

# BLR

## Security & Health Status Report

Prepared by the Security Team

Date: -15/09/2023

\*\*\*\*\*

### 1. Fortinet1100E

- 1.1 CPU, Memory status
- 1.2 License details
- 1.3 HA status
- 1.4 Interface status

### 2. Distributed Denial-of-service (DDoS)

- 2.1 CPU, Memory and Current Connection status
- 2.2 Interface status
- 2.3 HA status
- 2.4 Attack status
- 2.5 License Status

### 3. Link Load Balancer (LLB)

- 3.1 CPU, Memory and Current Connection status
- 3.2 Interface status
- 3.3 HA status
- 3.4 License Status

### 4. Web Application Firewall (WAF)

- 4.1 CPU, Memory and Current Connection status
- 4.2 Interface status
- 4.3 HA status
- 4.4 License Status
- 4.5 Attack status

### 5. Server Load Balancer (SLB)

- 5.1 CPU and Memory and Current Connection status
- 5.2 Interface status
- 5.3 HA status
- 5.4 License Status

### 6. FireEye\_IA

- 6.1 Health status

### 7. FireEye\_PX

- 7.1 System view

### 8. Forti-Analyzer

- 8.1 System Information

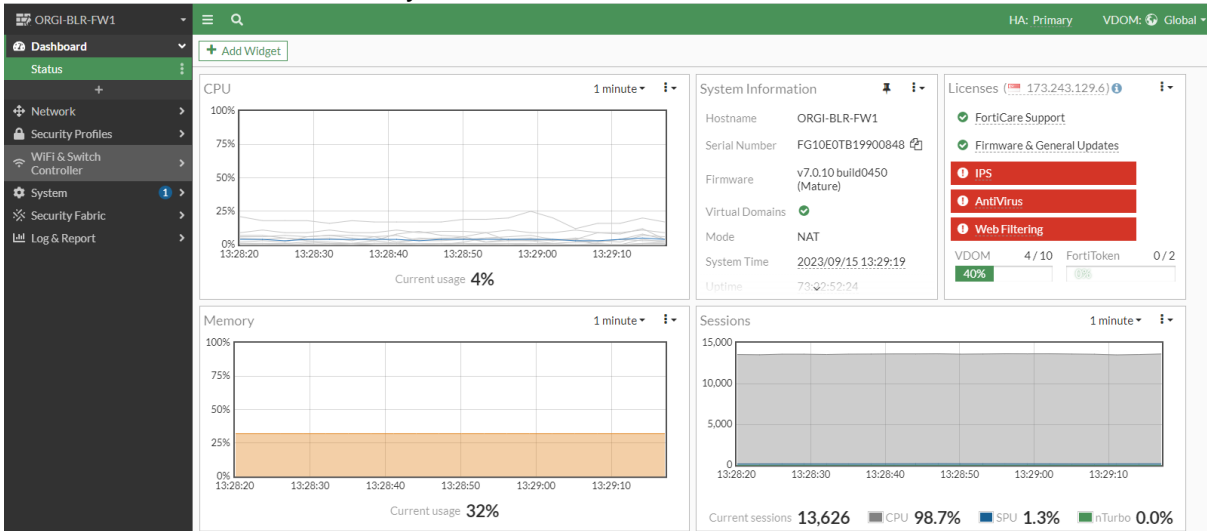
## Network Security Summary -15/09/2023

Device Parameter	Status	Remarks
Firewall CPU and Memory	CPU and Memory utilization is normal	Ok
Firewall License details		
Firewall HA Status	Both devices are in synced	Ok
Interface status	Connected Interfaces are up	Ok
DDOS CPU, Memory and Current Connection status	CPU and Memory is Normal	Ok
DDOS Interface Status	Connected Interfaces are up	
DDOS HA status	Both devices are in synced.	Ok
DDOS Attack status	Critical:0,High:0,Moderate:1,Low:0	Observe
DDOS License Status		Ok
LLB CPU, Memory and Current Connection status	CPU and Memory utilization is normal	Ok
LLB Interface Status	Connected Interfaces are up	
LLB HA status	Both devices are in synced	Ok
LLB License Status	Normal traffic	Ok
WAF CPU, Memory and Current Connection status	CPU and Memory utilization is normal	Ok
WAF Interface status	Connected Interfaces are up	
WAF HA status	Both devices are in synced	Ok
WAF License Status		
WAF attack status	Zero attacks	Ok
SLB CPU, Memory and Current Connection status	CPU and Memory utilization is normal	Ok
SLB Interface status	Connected Interfaces are up	
SLB HA status	Both devices are in synced	Ok
SLB License Status		
FireEye_IA	Health status	Ok
FireEye_PX	System view	Ok
8 Forti-Analyzer	System Information	Ok

