FortiAnalyzer Analyst Lab Guide

for FortiAnalyzer 7.2

FORTINET
Training Institute

Fortinet Training Institute - Library

https://training.fortinet.com

Fortinet Product Documentation

https://docs.fortinet.com

Fortinet Knowledge Base

https://kb.fortinet.com

Fortinet Fuse User Community

https://fusecommunity.fortinet.com/home

Fortinet Forums

https://forum.fortinet.com

Fortinet Product Support

https://support.fortinet.com

FortiGuard Labs

https://www.fortiguard.com

Fortinet Training Program Information

https://www.fortinet.com/nse-training

Fortinet | Pearson VUE

https://home.pearsonvue.com/fortinet

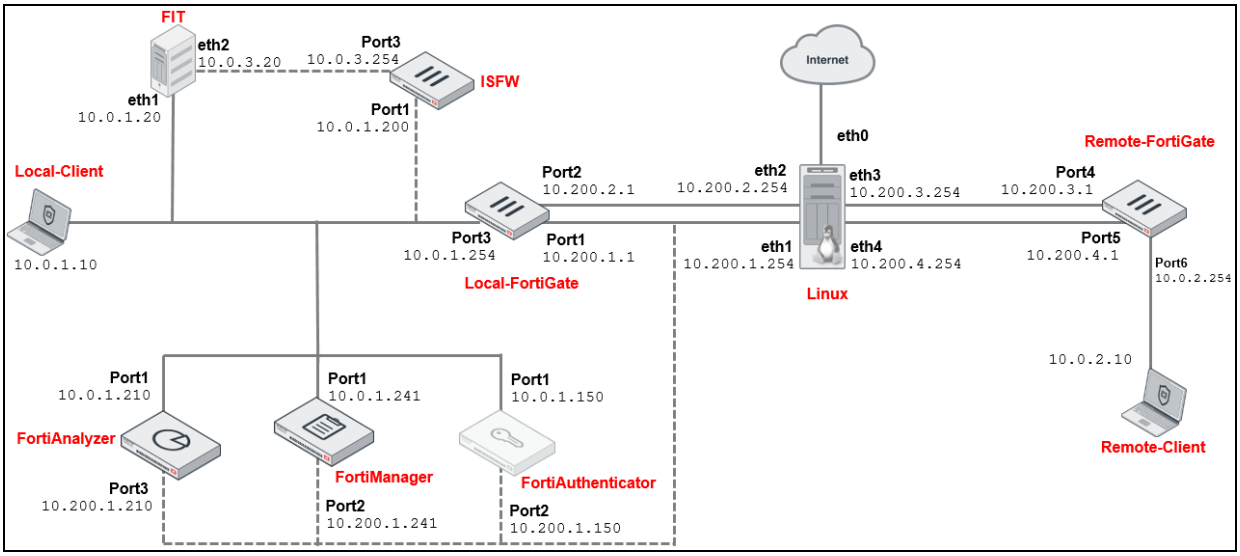
Fortinet Training Institute Helpdesk (training questions, comments, feedback)

https://helpdesk.training.fortinet.com/support/home

12/1/2022

TABLE OF CONTENTS

Network Topology



Lab 1: Initial Configuration

In this lab, you will access FortiAnalyzer from the CLI and GUI.

Objectives

- Explore FortiAnalyzer GUI and CLI interfaces

Time to Complete

Estimated: 25 minutes

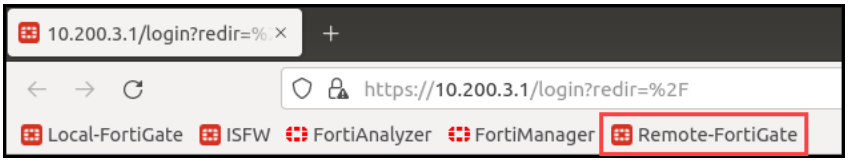
Prerequisites

Before beginning this lab, you must update the firmware and initial configuration on Local-FortiGate, ISFW, and Remote-FortiGate.

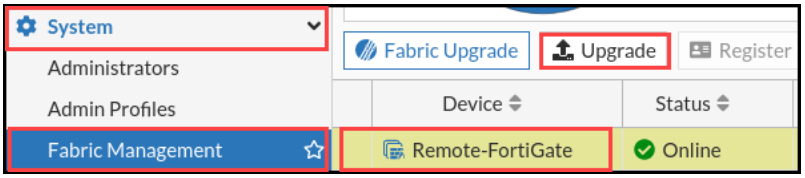
This lab environment is also used for the FortiGate Security and FortiGate Infrastructure 7.2.0 training, and initializes in a different state from what is required for the FortiAnalyzer 7.2.1 training.

To update the FortiGate firmware on all FortiGate devices

1. Log in to the Local-Client VM with the username `Administrator` and password `password`.
2. Open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.You can use the links in the favorites bar to access all devices, as shown in the following image:

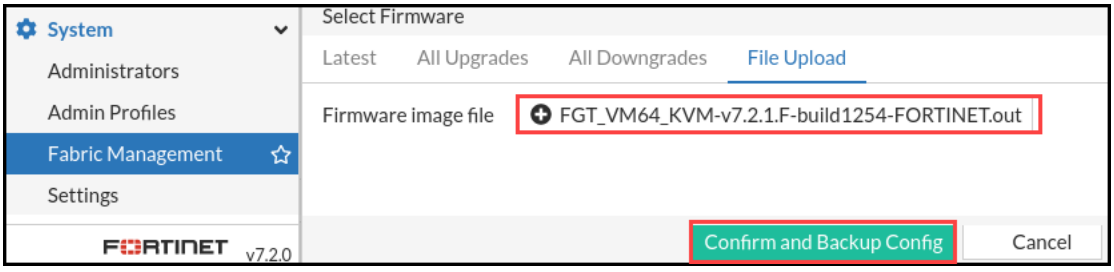


3. Click **System** > **Fabric Management** > **Remote-FortiGate**, and then click **Upgrade**.



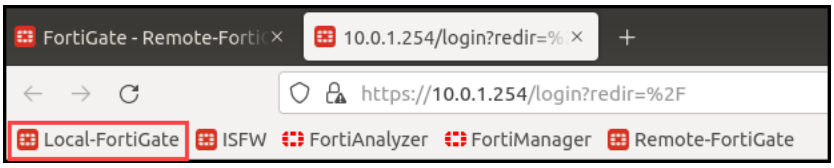
4. Click **File Upload**, and then click **Browse**.

5. Browse to **Desktop** > **Resources** > **FortiAnalyzer Analyst** > **FGT-Firmware**, select `FGT_VM64_KVM-v7.2.1-build1254-FORTINET.out`, and then click **Select** to load the file.
6. Click **Confirm and Backup Config**, and then click **Continue** on the warning window to initiate the upgrade.

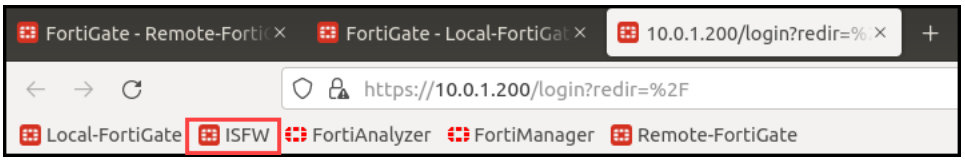


The system starts rebooting.

7. Open another browser tab, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.



8. Repeat this procedure to update the firmware for Local-FortiGate.
9. Open a third browser tab, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.

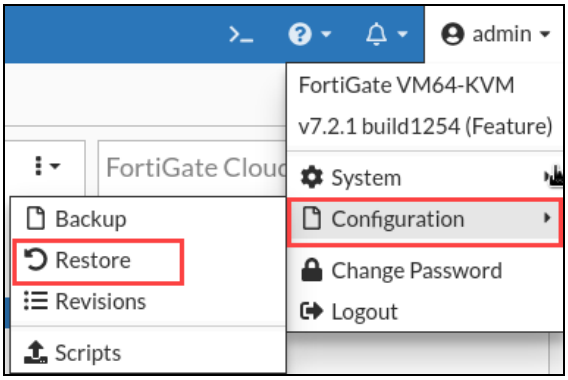


10. Repeat this procedure to update the firmware for ISFW.

To restore the Remote-FortiGate configuration file

Make sure you restore the correct configuration file on the correct device. The name of the configuration file matches the name of the device that it must be restored on.

1. On the Local-Client VM, open a browser, and then log in to the Remote-FortiGate GUI at `10.200.3.1` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.

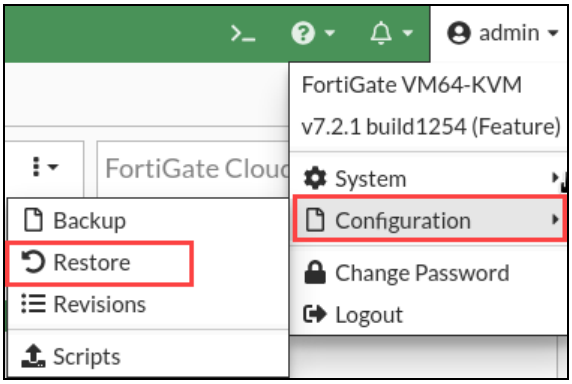


3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer Analyst** > **LAB-1** > `Remote-FortiGate_initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the Local-FortiGate configuration file

1. On the Local-Client VM, open a browser, and then log in to the Local-FortiGate GUI at `10.0.1.254` with the username `admin` and password `password`.

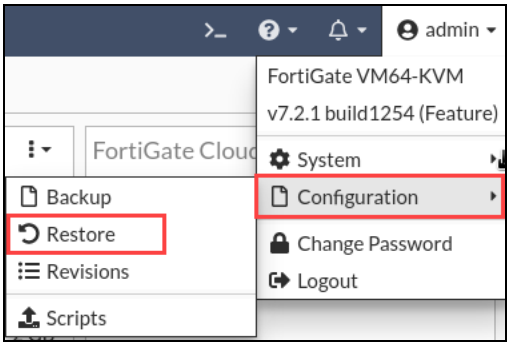
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer Analyst** > **LAB-1** > `Local-FortiGate_initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

To restore the ISFW configuration file

1. On the Local-Client VM, open a browser, and then log in to the ISFW GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the upper-right corner of the screen, click **admin**, and then click **Configuration** > **Restore**.



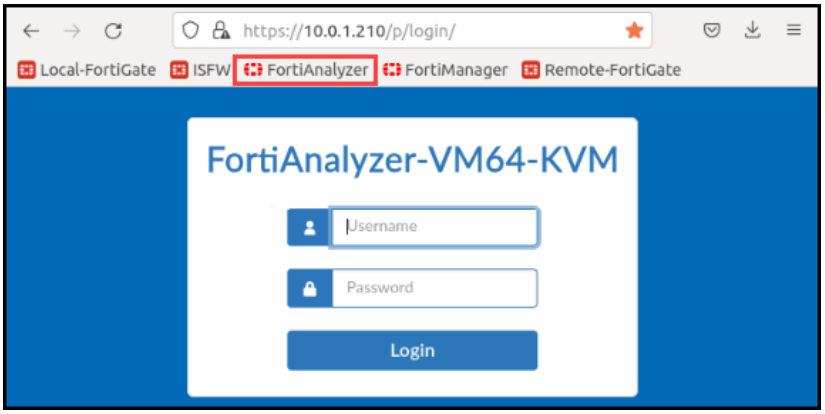
3. Click **Local PC**, and then click **Upload**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer Analyst** > **LAB-1** > `ISFW_initial.conf`, and then click **Select**.
5. Click **OK**.
6. Click **OK** to reboot.

Exercise 1: Accessing the FortiAnalyzer GUI and CLI

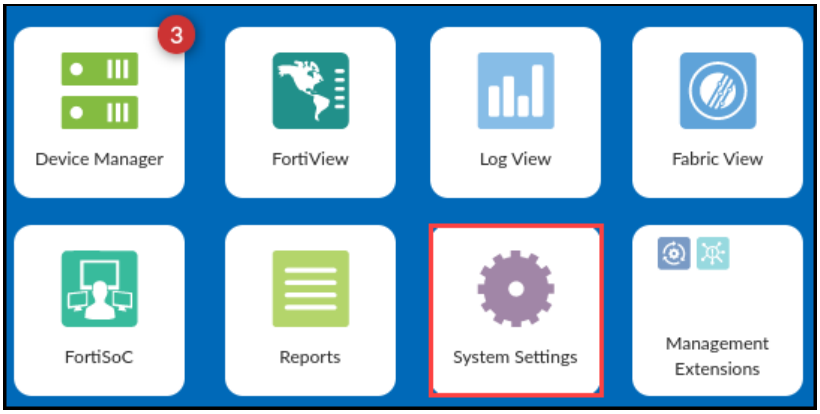
In this exercise, you will access FortiAnalyzer using the GUI and CLI. You will also restore the FortiAnalyzer configuration to the initial state required for this lab.

To access the GUI and restore from a backup

1. Log in to the Local-Client VM with the username `Administrator` and password `password`.
2. Open a browser, and then log in to FortiAnalyzer at `10.0.1.210` with the username `admin` and password `password`.
   You can also access FortiAnalyzer from the bookmarks bar in the Firefox browser.



3. On the main tiles, click **System Settings**.



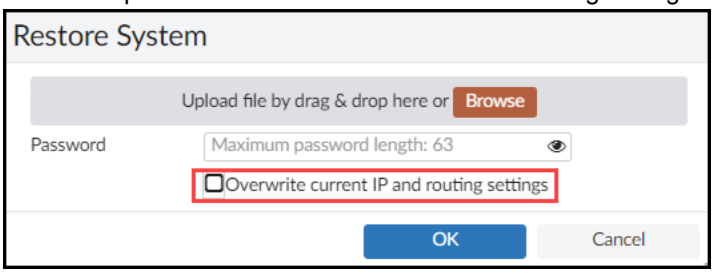
   The dashboard appears.

4. Examine the **System Information**, **License Information**, and **System Resources** widgets to display the following information:
   - Firmware version
   - ADOM status
   - System time and time zone
   - License status (VM)
   - CPU, memory, and disk usage

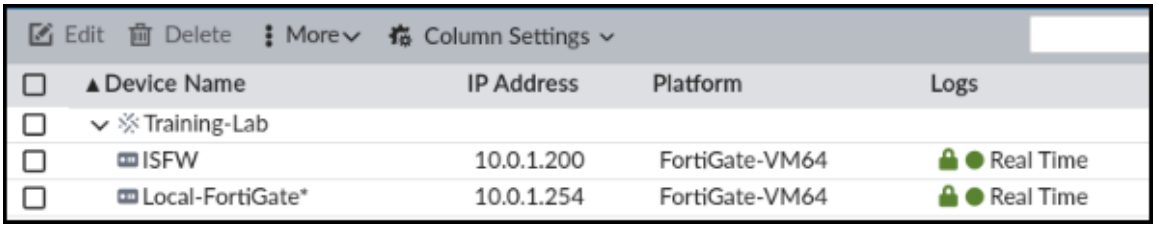
The information in these widgets provides a quick overview of the FortiAnalyzer current state and performance.

5. In the **System Information** widget, click the icon shown in the following image to perform a configuration restore:

6. Clear the option to overwrite the current IP and routing settings.



7. Click **Browse**, navigate to **Desktop** > **Resources** > **FortiAnalyzer** > **Analyst** > **LAB-1**, and then select `FAZ_Analyst_initial.dat`.
8. Click **Select**, and then click **OK**.
   The restore process begins and FortiAnalyzer restarts.
9. Wait for FortiAnalyzer to restart, and then log back in to the FortiAnalyzer GUI.
10. Click **ADOM1**, and then click **Device Manager**.
    You should see two FortiGate devices listed as shown in the following image:



11. Click **ADOM: ADOM1**.

12. Click **ADOM2**, and then verify that there is one FortiGate in **Device Manager**.

The backup configuration has ADOMs enabled, and some ADOMs were created. This is why you had to choose which ADOM you wanted to access after you logged in.

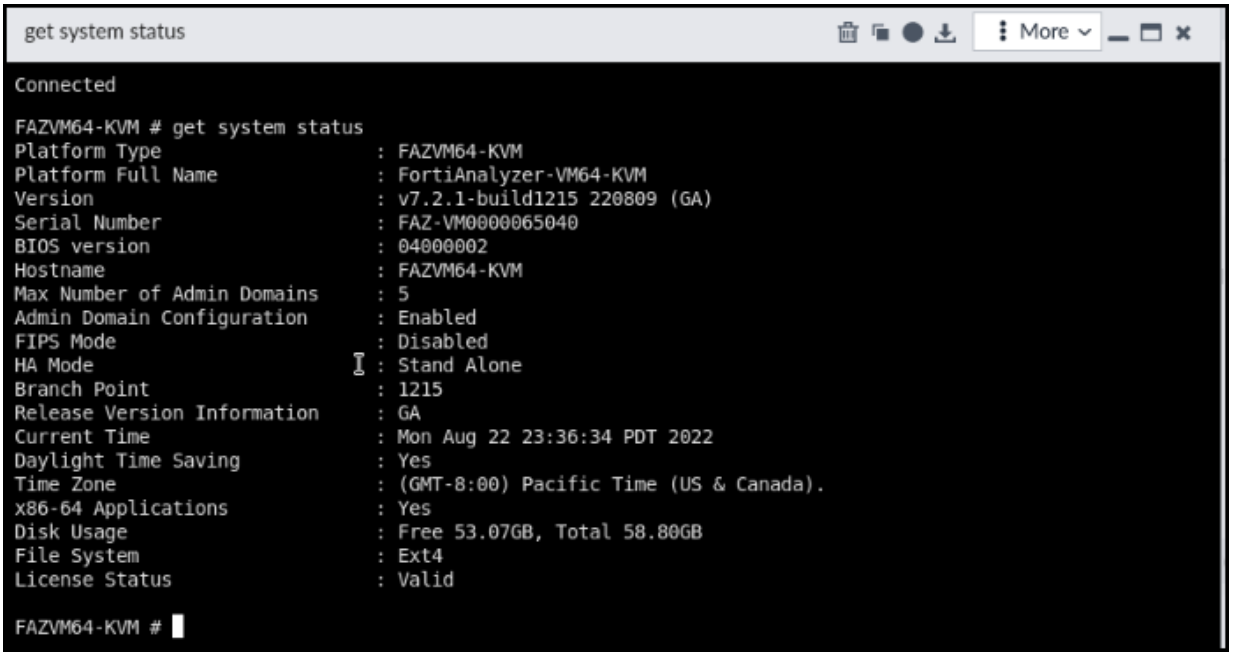
To access the CLI

You can access the CLI using a terminal emulator like PuTTY, and establishing an SSH session. However, if you have access to the GUI, a built-in CLI console is included for easy access.

1. Continuing on the FortiAnalyzer GUI, on the top bar, click the CLI icon.

   A **CLI Console** window opens.

2. Click inside the console, and then press `Enter`.
3. Type the command `get system status`, and then press `Enter`.
   You should see an output like the one in the following image:



Note this is the same information you found using some of the widgets under **System Settings**.

4. Close the CLI console, and then keep the GUI open for the next lab.

Lab 2: Logs

In this lab, you will generate some traffic so you can see where logs are stored on FortiAnalyzer, what information is included in logs, and different ways of viewing log data.

After traffic has passed through the network for a while, you will examine the used storage statistics, and then modify the ADOM disk quota based on this information.

Objectives

- Examine logs using **Log View**
- Examine summarized information in **FortiView**
- Gather logs statistics and used storage information

Time to Complete

Estimated: 40 minutes

Exercise 1: Generating Traffic

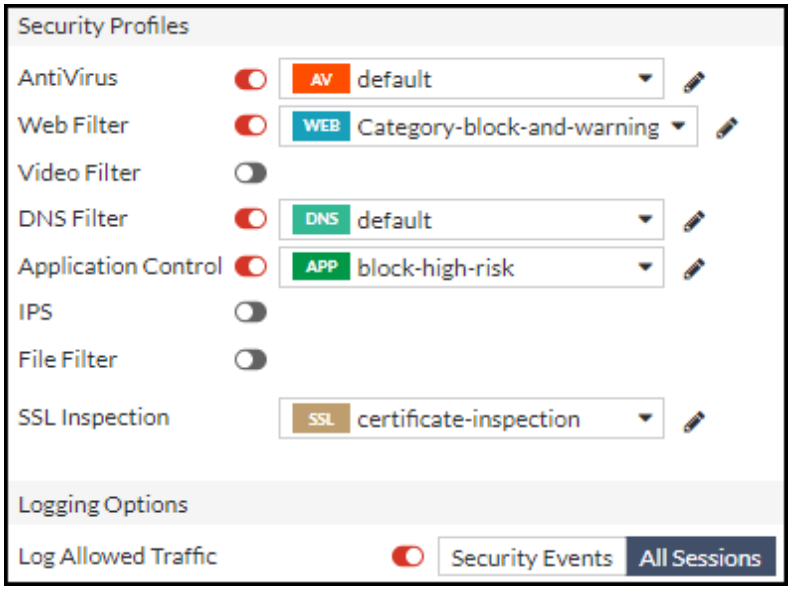
In this exercise, you will use two different tools to generate different types of traffic. You must generate this traffic so you can then see the logs that FortiAnalyzer receives.

The traffic you generate will go through ISFW and Local-FortiGate. The firewall policies were preconfigured for you, and logging for all sessions is enabled. To view the firewall policies on the Local-FortiGate GUI, click **Policy & Objects** > **Firewall Policy**.

Generate Traffic Using FIT

The firewall inspection tester (FIT) VM generates web browsing traffic, application control, botnet IP hits, malware URLs, and malware downloads.

In this lab, you will direct FIT-generated traffic through the ISFW **Full_Access** firewall policy. This firewall policy was preconfigured for you, and includes the following security policies and logging options:



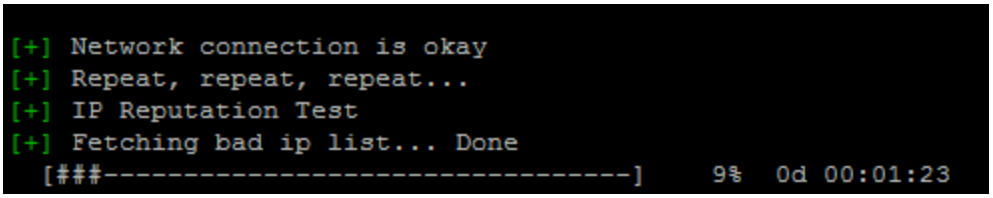
Because the FIT-generated traffic originates from the IP address of the FIT VM (`10.0.3.20`), all of these logs show the same source IP address in the FortiAnalyzer logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IP addresses for your traffic.

To generate traffic using FIT

1. On the Local-Client VM, open PuTTY, and then connect over SSH to the FIT saved session.
2. Log in with the username `student` and password `password`.

3. Enter the following command to run a script that changes the default route of FIT to send traffic through ISFW (see Network Topology on page 5):
   ```
   $ sudo ./default3
   ```
4. When prompted, enter the password again.
5. Enter the following command to check the default route:
   ```
   $ ip route
   ```
   You should see the default route through `10.0.3.254`.
6. Enter the following commands:
   ```
   # cd FIT

   # ./fit.py all --repeat
   ```
   Traffic begins to generate, and the script repeats each time it completes.



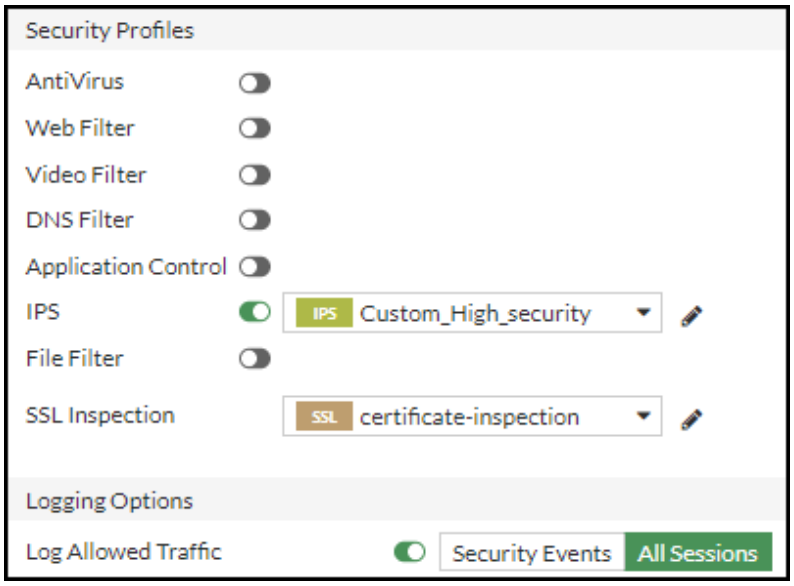
7. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate—this will run throughout the remainder of the lab.

Do not close the FIT PuTTY session or traffic will stop generating.

Generate Traffic Using Nikto

Nikto generates intrusion prevention system (IPS) traffic.

You will direct the traffic that Nikto generates through the Local-FortiGate **IPS-traffic-policy** firewall policy. This firewall policy was preconfigured for you, and includes the following security policies and logging options:



Because the traffic that Nikto generates originates from the IP address of the Linux VM where Nikto is installed (`10.200.1.254`), all of these logs show the same source IP address in the FortiAnalyzer logs. This is a limitation of the lab environment. In a real-world scenario, you will likely see many different source IP addresses for your traffic. Note that `10.200.1.10` is a virtual IP address configured on Local-FortiGate.

