

## **KAMAL STEEL**

**SOPHOS RED 60 CONFIGURATIONS**

**PREPARED BY: KEVIN MRANDA**

**DATE: 7<sup>TH</sup> January 2026**

This document provides the configuration details for the Sophos RED 60 device deployed at Kamal Steel Refinery

## Device Information

- Sophos Red 60
- Serial Number: R60005X36KGTCB
- Installed location: Kamal refinery

## Connection to Sophos Firewall

- RED ID: R60005X36KGTCB
- Provisioning Server: firewall.sophos.com
- Firewall IP: 41.207.241.90
- Tunnel mode: Standard

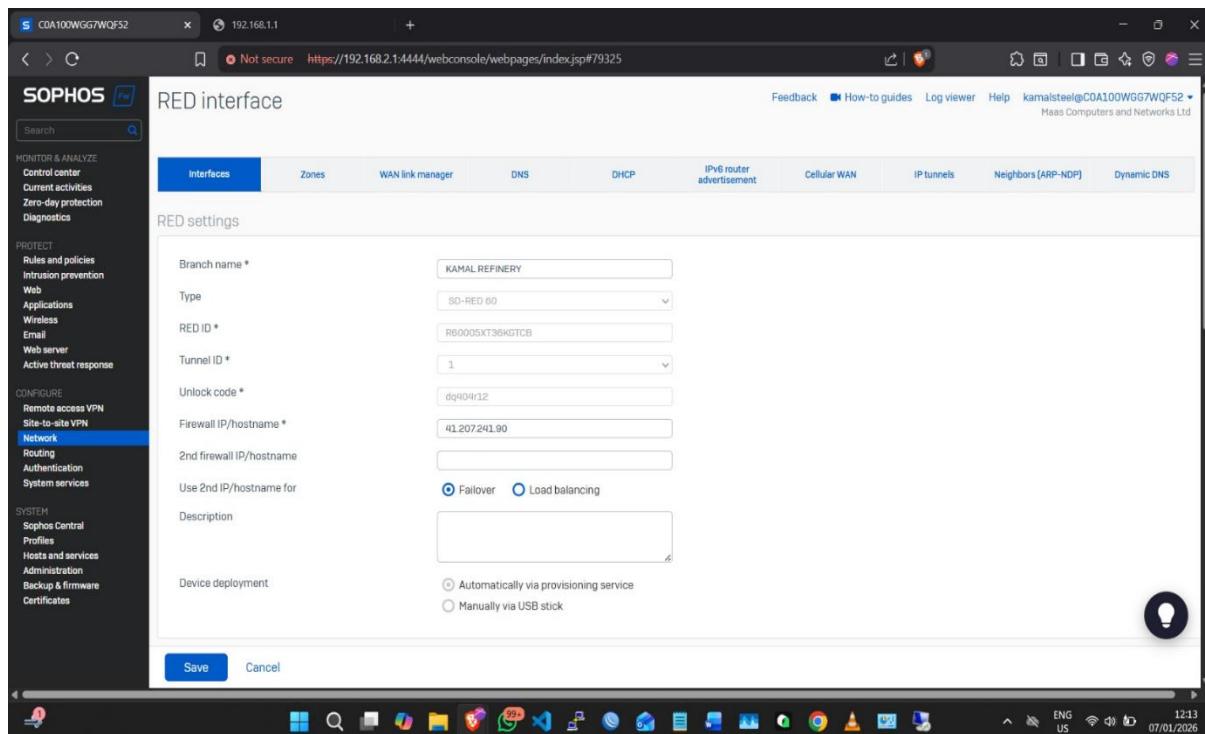


figure 1.0: shows RED settings

## Network settings

### Uplink Settings

**Connection Type: DHCP**



## RED Network settings

RED IP :192.168.100.1

RED operational mode: Standard

Remote IP assignment: DHCP

| Interface                           | Status/Interface speed     | IP address                              | Misc   | Usage |
|-------------------------------------|----------------------------|---|--|-------|
| KAMAL REFINERY<br>red<br>LAN<br>RED | Enabled<br>Auto-negotiated | 192.168.100.254/255.255.255.0<br>Static | Online From: 192.168.2.171<br>WAN1 Uplink IP: 192.168.2.171<br>WAN2 Uplink IP: 192.168.2.159 | 1     |

