Palo Alto Networks PANOS 6.1, Cisco WLC 5500, Kiwi Syslogd integration guide

Alberto Rivai

Systems Engineer – Major Accounts

Palo Alto Networks

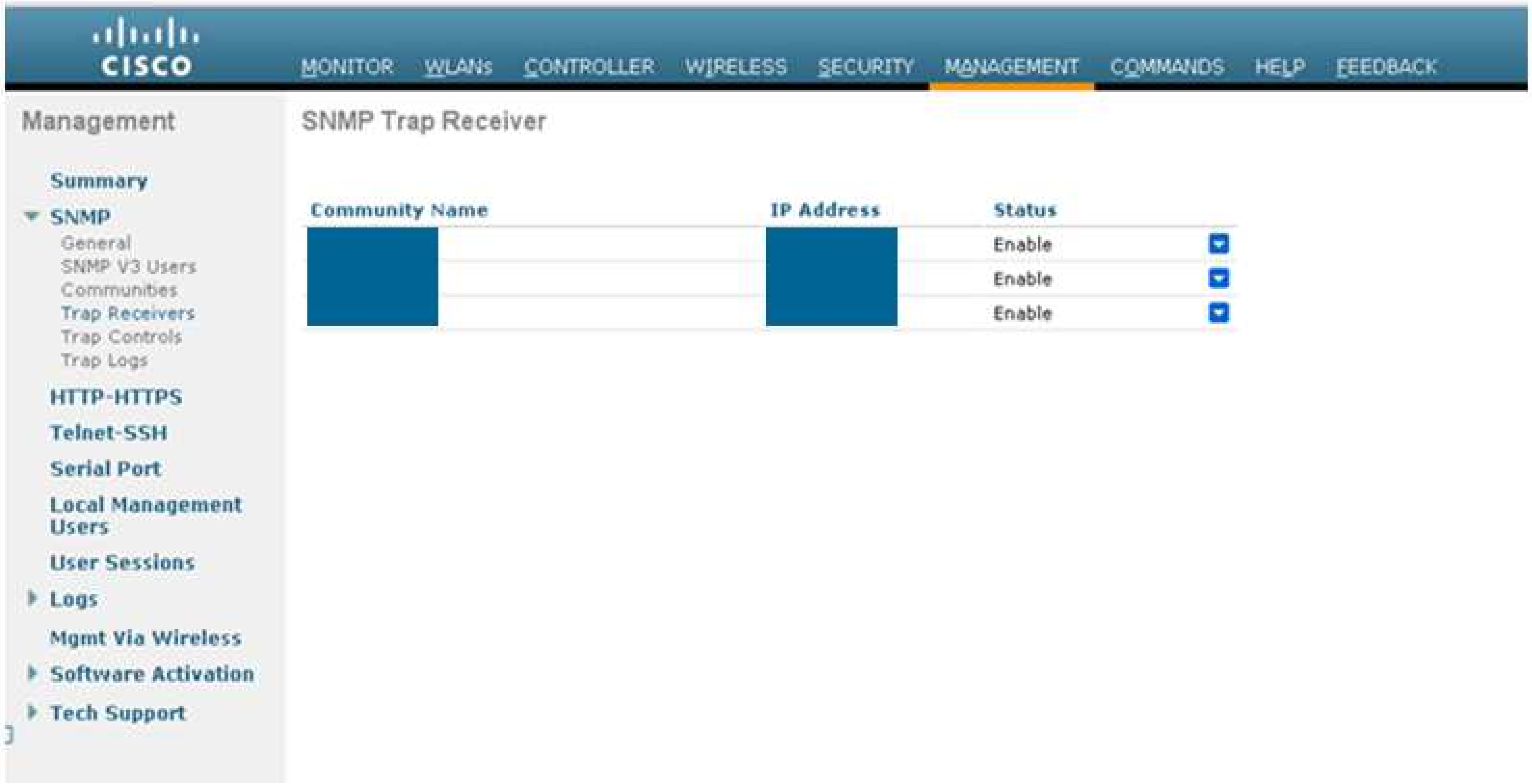
Melbourne, Australia

Summary

- PAN-OS 6.0 introduced the ability to use the Palo Alto Networks firewall and the User-ID Agent as a syslog listener for collecting syslogs from different systems in the network, and to map users to IP addresses. The user to IP mappings could be used in security rules and policies.
- The problem with Cisco Wireless LAN Controller, it does not send successful user authentication message through syslog. Cisco WLC generates SNMP traps which we can utilize to get the user to IP mapping.
- This document shows a quick configuration guide on how to configure Cisco WLC to send SNMP traps to Kiwi Syslogd, which then converts and forwards the messages through syslog protocol to Palo Alto Networks syslog receiver.

