Enable Syslog on Port 514 and Allow via Firewall (Ubuntu)

Step 1: Install rsyslog

1. Open terminal.
2. Run the following commands:

```
sudo apt update
sudo apt install rsyslog -y
sudo systemctl enable rsyslog
sudo systemctl start rsyslog
```

Step 2: Enable Syslog Reception on Port 514

1.Open the rsyslog configuration file:

```
sudo nano /etc/rsyslog.conf
```

2. Find and uncomment or add these lines:

```
module(load="imudp")
input(type="imudp" port="514")
module(load="imtcp")
input(type="imtcp" port="514")
```

3.Save and exit (Ctrl+X, then Y, then Enter).

Step 3: Restart rsyslog

```
sudo systemctl restart rsyslog
```

Step 4: Allow Port 514 in UFW Firewall

1. Run the following:

```
sudo ufw allow 514/udp
sudo ufw allow 514/tcp
sudo ufw reload
```

2. Check status:

```
sudo ufw status
```

Step 5: Confirm Port is Listening

```
sudo ss -tulnp | grep 514
```

Or if netstat is available:

```
sudo netstat -tulnp | grep 514
```

Step 6: Optional - Test from Remote Client

From another machine:

```
logger -n <server-ip-address> -P 514 "Test syslog message"
```

Then on the Ubuntu server:

```
sudo tail -f /var/log/syslog
```

Step 7: End-to-End Connectivity Test (Ping)

From Azure VM (log collector), test connectivity to Cisco Meraki and Palo Alto devices.

Ping Cisco Meraki:

```
ping <meraki_ip_address>
```

Ping Palo Alto:

```
ping <palo_alto_ip_address>
```

> **If ping is successful, you'll see replies with time. If not, verify:**

- NSG and UFW rules in Azure
- On-prem firewall rules
- IP reachability and routing

*If you need further assistance, kindly contact our support at **support@cytechint.com** for prompt assistance and guidance.*

Revision #4
Created 7 July 2025 09:51:51 by Richmond Abella
Updated 7 July 2025 10:20:34 by Richmond Abella