

GigaVUE Cloud Suite for AWS



Table of Content

1. About Test Drive.....	3
2. Introduction to the Visibility Platform for AWS	3
3. Architecture	3
4. Test Drive Environment:	4
5. Getting Started.....	4
5.1. Use Case 1: Gaining Traffic Visibility using all traffic and specific traffic Flow Maps	5
5.2. Use Case 2: Detecting Threats	17
5.3. Use Case 3: GigaSMART De-Duplication	22
5.3.1. Without using De-Duplication App.....	23
5.3.2. With using De-duplication App.....	25

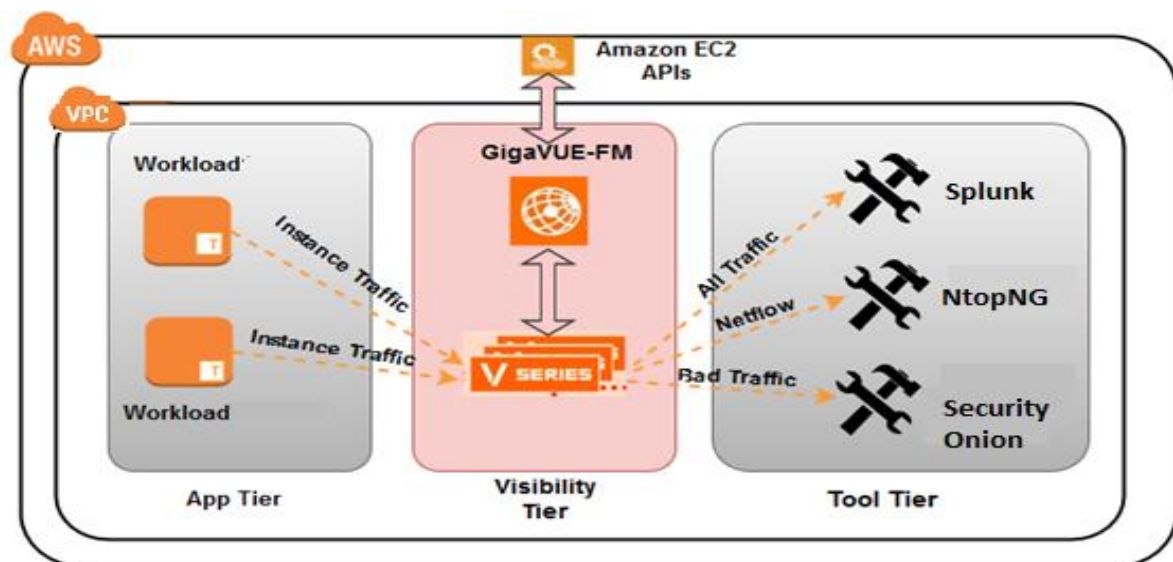
1. About Test Drive

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:

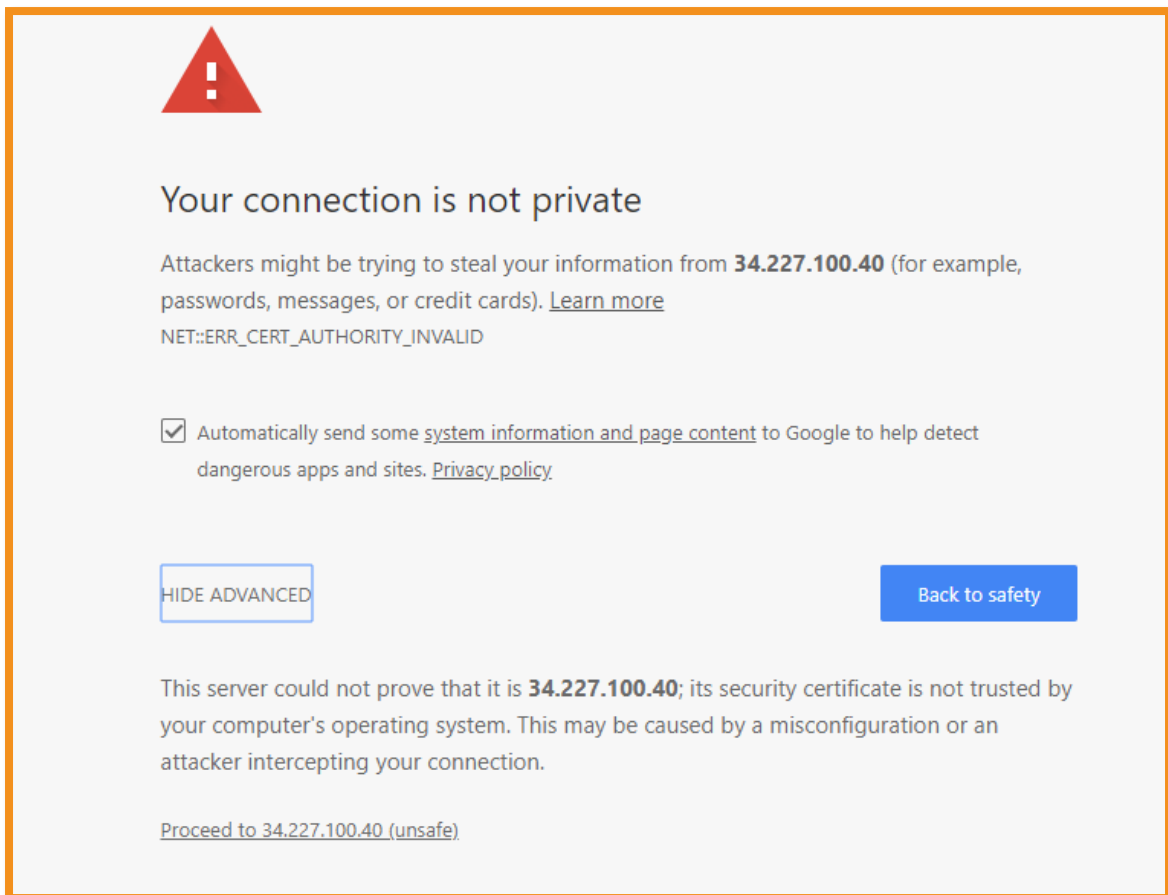
- **Use Case 1: Gaining Traffic visibility using all traffic and specific traffic Flow Maps -**
Create the flow maps to send all type of traffic into the Splunk (Netflow), and Security Onion. Then send http and icmp traffic to NtopNG using specific flow maps.
- **Use Case 2: Detecting Threats -** Send traffic to the security tool in the applications VPC to see if there is any suspicious traffic.
- **Use Case 3: 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 Traffic Visibility using all traffic and specific traffic Flow Maps

In this use case, create a flow map to send all traffic types from the workloads to the monitoring tools→ Splunk (Netflow), and Security Onion. Whereas more granular traffic such as ICMP and HTTP is sent to NtopNG.

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.



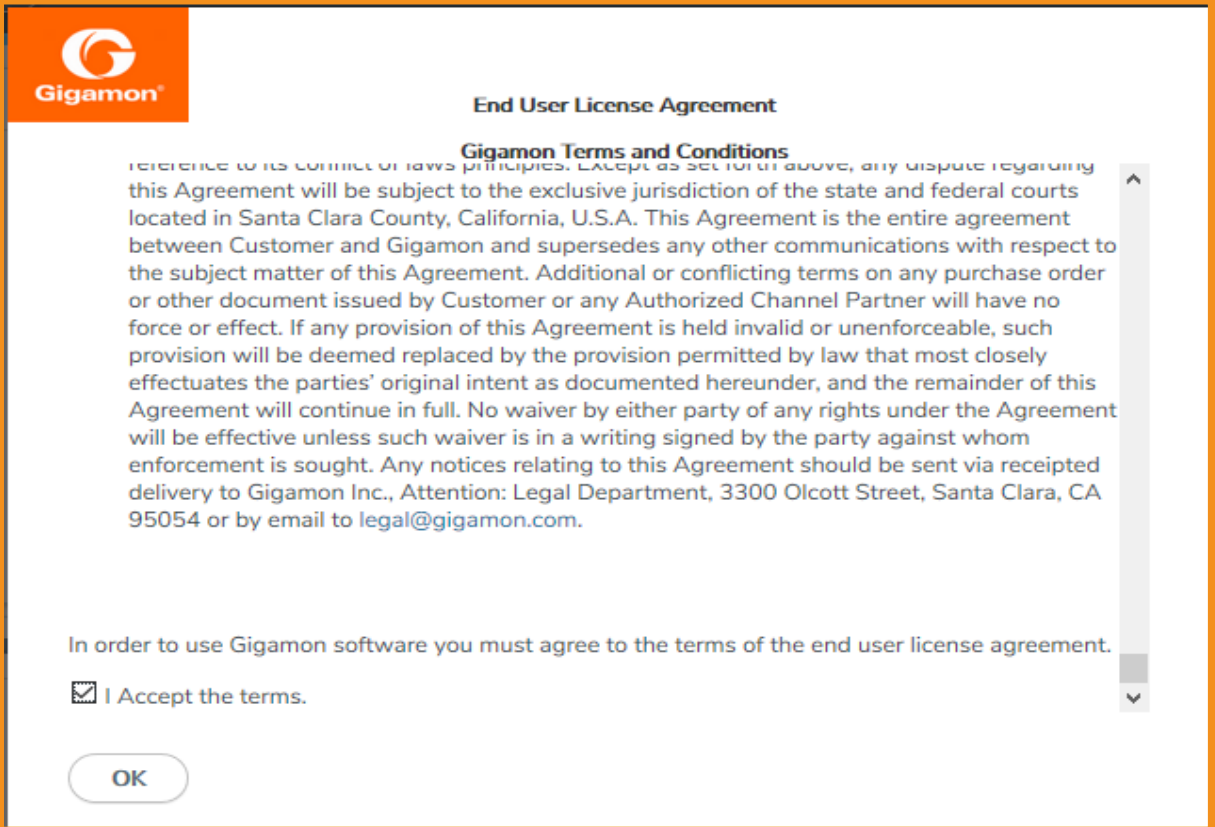
- Login to **GigaVUE-FM** with the **Username** and **Password** provided in the Test Drive launch page and click the **Log In** button.



The login screen for GigaVUE-FM features a dark blue background with an orange border. At the top left is the GigaVUE-FM logo, which consists of a globe icon and the text "GigaVUE-FM". Below the logo are two input fields: the first contains the username "admin", and the second contains a series of dots representing a password. To the right of the password field is a red "Log In" button. At the bottom, there is a placeholder text: "Placeholder for a customizable pre-login banner. Refer to the online help or user guide for customizing this banner".

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.

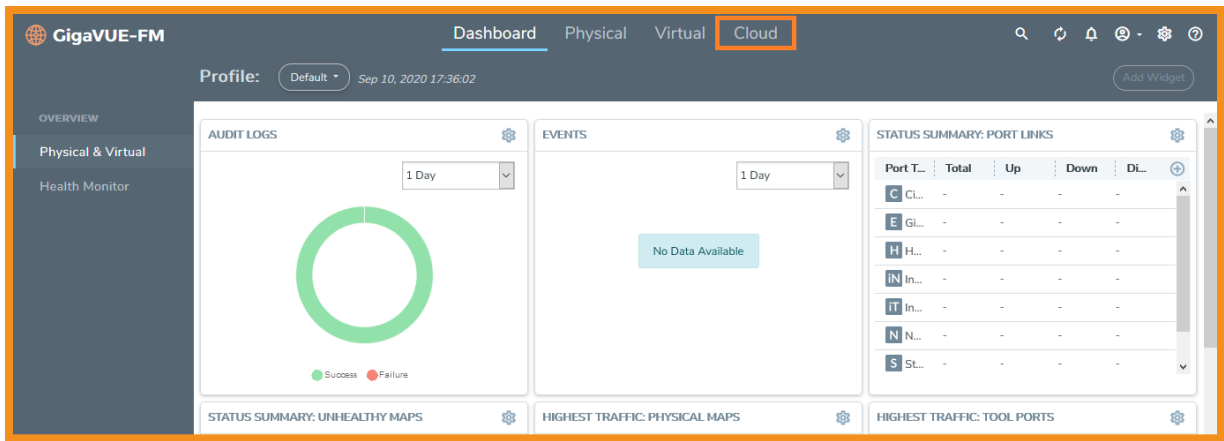
- Click **See EULA**, and scroll down to accept the terms.



