GigaSECURE® Cloud

Test Drive On AWS

Gigamon®

Table of Content

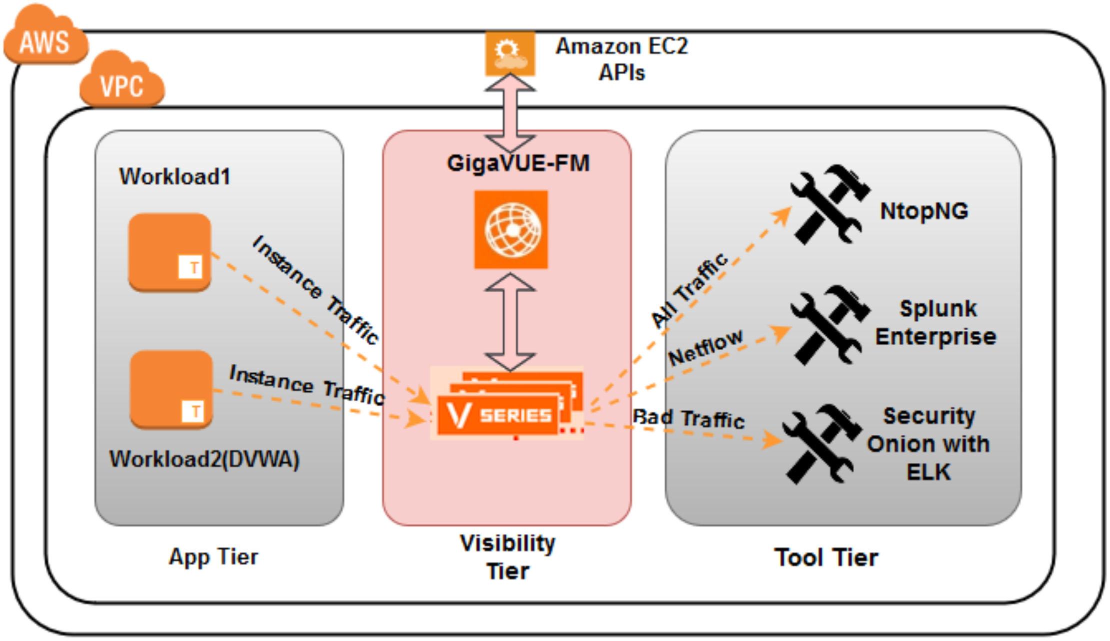
1. About Test Drive

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

2. Introduction to GigaSECURE Cloud 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 GigaSECURE Cloud for AWS, the industry's first pervasive visibility platform that provides consistent visibility into data-in-motion across the entire enterprise. The Gigamon GigaSECURE Cloud 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



GigaSECURE Cloud for AWS extends an enterprise's on-premise visibility to the AWS public cloud regardless of where your applications reside. Refer to the figure above. The entire GigaSECURE Cloud 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 GigaSECURE Cloud 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 GigaSECURE Cloud.
- **Splunk (Tool):** A monitoring tool present inside the applications VPC for receiving Netflow traffic from the GigaSECURE Cloud.
- **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:

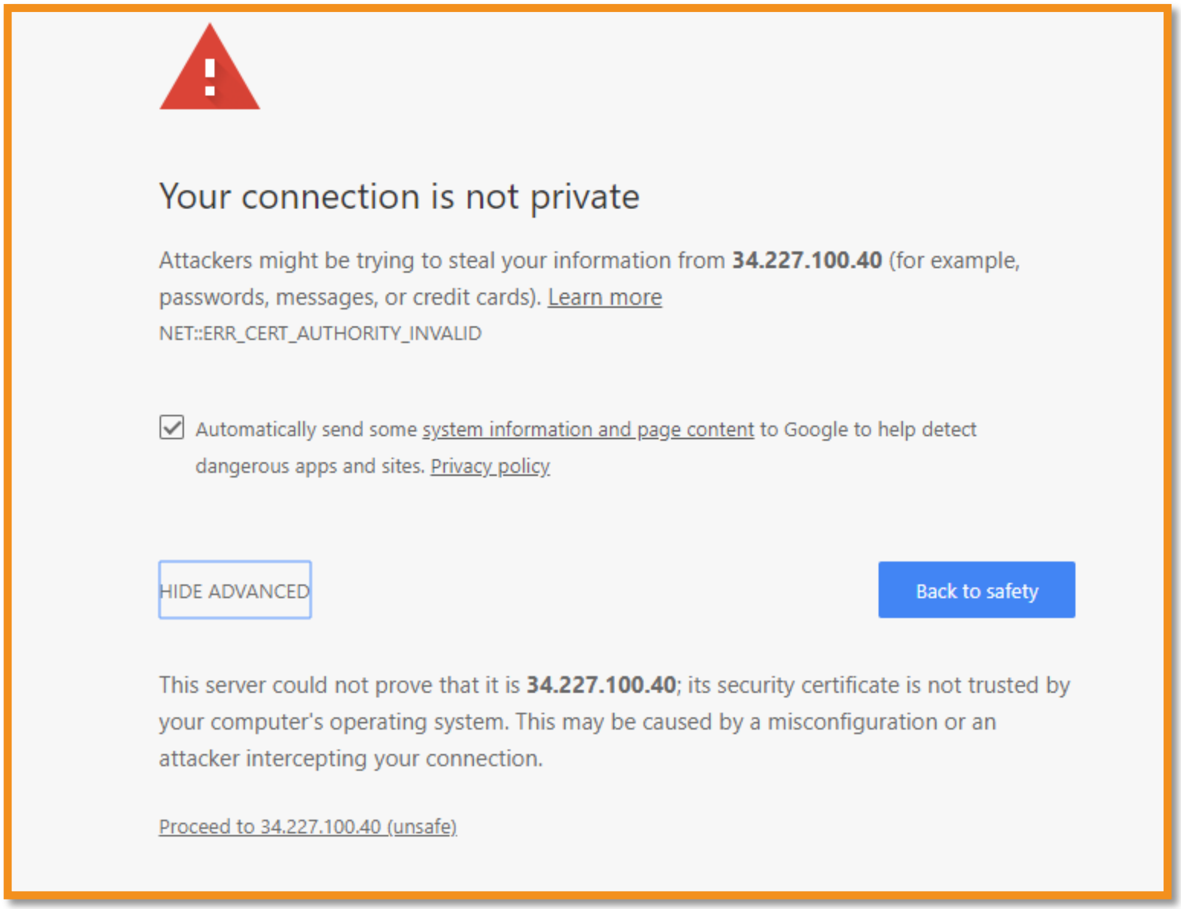
- **Use Case 1: Gaining Visibility -** Create the flow maps to send all type of traffic into the Splunk (Netflow), NtopNG and Security Onion.
- **Use Case 2: Creating Traffic Specific Flow Maps -** Create multiple flow maps to send specific traffic to specific tools.
- **Use Case 3: Detecting Threats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

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 public ip provided in the Test Drive launch page. Click **Advanced > Proceed to IP address** link in the warning screen.



Your connection is not private

Attackers might be trying to steal your information from **34.227.100.40** (for example, passwords, messages, or credit cards). Learn more

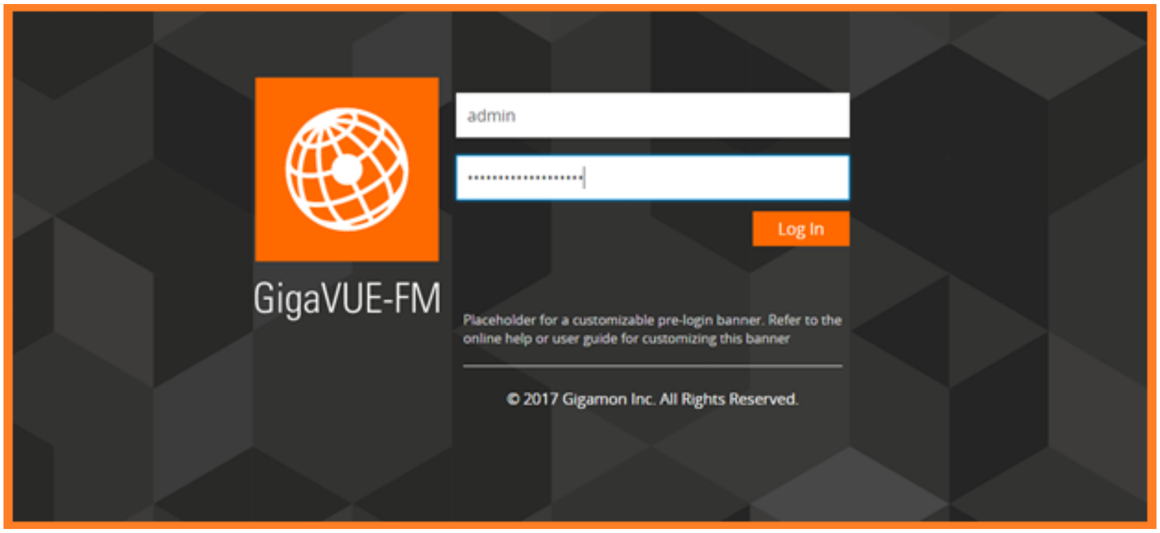
NET::ERR_CERT_AUTHORITY_INVALID

☑ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

This server could not prove that it is **34.227.100.40**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 34.227.100.40 (unsafe)

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



admin

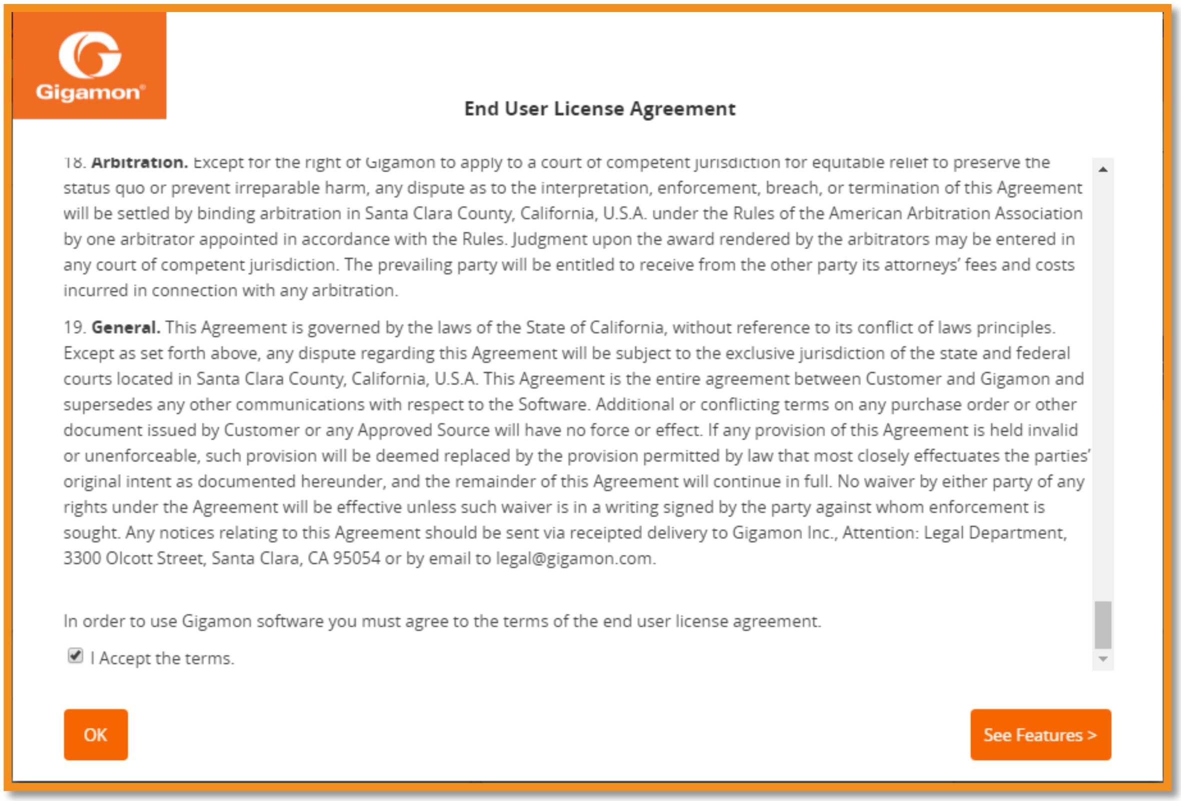
••••••••••••••••••••

Placeholder for a customizable pre-login banner. Refer to the online help or user guide for customizing this banner

© 2017 Gigamon Inc. All Rights Reserved.

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 deemo lab.

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



End User License Agreement

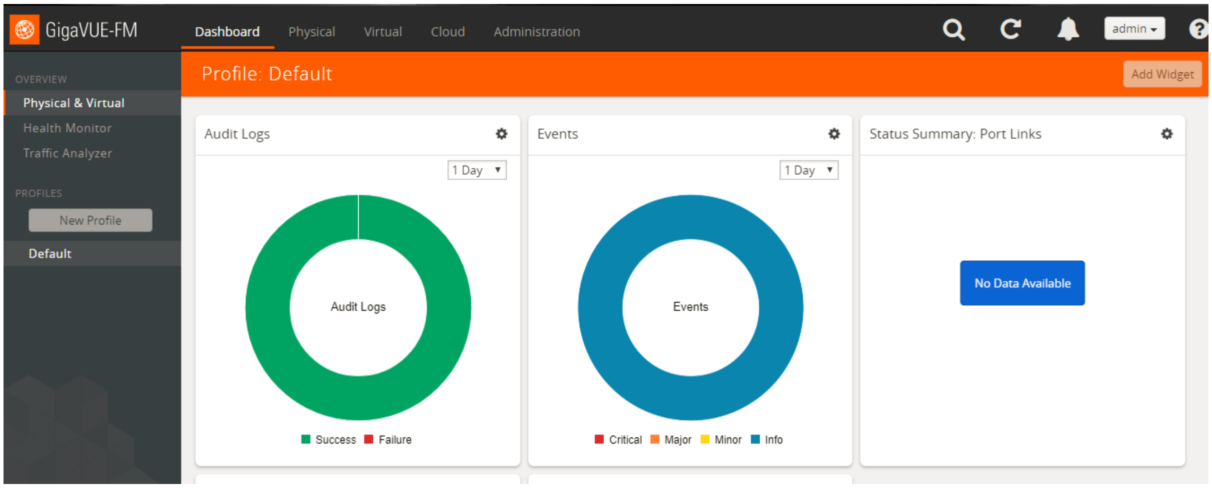
18. **Arbitration.** Except for the right of Gigamon to apply to a court of competent jurisdiction for equitable relief to preserve the status quo or prevent irreparable harm, any dispute as to the interpretation, enforcement, breach, or termination of this Agreement will be settled by binding arbitration in Santa Clara County, California, U.S.A. under the Rules of the American Arbitration Association by one arbitrator appointed in accordance with the Rules. Judgment upon the award rendered by the arbitrators may be entered in any court of competent jurisdiction. The prevailing party will be entitled to receive from the other party its attorneys' fees and costs incurred in connection with any arbitration.

