PROJECT REPORT
NETWORK MANAGEMENT
BCN3023
SEM 2 2022/2023

TITLE : FLOWMON NETWORK MONITORING

LECTURER NAME : DR SURAYA BINTI ABU BAKAR
DATE OF SUBMISSION : 19 MAY 2023

PREPARED BY:

NAME	MATRIX ID
MUHAMMAD AFIQ BIN SHAMSUDIN	**CA21083**
MUHAMMAD NUR AIMAN BIN ALI	**CA21062**
AMYSHA SOFEA BINTI MD ROSLEE	**CA21071**

ABSTRACT

The rising complexity and volume of modern computer networks has forced the use of advanced network monitoring systems to assure optimal performance, security, and dependability. This abstract introduces FlowMon, a novel network monitoring project that provides extensive visibility and analysis of network traffic patterns. FlowMon, which uses advanced flow-based monitoring techniques, provides real-time monitoring, analysis, and reporting capabilities to provide network administrators with actionable insights for network optimisation, security enhancement, and troubleshooting.

FlowMon captures and processes network traffic data at rapid speeds by combining the power of deep packet inspection (DPI) with flow analysis. FlowMon identifies network irregularities, performance bottlenecks, and security concerns by collecting and analysing flow-level information such as source and destination IP addresses, ports, protocol types, and packet counts. The project classifies and categorises network flows using advanced algorithms and machine learning approaches, allowing administrators to get a granular understanding of network behaviour and take preventative measures.

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who have contributed to the successful completion of the FlowMon network monitoring project.

First and foremost, we extend our heartfelt appreciation to our project supervisor Dr. Suraya, whose guidance, expertise, and valuable insights were instrumental in shaping the project's direction and ensuring its successful execution. Their unwavering support, patience, and mentorship have been invaluable throughout the entire duration of this project.

We would also like to thank the entire project team for their dedication, hard work, and collaborative spirit. Each team member played a crucial role in the development, implementation, and testing phases, contributing their unique skills and expertise to achieve the project's goals. Their commitment, professionalism, and teamwork were instrumental in overcoming challenges and delivering a high-quality solution.

TABLE OF CONTENTS

INTRODUCTION

Computer networks are critical in today's interconnected world for simplifying communication, data sharing, and commercial processes. As networks get more sophisticated and large, monitoring and analysing network traffic becomes increasingly vital to maintain optimal performance, security, and dependability. FlowMon is a revolutionary network monitoring project that provides extensive visibility and analysis of network traffic flows. FlowMon is designed to help network administrators understand and manage the massive amounts of data that traverse their networks. Traditional monitoring solutions frequently lack the ability to gather and analyse network traffic at high rates, resulting in limited visibility and the identification of network anomalies or security threats being delayed. Furthermore, the ever-changing nature of network technology, as well as the rise of sophisticated assaults, need the use of advanced monitoring systems that can adapt and deliver real-time insights. To address these issues, FlowMon employs innovative flow-based monitoring algorithms. FlowMon gives a comprehensive picture of network traffic patterns and behaviours by capturing and analysing flow-level information such as source and destination IP addresses, ports, protocol types, and packet counts. Administrators can use this to detect performance bottlenecks, security vulnerabilities, and anomalies in real time, allowing them to take proactive measures to optimise network operations and improve security.

SOFTWARE DESCRIPTION

FlowMon is a complete network monitoring programme that allows for real-time viewing, analysis, and reporting of network traffic flows. FlowMon provides precise and actionable insights into network performance, security, and resource utilization by utilizing advanced flow-based monitoring techniques, deep packet inspection (DPI), and intelligent anomaly detection. FlowMon's real-time traffic monitoring capability continuously monitors and analyses network traffic flows, allowing administrators to discover and respond to any issues and ensure optimal network performance. Additionally, the programme offers complete flow analysis capabilities, allowing administrators to obtain insights into application performance, resource utilization, and user behaviour. Administrators can discover bottlenecks, optimise network setups, and distribute resources effectively by evaluating precise flow-level information such as source and destination IP addresses, ports, protocols, and packet counts. FlowMon uses DPI technology, which allows for deep packet inspection and analysis of network traffic to detect specific programmes, protocols, or malware, hence improving security and facilitating network troubleshooting. Furthermore, FlowMon incorporates machine learning algorithms for intelligent anomaly identification, allowing administrators to discover anomalous traffic patterns associated with network assaults, strange behaviours, or performance degradation in real time. The programme also includes customisable reporting features, allowing administrators to generate thorough reports and visualisations based on network traffic data collected, helping data-driven decision-making and compliance requirements.
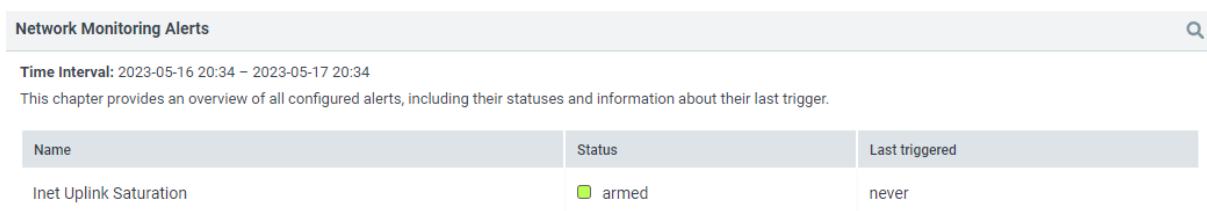
FCAPS ELEMENT

FAULT MANAGEMENT

To detect and monitor network faults and failures, FlowMon includes fault management functionalities. It provides real-time traffic monitoring and intelligent anomaly detection to discover and notify administrators of network issues such as connectivity issues, hardware failures, or service outages.

a) Network admin notification

The alerting component of Flowmon is extremely flexible, enabling you to alter the notifications you get and the channels through which they are sent. Additionally, you can configure alerts depending on predetermined criteria, such as when a particular threshold is reached or network equipment encounters a problem. The example of alerting in FlowMon via internet link utilization.

Figure shows that network monitoring alert

b) Fault detection

FlowMon actively monitors network activity and behaviour in order to spot errors or anomalies. It examines flow information, packet statistics, and performance indicators to spot any differences from the way the network should operate. Continuous network monitoring by FlowMon allows it to quickly identify and issue alerts for various fault types. Machine learning algorithms can be used by FlowMon to find irregularities in network traffic patterns. FlowMon may learn the typical patterns of network behaviour by continuously observing network traffic. It can then spot any variations that point to a problem or anomaly.

	QoS Type	AVG RTT	AVG SRT	AVG RTR	Maximal bits/s	Bits per second	Bytes
1	Best Effort	123.674 ms	119.964 ms	2.0	65.28 Mb/s	6.01 Mb/s	60.46 GiB
2	Others	43.26 ms	44.726 ms	0.1	2.07 Mb/s	133.20 Kb/s	1.34 GiB
3	Class Selector	216.533 ms	10.773 ms	0.0	126.91 Kb/s	7.11 Kb/s	73.22 MiB
4	Assured Forwarding	179.345 ms	10.014 ms	0.1	250.17 Kb/s	1.66 Kb/s	17.09 MiB
5	Expedited Forwarding	0 ms	0 ms	0	114.17 Kb/s	1.55 Kb/s	15.92 MiB
	All traffic	**123.905 ms**	**119.216 ms**	**2.0**	**65.33 Mb/s**	**6.15 Mb/s**	**61.90 GiB**

Figure shows network traffic

CONFIGURATION MANAGEMENT

FlowMon configuration management refers to the process of managing and maintaining the configuration settings and parameters of the FlowMon security management system. This includes setting up and configuring various components of FlowMon, such as network devices, sensors, flow collectors, and monitoring policies.