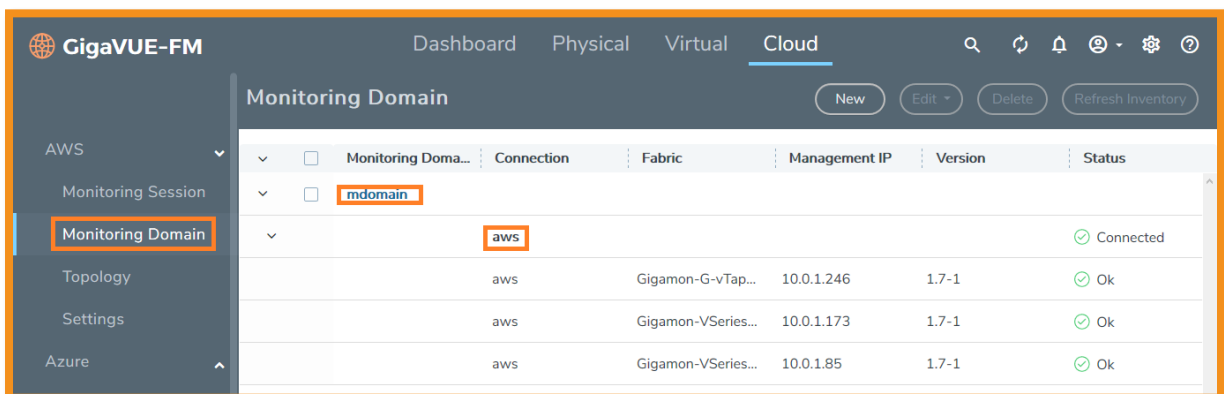
The End User License Agreement (EULA) window for Gigamon features a white background with an orange border. In the top left corner is the Gigamon logo. The title "End User License Agreement" is centered at the top. Below the title is the section "Gigamon Terms and Conditions". The main body of the agreement contains the following text: "reference to its contract or laws principles. Except as set forth above, any dispute regarding this Agreement will be subject to the exclusive jurisdiction of the state and federal courts located in Santa Clara County, California, U.S.A. This Agreement is the entire agreement between Customer and Gigamon and supersedes any other communications with respect to the subject matter of this Agreement. Additional or conflicting terms on any purchase order or other document issued by Customer or any Authorized Channel Partner will have no force or effect. If any provision of this Agreement is held invalid or unenforceable, such provision will be deemed replaced by the provision permitted by law that most closely effectuates the parties' original intent as documented hereunder, and the remainder of this Agreement will continue in full. No waiver by either party of any rights under the Agreement will be effective unless such waiver is in a writing signed by the party against whom enforcement is sought. Any notices relating to this Agreement should be sent via receipted delivery to Gigamon Inc., Attention: Legal Department, 3300 Olcott Street, Santa Clara, CA 95054 or by email to legal@gigamon.com."

Below the agreement text, it states: "In order to use Gigamon software you must agree to the terms of the end user license agreement." This is followed by a checkbox labeled "I Accept the terms." which is checked. At the bottom left is an "OK" button. On the right side, there is a vertical scrollbar with up and down arrows.

- 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.

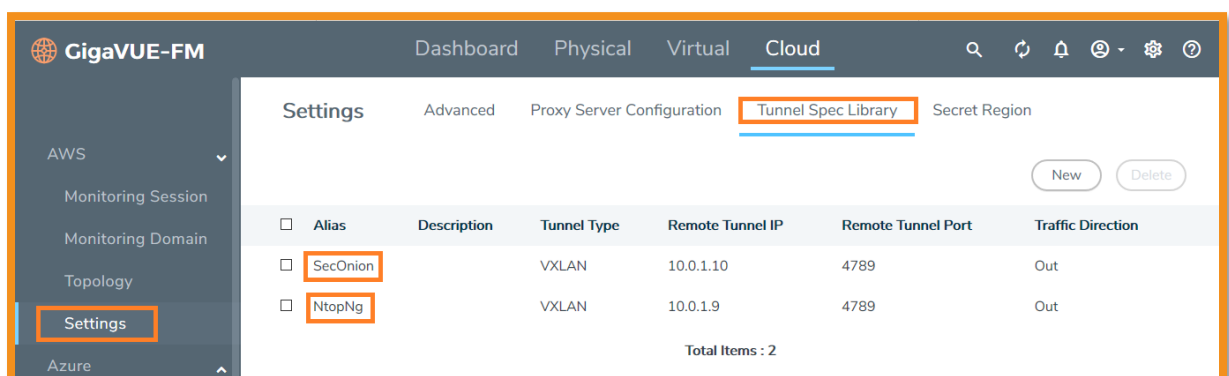


- Navigate to **Monitoring Domain** under **AWS** from the left menu. Here you can see that monitoring domain(**mdomain**) and a AWS connection (**aws**) is already created for testdrive.



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

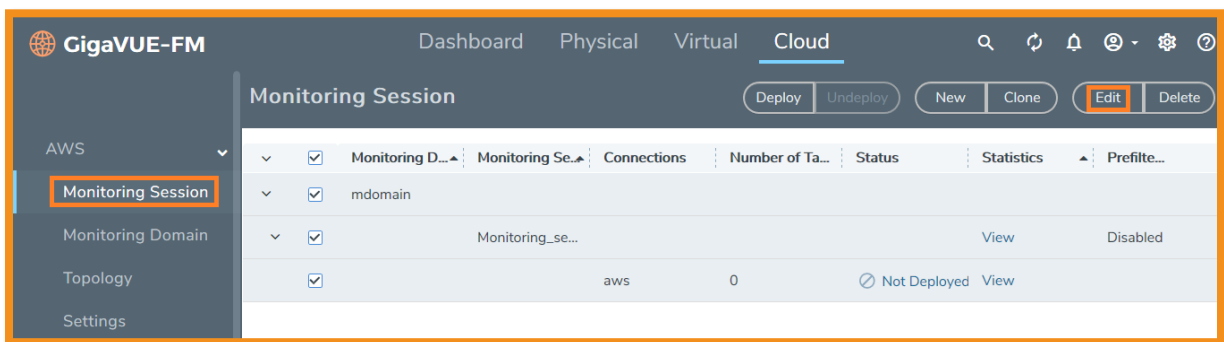
NOTE: A standard Vxlan tunnel is established to distribute the customized traffic from the V Series node to the monitoring tools.



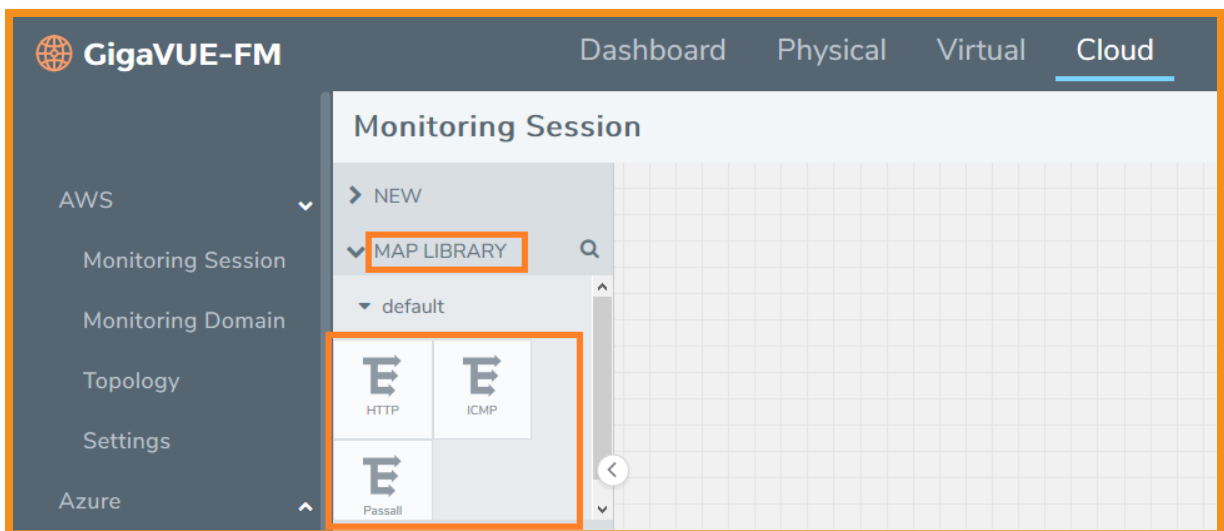
- Click **Monitoring Session** option from the left menu to open the **Monitoring Session** page.

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.

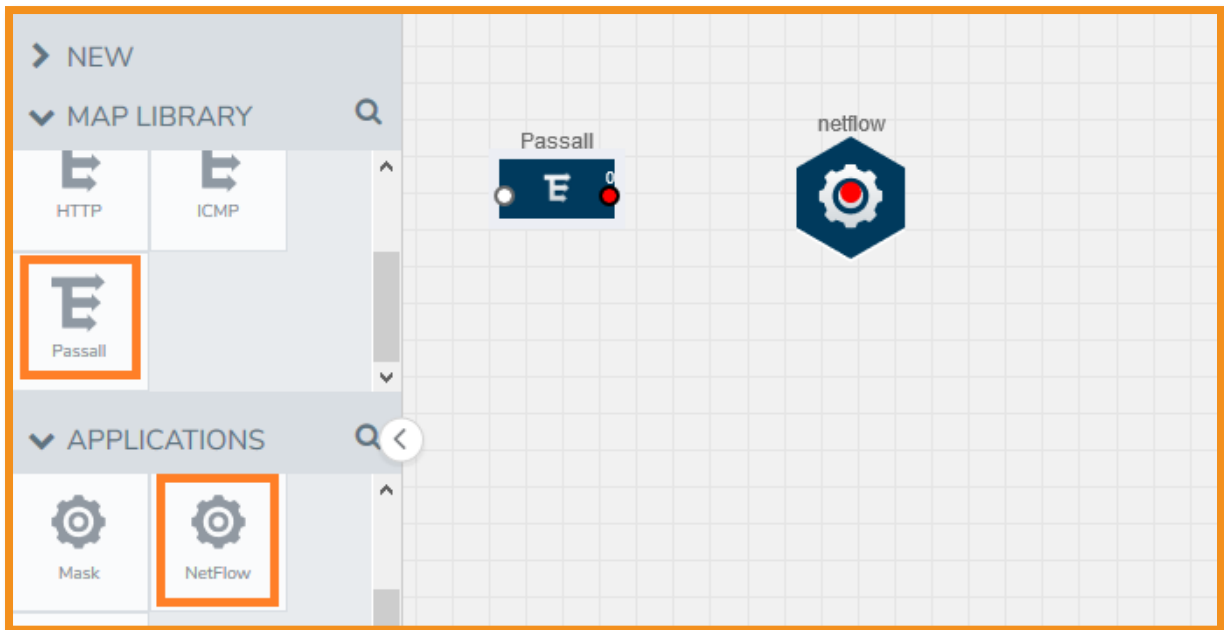


- In this Monitoring Session, the maps (**Passall, ICMP and HTTP**) are already created in the **Map library**.