19. **General.** This Agreement is governed by the laws of the State of California, without reference to its conflict of 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 Software. Additional or conflicting terms on any purchase order or other document issued by Customer or any Approved Source 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.

In order to use Gigamon software you must agree to the terms of the end user license agreement.

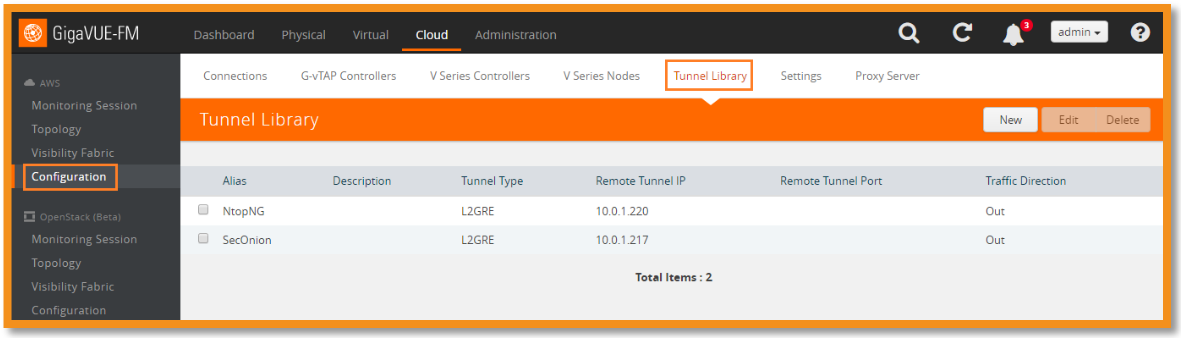
☑ I Accept the terms.

- 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 **L2 GRE tunnels (NtopNG and SecOnion)** are been automated.

NOTE: A standard L2 GRE tunnel is established to distribute the customized traffic from the V Series node to the monitoring tools.



Tunnel Library

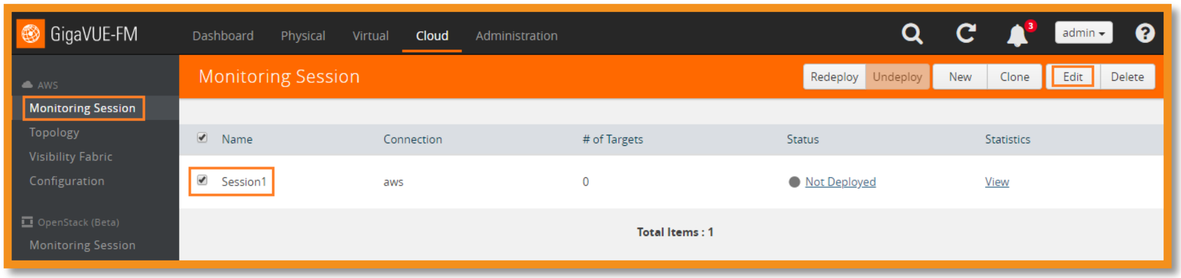
Alias	Description	Tunnel Type	Remote Tunnel IP	Remote Tunnel Port	Traffic Direction
□ NtopNG		L2GRE	10.0.1.220		Out
□ SecOnion		L2GRE	10.0.1.217		Out

Total Items : 2

- 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.

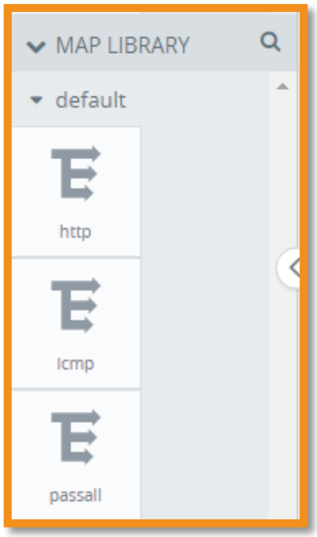


Monitoring Session

☑ Name	Connection	# of Targets	Status	Statistics
☑ Session1	aws	0	● Not Deployed	View

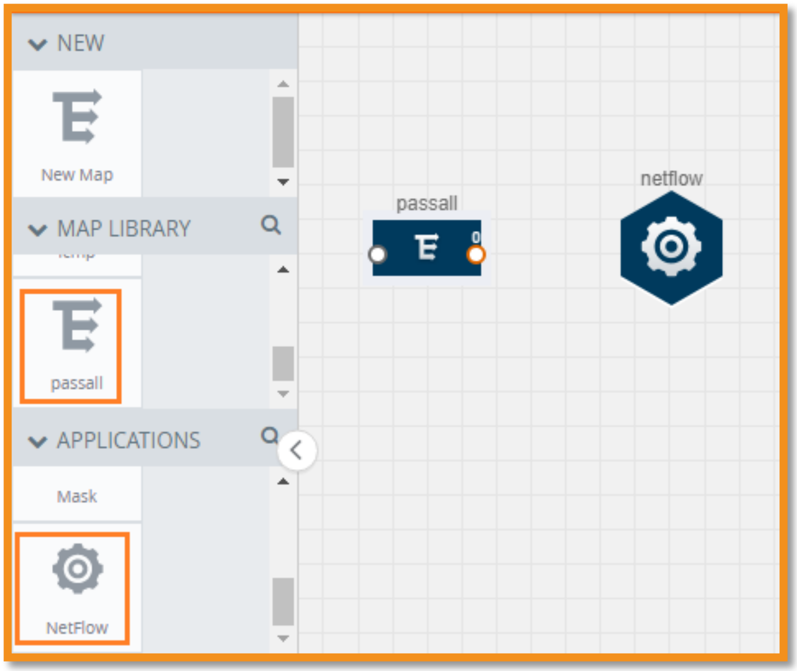
Total Items : 1

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

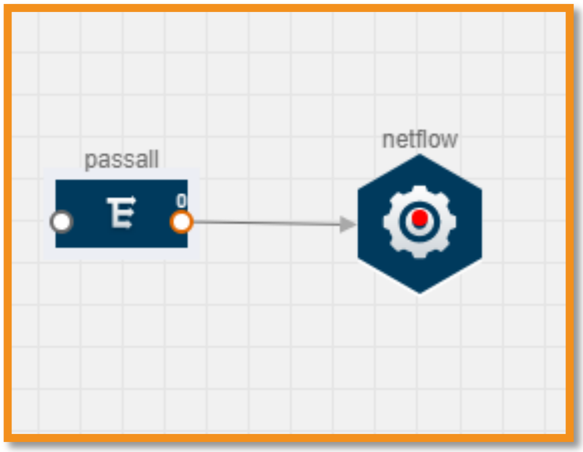


2. Creating a flow map.

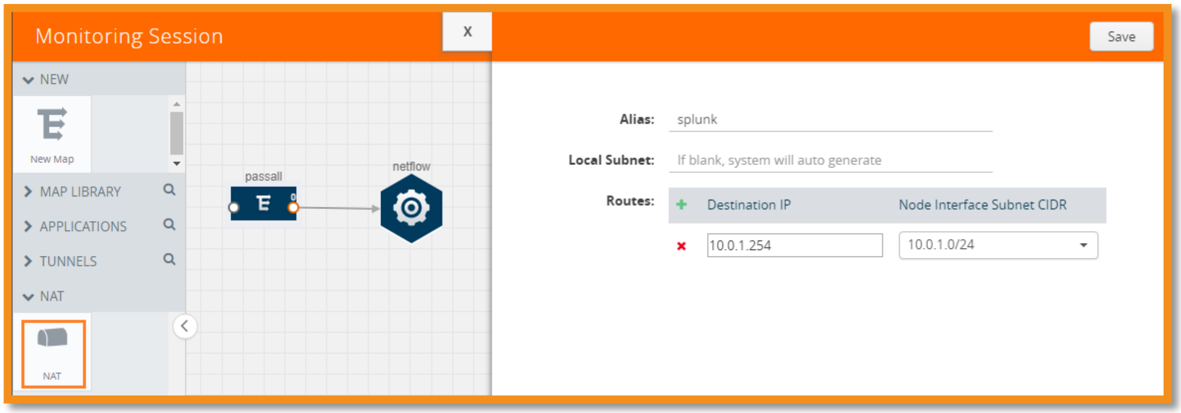
- Drag and drop the **passall** map from the **MAP LIBRARY** section and **Netflow** from **APPLICATIONS** section to the empty map area.



- 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.
  - In the **Alias** field, enter **Splunk** as the NAT name.
  - Click the **+** sign adjacent to the **Destination IP** heading a box and a dropdown is displayed
  - Enter Splunk private IP in the box that you have in your deemo lab launch page
  - Select the **Node Intgerface Subnet CIDR** as (10.0.1.0/24) from dropdown list.
  - Click **Save** button on the top right corner of the page.



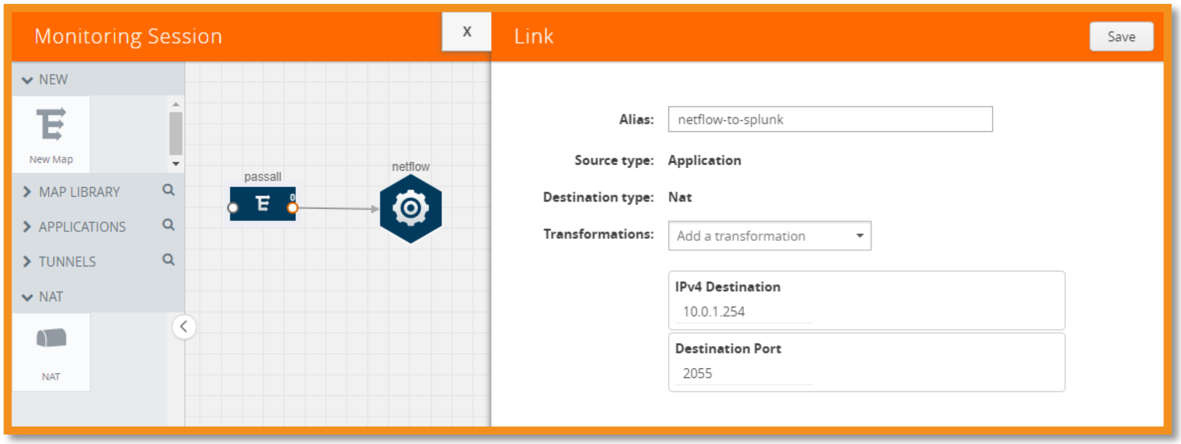
Alias: splunk

Local Subnet: If blank, system will auto generate

Routes:

Destination IP	Node Interface Subnet CIDR
10.0.1.254	10.0.1.0/24

- Hover over the netflow and drag a line to connect the red dots from the netflow to the Splunk and enter the required information.
  - In the **Alias** field, enter **netflow-to-splunk** as the alias name.
  - Enter Splunk private IP in the **IPv4 Destination**.
  - Click **Save** button on the top right corner of the page.