Cisco WLC configuration

- Create SNMP receiver by going to Management tab and Trap Receivers

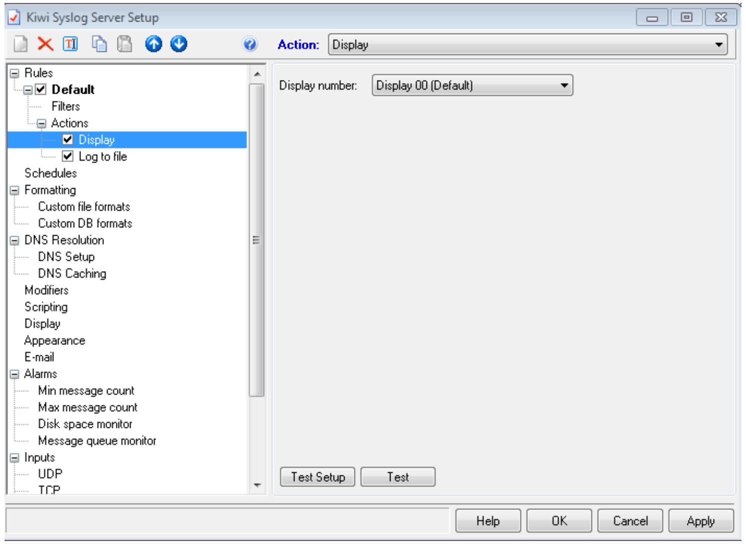


SNMP Trap Receiver

Community Name	IP Address	Status
[redacted]	[redacted]	Enable
[redacted]	[redacted]	Enable
[redacted]	[redacted]	Enable

Kiwi Syslogd configuration - 1

- Open Kiwi Syslog server console, go to File -> Setup



Kiwi Syslog Server Setup

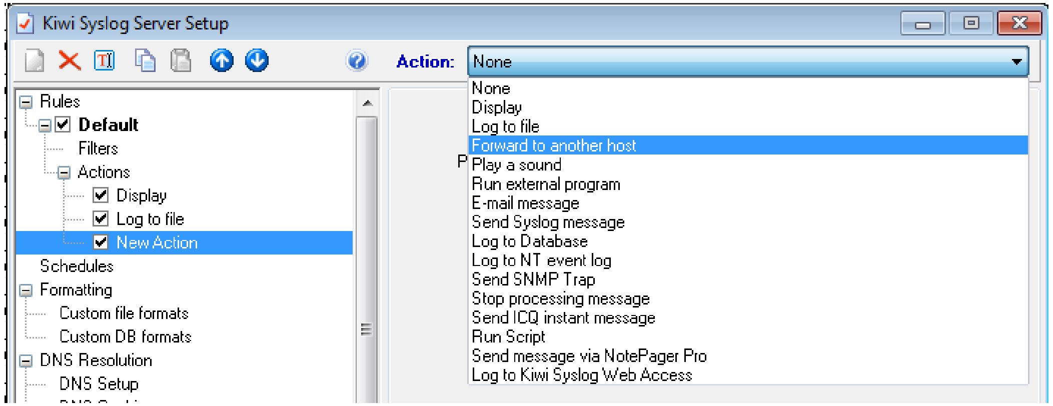
Action: Display

Display number: Display 00 (Default)