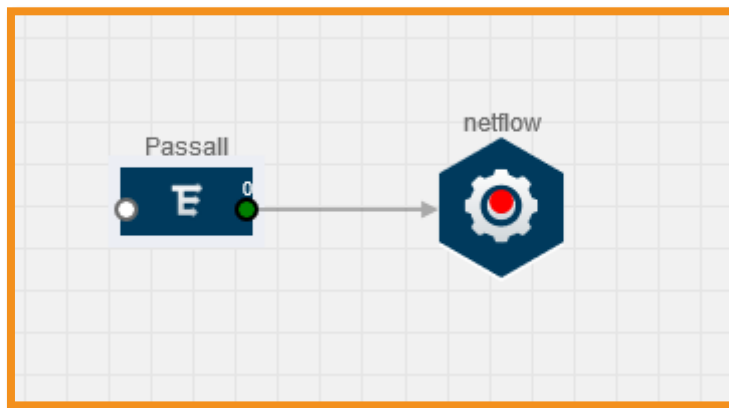


2. Creating a flow map.

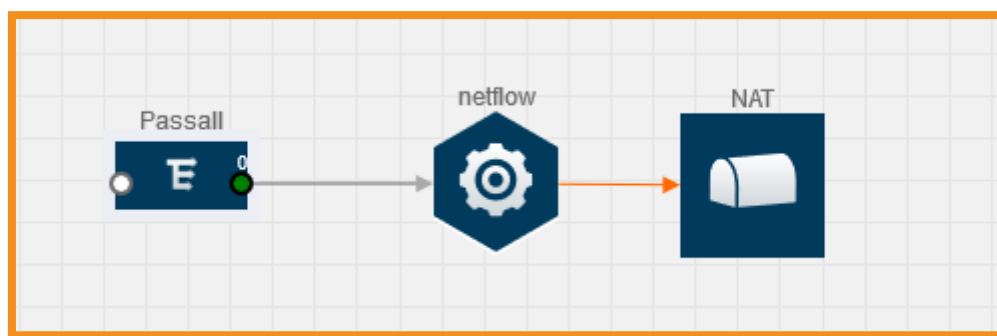
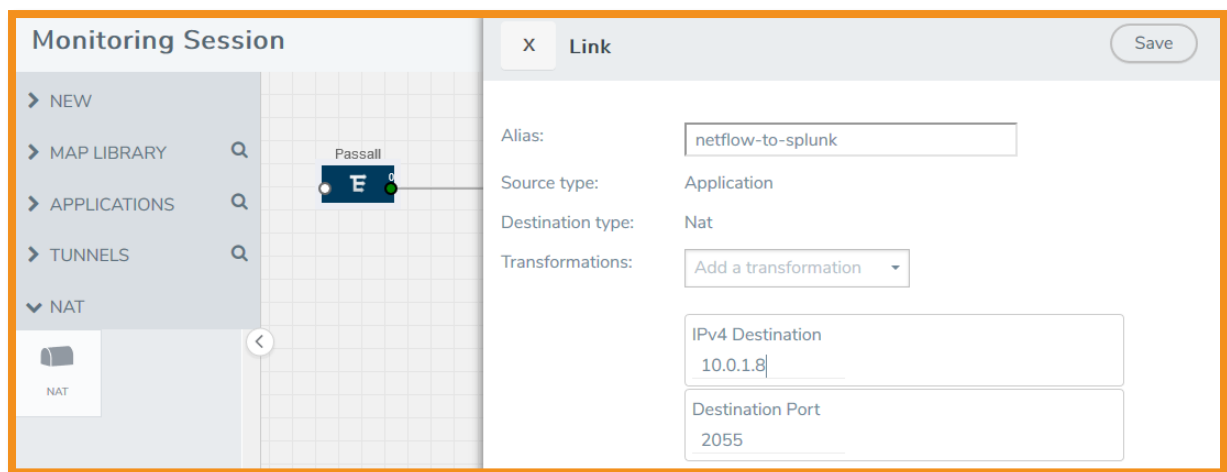
- Drag and drop the **Passall** map from the **MAP LIBRARY** section and **Netflow** from **APPLICATIONS** section to the empty map area.



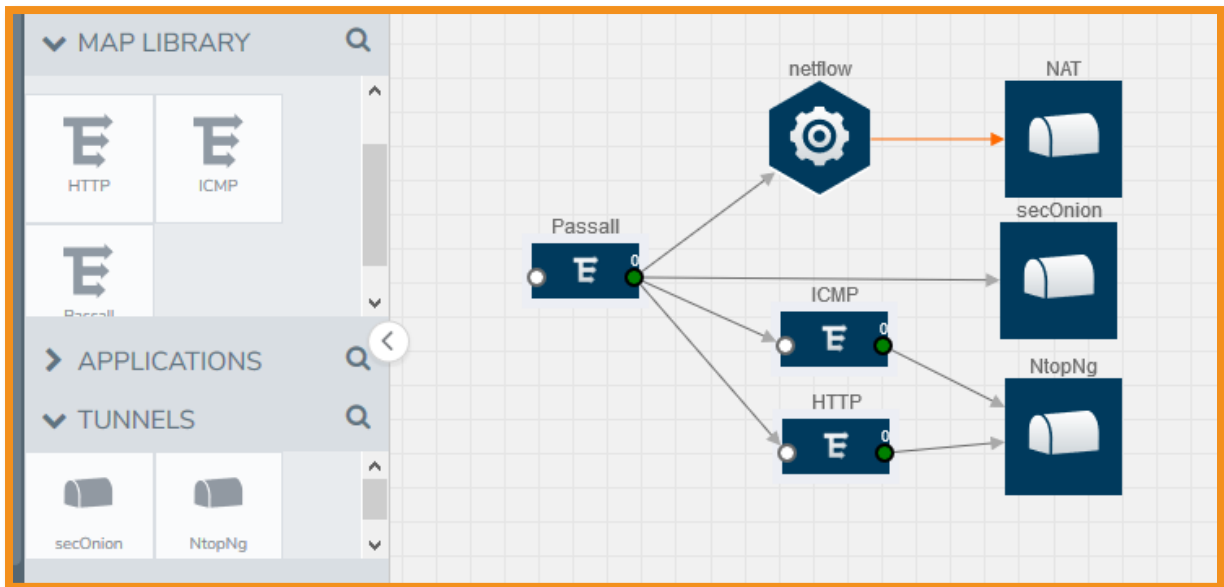
- Hover over the **Passall** map and drag a line to connect the red dots from the **Passall** map to the **Netflow** application.



- 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** section.
- Drag and Drop the **ICMP** and **HTTP** maps from the **MAP LIBRARY**
- Hover over the **Passall** and drag a line to connect the red dots to **SecOnion**.
- Hover over the **Passall** map and drag a line to connect the red dots to **HTTP** map and **ICMP** map.
- Hover over the **HTTP** and **ICMP** maps and drag a line to connect the red dots to **NtopNG** tunnel
- Once you have completed above steps, your configuration will look as shown in the following diagram,

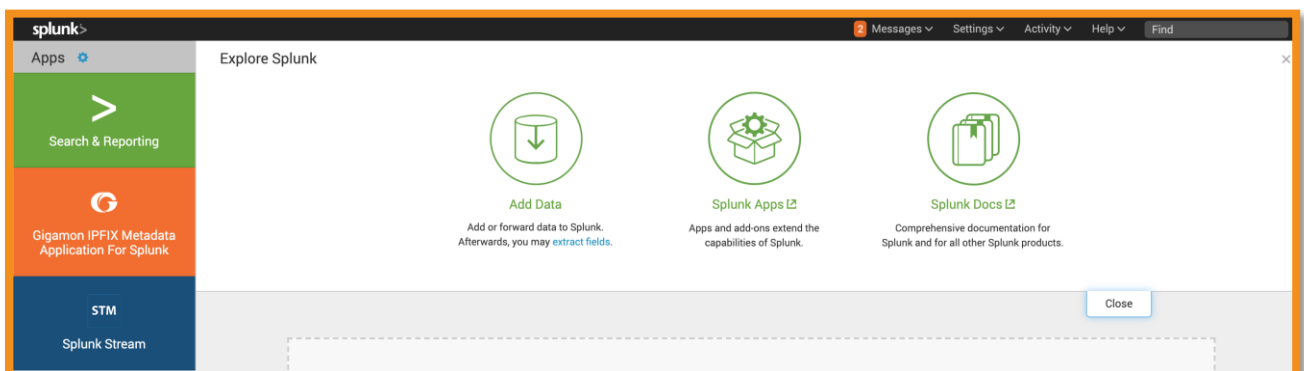


- Click **Deploy** button. Now the traffic starts flowing to the **Splunk**, **NtopNG** and **SecurityOnion**.

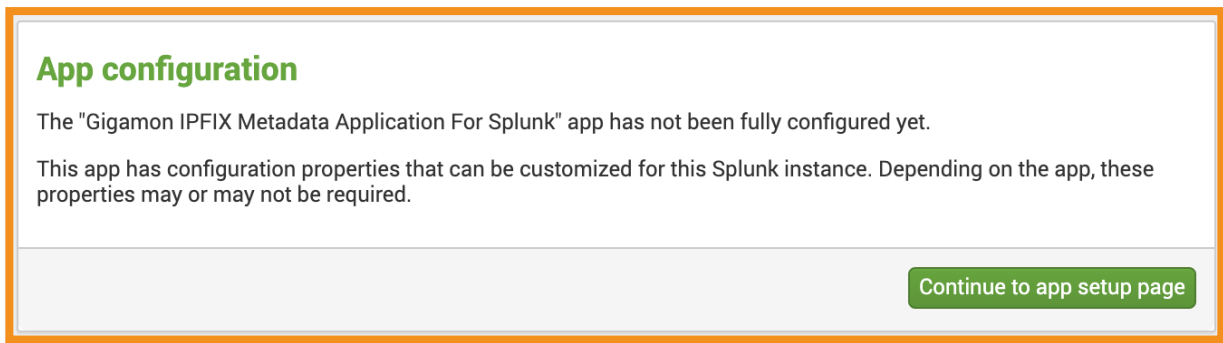
Monitoring Session							
<div> Deploy Undeploy New Clone Edit Delete </div>							
▼	<input type="checkbox"/>	Monitoring D...	Monitoring Se...	Connections	Number of Ta...	Status	Statistics
▼	<input type="checkbox"/>	mdomain					
▼	<input type="checkbox"/>	Monitoring_se...					View
	<input type="checkbox"/>		aws	2	✓ Success	View	Enabled

3. Login to the Splunk

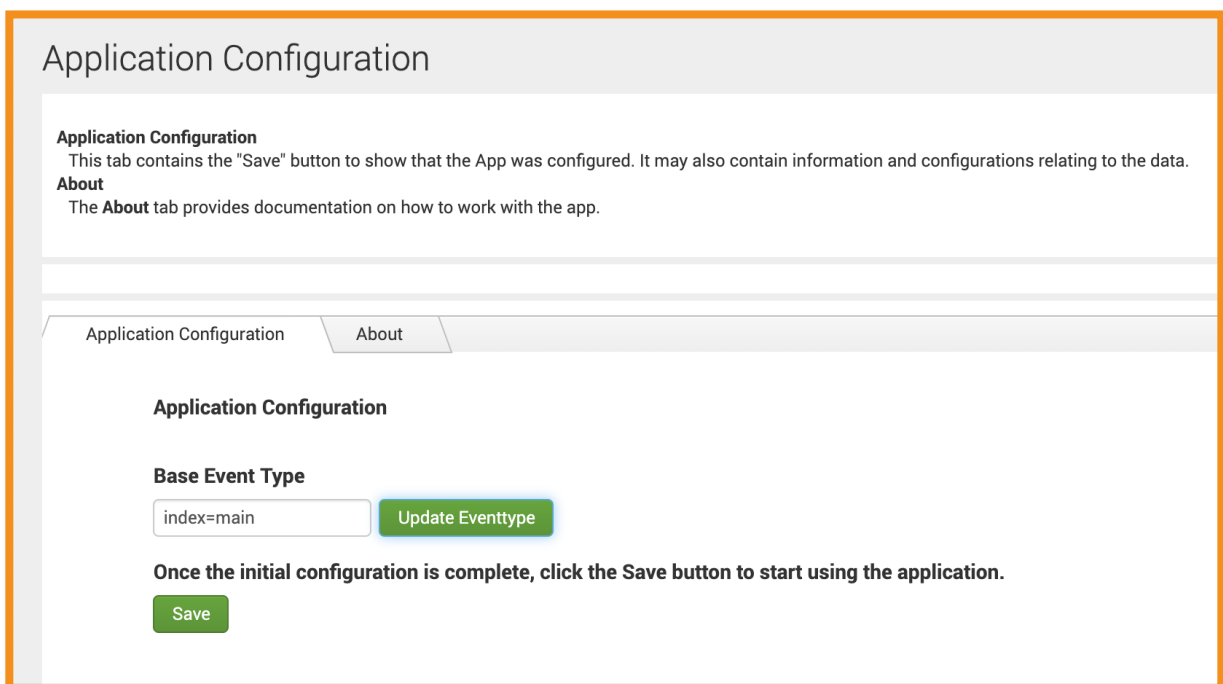
- Go to **Splunk Enterprise** by using its **Splunk web url** provided in test drive launch page.
- Click **Gigamon IPFIX Metadata Application For Splunk** on left menu.