Alias: netflow-to-splunk

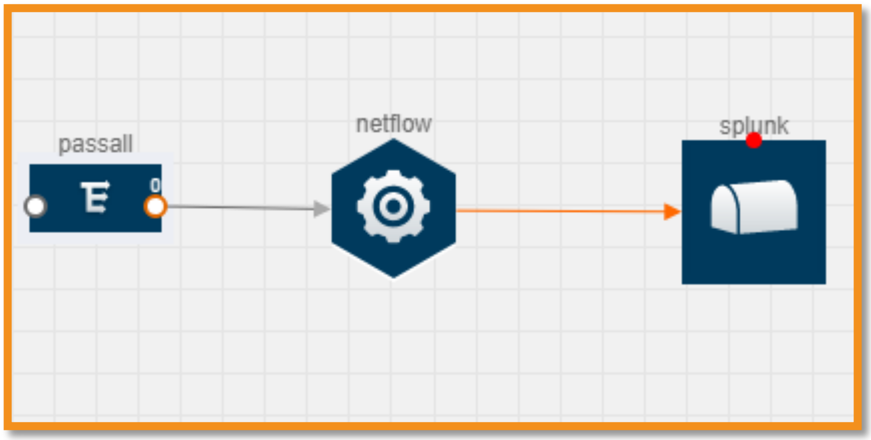
Source type: Application

Destination type: Nat

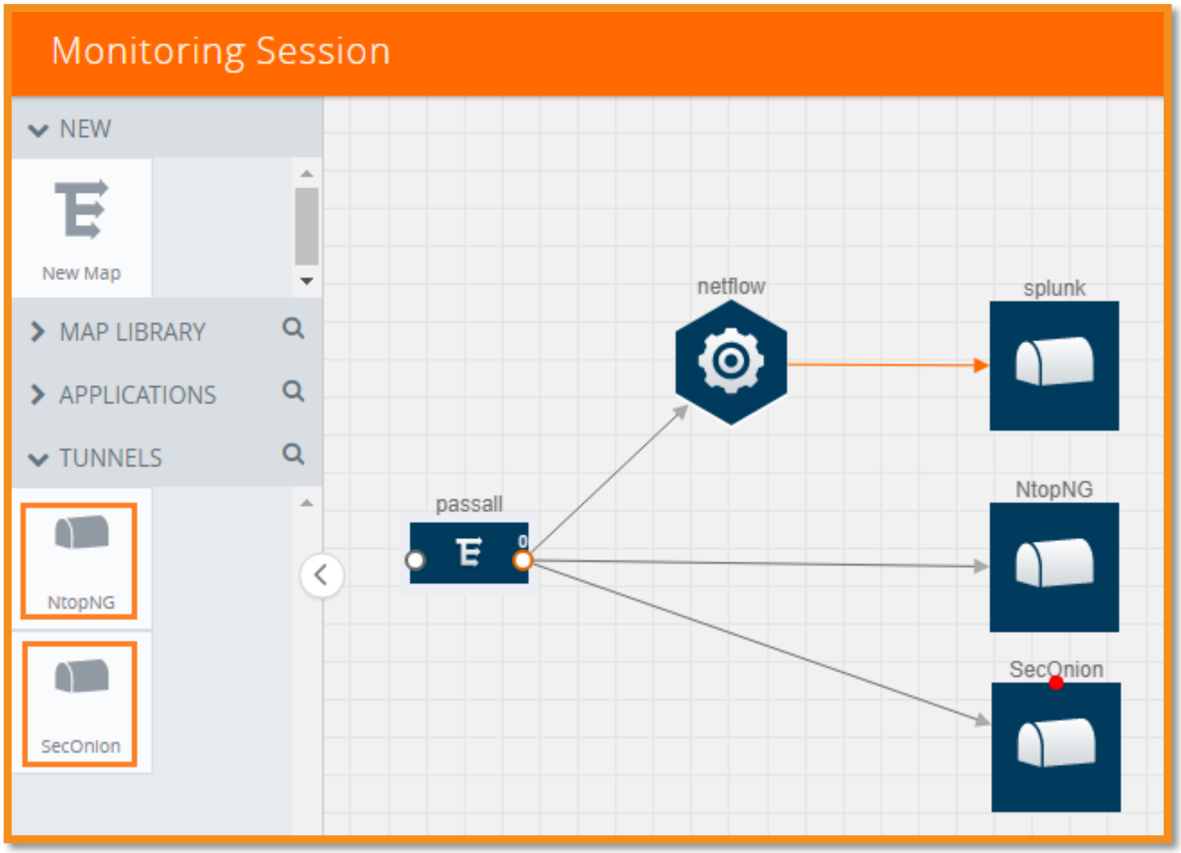
Transformations: Add a transformation

IPv4 Destination: 10.0.1.254

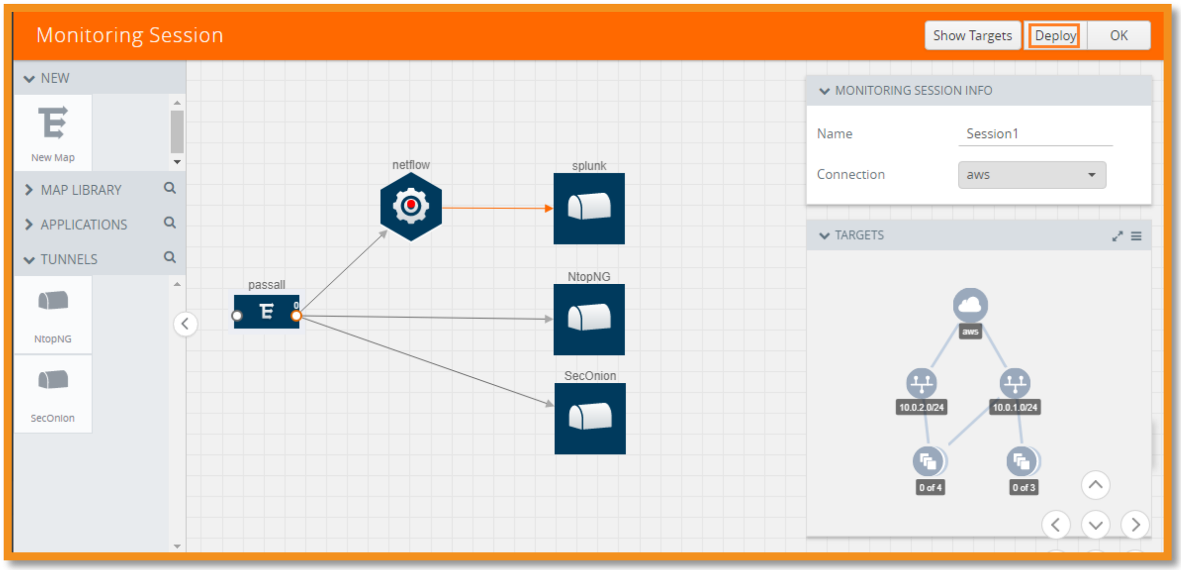
Destination Port: 2055



- Drag and drop the **NtopNG** and **SecOnion** maps From the **MAP LIBRARY**.
- 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**.

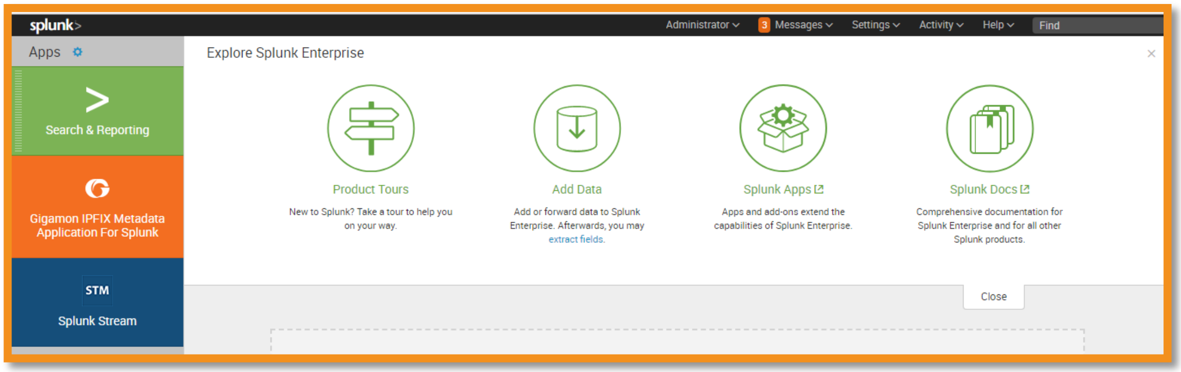


Name Session1

Connection aws

3. Login to the Splunk

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



Explore Splunk Enterprise

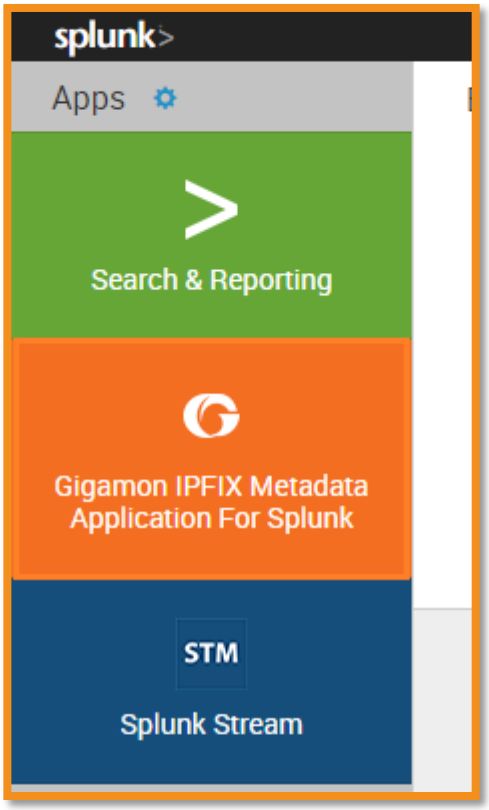
Product Tours
New to Splunk? Take a tour to help you on your way.

Add Data
Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

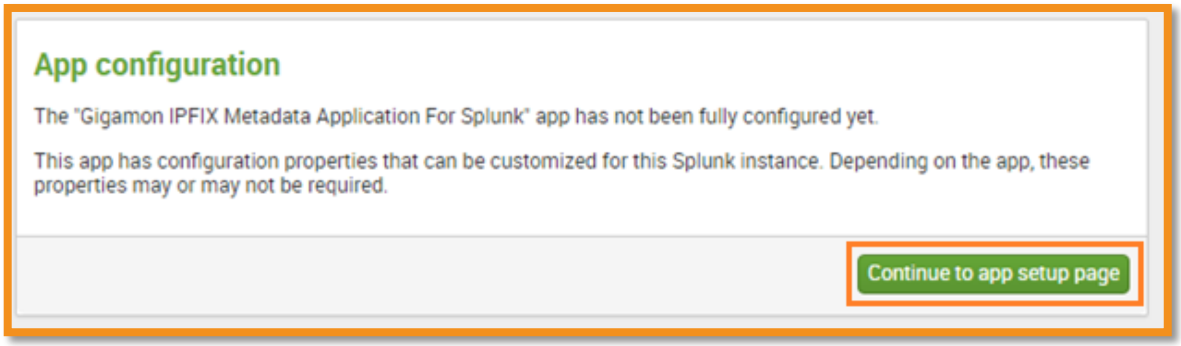
Splunk Apps
Apps and add-ons extend the capabilities of Splunk Enterprise.

Splunk Docs
Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

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



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

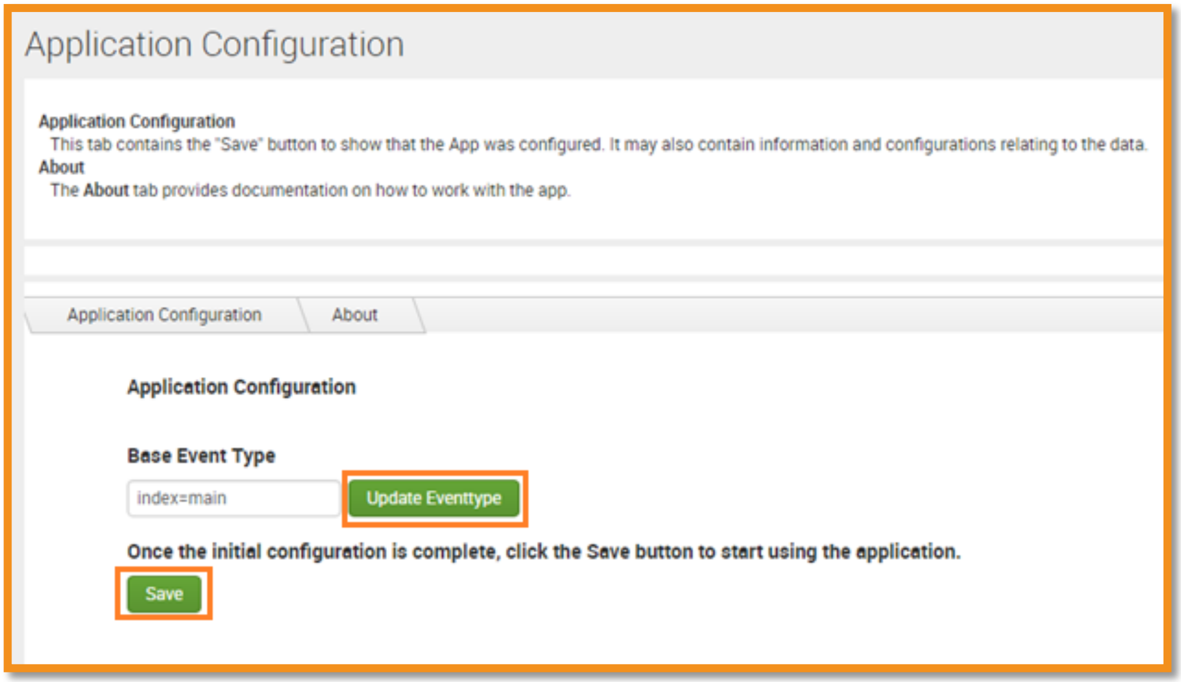


App configuration

The "Gigamon IPFIX Metadata Application For Splunk" app has not been fully configured yet.

This app has configuration properties that can be customized for this Splunk instance. Depending on the app, these properties may or may not be required.

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



Application Configuration

Application Configuration
This tab contains the "Save" button to show that the App was configured. It may also contain information and configurations relating to the data.
About
The **About** tab provides documentation on how to work with the app.

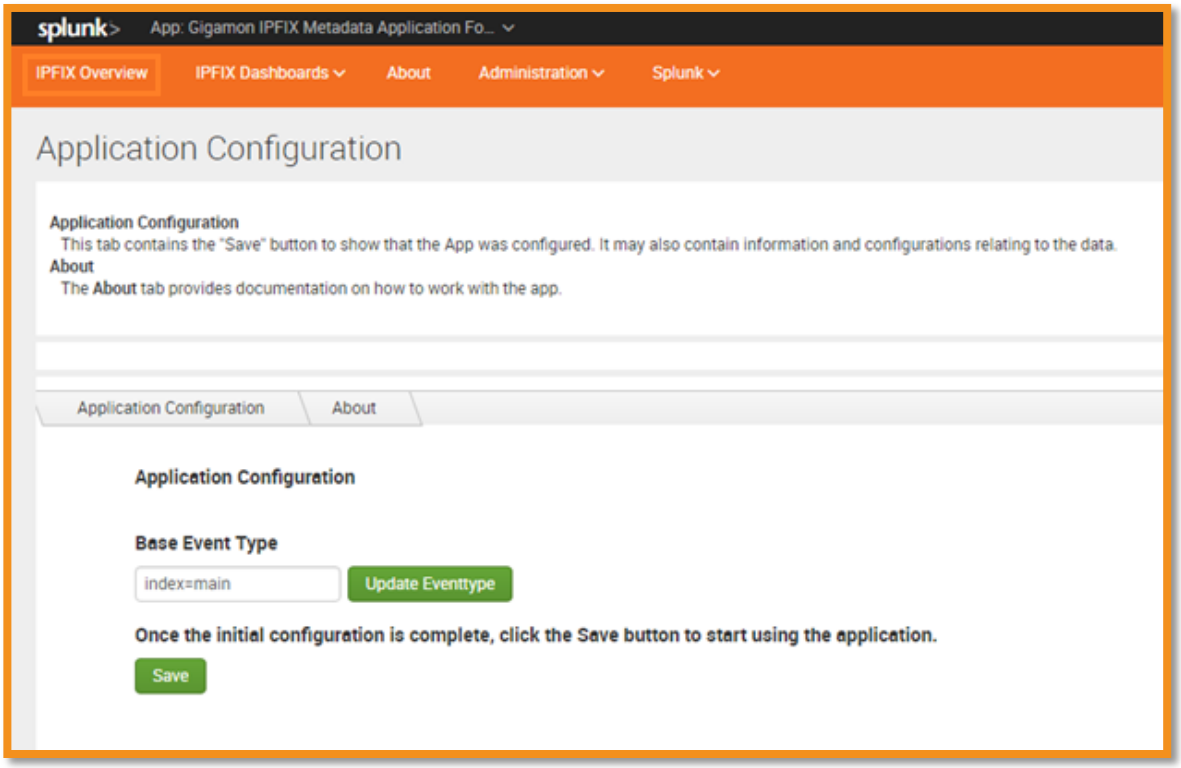
Application Configuration

Base Event Type

index=main

Once the initial configuration is complete, click the Save button to start using the application.

