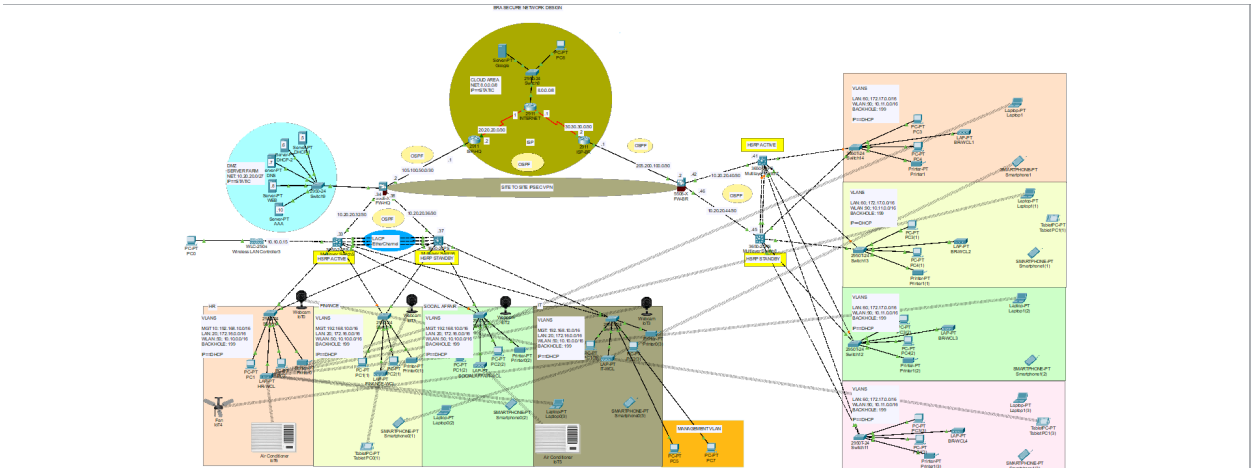
Secure IoT Network Architecture for BRA’s Future Safety Systems

1. Task Objectives

Develop a robust, scalable, and security-hardened network architecture that integrates thousands of distributed IoT
devices, local edge gateways, and cloud services, incorporating advanced security models, failover strategies, and
performance optimization techniques for smart safety and automation systems.

1. In this documentation , I am going to take you through the Network Topology below



	Configuration Steps
1	Netwok Design
2	Subnetting and IP addressing
3	Basic settings to all devices + SSH + Standard ACL for SSH
4	VLAN assignment plus all access and trunk ports on 12 and 13 switches.
	4.1. STP Portfast and BPDUguard configs on all access ports.
5	EtherChannel
6	Static IP address to DMZ/server farm devices.
7	DHCP server device configurations
8	HSRP and Inter-VLAN routing on the 13 switches plus ip dhcp helper addresses.
9	OSPF on the firewall, routers and switches.
10	Firewall interface security zones and levels
11	Firewall inspection policy configuration
12	Wireless network configurations
13	IPsec VPN on the Firewalls
14	AAA Using Tacas+
15	Verifying and testing configurations.

2. IP Addressing

Category	Network & SM	Valid Host Addresses	Default Gateway	Broadcat Address	USERS
WLAN	10.10.0.0/16 **(HQ)** 10.11.0.0/16 **(BR)**	10.10.0.1 - 10.10.255.254	10.10.0.1	10.10.255.254	VLAN FOR WIFI USERS
LAN	172.16.0.0/16 (HQ) 172.17.0.0/16 (BR)	192.168.0.1 - 192.168.255.254	192.168.0.1	192.168.255.254	VLAN FOR LAN VIA CABLES
Management	192.168.10.0/24	172.16.10.1 - 172.16.10.254	172.16.10.1	172.16.10.254	VLAN FOR IT DEPARTMENT
DMZ	10.20.20.0/27	10.20.20.1 - 10.20.20.30	10.20.20.1	10.20.20.30	SERVER FARM
IOT	172.22.0.0/25	172.22.0.1 - 172.23.255.254	172.22.0.1	172.23.255.255	VLAN FOR IOT

Between the Cloud, ISP, Firewall, Routers and Layer-3 Switch

No	Network Address
Cloud Area	8.0.0.0/8
HQ-ISP-Internet	20.20.20.0/30
Br-ISP-INTERNET	30.30.30.0/30
HQ-FWL-ISP	105.100.50.0/30
Br-FWL-ISP	205.200.100.0/30
HQ-FWL to MLSW1	10.20.20.32/30
HQ-FWL to MLSW2	10.20.20.36/30
BR-FWL to MLSW1	10.20.20.40/30
BR-FWL to MLSW2	10.20.20.44/30