a) Collector Configuration

Configuring collectors, which are elements in charge of receiving and storing flow data gathered by the sensors in the FlowMon security monitoring system, is a component of managing FlowMon setup. Set up the collectors in the FlowMon system first. The name of the collector and its fundamental parameters are normally specified in this.
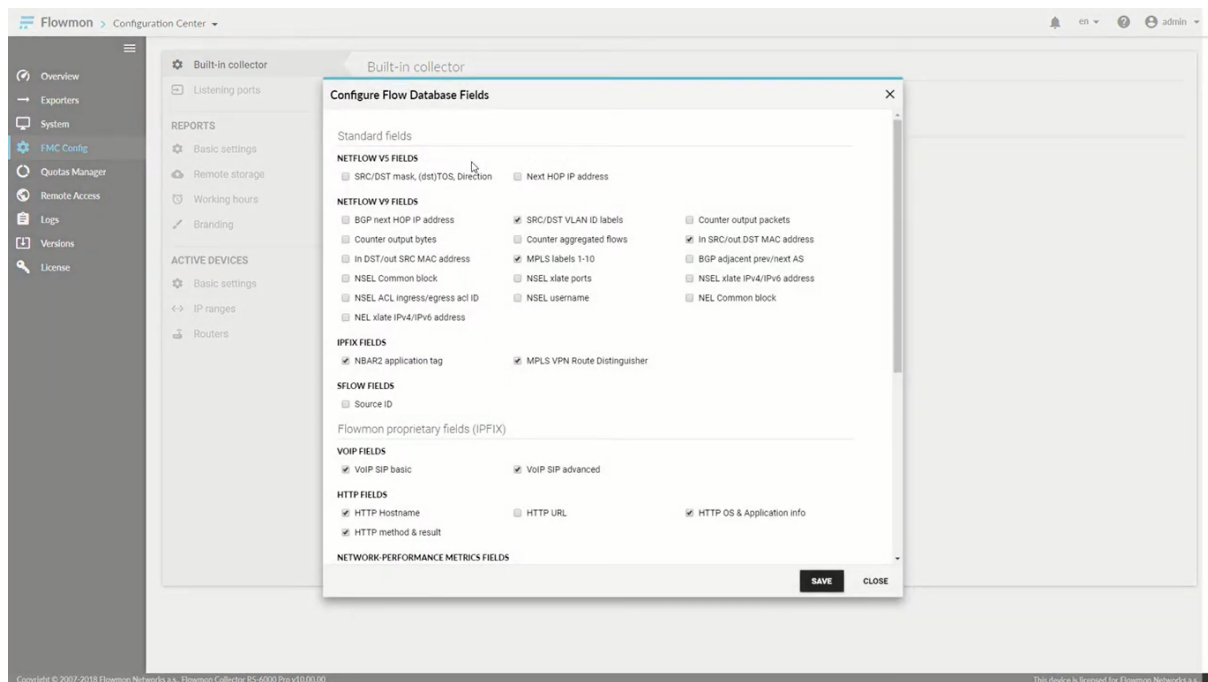
Figure shows database fields

b) User Configuration

User configuration, which involves controlling user accounts and the permissions attached to them within the FlowMon security management system, is a part of FlowMon configuration management. To begin, make user accounts for each person who will access and use FlowMon. Typically, this entails giving basic details like a login, password, and contact information. Depending on their duties and access needs, assign the proper roles to each

user account. FlowMon normally offers a variety of jobs, each with increasing levels of access and permissions, including administrator, operator, and viewer.
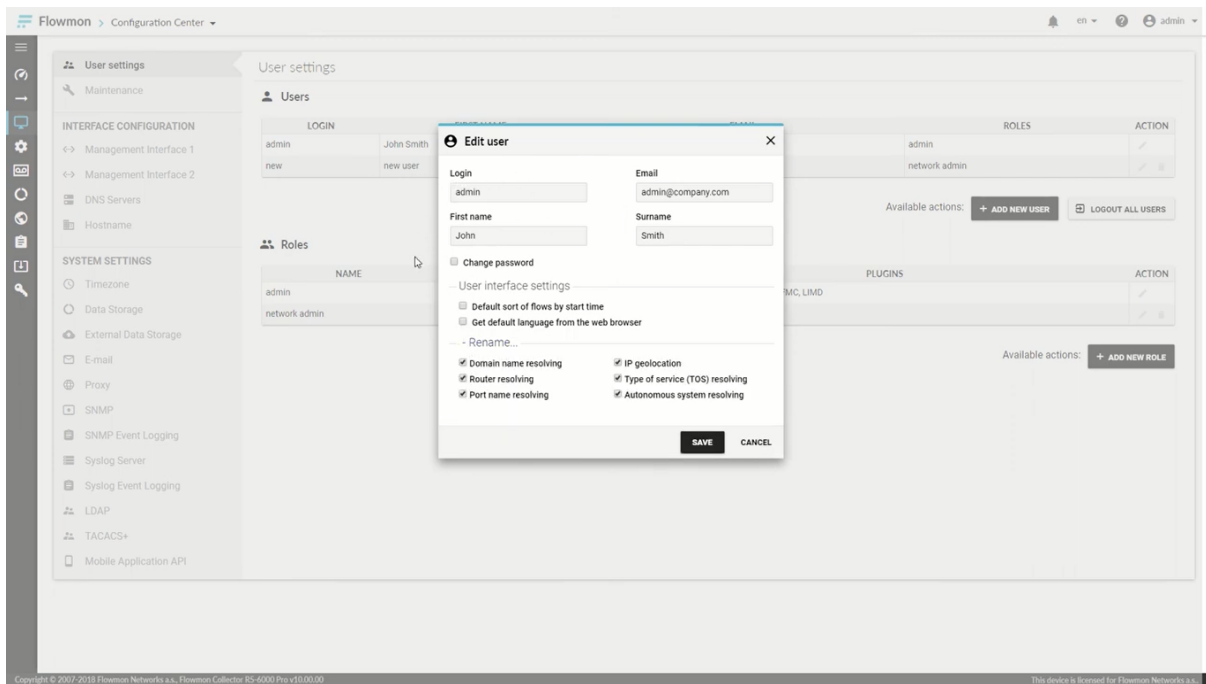
Figure shows edit user for configuration

ACCOUNTING MANAGEMENT

Flowmon offers solutions to every company's network difficulties that share the identical features but only vary in the monitoring requirements. There are two popular solution packages that Flowmon offers are Network Security and Monitoring Solution and the other one is Network Monitoring Solution.

a) Network Security and Monitoring Solution

This package emphasises robust network security capabilities as well as powerful monitoring features. Intelligent anomaly detection, deep packet inspection (DPI), threat identification, and mitigation are all included. Administrators may monitor and analyse network traffic flows in real time, discover security concerns, and take preventative measures to protect network infrastructure.

b) Network Monitoring Solution

This package is designed primarily for network monitoring requirements. It provides real-time visibility into network traffic flows, as well as performance monitoring and detailed flow analysis. Administrators may track network behaviour, detect bottlenecks in performance, optimise network configurations, and assure optimal network performance and availability.
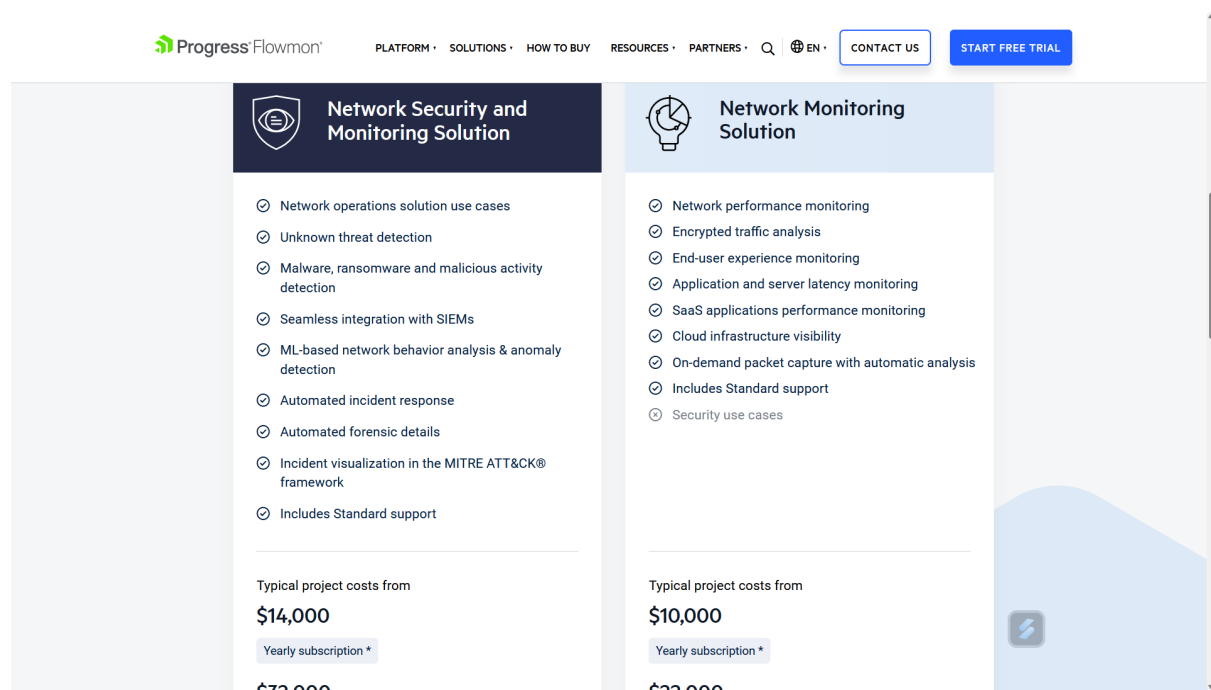
Figure show the comparison between the Flowmon packages