To generate traffic using Nikto

1. Continuing on the Local-Client VM, open a second PuTTY application, and then connect over SSH to the LINUX saved session.
2. Log in with the username `student` and password `password`.
3. Enter the following command:

   ```
   nikto.pl -host 10.200.1.10
   ```

   The script starts generating traffic.

```
- ***** SSL support not available (see docs for SSL install) *****
- Nikto v2.1.5
---------------------------------------------------------------------------
+ Target IP:          10.200.1.10
+ Target Hostname:    10.200.1.10
+ Target Port:        80
+ Start Time:         2017-03-17 06:58:33 (GMT-7)
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/8.5
+ Server leaks inodes via ETags, header found with file /, fields: 0x35e578bc95b
2d11:0
+ The anti-clickjacking X-Frame-Options header is not present.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Server banner has changed from 'Microsoft-IIS/8.5' to 'Microsoft-HTTPAPI/2.0'
which may suggest a WAF, load balancer or proxy is in place
```

   The scan will continue for approximately 25 minutes. When the scan is complete, the window displays an end time and indication that one host has been tested.

```
+ End Time:           2017-03-17 07:33:35 (GMT-7) (2102 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

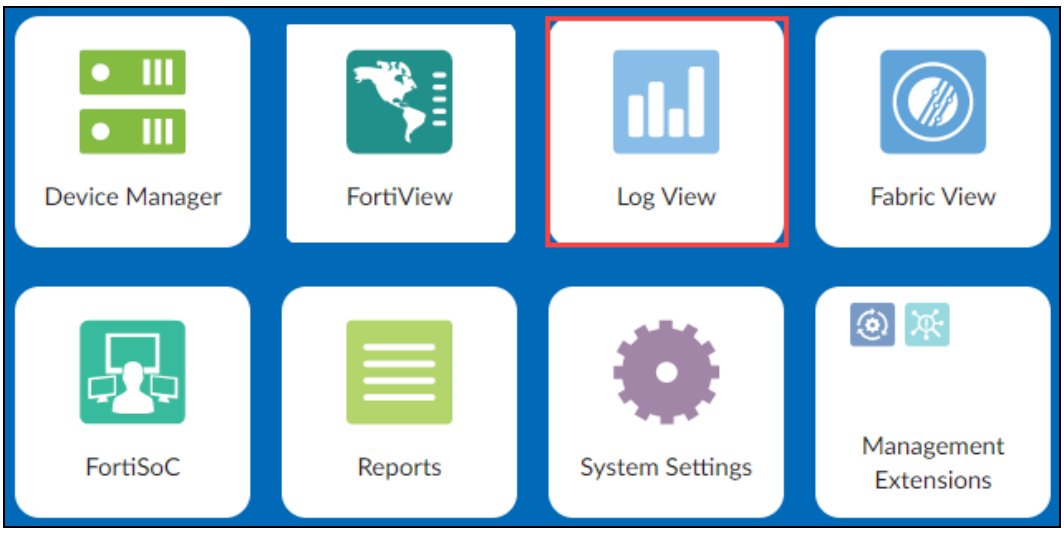
You can run the command again. Press the up arrow, and then press `Enter` to generate more logs—however, this is not required. One cycle provides enough logs for the purposes of this lab.

4. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate—this will run for the remainder of the lab.

Do not close the LINUX PuTTY session or traffic will stop generating.

Exercise 2: Examining Logs With Log View

There are many ways to view logs in FortiAnalyzer. In this exercise, you will familiarize yourself with **Log View**, and use its log filtering capabilities to find relevant information.



Because of simulated traffic limitations in this lab, not all views will be populated.

View Logs in Log View

Log View allows you to view traffic logs (also referred to as firewall policy logs), event logs, and security logs for each device or for each log group. Log groups are not used in this lab.

When ADOMs are enabled, each ADOM has its own information displayed in **Log View**.

Log View displays log messages from analytics logs and archive logs.

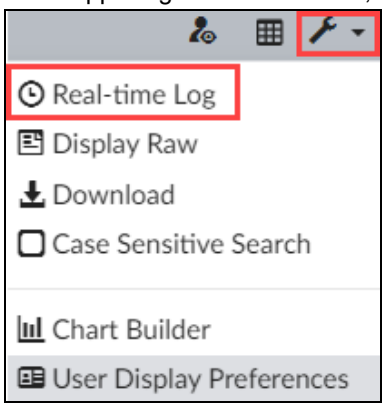
- Historical logs and real-time logs in **Log View** are from analytics logs.
- **Log Browse** can display logs from both the current, active log file and any of the compressed log files.

You will examine traffic logs and security logs only.

To view logs in Log View

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Select **ADOM1**.
3. Click **Log View**.
4. In the menu on the left, select **FortiGate** > **Traffic**.
5. Explore the different ways of viewing logs, such as real time, historical, and raw.

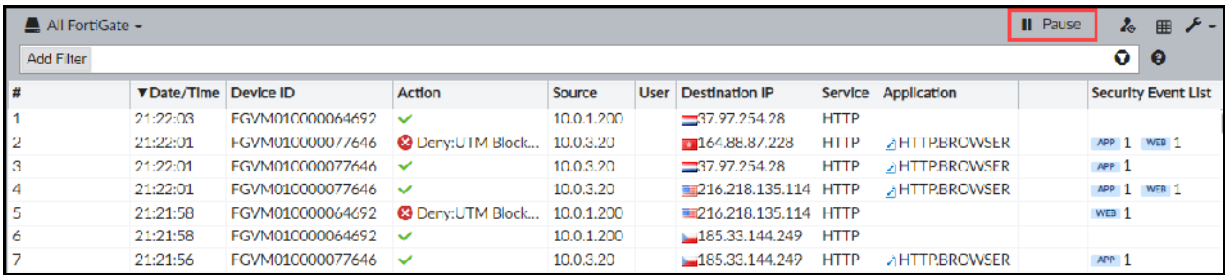
- In the upper-right side of the GUI, click **Tools** > **Real-time Log**.



You should see traffic logs in real time and in the formatted view.

Note that you can click **Pause** to stop the traffic if you want to look at one or more logs without losing them among all the real-time logs constantly dropping in. Click **Resume** to resume.

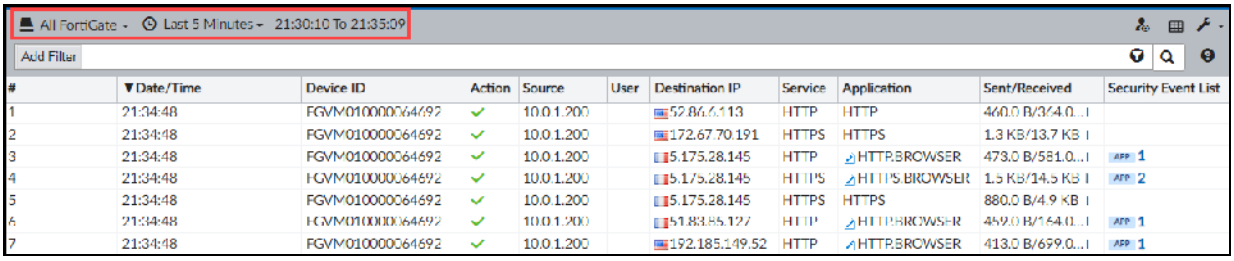
Real-time logs are temporarily considered compressed, but are indexed as soon as FortiAnalyzer has available CPU and memory.



- Click **Tools** > **Historical Log**.

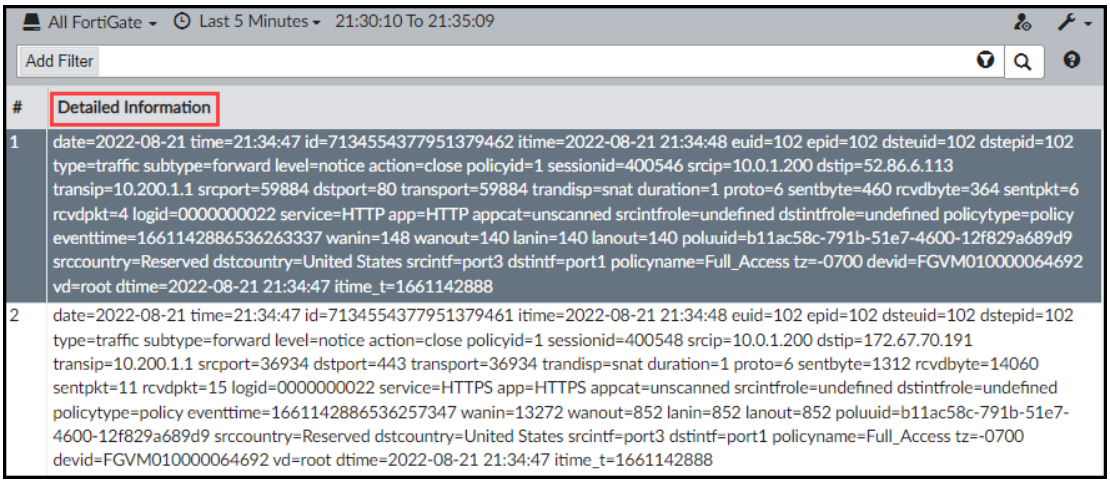
You should see formatted, historical logs according to the filters that are set. For example, **All FortiGate**, **Custom**. Historical logs are the default view. Double-click a log to see more details.

You can view details about historical logs, because they have been indexed in the SQL database.



- Click **Tools** > **Display Raw**.

  You should see the raw logs (not formatted).



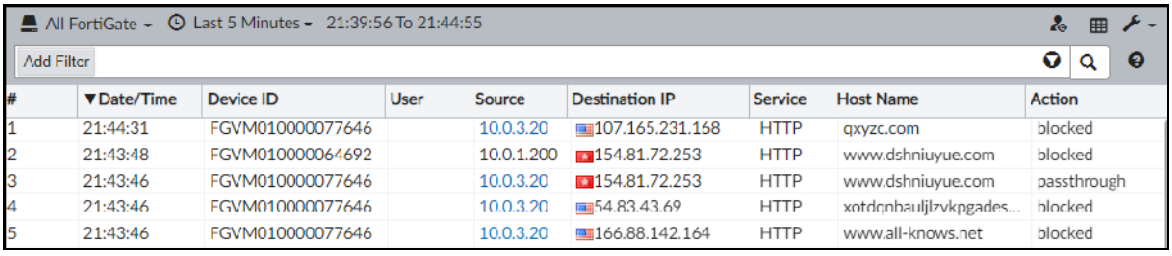
6. Click **Tools** > **Formatted Log** to return the view to formatted logs.

   Security logs from FortiAnalyzer include antivirus, web filtering, application control, intrusion prevention, email filtering, data leak prevention, SSL/SSH scan, and VoIP. The logs displayed on FortiAnalyzer are dependent on the device type logging to it, the traffic, and the features enabled. In this lab, only web filter, application control, and intrusion prevention logs are triggered.

You can also view security logs in real time or historical, and in raw or formatted format.

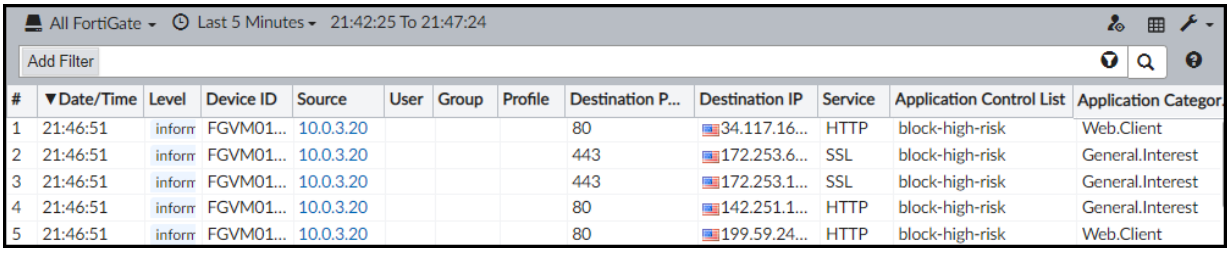
- In the menu on the left, click **Security** > **Web Filter**.

  You should see all logs that match web filter traffic. You can double-click a log for more details.



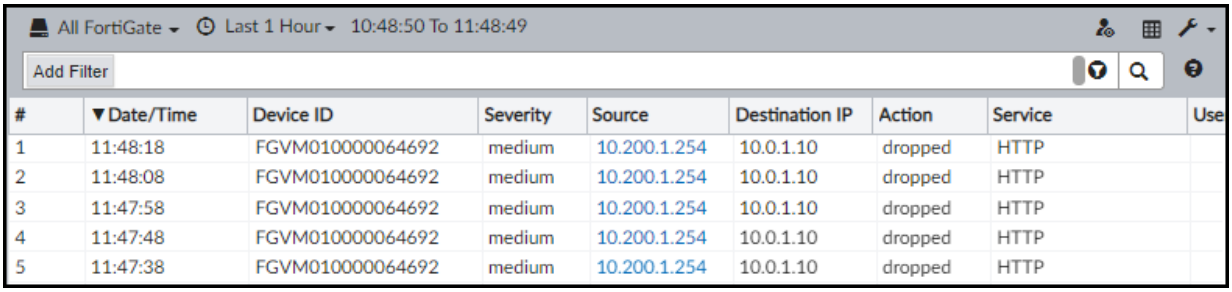
- Click **Security** > **Application Control**.

  You should see all logs that match application control traffic. You can double-click a log for more details.



- Click **Security** > **Intrusion Prevention**.

You should see all logs that match IPS traffic. You can double-click a log for more details.



#	Date/Time	Device ID	Severity	Source	Destination IP	Action	Service	Use
1	11:48:18	FGVM010000064692	medium	10.200.1.254	10.0.1.10	dropped	HTTP	
2	11:48:08	FGVM010000064692	medium	10.200.1.254	10.0.1.10	dropped	HTTP	
3	11:47:58	FGVM010000064692	medium	10.200.1.254	10.0.1.10	dropped	HTTP	
4	11:47:48	FGVM010000064692	medium	10.200.1.254	10.0.1.10	dropped	HTTP	
5	11:47:38	FGVM010000064692	medium	10.200.1.254	10.0.1.10	dropped	HTTP	

Use Log Filters

You can use log filters to narrow down search results and locate specific logs.

Tips:

- Check the filter drop-down list first to select the SQL column filter name that you want to filter on.
- You can right-click a column value to use that value as a filter. Add the columns that you want from the **Column Settings** drop-down list.
- Ensure the time filter covers the logs that you are searching for.
- Ensure the device is set accordingly for the logs you want to return.
- Verify whether case-sensitive search is enabled or disabled (**Tools**).
- Ensure you are searching on the appropriate log type for the logs you want to return (for example, traffic, web filter, application control, IPS, and so on).
- Ensure you are not filtering on real-time logs if you want to search on historical logs.

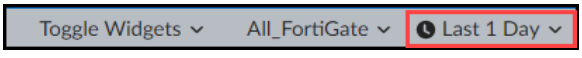
Use filters to find the following logs in ADOM1.

To use log filters to find details about specific traffic

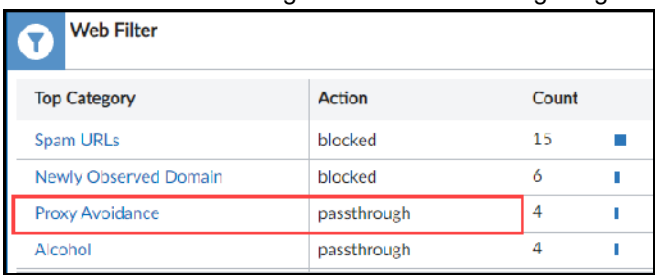
If you don't find the entries mentioned in this exercise, ensure you adjust the time filter to include the expected traffic. Additionally, you may need to edit the number of items displayed per page. This is done at the bottom of the interface.

Scenario 1: You need to find if, in the last 24 hours, any traffic was allowed to websites that could be used to circumvent internet access policies by using anonymous proxy servers.

1. Continuing on the FortiAnalyzer GUI (ADOM1), click **Log View**.
2. Click **Security** > **All Types**.
3. If required, adjust the time filter to include only the last day.

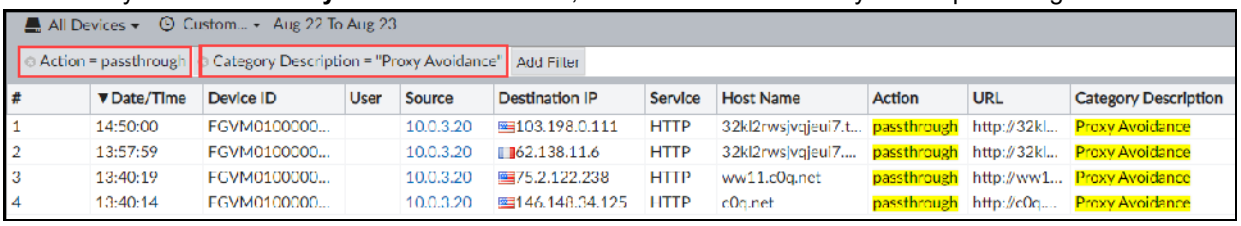


4. Examine the **Web filter** widget by scrolling down and looking for the **Proxy Avoidance** category.
You should see something similar to the following image. However, the count may be different.

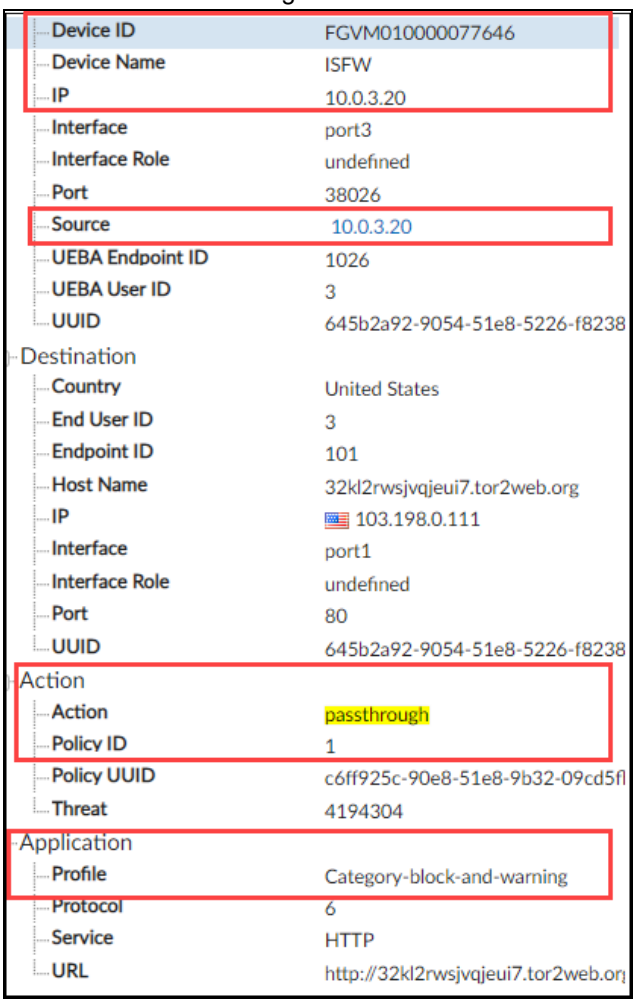


Note that the action for all the **Proxy Avoidance** entries is **passthrough**. This means the traffic was allowed, and the corresponding access policy may be misconfigured.

5. Click **Proxy Avoidance**.
This takes you to the **Security** > **Web Filter** section, with a filter to include only those specific logs.



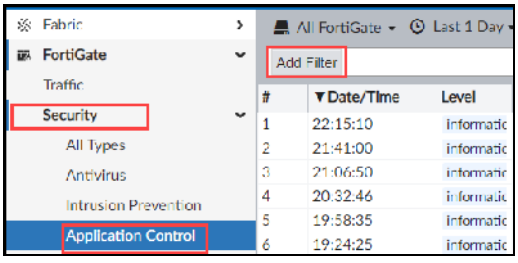
6. Double-click one of the logs to see the details.



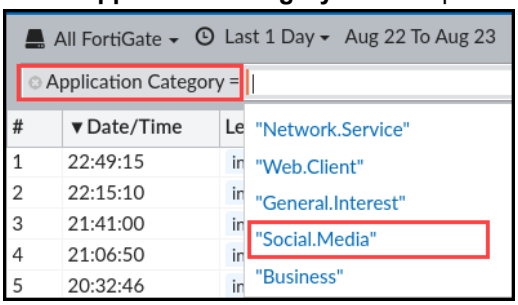
With this information, you can now notify the team in charge of the ISFW firewall about a possible issue in the firewall policy with an ID of 1, and/or the settings of the security profile attached to it (**Category-block-and-warning**), which is allowing the device with IP address `10.0.3.20` to visit potentially dangerous websites.

Scenario 2: You received an email claiming that a user is able to access social media sites. This goes against the company's security policy, which states that this is not allowed. You need to investigate if this is true and, if it is, find clues about why it is happening.

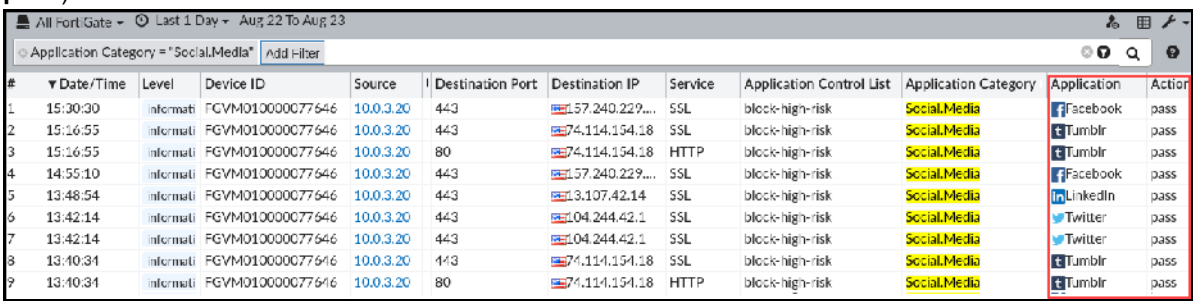
1. Continuing on the FortiAnalyzer GUI (ADOM1), click **Log View**.
2. Click **Security** > **Application Control**, and then click **Add Filter**.



3. Select **Application Category** in the drop-down list, and then select **Social.Media**.



4. Examine the results after applying this filter.
You should see several logs related to traffic to social media sites that were allowed by the firewall (**Action** = **pass**).



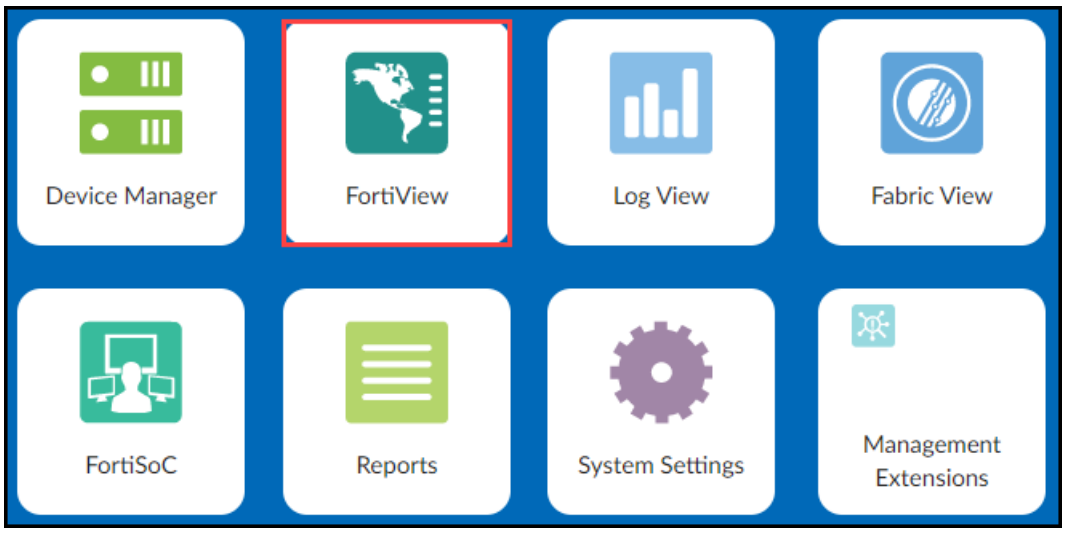
Based on your findings, you just confirmed that the traffic to social media sites is indeed happening, and that is coming from the device with IP address `10.0.3.20`. Additionally, this traffic is being logged by a policy with the application control security profile called **block-high-risk**. Based on its name, it is obvious that this profile is not doing what it is intended to do. You can now notify the firewall administration team about these issues.

For demonstration purposes, the firewall policies, and the security profiles used in this lab, were intentionally configured to allow (monitor) some of the traffic that could easily be blocked by FortiGate.

5. Keep your FortiAnalyzer session open for the next exercise.

Exercise 3: Using FortiView

Another way to view log-related information in FortiAnalyzer is by using FortiView. In this exercise, you will familiarize yourself with the options available in this tool.



Because of simulated traffic limitations in this lab, not all views will be populated.

View Summary Information in FortiView

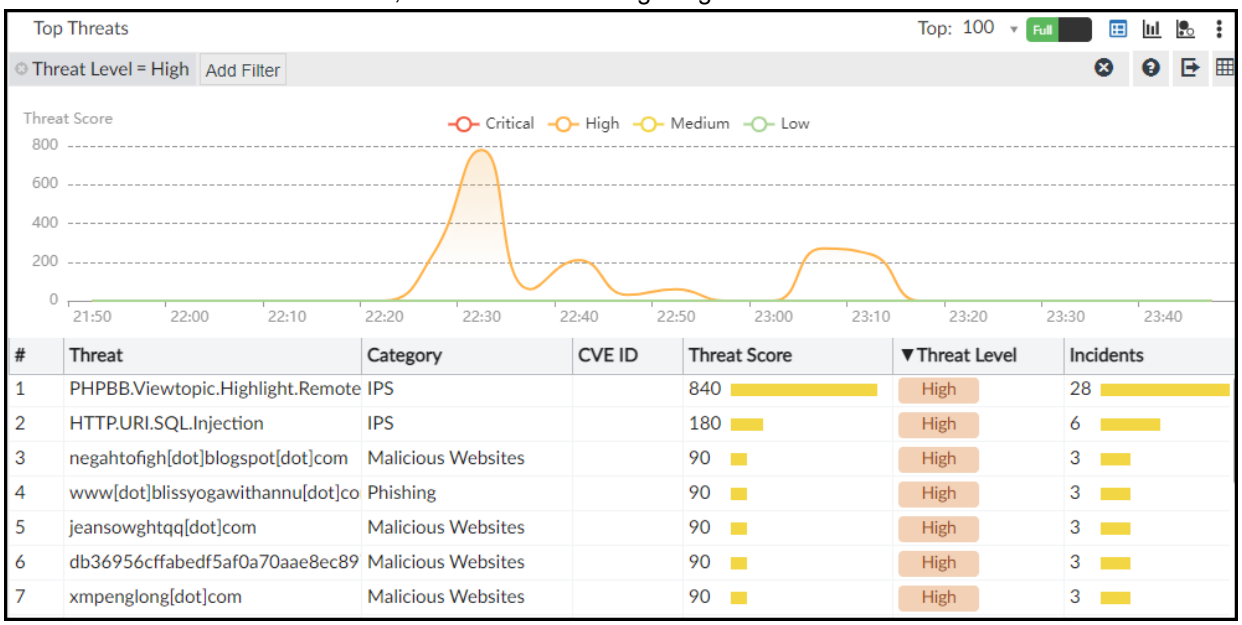
You can view summaries of log data in FortiView in both tabular and graphical formats. For example, you can view top threats to your network, top sources of network traffic, and top destinations of network traffic, to name a few. For each summary view, you can drill down into details.

When ADOMs are enabled, each ADOM has its own data analysis in FortiView.

To view logs in FortiView

1. In the drop-down menu in the upper-left, click **Log View** > **FortiView**.
2. Click **Threats** > **Top Threats**.
   You may need to adjust the time filter to include the traffic being generated in the background (Exercise 1).
3. Click **Add Filter**, and then select **Threat Level** in the drop-down list.
4. Select **High**.

You should see several items listed, similar to the following image:



#	Threat	Category	CVE ID	Threat Score	▼Threat Level	Incidents
1	PHPBB.Viewtopic.Highlight.Remote	IPS		840	High	28
2	HTTP.URI.SQL.Injection	IPS		180	High	6
3	negahtofigh[dot]blogspot[dot]com	Malicious Websites		90	High	3
4	www[dot]blissyogawithannu[dot]co	Phishing		90	High	3
5	jeansowghtqq[dot]com	Malicious Websites		90	High	3
6	db36956cffabedf5af0a70aae8ec89	Malicious Websites		90	High	3
7	xmpenglong[dot]com	Malicious Websites		90	High	3

Note that the threat score for each threat is given by the number of incidents multiplied by the value assigned to its level. In this case, high has a value of 30.

5. If you see an entry with an associated CVE ID, you can click the CVE ID to open the NIST page that provides more information.
6. Clear the current filter before continuing to the next step.

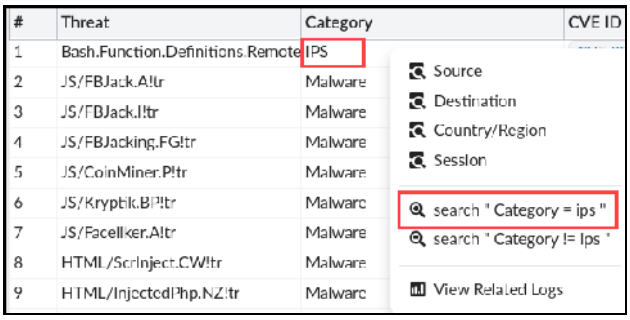
Obtain More Detailed Information in FortiView

Starting from the summarized information provided by FortiView, you can dig deeper to obtain very detailed data about any of the entries displayed. You will explore this with a simple scenario.

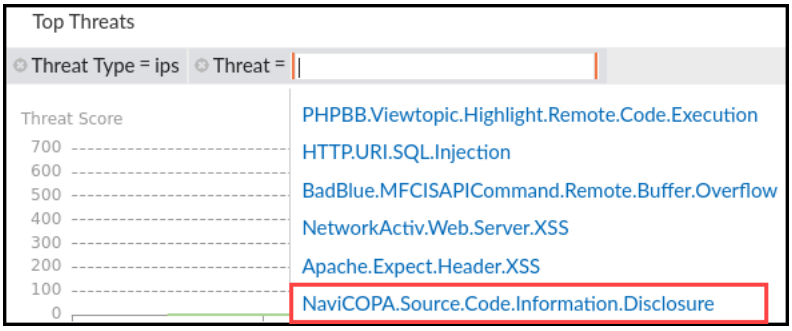
Scenario: You receive an email explaining that an old server running **NaviCOPA Web Server 3.01** has been executing some apparently random codes in the background. All signs indicate that this server has been compromised. You must investigate and try to find clues about why this is happening.

To obtain more detailed information in FortiView

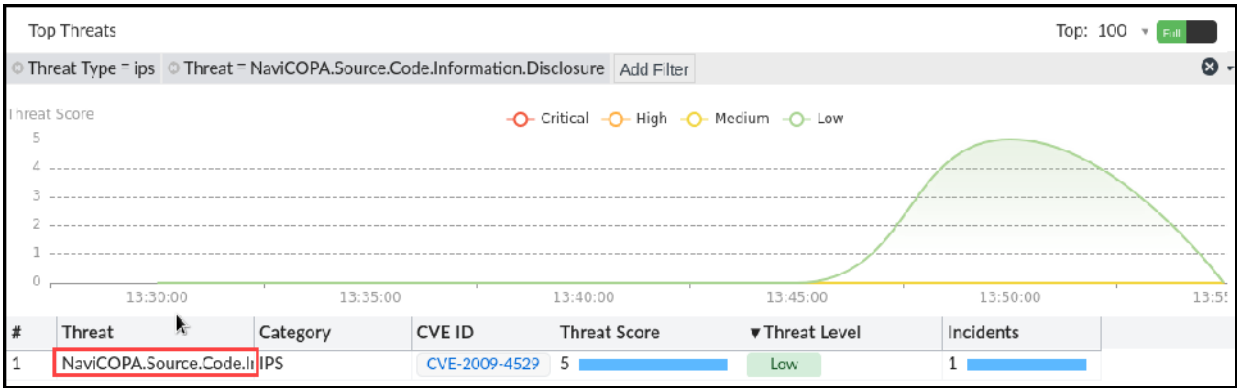
1. Continuing on **Threats** > **Top Threats**, right-click the column with one of the entries with the category **IPS**, and then select to filter based on that parameter.



2. Click **Add Filter**, and then select **Threat** in the drop-down list.
3. Since the problem reported relates to NaviCOPA, in the text box, start typing `Navi`.
   You should see the name **NaviCOPA.SourceCode.Information.Disclosure** in the list.



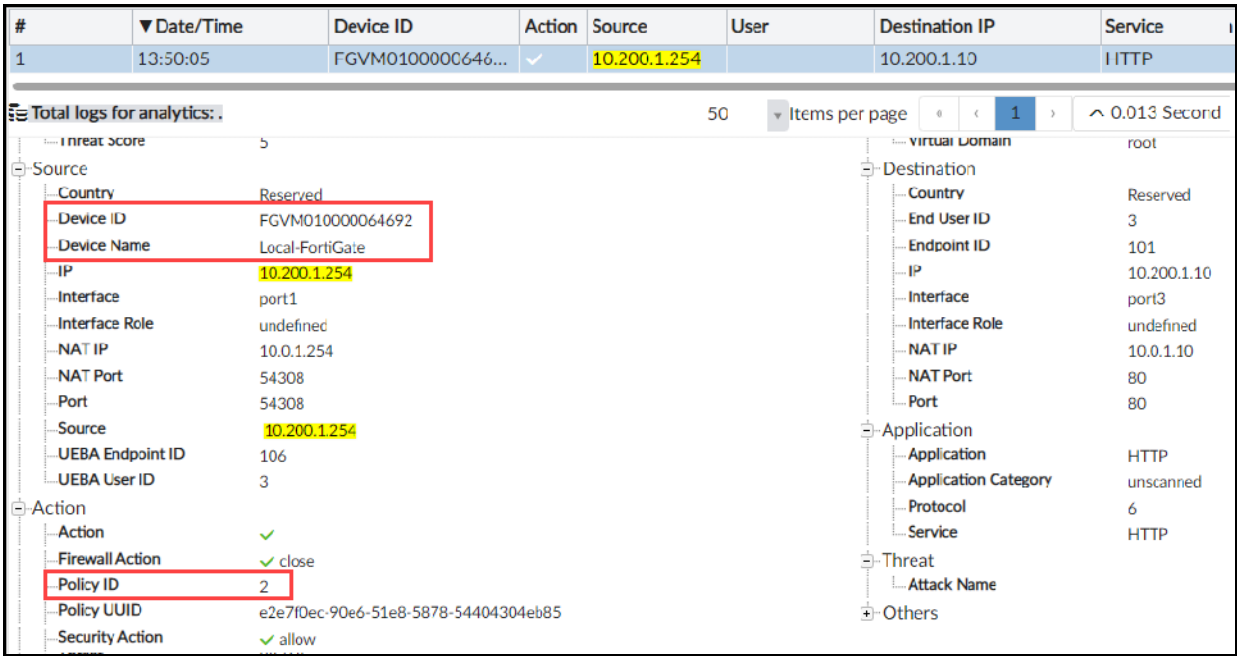
4. Click that entry to apply the filter.



5. Double-click the entry displayed to obtain more details.

Note that, despite being labeled as low risk, this threat was allowed by the firewall. This confirms the information from the email about the server being compromised. The source of this attack is the IP address `10.200.1.254`.

6. Double-click the entry listed to see the associated logs, and then double-click one of the logs to get more details.



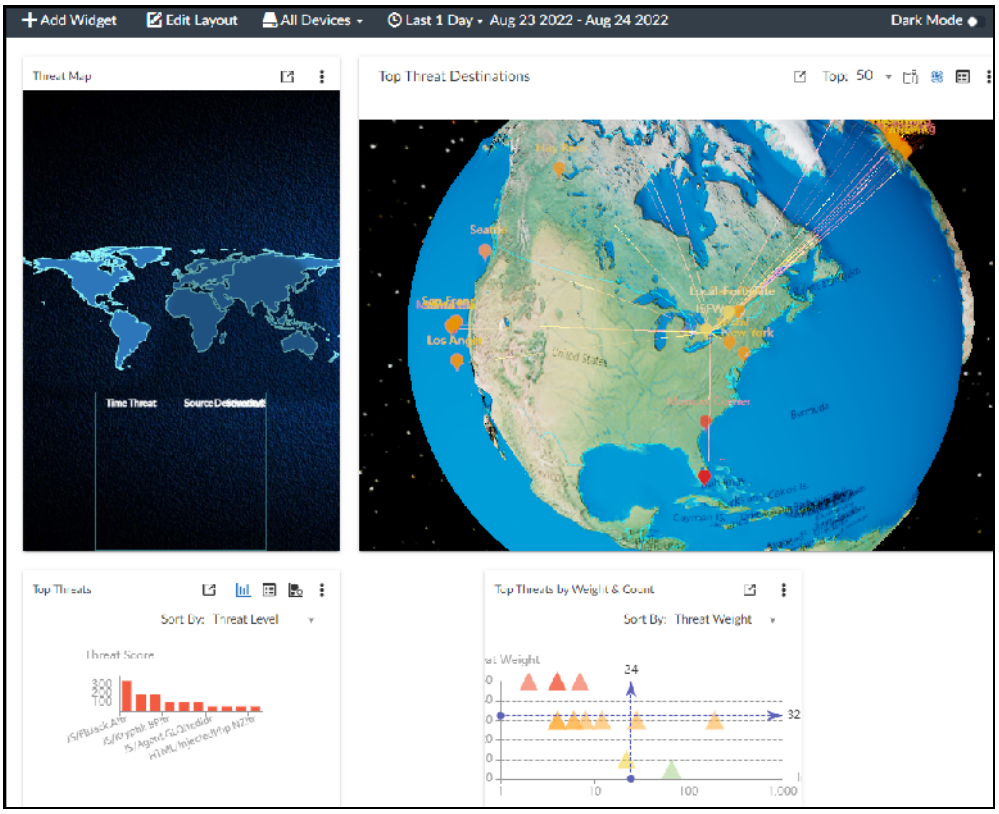
From the information you obtained, you can now notify the team in charge of the Local-FortiGate firewall about an issue with the policy with the ID 2, that is allowing unwanted traffic through.

Explore FortiView Monitors

FortiView Monitors uses multiple dashboards and widgets that provide a general overview of current traffic, threats, and many other pieces of information of interest. Although the dashboards were designed to be displayed on large monitors, you can also use them to obtain detailed information.

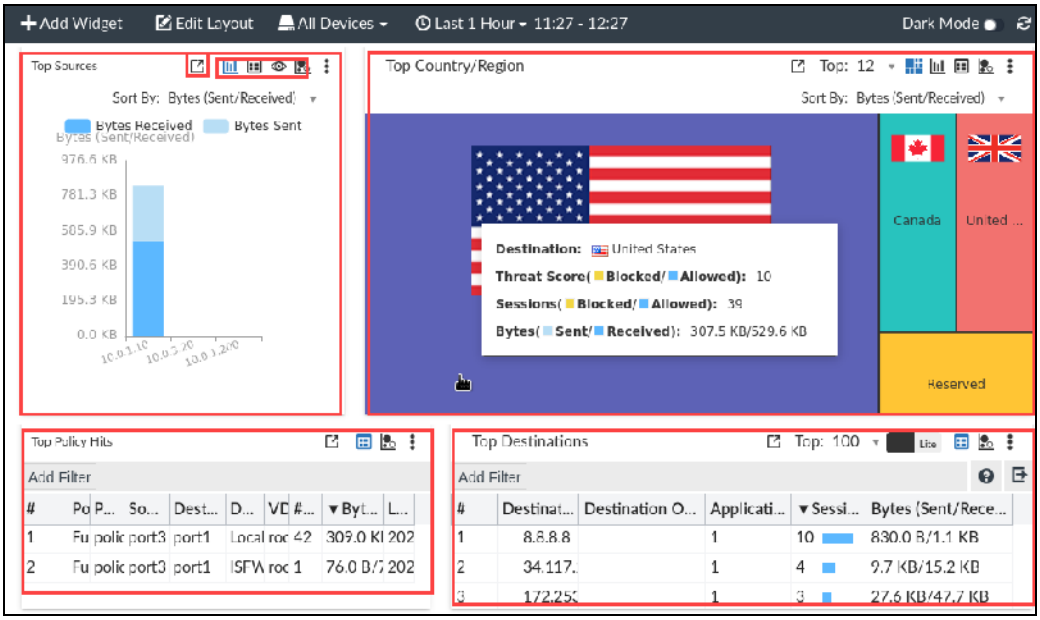
To access the FortiView Monitors dashboards

1. Continuing on the FortiAnalyzer GUI (ADOM1), click **FortiView** > **Monitors**.
2. In the menu on the left, click **Threats**.
   The **Threats** dashboard includes five widgets by default. You can customize which ones are displayed and their layout.



The widgets display the data from the time interval set at the dashboard level.

3. In the left pane, click **Traffic**.