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



Application Configuration

Application Configuration
This tab contains the "Save" button to show that the App was configured. It may also contain information and configurations relating to the data.
About
The **About** tab provides documentation on how to work with the app.

Application Configuration

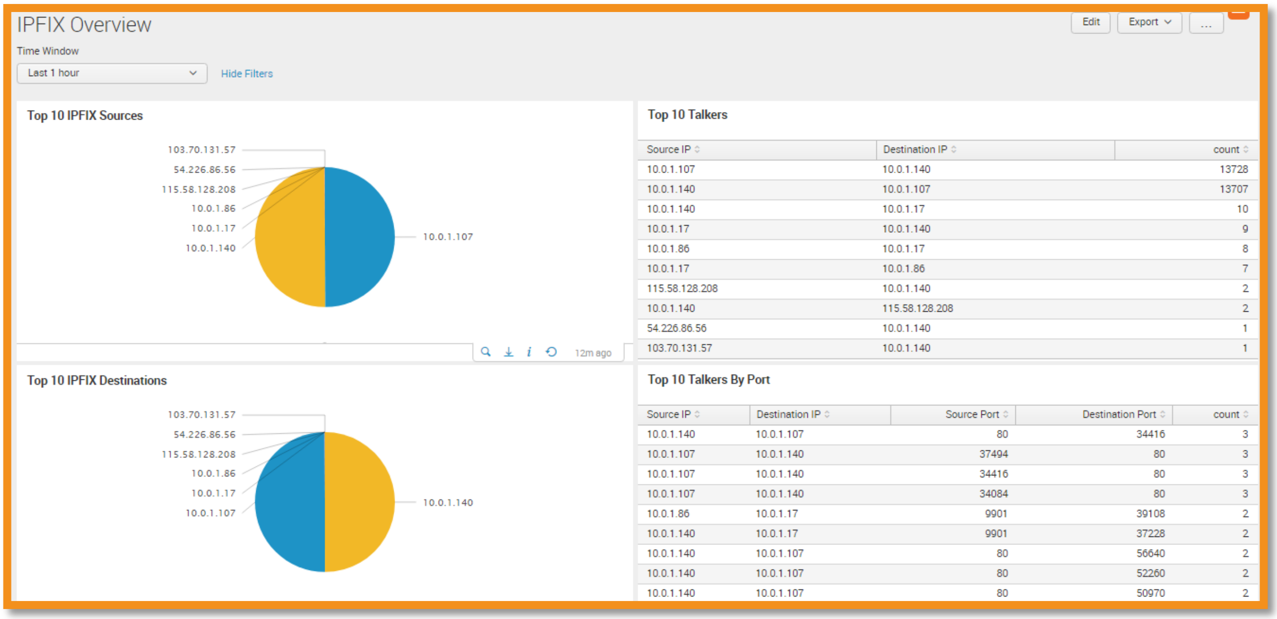
Base Event Type

index=main

Once the initial configuration is complete, click the Save button to start using the application.

- 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.



IPFIX Overview

Top 10 Talkers

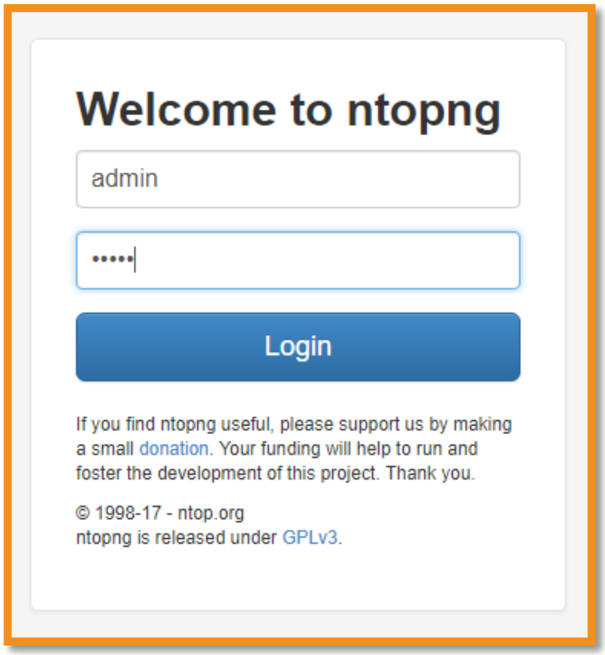
Source IP	Destination IP	count
10.0.1.107	10.0.1.140	13728
10.0.1.140	10.0.1.107	13707
10.0.1.140	10.0.1.17	10
10.0.1.17	10.0.1.140	9
10.0.1.86	10.0.1.17	8
10.0.1.17	10.0.1.86	7
115.58.128.208	10.0.1.140	2
10.0.1.140	115.58.128.208	2
54.226.86.56	10.0.1.140	1
103.70.131.57	10.0.1.140	1

Top 10 Talkers By Port

Source IP	Destination IP	Source Port	Destination Port	count
10.0.1.140	10.0.1.107	80	34416	3
10.0.1.107	10.0.1.140	37494	80	3
10.0.1.107	10.0.1.140	34416	80	3
10.0.1.107	10.0.1.140	34084	80	3
10.0.1.86	10.0.1.17	9901	39108	2
10.0.1.140	10.0.1.17	9901	37228	2
10.0.1.140	10.0.1.107	80	56640	2
10.0.1.140	10.0.1.107	80	52260	2
10.0.1.140	10.0.1.107	80	50970	2

4. **Login to NtopNG.**

- Login to **NtopNG** by using its Public IP and credentials provided in the deemo lab launch page.



Welcome to ntopng

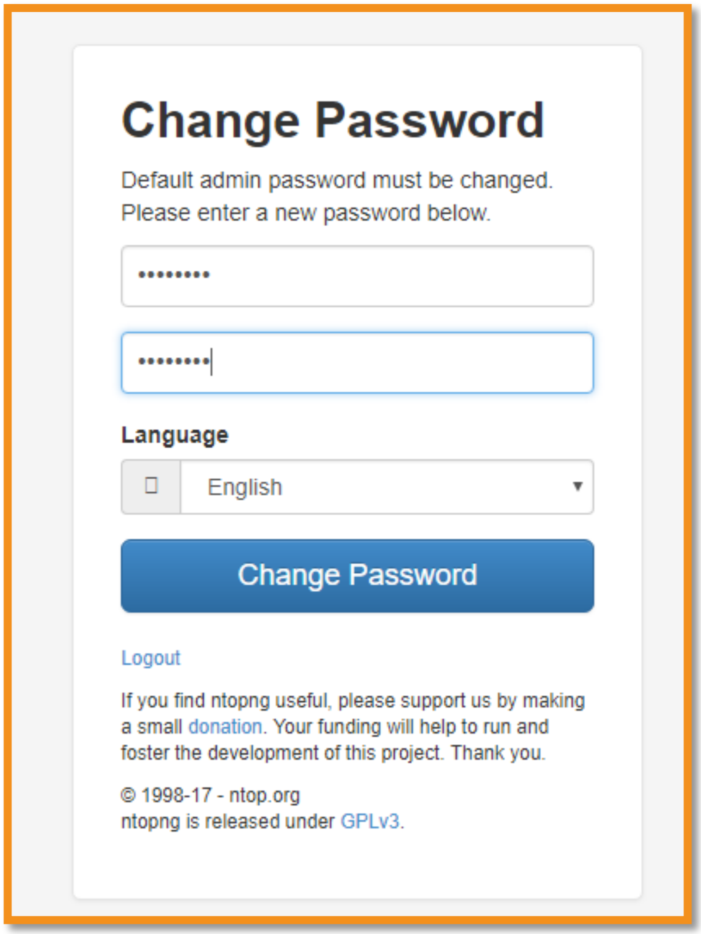
admin

•••••

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.

© 1998-17 - ntop.org
ntopng is released under GPLv3.

- Change the Password form the change password page.



Change Password

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

••••••••

••••••••

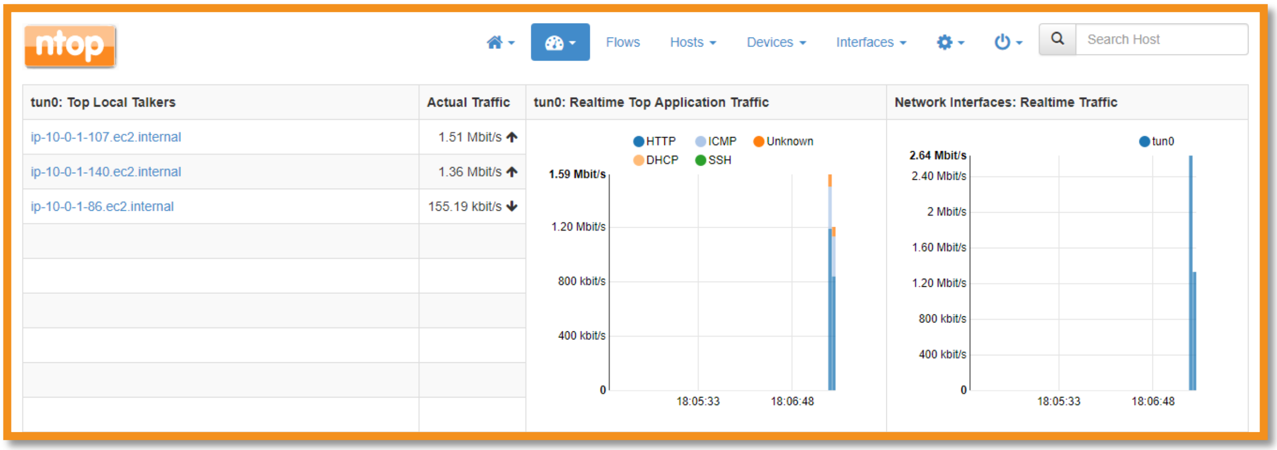
Language

English ▾

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.

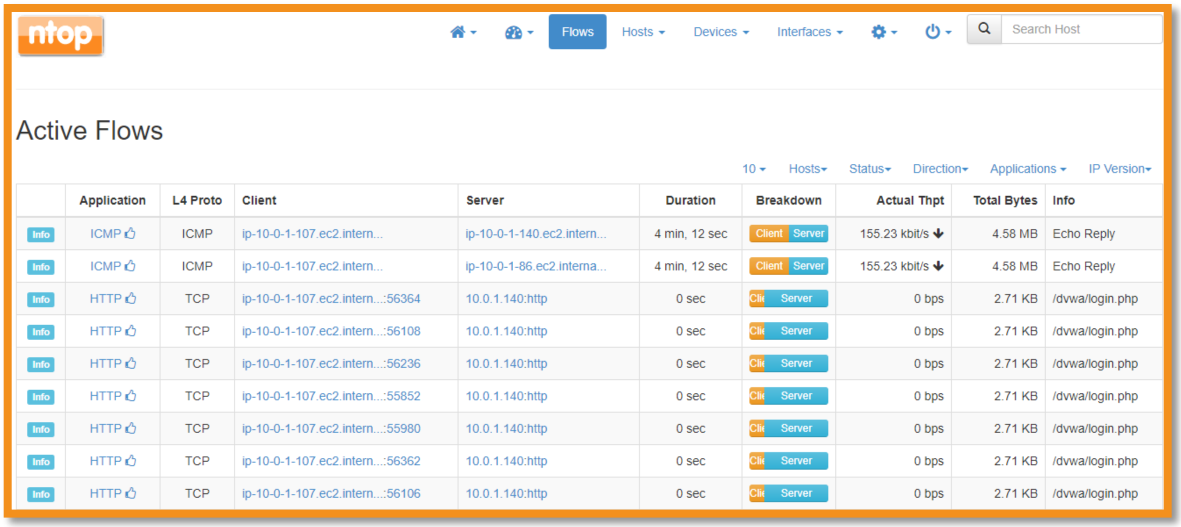
© 1998-17 - ntop.org
ntopng is released under GPLv3.

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



tun0: Top Local Talkers	Actual Traffic
ip-10-0-1-107.ec2.internal	1.51 Mbit/s ↑
ip-10-0-1-140.ec2.internal	1.36 Mbit/s ↑
ip-10-0-1-86.ec2.internal	155.19 kbit/s ↓

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

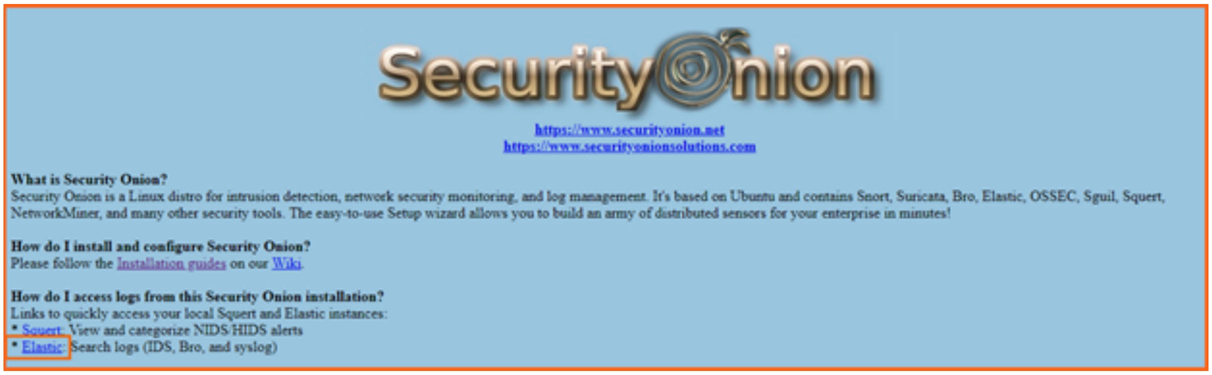


Active Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	ICMP	ICMP	ip-10-0-1-107.ec2.intern...	ip-10-0-1-140.ec2.intern...	4 min, 12 sec	Client Server	155.23 kbit/s ↓	4.58 MB	Echo Reply
Info	ICMP	ICMP	ip-10-0-1-107.ec2.intern...	ip-10-0-1-86.ec2.interna...	4 min, 12 sec	Client Server	155.23 kbit/s ↓	4.58 MB	Echo Reply
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:56364	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:56108	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:56236	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:55852	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:55980	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:56362	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:56106	10.0.1.140:http	0 sec	Clie Server	0 bps	2.71 KB	/dvwa/login.php

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

- Go to **Security Onion** using its public ip provided in the deemo lab 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.



