Visibility Platform Test Drive On AWS

Table of Content

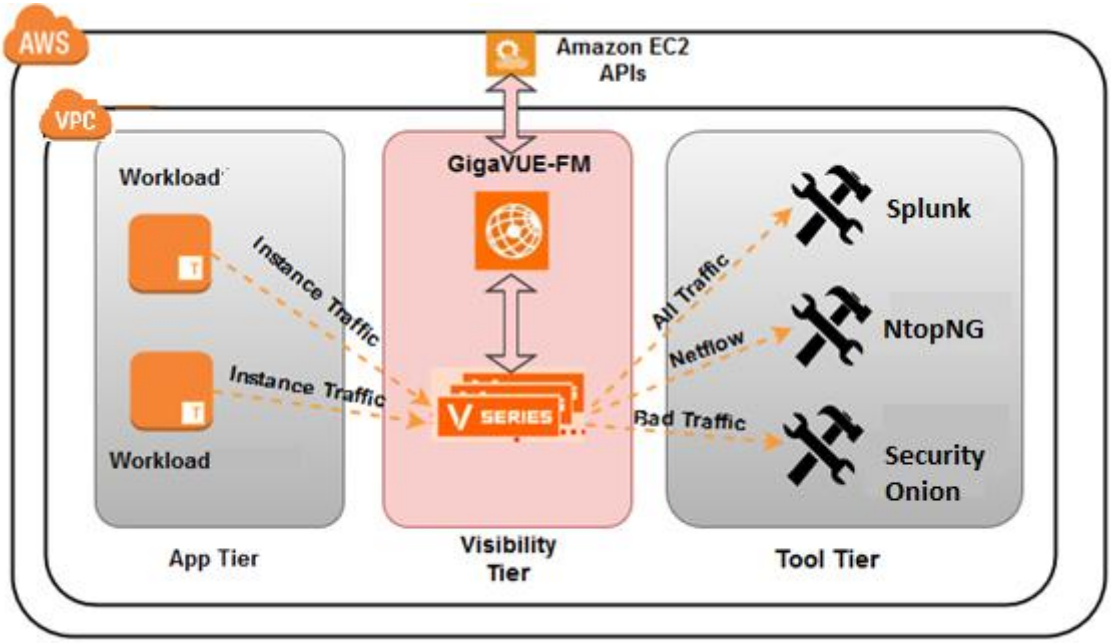
1. About Test Drive

The purpose of the Visibility Platform for AWS Test Drive is to quickly and easily explore the benefits of using the Gigamon Visibility Platform for AWS features. This Test Drive is focused on demonstrating how Gigamon Visibility Platform for Amazon Web Services (AWS) provides consistent visibility into data-in-motion across the entire enterprise.

2. Introduction to the Visibility Platform for AWS

The biggest challenge in managing and securing the data traversing the public cloud today include the inability to access all traffic and data, lack of visibility into East-West traffic needed for compliance, lateral threat mitigation, and more. In an on-premise deployment, there are options to get access to traffic from the infrastructure for real-time analysis via TAPs (physical or virtual) and SPAN sessions. When deploying applications and workloads in the public cloud, none of these options are available. Using agent-based monitoring could lead to a very complex architecture, especially if multiple tools need access to the same traffic for inspection and analysis. An efficient and optimal solution to overcome these challenges is to use the Gigamon Visibility Platform for AWS, the industry's first pervasive visibility platform that provides consistent visibility into data-in-motion across the entire enterprise. The Gigamon Visibility Platform for AWS integrates with your AWS environment, mirrors the application traffic, and replicates the traffic customized using Flow Mapping® to network and security tools that reside on cloud.

3. Architecture



The Gigamon Visibility Platform for AWS extends an enterprise's on-premise Gigamon Visibility Platform to the AWS public cloud regardless of where your applications reside. Refer to the figure above. The entire Visibility Platform is managed by a single management appliance called GigaVUE Fabric Manager (GigaVUE-FM). Using GigaVUE-FM, the traffic flow maps can be created to customize and send the monitored traffic to the specific tools in the AWS public cloud. Once a map is configured, GigaVUE FM updates all the nodes in the Visibility Platform automatically. As your instances/workloads scale, they are automatically added to the flow maps and the traffic is monitored immediately.

4. Test Drive Environment:

Within AWS, the following necessary components are configured to provide enough infrastructure to complete this Test Drive:

- **GigaVUE Fabric Manager (GigaVUE-FM):** A web-based interface for creating flow maps and sending monitored traffic to specific tools.
- **GigaVUE V Series Node:** A visibility node that aggregates mirrored traffic from an AWS instance, applies filters, and distributes the optimized traffic to the monitoring tools using the standard Layer 2 (L2) GRE tunnels.
- **NtopNG (Tool):** A monitoring tool present inside the applications VPC for receiving the monitored traffic from the Visibility Platform.
- **Splunk (Tool):** A monitoring tool present inside the applications VPC for receiving Netflow traffic from the Visibility Platform.
- **Security Onion (Kibana) (Tool):** A monitoring tool present inside the applications VPC to show the malicious traffic generated by vulnerable web applications.

5. Getting Started

After the Test Drive provisioning is complete, login credentials are provided in the Test Drive launch page.

The Test Drive environment helps you focus on the tasks defined in the following use cases:

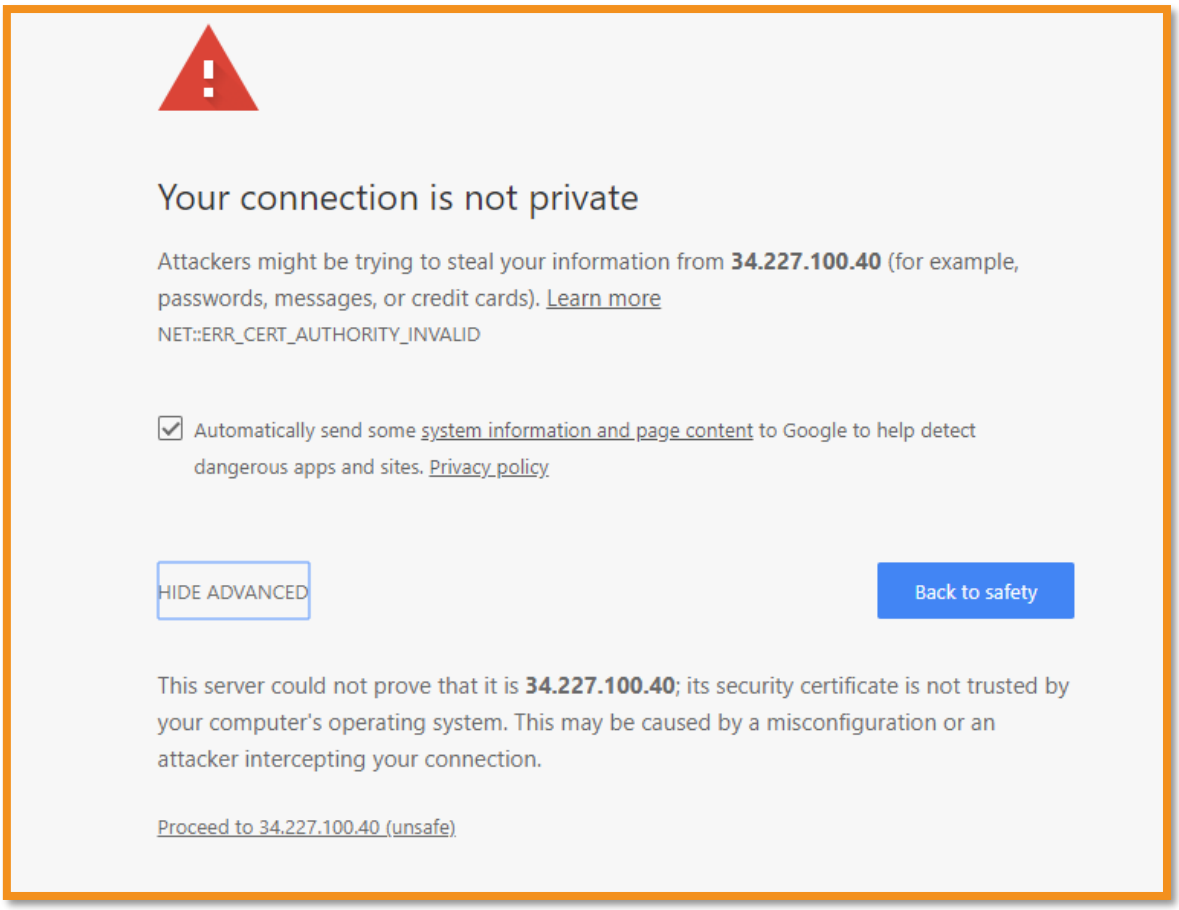
- **Use Case 1: Gaining Visibility -** Create the flow maps to send all type of traffic into the Splunk (Netflow), NtopNG and Security Onion.
- **Use Case 2: Creating Traffic Specific Flow Maps -** Create multiple flow maps to send specific traffic to specific tools.
- **Use Case 3: Detecting Threats -** Create a flow map to send the traffic to the security tool in the applications VPC to see if there is any suspicious traffic.
- **Use Case 4: De-duplication -** Create a flow map to identify and eliminate the duplicate packets and send an optimized feed to the tools.

5.1. Use Case 1: Gaining Visibility

In this use case, create a flow map to send all traffic types from the workloads to the

monitoring tools→ Splunk (Netflow), NtopNG and Security Onion.

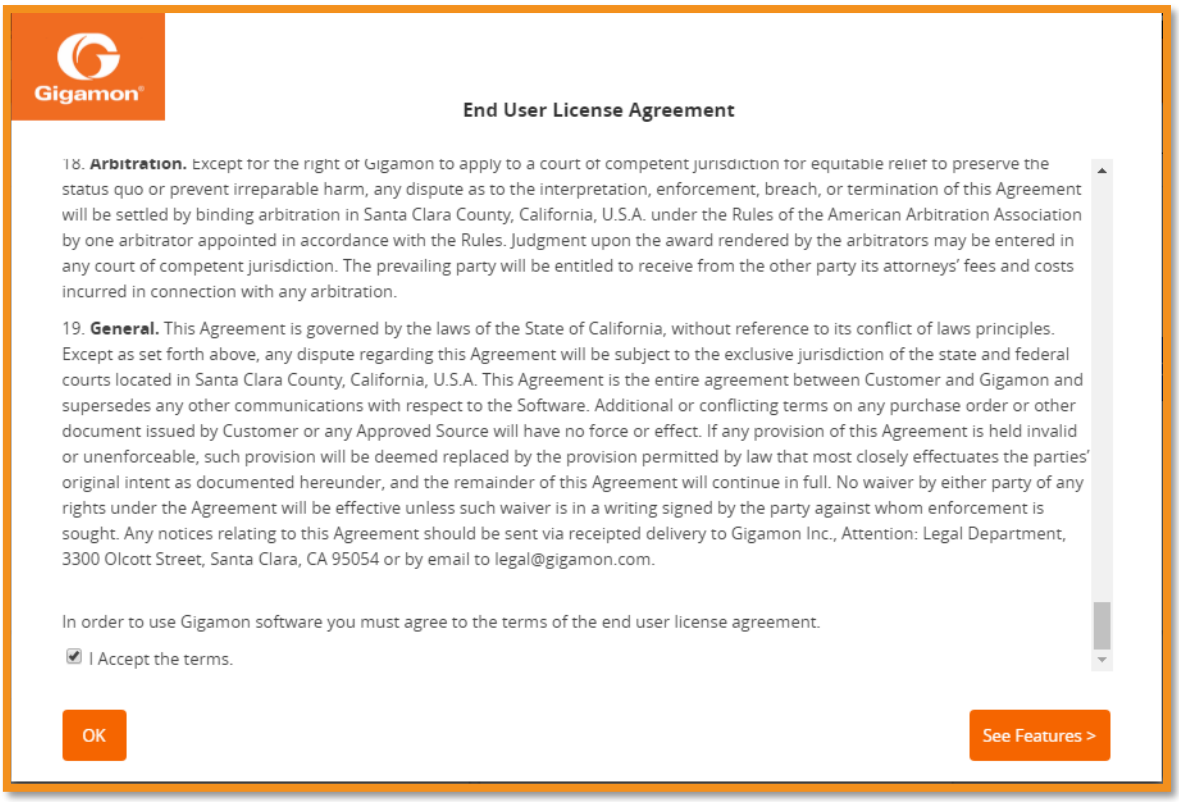
1. **Login to GigaVUE-FM.**
   - Go to **GigaVUE-FM** using its **url** provided in the Test Drive launch page. Click **Advanced > Proceed to IP address** link in the warning screen.



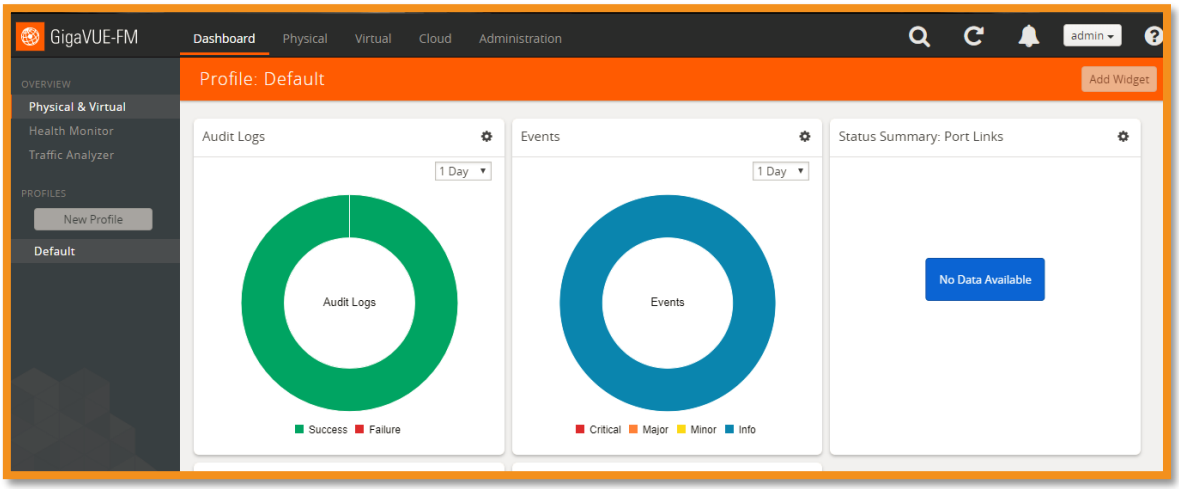
- Login to **GigaVUE-FM** with the **Username** and **Password** provided in the Test Drive launch page and click the **Log In** button.