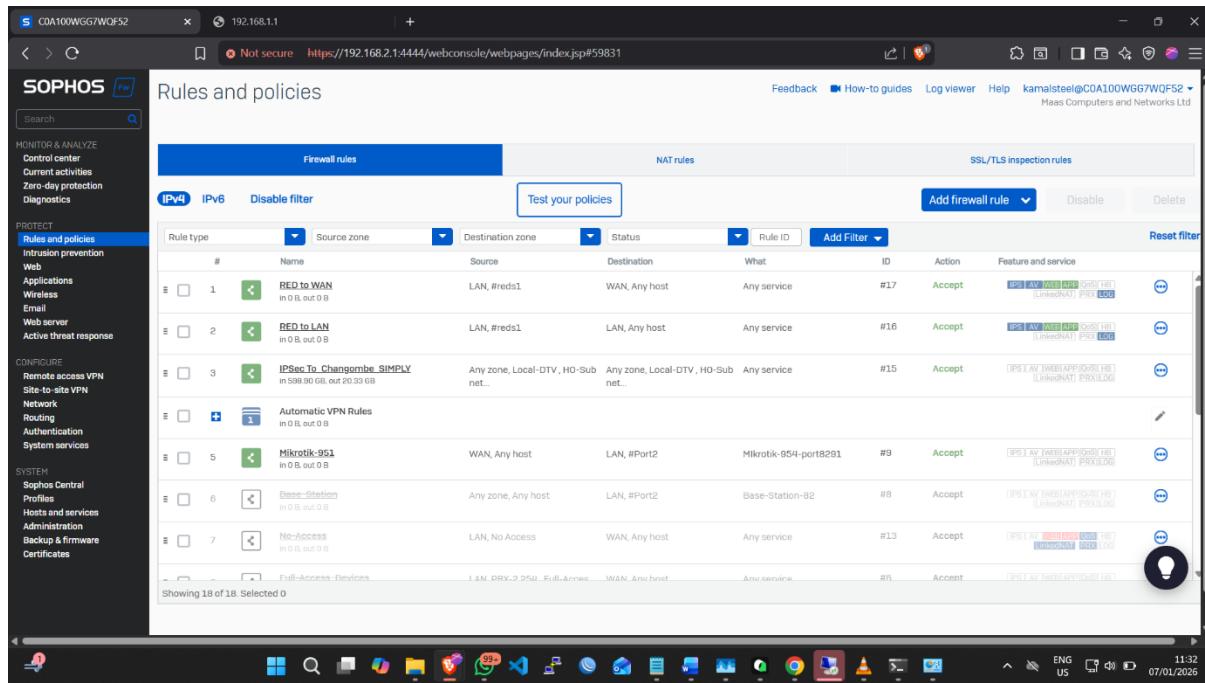
Figure 1.1: shows Network interface

| Leased IP     | Leased start time        | Leased end time          | Client physical address | Client hostname | Lease type |
|---------------|--------------------------|--------------------------|-------------------------|-----------------|------------|
| 192.168.100.1 | Wed 07 Jan 11:01:36 2026 | Thu 08 Jan 11:01:36 2026 | a8:91:62:15:3f:c5       | R60005XT36KGTCB | Dynamic    |
| 192.168.100.2 | Wed 07 Jan 11:03:12 2026 | Thu 08 Jan 11:03:12 2026 | 00:e0:4c:3e:39:90       | FNT-TECH-KEV1   | Dynamic    |
| 192.168.2.138 | Tue 06 Jan 13:18:42 2026 | Wed 07 Jan 13:18:42 2026 | a8:e2:91:e2:b4:24       | KSL-LG-VNM      | Dynamic    |
| 192.168.2.194 | Tue 06 Jan 13:30:50 2026 | Wed 07 Jan 13:30:50 2026 | 18:e7:77:f2:e9:27       | vwan-1820       | Dynamic    |

## Firewall Rules / Access Allowed

### Summary of RED Network Access

| Traffic Type              | Allowed?      | Notes                     |
|---------------------------|---------------|---------------------------|
| RED → Internet            | ✓ Allowed     | Via Rule #17 (Rule ID)    |
| RED → HQ LAN              | ✓ Allowed     | Via Rule #16 (Rule ID)    |
| HQ LAN → RED              | ✓ Allowed     | Returned traffic allowed  |
| RED → VPN sites           | ✓ Allowed     | If covered by IPsec rules |
| RED → Restricted Networks | ✗ Not Allowed | Unless explicitly defined |