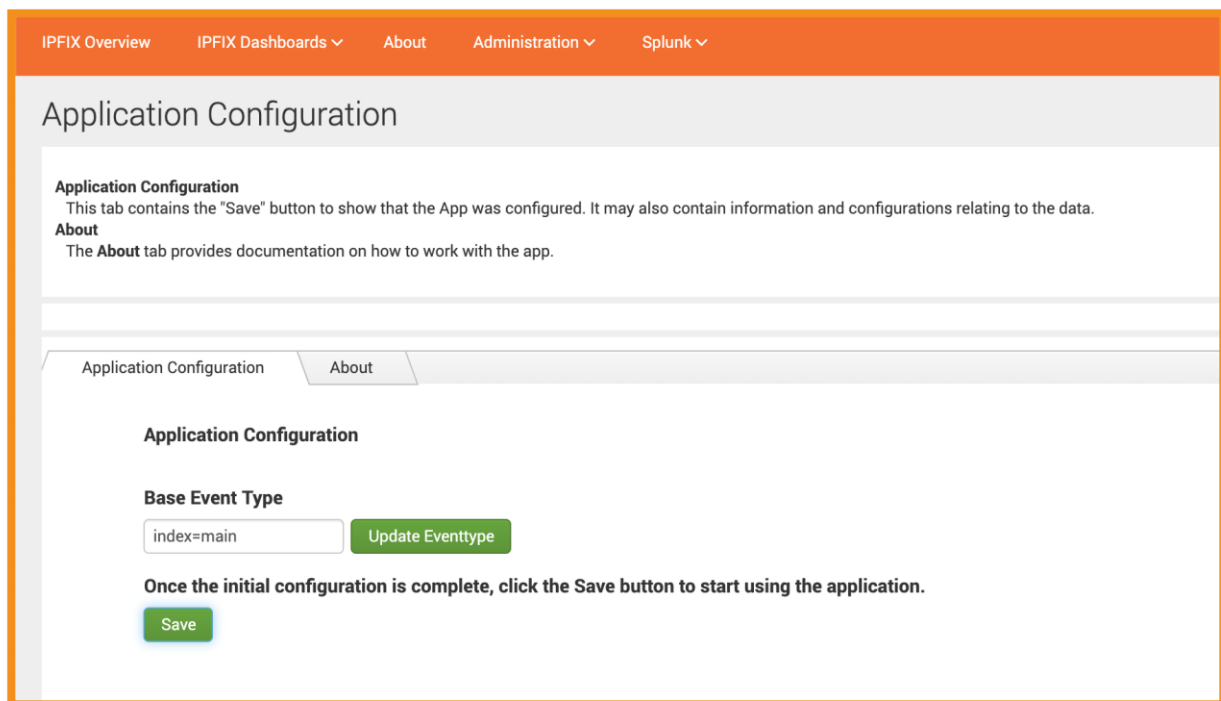
- Click **Continue app setup page** button as shown in the following figure.



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

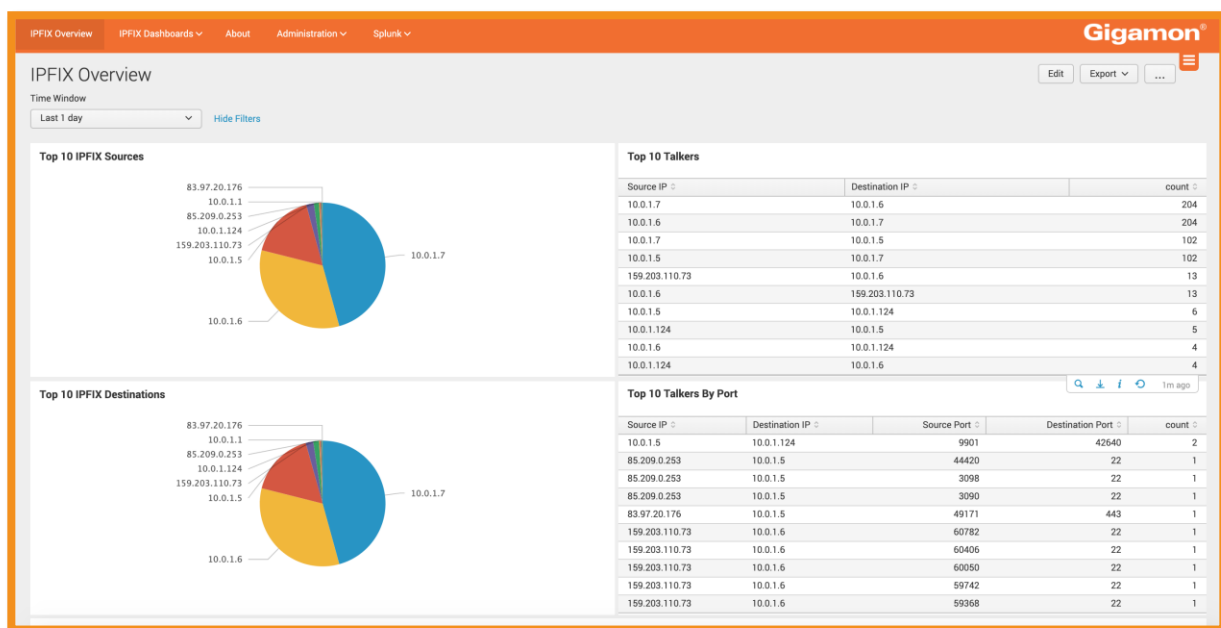


- Click **IPFIX Overview** from the top menu as shown in the following figure.



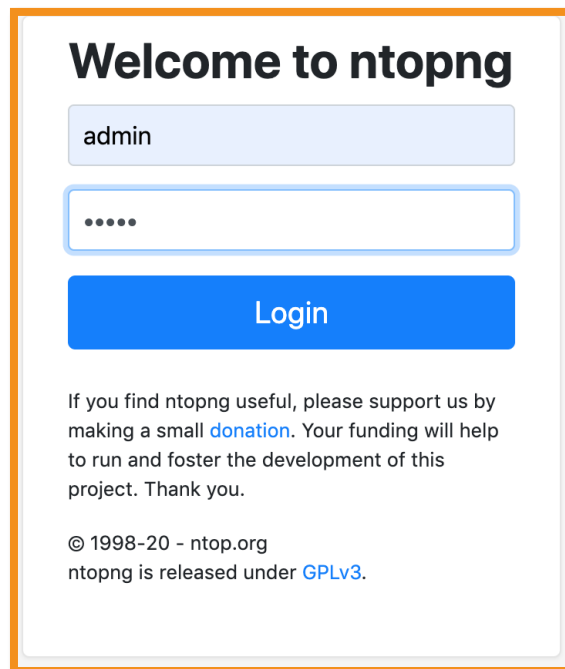
- In the **IPFIX Overview** page you can see the Netflow data as shown in the following figure.

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 access information via mail test drive launch page.



The image shows the NtopNG login interface. It has a title 'Welcome to ntopng'. Below the title are two input fields: the first contains the text 'admin' and the second contains five dots, representing a password. Below these fields is a blue button labeled 'Login'. Under the button, there is a paragraph of text: 'If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.' At the bottom, it says '© 1998-20 - ntop.org' and 'ntopng is released under [GPLv3](#)'.

Welcome to ntopng

admin

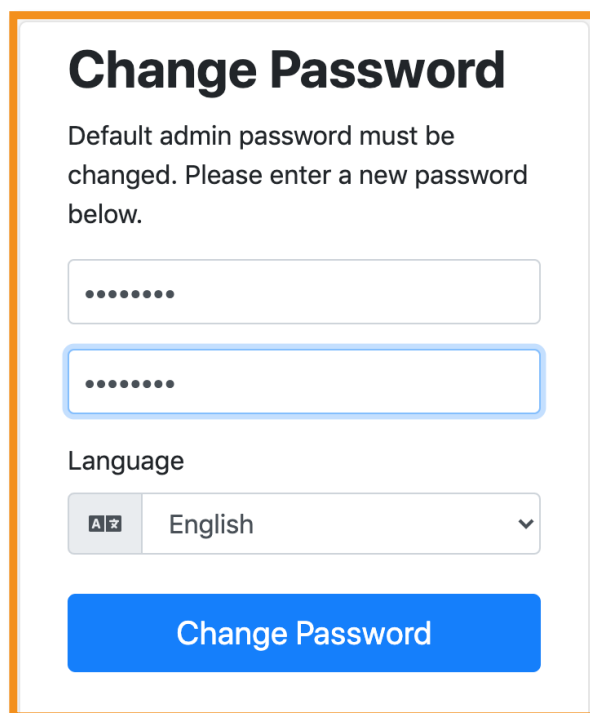
.....

Login

If you find ntopng useful, please support us by making a small [donation](#). Your funding will help to run and foster the development of this project. Thank you.

© 1998-20 - ntop.org
ntopng is released under [GPLv3](#).

- Change the **Password** form the change password page.



The image shows the 'Change Password' form. It has a title 'Change Password'. Below the title is a paragraph: 'Default admin password must be changed. Please enter a new password below.' There are two password input fields, each with seven dots. Below the fields is a 'Language' section with a dropdown menu showing 'English' and a small icon of a document with a checkmark. At the bottom is a blue button labeled 'Change Password'.


Change Password

Default admin password must be changed. Please enter a new password below.

.....

.....

Language

 English

Change Password

- In **NtopNG Traffic Dashboard** under **Flows**, you can view the intended **HTTP** and **ICMP** traffic flows are being received as configured in monitoring session.



	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	ICMP	ICMP	ip-10-0-1-6.ec2.internal...	ip-10-0-1-5.ec2.internal...	15:20	Client Server	3.10 kbit/s ↓	352.28 KB ↑	Echo
Info	ICMP	ICMP	ip-10-0-1-7.ec2.internal...	ip-10-0-1-6.ec2.internal...	15:20	Client Server	1.60 kbit/s ↓	176.29 KB ↑	Echo Reply
Info	ICMP	ICMP	ip-10-0-1-7.ec2.internal...	ip-10-0-1-5.ec2.internal...	15:20	Client Server	1.60 kbit/s ↓	176.29 KB ↑	Echo Reply
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:49706	10.0.1.5:http	< 1 sec	Client	0 bps	542.00 Bytes	10.0.1.5
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:49700	10.0.1.5:http	< 1 sec	Client	0 bps	542.00 Bytes	10.0.1.5
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:59860	10.0.1.6:http	< 1 sec	Client	0 bps	542.00 Bytes	10.0.1.6
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:49712	10.0.1.5:http	< 1 sec	Client	0 bps	542.00 Bytes	10.0.1.5
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:59876	10.0.1.6:http	< 1 sec	Client	0 bps	533.00 Bytes	10.0.1.6
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:59870	10.0.1.6:http	< 1 sec	Client	0 bps	533.00 Bytes	10.0.1.6
Info	HTTP	TCP	ip-10-0-1-7.ec2.internal...:59864	10.0.1.6:http	< 1 sec	Client	0 bps	533.00 Bytes	10.0.1.6

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.