NOTE: GigaVUE-FM will log out automatically if inactive for 10 minutes. Keep the login credentials information handy to be able to **log In** again to GigaVUE-FM to complete the test drive.

- Click **See EULA**, and scroll down to accept the terms.

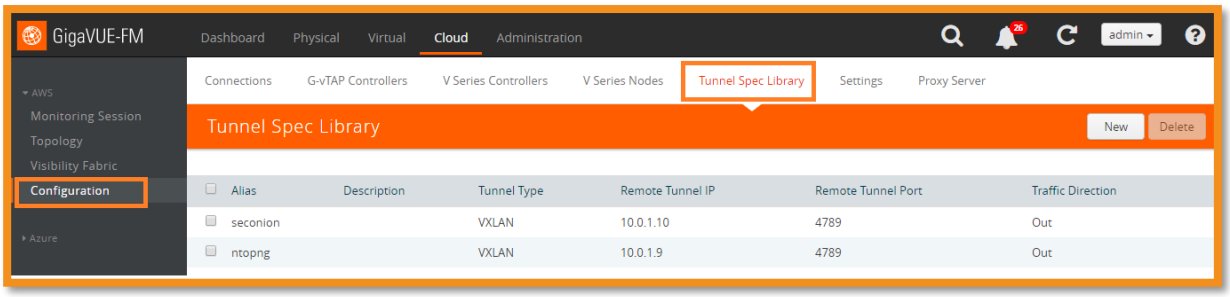


- Select the **I Accept the terms** checkbox and Click **OK,** the dashboard page is displayed
- Click Cloud menu option as shown in the following figure.



- Navigate to **Configuration** under **AWS** from the left menu and click **Tunnel Library** tab.
- Here you can see that the **VXLAN tunnels (NtopNG and SecOnion)** are been automated.

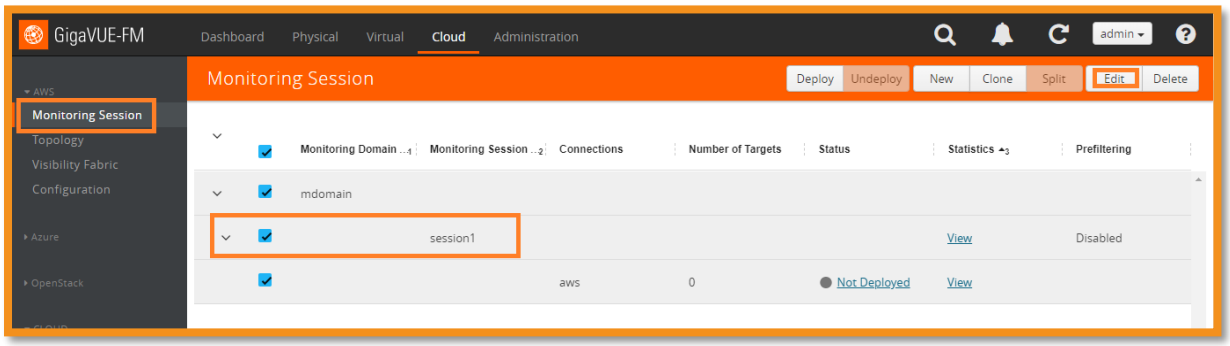
NOTE: A standard Vxlan tunnel is established to distribute the customized traffic from the V Series node to the monitoring tools.



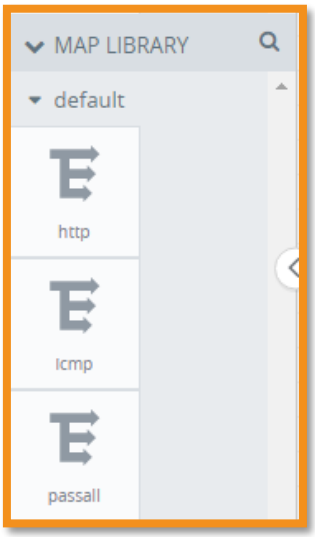
- Click **Monitoring Session** option from the left menu to open the **Monitoring Session** page.

NOTE: Monitoring session directs the traffic from the workloads to the monitoring tools (Splunk, NtopNG and Security Onion-kibana).

- Select the monitoring session (**Session1**) check box and click **Edit** button on the top right corner as shown in the following figure.



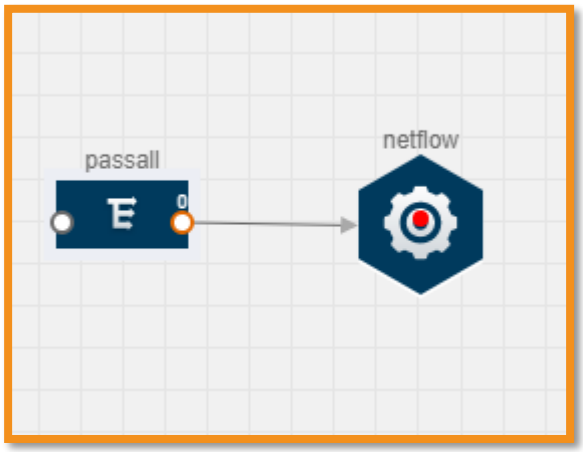
- In this Monitoring Session, the maps (passall,ICMP and http) are already created in the map library.



2. **Creating a flow map.**

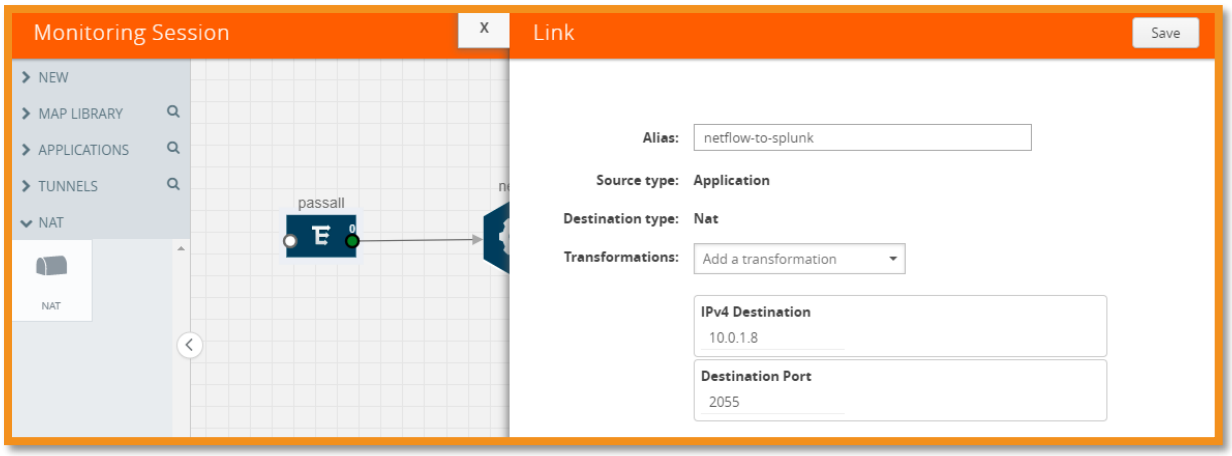
- Drag and drop the **passall** map from the **MAP LIBRARY** section and **Netflow** from **APPLICATIONS** section to the empty map area.

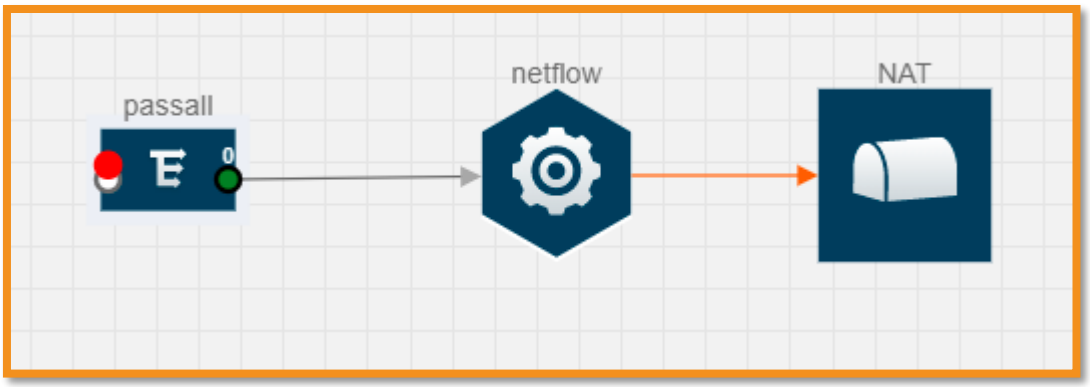
- Hover over the passall map and drag a line to connect the red dots from the **passall** map to the **Netflow** application.



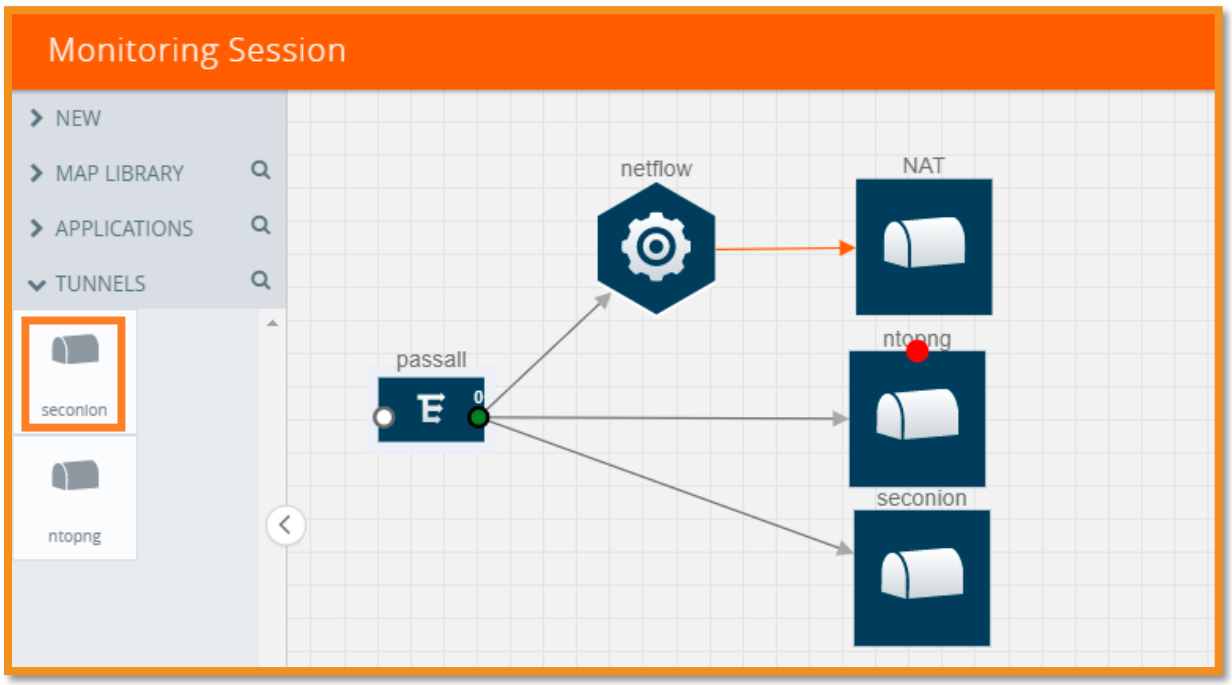
- Drag and drop the **NAT** from the left pane and enter the required information as shown in the following figure.
- Hover over the netflow and drag a line to connect the red dots from the netflow to the **NAT** and enter the required information.
    - In the **Alias** field, enter **netflow-to-splunk** as the alias name.

- Enter Splunk private IP(provided in test drive launch page) in the **IPv4 Destination**.
    - Click **Save** button on the top right corner of the page.





- Drag and drop the **NtopNG** and **SecOnion** maps From **Tunnels**.
- Hover over the **passall** and drag a line to connect the red dots to **NtopNG** and **SecOnion**.

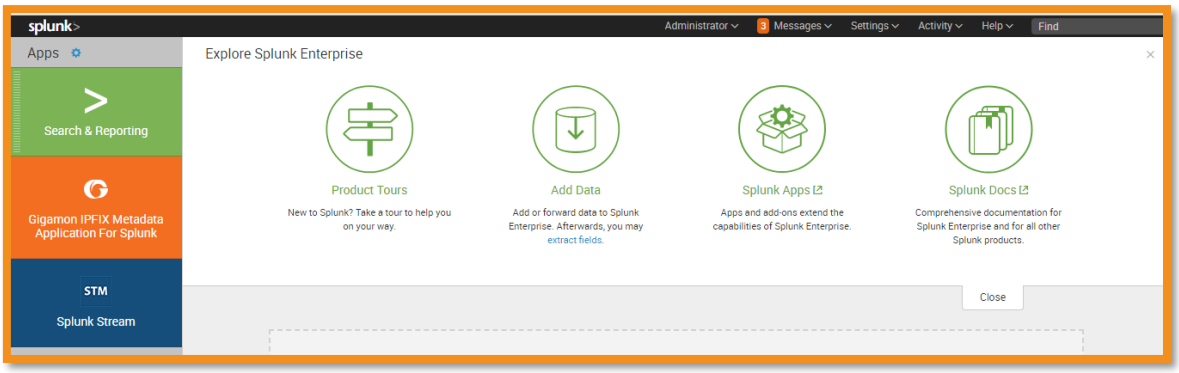


- Click **Deploy** button and click **Close**.