3. Suricata (IDS) Installation and Custom Rules Configuration (local Machine (Kali Linux))

1. **Install Suricata**

..> sudo apt update && sudo apt install suricata -y (# Installation)
..> sudo nano /etc/suricata/suricata.yaml (# Configure IP, Interface, rule-file)
..> sudo nano /etc/suricata/rules/local.rules (# Add custom rules)

→ sudo suricata -T -c /etc/suricata/suricata.yaml (# Check configuration Error)
..> sudo systemctl start suricata.service
..> sudo systemctl status suricata.service
..> sudo suricata-update
..> tail -f /var/log/suricata/fast.logs (# This is where logs generated are kept)

```
vars:
  # more specific is better for alert accuracy and perform>
  address-groups:
    HOME_NET:   "[10.0.2.15/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"
```

1

```
default-rule-path: /var/lib/suricata/rules

rule-files:
  - suricata.rules
  - /etc/suricata/rules/local.rules
##
```

Custom rules

1

This shows that the yaml configuration is correct and has no errors.

```
┌──(kali㉿26487)-[/var/www/html]
└─$ sudo suricata -T -c /etc/suricata/suricata.yaml

i: suricata: This is Suricata version 7.0.7 RELEASE running in SYSTEM mode
i: suricata: Configuration provided was successfully loaded. Exiting.
```

Custom rules created

```
 GNU nano 8.0                    /etc/suricata/rules/local.rules *
alert ssh any any -> any any (msg:"[26487] SSH Login Failure Detected"; flow:established,to_server; threshold:>

alert tcp any any -> any any (msg:"[26487] Nmap SYN Scan Detected"; flags:S; ack:0; threshold:type limit, trac>

alert ssh any any -> any any (msg:"[26487] Brute Force Attack Detected"; flow:established,to_server; threshold>

<v:1; threshold:type limit, track by_src, count 5, seconds 10;)

alert ssh any any -> $HOME_NET any (msg:"[26487] SSH Brute Force Attack Detected"; flow:established,to_server;>
```

Testing how we may trigger the configured alerts (Nmap Syn scan , ssh bruetforcing, multiple fail

ssh login attempts)

```
┌──(kali㉿26487)-[~]
└─$ for i in {1..50}; do ssh kali@10.0.2.15 -p 26488; done
kali@10.0.2.15's password:
Permission denied, please try again.
kali@10.0.2.15's password:
Permission denied, please try again.
kali@10.0.2.15's password:
kali@10.0.2.15: Permission denied (publickey,password).
kali@10.0.2.15's password:
Permission denied, please try again.
kali@10.0.2.15's password:
```

Multiple login attempts

```
┌──(kali㉿26487)-[~]
└─$ nmap -sS 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-18 00:05 CAT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --sy
ify valid servers with --dns-servers
Nmap scan report for 10.0.2.15
Host is up (0.000024s latency).
All 1000 scanned ports on 10.0.2.15 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

We can check for logs

```
)] [Priority: 3] {TCP} 10.0.2.2:60072 -> 10.0.2.15:26488
11/17/2[redacted]3:25:23.187679  [**] [1:50026487:1] [26487] SSH Brute Force Attack Detected [**] [Classification: A
ttempte[redacted]r Privilege Gain] [Priority: 1] {TCP} 10.0.2.2:60072 -> 10.0.2.15:26488
11/17/2[redacted]3:25:24.291456  [**] [1:10026487:1] [26487] SSH Login Failure Detected [**] [Classification: (null)
] [Prio[redacted]3] {TCP} 10.0.2.2:[redacted]72 -> 10.0.2.15:26488
11/17/2[redacted]3:26:00.435367  [**] [1:50026487:1] [26487] SSH Brute Force Attack Detected [**] [Classification: A
ttempte[redacted]r Privilege Gain] [Priority: 1] {TCP} 10.0.2.2:60072 -> 10.0.2.15:26488
11/17/2[redacted]3:26:00.435367  [**] [1:10026487:1] [26487] SSH Login Failure Detected [**] [Classification: (null)
] [Prio[redacted]3] {TCP} 10.0.2.2:60072 -> 10.0.2.15:26488
11/17/2[redacted]3:26:11.179743  [**] [1:70026488:1] [26487] Nmap SYN Scan Detected [**] [Classification: (null)] [P
riority[redacted]{TCP} 10.0.2.2:60169 -> 10.0.2.15:26488
11/17/2[redacted]3:28:19.678211  [**] [1:50026487:1] [26487] SSH Brute Force Attack Detected [**] [Classification: A
ttempted User Privilege Gain] [Priority: 1] {TCP} 10.0.2.2:60169 -> 10.0.2.15:26488
```

3. Challenges

1. Time : this projects has limited time to accomplish everything within.
2. Resources intensive : This project required some advanced simulation softwares such as PnetLab, GNS3 so that i may utilize different tools and

technologies mentioned in project such as **SD-WAN, ZERO TRUST PRINCIPLE , NGFW , IOT Intergration** , **Zabbix f**or monitoring among many others