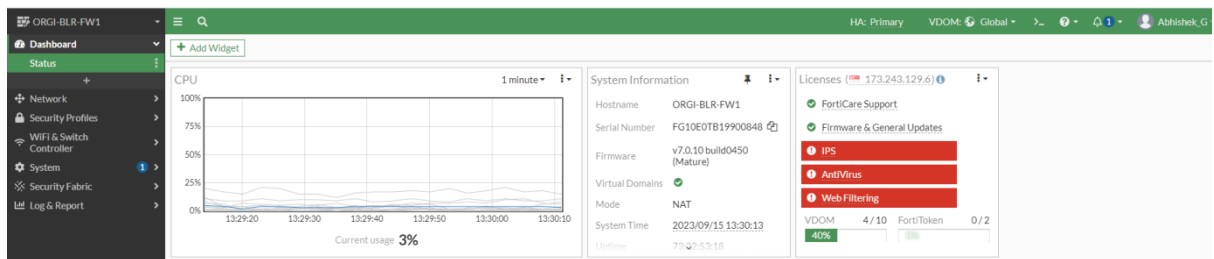
# 1 Fortinet 1100E

## 1.1 CPU and Memory status:

**Comment:** CPU and Memory utilization is normal

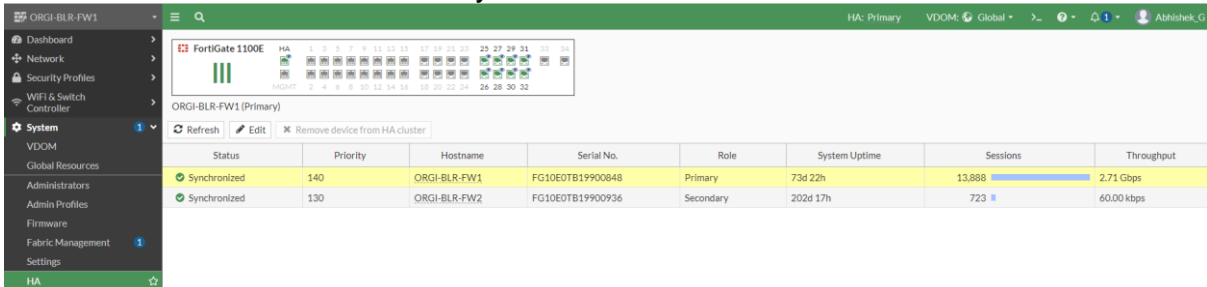


## 1.2 License details:



## 1.3 HA Status:

**Comment:** Both Devices are in Synced



## 1.4 Interfaces Status

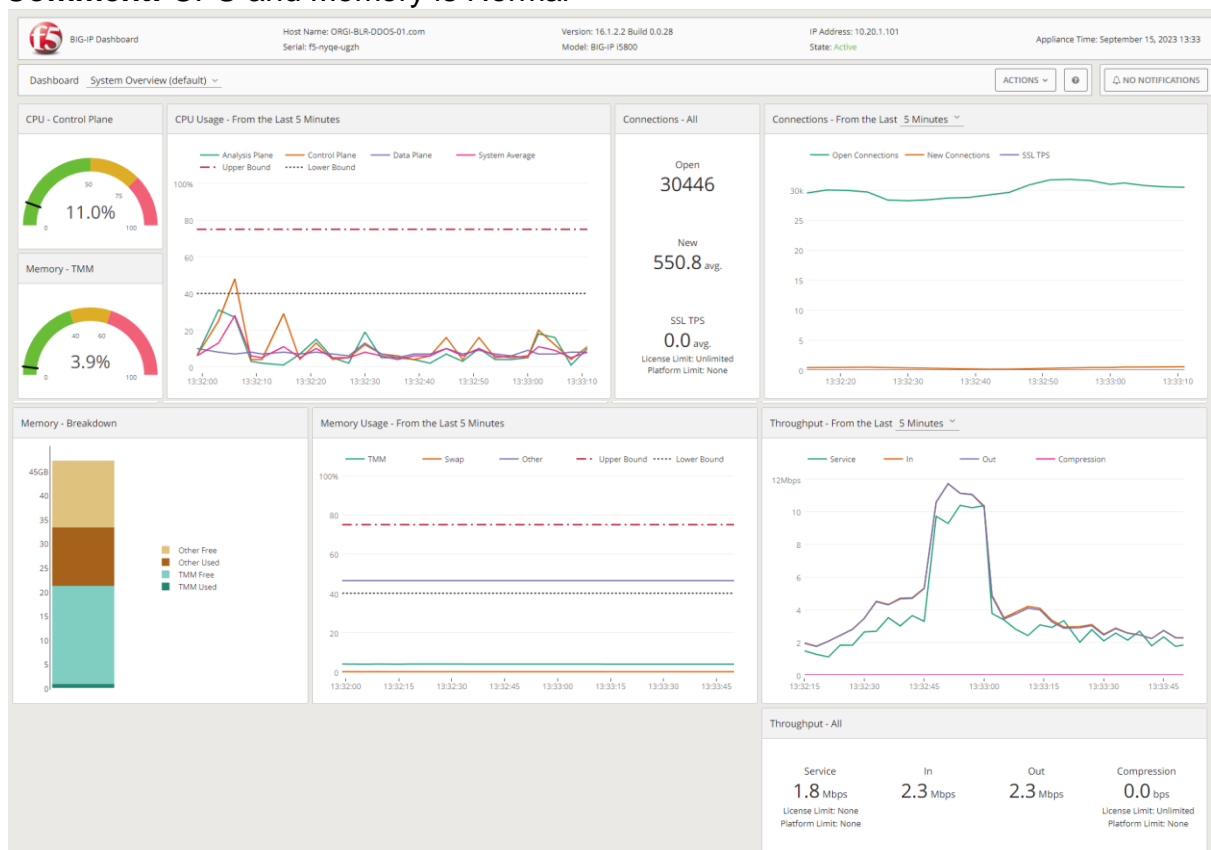
Comment: All Interfaces is up and working fine

Name	Type	Members	IP/Netmask	Transceiver(s)	Administrative Access	DHCP Clients	DHCP Ranges	Virtual Domain	Ref.
LACP_Core	802.3ad Aggregate	port32 port29 port30 port31	0.0.0.0/0.0.0.0	FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL	PING SNMP			root	23
LACP_WAN_SW	802.3ad Aggregate	port25 port26 port27 port28	0.0.0.0/0.0.0.0	FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL FINISAR CORP. FTUX8574D3BCL	PING SNMP			root	6

## 2 DDOS

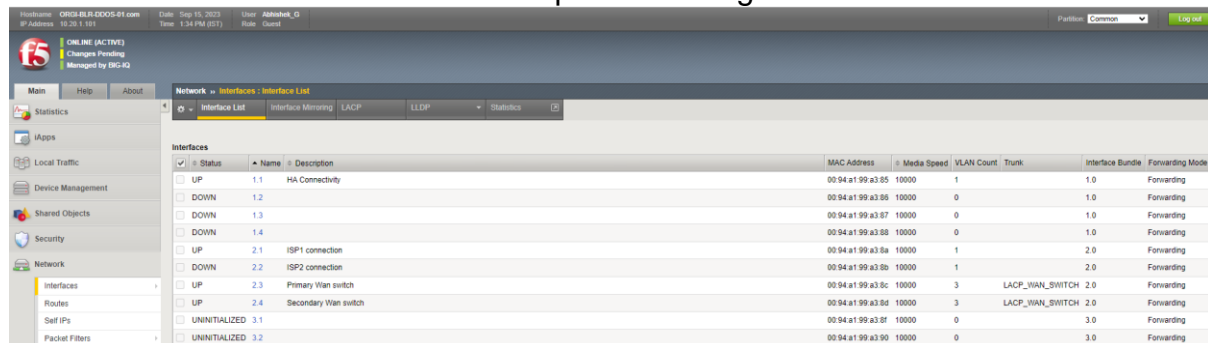
### 2.1 CPU and Memory Connections status:

Comment: CPU and Memory is Normal



## 2.2 Interface Status:

**Comment:** All connected interface is up and working fine.

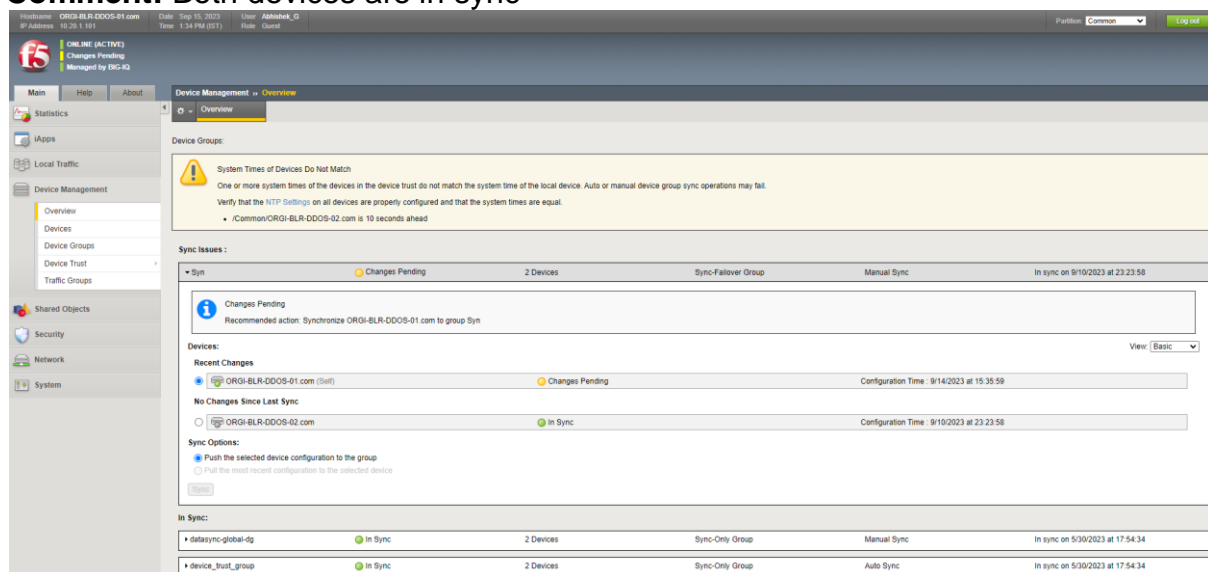


The screenshot shows the Mikrotik WinBox interface with the 'Interface List' tab selected. The table displays the status of various network interfaces.

Status	Name	Description	MAC Address	Media Speed	VLAN Count	Trunk	Interface Bundle	Forwarding Mode
UP	1.1	HA Connectivity	00:94:a1:99:a3:05	10000	1		1.0	Forwarding
DOWN	1.2		00:94:a1:99:a3:06	10000	0		1.0	Forwarding
DOWN	1.3		00:94:a1:99:a3:07	10000	0		1.0	Forwarding
DOWN	1.4		00:94:a1:99:a3:08	10000	0		1.0	Forwarding
UP	2.1	ISP1 connection	00:94:a1:99:a3:0a	10000	1		2.0	Forwarding
DOWN	2.2	ISP2 connection	00:94:a1:99:a3:0b	10000	1		2.0	Forwarding
UP	2.3	Primary Wan switch	00:94:a1:99:a3:0c	10000	3	LACP_WAN_SWITCH	2.0	Forwarding
UP	2.4	Secondary Wan switch	00:94:a1:99:a3:0d	10000	3	LACP_WAN_SWITCH	2.0	Forwarding
UNINITIALIZED	3.1		00:94:a1:99:a3:0f	10000	0		3.0	Forwarding
UNINITIALIZED	3.2		00:94:a1:99:a3:90	10000	0		3.0	Forwarding

## 2.3 HA Status:

**Comment:** Both devices are in sync



The screenshot shows the Mikrotik WinBox interface with the 'Device Management' > 'Overview' tab selected. It displays a warning about system times not matching and a table showing the sync status of two devices.

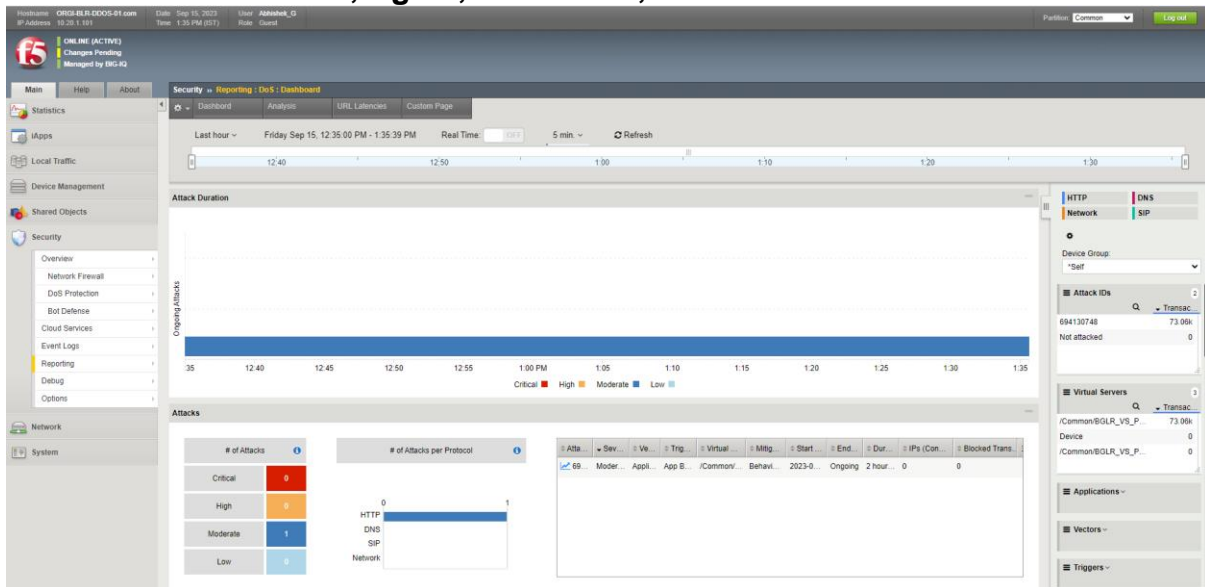
**System Times of Devices Do Not Match**  
One or more system times of the devices in the device trust do not match the system time of the local device. Auto or manual device group sync operations may fail.  
Verify that the [NTP Settings](#) on all devices are properly configured and that the system times are equal.  
• /Common/ORIGI-BLR-DDOS-02.com is 10 seconds ahead