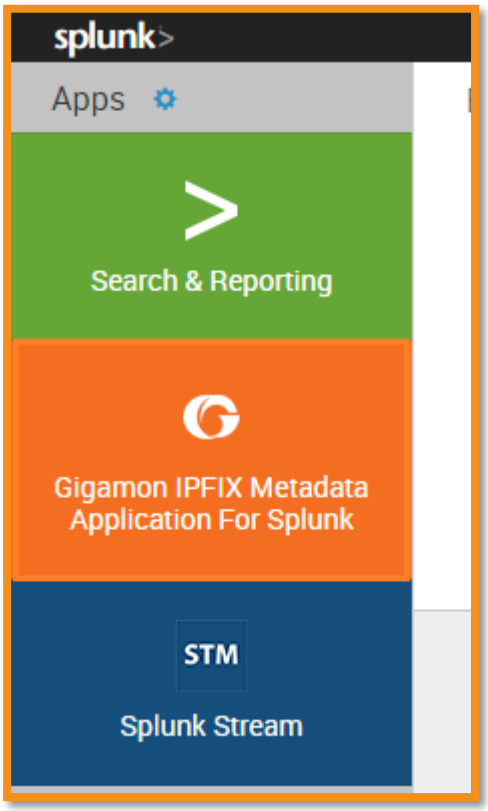
- Now the traffic starts flowing to the **Splunk**, **NtopNG** and **SecurityOnion**.

3. Login to the Splunk

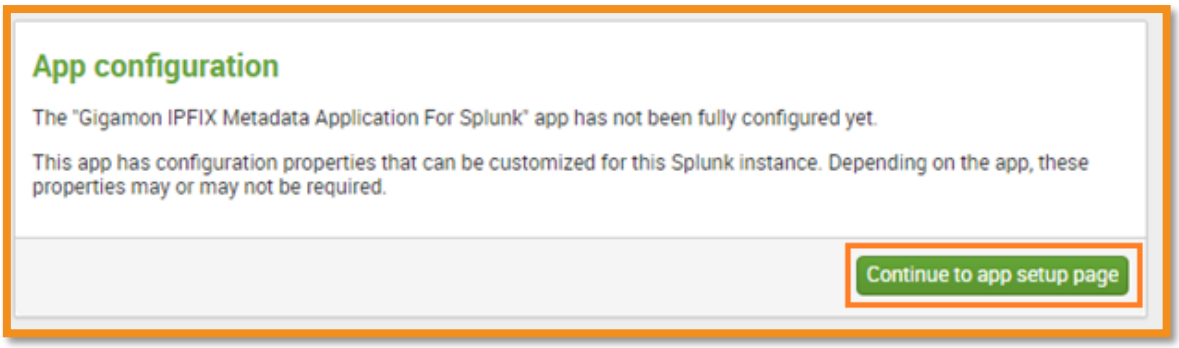
- Go to **Splunk Enterprise** by using its **Splunk web url** provided in test drive launch page.



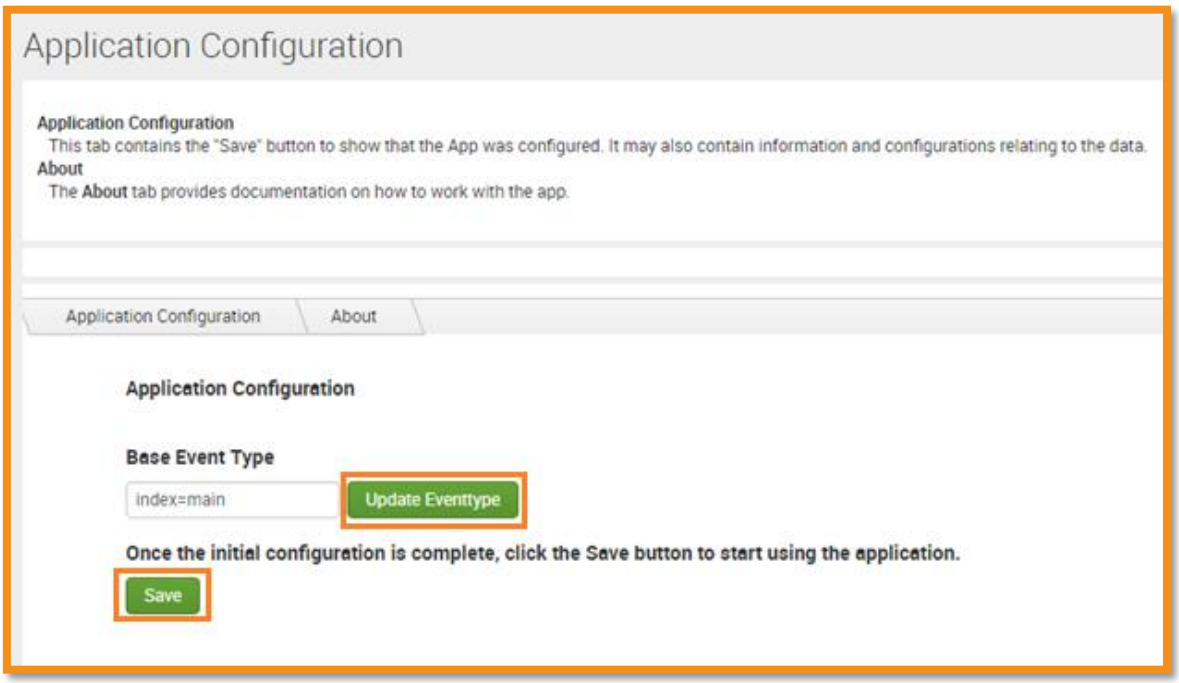
- Go to the **Gigamon IPFIX Metadata Application For Splunk**.



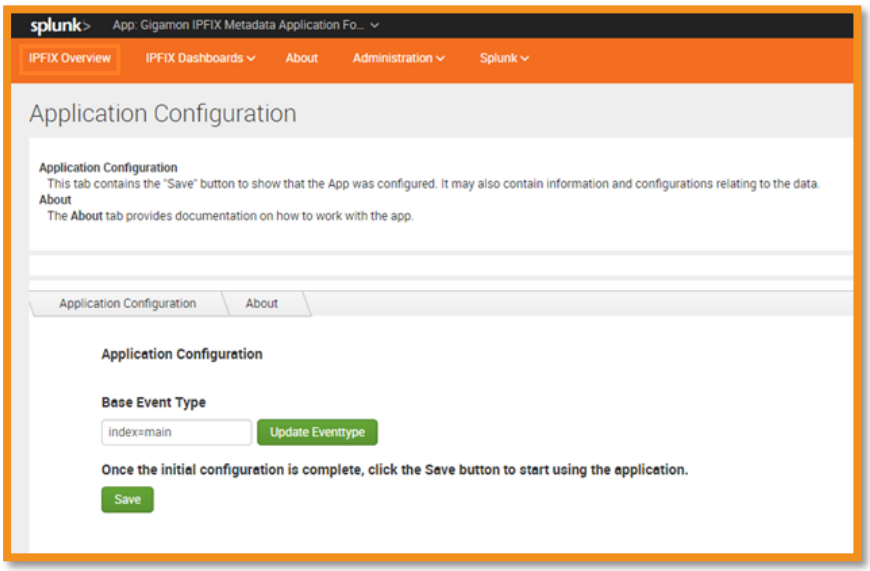
- Click **Continue app setup page** button as shown in the following figure.



- Click **Update Eventtype** button and Click **Save** button as shown in the following figure.

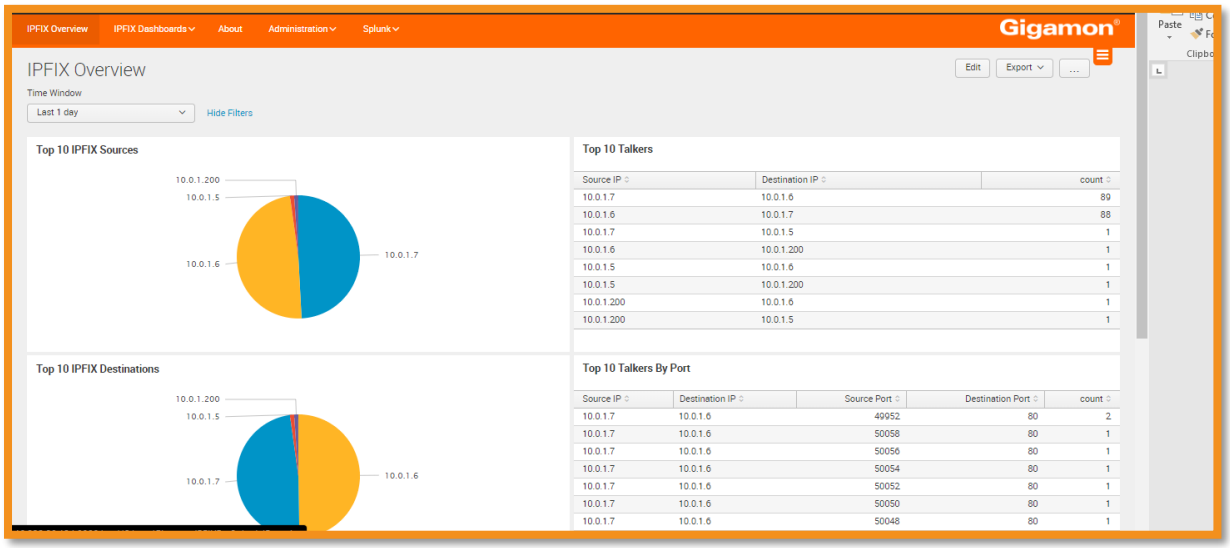


- Click **IPFIX Overview** from the top menu as shown in the following figure.



- In the **IPFIX Overview** page you can see the Netflow data as shown in the following figure.

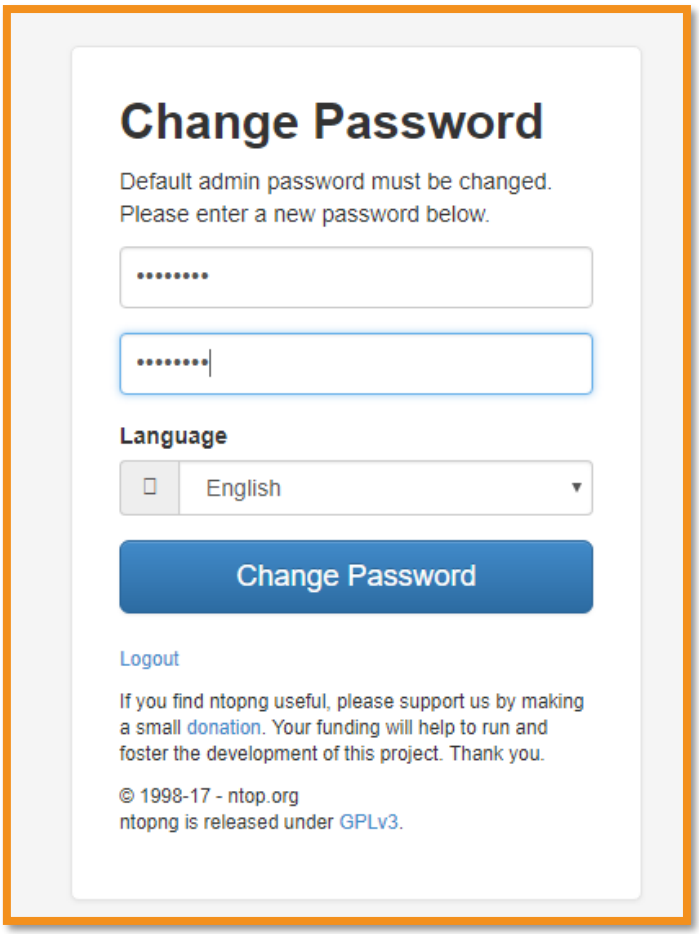
Note: NetFlow is a network protocol for collecting IP traffic information and monitoring network traffic.Using Splunk, you can see where network traffic is coming from and going to and how much traffic is being generated.



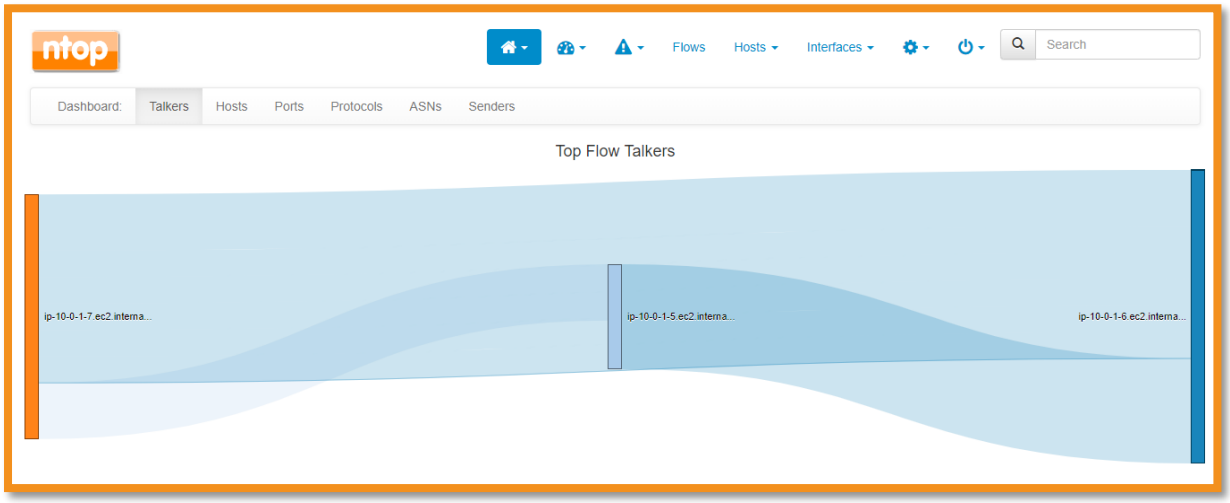
4. **Login to NtopNG.**

- Login to **NtopNG** by using its **url** and credentials provided in the test drive launch page.