Figure shows the comparison between the Flowmon packages

PERFORMANCE MANAGEMENT

In Flowmon, performance management entails tracking, evaluating, and improving network performance to guarantee dependable and effective operation. It has a number of components that aid in evaluating and enhancing network performance. Administrators are given the ability to proactively monitor and improve network performance using Flowmon's performance management components. Flowmon aids in maintaining a high-performing network infrastructure by utilizing real-time data, examining traffic patterns, and generating performance insights.

a) Network performance monitoring

In order to provide real-time insights into network performance, Flowmon continuously monitors network traffic and performance. This makes it possible for network managers to spot potential performance problems right away and take appropriate action to enhance network performance. Administrators can monitor performance trends over time with Flowmon's thorough historical reports on network performance. Making decisions about network performance optimization can be done using this data to spot trends and future problems.
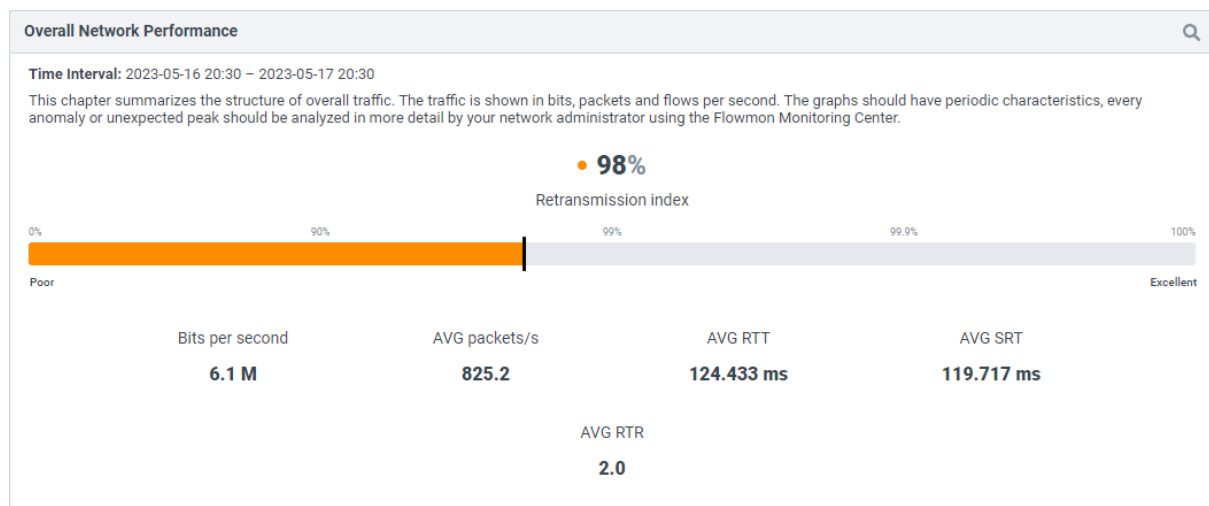
Figure shows overall network performance

b) Notifications to network admin about network degradation

Flowmon does more than just keep track of red and green statuses. You may get a complete insight into the performance of the entire digital environment by tracking how specific users interact with particular applications. With this all-encompassing strategy, you can quickly

determine what issues arise, which users and services are impacted, and who is in charge of fixing them.
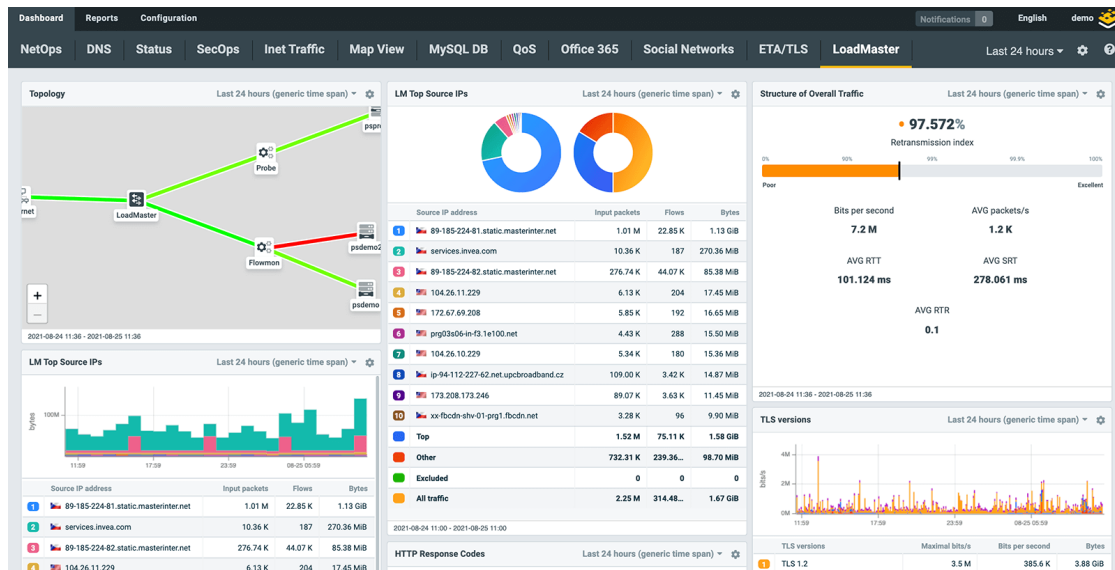
Figure shows about network degradation

SECURITY MANAGEMENT

Organisations may monitor and control their network traffic with the aid of FlowMon, a comprehensive security management system, in order to spot and address any potential security issues. It gives admins real-time visibility into network activity, allowing them to spot anomalies, suspicious activities, and security incidents.

FlowMon makes use of flow-based monitoring, which gathers and examines network traffic information such IP addresses, ports, protocols, and packet headers. FlowMon can analyse this data to identify a range of security problems, such as network intrusions, malware infections, DDoS attacks, and efforts at data exfiltration.

a) Threat detection and prevention

Using machine learning techniques, predetermined security rules, and real-time network flow analysis, FlowMon can spot and stop suspicious activity. It may identify unusual traffic patterns, well-known attack signatures, and behaviour suggestive of sophisticated persistent threats.Bypassing conventional security solutions, the Flowmon detection & response system enables Security Operation to find anomalies and early signs of compromise.

To find any concealed malicious actions, Flowmon uses the principles of machine learning and artificial intelligence (AI).
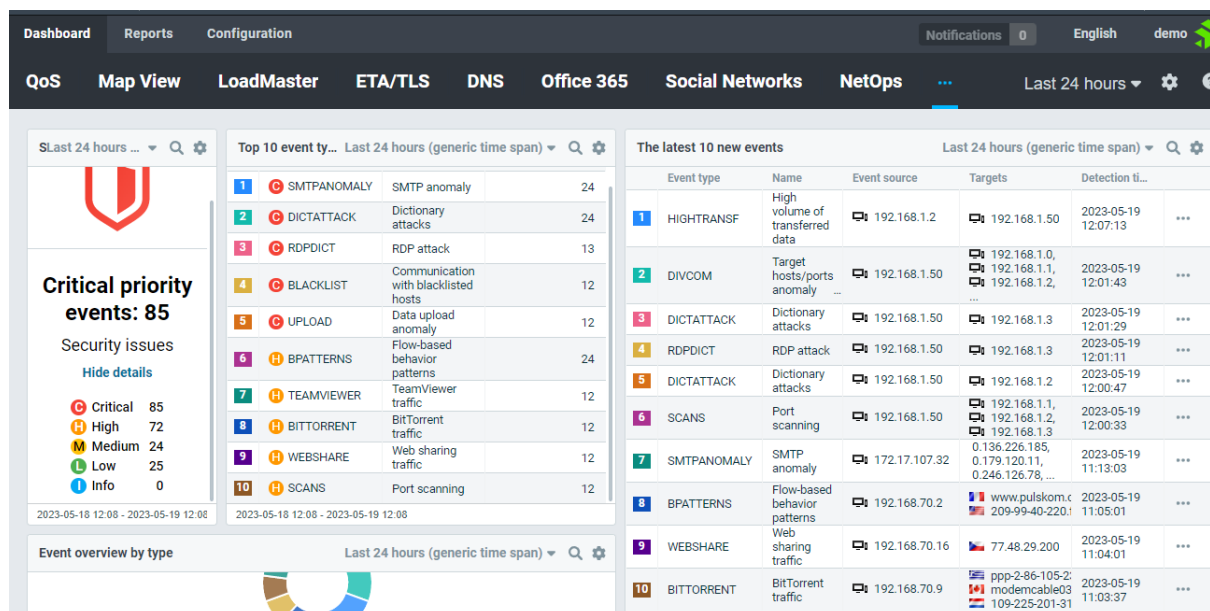
Figure shows threat detection