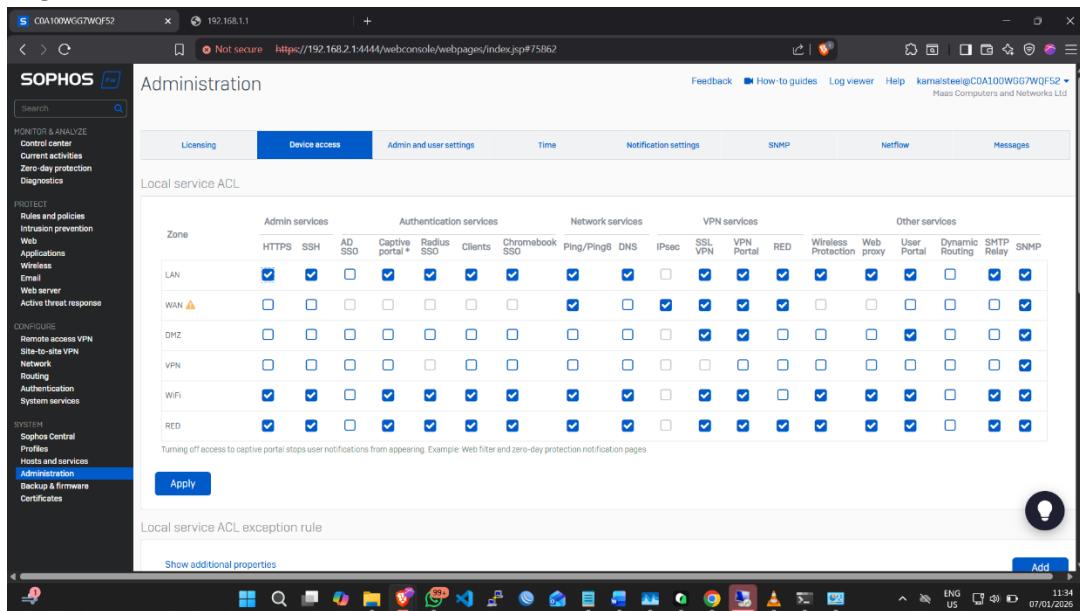
The screenshot shows the Sophos Firewall Rules and Policies interface. The left sidebar includes sections for MONITOR & ANALYZE, PROTECT (selected), and SYSTEM. The main content area displays a table of firewall rules:

| #  | Name   | Source                              | Destination                         | What                  | ID     | Action                                    | Feature and service                       |
|----|--|-------------------------------------|-------------------------------------|-----------------------|--------|---|---|
| 1  | RED to WAN<br>in 0.0.0.0 out 0.0.0.0                         | LAN, #red\$1                        | WAN, Any host                       | Any service           | #17    | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 2  | RED to LAN<br>in 0.0.0.0 out 0.0.0.0                         | LAN, #red\$1                        | LAN, Any host                       | Any service           | #16    | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 3  | IPSec To Changombe SIMPLY<br>in 598.90.0.0/8 out 20.33.0.0/8 | Any zone, Local-DTV , HO-Sub net... | Any zone, Local-DTV , HO-Sub net... | Any service           | #15    | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 4  | Automatic VPN Rules<br>in 0.0.0.0 out 0.0.0.0                |                                     |                                     |                       |        |   |   |
| 5  | Mikrotik-951<br>in 0.0.0.0 out 0.0.0.0                       | WAN, Any host                       | LAN, #Port2                         | Mikrotik-954-port8291 | #9     | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 6  | Base-Station<br>in 0.0.0.0 out 0.0.0.0                       | Any zone, Any host                  | LAN, #Port2                         | Base-Station-82       | #8     | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 7  | NoAccess<br>in 0.0.0.0 out 0.0.0.0                           | LAN, No Access                      | WAN, Any host                       | Any service           | #13    | Accept                                    | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |
| 8  | Full-Access_Devices<br>in 192.168.2.0/24 out 192.168.0.0/24  | WAN, Any host                       | Any service                         | #11                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 9  | Full-Access_WAN<br>in 0.0.0.0 out 0.0.0.0                    | WAN, Any host                       | Any service                         | #10                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 10 | Full-Access_LAN<br>in 0.0.0.0 out 0.0.0.0                    | LAN, Any host                       | Any service                         | #12                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 11 | Full-Access_Rules<br>in 0.0.0.0 out 0.0.0.0                  | WAN, Any host                       | Any service                         | #14                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 12 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #15                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 13 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #16                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 14 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #17                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 15 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #18                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 16 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #19                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 17 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #20                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |
| 18 | Full-Access_Services<br>in 0.0.0.0 out 0.0.0.0               | WAN, Any host                       | Any service                         | #21                   | Accept | IPS AV WEB APP (GWS) (B) [LinkNat] PROLOG |   |

figure 1.2: shows firewall rules

## Device Access Configuration

The device access configuration defines which services are accessible from specific network zones (e.g., LAN, WAN, Wi-Fi, VPN zones).