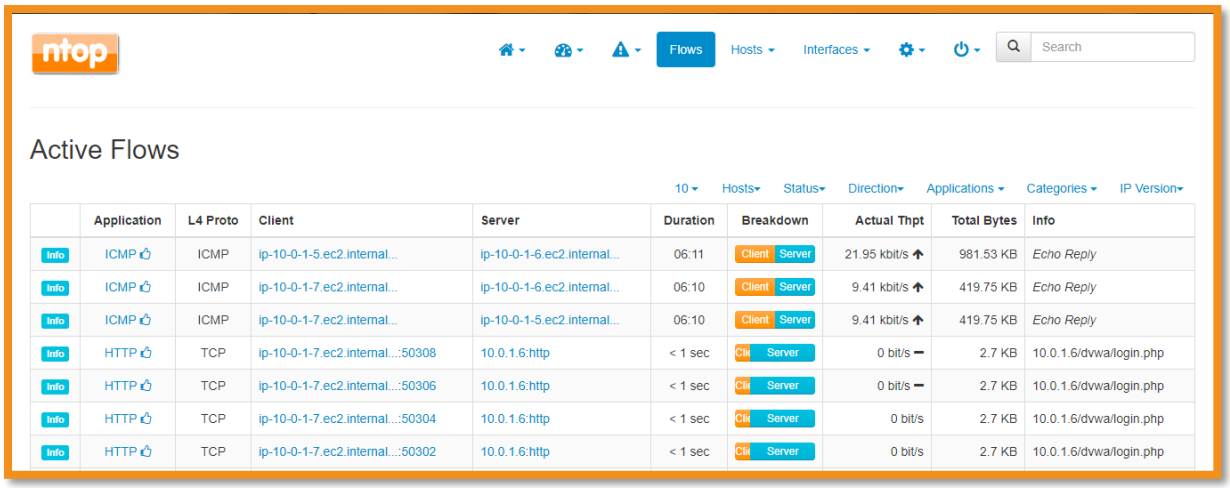
- Change the Password form the change password page.



- In **NtopNG Traffic** Dashboard,you can see the traffic flowing from workloads as shown in the following figure.

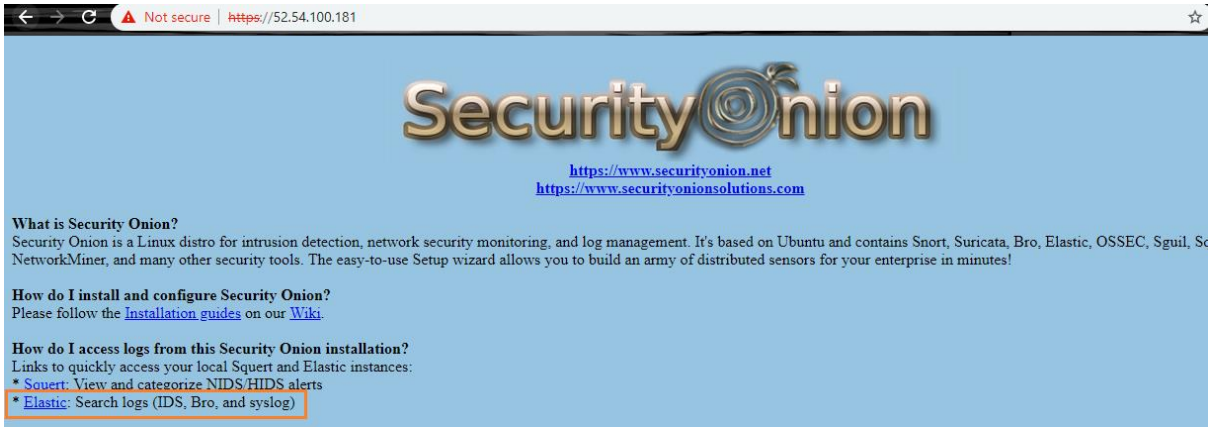


- Click **Flows** from the top menu to view the all traffic types coming from workloads as shown in the following figure.

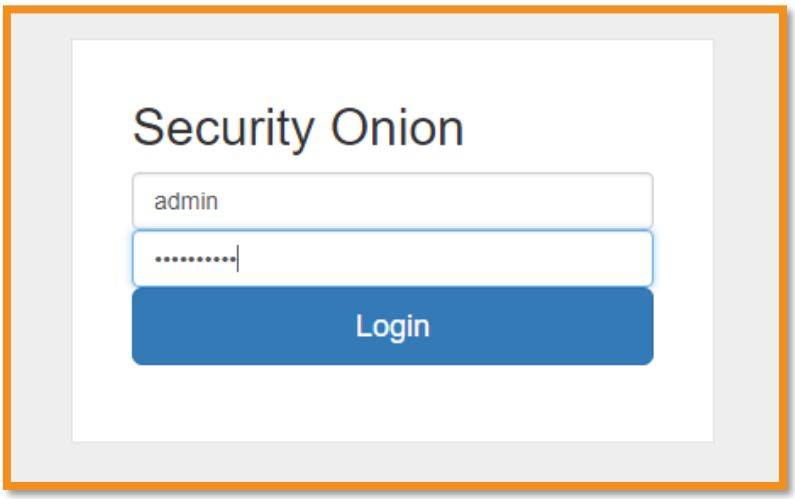


5. **Login to the Security Onion.**

- Go to **Security Onion** using its **url** provided in the test drive launch page. Click **Advanced > Proceed to Public IP** link in the warning screen.
- Select **Elastic** from **Security Onion** home page as shown in the following figure.

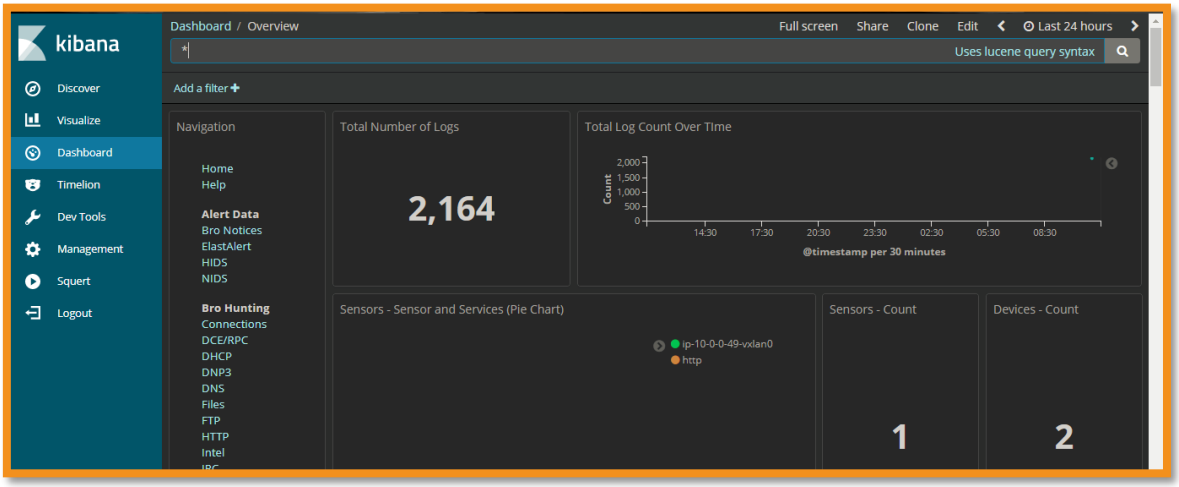


- Login to the **elastic** using the **Kibana** credentials provided in the test drive launch page.

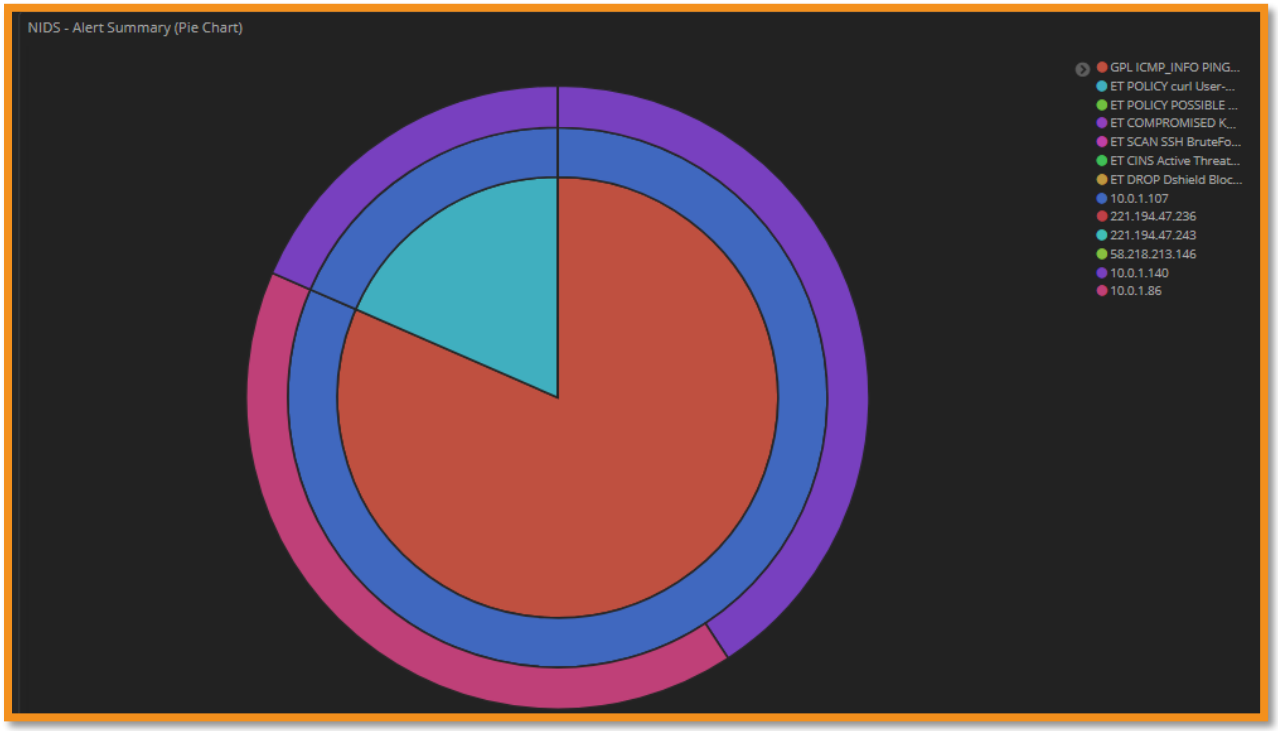


- Once logged in, the **Kibana** dashboard id displayed.

- Select **NIDS** on the left side **Navigation** section of the dashboard as shown in the following figure.



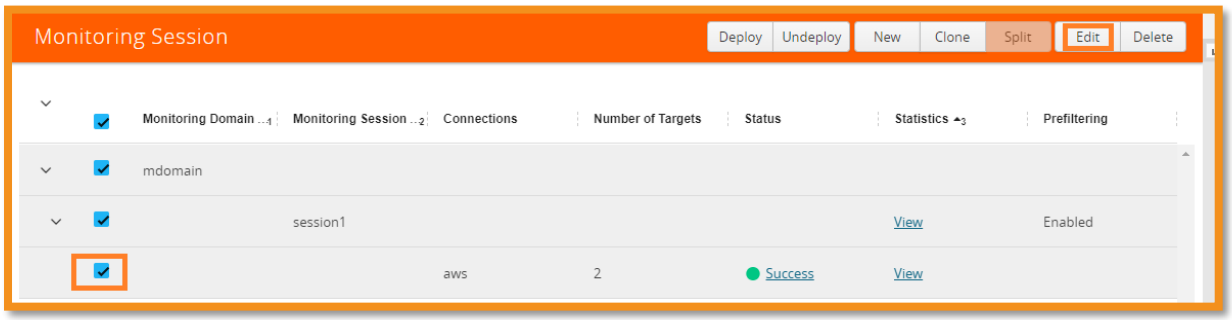
- Here, you can see the traffic alerts coming from workloads.
- Scroll down for more visibility as shown in the following figure.



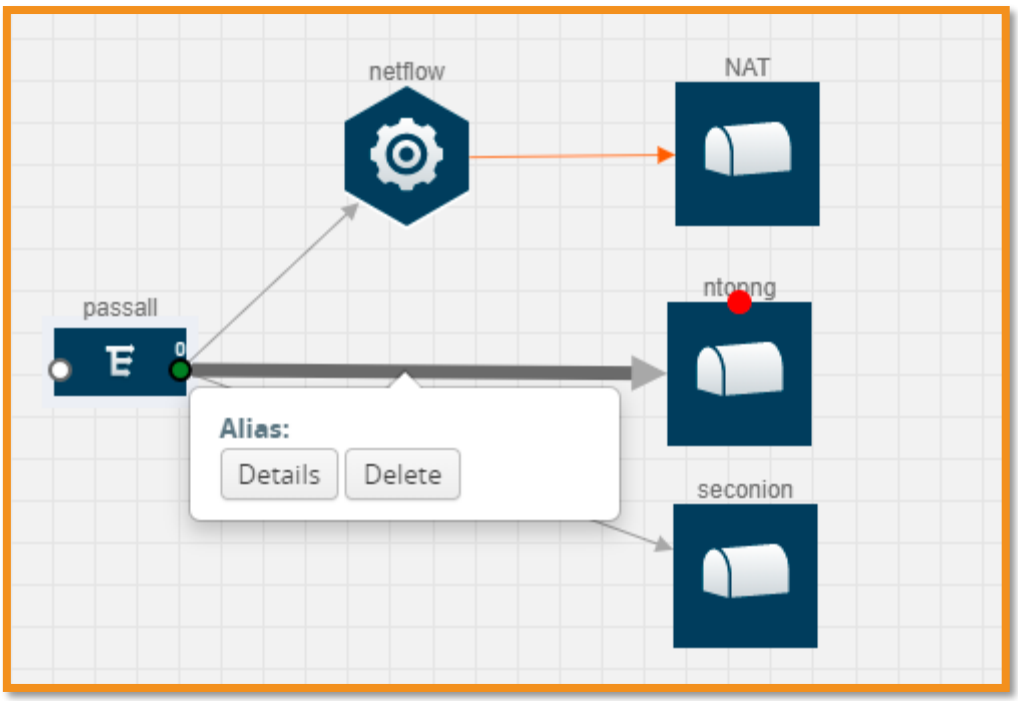
5.2. Use Case 2: Creating Traffic Specific Flow Maps

In this use case, two additional flow maps are created to customize and distribute the application traffic to specific tools. The ICMP traffic coming from the workloads are sent to the **NtopNG** tool tunnel and the HTTP traffic (port 80) are sent to the **Security Onion** tool tunnel.