**Sync Issues:**

Sync	Changes Pending	2 Devices	Sync-Failover Group	Manual Sync	In sync on 9/19/2023 at 23:23:58
<b>Changes Pending</b> Recommended action: Synchronize ORIGI-BLR-DDOS-01.com to group Sync					
<b>Devices:</b>					
<b>Recent Changes</b>					
ORIGI-BLR-DDOS-01.com (Self) Changes Pending Configuration Time: 9/14/2023 at 15:35:59					
<b>No Changes Since Last Sync</b>					
ORIGI-BLR-DDOS-02.com In Sync Configuration Time: 9/10/2023 at 23:23:58					
<b>Sync Options:</b>					
Push the selected device configuration to the group					
Pull the most recent configuration to the selected device					
<b>In Sync:</b>					
datasync-global-dg In Sync 2 Devices Sync-Only Group Manual Sync In sync on 5/30/2023 at 17:54:34					
device_trust_group In Sync 2 Devices Sync-Only Group Auto Sync In sync on 5/30/2023 at 17:54:34					

## 2.4 Attack status:

Comment: Critical:0,High:0,Moderate:1,Low:0



## 2.5 License status:

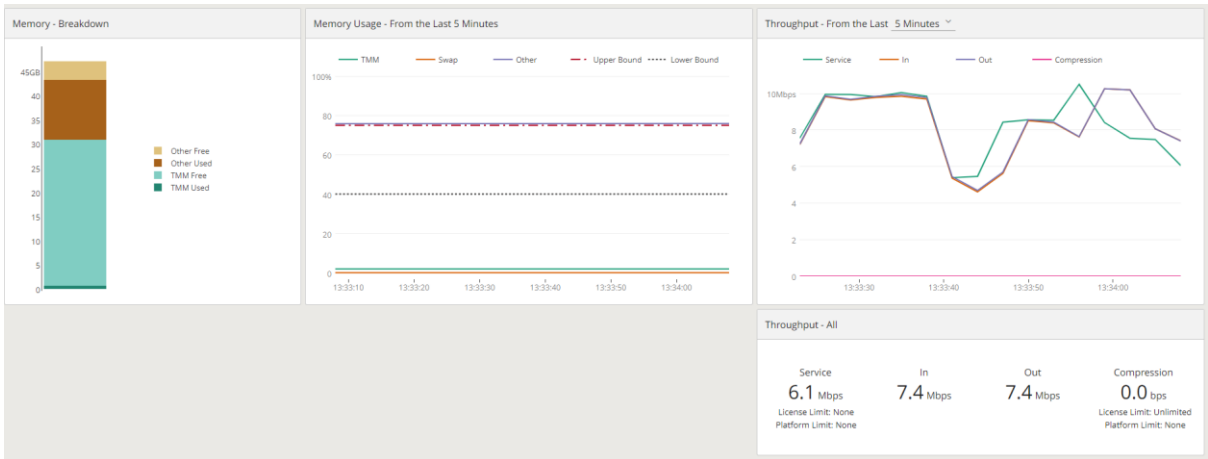
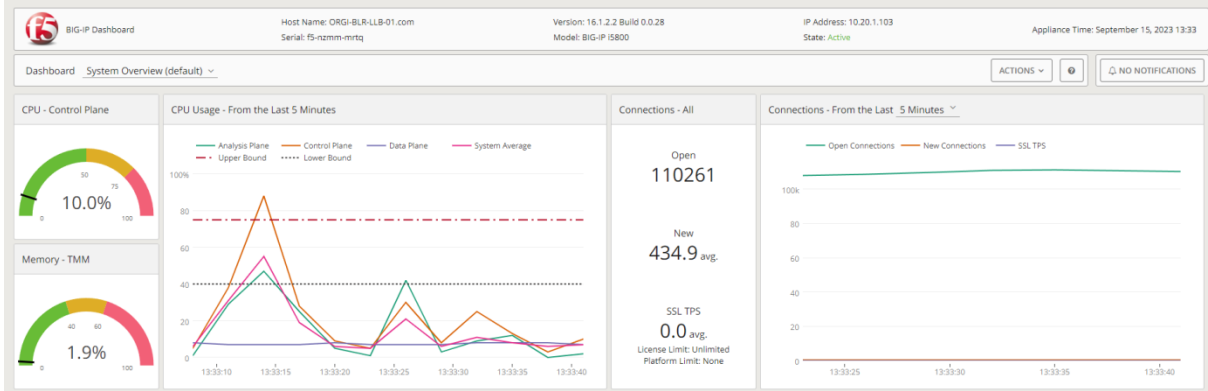
Comment: License is Ok

The screenshot displays the Fortinet System License page. The top status bar shows the system is ONLINE (ACTIVE) with changes pending, managed by RRG-2. The left sidebar contains navigation links for Main, Help, About, Statistics, Apps, Local Traffic, Device Management, Shared Objects, Security, and Network. The main content area is titled 'System - License' and includes tabs for Summary and Module Allocation. The 'General Properties' section shows the license type as Production, licensed on Sep 16, 2020, and the active modules as DDOS Hybrid Defender (5000/Perpetual) (LHEGOTN-XCESDWB). The 'Optional Modules' section shows IP Intelligence 1Yr and IP Intelligence 3Yr. The 'Inactive Modules' section is empty.