   This dashboard includes four widgets by default, but you can add up to 10.
4. Hover over the **Top Country/Region** widget to see statistics about each country (represented by its flag).

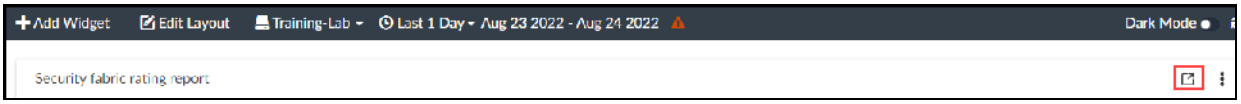


Explore the Fabric State of Security Dashboard

One of the most useful dashboards included is the **Fabric State of Security**. This is available when you create a Fortinet Security Fabric and add it to FortiAnalyzer.

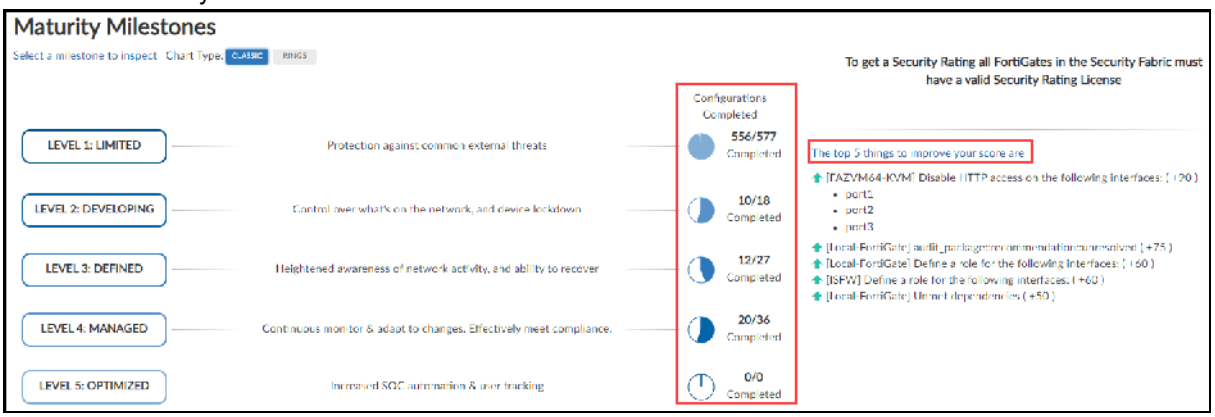
To access the Fabric State of Security Dashboard

1. In the menu on the left, click **Fabric State of Security**.
2. Click the icon to expand the **Security fabric rating report** widget.



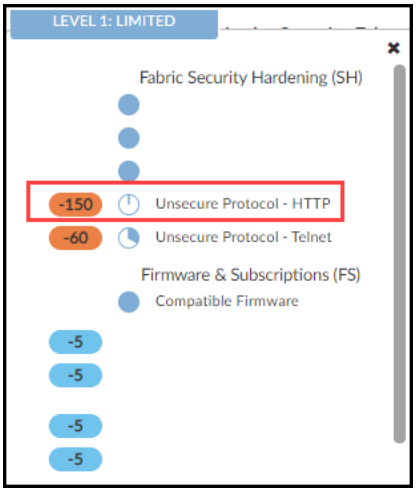
Note that you may need to click the refresh icon on the upper-right corner.

This widget shows the current progress, updated every five minutes by default, of each one of the five levels of Fortinet maturity milestones.



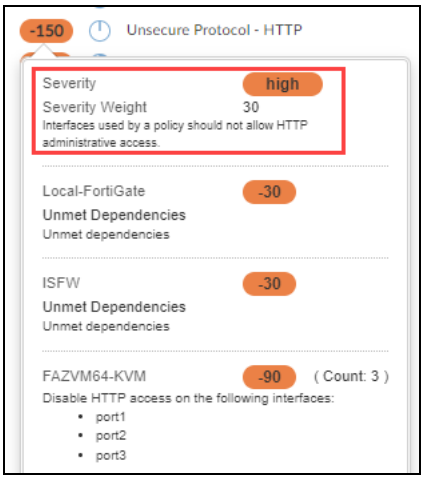
Also, on the right side, notice the top five configurations that will make your score improve.

3. Click anywhere over the **Level 1** area to display details about the issues affecting your score.
You should see a new pane similar to the following image:



4. Hover over one of the scores to see why it was assigned that value.
For example, in the following image, the score is **-150** because HTTP administrative access is enabled on one or

more of the interfaces of several devices in the Security Fabric.



5. Repeat the process to find out other configurations that will help you improve your score.

In the image above, a high security level is assigned a weight of 30 (negative). Since there are 5 interfaces with that risk, the total is 5 x (-30) = -150.

With the information you obtained, you can now contact the staff responsible for administering those devices, and provide them with the list of recommended configurations.

6. Keep your FortiAnalyzer session open for the next exercise.

Exercise 4: Viewing Log Statistics and Used Storage Space

Now that FortiAnalyzer is collecting logs, you should view the log statistics and used storage space to determine whether FortiAnalyzer is adequately configured to store the logs it receives from the registered devices in your network.

View the Raw Log Receiving Rate

The fortilogd daemon is the process responsible for receiving the raw logs at FortiAnalyzer. Multiple diagnostic commands show the rate at which the logs and messages are received and the status of the process.

This allows you to identify and understand the following:

- The log rate
- The log message rate
- The log message volumes and whether they are well-balanced among the devices
- The log message type distribution (traffic, event, and so on)

To view the raw log receiving rate

1. On the FortiAnalyzer CLI, log in with the username `admin` and password `password`.
2. Enter the following commands to view fortilog daemon information:

Diagnostic	Command
What is the log rate every second/30 seconds/60 seconds?	`diagnose fortilogd lograte`
What is the message log rate every second/30 seconds/60 seconds?	`diagnose fortilogd msgrate` One log message can consist of multiple logs in LZ4 format. Therefore, the rate should be lower for `msgrate` than `lograte`.
What is the log message rate per device per second?	`diagnose fortilogd lograte-device` Since all traffic is going through Local-FortiGate and ISFW, the totals for the Local-FortiGate and ISFW should be higher than Remote-FortiGate.
What is the log type distribution per second?	`diagnose fortilogd lograte-type` FortiGate sends only two types of log files to FortiAnalyzer: `tlog` (traffic) and `elog` (event). All UTM logs are sent with `tlog`.

3. Close the FortiAnalyzer CLI session.

View the Insert Rate Versus the Receive Rate

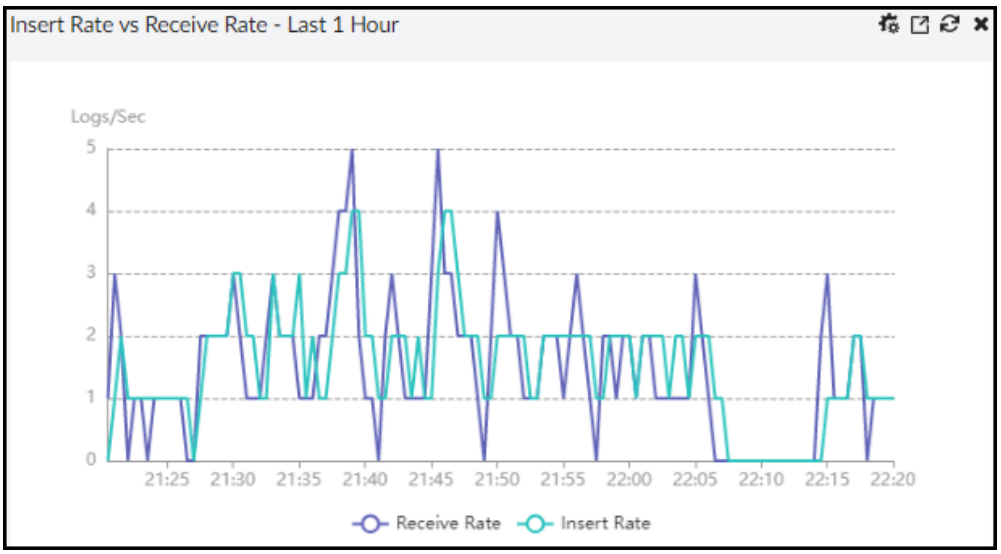
The FortiAnalyzer dashboard includes a widget that shows the rate at which raw logs are reaching FortiAnalyzer (receive rate) and the rate at which they are indexed by the SQL database (insert rate) by the sqlplugind daemon.

Another widget displays the log insert lag time (how many seconds the database is behind in processing the logs).

To view log rates

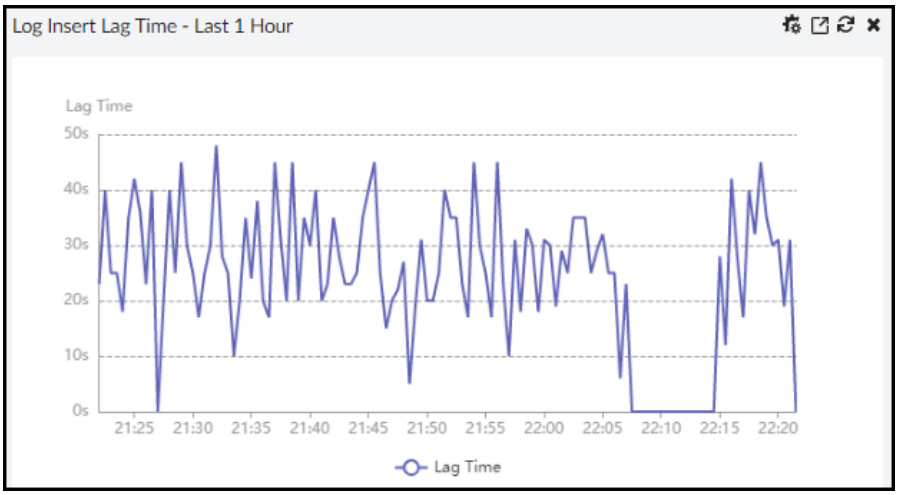
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **System Settings**.
4. On the dashboard, view the information in the following widgets:
   - **Insert Rate vs. Receive Rate**

     If, at any point, the log receive rate is higher than the log insert rate, this indicates that the raw logs are being received faster than they can be indexed (inserted) in the database.



   - **Log Insert Lag Time**

     If, at any point, there is a high lag time, this indicates how many seconds the database is behind in processing the logs.



Acceptable values for these parameters depend on the specific scenario. You should create a baseline during normal performance to have a reliable reference. The baseline must also be updated after significant changes occur in your environment.

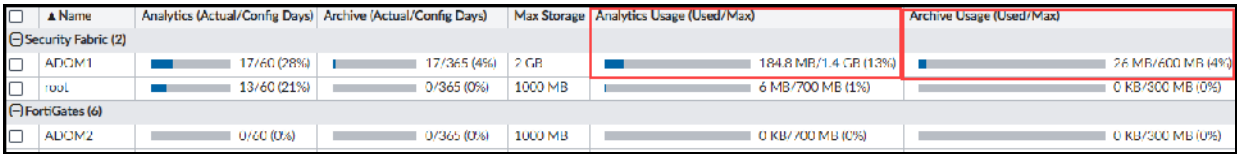
View Used Storage Statistics

Earlier, you obtained your data policy and disk utilization information. Now that FortiAnalyzer has collected some logs, you will view the current status for the used storage.

You can also use the `diagnose log device` CLI command to obtain this information.

To view the current used storage

1. Continuing on the FortiAnalyzer GUI (ADOM1), in the drop-down menu on the left, click **System Settings** > **Storage Info**.
2. Review the storage used by **ADOM1**.



Due to the relatively low volume of logs being generated in the lab environment, you may see that very little storage is being used.

3. Log out of FortiAnalyzer and close the PuTTY sessions to FIT and LINUX .

Lab 3: Events and Incidents Management

In this lab, you will examine some of the components included in the FortiSoC feature on FortiAnalyzer. You will gain experience managing events, event handlers, and tools that you can use to analyze incidents on FortiAnalyzer. For some of the tasks, you must generate traffic that will trigger the creation of new events. Finally, you will explore how you can be proactive in a SOC environment, with the help of the available threat-hunting capabilities.

Objectives

- Examine the FortiSoC dashboards
- Examine and manage events
- Clone and customize event handlers
- Create a custom event handler
- Manage incidents
- Explore threat hunting
- Explore the Outbreak Detection Service

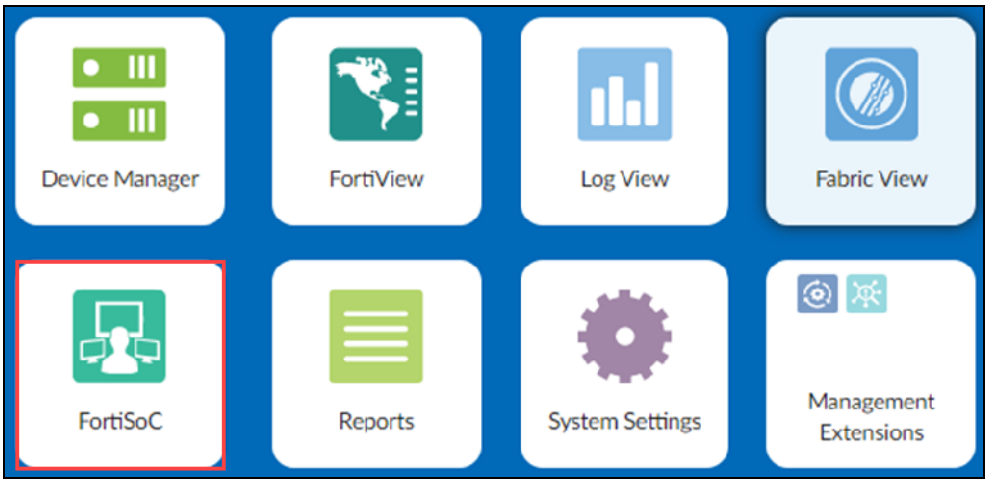
Time to Complete

Estimated: 60 minutes

Exercise 1: Examining the FortiSoC Dashboards

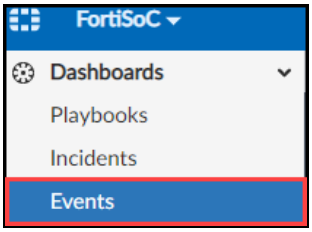
In this exercise, you will examine two of the dashboards included with the FortiAnalyzer **FortiSoC** module, and familiarize yourself with the information they provide.

Later in this lab, you will refer to these dashboards to verify that they are being updated with all the expected data.

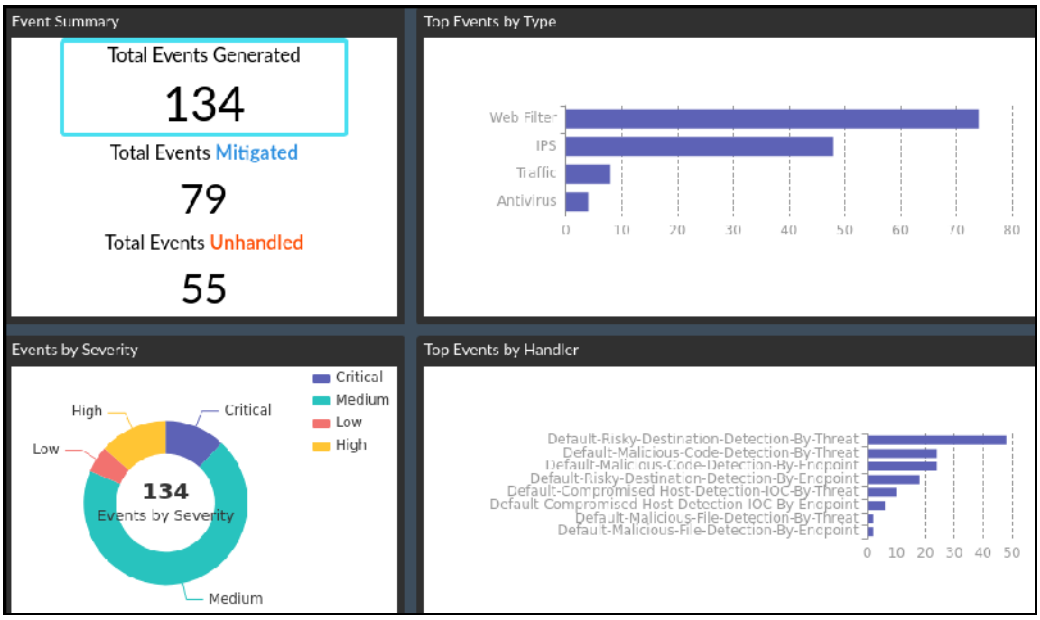


To examine the FortiSoC dashboards

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**.
4. Click **Dashboards** > **Events**.



The right pane should look similar to the following image, but with different details since it depends on the traffic generated in a previous lab.



Depending on your screen resolution, you may need to zoom out the page in your browser to view all the components in this dashboard.

The information displayed on the **Events** dashboard provides a general overview of the number of events that have been generated in your environment and their severity. For example, in the image above, 55 events are categorized as **Unhandled** out of a total of 134 events. This could be an indication of security breaches that require your attention.

5. Hover over the doughnut-shaped chart to show details about the number of events based on their severity.
   In the image above, 14 events are critical severity, and the majority of the events—93—are medium severity.

   The dashboard also displays details about the top event types, as well as the top event handlers that are generating events.

6. Click **Dashboards** > **Incidents**, and then click **Dashboards** > **Playbooks**.
   These two dashboards should show zero activity because you haven't generated any incidents or executed any playbooks.

   Later in this lab, you will verify that the latest information is reflected on the **Incidents** dashboard.

7. Stay logged in for the next exercise.

Exercise 2: Examining and Managing Events

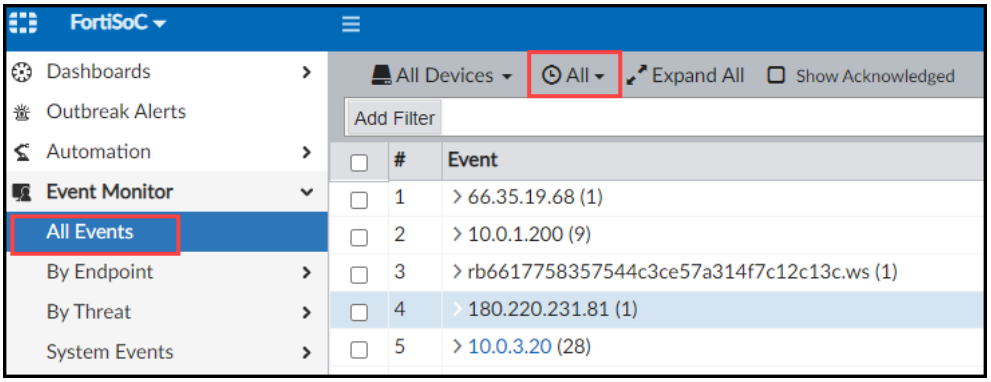
In this exercise, you will examine how you can find the details of existing events in FortiAnalyzer and the logs that generated them. You will also explore how you can use filters to display only the events that have specific parameters.

Examine Existing Events

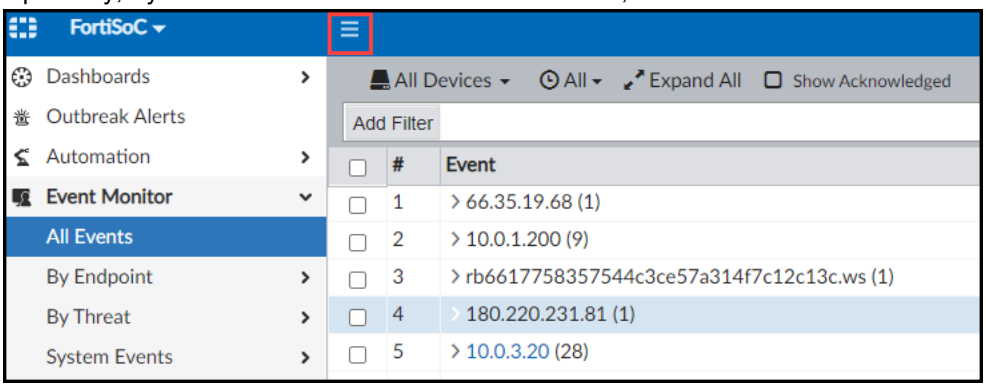
Examining events allows you to identify existing and potential security threats in your environment. You will use the filtering capabilities included in FortiAnalyzer to help you with this task.

To examine events

1. Continuing in the FortiSoC module (ADOM1) , click **Event Monitor** > **All Events**.
   In the panel on the right, you should see multiple events that were created by the traffic generated in a previous lab. If you don't see any events, set the filter to **All**.



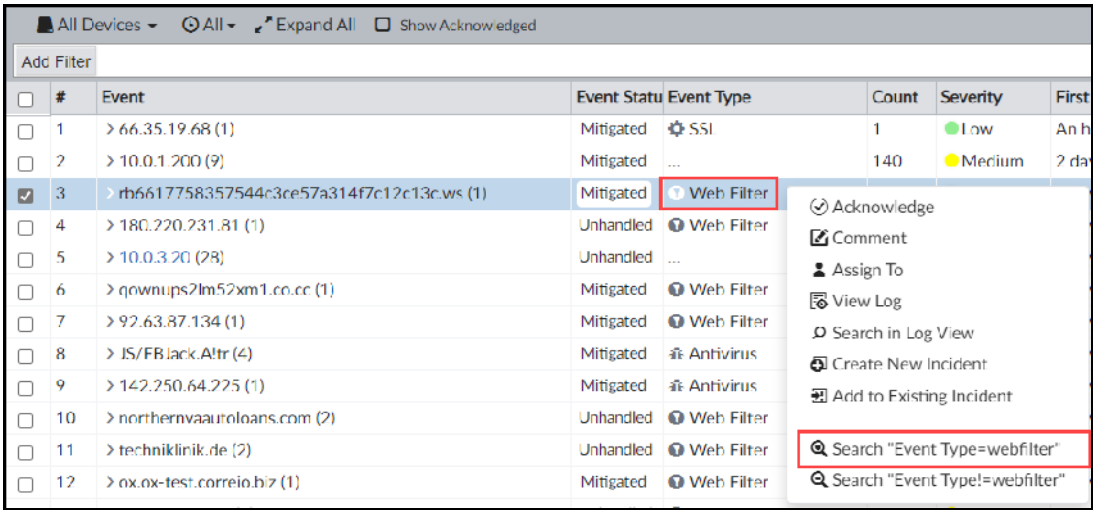
2. Optionally, if you need more room to see all the columns, click the menu button to hide the side menu.



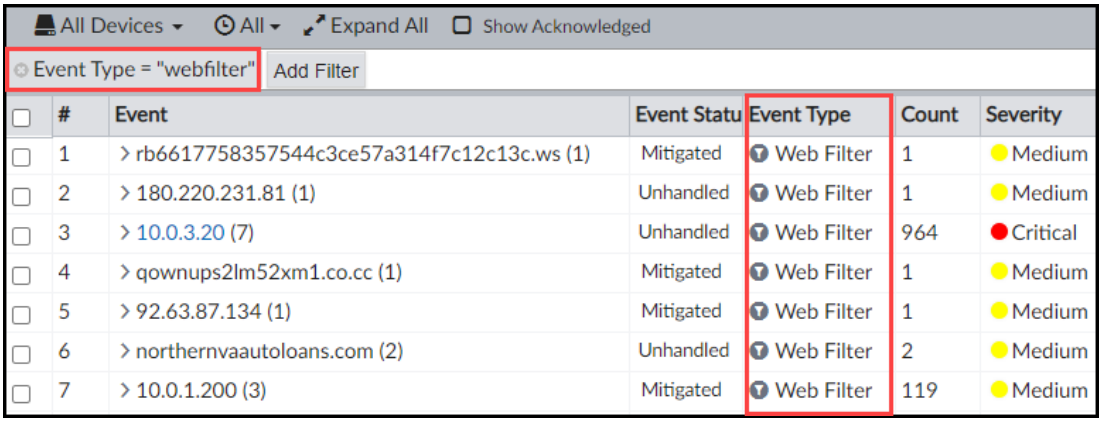
For the remainder of this exercise, we are assuming that the top event type displayed in the **Events** dashboard was **Web Filter**, and that is why we are investigating these events.

Depending on how long you let the traffic generators run, another event type might be the most common.

3. In the **Event Type** column, right-click one of the **Web Filter** entries, and then select **Search "Event Type=webfilter"** to filter the events displayed.



The resulting view includes only those events that match the filter you selected.



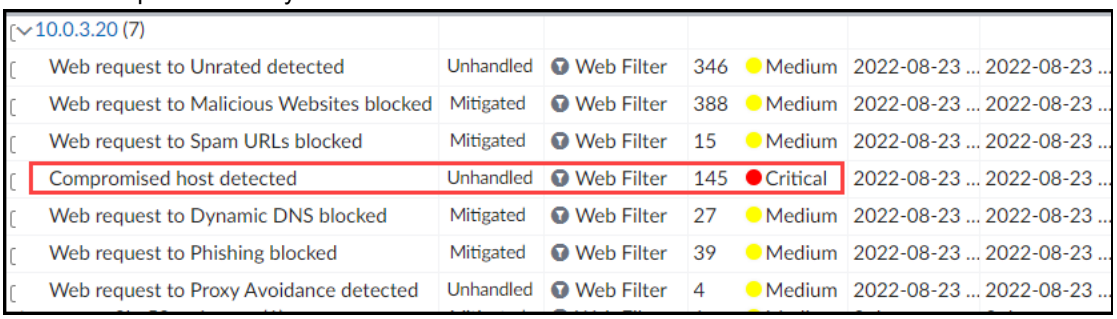
Notice the **>** beside each entry. It indicates that the event handlers have grouped multiple events based on different criteria, such as threat or endpoint.

The top-level entries are not the actual events—they are just the parameters used to group similar events.

Depending on the event handlers enabled, you may find the same event in more than one entry.

4. Find the event container listed as **10.0.3.20**.
This entry shows a severity level of **Critical**, so it should take priority.

5. Click **>** to expand the entry.

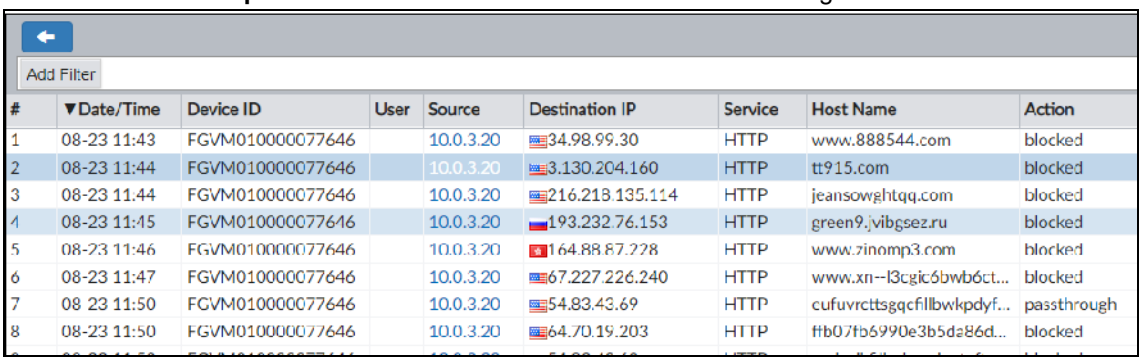


10.0.3.20 (7)						
Web request to Unrated detected	Unhandled	Web Filter	346	Medium	2022-08-23 ...	2022-08-23 ...
Web request to Malicious Websites blocked	Mitigated	Web Filter	388	Medium	2022-08-23 ...	2022-08-23 ...
Web request to Spam URLs blocked	Mitigated	Web Filter	15	Medium	2022-08-23 ...	2022-08-23 ...
Compromised host detected	Unhandled	Web Filter	145	Critical	2022-08-23 ...	2022-08-23 ...
Web request to Dynamic DNS blocked	Mitigated	Web Filter	27	Medium	2022-08-23 ...	2022-08-23 ...
Web request to Phishing blocked	Mitigated	Web Filter	39	Medium	2022-08-23 ...	2022-08-23 ...
Web request to Proxy Avoidance detected	Unhandled	Web Filter	4	Medium	2022-08-23 ...	2022-08-23 ...

You should see multiple events within this entry. One event is **Critical**, and should be the first one you check.

In the image above, two elements signal that the **Compromised host detected** event should be your first priority. One is the severity level of **Critical**. The other is that the event is marked as **Unhandled**, meaning that this event hasn't been mitigated or contained. This example shows multiple **Unhandled** events, but only one is a severity level of **Critical**.

8. Double-click the **Compromised host detected** event to see the related logs.

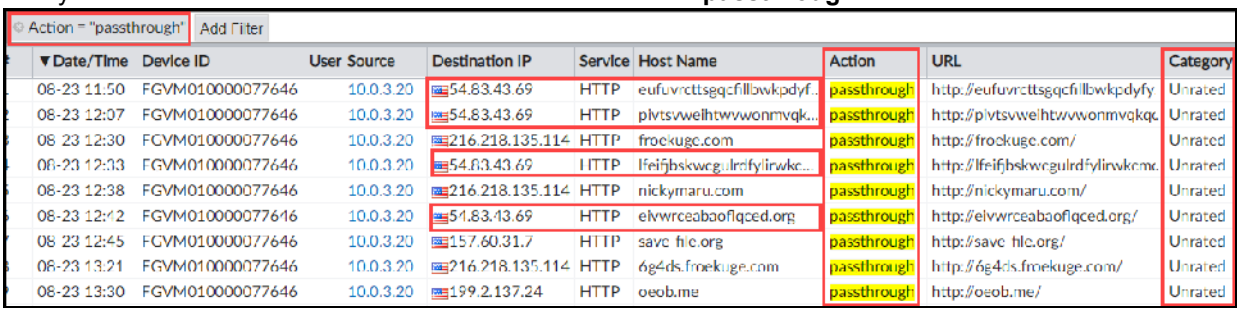


Add Filter

#	▼Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action
1	08-23 11:43	FGVM010000077646		10.0.3.20	34.98.99.30	HTTP	www.888544.com	blocked
2	08-23 11:44	FGVM010000077646		10.0.3.20	3.130.204.160	HTTP	tt915.com	blocked
3	08-23 11:44	FGVM010000077646		10.0.3.20	216.218.135.114	HTTP	jeansowghtqq.com	blocked
4	08-23 11:45	FGVM010000077646		10.0.3.20	193.232.76.153	HTTP	green9.jvibgsez.ru	blocked
5	08-23 11:46	FGVM010000077646		10.0.3.20	164.88.87.228	HTTP	www.zinomp3.com	blocked
6	08-23 11:47	FGVM010000077646		10.0.3.20	67.227.226.240	HTTP	www.xn--l3cgic6bwb6ct...	blocked
7	08-23 11:50	FGVM010000077646		10.0.3.20	54.83.43.69	HTTP	cufuvrcttsgqcfillbwkpdyf...	passthrough
8	08-23 11:50	FGVM010000077646		10.0.3.20	64.70.19.203	HTTP	ffb07fb6990e3b5da86d...	blocked

Note that most of the logs indicate that the traffic was blocked.

9. Apply a filter to include only logs with the action set to **passthrough**.
It may take a few minutes for some events with the action set to **passthrough** to show in the list



Action = "passthrough" Add Filter

▼Date/Time	Device ID	User	Source	Destination IP	Service	Host Name	Action	URL	Category
08-23 11:50	FGVM010000077646		10.0.3.20	54.83.43.69	HTTP	eufuvrcttsgqcfillbwkpdyf...	passthrough	http://eufuvrcttsgqcfillbwkpdyfy	Unrated
08-23 12:07	FGVM010000077646		10.0.3.20	54.83.43.69	HTTP	plvtsvwelhtwvwonmvqk...	passthrough	http://plvtsvwelhtwvwonmvqkqc	Unrated
08-23 12:30	FGVM010000077646		10.0.3.20	216.218.135.114	HTTP	frockuge.com	passthrough	http://frockuge.com/	Unrated
08-23 12:33	FGVM010000077646		10.0.3.20	54.83.43.69	HTTP	lfeifjbskwcgulrdfylirwkc...	passthrough	http://lfeifjbskwcgulrdfylirwkcmc	Unrated
08-23 12:38	FGVM010000077646		10.0.3.20	216.218.135.114	HTTP	nickymaru.com	passthrough	http://nickymaru.com/	Unrated
08-23 12:42	FGVM010000077646		10.0.3.20	54.83.43.69	HTTP	elvwrceabaoflqced.org	passthrough	http://elvwrceabaoflqced.org/	Unrated
08-23 12:45	FGVM010000077646		10.0.3.20	157.60.31.7	HTTP	save hlc.org	passthrough	http://save hlc.org/	Unrated
08-23 13:21	FGVM010000077646		10.0.3.20	216.218.135.114	HTTP	6g4ds.froekuge.com	passthrough	http://6g4ds.froekuge.com/	Unrated
08-23 13:30	FGVM010000077646		10.0.3.20	199.2.137.24	HTTP	oeob.me	passthrough	http://oeob.me/	Unrated

This view should bring several important details to your attention.

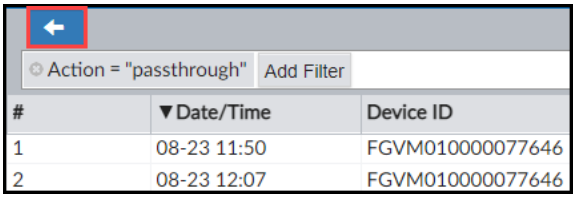