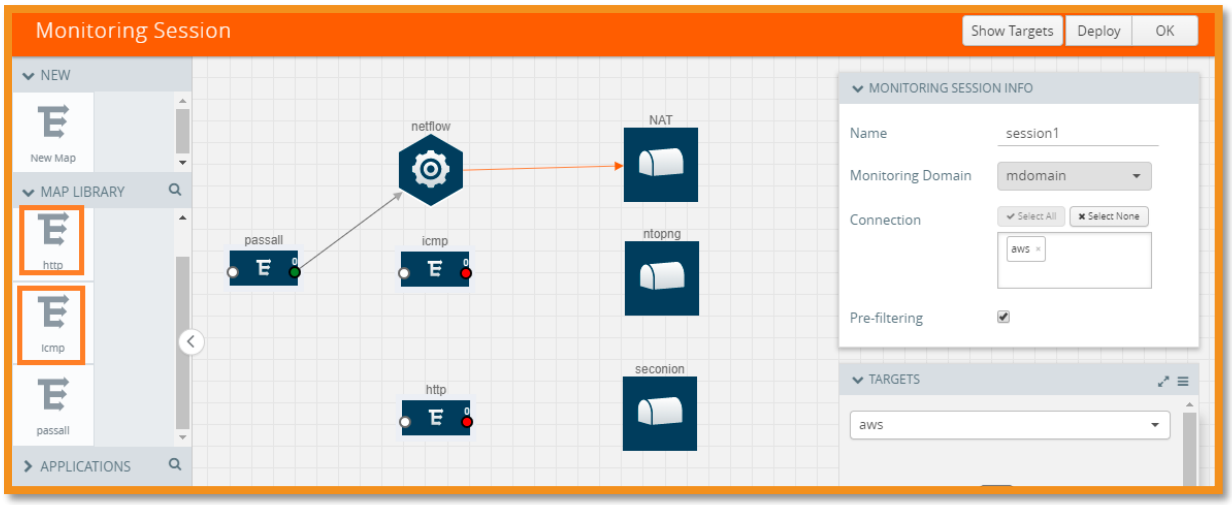
1. **Return to GigaVUE Fabric Manager and edit the monitoring session again.**
   - Login to **GigaVUE-FM** and click **Cloud** from the top menu.
   - Select **Monitoring Session** option from the left menu to open **Monitoring Session** page.
   - Select the check box next to the monitoring session and click **Edit** button as shown in the following figure.



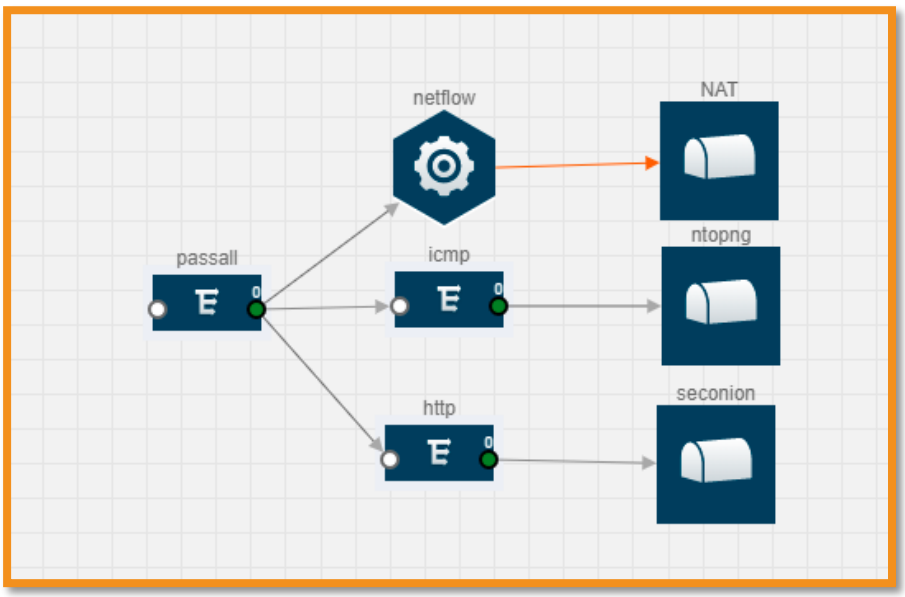
2. **Deleting the links.**
   - Delete the links (Connector arrows) from **passall** to **NtopNG** and **SecOnion** tunnels.



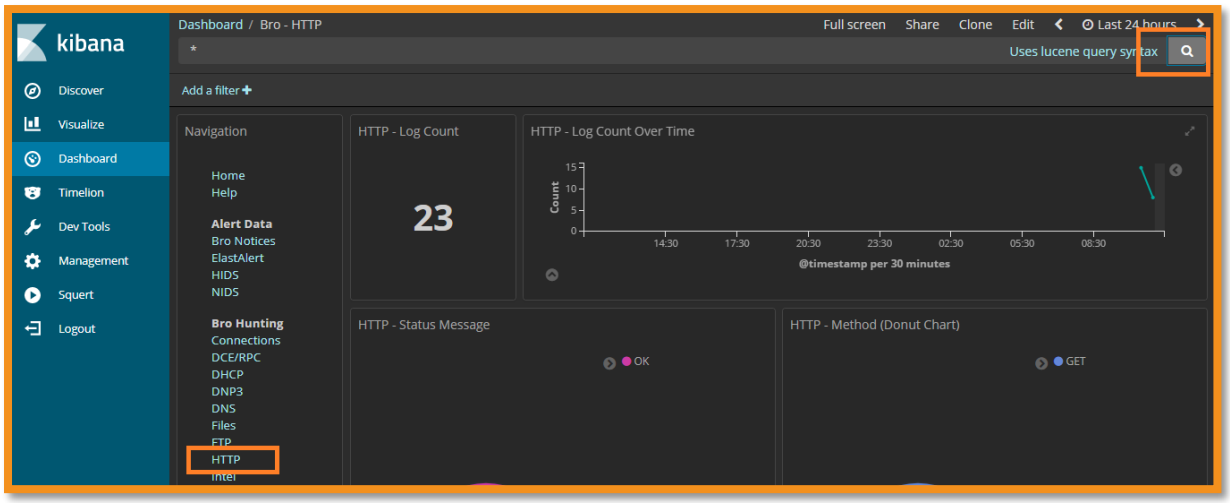
   - Drag and Drop the **ICMP** and **http** maps from the **MAP LIBRARY** section as shown in the following figure.



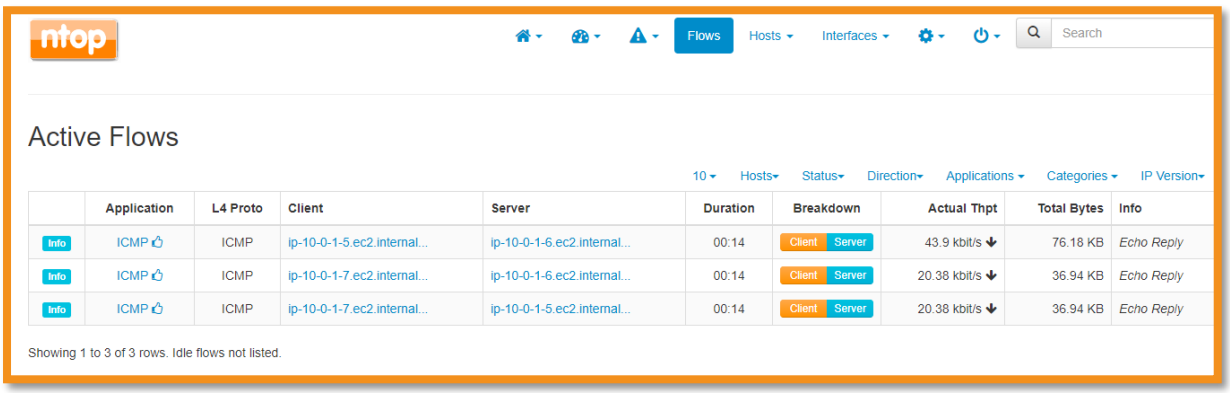
- Hover over the **passall** map and drag a line to connect the red dots to **http** map and **icmp** map.
- Hover over the **ICMP** map and drag a line to connect the red dots to **NtopNG** tunnel and from **http** map to **SecOnion** tunnel.



- Click **Deploy** button and click **Close**.
- Go back to the **Kibana** dashboard to check **http** traffic.
- select **http** on the left side Navigation section of the dashboard as shown in the following figure,
- Refresh the page you can see the number of **https** logs will increase for every refresh.
- Scroll down to the page to view the detailed information of http traffic.



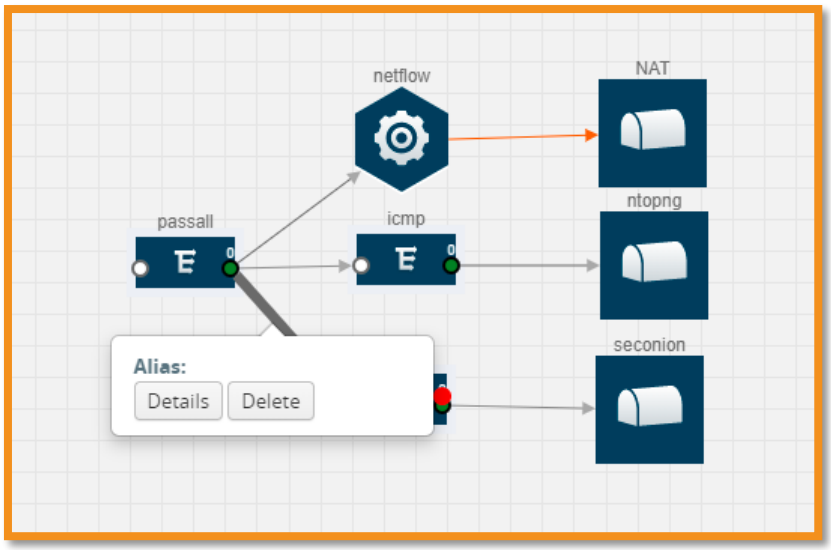
- Go back to the **NtopNG**, wait for some time and refresh the page.
- Click **Flows** from the top menu and you can see the only **ICMP** flows coming from workloads to **NtopNG**.



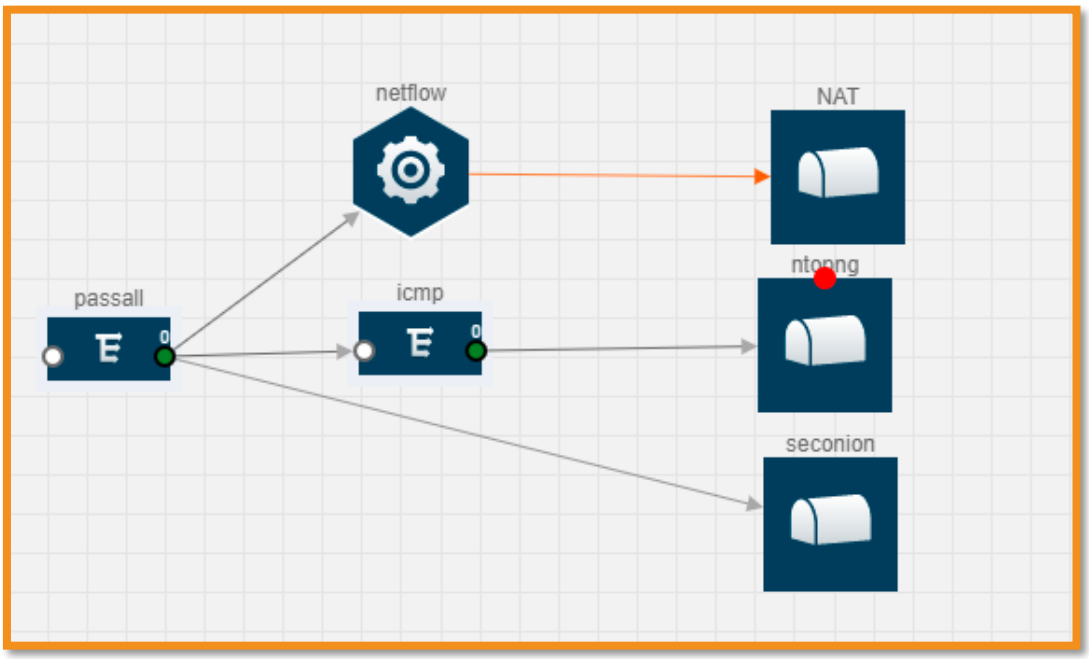
5.3. Use Case 3: Detecting Threats

In this use case, all traffic types are sent to **SecOnion** using **passall** map. On workload 2, you will do some sql injections and brute force attacks to send suspicious traffic to the vulnerable application(DVWA).