b) Network visibility and traffic analysis

In the event of a security incident, FlowMon gives comprehensive details about the attack, including its source, target, and effects. This aids security personnel in their investigation of and quick response to occurrences. For forensic investigations and compliance reporting, FlowMon also provides analysis of past data.The detection of events that are associated with specific anomalies and are categorized in accordance with the characteristics of network traffic that has been determined to be anomalous is demonstrated in the example below. Each event has a priority, and they are organized by category.
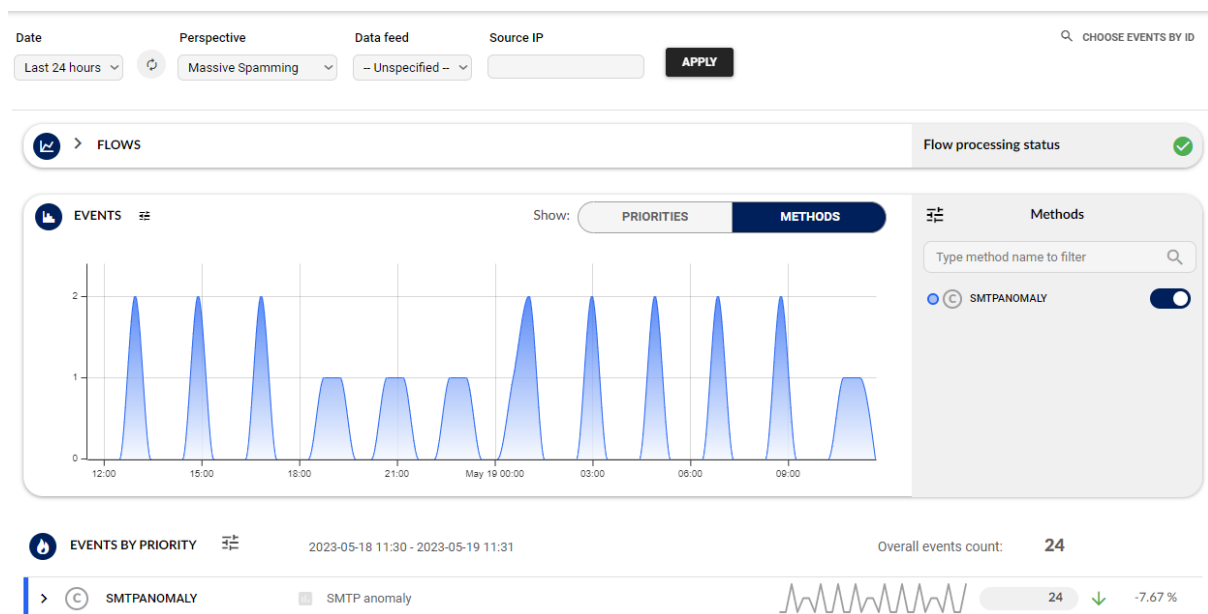
Figure shows incident response

With the help of Flowmon, businesses like manufacturers, financial institutions, and telecommunications providers can confidently manage and safeguard their computer networks.Administrators can keep an eye on user behavior, application usage, and bandwidth utilization with the help of FlowMon, which offers detailed visibility into network traffic. It aids in the detection of snags, performance optimization of the network, and detection of unauthorized or excessive usage of network resources. Network administrators, security engineers, and IT operations can use FlowMon's comprehensive suite of enterprise-class features for real-time network traffic visibility to find out who is utilizing the network and how.

SOFTWARE TESTING

The presets are presented by Flowmon Monitoring Center in the presets gallery, which provides a brief explanation of the use case and a sneak peek at the dashboard and widgets. Users can check the precise technical specifications of what the preset will configure if they so choose. There is also the option to do so.
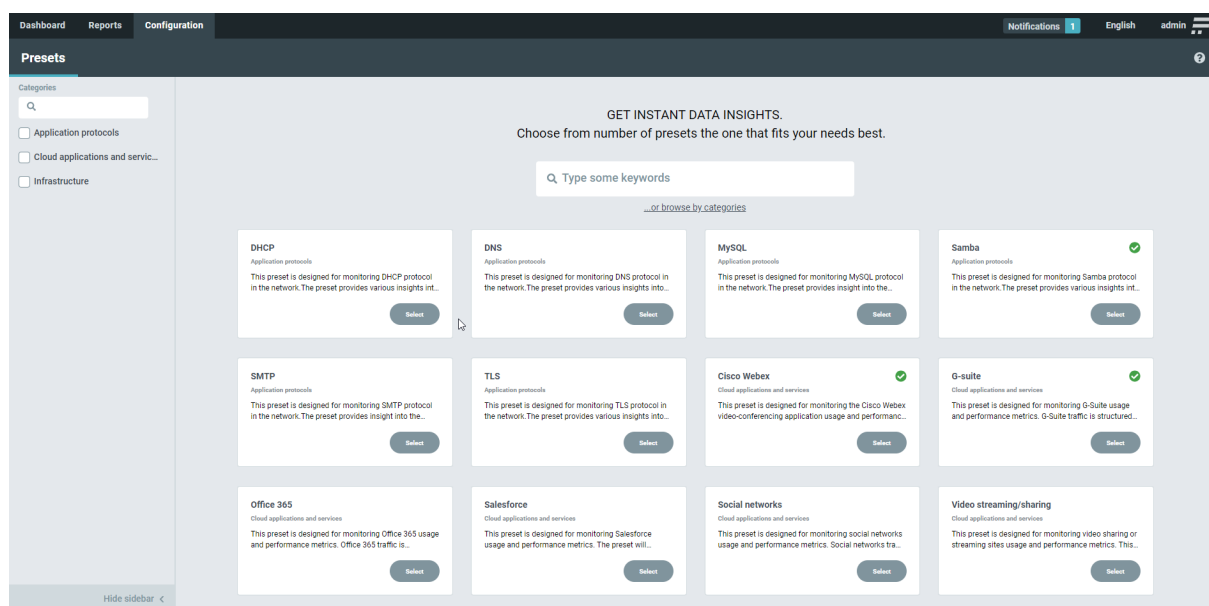
Figure shows presets in FlowMon configuration centre