- Right click on Actions and create a new action

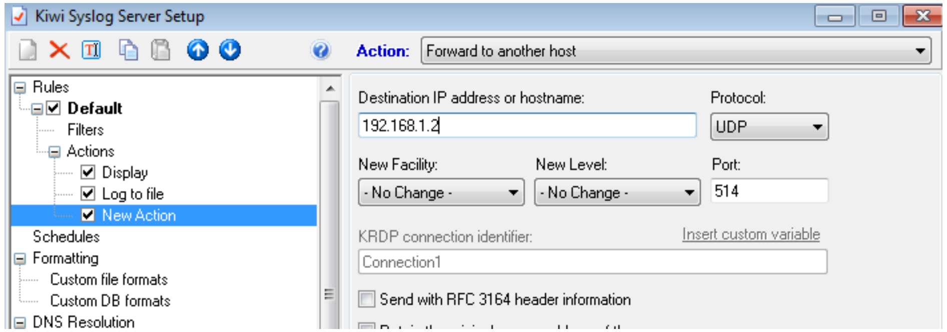
Kiwi Syslogd configuration - 2

- Select Forward to another host



Action: None

- Enter the IP address of the Palo Alto Networks syslog receiver



Action: Forward to another host

Destination IP address or hostname: 192.168.1.2

Protocol: UDP

New Facility: - No Change -

New Level: - No Change -

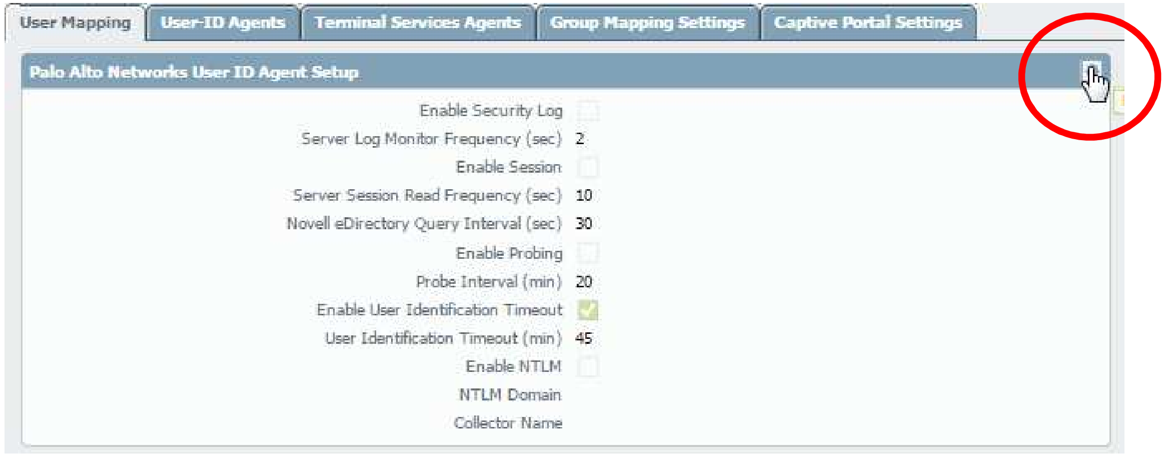
Port: 514

KRDP connection identifier: Connection1

□ Send with RFC 3164 header information

Palo Alto Networks configuration - 1

- Login to the WebUI
- Go to Device -> User Identification
- Click on the gear icon on the Palo Alto Networks User ID Agent setup window

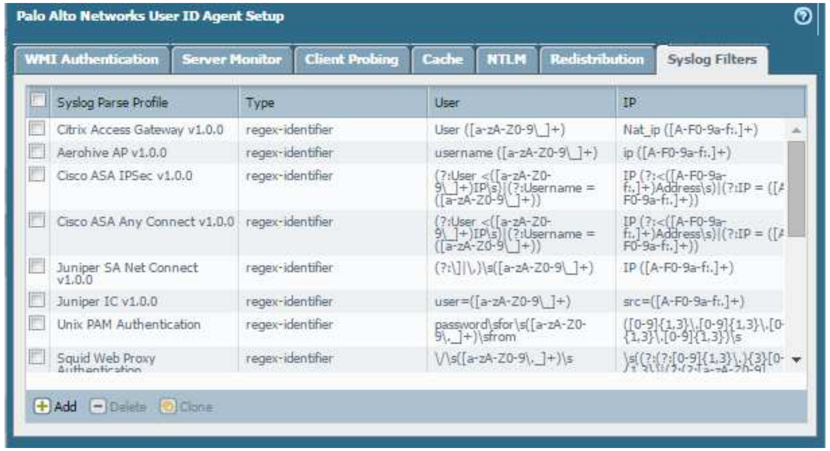


Palo Alto Networks User ID Agent Setup

Enable Security Log	□
Server Log Monitor Frequency (sec)	2
Enable Session	□
Server Session Read Frequency (sec)	10
Novell eDirectory Query Interval (sec)	30
Enable Probing	□
Probe Interval (min)	20
Enable User Identification Timeout	☑
User Identification Timeout (min)	45
Enable NTLM	□
NTLM Domain	
Collector Name	