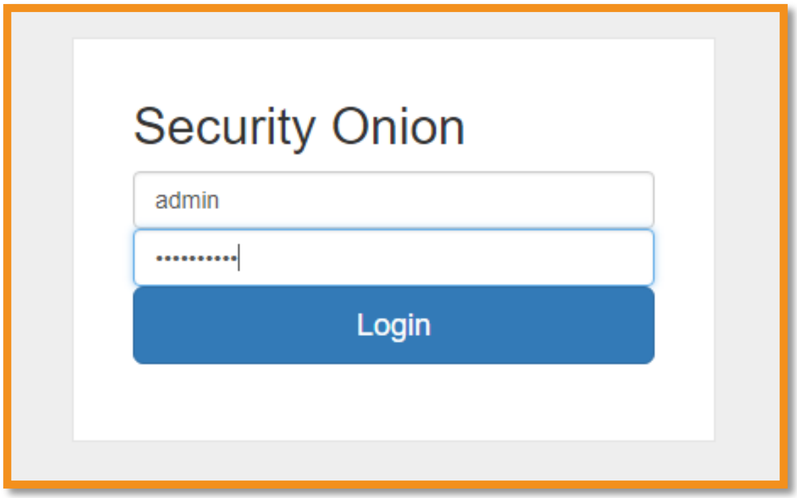
https://www.securityonion.net
https://www.securityonionsolutions.com

What is Security Onion?
Security Onion is a Linux distro for intrusion detection, network security monitoring, and log management. It's based on Ubuntu and contains Snort, Suricata, Bro, Elastic, OSSEC, Sguil, Squert, NetworkMiner, and many other security tools. The easy-to-use Setup wizard allows you to build an army of distributed sensors for your enterprise in minutes!

How do I install and configure Security Onion?
Please follow the Installation guides on our Wiki.

How do I access logs from this Security Onion installation?
Links to quickly access your local Squert and Elastic instances:
* Squert: View and categorize NIDS/HIDS alerts
* Elastic: Search logs (IDS, Bro, and syslog)

- This will launch **Kibaba**. Login to the **Kibana** using the credentials provided in the deemo lab launch page.



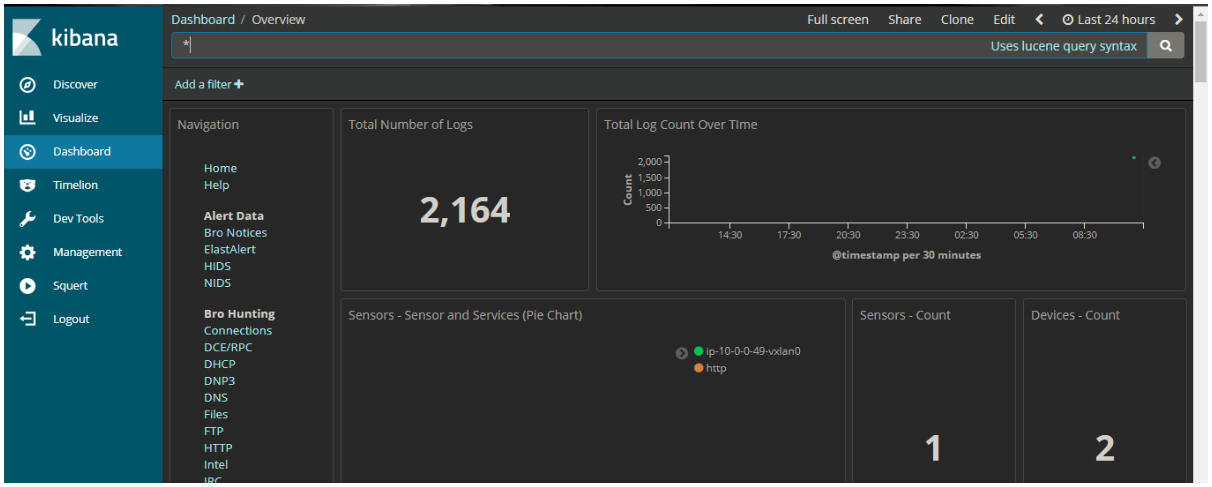
Security Onion

admin

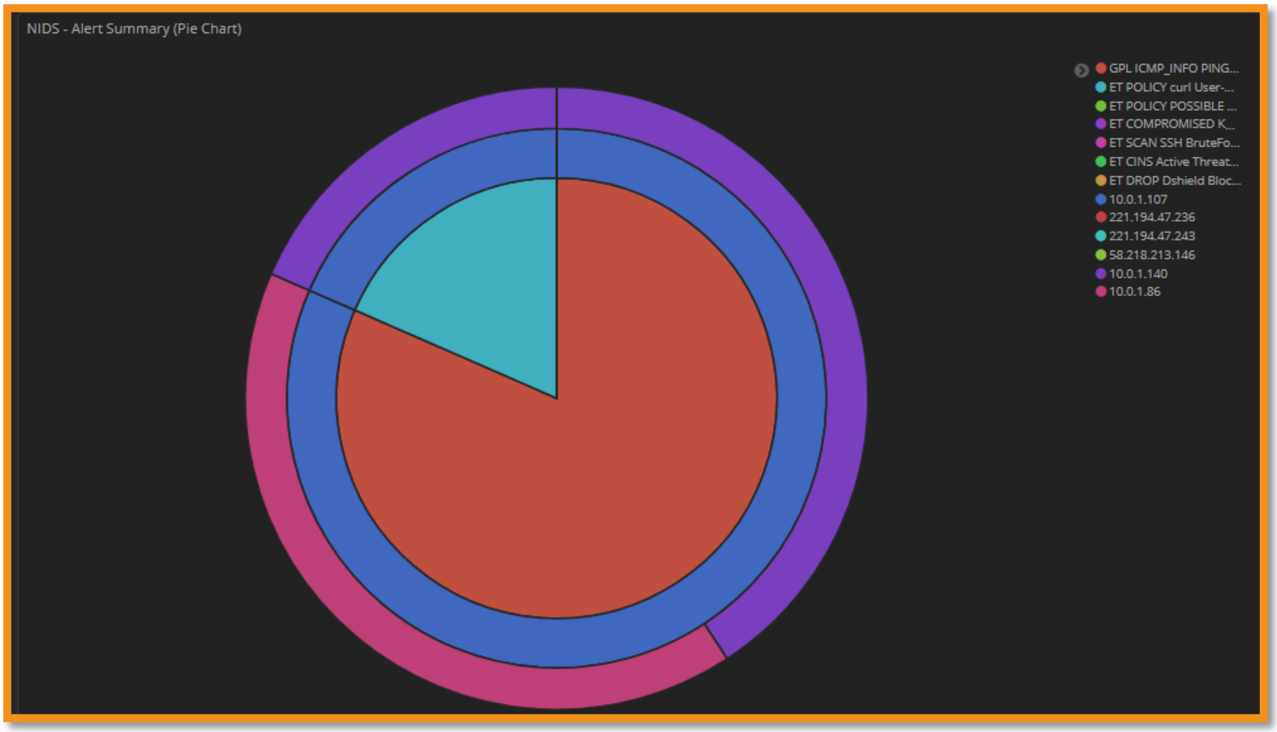
••••••••••

- 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.



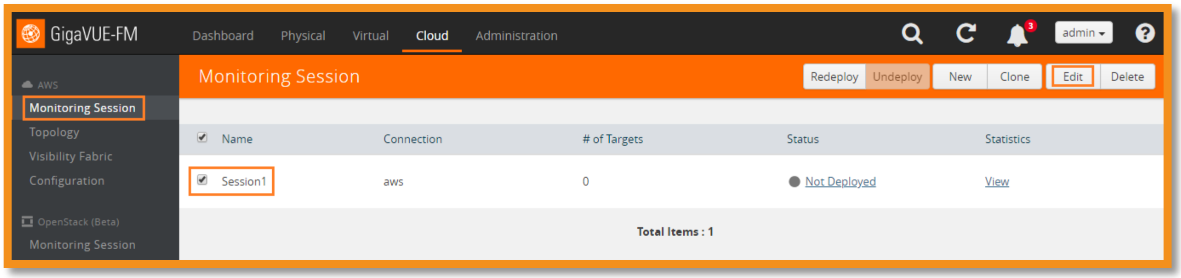
- Here, you can see the traffic alerts coming from workloads.
- Scroll down for more visibility as shown in the following figure.



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 **Security Onion** tool tunnel and the HTTP traffic (port 80) are sent to the **NtopNG** tool tunnel.

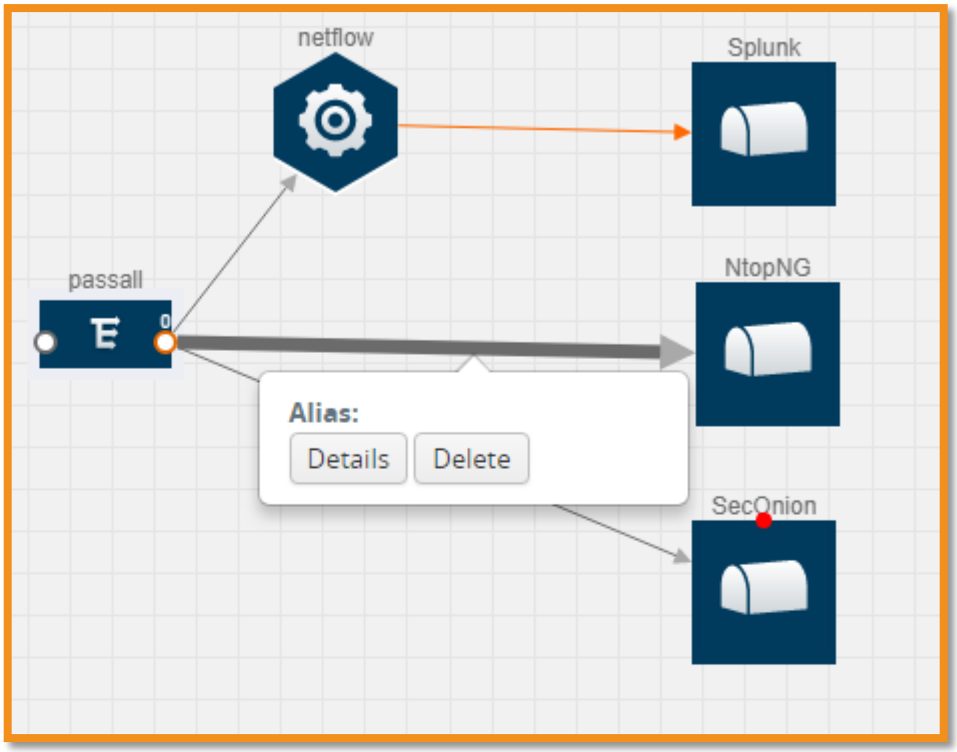
1. **Return to GigaVUE Fabric Manager and edit the monitoring session again.**
    - Login to **GigaVUE-FM** and click **Cloud** from the top menu.
    - Select **Monitoring Session** option from the left menu to open **Monitoring Session** page.
    - Select the check box next to the monitoring session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



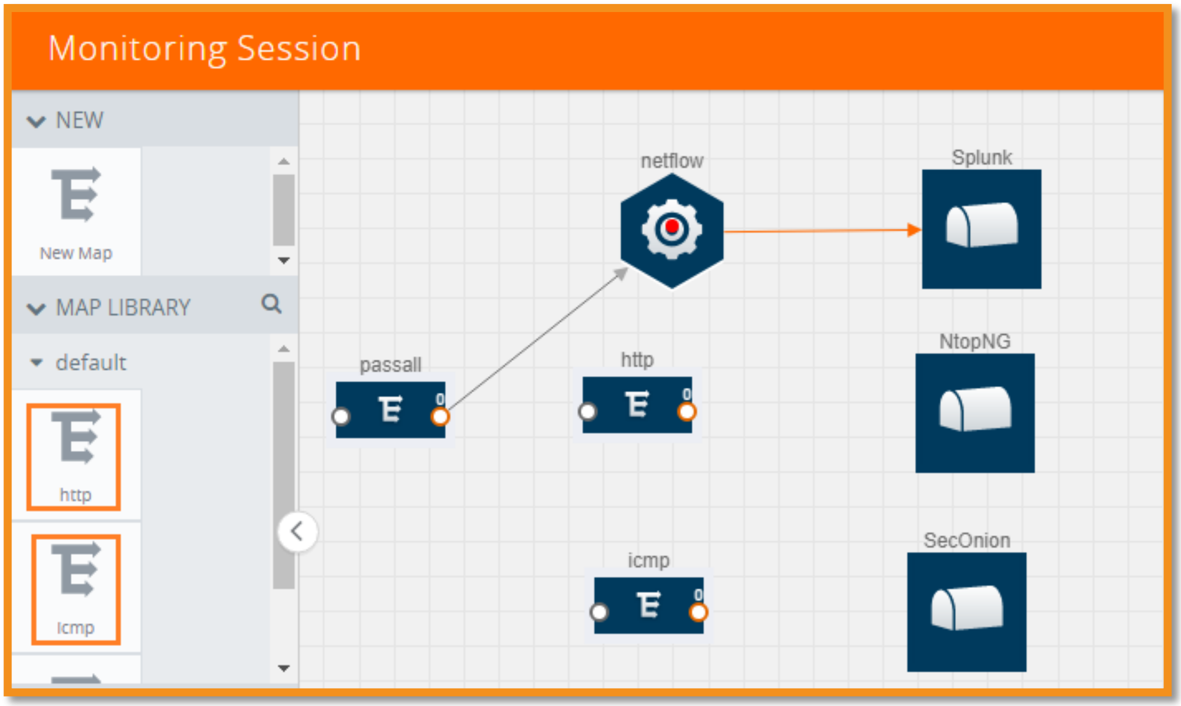
☑ Name	Connection	# of Targets	Status	Statistics
☑ Session1	aws	0	● Not Deployed	View

Total Items : 1

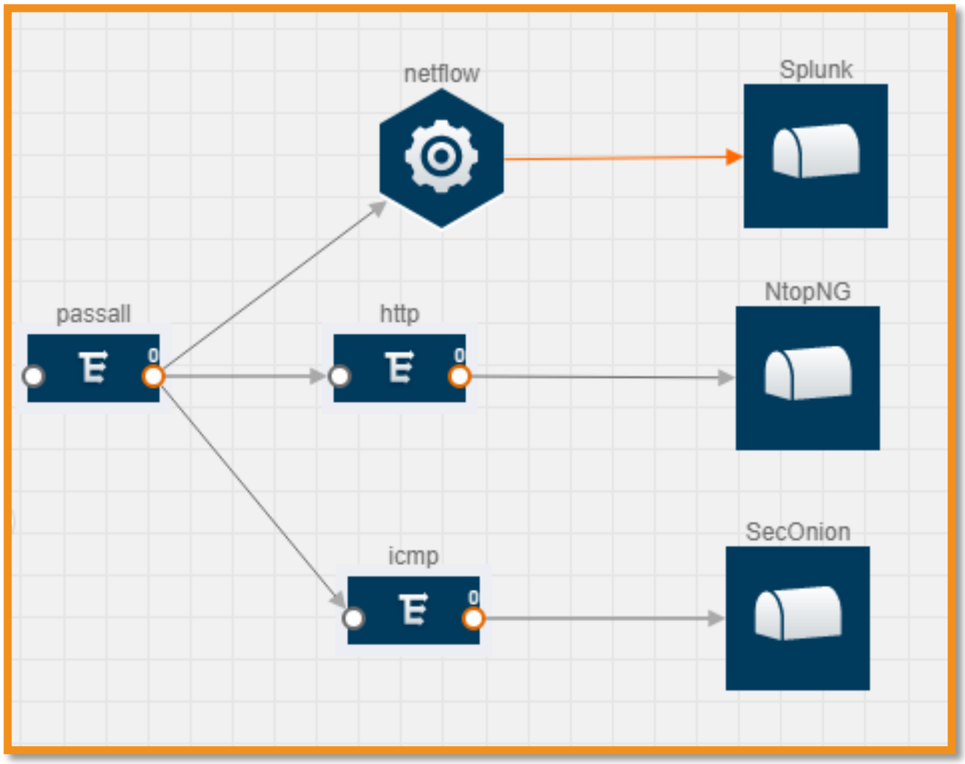
2. **Deleting the links.**
    - Delete the links (Connector arrows) from **passall** to **NtopNG** and **SecOnion** tunnels.