First, the firewall policy categorized these sites as **Unrated**. You should recommend that the firewall administrators adjust the policy settings to block this traffic until it is deemed safe.

Second, all domains pointing to the IP address **54.83.43.69** look suspiciously random. This is a common sign that malware is trying to connect to a command and control (C2) server. These must be blocked.

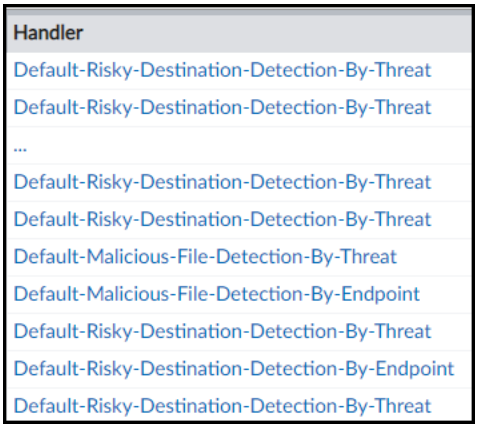
Third, several less random-looking domain names are associated with the same IP address **216.218.135.114**. If you eliminate the action filter from step 9, you will find that traffic to other domains associated with this IP address was blocked, which makes it highly suspicious.

Lastly, some domain names in the list seem to be valid. Further investigation is needed to verify this, and if needed, add some exceptions to the firewall policy.

10. Click the back arrow to return to the **All Events** view, and then clear any remaining filters you may have applied.



11. Scroll to the right to display the **Handler** column, and note the names of the event handlers that generated the events.



You will work with event handlers later in this lab.

The three dots that appear in the previous image indicate that more that one handler generated the events in the container. Click **>** to see the names of the handlers.

12. Stay logged in to FortiAnalyzer for the next exercise.

Exercise 3: Customizing Predefined Event Handlers

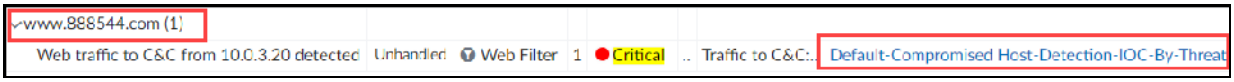
In this exercise, you will examine which event handler generated an event. You will then configure that handler to send a notification email every time it generates a new event. Finally, you will generate some traffic to test the new configuration.

Find the Event Handler and the Log That Generated an Event

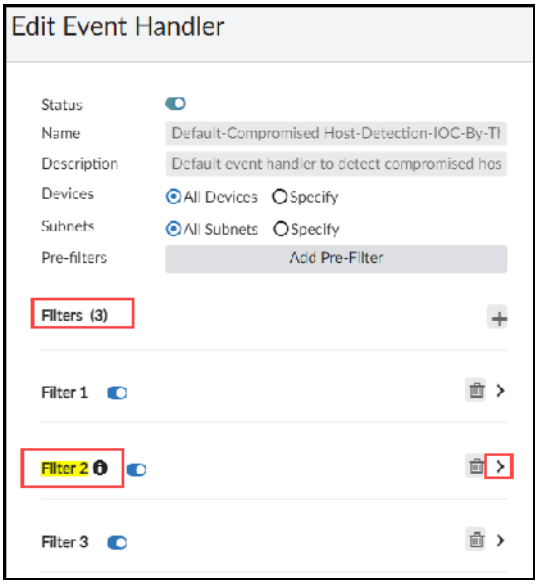
You can find important details about an event by locating which event handler and traffic log that generated it.

To find the event handler and the log that generated an event

1. Navigate to **FortiSoC** > **Event Monitor** > **All Events**, and then apply a filter to include only events with a severity of **Critical**.
2. In the filtered view, find the event related to the domain **www.888544.com**, and then click **>** to expand it.

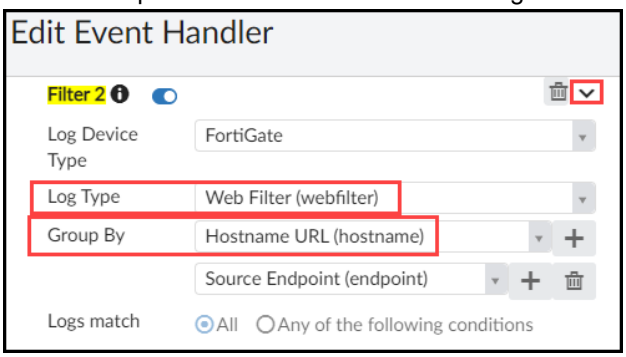


3. Take note of the event handler listed on the right of the entry, and then click it to see its details.
The **Edit Event Handler** window opens and you can see how many filters are included in this handler.
4. Note the specific filter that found the match that generated this event, highlighted in yellow.



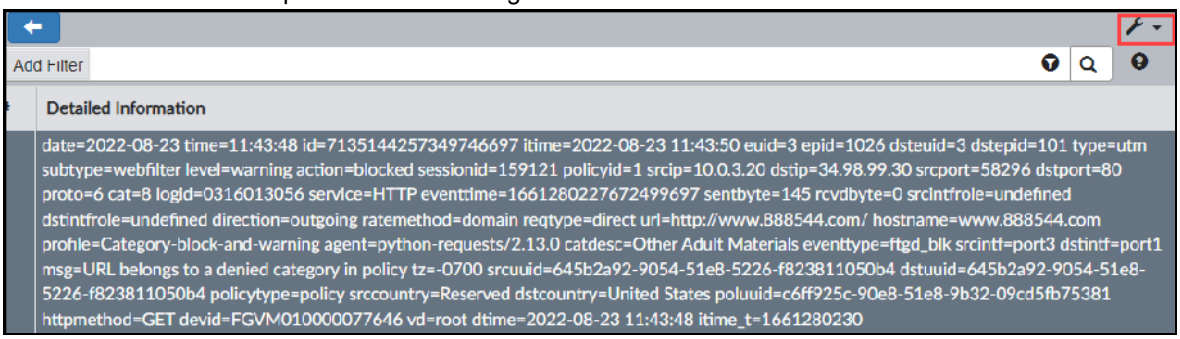
This handler has three filters. **Filter 2** was the one that found a match, and generated the event you are examining.

5. Click **>** to expand the filter and see all its settings.



The handler shown here is one of several predefined handlers that come with FortiAnalyzer. You can make some minor changes to these handlers. To make bigger changes you must clone them, and then edit the clones.

6. Click **OK** to close the **Edit Event Handler** window.
7. Double-click the event to open its associated log, and then click the tool icon to change the view to **Raw**. This view includes all the parameters in this log.



8. Click the back arrow to return to the event view.

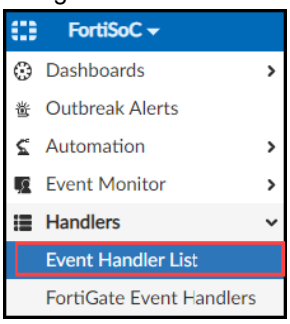
To customize the predefined event handler settings

Stop and think!

You now know which predefined event handler created the event we are interested in.

For this exercise, let's assume that this specific event requires special attention, and an email notification must be sent every time it is detected. Now, you will configure the handler to achieve this.

1. Navigate to **FortiSoC** > **Handlers** > **Event Handler List** to see all the predefined event handlers.

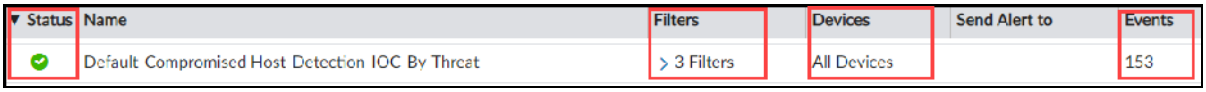


2. Note the predefined handlers are listed in the right pane.

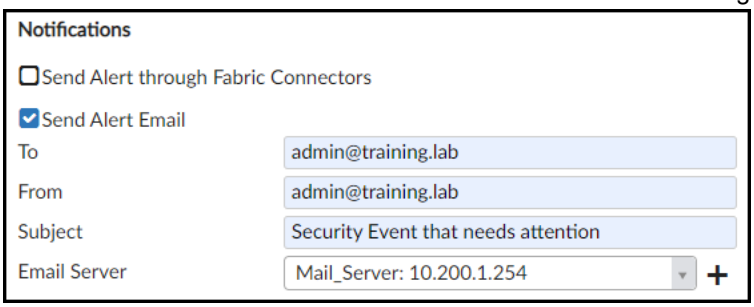
Not all predefined event handlers are enabled by default.

You cannot delete any of these handlers. However, you can disable them so they don't generate events.

3. Note that each entry listed shows the status of the handler, how many filters it has, the devices from which it will be examining logs, and the number of events it has generated so far.

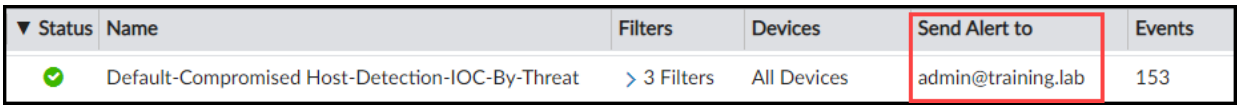


4. Double-click the handler named **Default-Compromised Host-Detection-IOC-ByThreat** to see its settings. The window displayed is the same one you saw before, except now it doesn't show any matched filters.
5. Edit the **Notifications** section at the bottom to look like the following image:



Note that the email server at `10.200.1.254` is already configured in FortiAnalyzer.

6. Click **OK** to close the handler settings page and return to the **Event Handlers List**.
7. Notice the email address under the **Send Alert to** column.

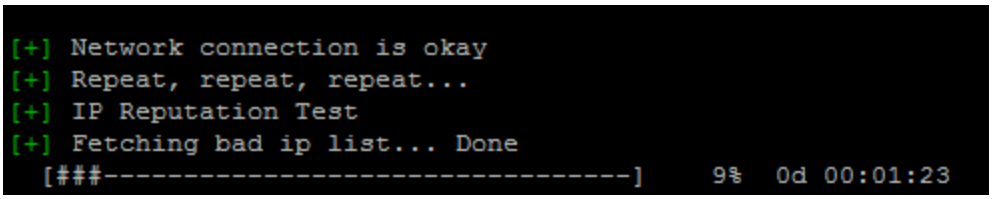


Generate Traffic to Create Events

Now, you will generate some traffic to test the change you made to the event handler.

To generate traffic using FIT

1. On the Local-Client VM, open PuTTY, and then connect to the FIT saved session (connect over SSH).
2. Log in with the username `student` and password `password`.
3. Enter the following command to run a script that changes the default route of FIT to send traffic through the Internal Segmentation Firewall (ISFW) (see Network Topology on page 5):
   ```
   $ sudo ./default3
   ```
4. When prompted, enter the password again.
5. Enter the following command to check the default route:
   ```
   $ ip route
   ```
   You should see the default route through `10.0.3.254`.
6. Enter the following commands:
   ```
   # cd FIT
   # ./fit.py all --repeat
   ```
   Traffic will begin to generate, and the script will repeat each time it completes.

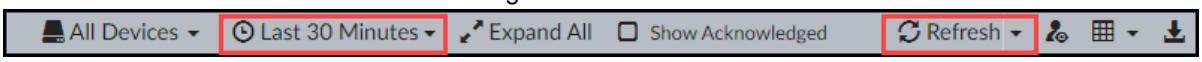
7. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate.

Verify that the Modified Event Handler Works

The traffic being generated should trigger the event handler to create new events.

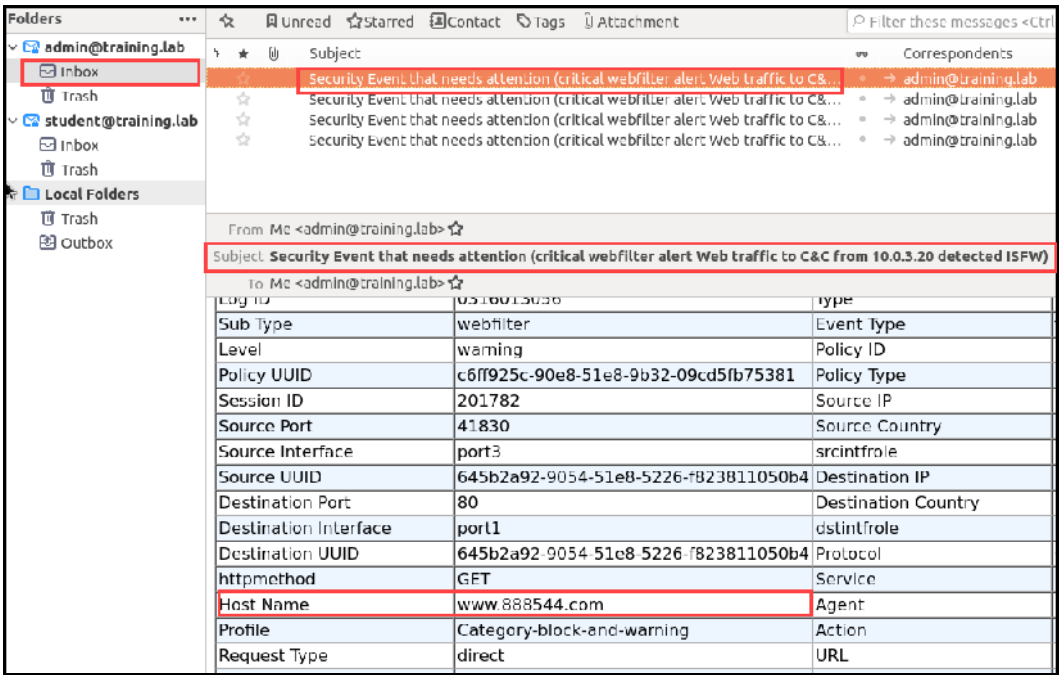
To verify that the custom handler generated new events and sent a notification email

1. Return to **FortiSoC** > **Event Monitor** > **All Events**.
2. Filter the view to the last 30 minutes and change the refresh rate to 10 seconds.

3. Verify that new events are showing while paying close attention to the **Event** column and looking for the entry **www.888544.com**.
4. Once you see that entry, return to the PuTTY session, and then press `Ctrl+Z` to stop the script.
   Leave the PuTTY session open for a later test.

5. Open Thunderbird, and then verify that you received an email notification with the configured subject in the **admin** mailbox.



Note that it may take several seconds for the email to appear in Thunderbird.

You should have received more than one email associated with this event. This is because you didn't change any of the filter settings in the handler, and other events also send email notifications.

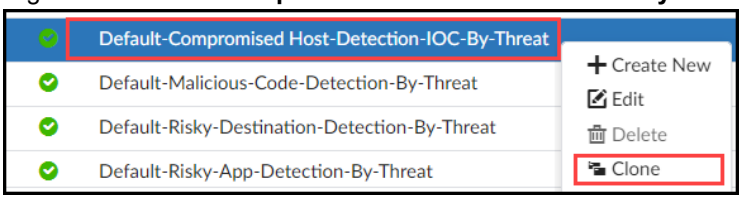
You will fix this in the next steps.

Clone and Customize an Event Handler

Following the scenario from above, and to ensure you receive email notifications only when a specific event occurs, you must be able to edit other settings in the handler. To do this, you will clone the predefined handler we know creates the desired event, and then edit the clone.

To clone and customize an event handler

1. Return to **FortiSoC** > **Handlers** > **Event Handlers List**.
2. Right-click **Default-Compromised Host-Detection-IOC-ByThreat**, and then select **Clone**.



A new window opens with all settings now available for editing.

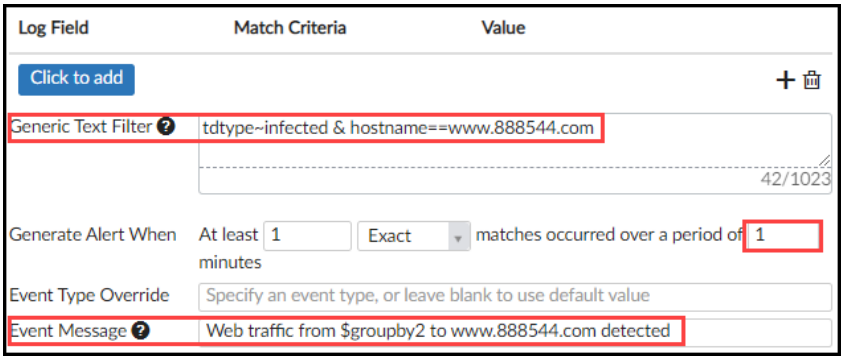
3. Change the name of the new handler to `Compromised Host-Detection-888544`.

4. Change the description to `Event handler to detect compromised hosts accessing www.888544.com`.
5. Click the toggle buttons to disable **Filter 1** and **Filter 3**.
   You can also delete these filters, but you would have to recreate them later if needed.

Stop and think!

We determined earlier that **Filter 2** is generating the events we are concerned about. That is why we are disabling the other filters.

6. Expand **Filter 2** by clicking **>**.
7. Edit the **Generic Text Filter** and **Event Message** fields to match the following image:



You set the period to 1 minute so that other exercises in this lab work properly. In a real-world scenario you should adjust this value depending on your specific requirements.

A short time period setting may generate too many events. However, a longer time period setting may cause you to miss important notifications.

Stop and think!

You added a condition in the generic text filter to match a specific hostname. You found the hostname by checking the raw view of the log. You can also use other log fields.

8. Click **OK** to save the changes.
9. Open the original event handler, **Default-Compromised Host-Detection-IOC-ByThreat**, and then remove the check mark in the notifications section to prevent FortiAnalyzer from sending other emails.
10. Click the toggle button to disable **Filter 2**.

You disable **Filter 2** to prevent the generation of duplicate events in this lab.

11. Click **OK** to save the changes.

Test the Cloned Event Handler

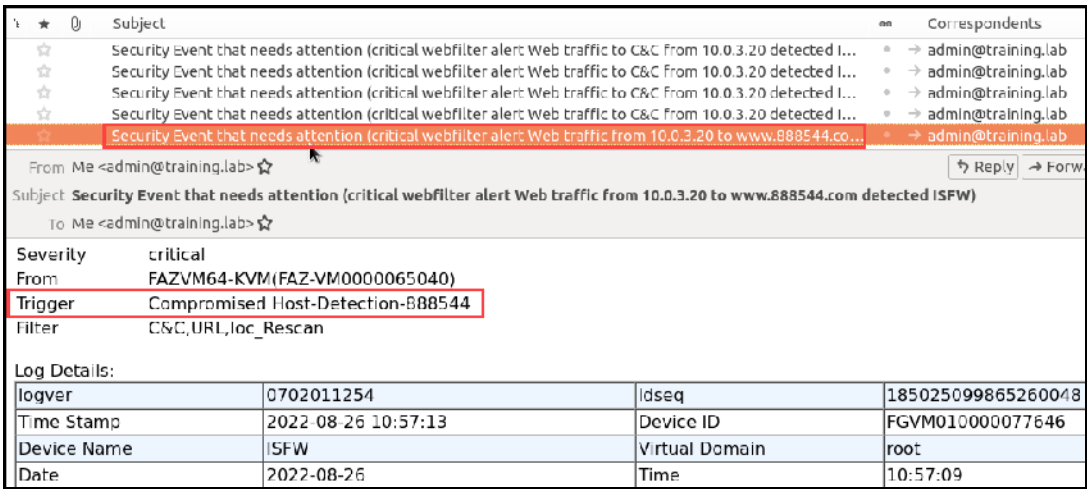
You will test the cloned event handler by generating traffic once again.

To generate traffic using FIT

1. Return to the PuTTY session, and enter:
   ```
   # ./fit.py all --repeat
   ```
   Traffic will begin to generate, and the script will repeat each time it completes.
2. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate.

To verify that the cloned event handler works

1. Return to **FortiSoC** > **Event Monitor** > **All Events**.
2. Filter the view to the last 30 minutes and change the refresh rate to 10 seconds.
3. Verify that new events are showing while paying close attention to the **Event** column and looking for an entry called **www.888544.com**.
4. Once you see that entry, return to the PuTTY session, and then press `Ctrl+Z` to stop the script.
5. Leave the PuTTY session open for a later test.
6. Return to Thunderbird, and then verify that you received an email notification with the configured subject in the **admin** mailbox.



This time you should have received a single email, generated after the specific event was created.

7. Minimize the Thunderbird window
8. Log out of FortiAnalyzer before proceeding to the next exercise.

Exercise 4: Creating a Custom Event Handler

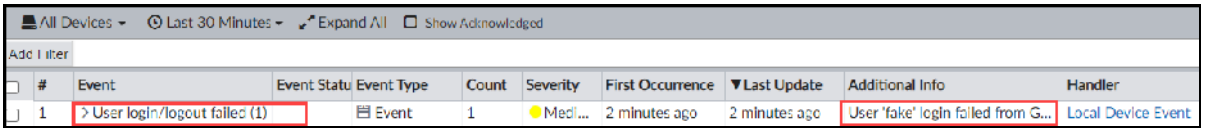
In this exercise, you will generate an event by using an invalid set of credentials to log in to FortiAnalyzer. Then, you will obtain the details from the log generated and use them to create a new event handler from scratch.

Create an Event and Find the Log That Generated It

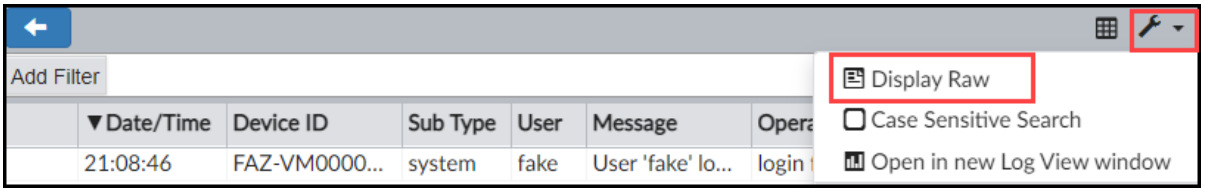
You can view the details of existing events to use as a reference when you create custom event handlers.

To force the generation of an event and view the log that generated it

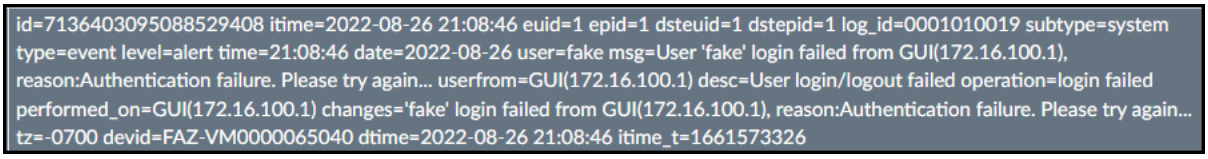
1. Log in to the FortiAnalyzer GUI with the username `fake` and password `fake`.
   This user does not exist, so you will receive an error that prevents you from logging in.
2. Log in with the correct credentials—`admin` and `password`—and then click the **root** ADOM.
3. Navigate to **FortiSoC** > **Event Monitor** > **System Events** > **Local Device**.
4. Filter the view to include only the **Last 30 Minutes**.
   You should see the event that the failed login attempt generated.



5. Double-click the event to see the details of the log that generated it.
6. Change the view to **Display Raw** to find all parameters that can be used to create generic text filters.



The raw view should look similar to the following image:



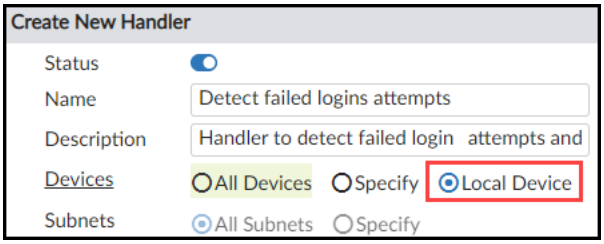
As you saw in the previous exercise, each field in this view can be used as part of a generic text filter.

Create a Custom Event Handler

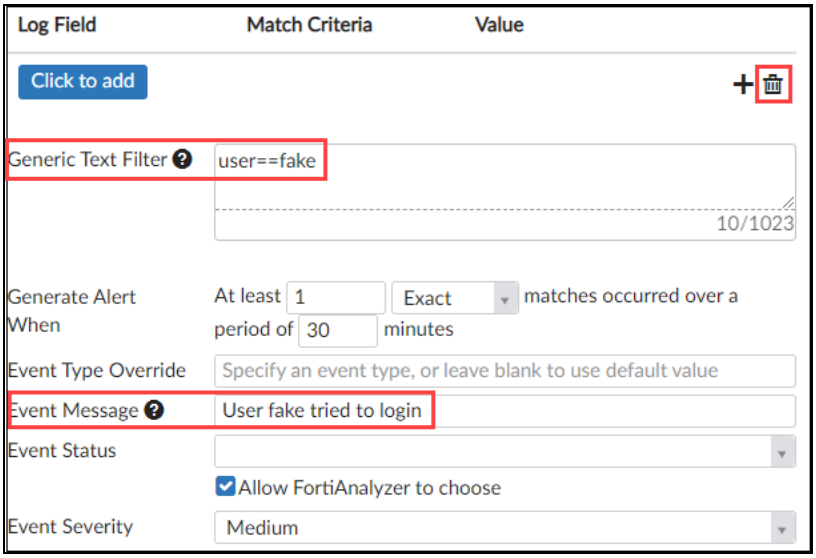
Now that you know the details of the log created after a failed login attempt, you will create a custom event handler based on those details.

To create a new event handler

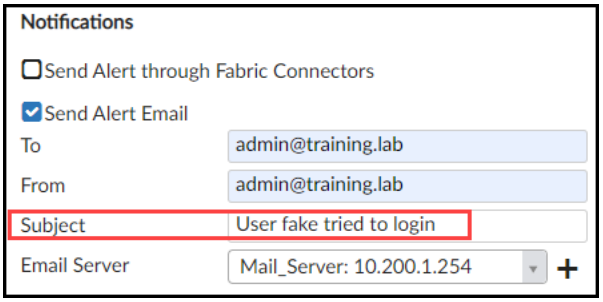
1. Navigate to **Handlers** > **Events Handler List**.
2. Click **Create new**.
3. Change the handler name to `Detect failed login attempts`.
4. Change the handler description to `Handler to detect failed logins and send an email notification`.
5. Select **Local Device**, and then click **OK** to accept the **Reset Filters** warning.
   This warning states that the filters available depend on the type of device that you select. Since you selected **Local Device**, all filters will be related to FortiAnalyzer.



6. Click the trash can icon to remove the **Log Field** filter.
7. Edit the **Generic Text Filter** and **Event Message** fields to match the following image:



   This filter matches only when a user tries to log in with the username **fake**.
8. Configure this handler to send an email with the **Subject** of `User fake tried to login`.



9. Click **OK** to save the changes.

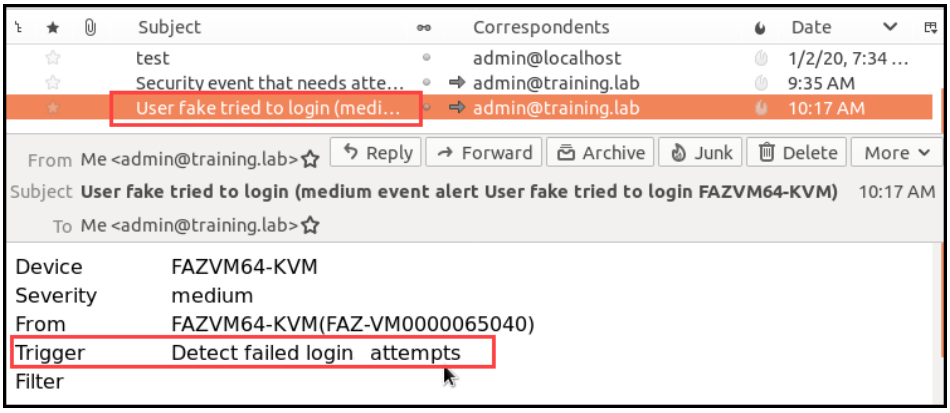
Test the Custom Event Handler

You will test the custom event handler by attempting to log in with invalid credentials.

To verify that the new event handler works

1. Log out of the FortiAnalyzer GUI, and then try to log in again with the username `fake`.
2. Log in to the **root** ADOM again with the username `admin` and password `password`.
   You should see that one event was generated by the new handler.

3. Open Thunderbird , and then verify that you received a new email with the correct subject.



4. Close the email client, and then log out of FortiAnalyzer.

Expert Challenge

Take the Expert Challenge!

Create another generic text filter.

If you require assistance, or to verify your work, use the step-by-step instructions that follow.

Edit the generic text filter in the custom event handler that you created in this exercise so it generates an event when a potential intruder tries to log in as the `admin` user, from any device other than the Local-Client VM.

Challenge solution

1. Review the original raw log.