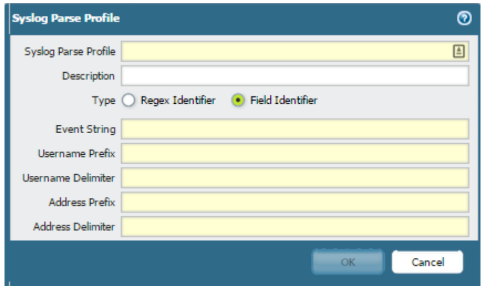
Palo Alto Networks configuration - 2

- Go to Syslog Filters tab and click Add



□	Syslog Parse Profile	Type	User	IP
□	Citrix Access Gateway v1.0.0	regex-identifier	User ([a-zA-Z0-9_]+)	Nat_ip ([A-F0-9a-f:.]+)
□	Aerohive AP v1.0.0	regex-identifier	username ([a-zA-Z0-9_]+)	ip ([A-F0-9a-f:.]+)
□	Cisco ASA IPSec v1.0.0	regex-identifier	(?:User <([a-zA-Z0-9_]+)IP\s)|(?:Username = ([a-zA-Z0-9_]+))	IP (?:<([A-F0-9a-f:.]+)Address\s)|(?:IP = ([A-F0-9a-f:.]+))
□	Cisco ASA Any Connect v1.0.0	regex-identifier	(?:User <([a-zA-Z0-9_]+)IP\s)|(?:Username = ([a-zA-Z0-9_]+))	IP (?:<([A-F0-9a-f:.]+)Address\s)|(?:IP = ([A-F0-9a-f:.]+))
□	Juniper SA Net Connect v1.0.0	regex-identifier	(?:\]|\.)\s([a-zA-Z0-9_]+)	IP ([A-F0-9a-f:.]+)
□	Juniper IC v1.0.0	regex-identifier	user=([a-zA-Z0-9_]+)	src=([A-F0-9a-f:.]+)
□	Unix PAM Authentication	regex-identifier	password\sfor\s([a-zA-Z0-9\._]+)\sfrom	([0-9]{1,3}\.[0-9]{1,3}\.[0-{1,3}\.[0-9]{1,3})\s
□	Squid Web Proxy Authentication	regex-identifier	\/\s([a-zA-Z0-9\._]+)\s	\s((?:(?:[0-9]{1,3}\.){3}[0-

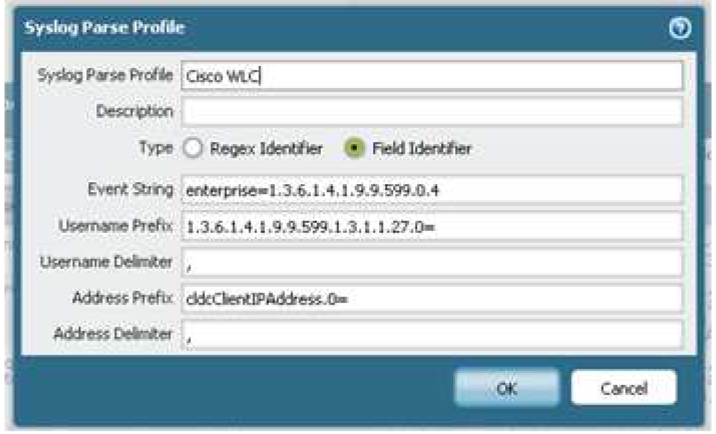
- Select Field Identifier



Syslog Parse Profile	
Description	
Type	○ Regex Identifier ● Field Identifier
Event String	
Username Prefix	
Username Delimiter	
Address Prefix	
Address Delimiter	