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

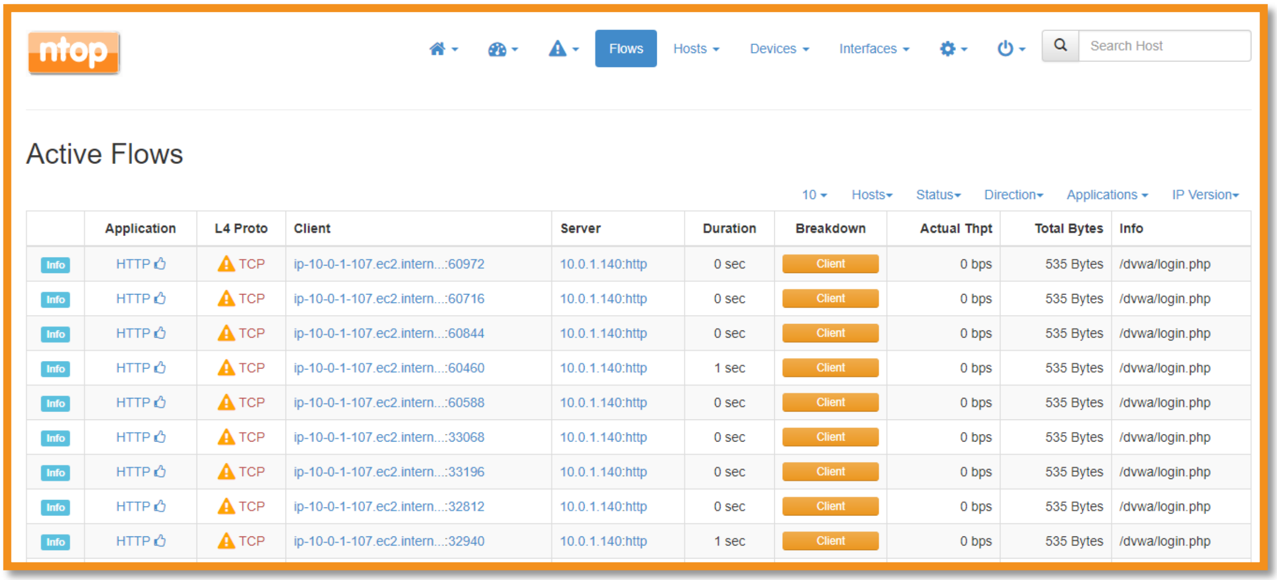


- Hover over the **passall** map and drag a line to connect the red dots to **http** map and **icmp** map.
- Hover over the **http** map and drag a line to connect the red dots to **NtopNG** tunnel and from **ICMP** map to **SecOnion** tunnel.
- Click **Deploy** button and click **Close**.



- Go back to the **NtopNG**, wait for some time and refresh the page.

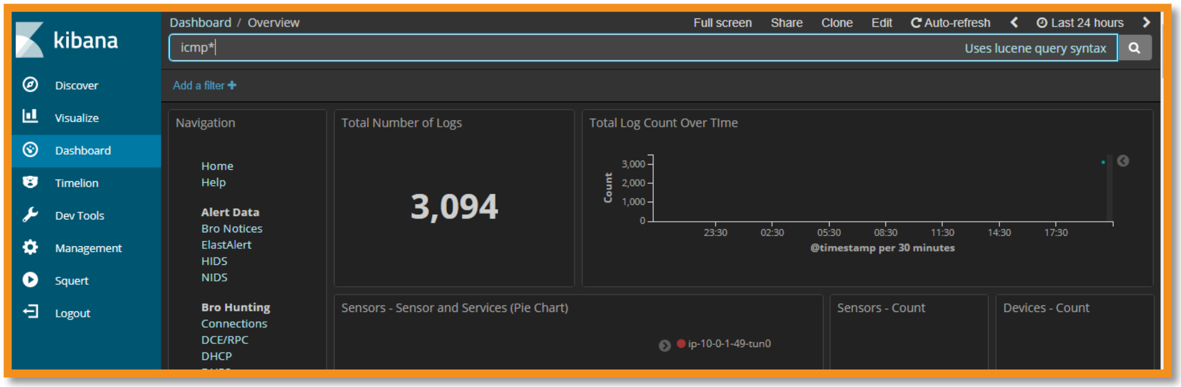
- Click **Flows** from the top menu and you can see the only **HTTP** flows coming from workloads to **NtopNG**.



Active Flows

	Application	L4 Proto	Client	Server	Duration	Breakdown	Actual Thpt	Total Bytes	Info
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:60972	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:60716	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:60844	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:60460	10.0.1.140:http	1 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:60588	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:33068	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:33196	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:32812	10.0.1.140:http	0 sec	Client	0 bps	535 Bytes	/dvwa/login.php
Info	HTTP	TCP	ip-10-0-1-107.ec2.intern...:32940	10.0.1.140:http	1 sec	Client	0 bps	535 Bytes	/dvwa/login.php

- Go back to the **Kibana** dashboard to check **ICMP** traffic.
- Refresh the page and type **icmp*** in search box ,
- You can see the number of **ICMP** logs will increase for every refresh.
- Scroll down to the page to view the detailed information of ICMP traffic.

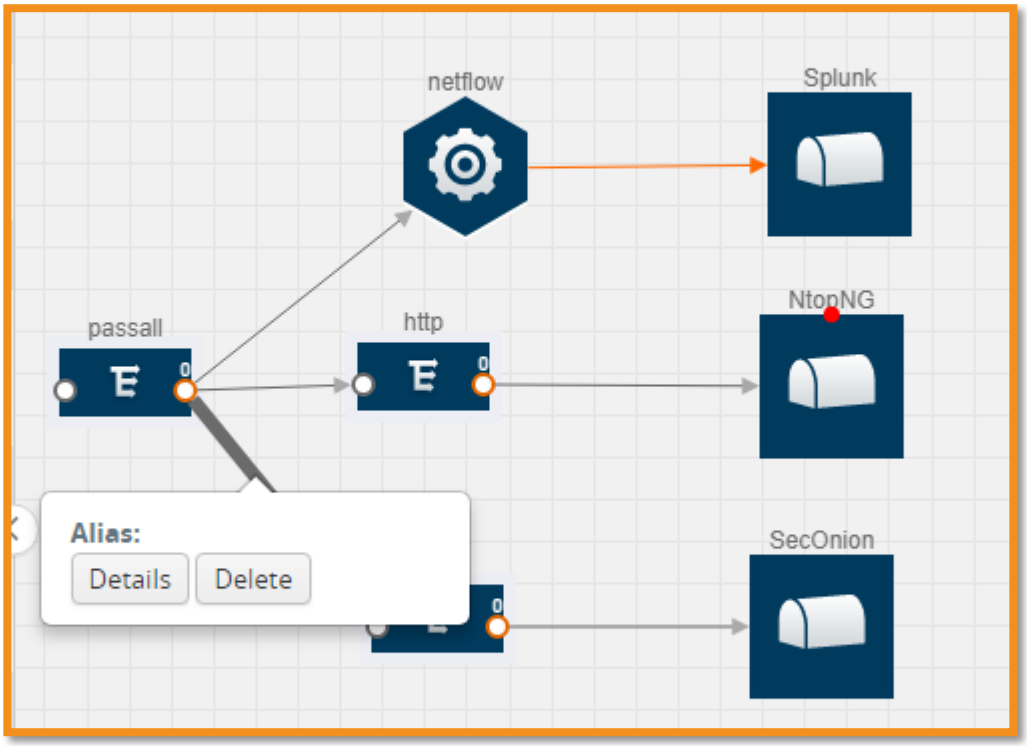


icmp*

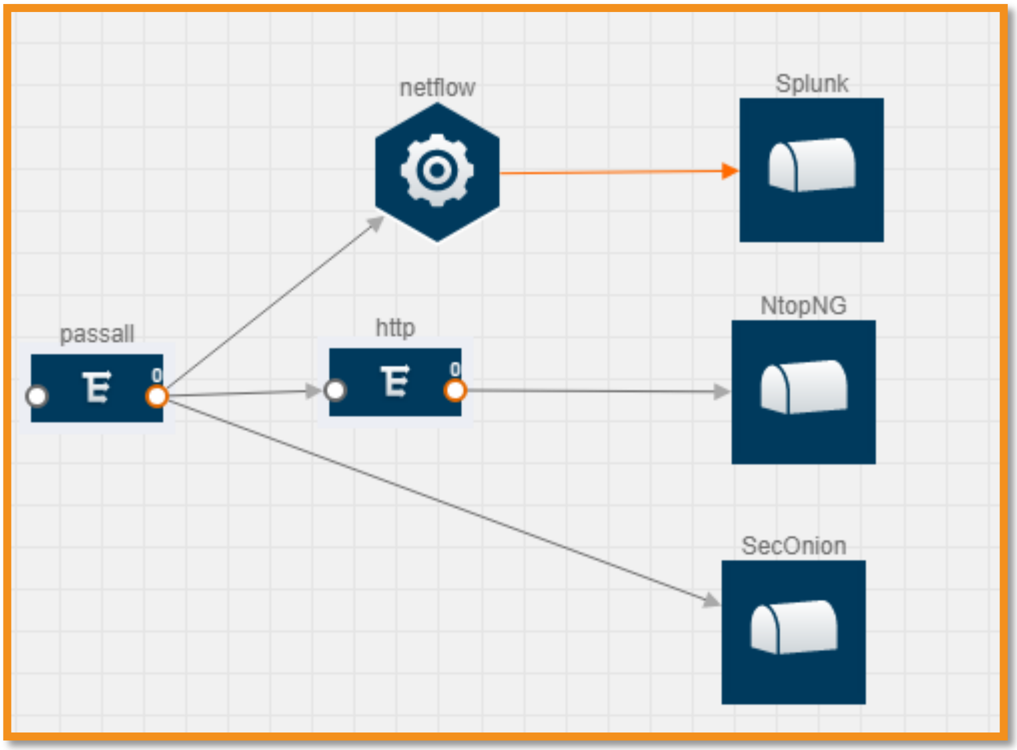
5.3. Use Case 3: Detecting Threats

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 icmp map.**
   - Go back to **Monitoring Session** in **GigaVUE-FM**, delete the links (Connector arrows) from **passall** to **icmp** and **icmp** to **SecOnion**.

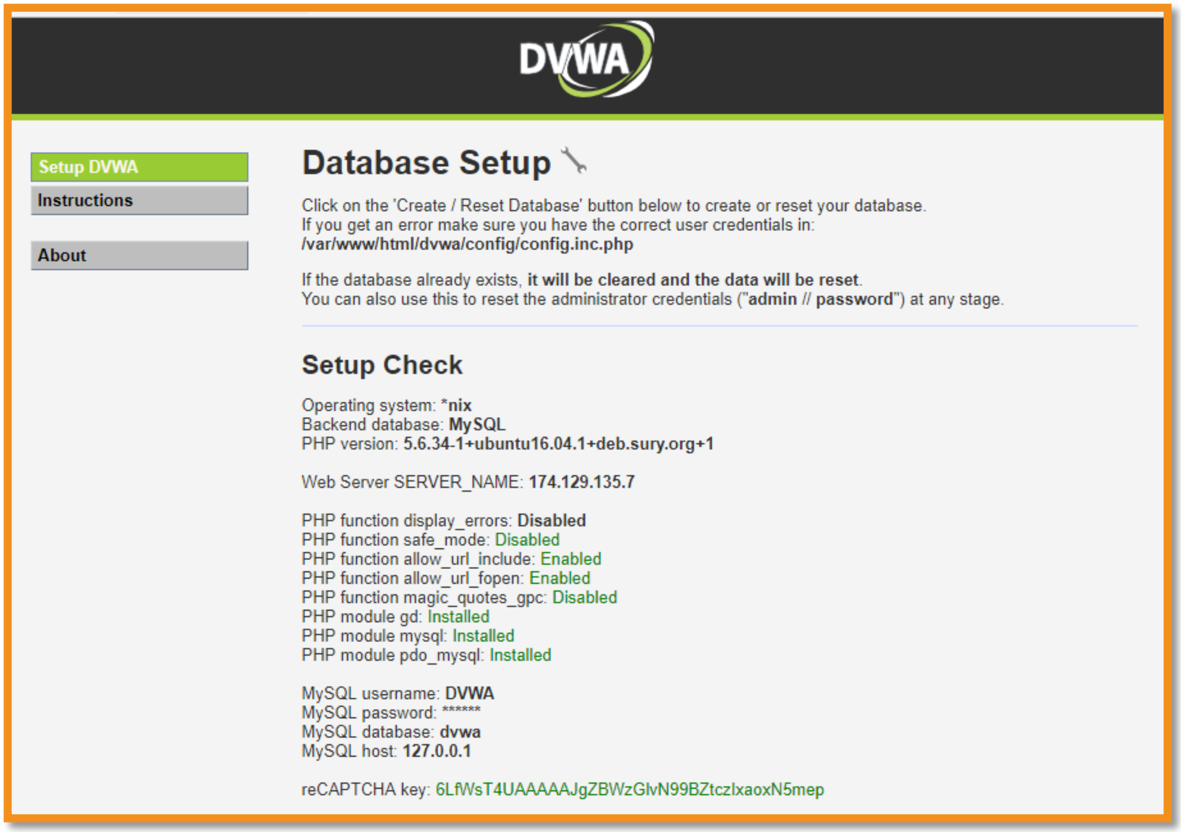


   - Delete **links** (Connector arrow) between **passall** to **icmp** and **SecOnion** and delete **icmp.**
   - Give connection from **passall** to **SecOnion.**
   - Click **Deploy** button and click **OK**.