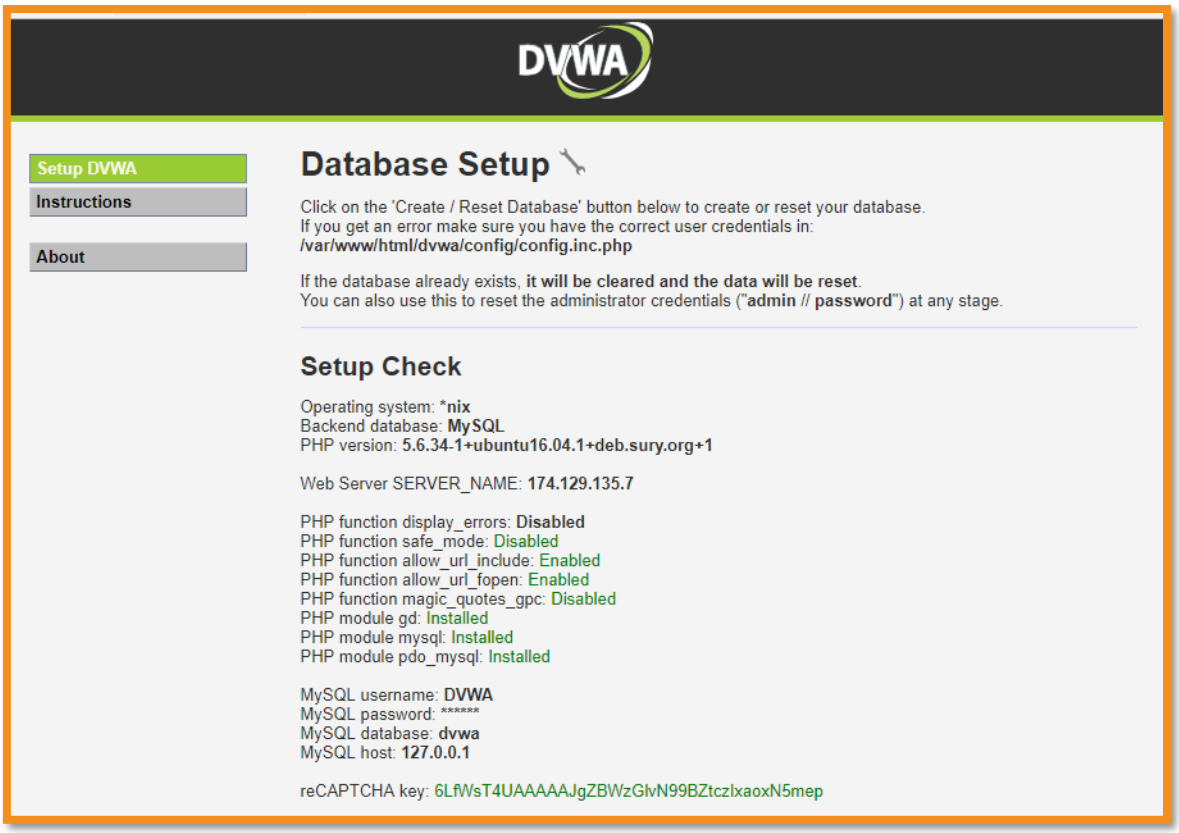
1. **Deleting http map.**
    - Go back to **Monitoring Session** in **GigaVUE-FM**, delete the links (Connector arrows) from **passall -> http** and **http -> SecOnion** also delete **http** map library.



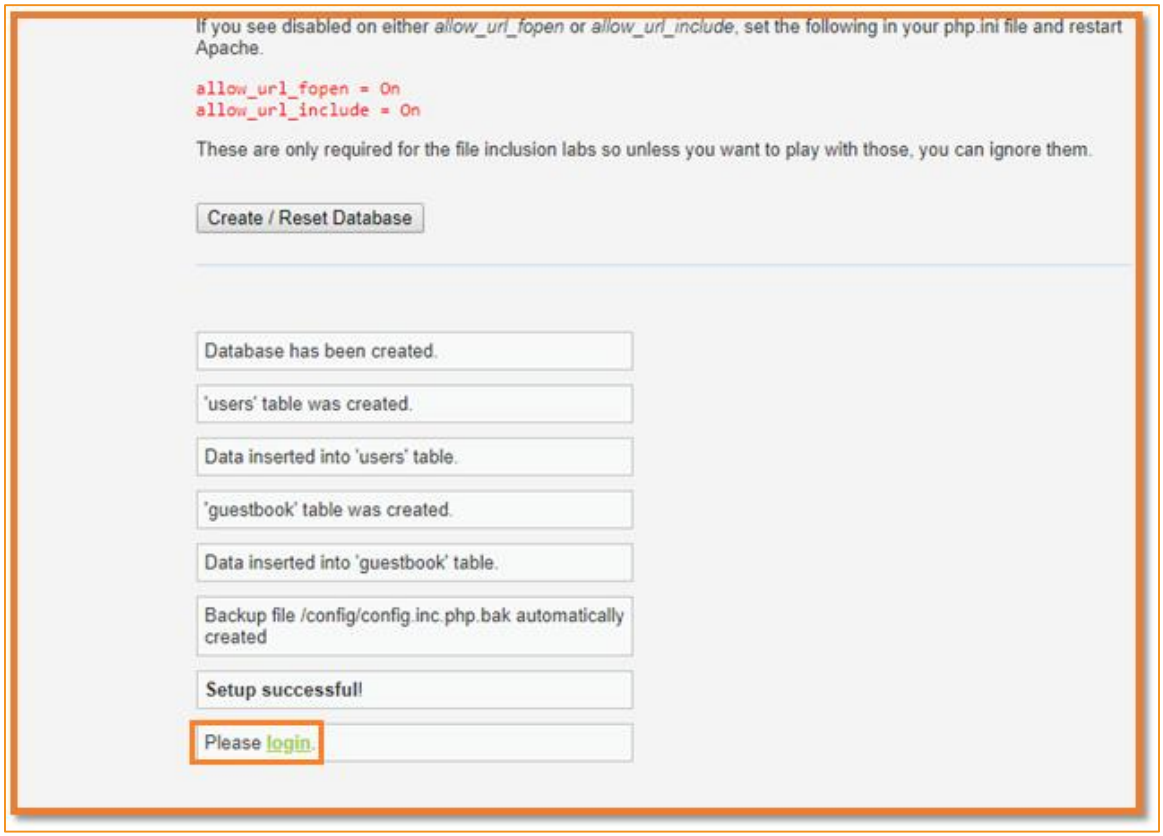
- Give connection from **passall** to **SecOnion.**
- Click **Deploy** button and click **OK**.



2. **Login to the DVWA.**
   - Open the **DVWA** by using its **url** provided in the test drive launch page.
   - Click **Create/Reset Database** button at the bottom of the **DVWA** Home page

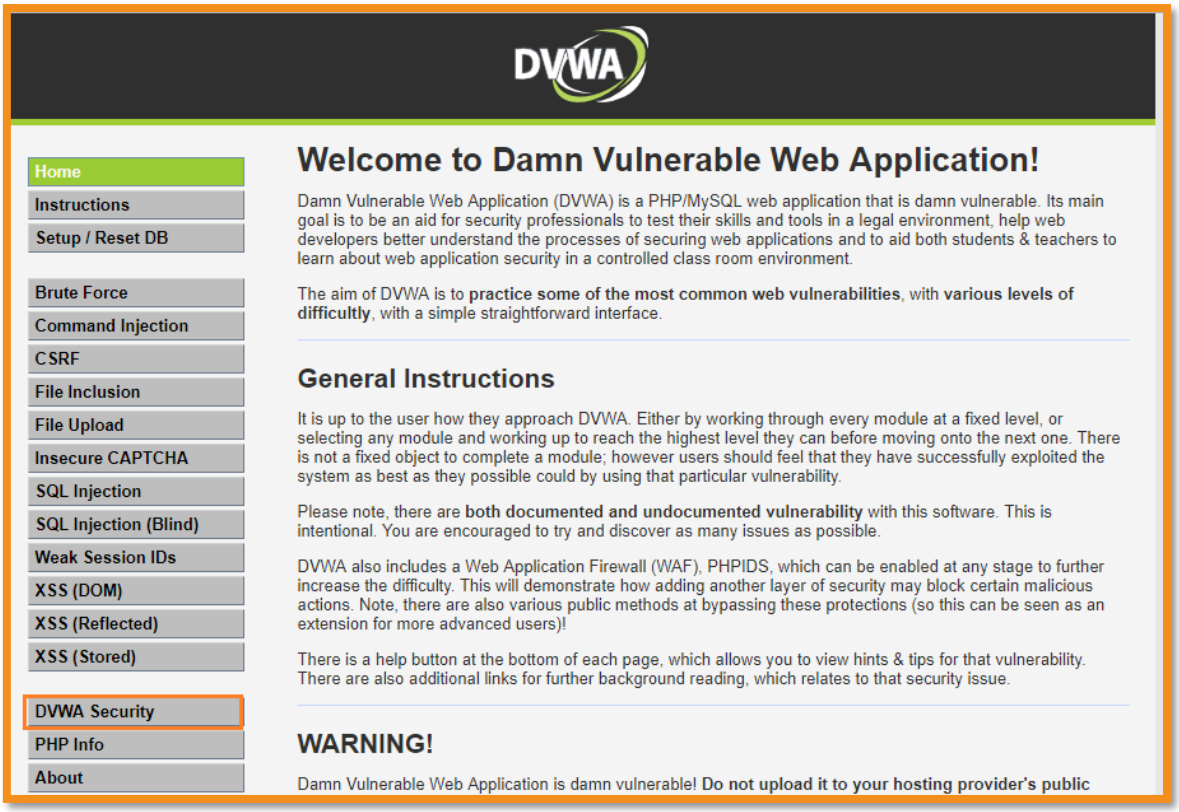


- Scroll down and click **login** as shown in the following figure.



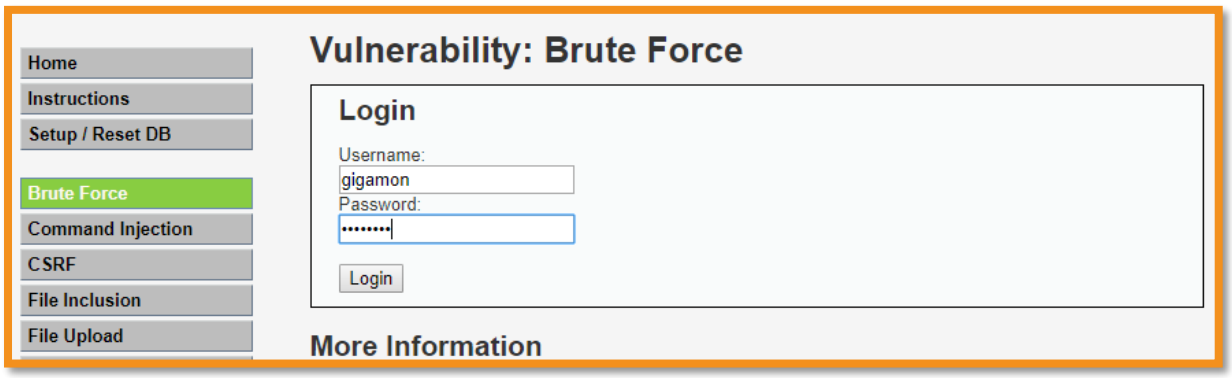
- Login to the **DVWA** by using DVWA credentials provided in the test drive launch page.

- On **DVWA** Home page, click **DVWA security** to set the Security level to low.

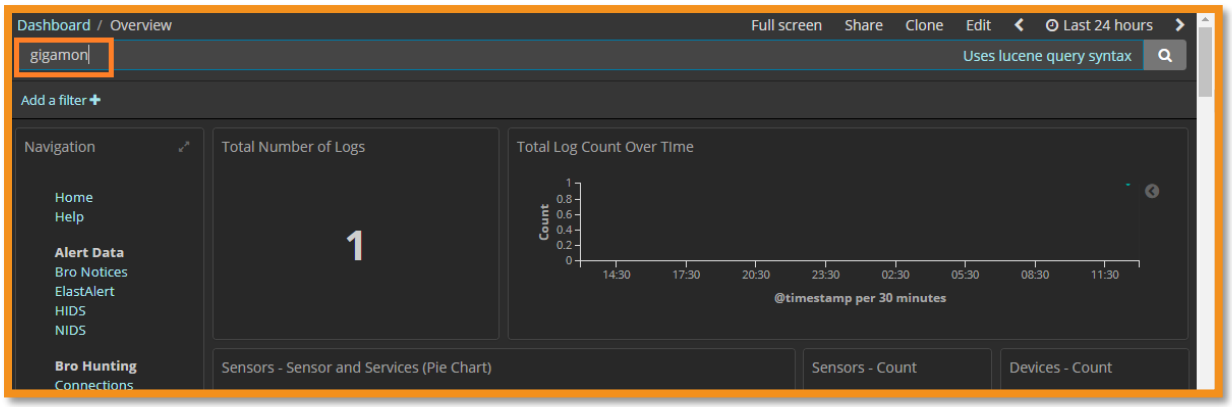


- Set Security Level to **Low** from the dropdown and click Submit as shown in the following figure.