Property	Value
License Type	Production
Licensed Date	Sep 16, 2020
Active Modules	<ul style="list-style-type: none"><li>DDOS Hybrid Defender (5000/Perpetual) (LHEGOTN-XCESDWB)<ul style="list-style-type: none"><li>Rate Shaping</li><li>Max SSL: 5000</li><li>Routing Bundle</li><li>Max Compression: 5000</li></ul></li></ul>
Optional Modules	<ul style="list-style-type: none"><li>IP Intelligence 1Yr</li><li>IP Intelligence 3Yr</li><li>SN2 SWS SWS</li></ul>
Inactive Modules	

### 3 Link Load Balancer

#### 3.1 CPU, Memory and Current Connection



#### 3.2 Interface status

The Network configuration page displays the status of various network interfaces. The table below provides a detailed view of the interface list, including their status, names, descriptions, MAC addresses, media speeds, VLAN counts, and forwarding modes.

Interface	Status	Name	Description	MAC Address	Media Speed	VLAN Count	Trunk	Interface Bundle	Forwarding Mode
UP	1.1	HA Connectivity		00:94:a1:96:51:05	10000	1		1.0	Forwarding
DOWN	1.2			00:94:a1:96:51:06	10000	0		1.0	Forwarding
DOWN	1.3			00:94:a1:96:51:07	10000	0		1.0	Forwarding
DOWN	1.4			00:94:a1:96:51:08	10000	0		1.0	Forwarding
DOWN	2.1			00:94:a1:96:51:0a	10000	0		2.0	Forwarding
DOWN	2.2			00:94:a1:96:51:0b	10000	0		2.0	Forwarding
DOWN	2.3			00:94:a1:96:51:0c	10000	0		2.0	Forwarding
DOWN	2.4			00:94:a1:96:51:0d	10000	0		2.0	Forwarding
UP	3.1	Primary Wan switch		00:94:a1:96:51:0f	10000	7	LACP-WAN-SW	3.0	Forwarding
UP	3.2	Primary Wan switch		00:94:a1:96:51:10	10000	7	LACP-WAN-SW	3.0	Forwarding

### 3.3 HA status

Comment: Both Devices are in sync

Hostname: ORG-BLR-LLB-01.com  
IP Address: 10.20.1.103

Date: Sep 15, 2023  
Time: 1:34 PM (IST)

User: Abhinav\_K  
Role: Guest

Partition: Common

Log out

ONLINE (ACTIVE)  
In Sync  
Managed by BIG-IP2

MainHelpAbout

Statistics  
Apps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Overview  
Devices  
Device Groups  
Device Trust  
Traffic Groups

Shared Objects

Device Management - Overview

Overview

Device Groups

In Sync:

SYNCIn Sync2 DevicesSync-Follower GroupManual SyncIn sync on 8/17/2023 at 15:44:34

In Sync

All devices are in sync. There are no changes pending.

Devices:

ORG-BLR-LLB-01.com (Self)In SyncConfiguration Time : 8/17/2023 at 15:44:34

ORG-BLR-LLB-02.comIn SyncConfiguration Time : 8/17/2023 at 15:44:34

Sync Options:

No sync options are available.

device\_trust\_groupIn Sync2 DevicesSync-Only GroupAuto SyncIn sync on 3/9/2023 at 17:12:21

### 3.4 License Status

Comment-ok

Hostname: ORG-BLR-LLB-01.com  
IP Address: 10.20.1.103

Date: Sep 15, 2023  
Time: 1:35 PM (IST)

User: Abhinav\_K  
Role: Guest

Partition: Common

Log out

ONLINE (ACTIVE)  
In Sync  
Managed by BIG-IP2

MainHelpAbout

Statistics  
Apps  
DNS  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network  
System  
Configuration  
File Management  
Certificate Management  
Disk Management  
Software Management  
License  
Resource Provisioning  
Platform  
High Availability  
Services  
Preferences  
iFlow  
Crypto Offloading  
Users

System - License

SummaryModule Allocation

General Properties

License TypeProduction

Licensed DateJun 4, 2022

Active Modules

- BIG-IP: DNS (1K)(Perpetual) (HNNHSMO-PHOUTK)
  - DNSSEC
  - OTM Rate Falback: 1000
  - DNS Rate Falback: 1000
  - DNS Rate Limit: 1000 QPS
  - OTM Rate: 1000
- Local Traffic Manager: (5000)(Perpetual) (AELSOA-KIUFOUT)
  - Rate Shaping
  - DNSSEC
  - Max SSL: 5000
  - APM: Limited
  - OTM Rate Falback: 1000
  - DNS Rate Falback: 1000
  - DNS Rate Limit: 1000 QPS
  - OTM Rate: 1000
  - Max Compression: 5000
  - Anti-Virus Checks
  - Base Endpoint Security Checks
  - Firewall Checks
  - Network Access
  - Secure Virtual Keyboard
  - APM: Web Application
  - Machine Certificate Checks
  - Predicted Workspace
  - Remote Desktop
  - App Tunnel

- Access Policy Manager: Base, 500X
- Access Policy Manager: Max, 500X
- Advanced Firewall Manager: 500X
- Advanced Protocols
- Advanced Web Application Firewall: 500X
- Anti-Bot Module: 500X
- App Mode (TMSH Only, No RootBash)
- Application Security Manager: 500X
- ASM to sWAP Upgrade: 500X
- BIG-IP: DNS and OTM Upgrade (1K TO MAX)
- BIG-IP: Multicast Routing
- BIG-IP: Privileged User Access: 100 Endpoints
- BIG-IP: Privileged User Access: 1000 Endpoints
- BIG-IP: Privileged User Access: 250 Endpoints
- BIG-IP: Privileged User Access: 50 Endpoints
- BIG-IP: Privileged User Access: 500 Endpoints
- SPDM: 500X