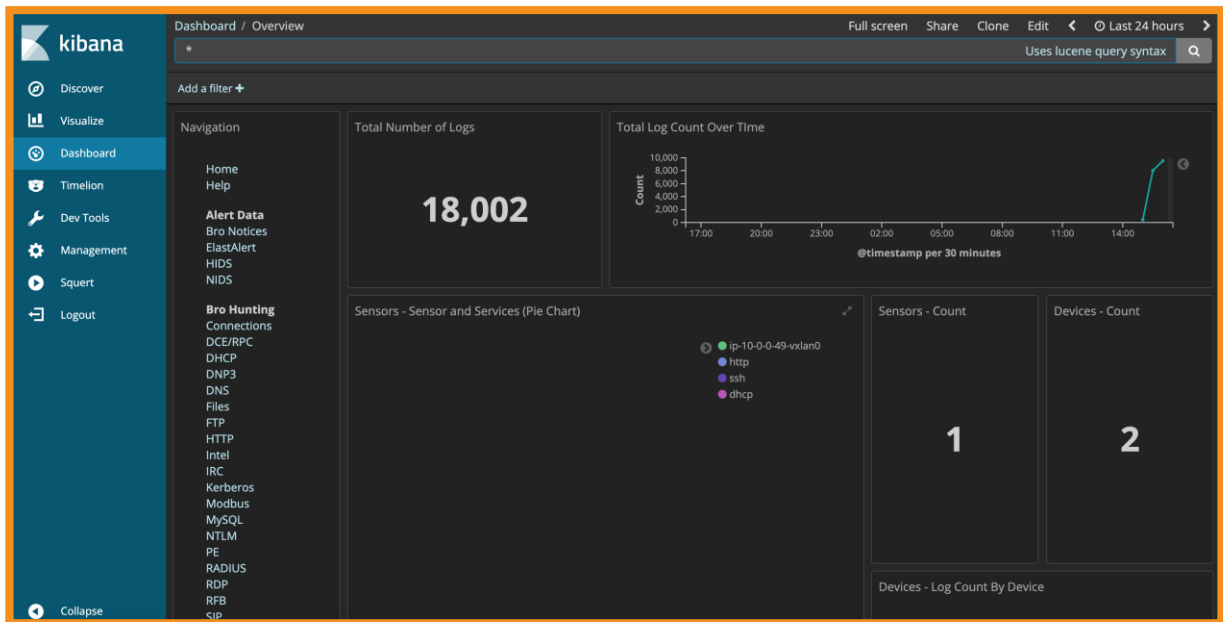


- Login to the **elastic** using the **Kibana** credentials provided in the test drive launch page.

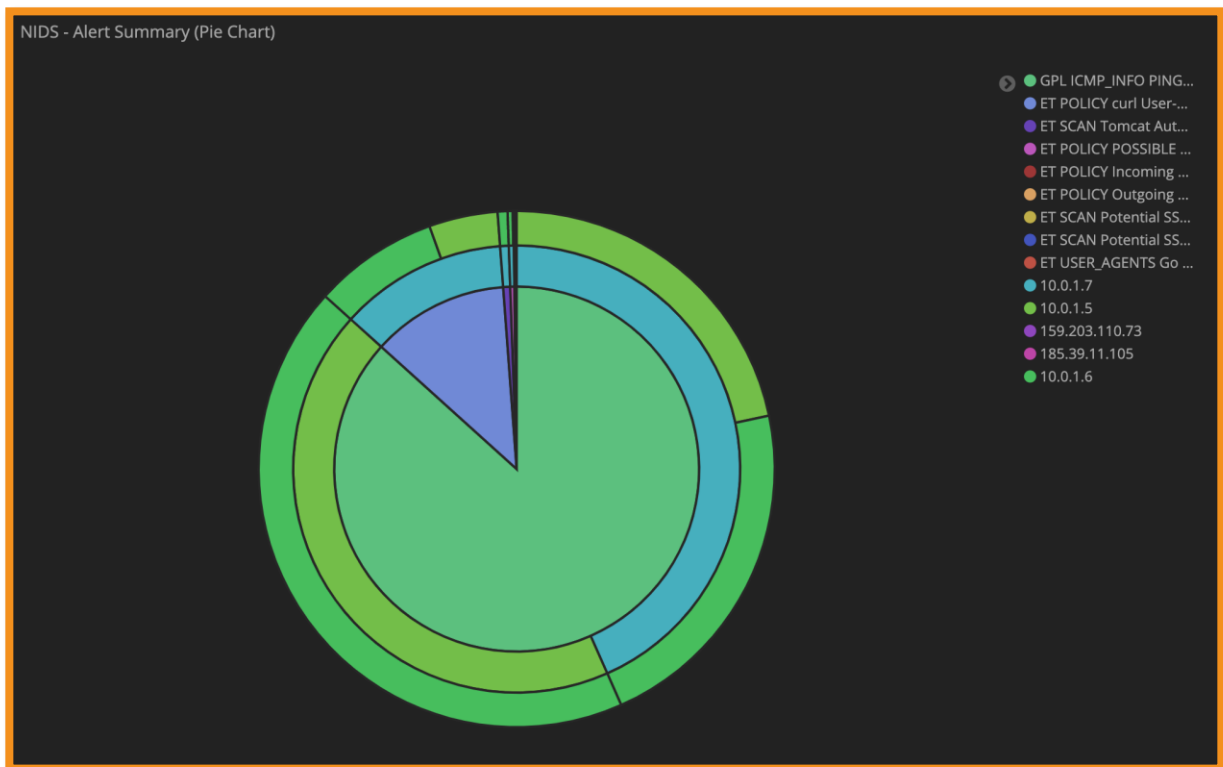
Security Onion

Login

- Once logged in, the **Kibana** dashboard is displayed.
- Here, you can see the traffic alerts coming from workloads.



- Scroll down for more visibility as shown in the following figure.



- Select **NIDS** or **HPPT** on the left side Navigation section of the dashboard.
- There you can see **NIDS** (ICMP,Sql) or **HTTP** traffic logs as per the selection.

5.2. Use Case 2: 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. 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

Setup DVWA

Instructions

About

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in:
`/var/www/html/dvwa/config/config.inc.php`

If the database already exists, it will be cleared and the data will be reset.
You can also use this to reset the administrator credentials ("admin // password") at any stage.

Setup Check

Operating system: *nix
Backend database: MySQL
PHP version: 5.6.34-1+ubuntu16.04.1+deb.sury.org+1

Web Server SERVER_NAME: 174.129.135.7

PHP function display_errors: Disabled
PHP function safe_mode: Disabled
PHP function allow_url_include: Enabled
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: DVWA
MySQL password: *****
MySQL database: dvwa
MySQL host: 127.0.0.1

reCAPTCHA key: 6LfWsT4UAAAAAJgZBWzGlvN99BZtczIxaoxN5mep

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

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the following in your `php.ini` file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

Create / Reset Database

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

Data inserted into 'guestbook' table.

Backup file `/config/config.inc.php.bak` automatically created

Setup successful!

Please login.

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



Username


admin

Password

.....

Login

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



Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

DVWA Security

PHP Info

About

Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

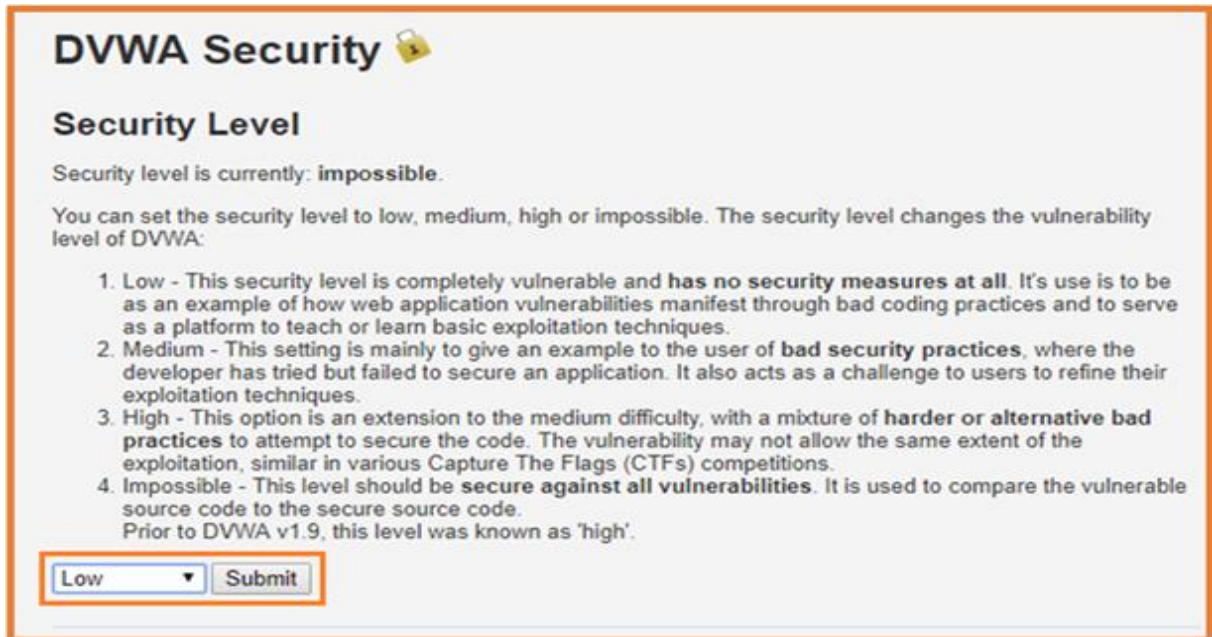
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!


There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's public

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



DVWA Security 

Security Level

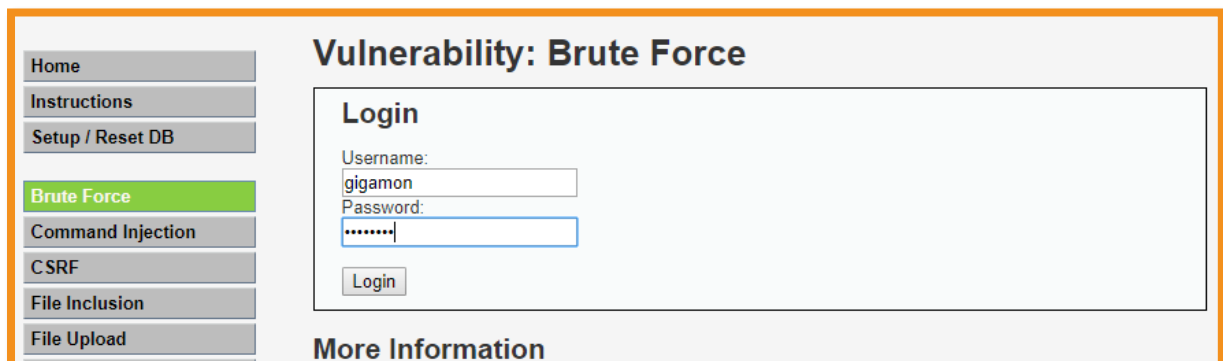
Security level is currently: **impossible**.