The majority of users will undoubtedly want to keep an eye on their fundamental operations, which devices are connecting to the network, specifics of their connection, or incoming and outgoing email, even though there may not be a single universal configuration. They will select DNS, DHCP, SMTP, and Samba from the presets gallery to accomplish this.
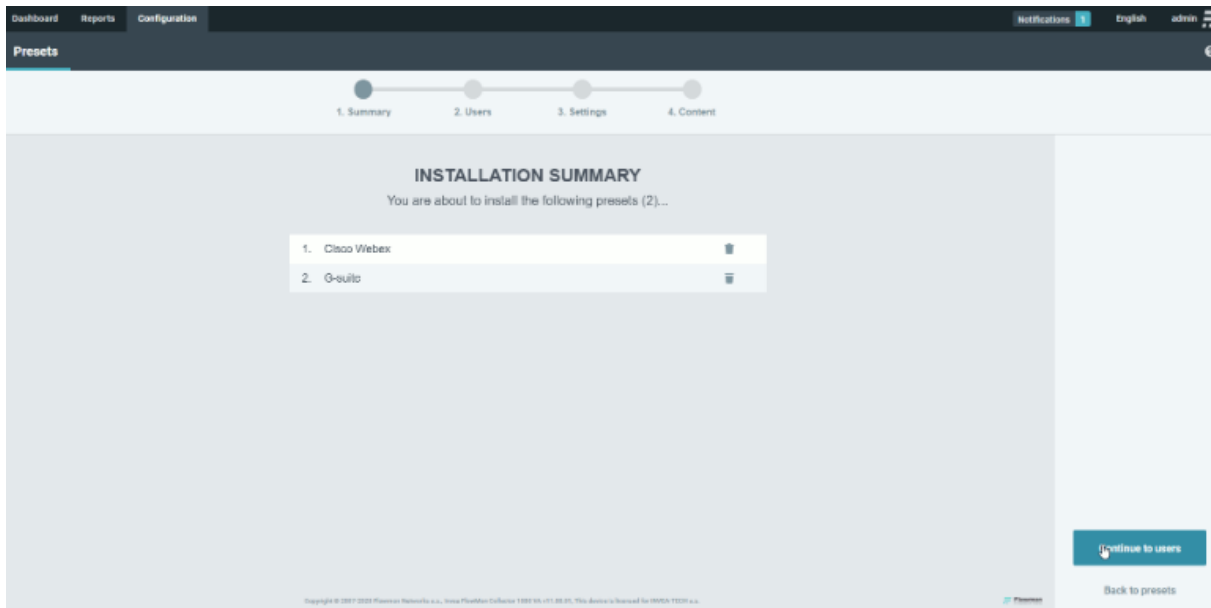
Figure shows where the user reviews and what presets are going to be applied
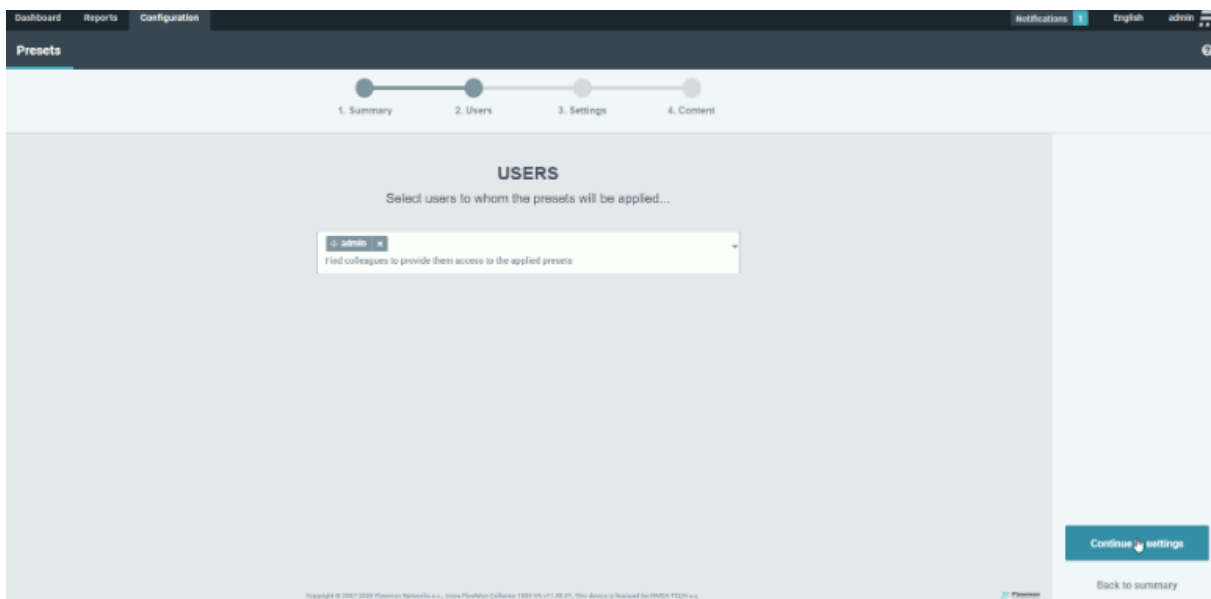
Figure shows which users the new configuration will involve
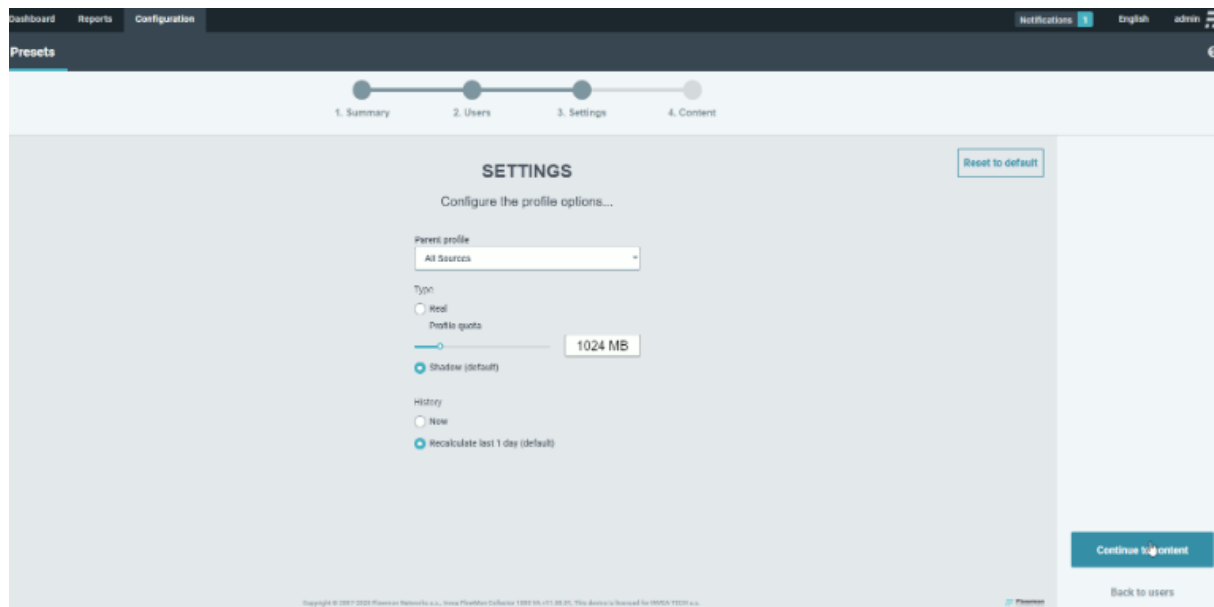
Figure shows where additional options about the profile can be set
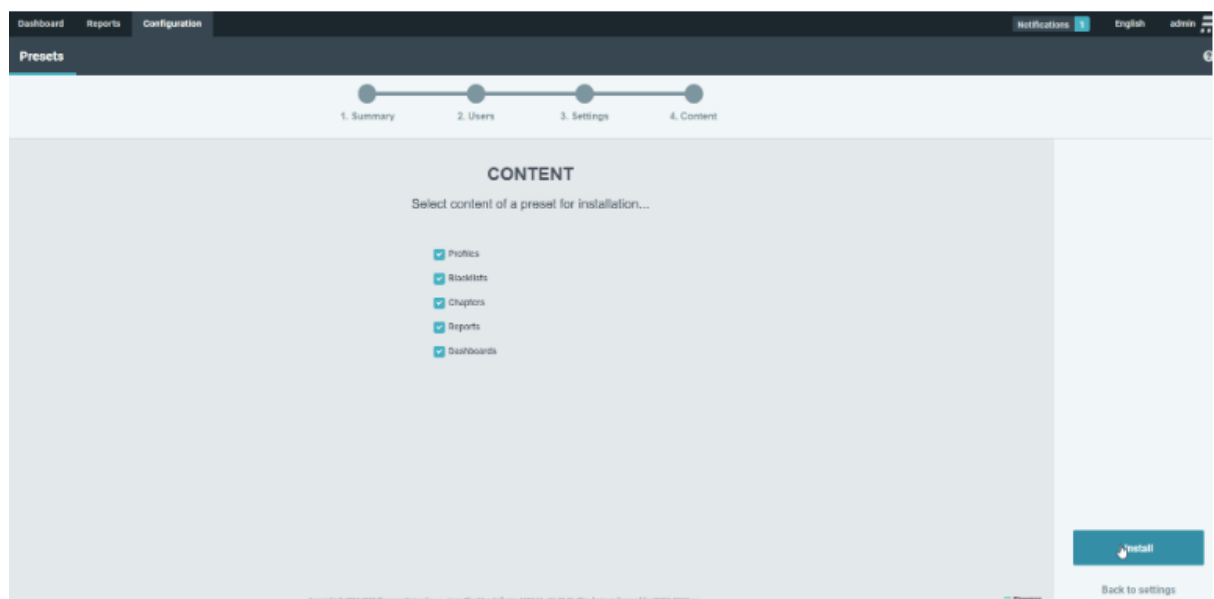
Figure shows which tells the system what content is to be installed (profiles, blacklists, chapters, reports, and dashboards)
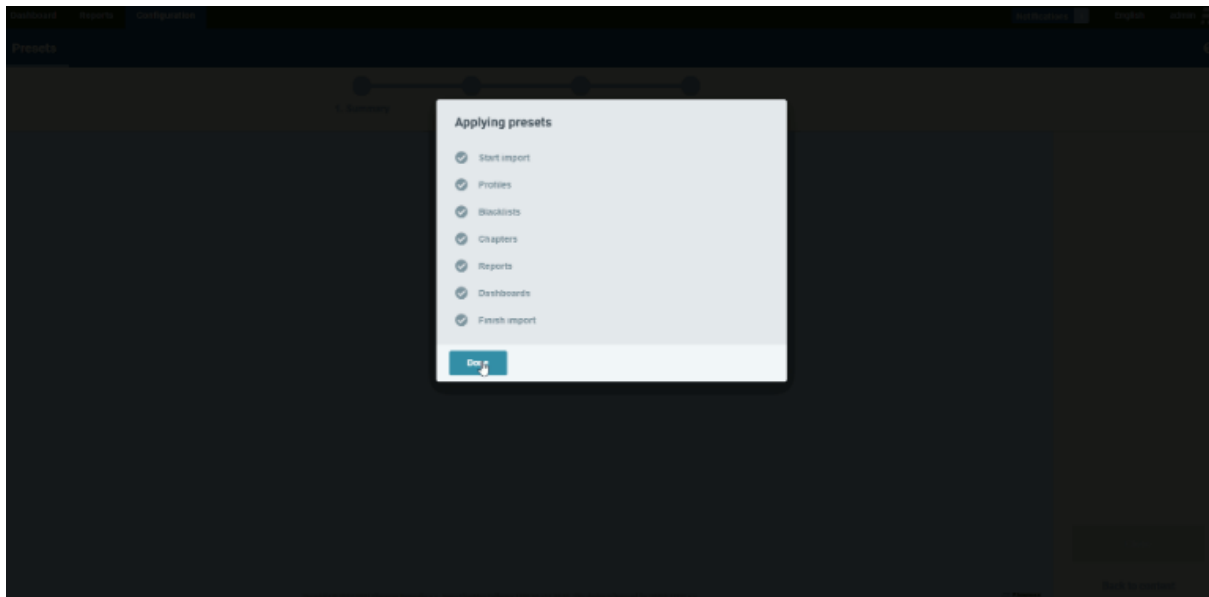
Figure shows presets that can be applied

After clicking Install , the preset will be automatically applied and right away, the user will see statistics from their real network traffic, perhaps even be informed about issues that may have emerged.