4.3 HA status

Comment: Both devices are in sync

Host Name: ORG1-BLR-WAF-01.com  
IP Address: 10.20.1.105

Date: Sep 16, 2023  
Time: 1:42 PM (IST)

User: Admin@bls\_01  
Role: Guest

Partition: Common

Log out

fs

CHLINE (ACTIVE)  
In Sync

MainHelpAbout

Statistics  
Apps  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network

Device Management Overview

Overview

Device Groups

Devices

Device Groups

Device Trust

Traffic Groups

Device Groups

In Sync:

data-sync-global-dg	In Sync	2 Devices	Sync-Only Group	Manual Sync	In sync on 7/14/2023 at 17:12:47
device-group-failover-502c1813aa39	In Sync	2 Devices	Sync-Failover Group	Manual Sync	In sync on 8/31/2023 at 17:12:30
<div>In Sync All devices are in sync. There are no changes pending.</div>					
Devices:					
ORG1-BLR-WAF-01.com (Self)	In Sync	Configuration Time: 8/31/2023 at 17:12:30		View: Basic	
ORG1-BLR-WAF-02.com	In Sync	Configuration Time: 8/31/2023 at 17:12:30			
Sync Options: No sync options are available.					
device_trust_group	In Sync	2 Devices	Sync-Only Group	Auto Sync	In sync on 7/14/2023 at 17:12:47

4.4 License Status

Host Name: ORG1-BLR-WAF-01.com  
IP Address: 10.20.1.105

Date: Sep 16, 2023  
Time: 1:43 PM (IST)

User: Admin@bls\_01  
Role: Guest

Partition: Common

Log out

fs

CHLINE (ACTIVE)  
In Sync

MainHelpAbout

Statistics  
Apps  
Local Traffic  
Acceleration  
Device Management  
Shared Objects  
Security  
Network  
System

System License

Summary

Module Allocation

General Properties

License Type	Production
Licensed Date	Sep 16, 2020
Active Modules	<ul style="list-style-type: none"><li>Advanced Web Application Firewall, 65000/Perpetual (VOJYOUS-BEXMNZF)<ul style="list-style-type: none"><li>Rate Shaping</li><li>Max SSL, 6500</li><li>Max Compression, 6500</li></ul></li><li>Anti-Bot Module, 65000/Perpetual (SVRNHYBN-BKRALRZ)</li></ul>
Optional Modules	<ul style="list-style-type: none"><li>Access Policy Manager, Base, 6500X</li><li>Access Policy Manager, Max, 6500X</li><li>Advanced Firewall Manager, 6500X</li><li>Advanced Protocols</li><li>APM-2500, 6500X</li><li>App Mode (TASD Only), No Root/Bash</li><li>Big-IP, DNS, 1K</li><li>Big-IP, DNS, Max</li><li>Big-IP, Multicast Routing</li><li>DNS Services</li><li>External Interface and Network HSM</li><li>FIX Low Latency</li><li>IP Intelligence, 1Y</li><li>IP Intelligence, 3Y</li><li>LTM + SSL, 6500X</li><li>LTM, 6500X</li><li>Routing Bundle</li><li>SD-WAN, 10M4</li><li>SSL Orchestrator, 5000/7000/6500/7000</li><li>SSL, Forward Proxy</li><li>SSL, Forward Proxy, 5000/7000/6500/7000</li><li>Threat Campaigns, 1Y</li><li>Threat Campaigns, 3Y</li><li>URL Filtering, 1Y</li><li>URL Filtering, 1Y</li><li>VPN Users</li></ul>
Inactive Modules	

4.5 Attack status

Comment: No attacks

fs

BIG-IP Dashboard

Host Name: ORG1-BLR-WAF-01.com  
Serial: FS-K00-qatv

Version: 16.1.2.2 Build 0.0.28  
Model: BIG-IP 5800

IP Address: 10.20.1.105  
State: Active

Appliance Time: September 15, 2023 13:44

DashboardBehavioral DoS

Actions

0

NO NOTIFICATIONS

Behavioral DoS - From last 5 Minutes

Protected Applications

Virtual ServerProfileAttacksStatus

No entries to display.