Palo Alto Networks configuration - 3

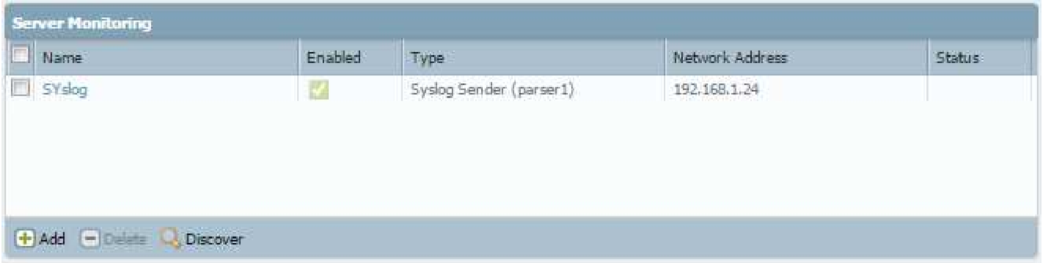
- Use the below identifier to identify the syslog message
  - Event String : enterprise=1.3.6.1.4.1.9.9.599.0.4
  - Username Prefix : 1.3.6.1.4.1.9.9.599.1.3.1.1.27.0=
  - Username Delimiter : ,
  - Address Prefix : cldcClientIPAddress.0=
  - Address Delimiter : ,



Syslog Parse Profile	Cisco WLC
Description	
Type	○ Regex Identifier ● Field Identifier
Event String	enterprise=1.3.6.1.4.1.9.9.599.0.4
Username Prefix	1.3.6.1.4.1.9.9.599.1.3.1.1.27.0=
Username Delimiter	,
Address Prefix	cldcClientIPAddress.0=
Address Delimiter	,

Palo Alto Networks configuration - 4

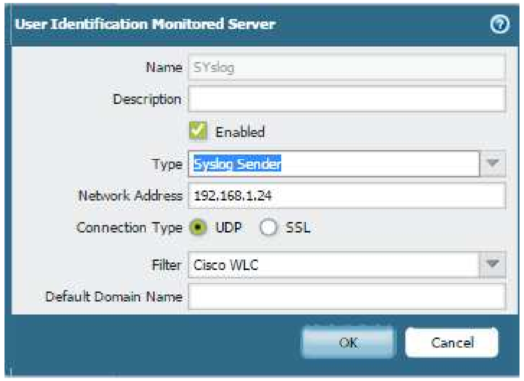
- Add Server Monitoring, go to Device – User Identification and click Add under Server Monitoring window



Server Monitoring

□	Name	Enabled	Type	Network Address	Status
□	SYslog	✓	Syslog Sender (parser1)	192.168.1.24	