You can set the security level to low, medium, high or impossible. The security level changes the vulnerability level of DVWA:

1. Low - This security level is completely vulnerable and **has no security measures at all**. It's use is to be as an example of how web application vulnerabilities manifest through bad coding practices and to serve as a platform to teach or learn basic exploitation techniques.
2. Medium - This setting is mainly to give an example to the user of **bad security practices**, where the developer has tried but failed to secure an application. It also acts as a challenge to users to refine their exploitation techniques.
3. High - This option is an extension to the medium difficulty, with a mixture of **harder or alternative bad practices** to attempt to secure the code. The vulnerability may not allow the same extent of the exploitation, similar in various Capture The Flags (CTFs) competitions.
4. Impossible - This level should be **secure against all vulnerabilities**. It is used to compare the vulnerable source code to the secure source code.
Prior to DVWA v1.9, this level was known as 'high'.

Low ▼ **Submit**

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



Vulnerability: Brute Force

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Login

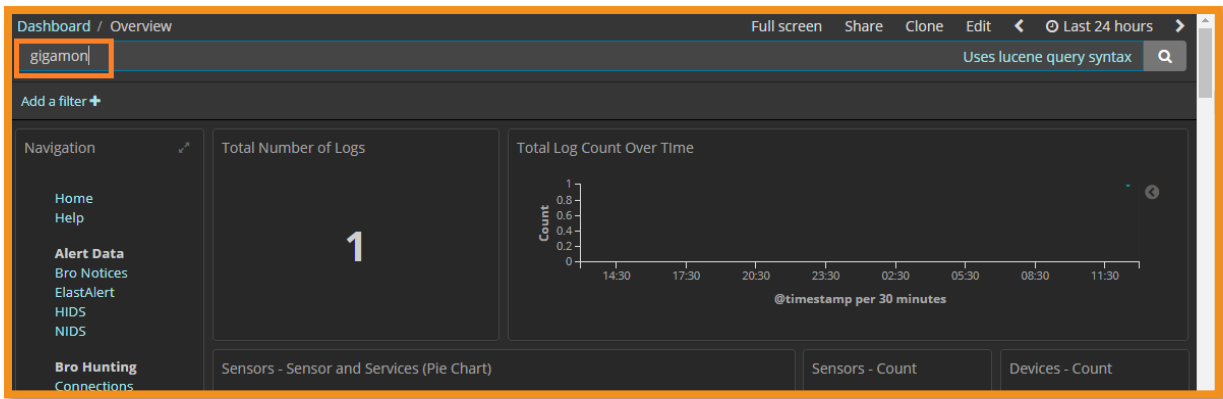
Username:
gigamon

Password:
.....

Login

More Information

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

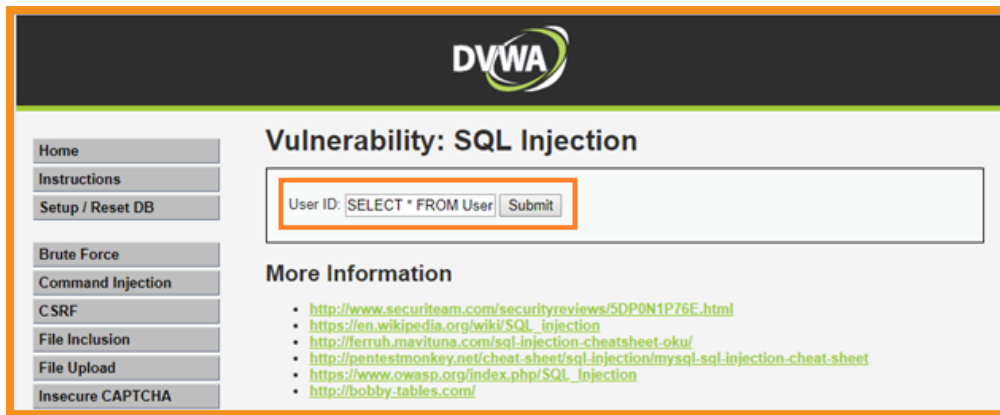


- Scroll down the page and check the logs to see the brute force attack message.
- You can view the wrong credentials that you gave in the Brute force attack.

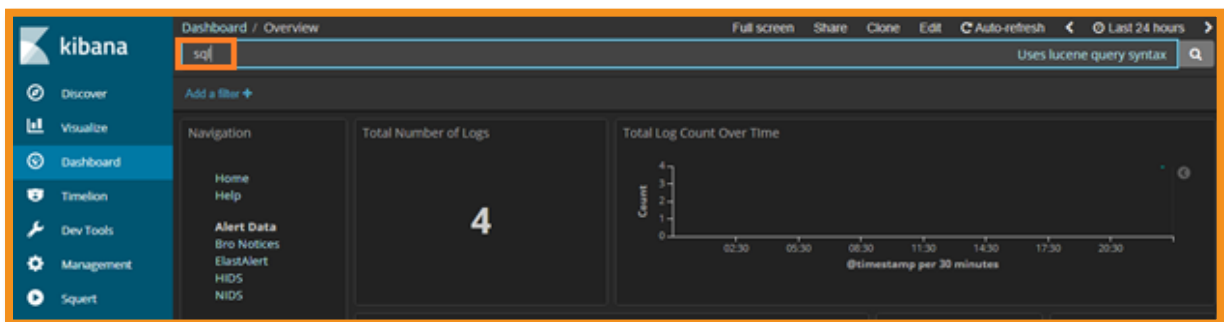
Table	JSON	View surrounding documents	View single document
@timestamp	June 17th 2019, 12:55:57.323		
@version	1		
_id	8kdUZGsBvWP89xuHpeig		
_index	ip-10-0-0-49:logstash-bro-2019.06.17		
_score	-		
_type	doc		
destination_ip	10.0.1.6		
destination_ips	10.0.1.6		
destination_port	80		
event_type	bro_http		
ips	14.98.166.186, 10.0.1.6		
logstash_time	3.31		
message	<pre>{ "ts": "2019-06-17T07:25:57.323592Z", "uid": "CyVbfEa96IzF5EtDb", "id.orig_h": "14.98.166.186", "id.orig_p": 40806, "id.resp_h": "10.0.1.6", "id.resp_p": 80, "trans_depth": 1, "method": "GET", "host": "54.175.220.129", "uri": "/dwa/vulnerabilities/brute/", "username": "gigamon", "password": "testddd\\u0026Login-Login", "referrer": "http://54.175.220.129/dwa/vulnerabilities/brute/", "version": "1.1", "user_agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/75.0.3770.90 Safari/537.36", "request_body_len": 0, "response_body_len": 4381, "status_code": 200, "status_msg": "OK", "tags": [], "resp_fuids": ["FGPZ4F2vC484XETjgf"], "resp_mime_type": ["text/html"]} </pre>		

- 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.

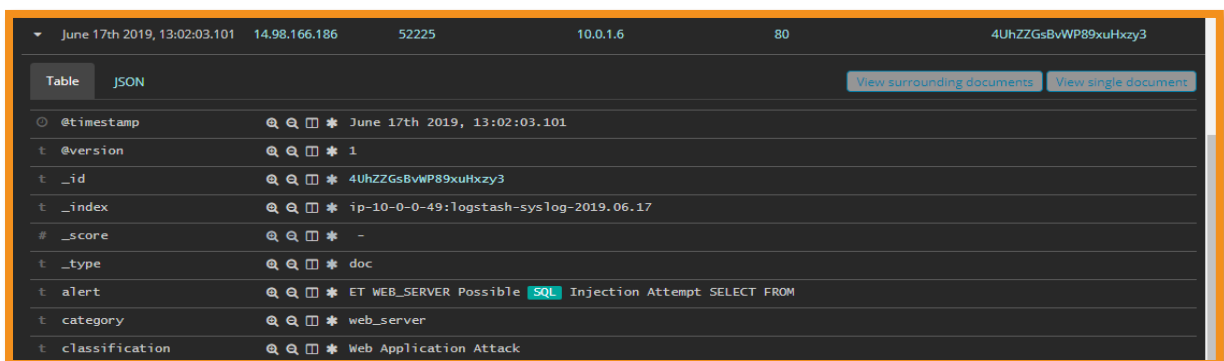
SELECT * FROM Users WHERE UserId = 105 OR 1=1;



- Go to **Kibana**, and click **Home** type “sql” in dashboard search box and click.
- 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.



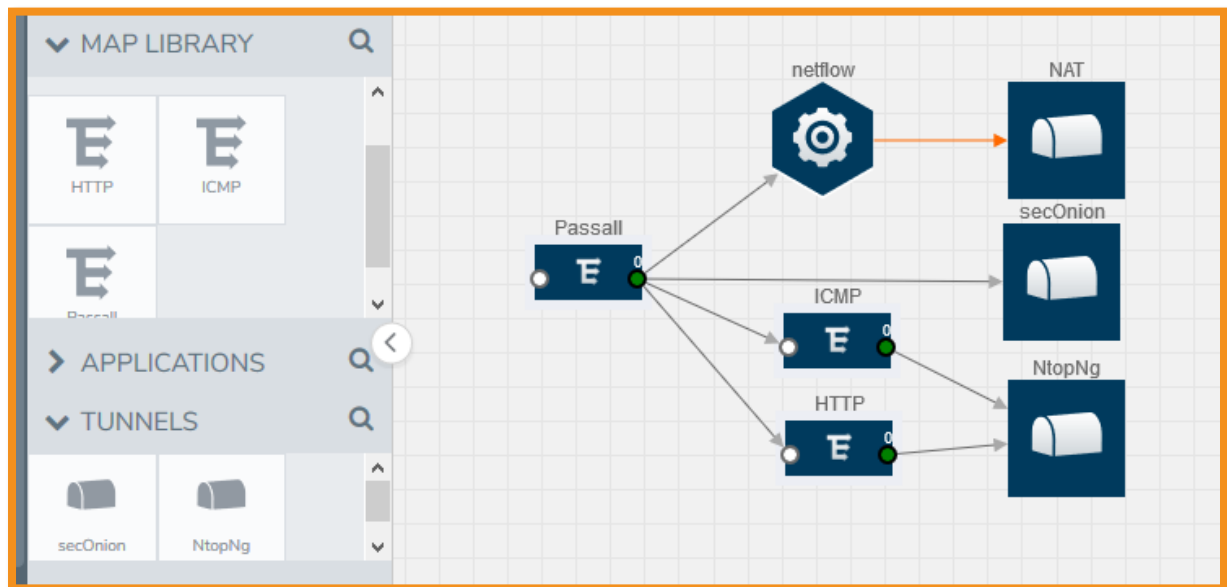
5.3. Use Case 3: GigaSMART De-Duplication

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 analyze 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).

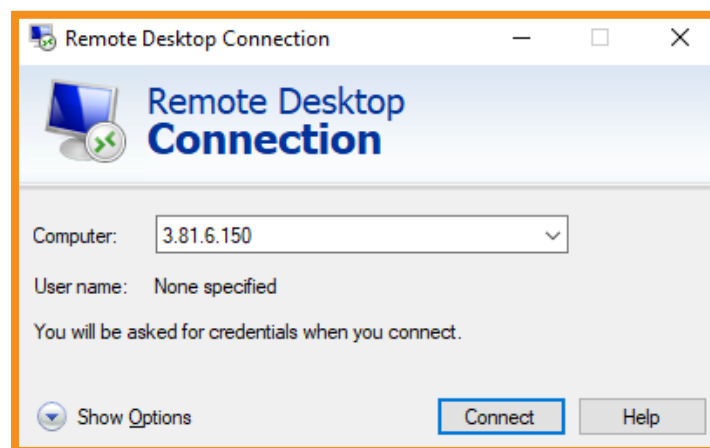
Note: The flow map is already created to send traffic to security onion as shown below



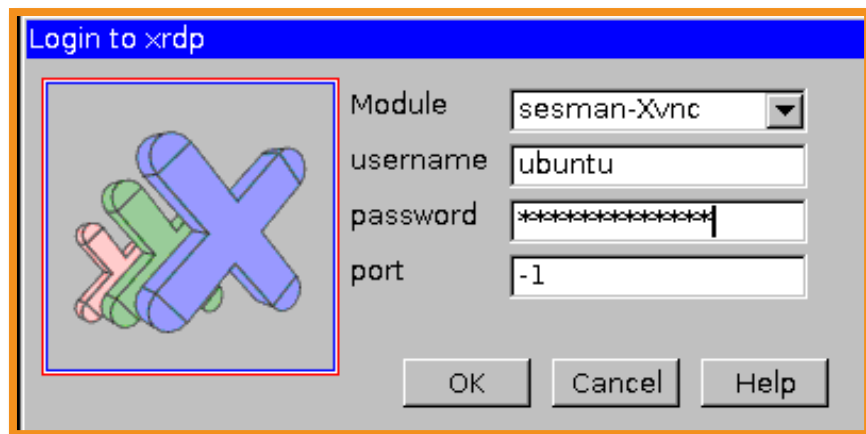
You need to perform the following steps to understand the use of GigaSMART De-Duplication App.

