"> Panorama SysLog [REDACTED] 	
Wififire_logs	wififire	All Logs		

3 Items

Buttons: Add, Delete, Clone, OK, Cancel

Syslog Server Profile

Name: 01A

Shared

Servers | Custom Log Format

NAME	SYSLOG SERVER	TRANSPORT	PORT	FORMAT	FACILITY
[REDACTED]	[REDACTED]	UDP	514	BSD	LOG_LOCAL7

Buttons: Add, Delete, OK, Cancel

Enter the IP address or FQDN of the Syslog server

```
14:21:33.095339 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 668
14:21:33.095366 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 811
14:21:33.095391 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 666
14:21:33.095417 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 840
14:21:33.095443 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 783
14:21:33.095468 IP [REDACTED] 46645 > [REDACTED] .syslog: SYSLOG local7.info, length: 654
```

```
admin@RHB-PRD-DMZ-FW01(active)>
admin@RHB-PRD-DMZ-FW01(active)> show netstat numeric-hosts yes numeric-ports yes all yes | match 514
tcp        0      0 127.0.0.1:51464      127.0.0.1:28260      ESTABLISHED
tcp6       0      0 :::10514              :::*                  LISTEN      RC
tcp6       0      0 127.0.0.1:28260      127.0.0.1:51464      ESTABLISHED
udp6       0      0 :::10514              :::*                  *
```