2. **Login to the DVWA.**

- Open the **DVWA** by using its Public IP provided in the deemo lab launch page.
- Click **Create/Reset Database** button at the bottom of the **DVWA** Home page



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**

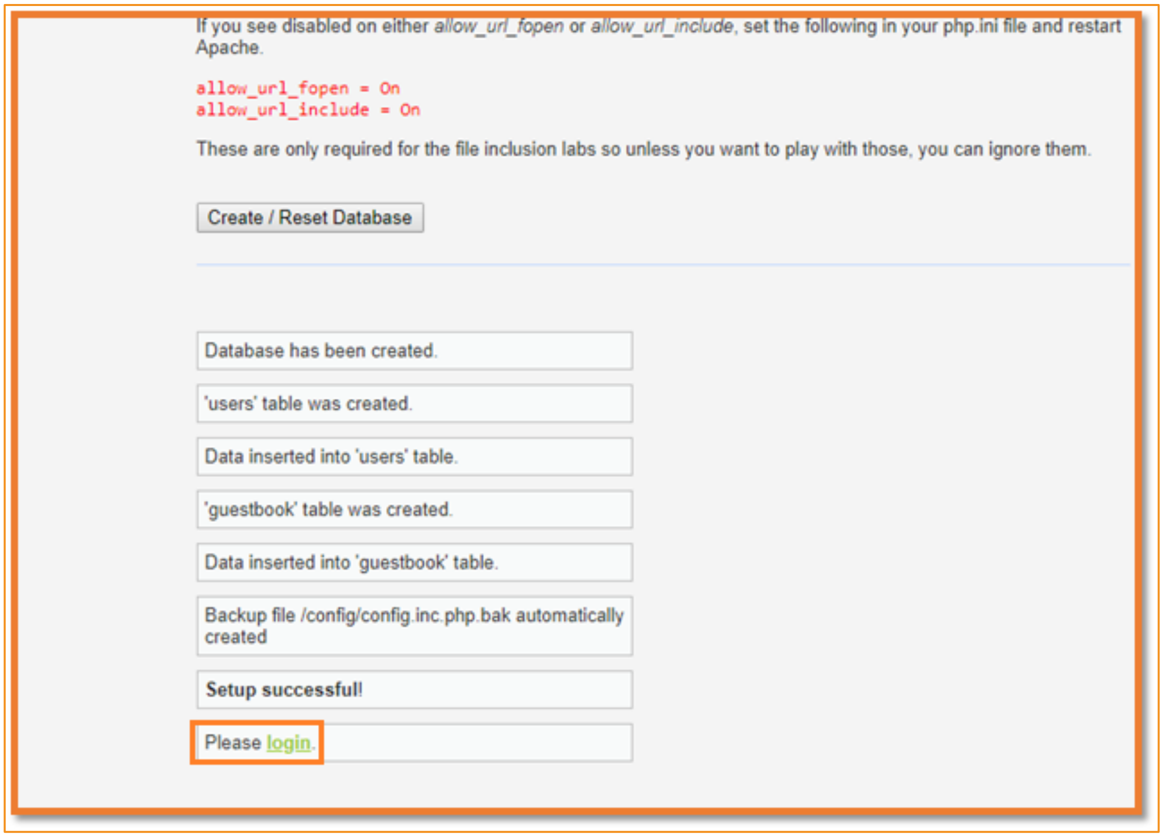
Web Server SERVER_NAME: **174.129.135.7**

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: 6LfWsT4UAAAAAJgZBWzGlvN99BZtczlxaoxN5mep

- 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.

Database has been created.

'users' table was created.

Data inserted into 'users' table.

'guestbook' table was created.

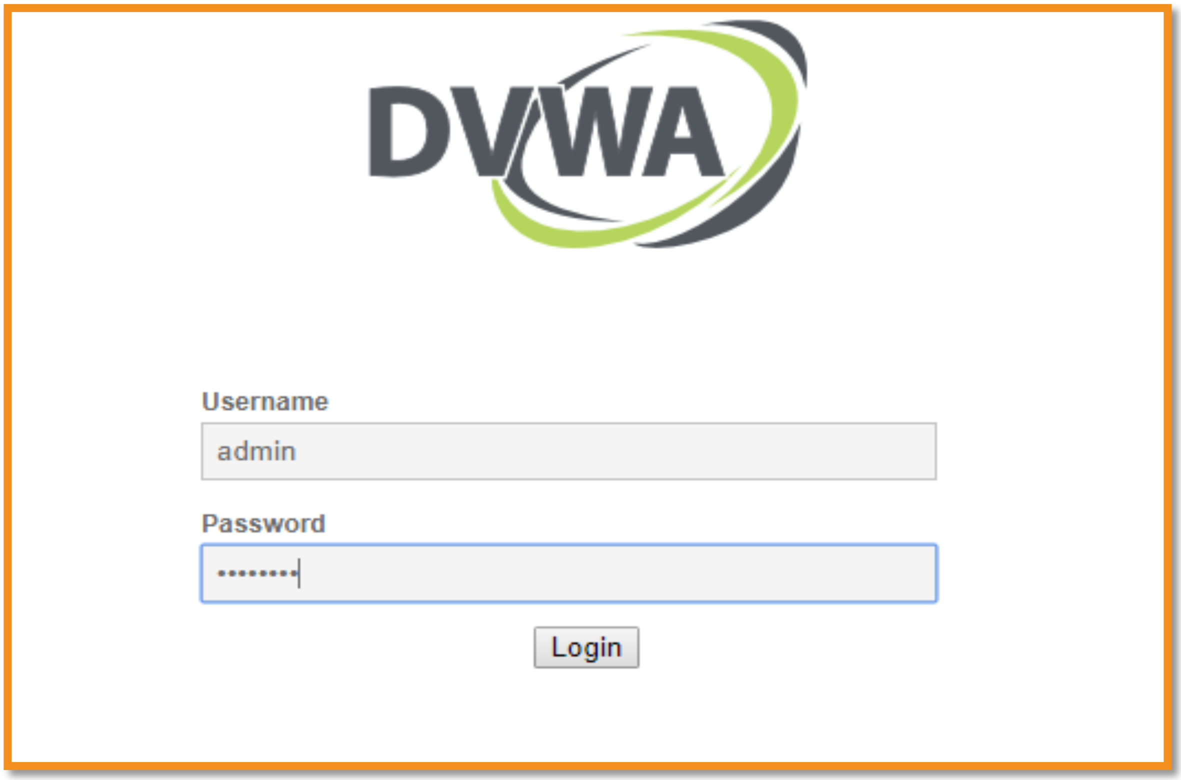
Data inserted into 'guestbook' table.

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

Setup successful!

Please login.

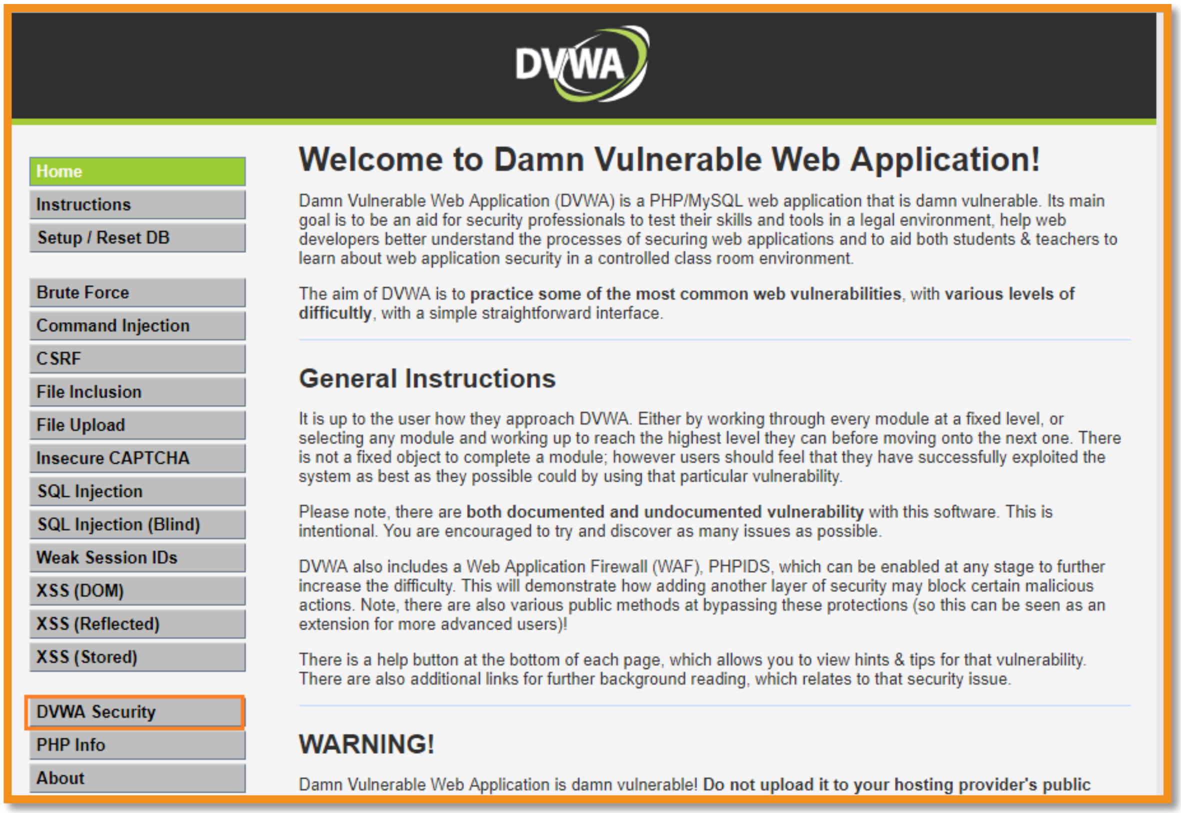
- Login to the **DVWA** by using DVWA credentials provided in the deemo lab launch page.



Username: admin

Password: ••••••••

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



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 difficultly**, 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.

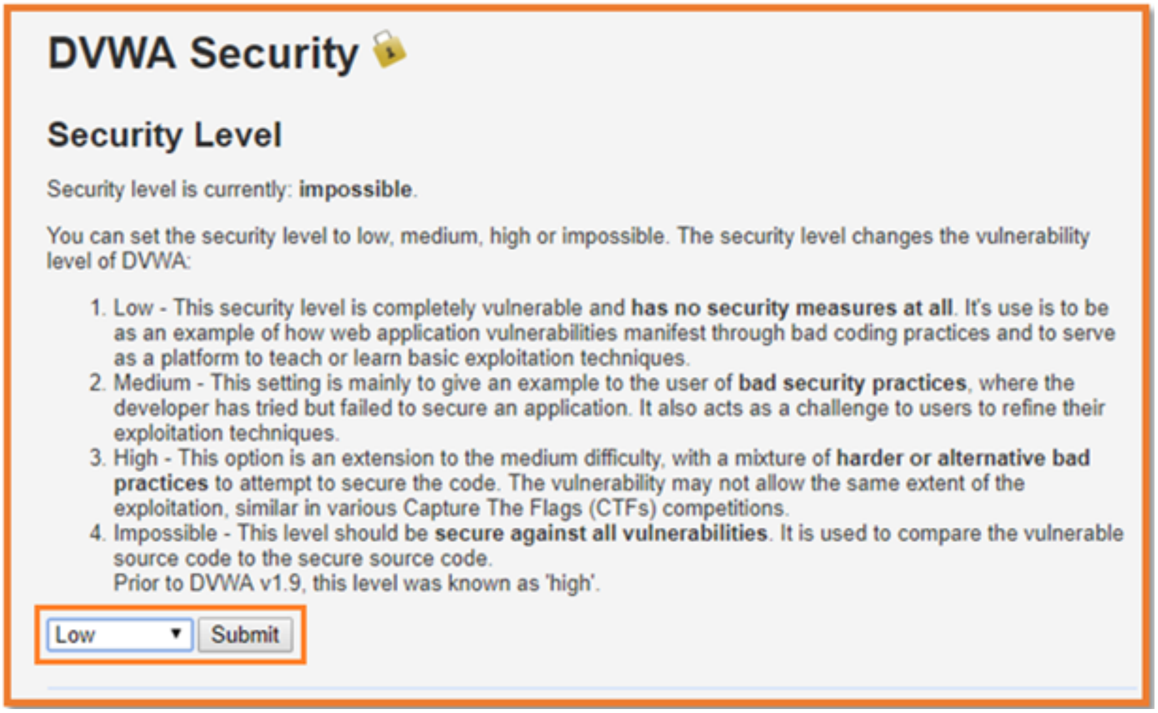
DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections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

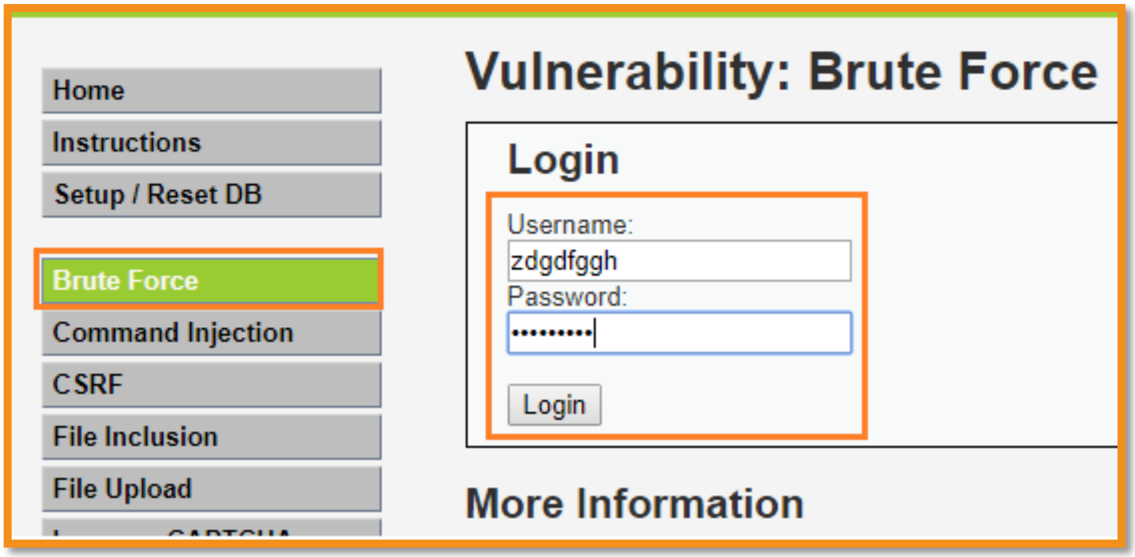
Security level is currently: **impossible**.