5.3.1. Without using De-Duplication App

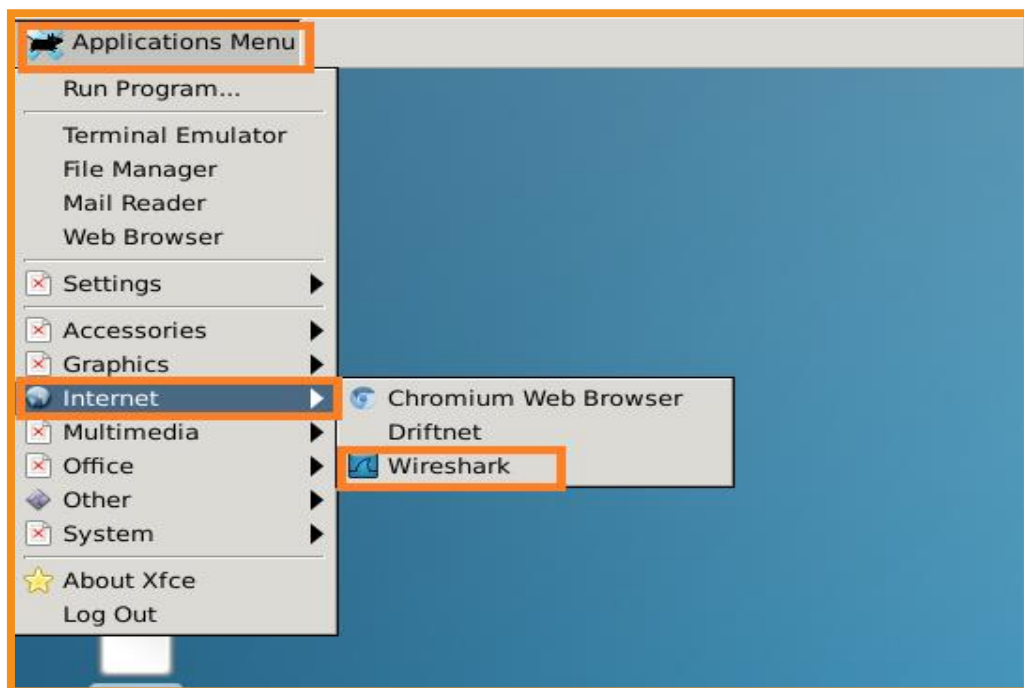
1. RDP using **Security Onion** IP address to access the **WireShark** tool as shown below.



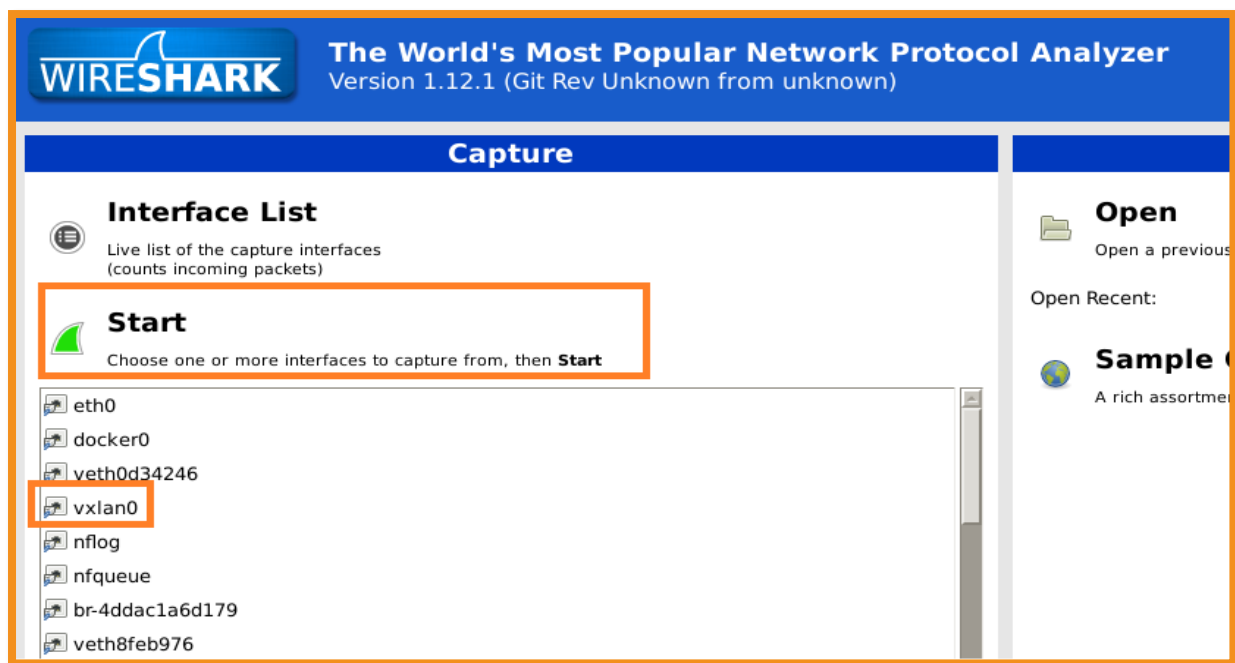
2. Enter the **WireShark** credentials provided in the Test drive launch page as shown below



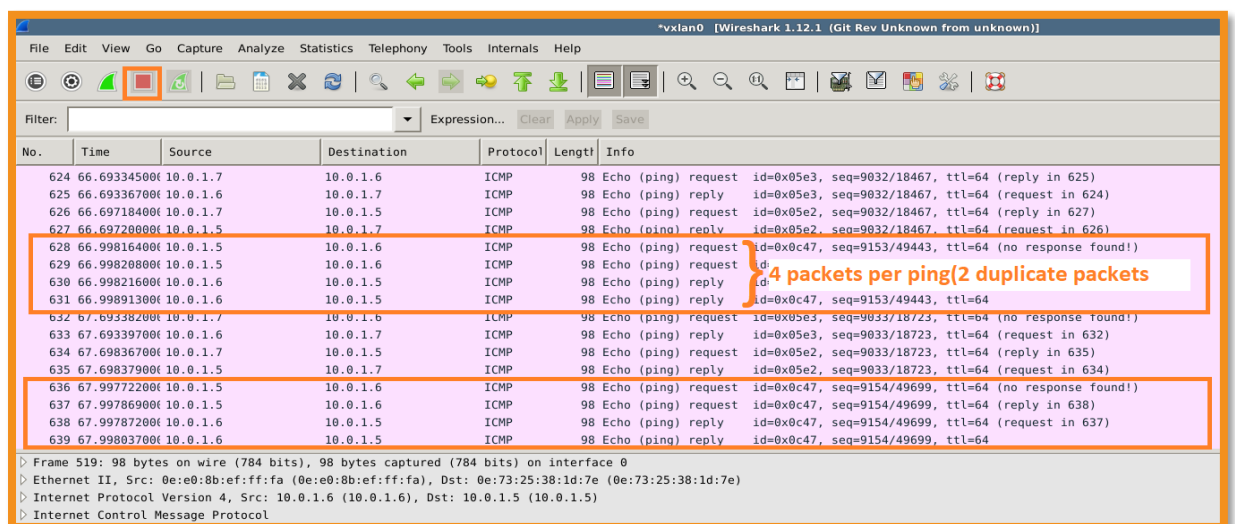
3. Once you RDP into the Wireshark tool navigate to **Applications Menu**
→Internet→Wireshark



4. Select **vxlano** and click on **Start** as shown below.You can see the traffic flow.

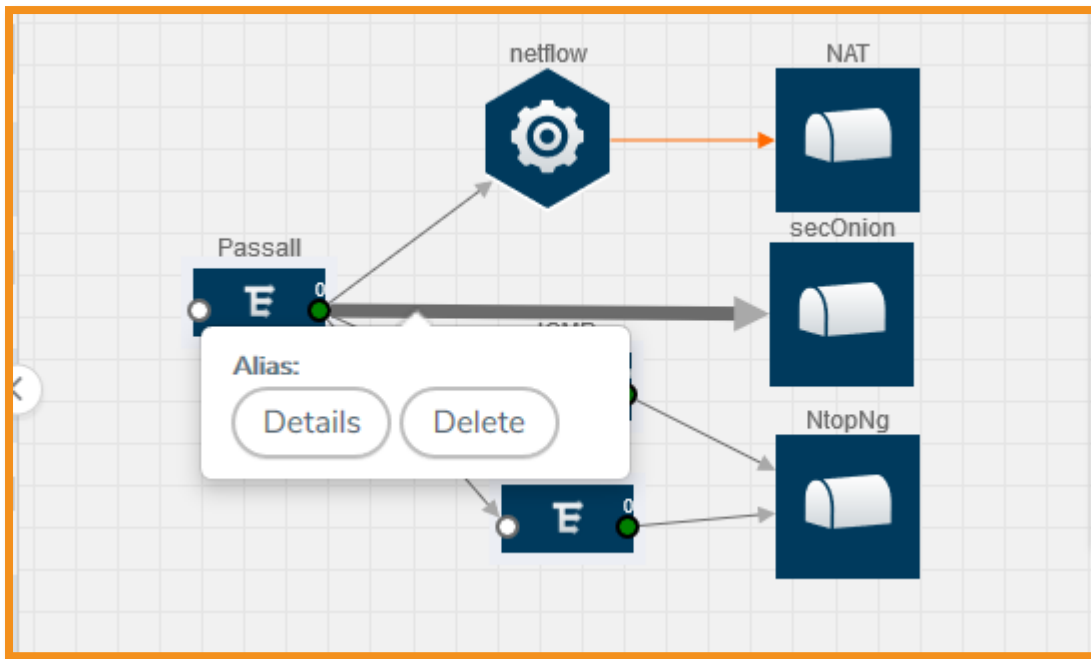


- Click **stop** on wireshark and you can observe that there are **4 packets per one ping** as shown below.