Detected Attacks

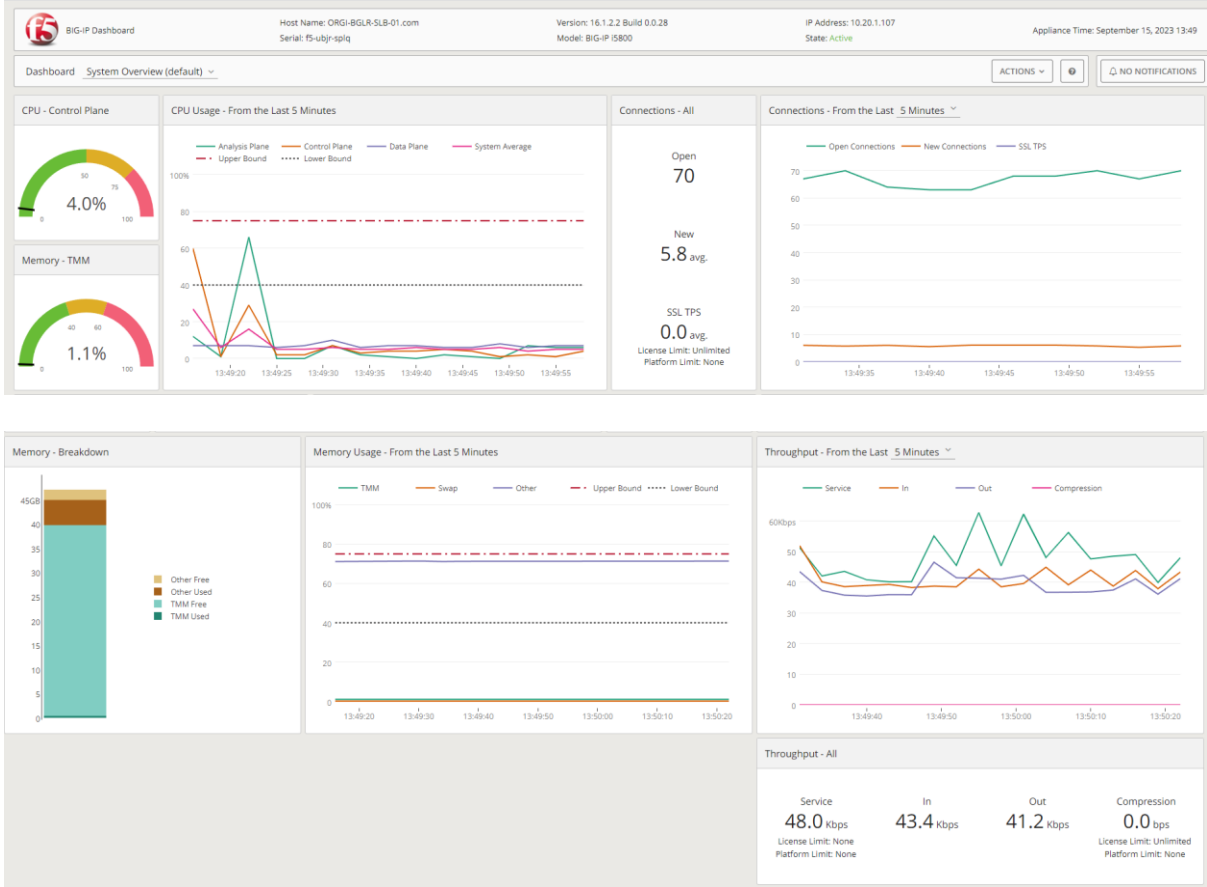
Attack IdStart TimeEnd TimeDuration

Select a Virtual Server to view attacks details

## 5 Server Load Balancer (SLB)

### 5.1 CPU and Memory and Current Connection status

Comment: CPU and Memory utilization is normal



### 5.2 Interface status

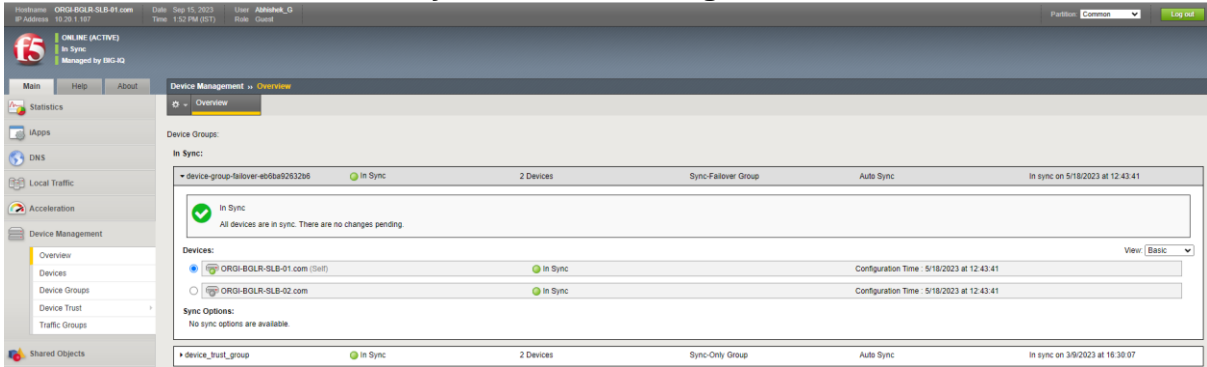
Comment:

The screenshot shows the 'Interface List' configuration page in the BIG-IP management console. It displays a table of network interfaces with their status, names, descriptions, MAC addresses, media speeds, VLAN counts, and forwarding modes.

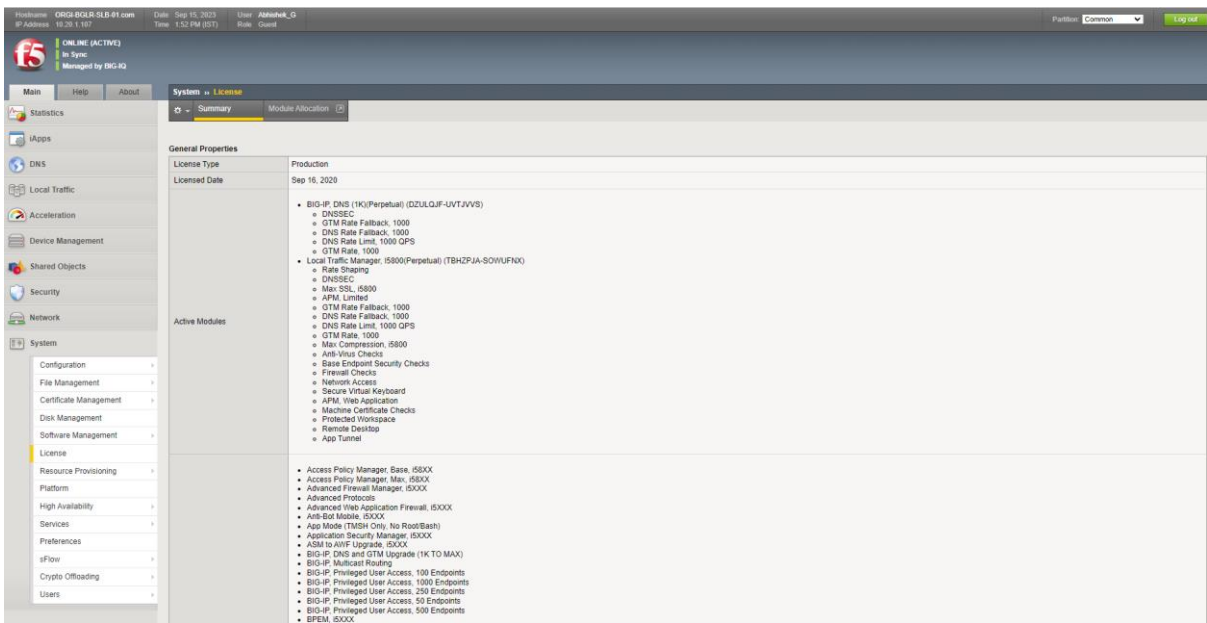
Status	Name	Description	MAC Address	Media Speed	VLAN Count	Trunk	Interface Bundle	Forwarding Mode
UP	1.1	HA Connectivity	00:94:a1:99:a0:05	10000	1		1.0	Forwarding
UNPOPULATED	1.2		00:94:a1:99:a0:06	10000	0		1.0	Forwarding
UNPOPULATED	1.3		00:94:a1:99:a0:07	10000	0		1.0	Forwarding
UNPOPULATED	1.4		00:94:a1:99:a0:08	10000	0		1.0	Forwarding
UP	2.1	Trunk port connected to core switch	00:94:a1:99:a0:0a	10000	4	SLB_LACP	2.0	Forwarding
UP	2.2	Trunk port connected to core switch	00:94:a1:99:a0:0b	10000	4	SLB_LACP	2.0	Forwarding
UNPOPULATED	2.3		00:94:a1:99:a0:0c	10000	0		2.0	Forwarding
UNPOPULATED	2.4		00:94:a1:99:a0:0d	10000	0		2.0	Forwarding
UNINITIALIZED	3.1		00:94:a1:99:a0:0f	10000	0		3.0	Forwarding
UNINITIALIZED	3.2		00:94:a1:99:a0:10	10000	0		3.0	Forwarding