TOPOLOGY
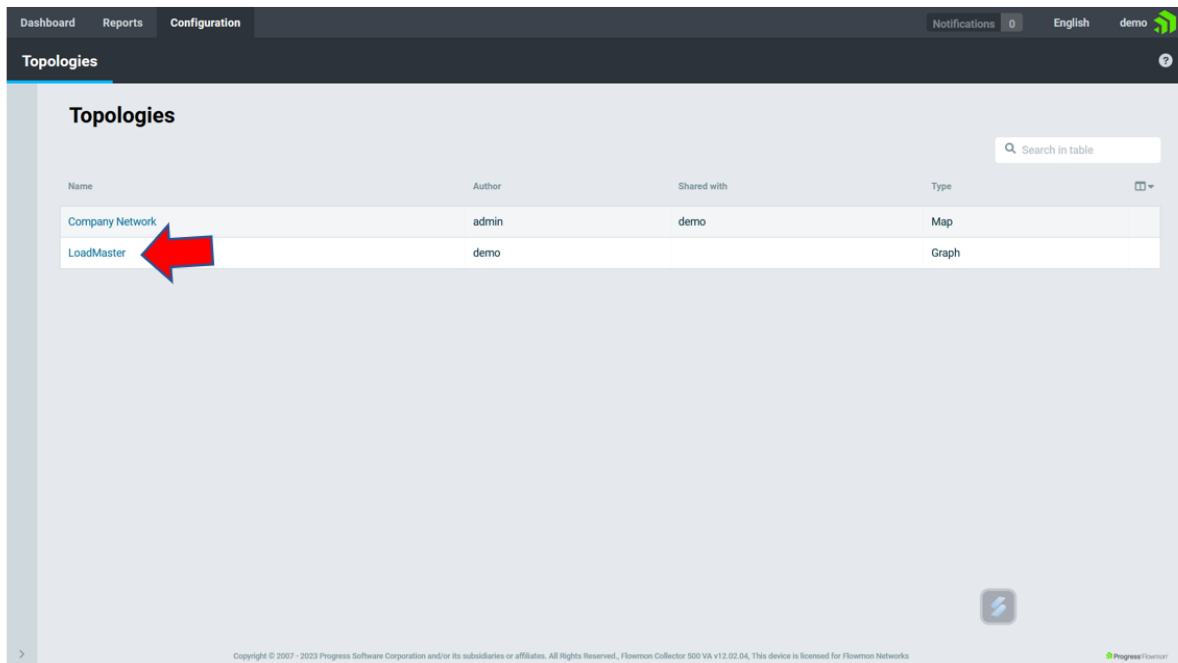
For the topology, we decided to use tree topology. Tree topology, also known as hierarchical topology, is a network design in which devices are connected in a tree-like hierarchical structure. The tree architecture is made up of a root node at the top that serves as the network's focal point, and succeeding tiers of nodes branching out from the root.

Each level of nodes in a tree topology is connected to a higher-level node, eventually going back to the root node. This results in a hierarchical structure that enables for centralised network control and management. The lower-level nodes are connected to the leaf nodes, which are end devices such as computers, printers, or servers.

Using this Flowmon software, you can also view the network topology. The first step is to go "Configuration" on the homepage.
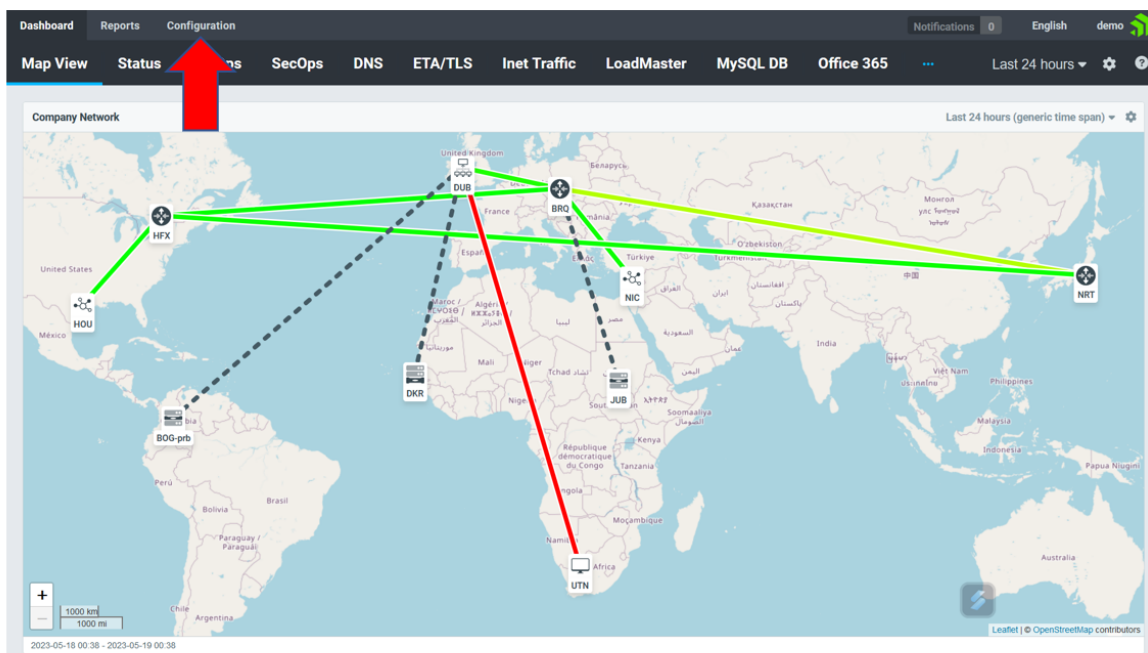
The next step is to choose the server, as example "LoudMaster".

Finally, you will see the example of network topology for server LoudMaster. As you can see this is a tree topology.
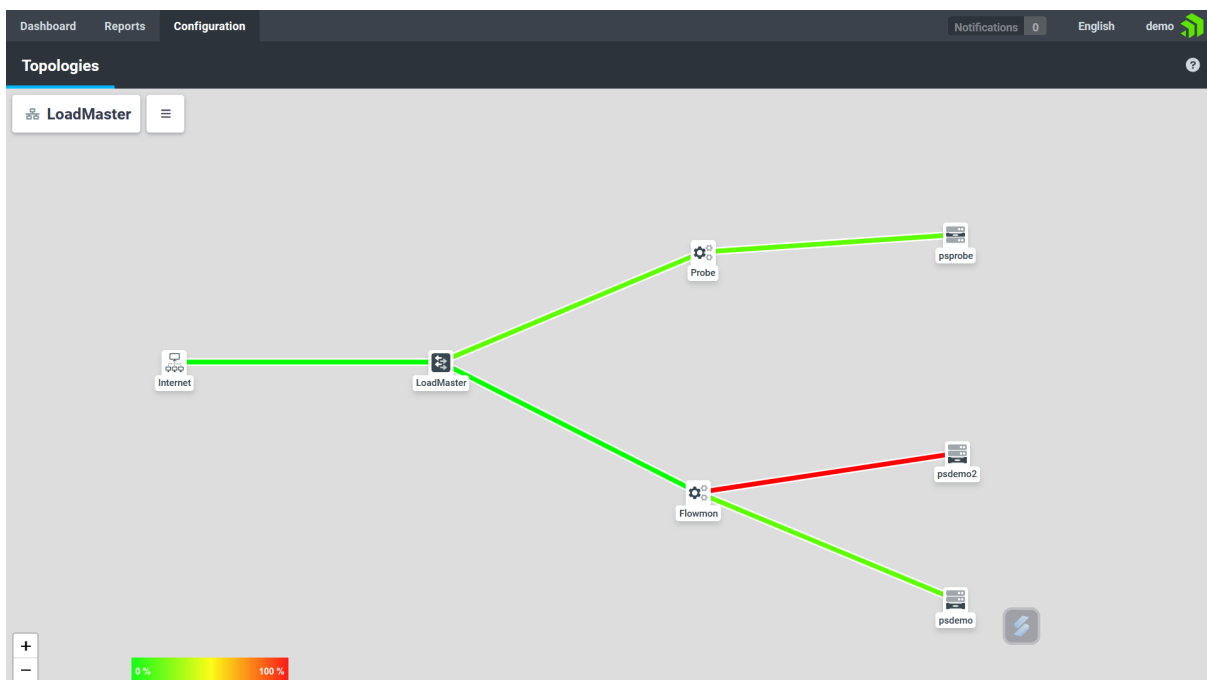
Otherwise you can view the topology like this:
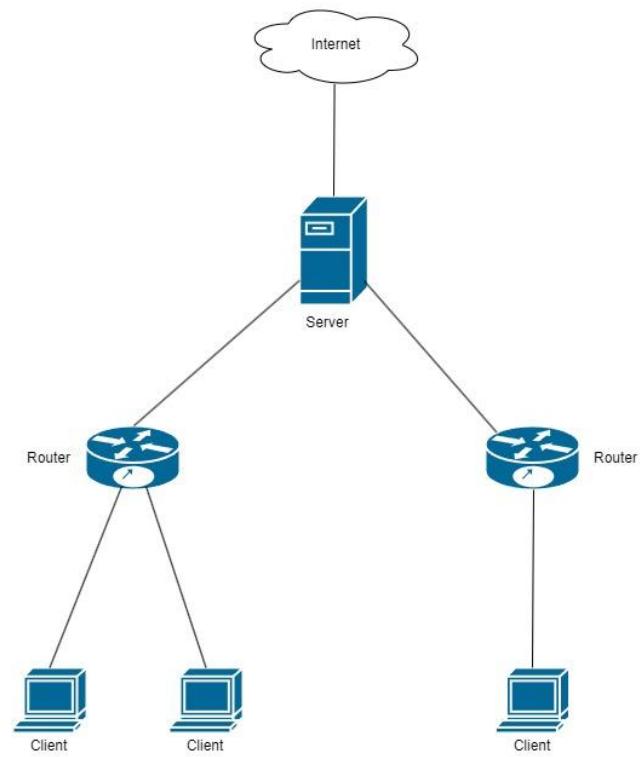
RESULT AND DISCUSSION