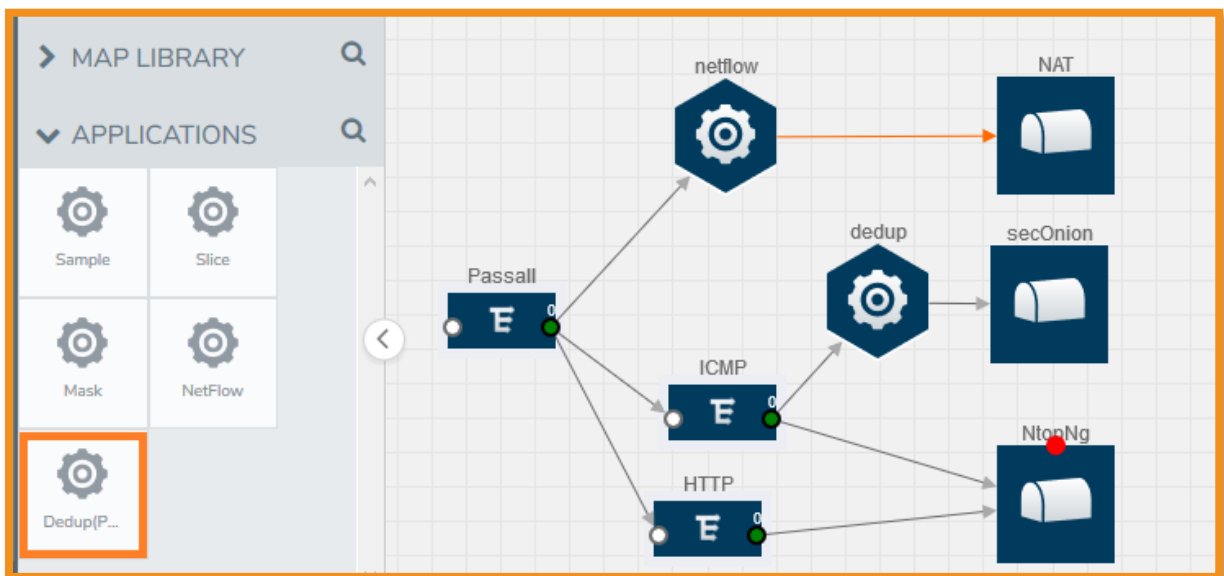


5.3.2. With using De-duplication App

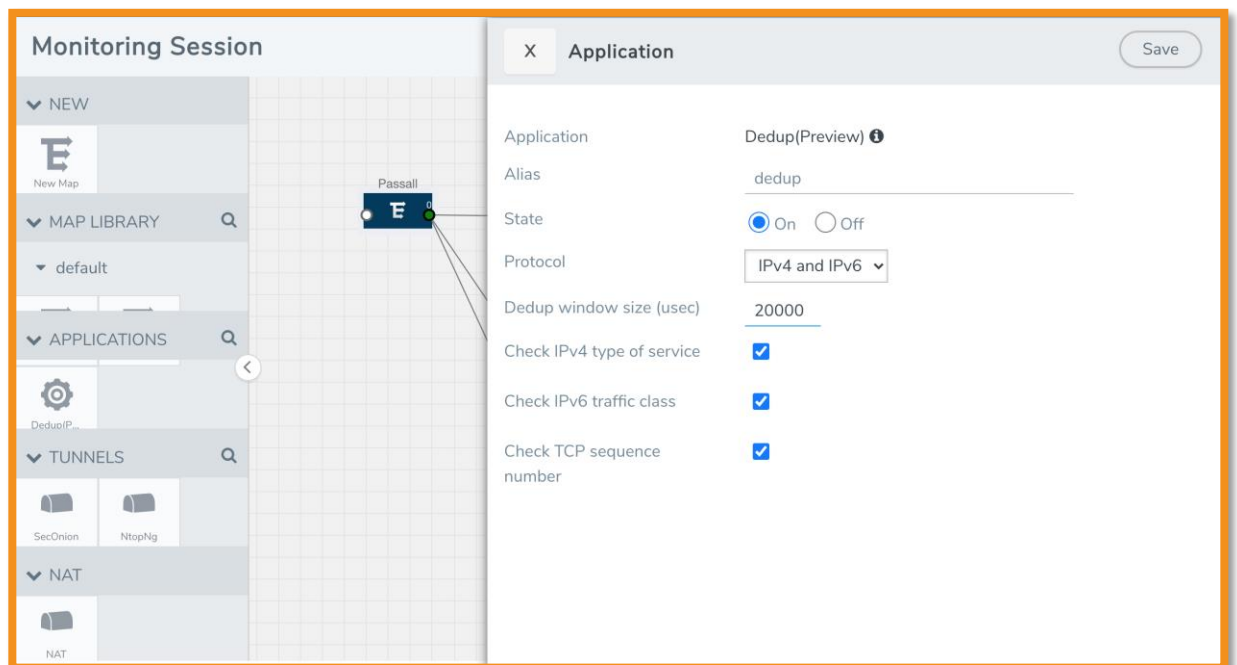
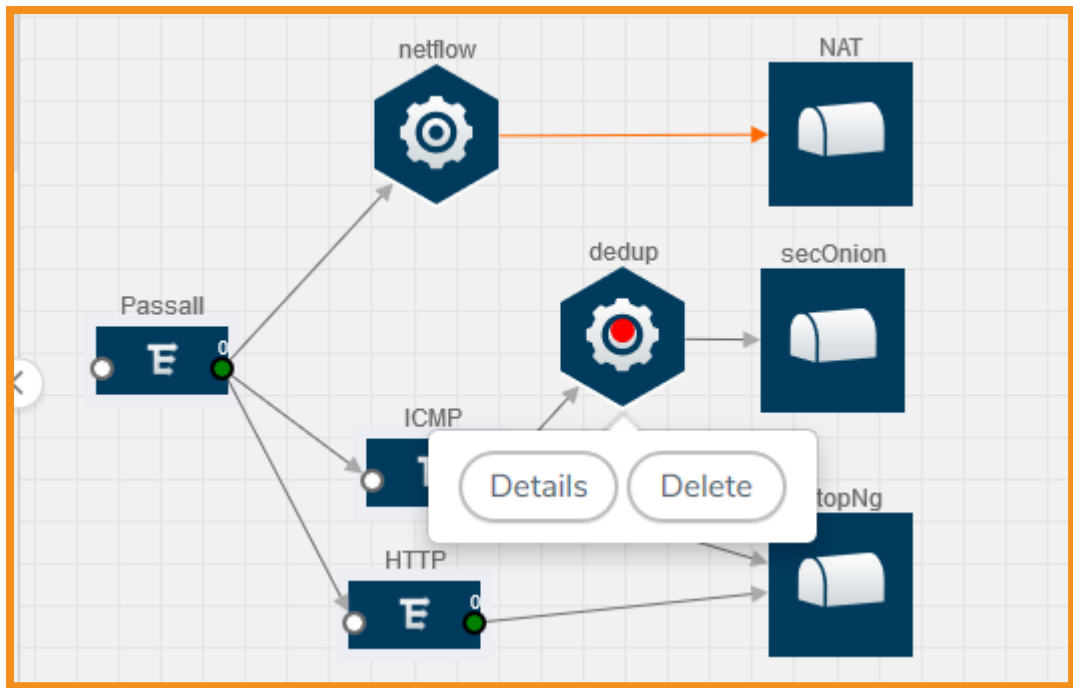
- Go back to **Monitoring Session** in **GigaVUE-FM**, delete the links (Connector arrows) from **Passall** to **seconion**



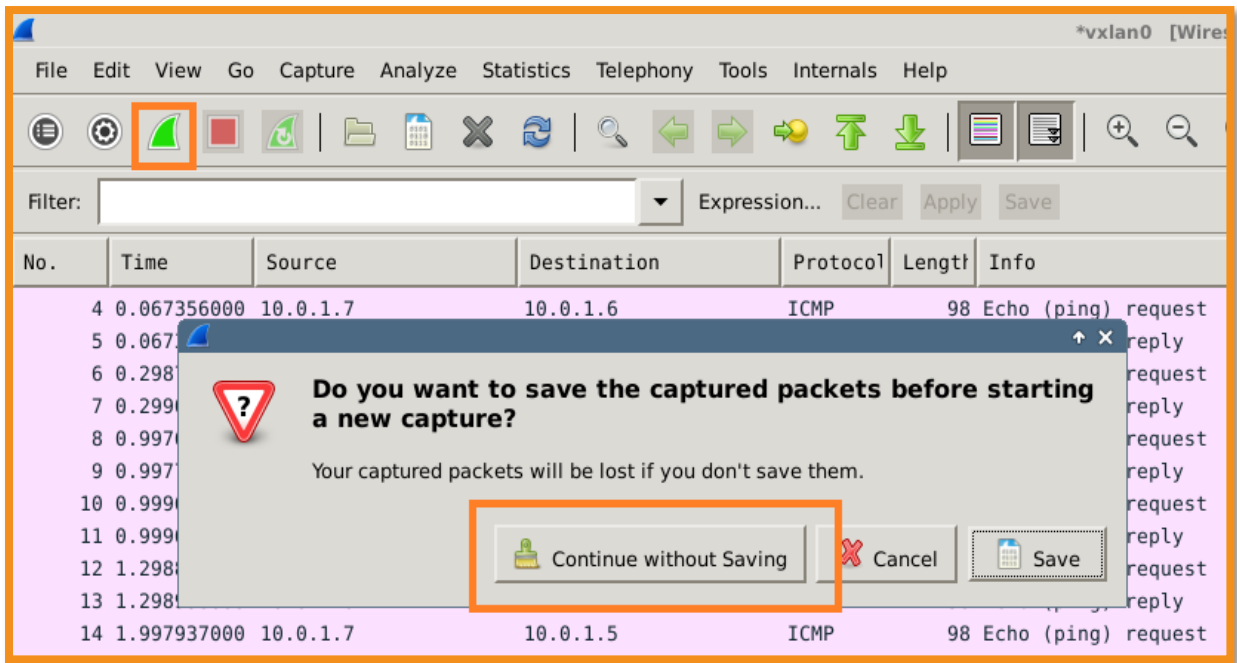
2. Drag and drop the **dedup** application from the left pane. Mousehover the **ICMP** map and drag a line to connect the red dots to **Dedup**, the same way connect **Dedup** to **SecOnion**. Then click on **deploy**.



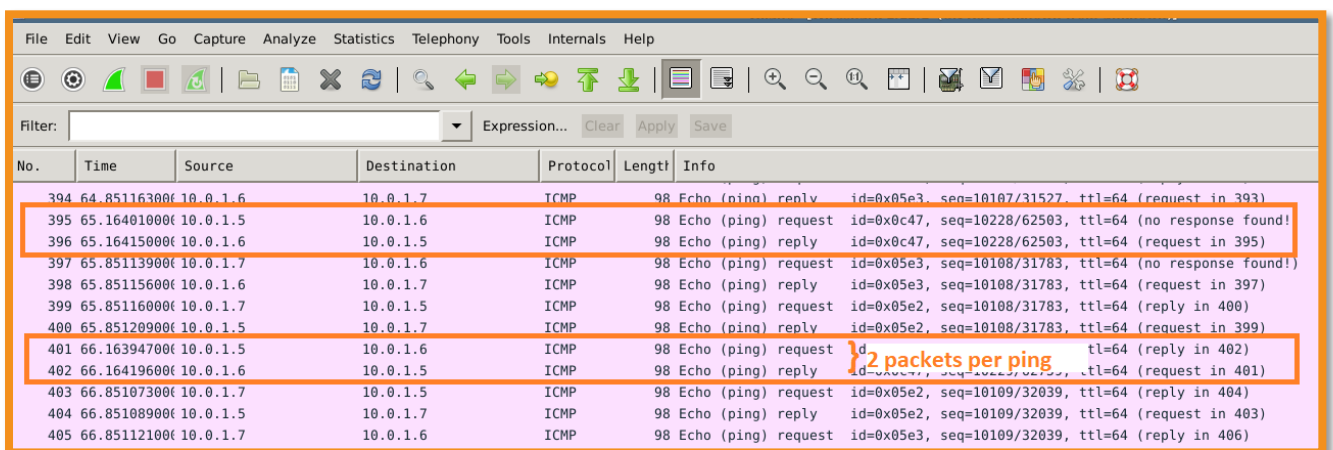
3. Click **dedup** and then click on **Details**, it will open a form. Change the value of **Dedup window size** to **20000** and click on **Save**. After saving the details click on **Deploy**.



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



5. Click Stop on wireshark tool, 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.