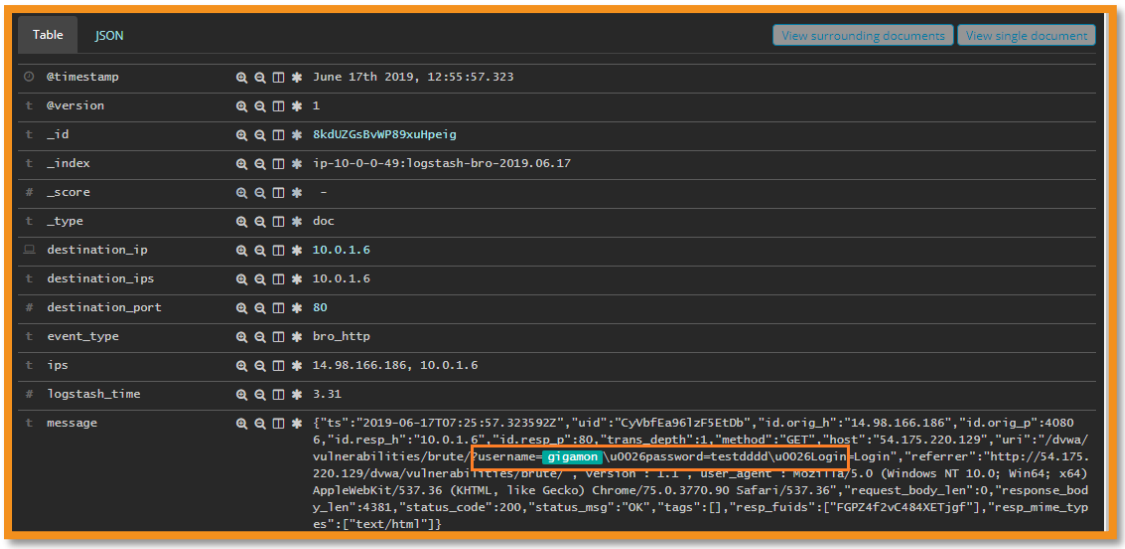
- Click **Brute Force** from the left menu of the page.
- Enter the wrong DVWA credentials to send the bad traffic.



- Go to **Kibana**, Click on **Home** and type **attacked username** or **brute** in dashboard search box.
  - To reflect the bad traffic, wait for few seconds and refresh the page.



- Scroll down the page and check the logs to see the brute force attack message.
- You can view the wrong credentials that you gave in the Brute force attack.

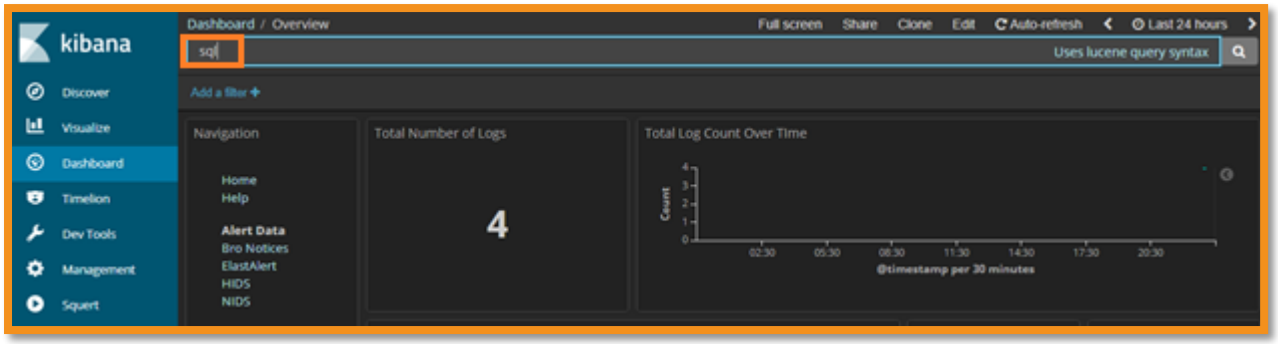


- Go back to the **DVWA** page and perform SQL injection, which is a suspicious activity.
- Click **SQL injection** from the left menu of the page.
- Enter the following SQL command.

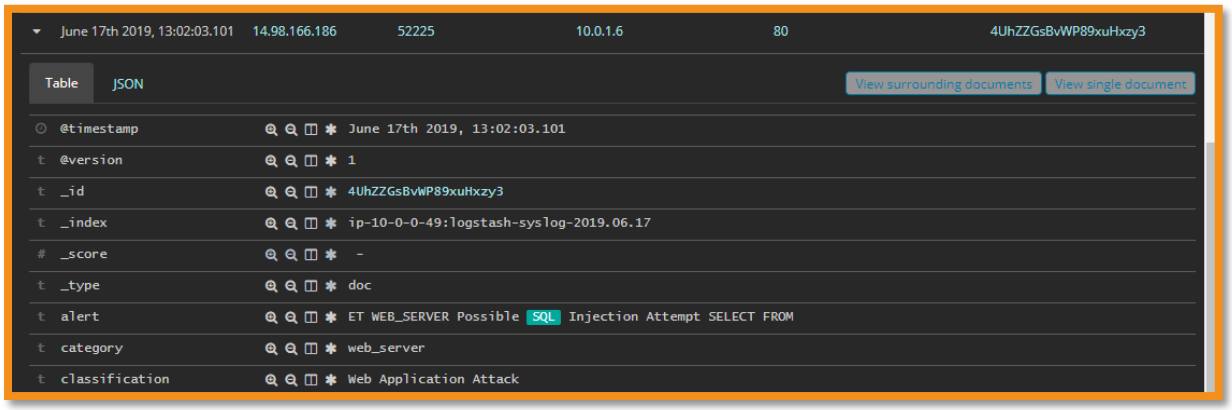
```
SELECT * FROM Users WHERE Username='1' OR '1' = '1' AND Password='1' OR '1' = '1'
```

Once you submit the page you will be navigated to another page which says “You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '1' OR '1' = '1' AND Password='1' OR '1' = '1'" at line 1”. Ignore it and continue with the next steps.

- Go to **Kibana**, and click **Home** type “**sql”** in dashboard search box.
- To reflect the bad traffic, wait for few seconds and refresh the page.



- Scroll down the page and check the logs to see the SQL injection message.



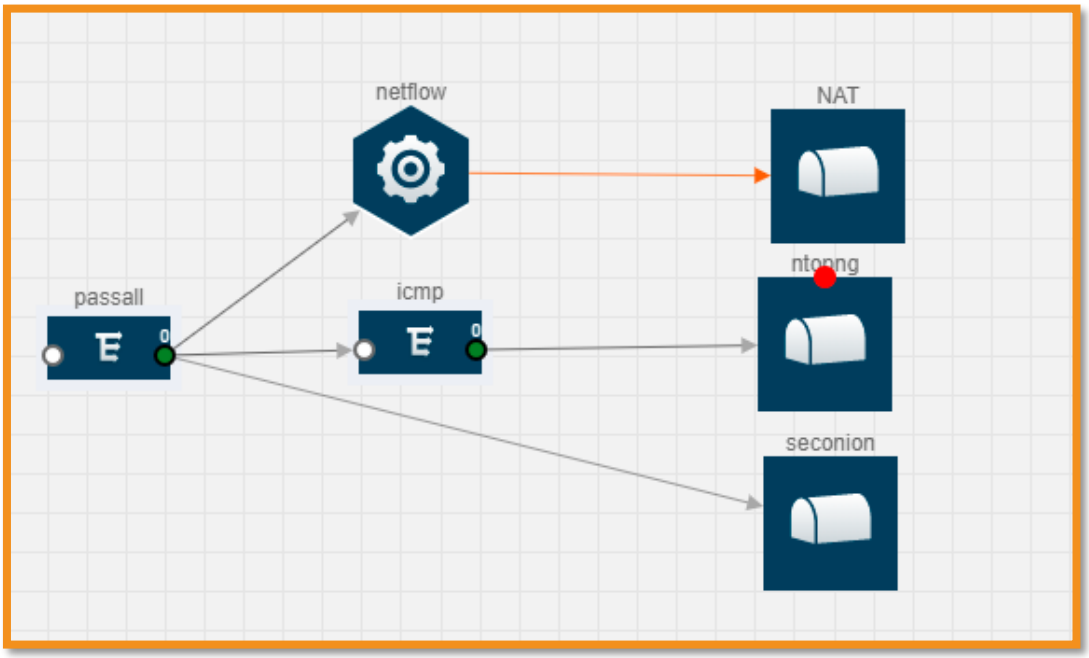
5.4. Use Case 4: GigaSMART De-Duplication

Tap and aggregation solutions collect packets from multiple points along a network path, resulting in duplicate copies being sent to your tools for analysis. Due to this you will get distorted results when evaluating application or network performance, leading to improper performance diagnosis and artificially elevated packet and byte counts.

In this use case the GigaSMART De-Duplication capabilities are demonstrated. You will analze the traffic with and with De-Duplication App to understand how the GigaSMART De-Duplication App is going to identifies and eliminates duplicate packets and sends an optimized feed to the tools.

To demonstrate the use-case, the test drive automates the generation of duplicate ICMP traffic from workload1(10.0.1.5) workload2(10.0.1.6).

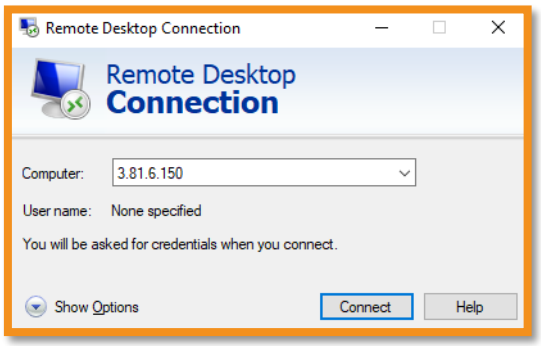
Note: The flow map is already created to send traffic to security onion as shown below



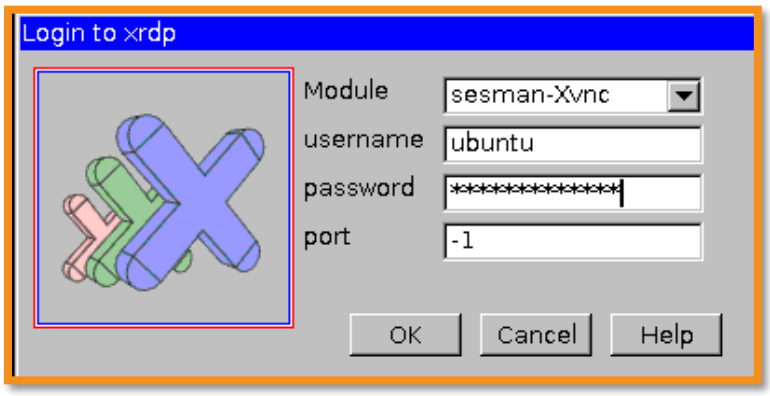
You need to perform the following steps to understand the use of GigaSMART De-Duplication App.

5.4.1. Without using De-Duplication App

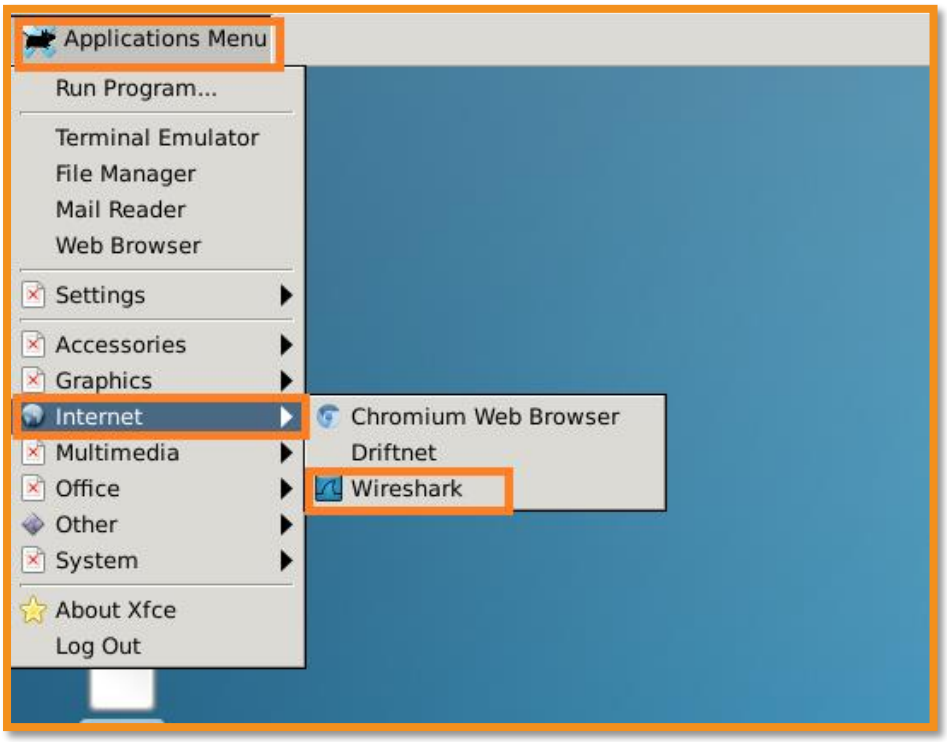
1. RDP using **Security Onion** IP address to access the **WireShark** tool as shown below.