### 5.3 HA status

Comment: Both devices in synced and working fine



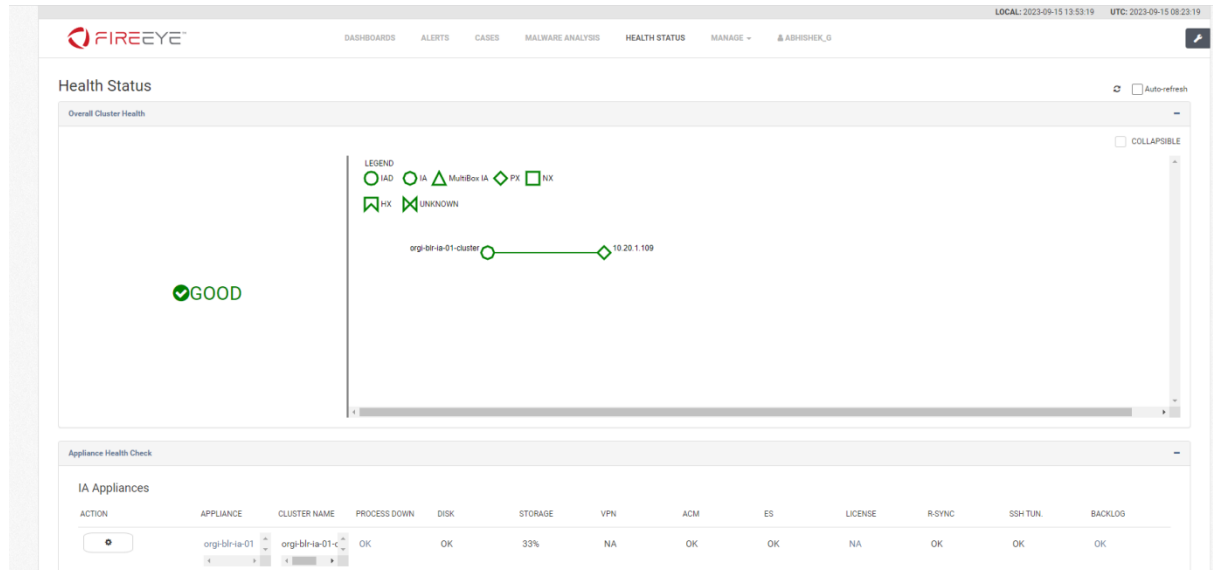
### 5.4 License Status



## 6.FireEye\_IA:-

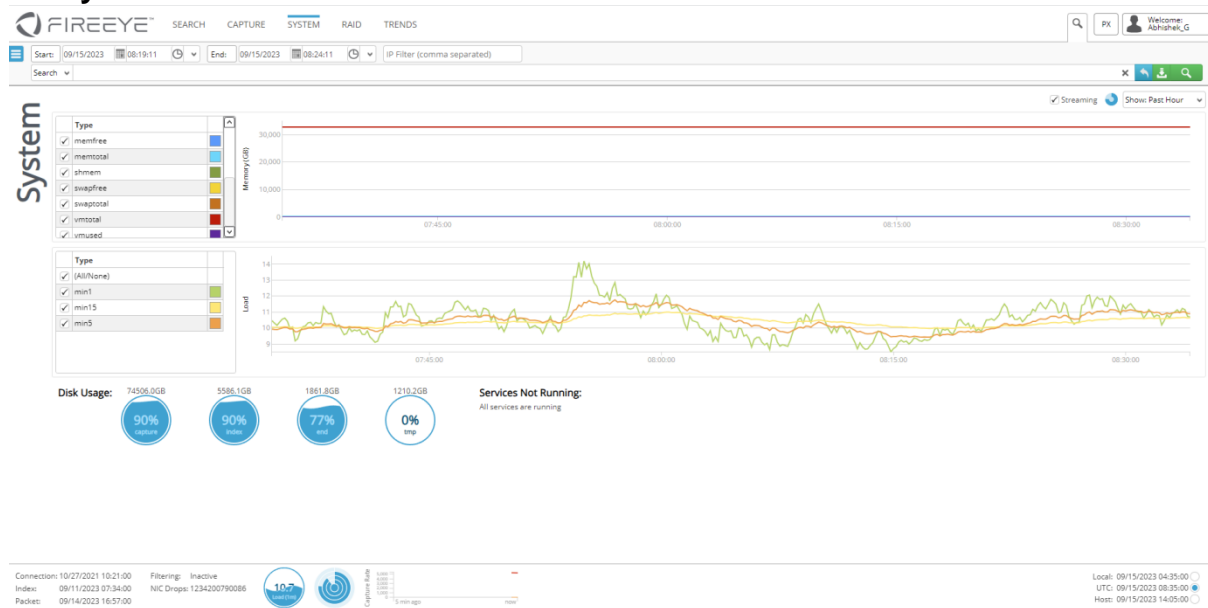
### 6.1:-

### Comment - Health Status Ok



## 7 FireEye\_PX:-

### 7.1 System view -



## 8. Forti-Analyzer

### 8.1 System Information