Based on the software testing, here are the results. When we ping from the laptop, it will show the graph of the FlowMon. The graph of FlowMon will show how many devices were actively communicating in the monitored network during the time interval. When you scroll down the graph, it will show the dashboard of FlowMon. It is just the same data but we can see it in more detail.
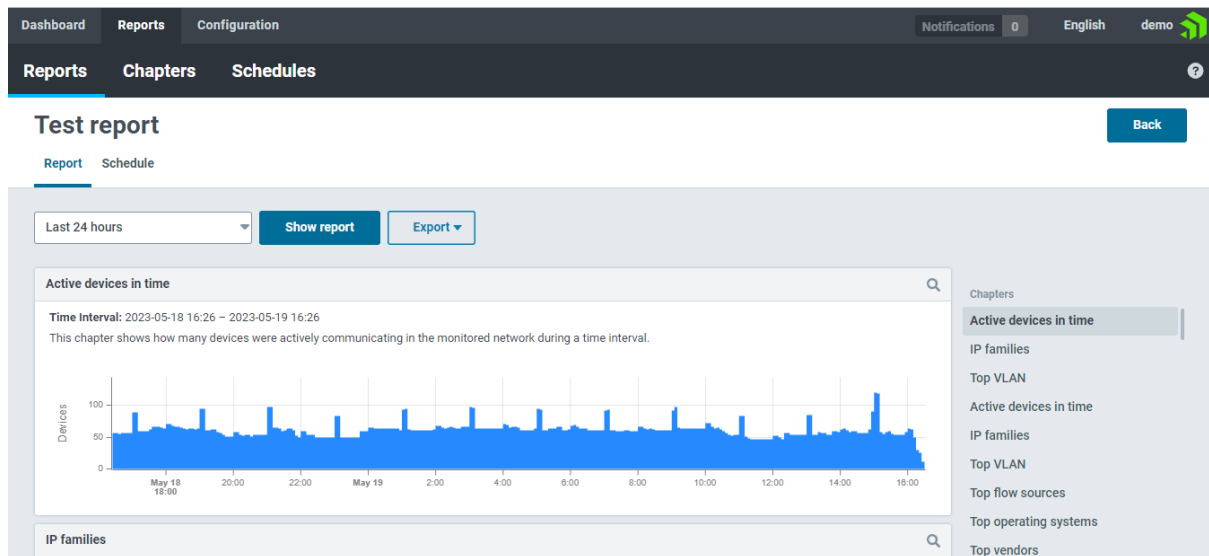
Figure shows active devices in time
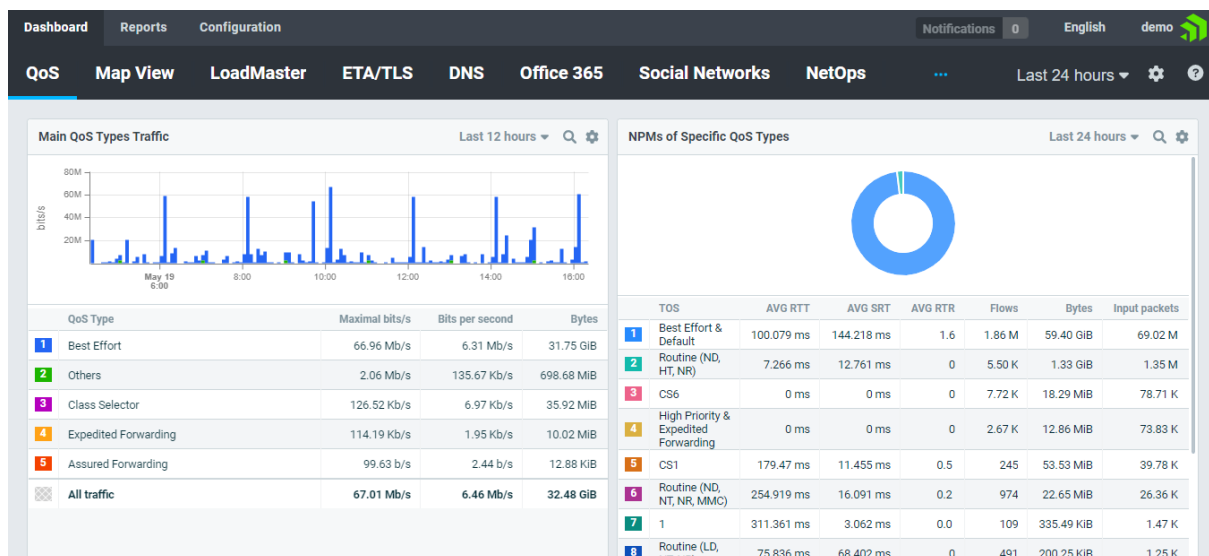
Figure shows dashboard of FlowMon

Next, to see how the connectivity between the wifi and the software is linked, as we do in software testing, we will refer to the graph of sensor traffic. In the graph, it shows the QoS type, the maximal bits, bits per second and bytes.
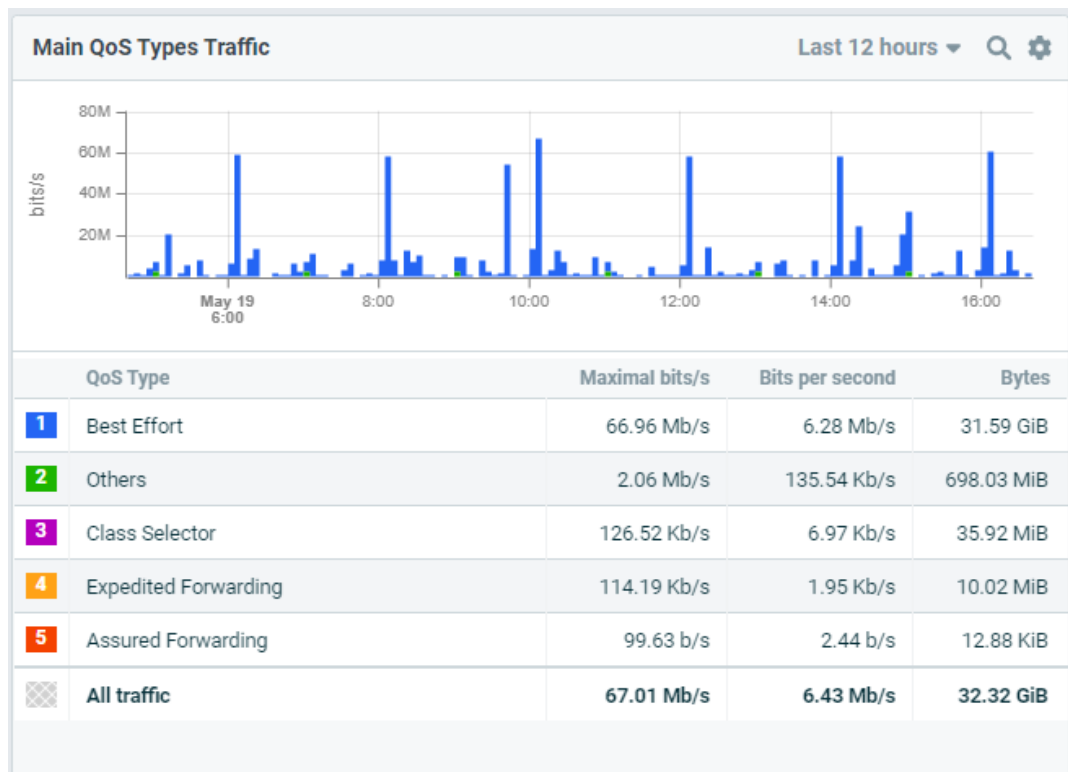
Figure shows types traffic

If we scroll down the graph, we can see more detail about the information in the graph. It shows the latest 10 new events. It shows the event types, name and detection time.