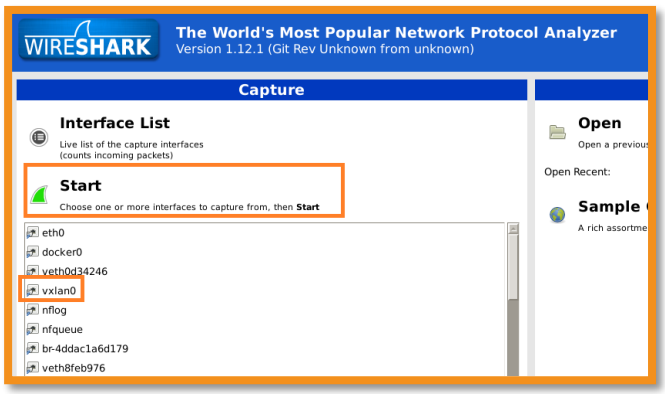
2. Enter the WireShark credentials provided in the Test drive launch page as shown below



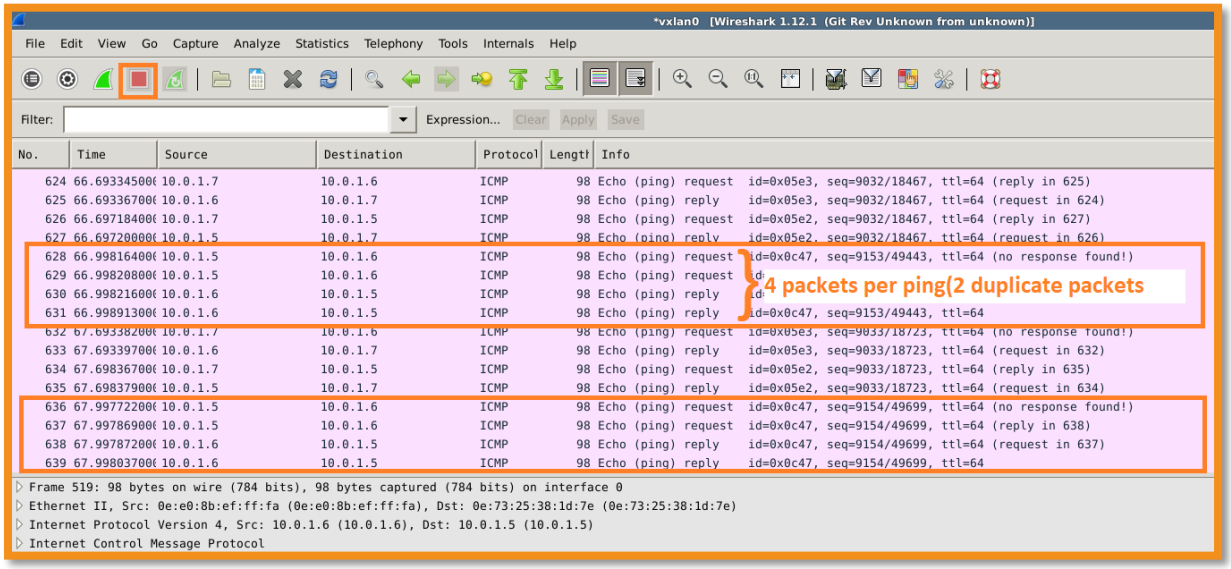
3. Once you RDP into the Wireshark tool navigate to **Applications Menu →Internet→Wireshark**



4. Select **vxlan0** and click on **Start** as shown below.

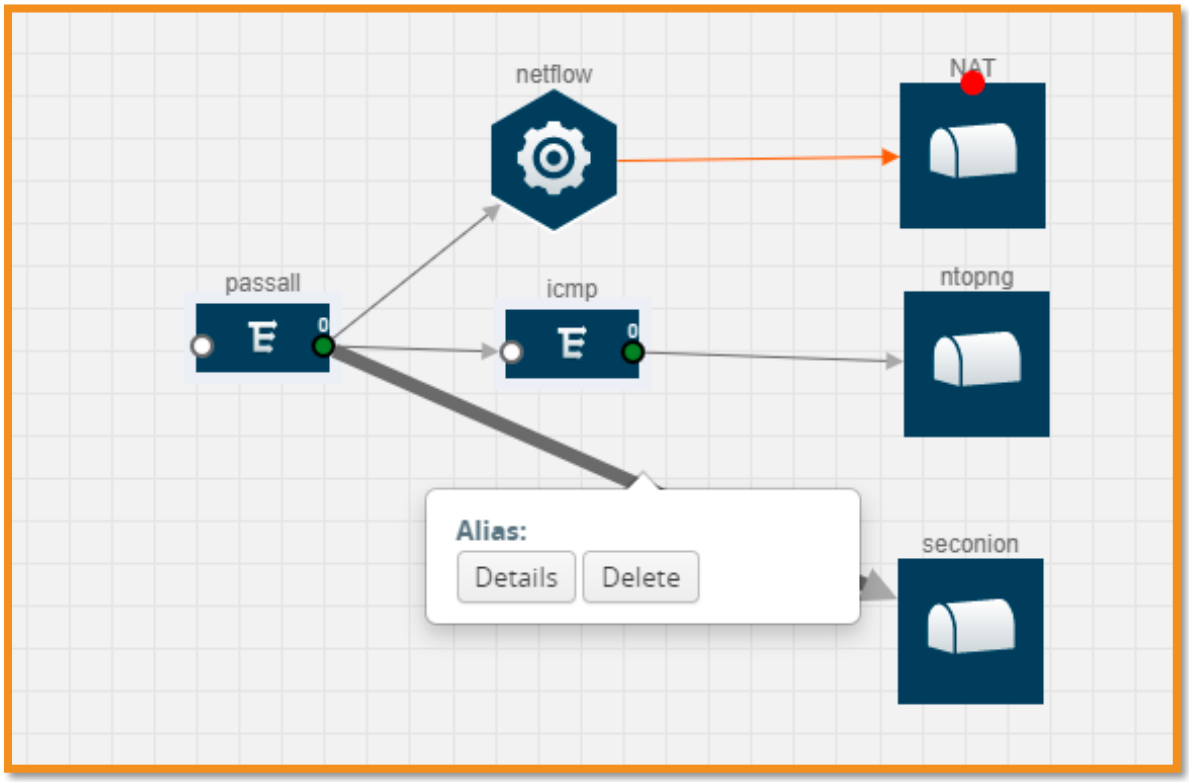


5. Click on stop and you can observe that there are **4 packets per one ping** as highlighted below.

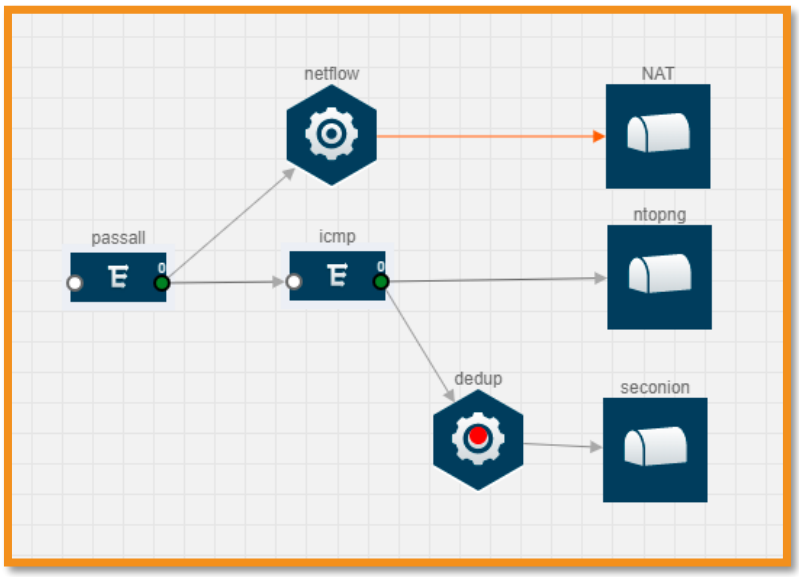


5.4.2. With using De-duplication App

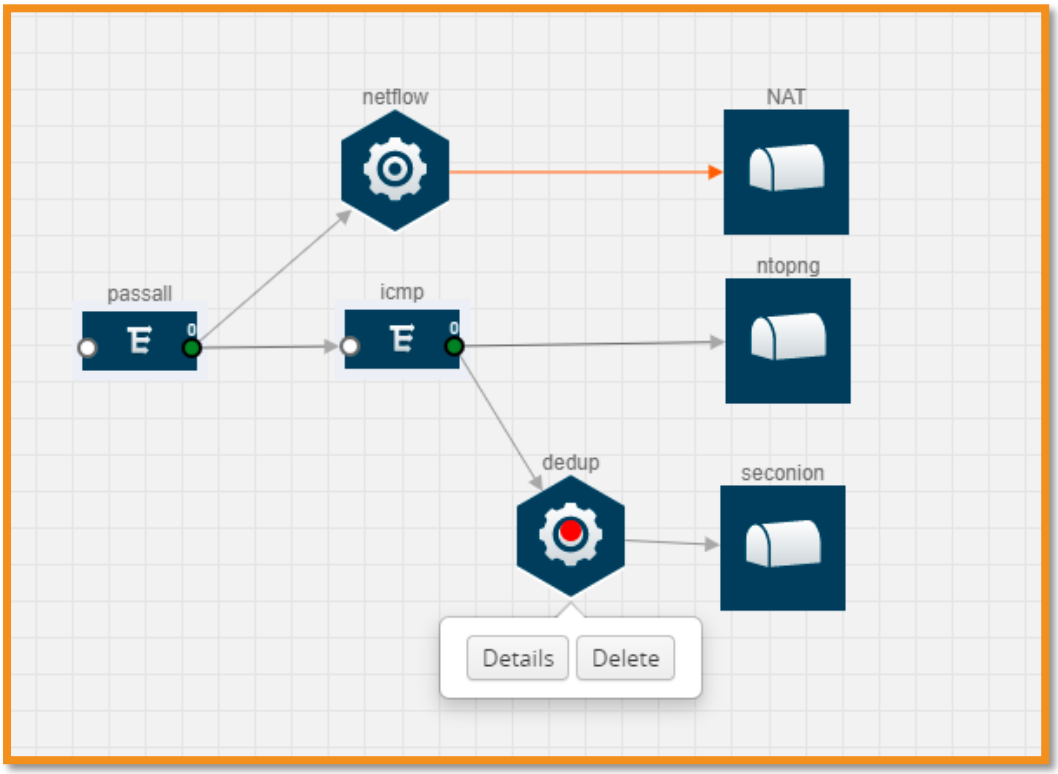
1. Go back to **Monitoring Session** in **GigaVUE-FM**, delete the links (Connector arrows) from **icmp - seconion**

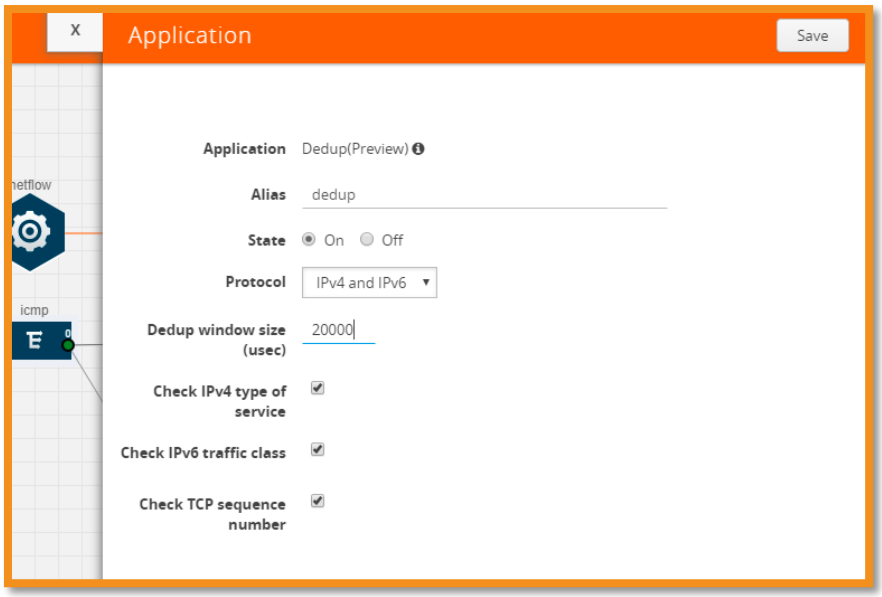


2. Drag and drop the **dedup** application from the left pane. mousehover the **ICMP** map and drag a line to connect the red dots to **Dedup,** the same way connect **Dedup** to **seconion.** Then click on **deploy.**

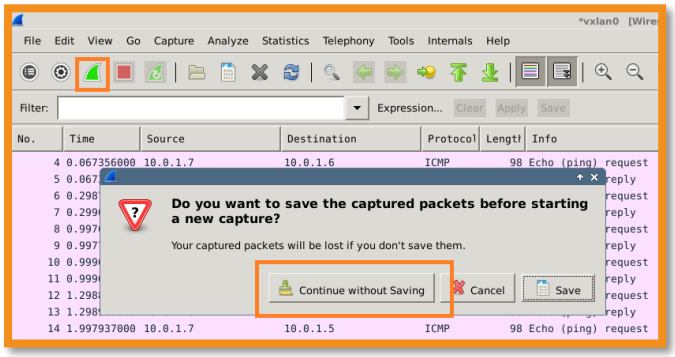


3. Click **dedup** and then click on **Details**, it will open a form. Change the value of **Dedup window size** to **20000** and click on **Save.** After saving the details click on Deploy.

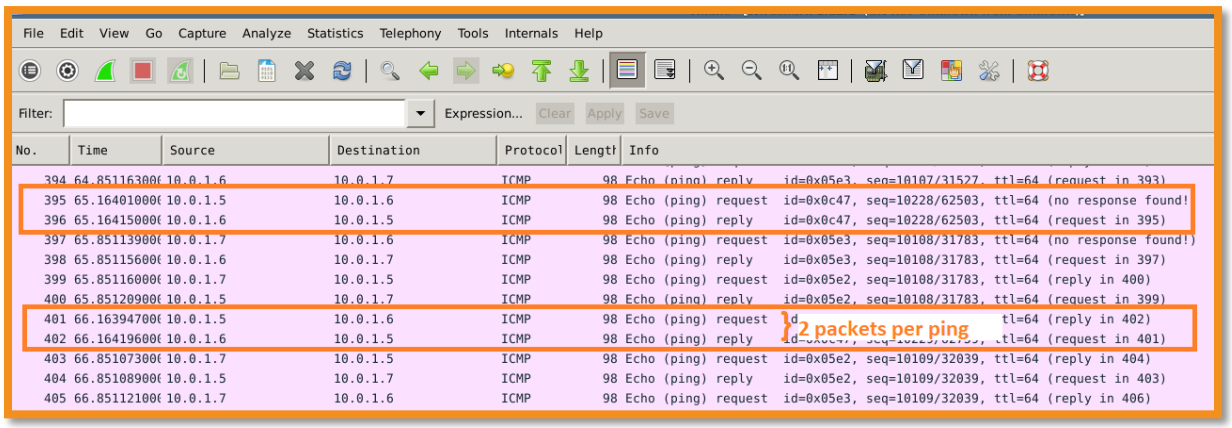




4. Go back to **Wireshark**, click on start as shown below then click on **Continue without Saving**.



5. Click on Stop as shown below, now you see only **2 packets per ping**.



GigaSMART De-duplication significantly improves the performance of connected tools, allowing them to analyze increased volumes of aggregated traffic on the network without increasing tool capital expenditure.