- Select type : Syslog Sender and enter the IP address of Kiwi Syslogd server

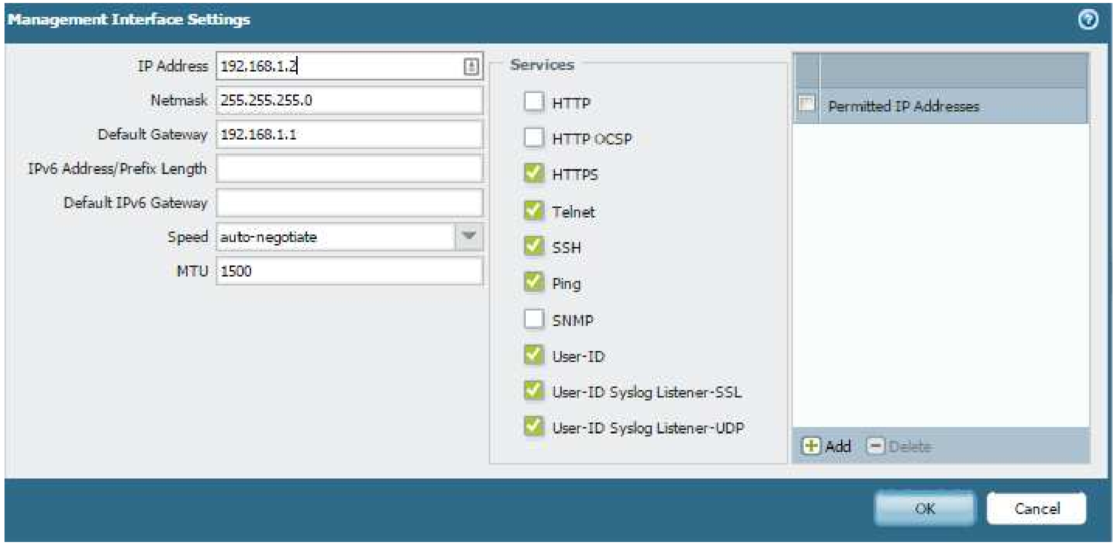


User Identification Monitored Server

Name	SYslog
Description	
	☑ Enabled
Type	Syslog Sender
Network Address	192.168.1.24
Connection Type	● UDP ○ SSL
Filter	Cisco WLC
Default Domain Name	

Palo Alto Networks configuration - 5

- Verify that the Syslog receiver is enabled
- Go to Device – Setup – Management – Management Interface Setting



Management Interface Settings

IP Address: 192.168.1.2
Netmask: 255.255.255.0
Default Gateway: 192.168.1.1
IPv6 Address/Prefix Length:
Default IPv6 Gateway:
Speed: auto-negotiate
MTU: 1500

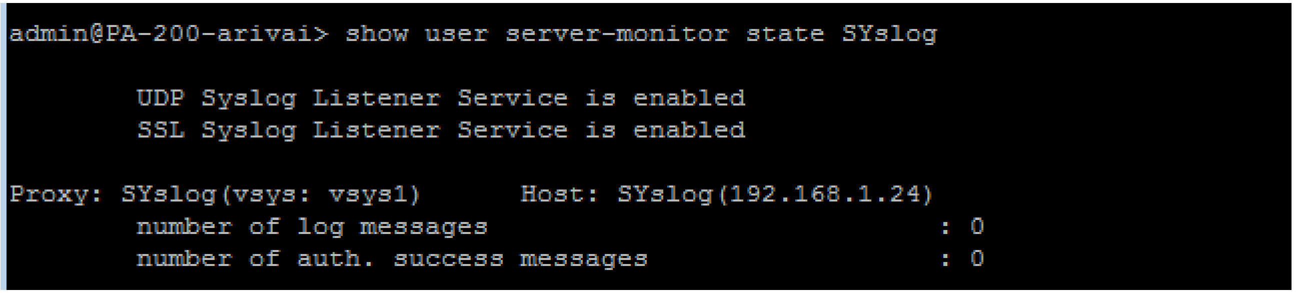
Services

- ☐ HTTP
- ☐ HTTP OCSP
- ☑ HTTPS
- ☑ Telnet
- ☑ SSH
- ☑ Ping
- ☐ SNMP
- ☑ User-ID
- ☑ User-ID Syslog Listener-SSL
- ☑ User-ID Syslog Listener-UDP

☐ Permitted IP Addresses

Verify syslog receiver

- Execute the below command
  - `admin@PA-200-arivai> show user server-monitor <syslog receiver name>`