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 ▾

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



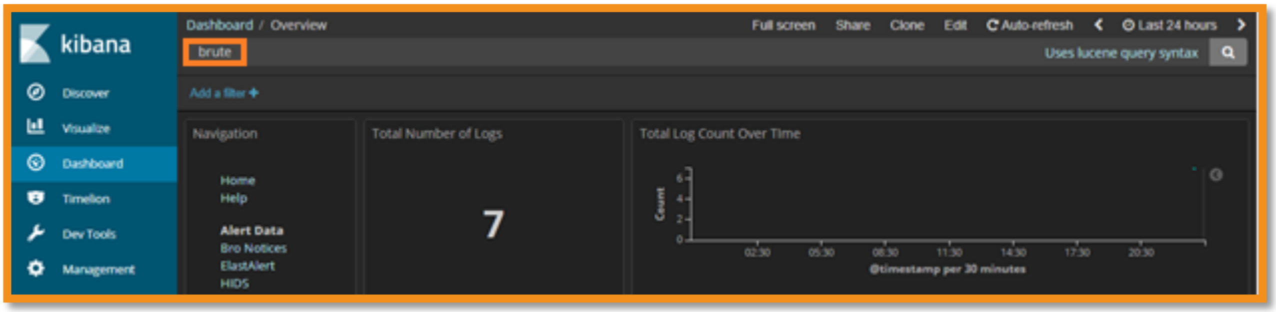
Vulnerability: Brute Force

Login

Username: zdgdfggh

Password: •••••••••

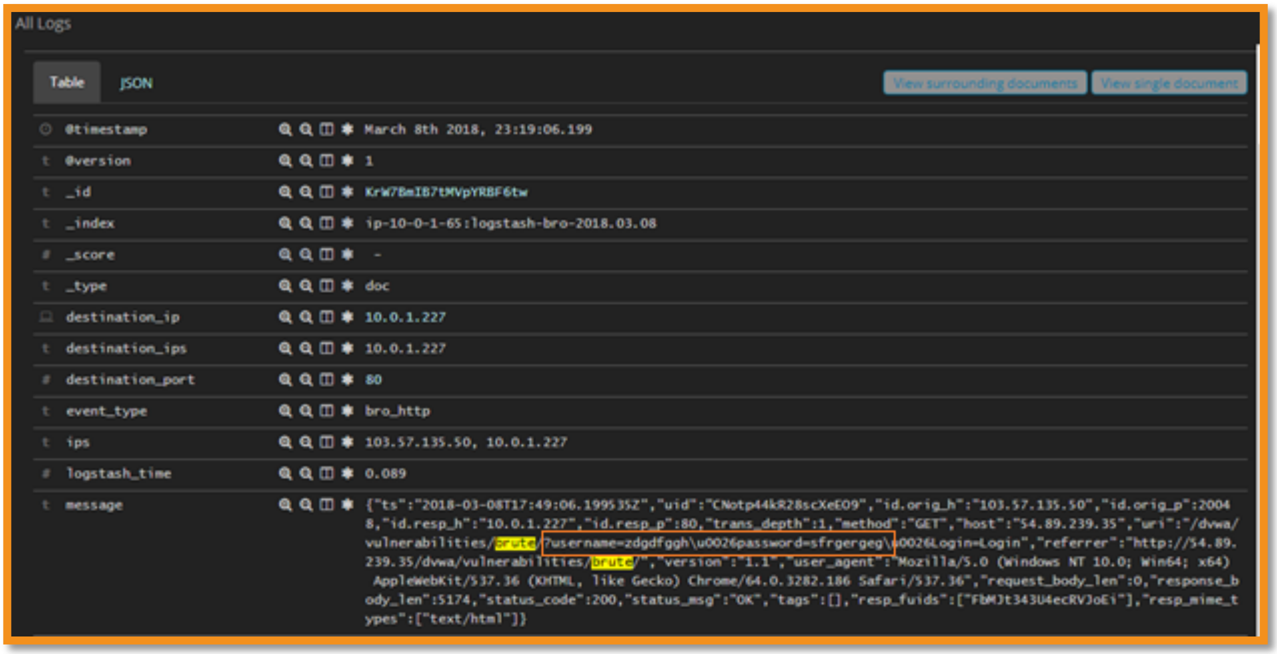
- Go to **Kibana**, and type "**brute" or attacked username** in dashboard search box.
- To reflect the bad traffic, wait for few seconds and refresh the page.



brute

7

- 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.

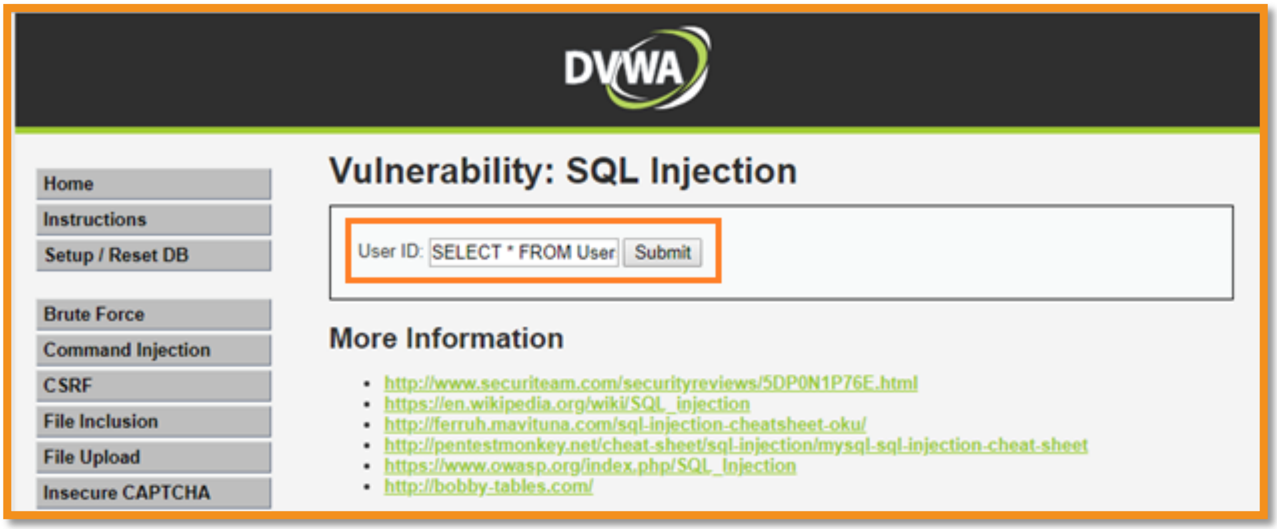


```
@timestamp          March 8th 2018, 23:19:06.199
@version            1
_id                 KrW7BmIB7tMVpYRBF6tw
_index              ip-10-0-1-65:logstash-bro-2018.03.08
_score              -
_type               doc
destination_ip      10.0.1.227
destination_ips     10.0.1.227
destination_port    80
event_type          bro_http
ips                 103.57.135.50, 10.0.1.227
logstash_time       0.089
message             {"ts":"2018-03-08T17:49:06.199535Z","uid":"CNotp44kR28scXeE09","id.orig_h":"103.57.135.50","id.orig_p":2004
                    8,"id.resp_h":"10.0.1.227","id.resp_p":80,"trans_depth":1,"method":"GET","host":"54.89.239.35","uri":"/dvwa/
                    vulnerabilities/brute/?username=zdgdfggh\u0026password=sfrgergeg\u0026Login=Login","referrer":"http://54.89.
                    239.35/dvwa/vulnerabilities/brute/","version":"1.1","user_agent":"Mozilla/5.0 (Windows NT 10.0; Win64; x64)
                     AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.186 Safari/537.36","request_body_len":0,"response_b
                    ody_len":5174,"status_code":200,"status_msg":"OK","tags":[],"resp_fuids":["FbMJt343U4ecRVJoEi"],"resp_mime_t
                    ypes":["text/html"]}
```

- 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'
```

6



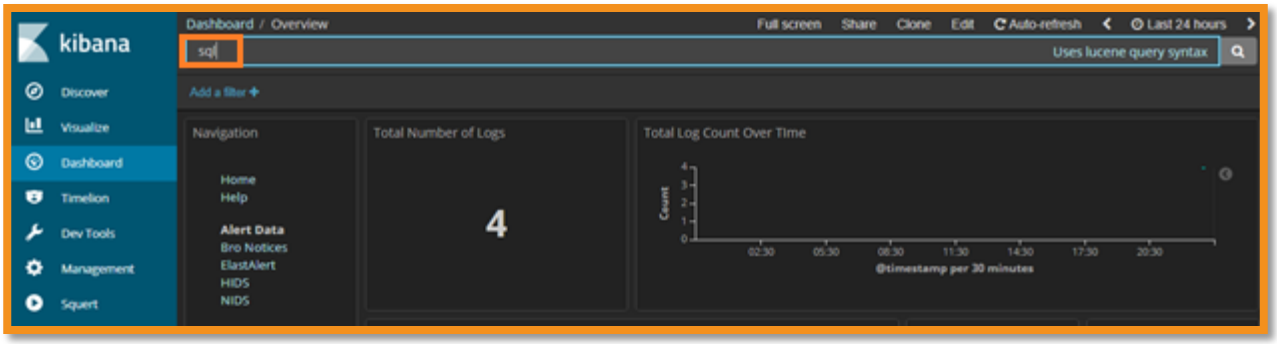
Vulnerability: SQL Injection

User ID: SELECT * FROM User

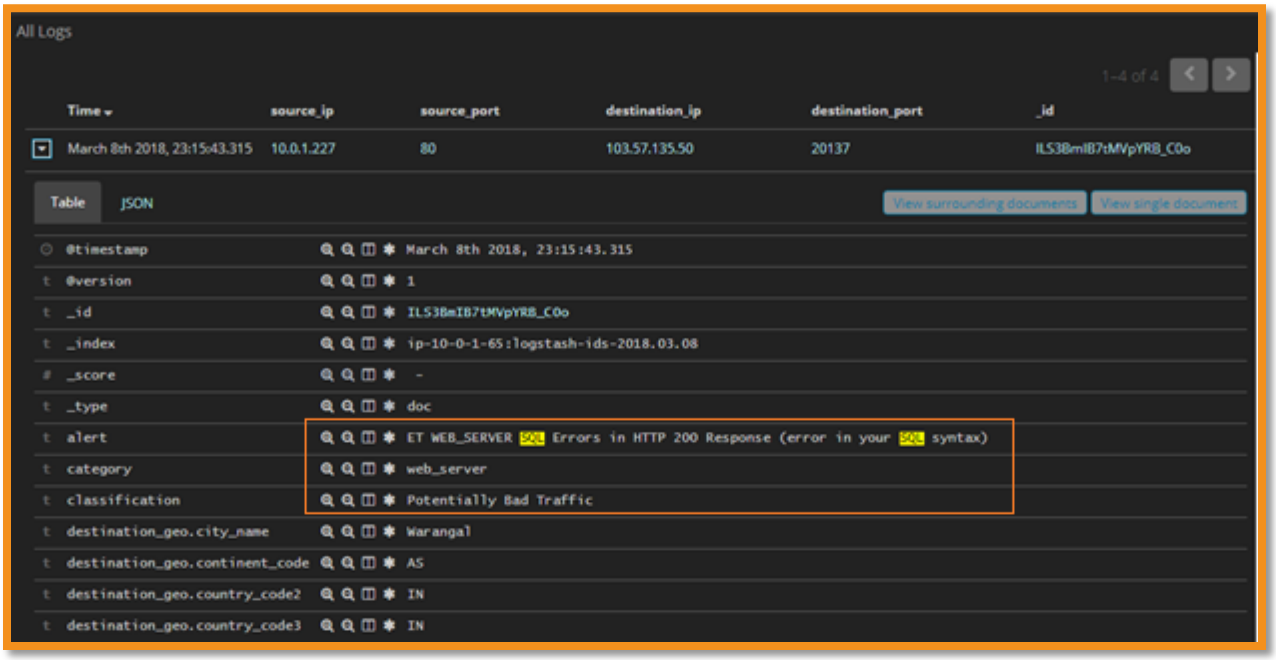
More Information

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
- https://en.wikipedia.org/wiki/SQL_injection
- http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
- http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

- Go to **Kibana**, and 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.



Time	source_ip	source_port	destination_ip	destination_port	_id
March 8th 2018, 23:15:43.315	10.0.1.227	80	103.57.135.50	20137	ILS3BmIB7tMVpYRB_COo

○	@timestamp	March 8th 2018, 23:15:43.315
t	@version	1
t	_id	ILS3BmIB7tMVpYRB_COo
t	_index	ip-10-0-1-65:logstash-ids-2018.03.08
#	_score	-
t	_type	doc
t	alert	ET WEB_SERVER SQL Errors in HTTP 200 Response (error in your SQL syntax)
t	category	web_server
t	classification	Potentially Bad Traffic
t	destination_geo.city_name	Warangal
t	destination_geo.continent_code	AS
t	destination_geo.country_code2	IN
t	destination_geo.country_code3	IN