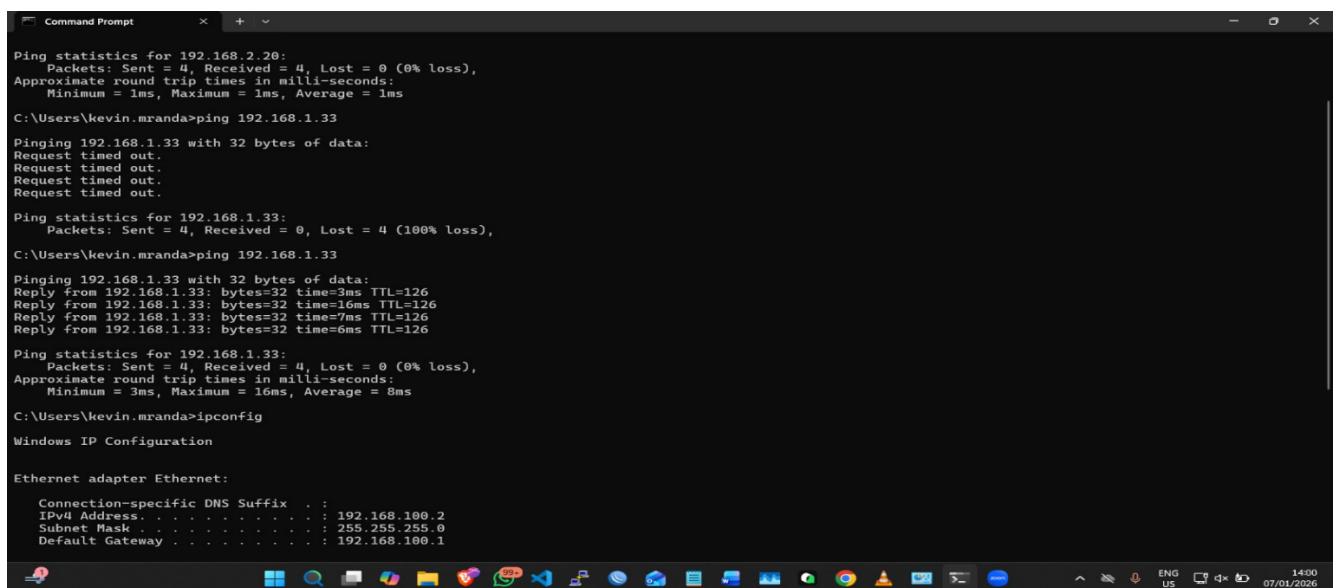


| Zone | Admin services                      |                                     |                          | Authentication services             |                                     |                                     | Network services                    |                                     |                                     | VPN services             |                                     |                                     | Other services                      |                                     |                                     |                                     |                                     |                                     |
|------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
|      | HTTPS                               | SSH                                 | AD SSO                   | Captive portal                      | Radius SSO                          | Clients                             | Chromebook SSO                      | Ping/Ping8                          | DNS                                 | IPSec                    | SSL VPN                             | VPN Portal                          | RED                                 | Wireless Protection                 | Web proxy                           | User Portal                         | Dynamic Routing                     | SMTP Relay                          |
| LAN  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| WAN  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| DMZ  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| VPN  | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/> | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            | <input type="checkbox"/>            |
| WiFi | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| RED  | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |

Figure 1.4: Device Access control interface showing enabled services for LAN, RED interface, and other zones.

## Connectivity Verification (Ping Test Results)

After completing the vRED 60 configuration and establishing the tunnel to the headquarters firewall, connectivity tests were performed to confirm successful communication on the network.



```

C:\Users\kevin.mranda>ping 192.168.2.20

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\kevin.mranda>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\kevin.mranda>ping 192.168.1.33

Pinging 192.168.1.33 with 32 bytes of data:
Reply from 192.168.1.33: bytes=32 time=3ms TTL=126
Reply from 192.168.1.33: bytes=32 time=16ms TTL=126
Reply from 192.168.1.33: bytes=32 time=7ms TTL=126
Reply from 192.168.1.33: bytes=32 time=6ms TTL=126

Ping statistics for 192.168.1.33:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 16ms, Average = 8ms

C:\Users\kevin.mranda>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet:
    Connection-specific DNS Suffix  . :
    IPv4 Address . . . . . : 192.168.100.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.100.1
  
```

figure 1.3: shows ping results



| Customer Support Contacts |  |
|---------------------------|--|
| Email                     | cs@flashnet.co.tz, support@flashnet.co.tz            |
| Call/WhatsApp             | +255 22 2113687 (Call), +255-777- 988-883 (WhatsApp) |