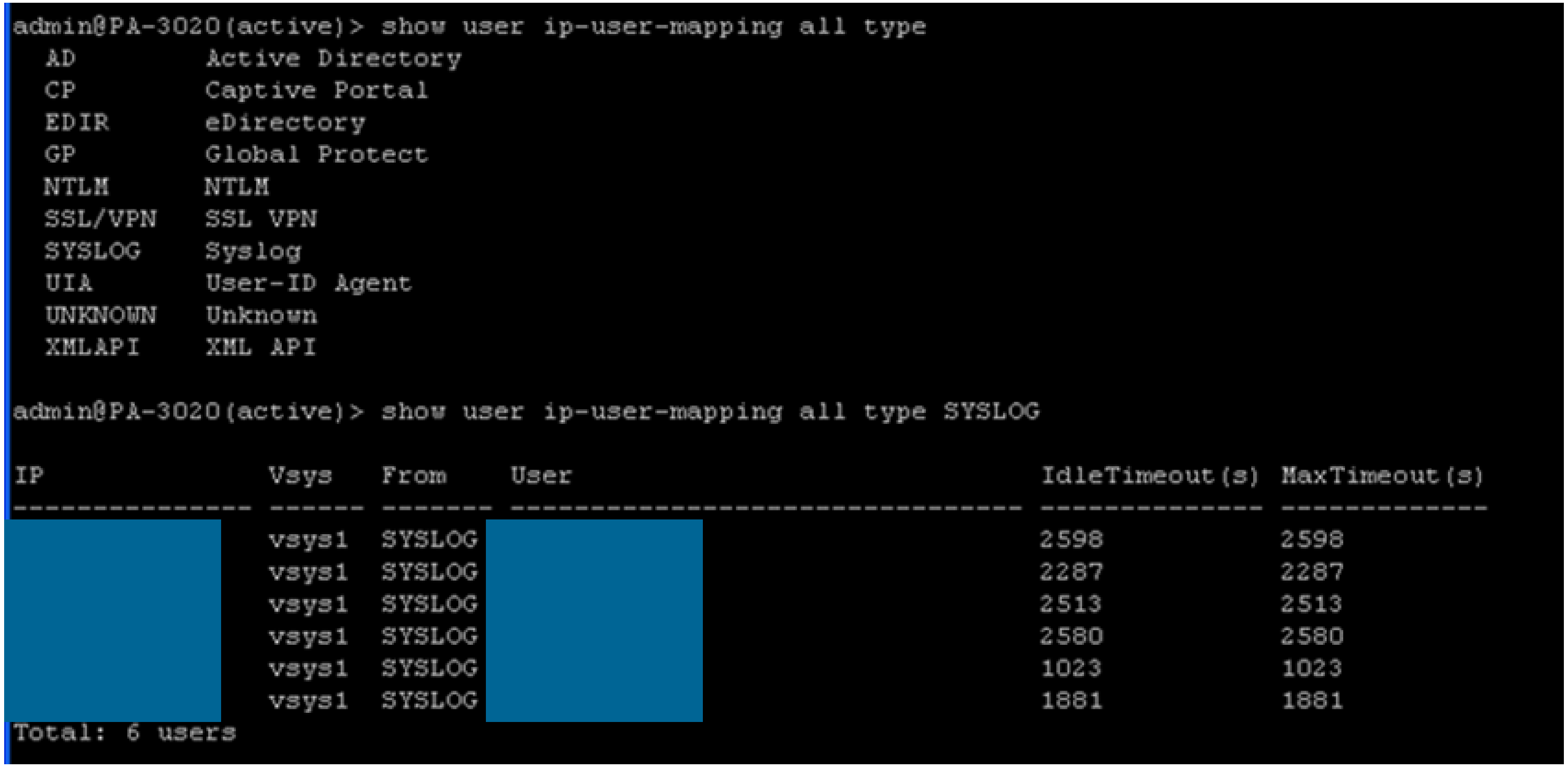


```
admin@PA-200-arivai> show user server-monitor state SYslog

        UDP Syslog Listener Service is enabled
        SSL Syslog Listener Service is enabled

Proxy: SYslog(vsys: vsys1)      Host: SYslog(192.168.1.24)
        number of log messages                            : 0
        number of auth. success messages                  : 0
```

- You will see the number of log messages increasing

Verify syslog receiver

- To identify if the syslog receiver successfully parsed the message and identify users, execute the below command
  - `admin@PA-200-arivai> show user ip-user-mapping all type SYSLOG`



```
admin@PA-3020(active)> show user ip-user-mapping all type
  AD          Active Directory
  CP          Captive Portal
  EDIR        eDirectory
  GP          Global Protect
  NTLM        NTLM
  SSL/VPN     SSL VPN
  SYSLOG      Syslog
  UIA         User-ID Agent
  UNKNOWN     Unknown
  XMLAPI      XML API

admin@PA-3020(active)> show user ip-user-mapping all type SYSLOG

IP               Vsys   From    User                             IdleTimeout(s) MaxTimeout(s)
---------------  ------ ------- -------------------------------- -------------- -------------
[redacted]       vsys1  SYSLOG  [redacted]                       2598           2598
                 vsys1  SYSLOG                                   2287           2287
                 vsys1  SYSLOG                                   2513           2513
                 vsys1  SYSLOG                                   2580           2580
                 vsys1  SYSLOG                                   1023           1023
                 vsys1  SYSLOG                                   1881           1881
Total: 6 users
```

paloalto networks®

the enterprise security company™