Figure shows the latest 10 new events

CONCLUSION

The FlowMon network monitoring project has been a massive endeavour aiming at improving network visibility, performance, and security. Throughout this research, we investigated the capabilities and features of FlowMon, a powerful software solution that provides real-time monitoring, analysis, and reporting of network traffic flows. FlowMon gives administrators precise insights into network performance, security threats, and resource utilisation by combining powerful flow-based monitoring techniques, deep packet inspection, and intelligent anomaly detection. FlowMon monitors and analyses network traffic flows in real time, allowing administrators to detect and respond to any issues and ensure optimal network performance. The software's complete flow analysis features provide significant insights into application performance, resource allocation, and user behaviour, allowing administrators to discover bottlenecks, optimise network setups, and manage resources effectively. Furthermore, FlowMon combines deep packet inspection (DPI) technology, allowing administrators to undertake detailed network traffic analysis, detect specific apps, protocols, or viruses, and improve security measures. The incorporation of machine learning techniques for intelligent anomaly detection enables administrators to proactively discover anomalous traffic patterns linked with network assaults, strange behaviours, or performance deterioration.

LESSON LEARN

Many businesses now have a highly complicated networking system in place. Because technology was not as advanced as it is now, just a few networks needed to be watched at the time. In this case,

In the contemporary era, network monitoring software is essential to be used because the network is highly complex and it will take millennia to figure out the network's problem, and the simplest way is to have a network monitoring system placed in the network. There are numerous network monitoring software solutions available to users. Users must analyse the situation and select the best programme for their needs.

REFERENCES

1. Flowmon Networks. (n.d.). Flowmon DDoS Defender. Retrieved from
   https://www.flowmon.com/en/products/flowmon-ddos-defender

2. Flowmon Networks. (n.d.). Flowmon Anomaly Detection System. Retrieved from
   https://www.flowmon.com/en/products/flowmon-ads

3. Flowmon Networks. (n.d.). Flowmon Solution. Retrieved from
   https://www.flowmon.com/en/products

4. Flowmon Networks. (n.d.). Flowmon Solution Overview. Retrieved from
   https://www.flowmon.com/en/products/flowmon

APPENDIX B

USER MANUAL OF FLOWMON NETWORK MONITORING

STEP 1:

Go to Flowmon website at
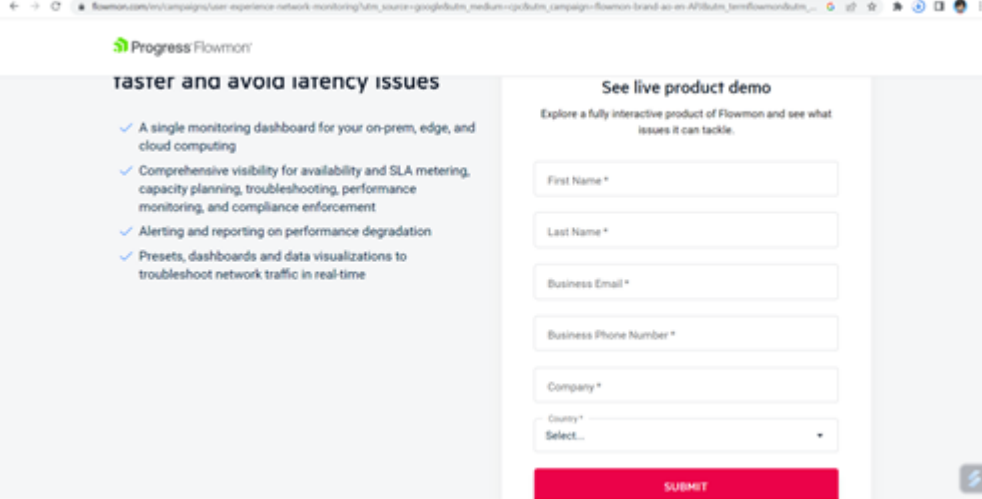
https://www.flowmon.com/en/campaigns/user-experience-network-monitoring?utm_source=google&utm_medium=cpc&utm_campaign=flowmon-brand-ao-en-APJ&utm_termflowmon&utm_id=19664482934&utm_contentkwd-17417371011&adgroupid=147601820084&network=g&gclid=CjwKCAjw8-OhBhB5EiwADyoY1XblPC2DCZDDdC9YfEenkBDsZEmsf1_bZovSvpu1sE9yTLpqE2UVvBoCwtgQAvD_BwE

And click the "LAUNCH LIVE DEMO" button.
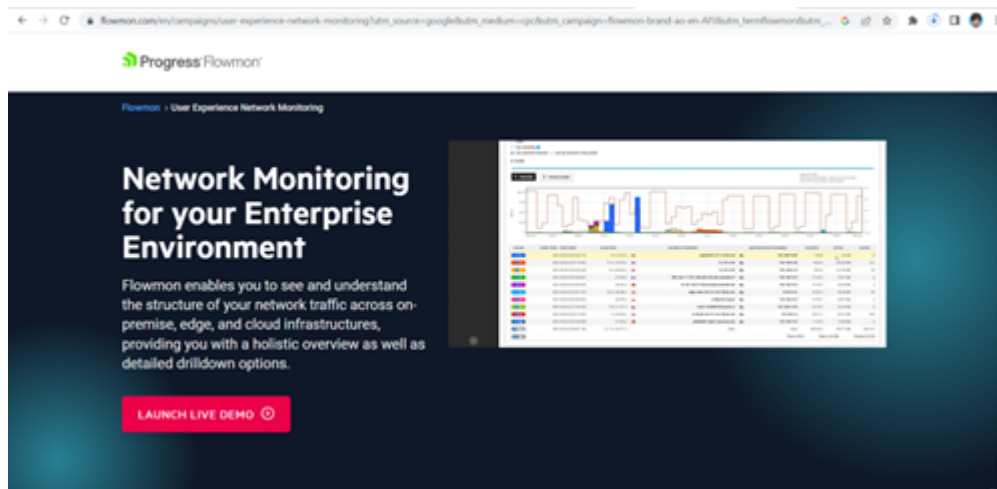
STEP 2:

Fill all the information in the box and click the submit button.

STEP 3:

After that, you will receive the login name and password.

Next, click the "LAUNCH DEMO" button.

Step 4:

After you click the previous button, you will be directed to the login page. In this page, you will need to fill the login name and password.
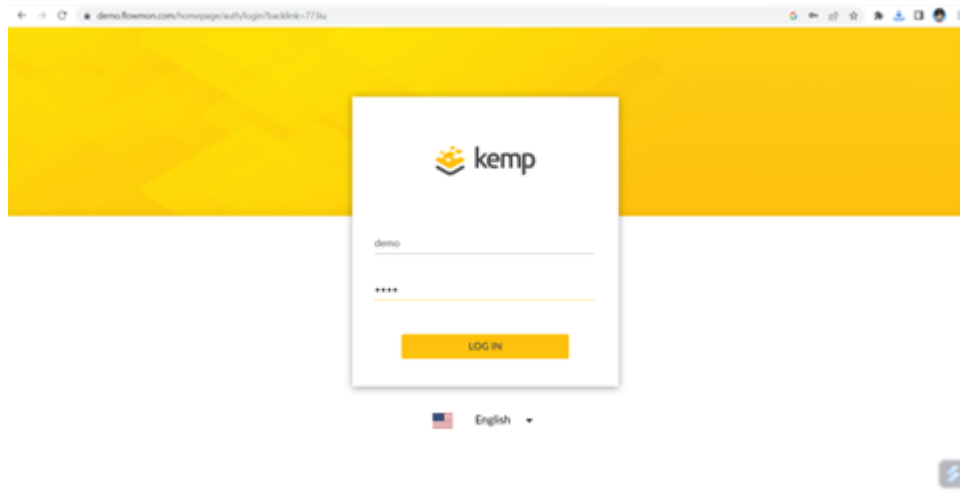
STEP 5:

Lastly, you will see Flowmon web interface and follow the on-screen instructions to complete the initial configuration.