```
id=7136403095088529408 itime=2022-08-26 21:08:46 euid=1 epid=1 dsteuid=1 dstepid=1 log_id=0001010019 subtype=system type=event level=alert time=21:08:46 date=2022-08-26 user=fake msg=User 'fake' login failed from GUI(172.16.100.1), reason:Authentication failure. Please try again... userfrom=GUI(172.16.100.1) desc=User login/logout failed operation=login failed performed_on=GUI(172.16.100.1) changes='fake' login failed from GUI(172.16.100.1), reason:Authentication failure. Please try again... tz=-0700 devid=FAZ-VM0000065040 dtime=2022-08-26 21:08:46 itime_t=1661573326
```

2. Notice the **user**, **performed_on**, and **operation** fields in the log.
3. Edit the generic text filter with `user==admin` to match any login attempts with that user.
4. Add the text `operation=="login failed"` to match only failed login attempts.
   If you don't include this condition, you will get more matches than what is required.
5. Add the text `performed_on!~10.0.1.10`.
   This includes any attempts coming from devices with an IP address that is not the one configured on the Local-Client computer.

You need this syntax because the requirements do not specify the method the attacker uses to try to access FortiAnalyzer.

If you were looking only for attempts using a browser, you could use `performed_on!="GUI(10.0.1.10)"` instead.

If you were looking only for attempts using SSH, you could use `performed_on!="ssh(10.0.1.10)"` instead.

6. Combine the three conditions with a logical `&`:
   `operation=="login failed" & user==admin & performed_on!~10.0.1.10`

Exercise 5: Managing Incidents

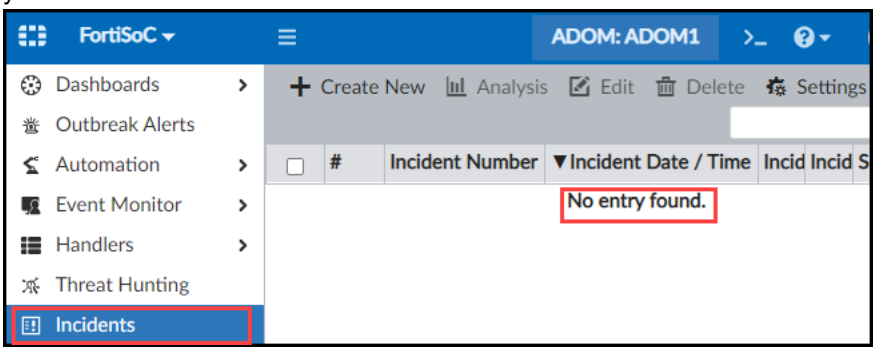
In this exercise, you will practice how to create, or raise, an incident manually in FortiAnalyzer, and you will explore some of the tools available to security analysts to work with existing incidents.

Create New Incidents Manually

You will create a new incident from several events that must be investigated.

To create an incident manually

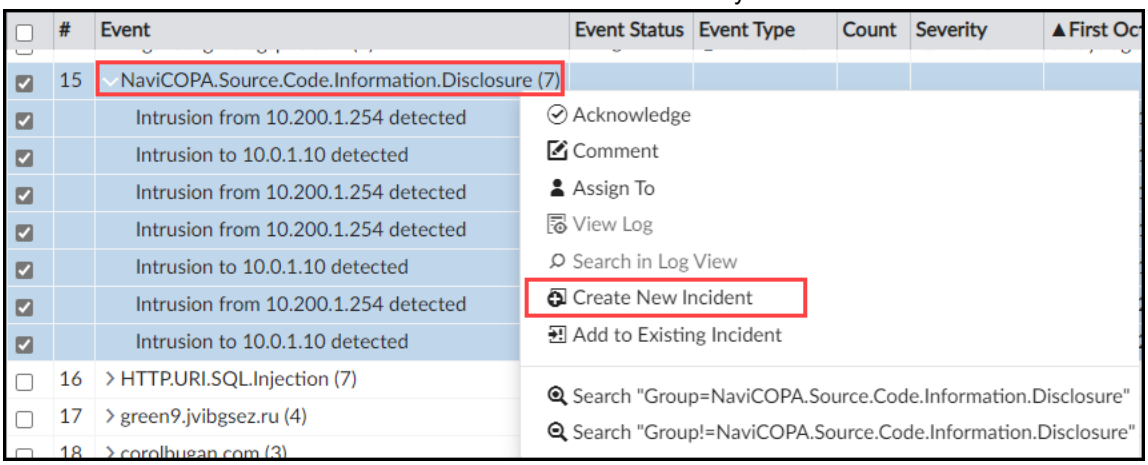
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**, and then click **Incidents**.
   As you saw before in the dashboard with the same name, no incidents have been created in this environment yet.



   Incidents can be raised from events the SOC analysts think require further investigation. For example, an event that appears as **Unhandled** should always be examined.

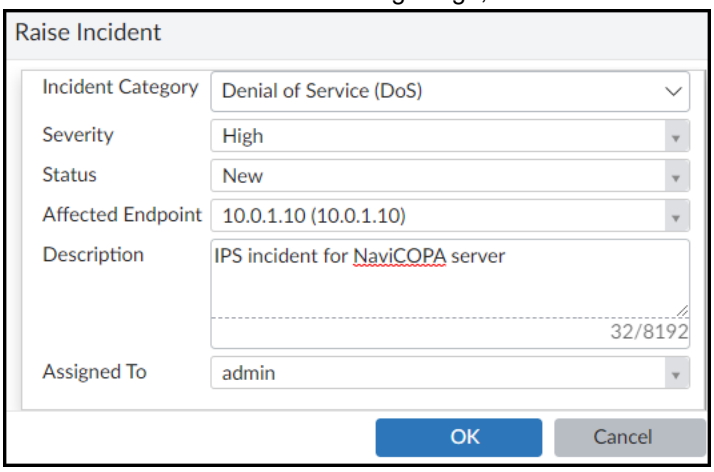
4. Click **FortiSoC** > **Event Monitor** > **All Events**.
5. Find the entry that starts with **NaviCOPA.Source.Code**.
   Remember that you can add a filter to help you with your search. Hint: Filter by **Group**.

6. Right-click the **NaviCOPA.Source.Code** entry, and then select **Create New Incident**.
This creates an incident that contains all the events within that entry.



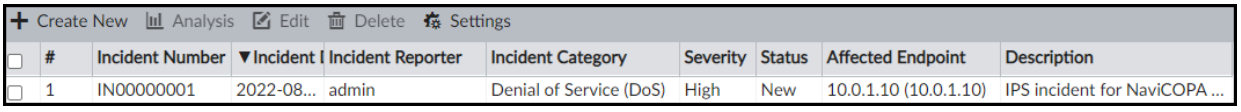
When creating an incident from a filtered view, the number of events included in the incident depends on the time period filter you set and on how many events were generated during that time frame.

7. Explore the available options on the **Raise Incident** window.
8. Edit each field to match the following image, and then click **OK**.

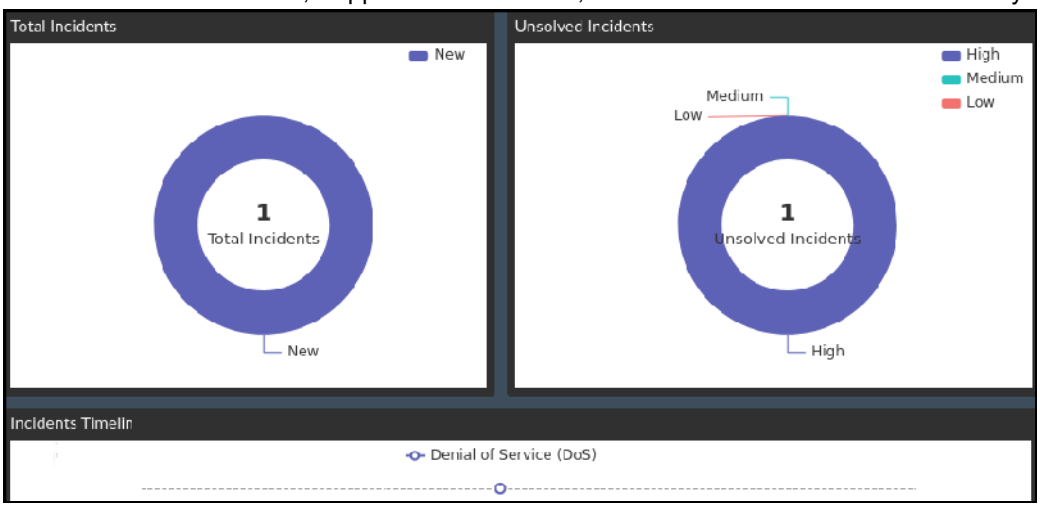


In a production scenario, adjust these values according to the severity and urgency of the event.

9. Click **Incidents**.
Now you should see the incident you just created.



10. Verify that the new incident appears in the **Incidents** dashboard.
Because it's a new incident, it appears as **Unsolved**, and the color code indicates its severity.

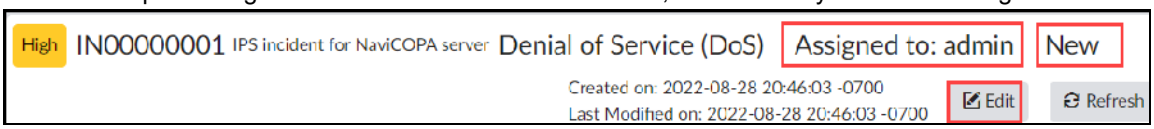


This dashboard allows SOC analysts to easily get an overview of how quickly their team is dealing with security incidents.

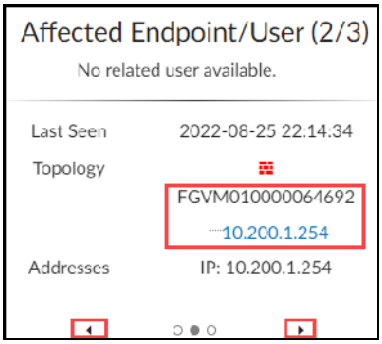
For example, depending on how many unsolved incidents are present, and what their severity is, higher priority can be given to the most important ones.

To examine the incident analysis window

1. Return to **FortiSoC** > **Incidents**, and then double-click the current incident to open its **Analysis** page.
2. Examine the top of this page.
This section provides general information about the incident, and the ability to edit its settings.

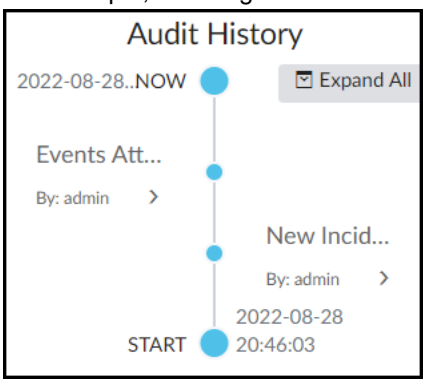


3. Examine the **Affected Endpoint/User** section.
This section shows all devices and users (if available) involved in the incident. You can change which one is displayed by clicking the navigation buttons. You can click the IP address of the device to open **Fabric View** in a new window.

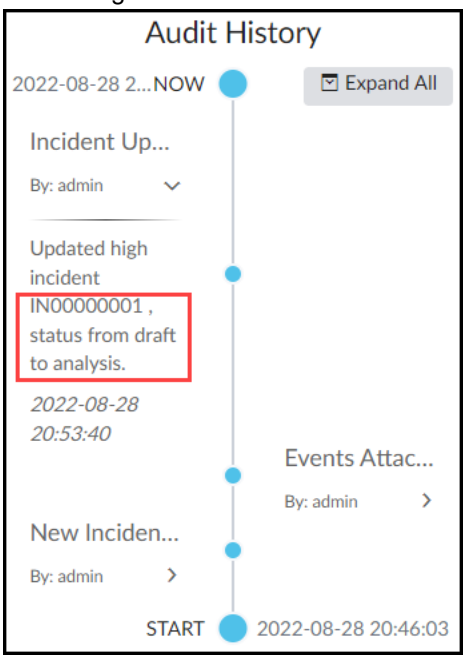


4. Examine the **Executed Playbooks** section.
This section includes any playbooks associated with the incident, and allows you to execute them, if required.

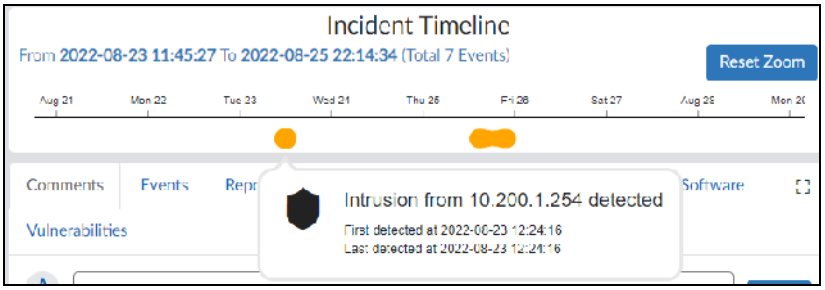
5. Examine the **Audit History** section.
This section allows you to keep track of all the activity since the incident was created.
For example, following the scenario above, the panel should look like the following image:



6. Click **Edit**, change the status of the incident to **Analysis**, and then click **OK**.
This change is reflected in the **Audit History**. You might need to refresh the **Analysis** page to see the update.

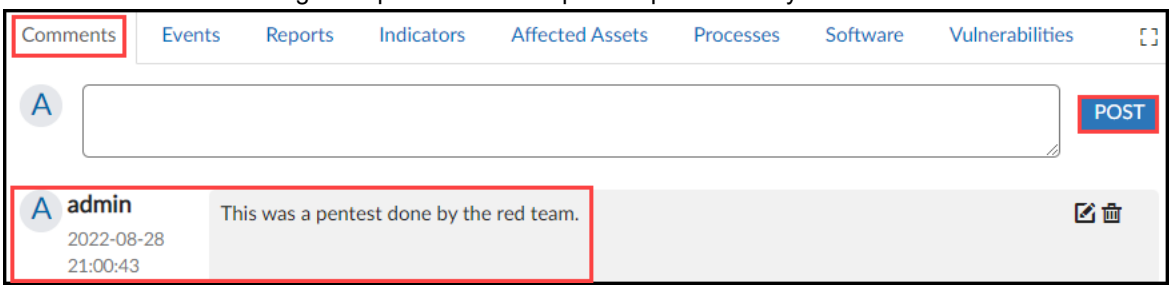


7. Examine the **Incident Timeline** section.
This section provides the exact dates and times the suspicious traffic was detected. Hover over the yellow dots to display more details in a pop-up window. You can also use the mouse to zoom in or out on the timeline.

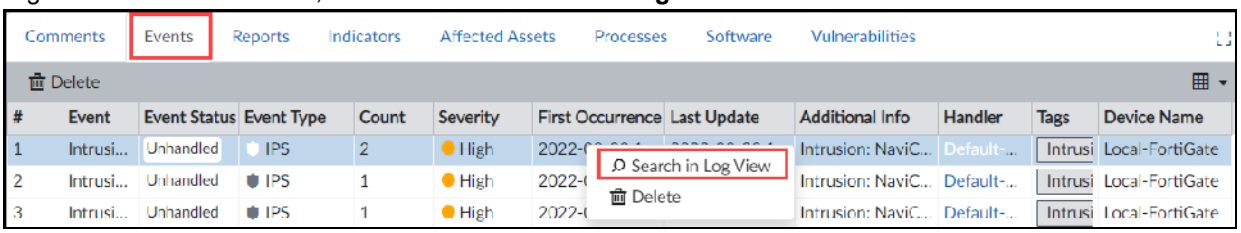


8. Examine the tabs at the bottom.

9. Click the **Comments** tab, start typing your comment in the text box, and then click **Post**.
The incident in the following example was due to a pentest performed by the red team:

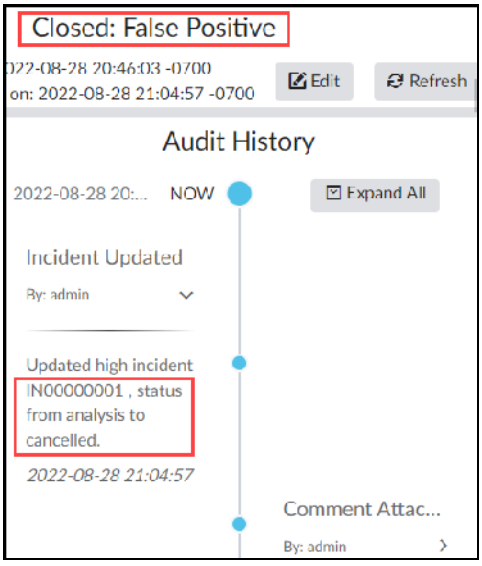


10. Verify that this action is also reflected in **Audit History**.
11. Click the **Events** tab to see all associated events.
12. Right-click one of the events, and then select **Search in Log View**.

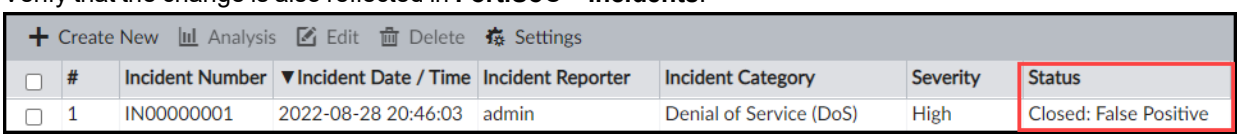


Log View opens in a new window with the related filter already applied.

13. Explore the other tabs to see the information they include.
Depending on the type of events associated with the incident, some tabs may not display any data.
14. Change the incident status to **Closed: False Positive**.
15. Verify that the change is reflected on the **Analysis** page.



16. Verify that the change is also reflected in **FortiSoC** > **Incidents**.



Closing an incident does not remove it from the list. The security policy determines when to remove it.

You should remove a closed incident only when you are sure it does not need to be reopened. This is especially important in environments that have a high volume of security-related activity.

17. Return to the **Incidents** dashboard, and notice that the number of unsolved incidents is now zero.

18. Keep the FortiAnalyzer session open for the next exercise.

Exercise 6: Exploring Threat Hunting

In this exercise, you will explore the Threat Hunting tool included with FortiAnalyzer.

Threat hunting uses a proactive approach when dealing with security threats. Many times, an apparently harmless event, such as intensive network activity at unexpected times of the day, can precede a dangerous attack.

Every threat-hunting activity starts with a hypothesis, or question. For this exercise, you will generate some traffic in the background, and your question is:

During the last hour, has DNS tunneling been used in the network to exfiltrate confidential data?

In this exercise you will hunt for threats using the logs from the last hour only. However, in a production scenario, you generally use logs from a longer period of time.

Also, keep in mind that this is a simulation exercise, and no actual attack takes place.

Generate Traffic

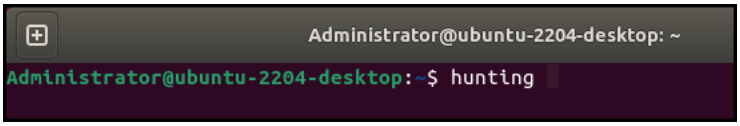
You will generate traffic to use in this exercise.

To generate traffic using a script

1. On the Local-Client VM, open a terminal session and enter the following command:

   ```
   $ hunting
   ```

   Traffic is generated in the background.



2. Leave the terminal session open while the traffic is being generated.

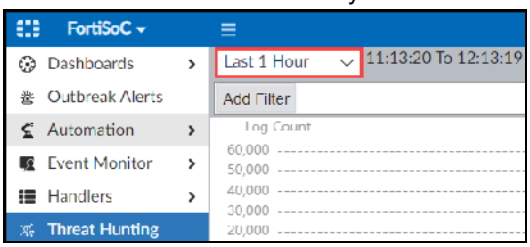
Let the script run for a few minutes before you proceed to the next step to ensure enough logs are created.

Performing Threat Hunting

Use the Threat Hunting tool to answer the question *During the last hour, has DNS tunneling been used in the network to exfiltrate confidential data?*

To access the Threat Hunting tool

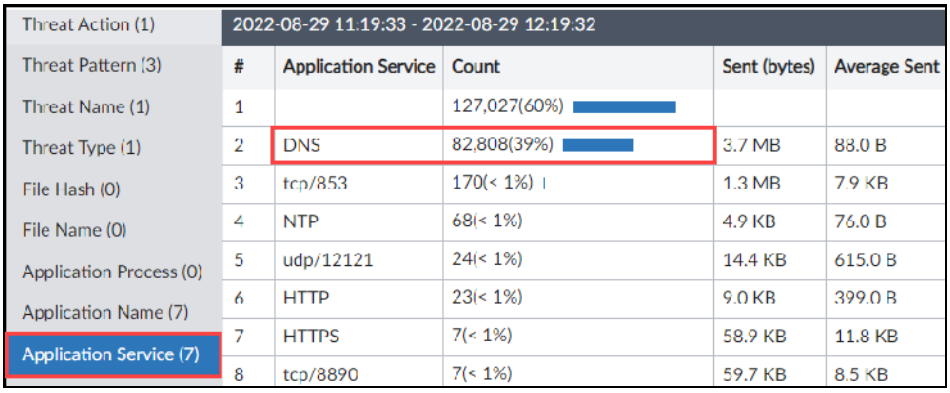
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**, and then click **Threat Hunting**.
4. In the right pane, observe the **Log Count**.
5. Use the time filter to include only the last hour.



When you use the **Log Count** chart, you can apply the same filters available in **Log View** to narrow down the details displayed.

For example, you can apply a filter to include traffic during the weekend or outside of office hours, and from specific IP addresses.

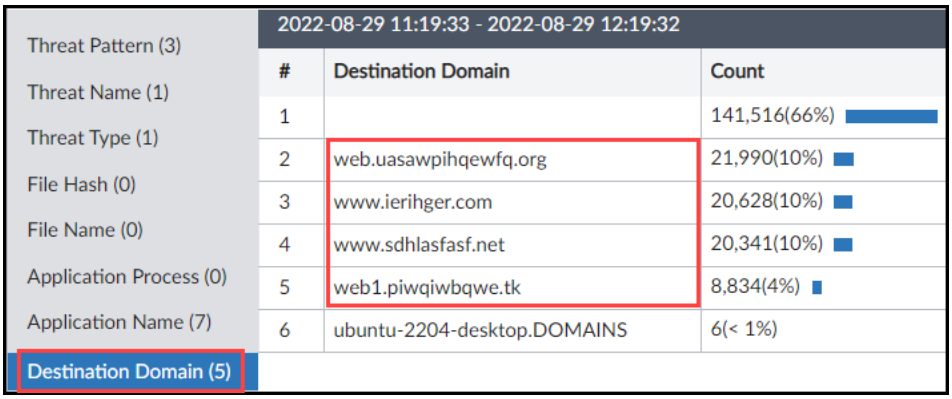
6. Observe the **SIEM Analytics table** located under the **Log Count** chart, and then click **Application Service**. You should see a considerable amount of logs due to DNS traffic.



A higher than normal amount of DNS traffic is an indication of a possible attack.

In the image above, 39% of the logs in the time frame examined are related to DNS. This is not normal and requires further investigation.

7. In the left pane, click **Destination Domain**.
You should see four domain names that look randomly generated.

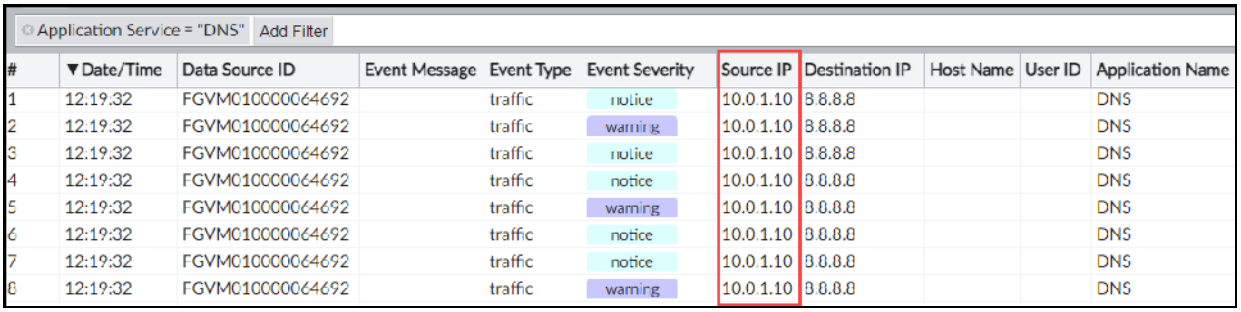


The use of randomly generated domains is a well-known technique used in DNS tunneling attacks.

Based on the information displayed above, about 34% of the DNS requests are related to these four domain names. This indicates that a DNS tunneling attack may be occurring.

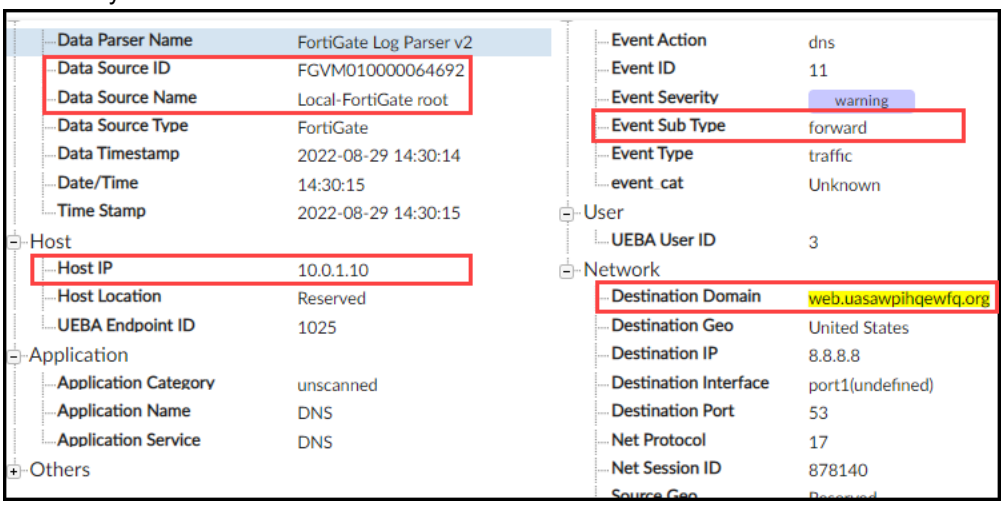
Note: In a real-world DNS tunneling attack, more than four domains may appear in the list.

8. In the left pane, click **Application Service**, and then double-click the DNS entry to obtain details about the suspicious traffic.
   You should see many logs similar to the ones in the following image:



9. Double-click some of the entries to display the details of the logs.
   Confirm that most of the logs are related to the four domain names you found previously, and that the traffic is

allowed by the firewall.



10. Additionally, you can navigate to **Log View** > **FortiGate** > **Security** > **DNS** to find other details such as the ID of the firewall policy that is allowing the traffic through.

Stop and think!

Based on the information you found, you can now escalate the issue to the proper team and provide them with the following details:

- The device with the IP address `10.0.1.10` is compromised.
- The excessive number of DNS requests and the apparently random generated domain names point to a DNS tunneling attack.
- The firewall reporting the traffic is `Local-FortiGate`, with serial number `FGVM010000064692`.
- At least some of the suspicious traffic is being forwarded by the firewall.
- The DNS server used for these queries is `8.8.8.8`, not the corporate DNS server.

11. Return to the terminal session, and then press `Ctrl-C` to stop the script.
12. Keep the FortiAnalyzer session open for the next exercise.

Exercise 7: Exploring the Outbreak Detection Service

In this exercise, you will explore the Outbreak Detection Service.

The FortiAnalyzer Outbreak Detection Service is a licensed feature that allows you to view outbreak alerts and automatically download related event handlers and reports from FortiGuard.

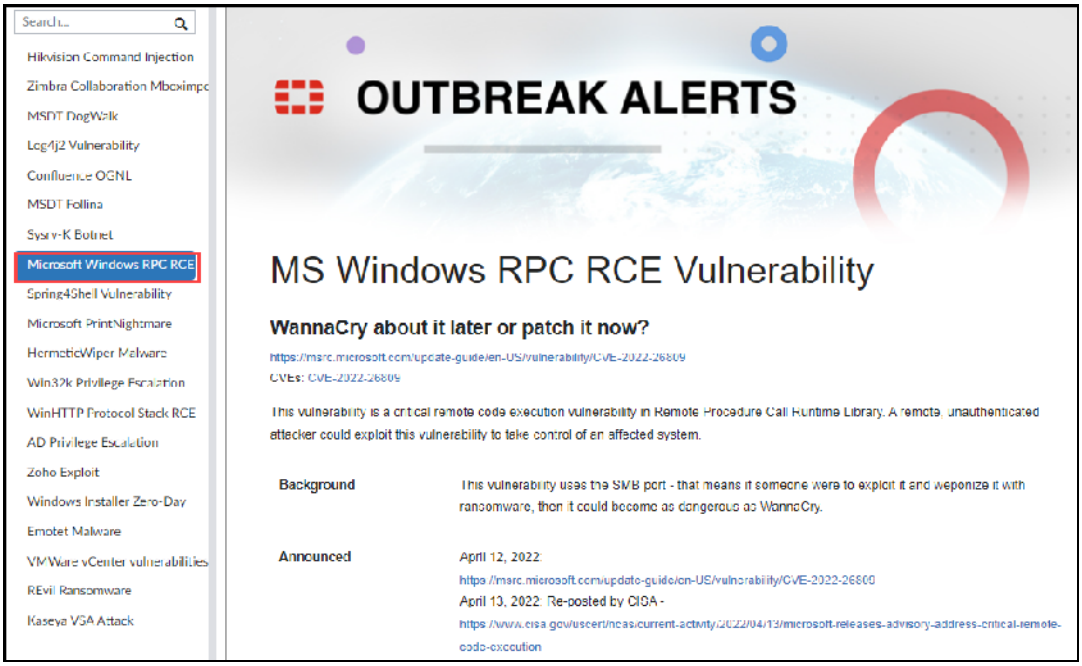
In the lab, you might not see the latest alerts because FortiAnalyzer is configured to work in a closed network environment.

Access the Outbreak Detection Service Dashboard

You will access the Outbreak Detection Service Dashboard to view current outbreak alerts.

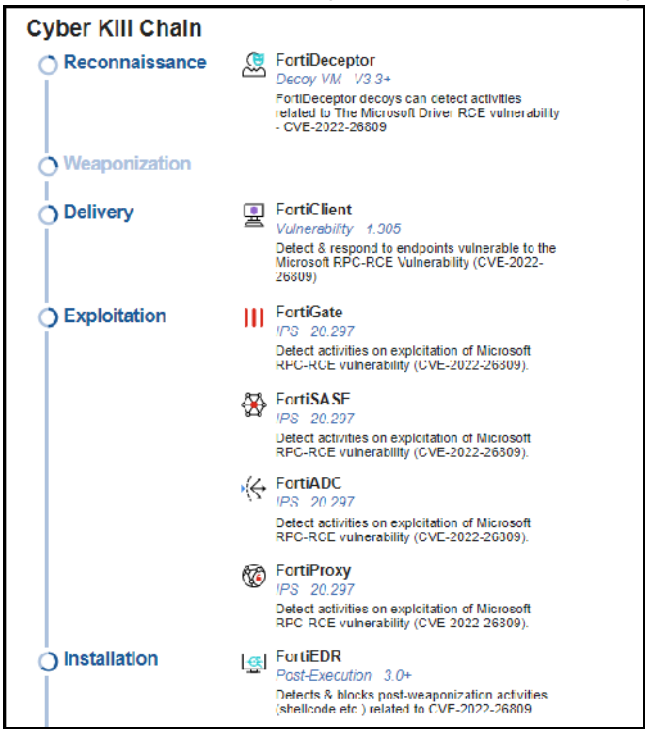
To access the Outbreak Detection Service dashboard

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**, and then click **Outbreak Alerts**.
4. In the right pane, observe the list of alerts.
   It may take a few seconds for the information to appear.
5. In the left pane, click **Microsoft Windows RPC RCE** to display the FortiGuard report about this vulnerability.



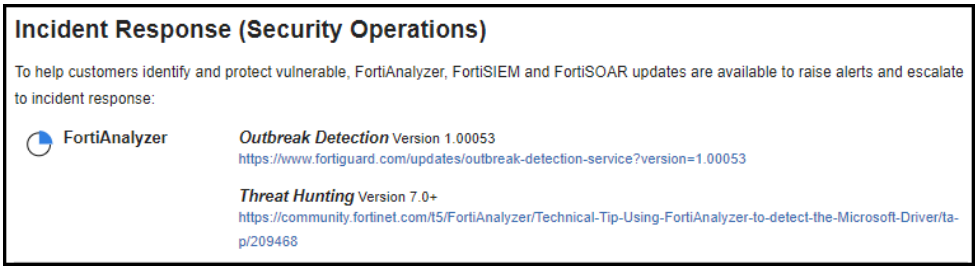
Several links provide access to more information.

6. Scroll down the FortiGuard report to see a list of Fortinet products that can protect you against this vulnerability.



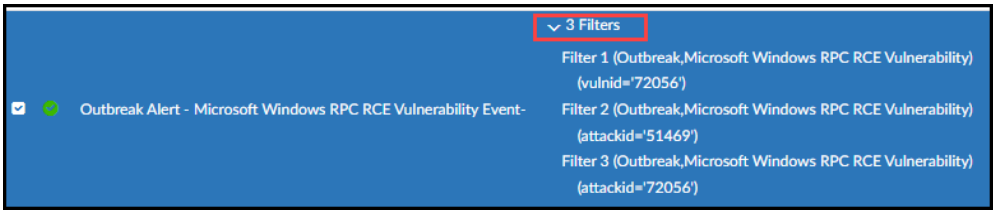
Note the reference to the stages in the Cyber Kill Chain where this vulnerability may be found.

7. Scroll further down in the FortiGuard report to the section labeled **Incident Response (Security Operations)**.



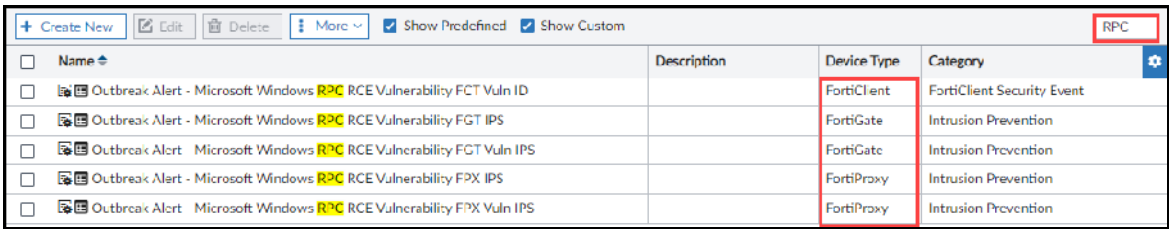
The links in this section allow you to get more information and, if needed, to manually download the event handler and report associated with this vulnerability.

8. In the left pane, navigate to **Handlers** > **Event Handlers list**, and then locate the handler named **Outbreak Alert - Microsoft Windows RPC RCE**.
9. Click **>** to expand the **3 Filters** section.



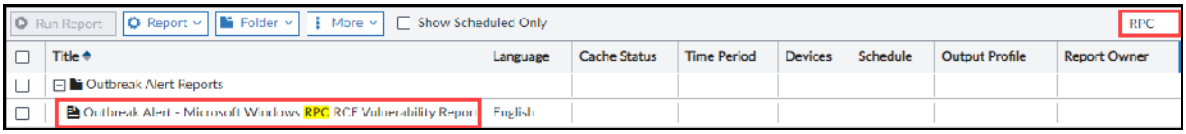
This handler consists of three filters that are configured to create an event when the vulnerability appears in a log from FortiClient, FortiGate, or FortiProxy.

10. In the upper-left corner, click **FortiSoC**, and then click **Reports**.
11. Click **Report Definitions** > **Chart Library**.
12. In the search box, type `RPC` to locate the charts that are used for the report about this vulnerability.
You should see five charts, as shown in the following image:

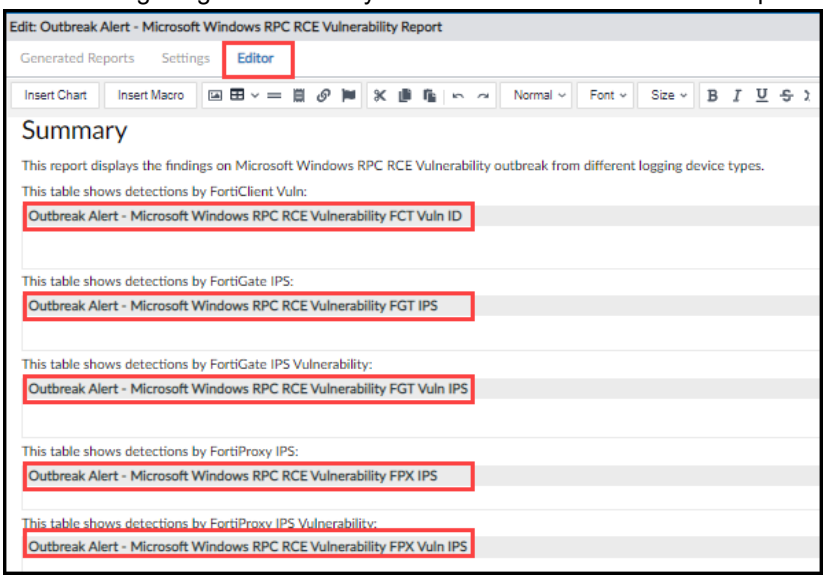


Note: You will learn about reports and charts in another lesson. In this example, each chart is a table.

13. On the left menu, click **All Reports**, and then expand the **Outbreak Alert Reports** container on the right pane.
14. Find and double-click the report named **Outbreak Alert - Microsoft Windows RPC RCE Vulnerability Report**. You can also use the search bar to find it.



15. Click the **Editor** tab to verify that the report includes the five charts from step 12. The following image includes only the headers of each chart in the report:



You can customize the handlers and reports downloaded by the Outbreak Detection Service. It is a best practice to first clone the handlers and reports, and then customize the clones.

SOC analysts should check the Outbreak Detection Service dashboard frequently to ensure they are up to date with the latest threats, and to be better prepared to detect and contain them.

16. Log out of FortiAnalyzer.

Lab 4: Reports

In this lab, you will examine the reporting capabilities included in FortiAnalyzer. You will generate a default report, build a chart based on a log search, and perform some diagnostic checks.

Objectives

- Generate one of the predefined reports
- Build a custom dataset
- Build a custom chart based on a log search
- Build a custom report
- Create a schedule for a report
- Configure an output profile to include a report in an email

Time to Complete

Estimated: 45 minutes

Exercise 1: Running a Default Report

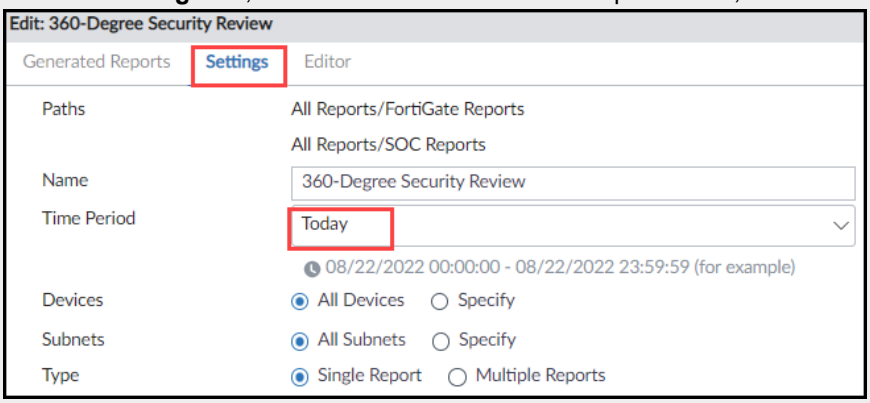
FortiAnalyzer includes many predefined reports to serve a wide variety of scenarios. In this exercise, you will run one of the predefined reports on demand. You will also examine the effect of enabling the Auto-cache feature in a report.

Generate a Default Report

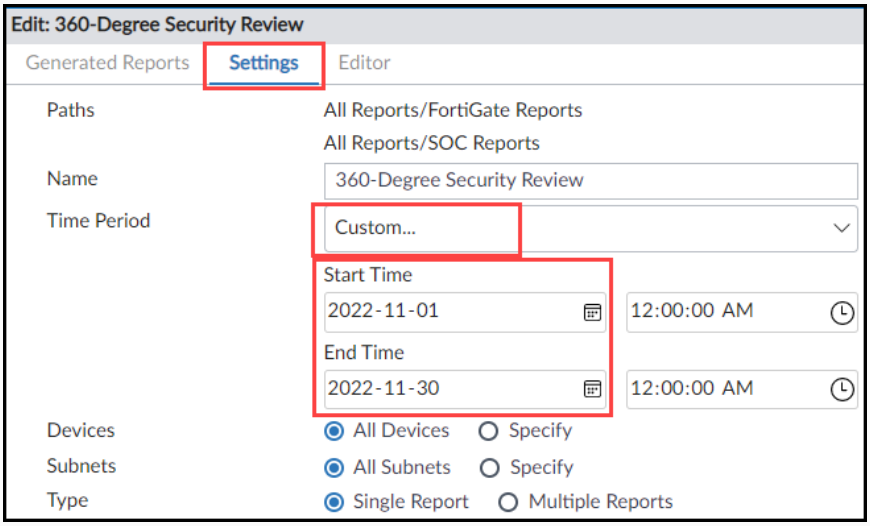
Scenario: Your supervisor has asked you to create a FortiAnalyzer report with a comprehensive security review of your company's network. The report must include information such as detected threats, applications, malicious sites, and malware. Additionally, you want to ensure that this report can be generated as quickly as possible in case you have to generate it frequently. To achieve this, you will enable hcache.

To generate a default report

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **Reports**.
4. In the left menu, select **Reports Definition** > **All Reports**.
   This page lists the available default reports.
5. Double-click the report at **SOC Reports** > **360-Degree Security Review**.
   This report provides the findings of a comprehensive security review conducted in your network, and includes all the required information.
6. Depending on the class format, do one of the following:

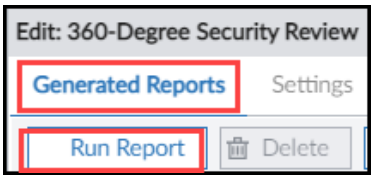
Class Format	Do This...
Instructor-led class	Click the **Settings** tab, and then in the **Time Period** drop-down list, select **Today**.  **Note**: If you didn't do the previous labs the same day you are doing this one, adjust the **Time Period** accordingly to avoid a report with little or no data.

Class Format	Do This...
Self-paced class	Click the **Settings** tab, and then in the **Time Period** drop-down list, select **Custom** and specify the time range shown in the image.

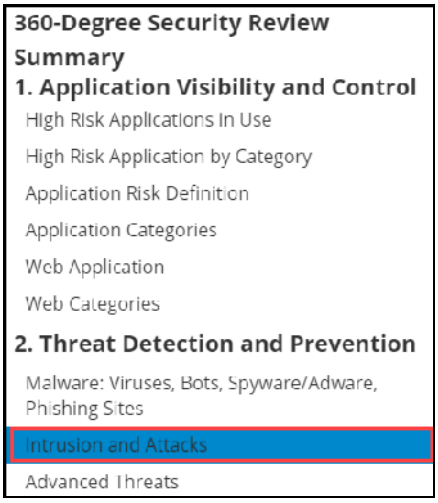


Note: Some traffic was generated during the time range specified to ensure that the resulting report is not empty.

7. Click **Apply**.
8. Click the **View Report** tab, and then click **Run Report**.

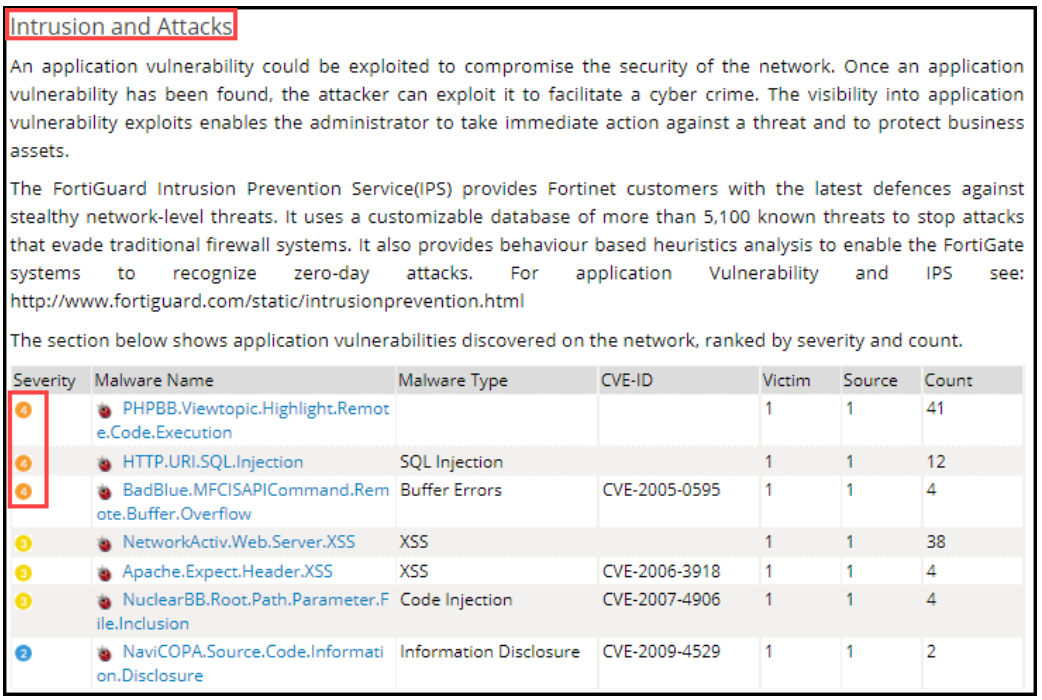


9. When the report is ready, in the **Format** column, click **HTML** to view the report in HTML format.
10. In the left menu, select **Intrusion and Attacks**.



As you can see from the report, several types of attacks are occurring in your network.

11. Look for any severity 4 attacks.



Intrusion and Attacks

An application vulnerability could be exploited to compromise the security of the network. Once an application vulnerability has been found, the attacker can exploit it to facilitate a cyber crime. The visibility into application vulnerability exploits enables the administrator to take immediate action against a threat and to protect business assets.

The FortiGuard Intrusion Prevention Service(IPS) provides Fortinet customers with the latest defences against stealthy network-level threats. It uses a customizable database of more than 5,100 known threats to stop attacks that evade traditional firewall systems. It also provides behaviour based heuristics analysis to enable the FortiGate systems to recognize zero-day attacks. For application Vulnerability and IPS see: http://www.fortiguard.com/static/intrusionprevention.html

The section below shows application vulnerabilities discovered on the network, ranked by severity and count.

Severity	Malware Name	Malware Type	CVE-ID	Victim	Source	Count
4	PHPBB.Viewtopic.Highlight.Remote.Code.Execution			1	1	41
4	HTTP.URI.SQL.Injection	SQL Injection		1	1	12
4	BadBlue.MFCISAPICommand.Remote.Buffer.Overflow	Buffer Errors	CVE-2005-0595	1	1	4
3	NetworkActiv.Web.Server.XSS	XSS		1	1	38
3	Apache.Expect.Header.XSS	XSS	CVE-2006-3918	1	1	4
3	NuclearBB.Root.Path.Parameter.File.Inclusion	Code Injection	CVE-2007-4906	1	1	4
2	NaviCOPA.Source.Code.Information.Disclosure	Information Disclosure	CVE-2009-4529	1	1	2

12. Click the malware name associated with one of the severity 4 entries to link to the FortiGuard website, where you can view more information about the attack.

Run Diagnostics on a Report and Enable HCACHE

FortiAnalyzer creates a diagnostic log for each report. You can examine this log to troubleshoot a report that did not provide the expected information, or that was slow to generate.

To run diagnostics on a report

1. Return to the FortiAnalyzer GUI, right-click the report you just ran, and then select **Retrieve Diagnostic**.
2. Save the file.
3. Open the `rpt_status.log` file that was saved to your **Downloads** folder.
4. Scroll down to the `Report Summary` section at the bottom of the file, and then record the following:

HCACHE building time
Rendering time
Total time

For example:

```
HCACHE building time: 0.69s
Rendering time: 4.14s
Total time: 4.84s
```

5. Return to the FortiAnalyzer GUI, click the **Settings** tab for the report, and then enable **Enable Auto-cache**.
   The HCACHE is updated when new logs come in, and new log tables are generated.
6. Click **Apply**.
7. Run the report one more time, and then run the diagnostics again. What is the output this time?

HCACHE building time
Rendering time
Total time

   For example:

```
HCACHE building time: 0.19s
Rendering time: 3.72s
Total time: 3.91s
```

   Although your lab environment does not have a large number of logs, you should still see that by enabling auto-cache, the report builds faster. This is more noticeable if FortiAnalyzer receives higher log volumes.
8. Keep the FortiAnalyzer session open for the next exercise.

Exercise 2: Building a Custom Dataset From Scratch

Datasets are the component that queries the database for specific logs. Although FortiAnalyzer comes with many predefined datasets, in some scenarios you may need to create custom ones. In this exercise, you will build a custom dataset by manually typing the SQL query that will fetch the desired information from the database.

Create a Dataset

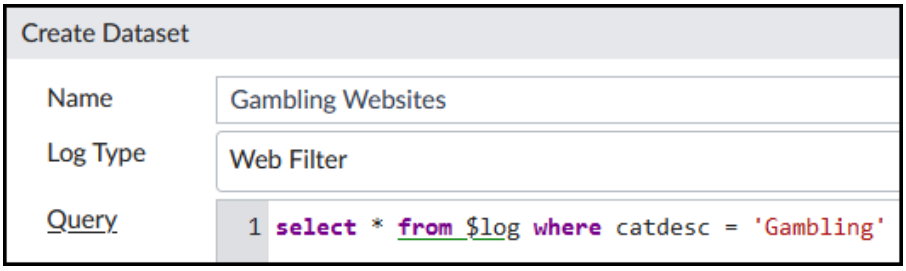
Scenario: You need to create a small dataset that fetches which sites are being visited based on their category, and then displays the source and destination IP addresses, and the URL of each site found. You will test the dataset with the category `Gambling`.

To create a dataset from scratch

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **Reports**.
4. Navigate to **Report Definitions** > **Datasets**.
5. Click **Create New**.
6. Type the following in the **Query** field:

```
select * from $log where catdesc = 'Gambling'
```

7. The result must look like the following image:



The **Web Filter** in the **Log Type** field must be for FortiGate.

Hover your mouse over the underlined **from $log** section to display all the fields (schema) available for you to use in queries for the log table.

8. Change the time period to **This Week**.
9. Click the **Go** button, and then verify that the query found some matches.

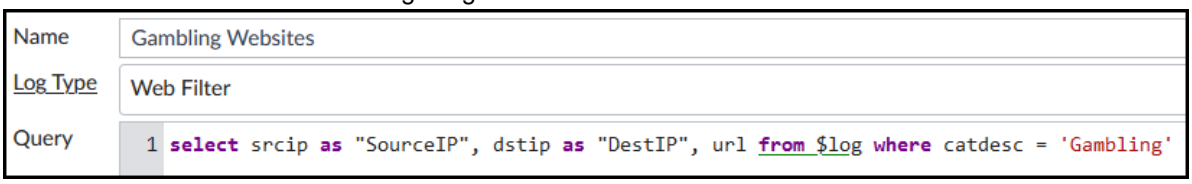
The word `Gambling` in this query is case sensitive.

Do not proceed to the next step until you find some matches.

10. Edit the query as shown below to include only the source IP address, destination IP address, and URL columns:

```
select srcip as "SourceIP", dstip as "DestIP", url from $log where catdesc =
'Gambling'
```

11. The result must look like the following image:



12. Click **Go** again, and then verify that there are some matches, and that only three columns are shown. Your results should look similar to the following image:

SourceIP	DestIP	url
10.0.1.20	51.161.21.1	http://bjmzw.net/
10.0.1.20	75.2.26.18	http://dalotto.com/
10.0.3.20	54.39.193.115	http://bjmzw.net/
10.0.1.200	54.39.193.115	http://bjmzw.net/
10.0.3.20	75.2.26.18	http://dalotto.com/
10.0.1.200	75.2.26.18	http://dalotto.com/
10.0.3.20	51.161.21.1	http://bjmzw.net/
10.0.1.200	51.161.21.1	http://bjmzw.net/
10.0.3.20	75.2.26.18	http://dalotto.com/
10.0.1.200	75.2.26.18	http://dalotto.com/

13. Click **OK** to save the custom dataset.

Stop and think!

You can easily edit this dataset for a different category.

Creating a dataset from scratch, or customizing a predefined dataset, requires some knowledge of the syntax used for SQL queries. However, FortiAnalyzer provides a much simpler method to create custom datasets. You will use this method in the next exercise.

14. Keep the FortiAnalyzer session open for the next exercise.

Exercise 3: Building a Custom Chart From Log View

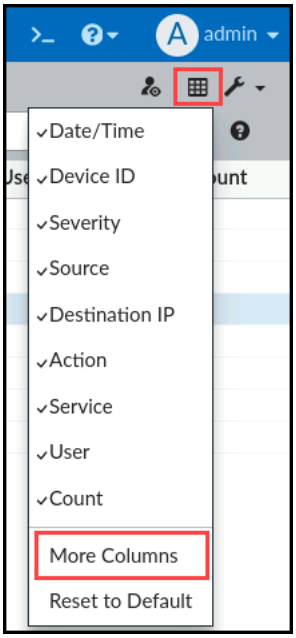
You can create custom charts that include only the information you need. The chart builder makes this process very easy. In this exercise, you will build a custom chart based on log filters. This process allows you to create a new dataset without requiring you to know the syntax used for SQL queries.

Create a Custom Chart

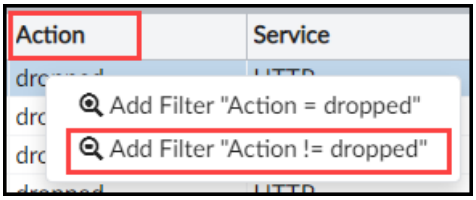
Scenario: You need to create a report for the network administration team with any IPS traffic that is not being blocked by the company's firewall. You will begin by creating a custom chart. You will include this chart in a report in the next exercise.

To create a chart based on a log search

1. In the upper-left corner, click **Reports**, and then click **Log View**.
2. In the menu on the left, navigate to **FortiGate** > **Security** > **Intrusion Prevention**.
   You may need to adjust the time filter so that it includes the traffic that you want.
3. In the upper-right, click **Column Settings** > **More Columns**.

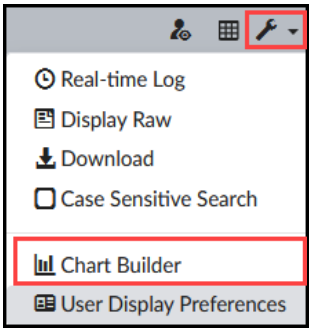


4. In **Column Settings**, find and select the column name **Attack Name**, and then click **OK**.
5. Right-click one of the entries under the **Action** column, and then select the filter to exclude dropped connections as shown in the following image:



You should see at least one entry after applying the filter. If you don't see any entries, adjust the time filter.

6. Click **Tools** > **Chart Builder**.



The dataset query is automatically generated based on your search filters. The **Preview** window indicates what the results will look like in a report.

7. Configure the following settings to fine-tune your results:

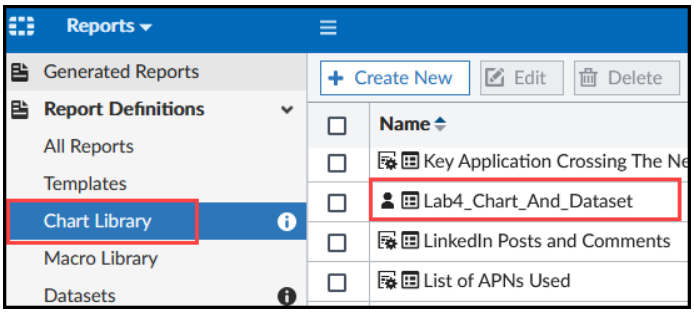
Field	Value
Name	Lab4_Chart_And_Dataset
Columns	Select: • Date/Time • Device ID • Severity • Destination IP • Attack Name The chart builder allows you to select only five columns. Cancel the selection of any other columns, if they are selected by default. This is not a limitation when building custom datasets manually.
Order By	Date/Time
Sort By	Descending
Show Limit	50

8. Click **Preview**.

The dataset query updates based on your modifications. Your query should look similar to the following image:

```
select from_itime(itime) as itime, string_agg(distinct `devid`, ' ') as devid__agg_, string_agg(distinct (`severity`)::text, ' ') as severity__agg_, string_agg(distinct ipstr(`dstip`), ' ') as dstip__agg_, string_agg(distinct `attack`, ' ') as attack__agg_ from ###(select `itime`, `devid`, `severity`, `dstip`, `attack` from $log where $filter and ( ( ( `action` IS NULL OR `action` != 'dropped'))) group by `itime`, `devid`, `severity`, `dstip`, `attack`)### t group by `itime`
```

9. Click **Save**.
10. Navigate to **Reports** > **Report Definitions** > **Chart Library**, and verify your chart are created, both with the same name.



You now have the chart that will get the desired information from the database. You will use this chart in a custom report in the next exercise.

11. Keep the session in FortiAnalyzer open for the next exercise.

Exercise 4: Building a Custom Report

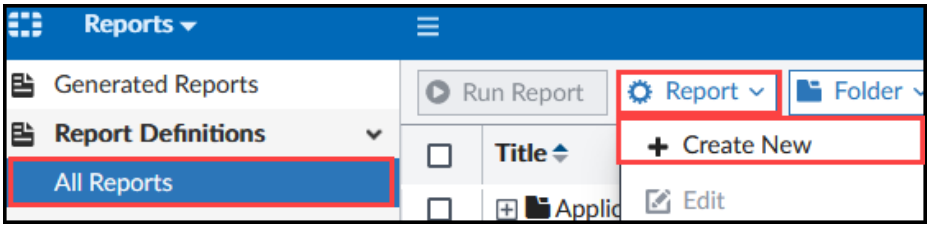
In this exercise, you will build a custom report using the chart you created.

Create and Run a Report Using a Custom Chart

Scenario: Continuing the task from the previous exercise, you will create a new report that uses the custom chart you built.

To create a report using a custom chart

1. Click **All Reports**, and then click **Report** > **Create New**.



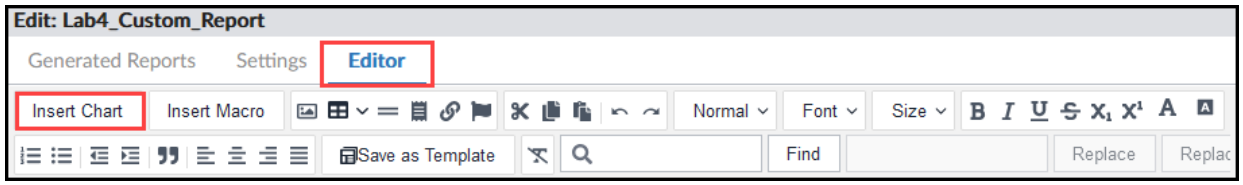
2. Configure the following settings:

Field	Value
Name	Lab4_Custom_Report
Create from	Blank

3. Click **OK**.
4. Click the **Settings** tab, and then select **Today** in the **Time Period** field.

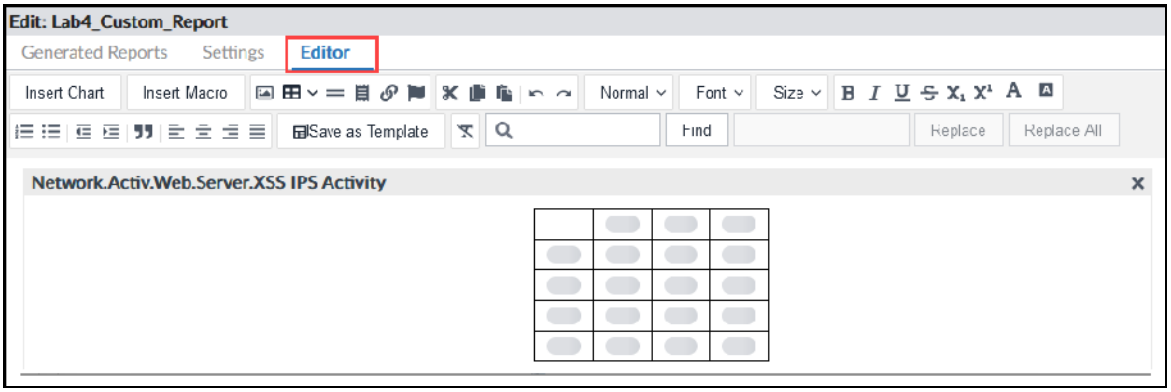
If you didn't do the previous labs the same day you are doing this one, adjust the **Time Period** accordingly to avoid a report with little or no data.

5. Click the **Editor** tab, and then click **Insert Chart**.

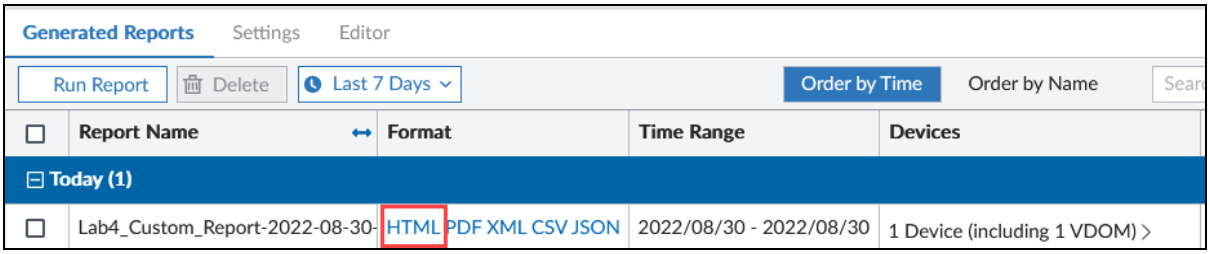


6. In the **Chart** drop-down list, select **Intrusion Prevention**.
7. In the **Click to select** box, start typing `Lab4_Chart_And_Dataset`, and then select it when it appears in the list.
8. In the **Title** box, type `IPS_Traffic_Not_Blocked_By_The_Firewall`.

9. Click **OK**.
10. Click **Apply**.



12. Click the **Generated Reports** tab, and then click **Run Report**.
13. In the **Format** column, click **HTML** to view the report in HTML format.



You have successfully created a report based on a chart and dataset created from a filtered search result. You can now send the PDF version of the report to the network administration team.

14. Keep the session in FortiAnalyzer open for the next exercise.

Exercise 5: Scheduling a Report

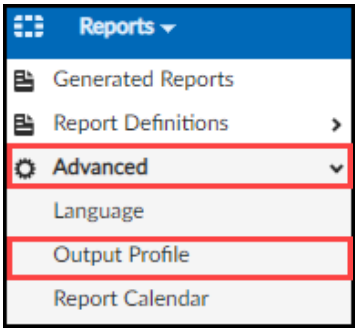
In this exercise, you will schedule a report to be generated daily, and configure it to be sent in an email using an output profile. This guarantees that the network administration team receives the information automatically at the end of each day.

Create and Configure an Output Profile

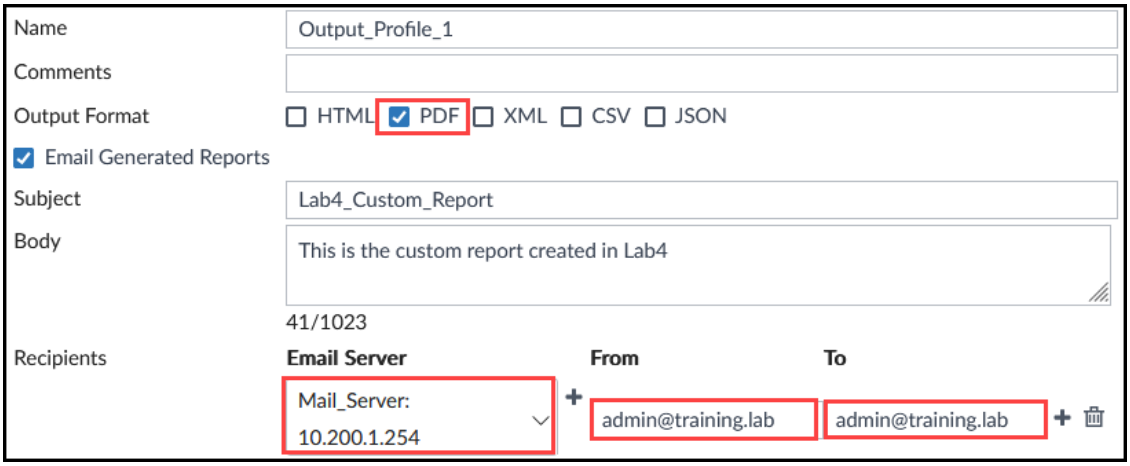
Output profiles allow you to send a copy of generated reports to other servers.

To configure an output profile

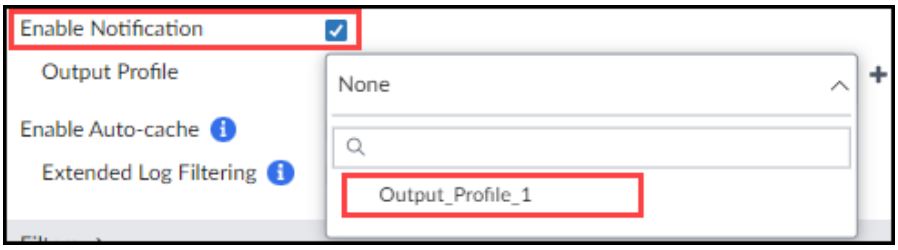
1. Navigate to **Reports** > **Advanced** > **Output Profile.**



2. Click **Create New**.
3. Complete the **Output Profile** settings as shown in the following image:



4. Click **OK**.
5. Navigate to **Report Definitions** > **All Reports**.
6. Find and double-click the report named **Lab4_Custom_Report**.
7. Click the **Settings** tab.
8. Select the **Enable Notification** checkbox.
9. Click the **Output Profile** box, and then select the profile you created in the previous steps.



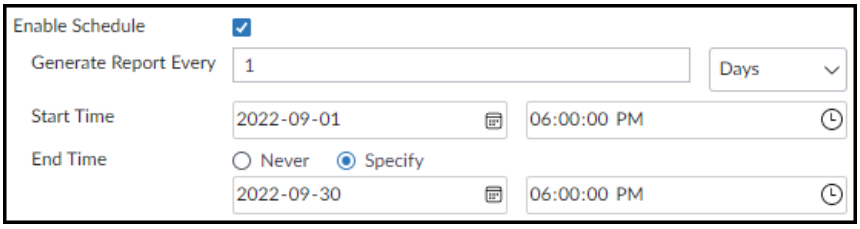
6. Click **Apply**.

Schedule Reports

When you need to generate the same report periodically, you can enable the report schedule feature.

To schedule a report

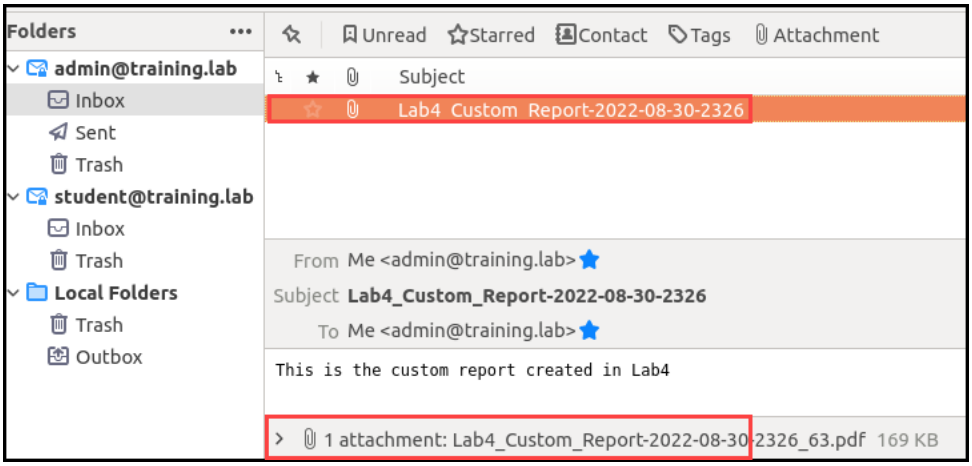
1. Select the **Enable Schedule** checkbox.
2. Configure the report to be generated every day, starting today, and to end one month after today. Adjust the start time so that the first occurrence is 5 minutes after the current time in FortiAnalyzer.
   For example, the following image shows a schedule that will run daily, starting on September 1st at 6:00 pm, and ending on September 30 at 6:00 pm.



3. Click **Apply** to save the changes.
4. In the menu on the left, click **Advanced** > **Report Calendar**, and then verify that the report is added and is **Pending** to run today.

To verify that an email was received with the report

1. Wait 5 minutes.
2. On the Local-Client VM, open Thunderbird, and then verify that it received an email with the daily report attached.



In this exercise, you used the option to send a report as an email attachment. However, if they are available, you can also upload a report to an FTP, SFTP, or SCP server.

You can select and configure the **Upload Report to Server** option in the output profile to achieve this.

3. Log out of FortiAnalyzer.

Lab 5: Playbook Management

In this lab, you will examine the use of playbooks on FortiAnalyzer. You will learn how to create, customize, and export playbooks, and then import them to a different ADOM.

Objectives

- Create simple playbooks with an on-demand trigger
- Create and customize simple playbooks with incident triggers or event triggers
- Import and customize playbooks
- Use FortiOS connectors in playbooks

Time to Complete

Estimated: 40 minutes

Exercise 1: Creating a Playbook With an On-Demand Trigger

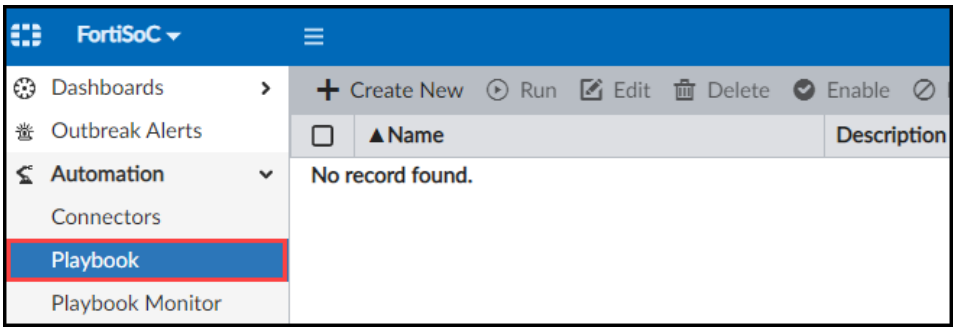
In this exercise, you will create a simple playbook that generates an incident. The playbook will use an on-demand trigger and will have only one task. You will also explore how to use the log associated with the playbook to troubleshoot its execution. Finally, you will verify that the playbook was executed successfully.

Create a New Playbook with an On-Demand Trigger

The creation of new playbooks is very simple. You will create a new playbook.

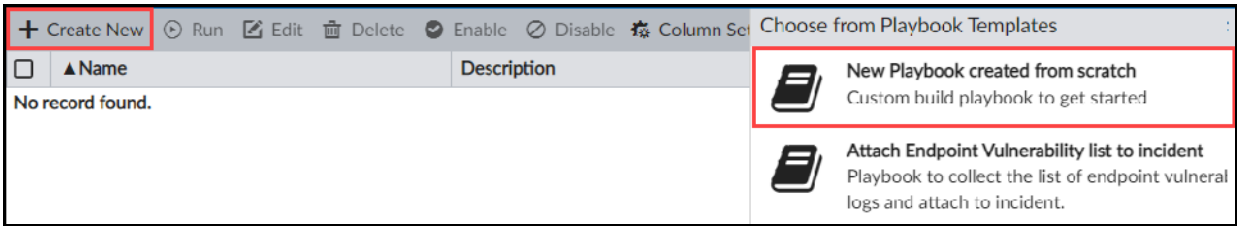
To create a new playbook from scratch

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**.
4. Click **Automation** > **Playbook**.

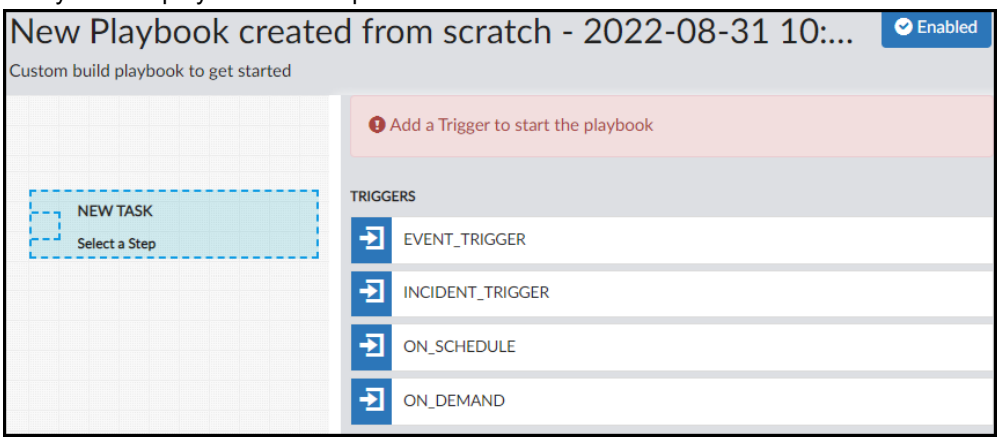


FortiAnalyzer has no default playbooks.

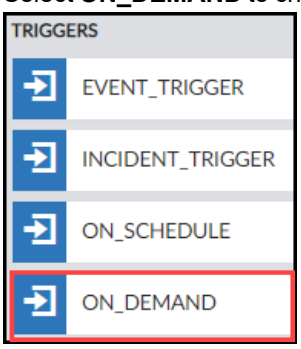
5. Click **Create New**, and then select **New Playbook created from scratch**.



6. Verify that the playbook editor opens.

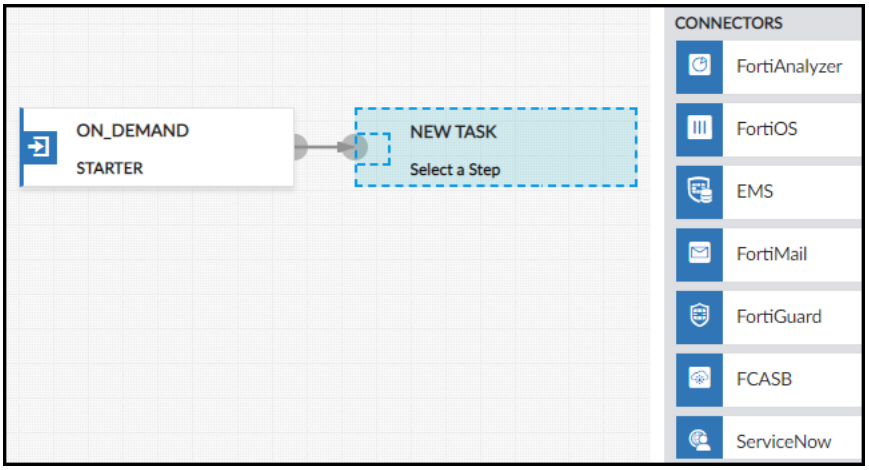


7. Select **ON_DEMAND** to choose that trigger type.

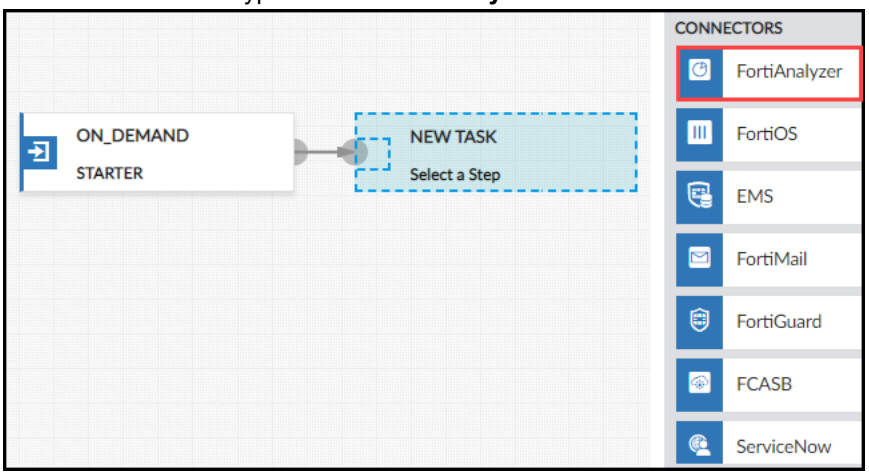


8. Verify that the playbook editor displays your choice, and then notice the hint about how to add a new task.

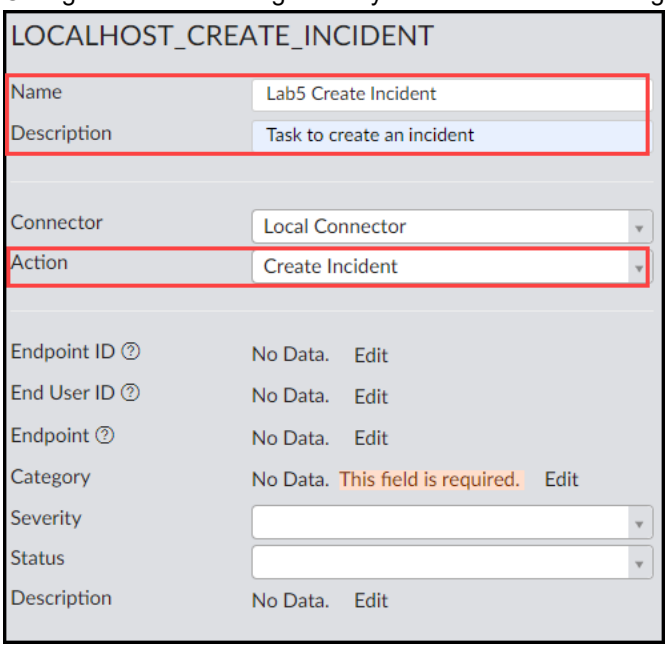
9. Drag one of the connectors to an empty area in the playbook editor.



10. Select the connector type labeled **FortiAnalyzer** for the new task.

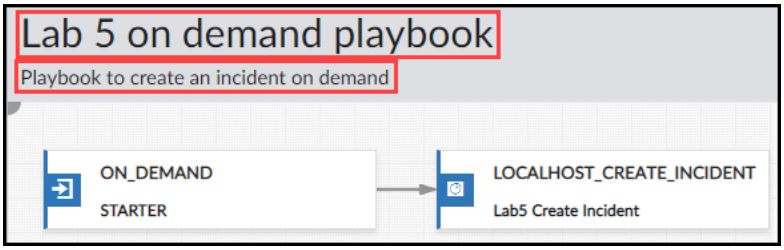


11. Configure the task settings exactly as shown in the following image:



The other fields in this task are not configured intentionally. This way, you will see the playbook fail, and then explore how you can find out why it happened.

12. Click **OK** to save the task settings and return to the playbook editor.
13. Change the name of the playbook and its description as shown in the following image:



It is important to change the default playbook name.

When you have many playbooks, using better naming conventions makes it easier to find specific playbooks.

14. Click **Save Playbook**.
15. Return to **Automation** > **Playbook**, and then verify that the new playbook is listed there.

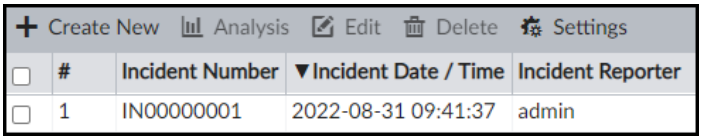
Do not try to run the playbook now because FortiAnalyzer requires some time to parse the playbook.

If you try to run the playbook before FortiAnalyzer parses it, you will receive an error like the one in the following image:

Verify the Current Number of Incidents

To verify the current number of incidents

1. Click **Incidents**, and then make a note of the number assigned to the newest incident in the list.
For example, in the following image, the newest incident is number **IN00000001**:



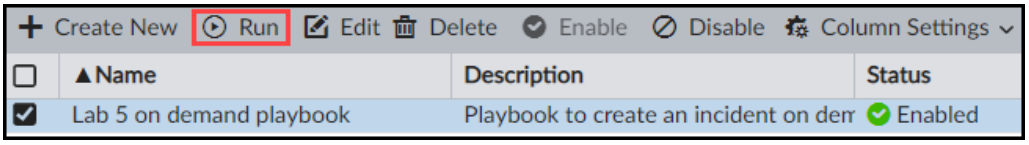
This step is included so that you can easily identify the new incidents that are created after you run the playbooks in this lab.

Run and Troubleshoot a Playbook

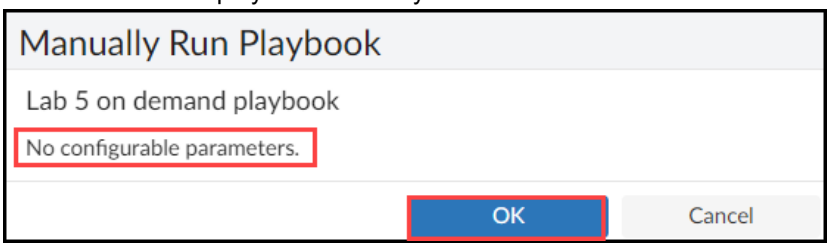
You will use the log information provided to troubleshoot a playbook that fails to run.

To run and troubleshoot a playbook

1. Return to **Automation** > **Playbook**.
2. Select the playbook you created, and then click **Run**.



3. Click **OK** to run the playbook manually.

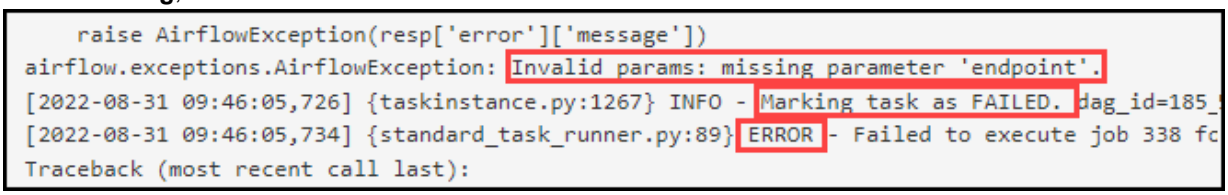


Notice that you cannot configure any parameters. This is the reason this playbook will fail, which you will verify later.

The parameters required vary depending on the type of task.

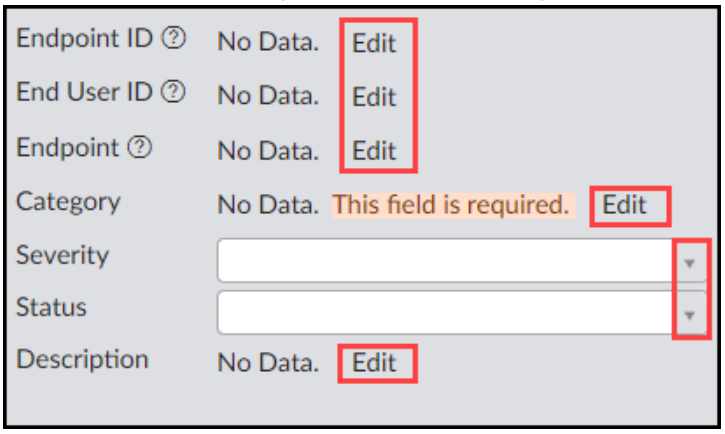
4. Click **Playbook Monitor**.
   After a few seconds, the status of the new playbook should be **Failed**.
5. Verify that the playbook failed, and then click **Details**.

6. Click **View Log**, and then look for the line that shows the reason for the failed run.

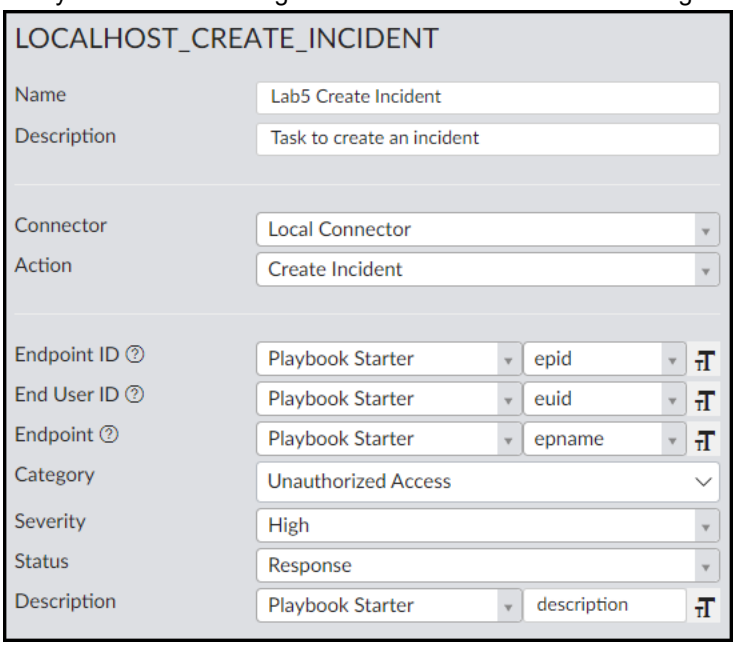


7. Click **Close** twice to return to **Playbook Monitor**.
8. Return to **Automation** > **Playbook**.
9. Double-click the playbook to open it in the editor.
10. Hover your mouse over the task, and then click the edit button.

11. Click **Edit** for each of the parameters and the drop-down menus as shown in the following image:



12. Verify that the final settings match those shown in the following image:

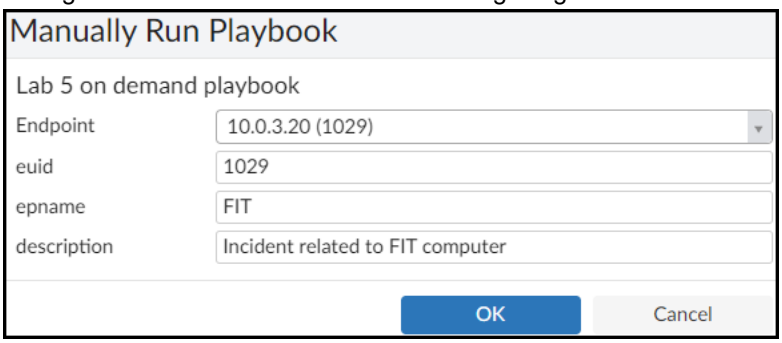


The **Playbook Starter** option used here prompts you to select or type the parameters.

This option is useful if, for example, you want to run the same playbook for different endpoints or users.

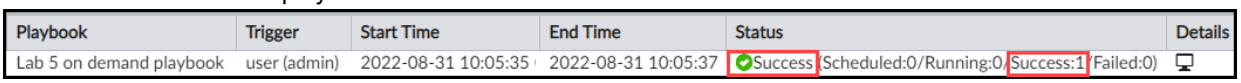
13. Click **OK** to save the changes.
14. Click **Save Playbook**.
15. Return to **Automation** > **Playbook**.
16. Click the playbook, and then run it again.
    This time you are prompted to configure some parameters.

17. Configure each field as shown in the following image:



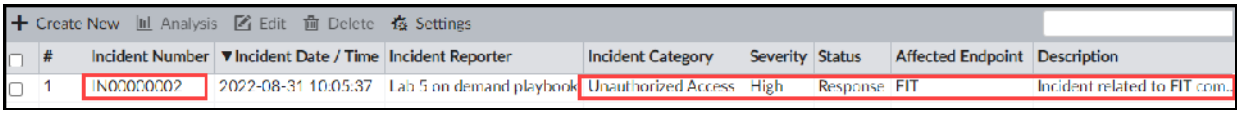
Note that the value shown in parentheses in the **Endpoint** field is the **euid**, and it may be different in your environment.

18. Click **OK**.
19. Click **Playbook Monitor**.
20. Wait until the status is displayed as **Success**.



Note the number of successful tasks, which is one in this example since this playbook only has a single task.

21. Click **Incidents**, and then verify that a new incident was created.



22. Double-click the new incident, and then verify that its settings match the settings in the playbook task.
23. Keep the FortiAnalyzer session open for the next exercise.

Exercise 2: Creating a Playbook With an Incident Trigger

In this exercise, you will create a playbook that uses an incident trigger and contains a task that updates an existing incident.

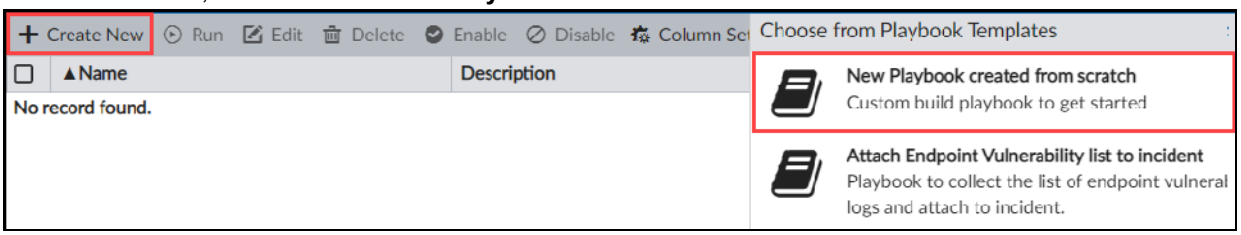
You will also explore how trigger variables are used to allow a task to use parameters provided by the trigger.

Create a Playbook with an Incident Trigger

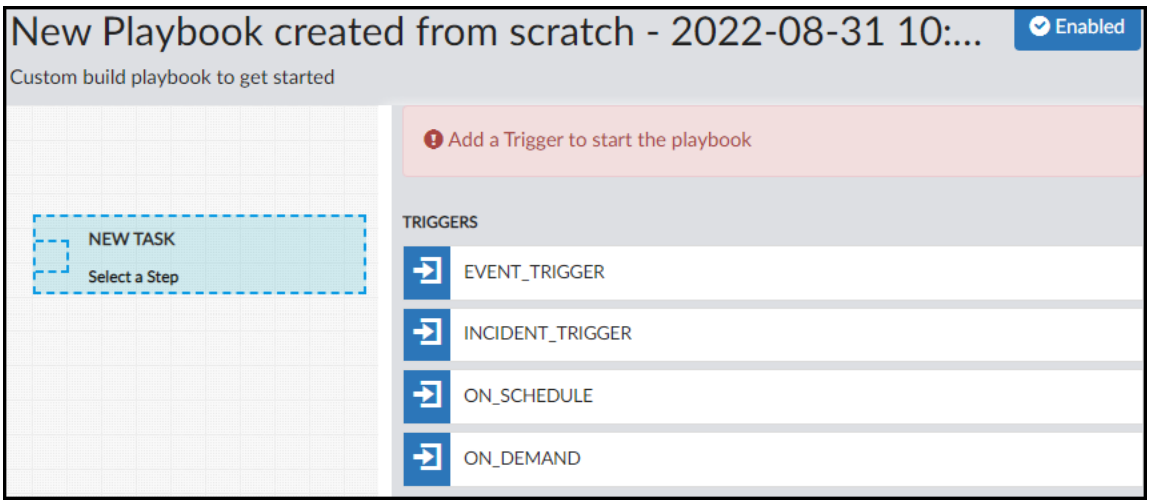
Use an incident trigger to run a playbook when FortiAnalyzer detects an incident with the specified criteria. You will create a playbook with an incident trigger.

To create a playbook with an incident trigger

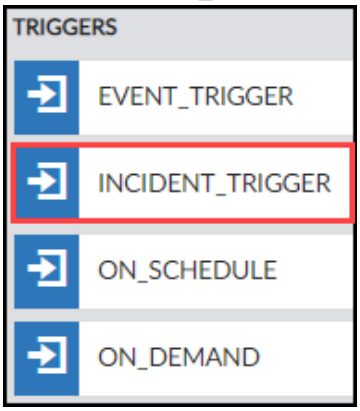
1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**.
4. Click **Automation** > **Playbook**.
5. Click **Create New**, and then select **New Playbook created from scratch**.



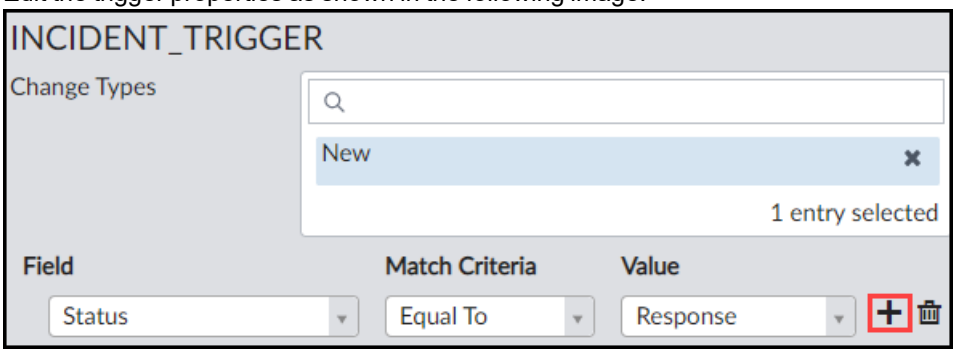
The playbook editor opens.



6. Select **INCIDENT_TRIGGER** to choose that trigger type.



7. Edit the trigger properties as shown in the following image:

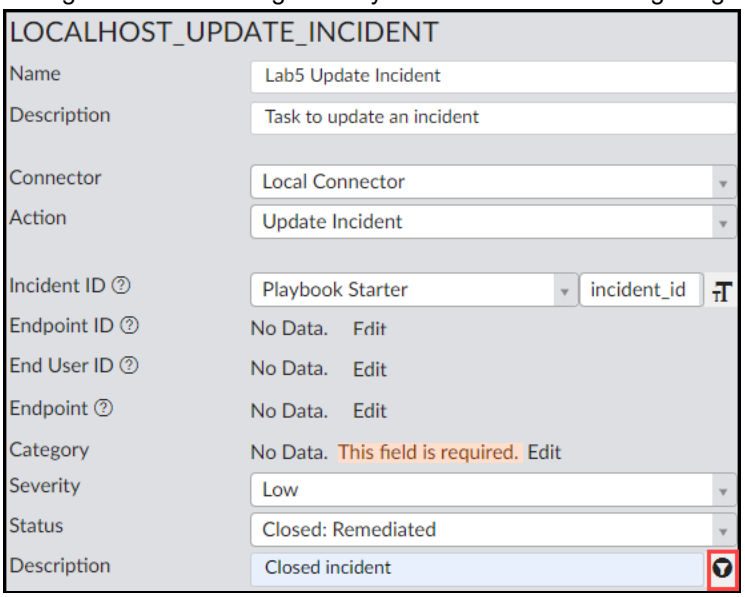


Response is the incident status that you configured for the **On_Demand** playbook in the previous exercise.

You will run that playbook again to create a new incident, and that will trigger this playbook to make some changes to the incident created by the first playbook.

8. Click **OK** to save the changes.
9. Drag one of the connectors to an empty area in the playbook editor.
10. Select the connector type labeled **FortiAnalyzer** for the new task.

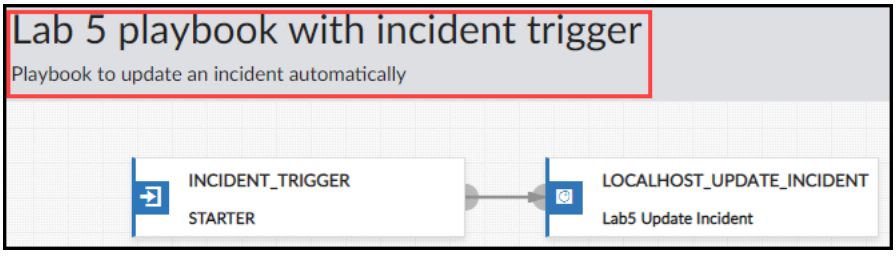
11. Configure the task settings exactly as shown in the following image:



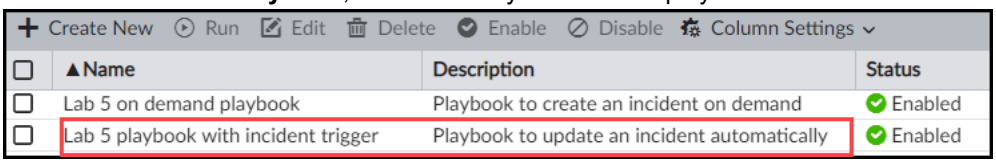
Note that to complete the **Description** field, you must click **Edit**, and then click the icon on the right to change to text mode.

> **Stop and think!**
>
> In this case, only the **Incident ID** parameter is required—the trigger provides this parameter. This means the trigger tells this task which incident must be updated using a trigger variable.
>
> Notice the changes in the bottom three fields, since they are reflected in the incident once it is updated.

12. Click **OK** to save the changes and return to the playbook editor.
13. Change the name and description of the playbook as shown in the following image:



14. Click **Save Playbook**.
15. Click **Automation** > **Playbook**, and then verify that the new playbook is listed.



16. Wait for 5 minutes to make sure FortiAnalyzer finishes the parsing process, and then continue with the next exercise.

Verify that the Playbook Runs Successfully

You will test the new playbook by running the playbook that you created in the previous exercise.

To test the execution of the playbook

1. Run the **Lab 5 on demand playbook** you created in the previous exercise.
2. Click **Playbook Monitor**.
3. Click **Refresh** every few seconds to see the progress.

Stop and think!

This time, FortiAnalyzer will execute two playbooks.

First, **Lab 5 on demand playbook** will create an incident, and then **Lab 5 playbook with incident trigger** will update that incident.

4. Verify that FortiAnalyzer successfully executed both playbooks.

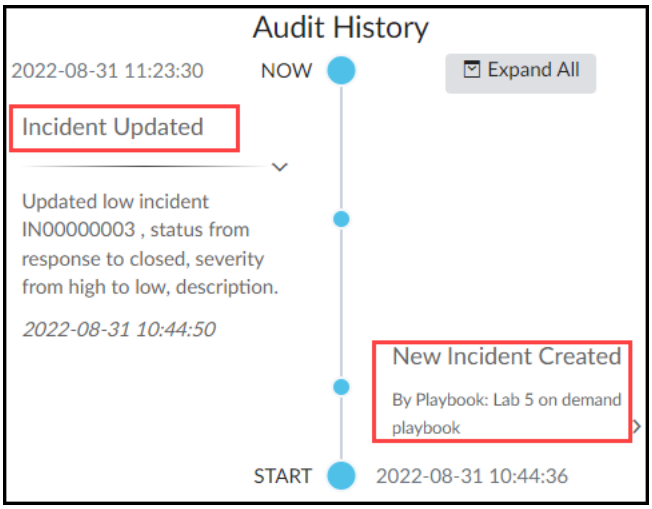
Playbook	Trigger	Start Time	End Time	Status	Details
Lab 5 playbook with incident trigger	Incident (IN00000003)	2022-08-31 10:44:48	2022-08-31 10:44:51	Success (Scheduled:0/Running:0/Success:1/Failed:0)	
Lab 5 on demand playbook	user (admin)	2022-08-31 10:44:34	2022-08-31 10:44:36	Success (Scheduled:0/Running:0/Success:1/Failed:0)	

The number shown in brackets for the second playbook refers to the incident created by the previous playbook.

5. Click **Incidents** to verify that the **Lab 5 playbook with incident trigger** added and updated the new incident.

#	Incident Number	▼Incident Date / Time	Incident Reporter	Incident Category	Severity	Status	Affected Endpoint	Description
1	IN00000003	2022-08-31 10:44:36	Lab 5 playbook with incident trigger	Unauthorized Access	Low	Closed: Remediated	FIT	Closed incident
2	IN00000002	2022-08-31 10:05:37	Lab 5 on demand playbook	Unauthorized Access	High	Response	FIT	Incident related to FIT computer
3	IN00000001	2022-08-31 09:41:37	admin	Uncategorized	Medium	New	10.0.1.200	

6. Double-click the incident to open its analysis page.
7. In the **Audit History** pane, view the incident activity.



8. Keep the FortiAnalyzer session open for the next exercise.

Exercise 3: Importing and Customizing a Playbook

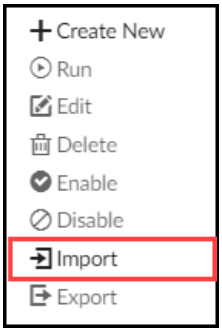
In this exercise, you will examine how to import and customize a playbook that includes multiple tasks and uses an event trigger. You will also explore how you can use output variables for one task to use the output of another task as its input.

Import and Customize a Playbook

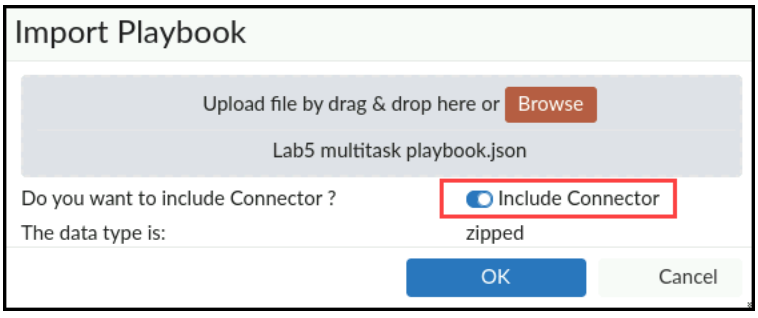
You can import a playbook created in a different ADOM or on a different FortiAnalyzer. After you import it, you can modify it to meet your needs.

To import and customize a playbook

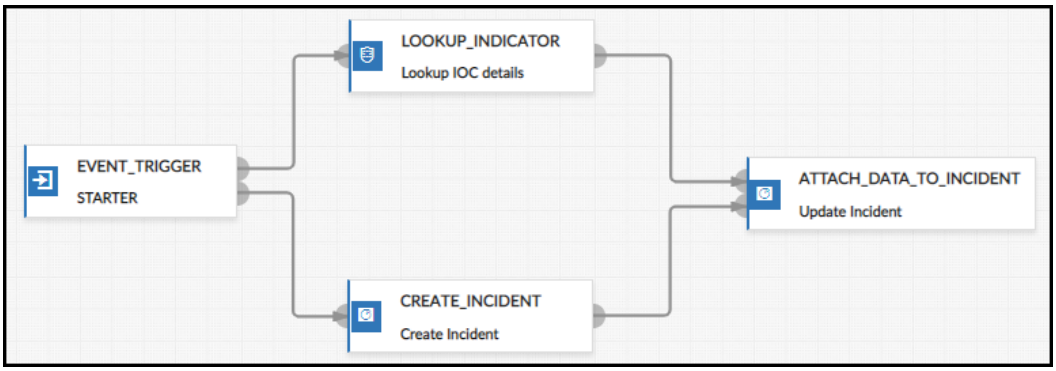
1. Continuing in **ADOM1**, navigate to **Automation** > **Playbook**.
2. Right-click an empty space in this pane, and then select **Import**.



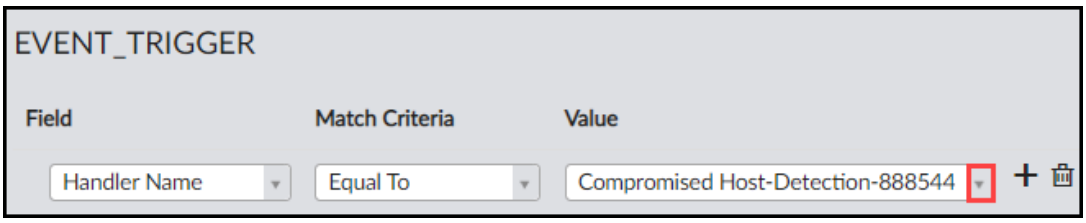
3. Click **Browse**.
4. Click **Desktop** > **Resources** > **FortiAnalyzer Analyst** > **LAB-5** > `Lab 5 multitask playbook.json`, and then click **Open**.
5. Enable the **Include Connector** option.



6. Click **OK** to import the playbook.
7. Double-click the playbook you just imported.
   It should look like the following image:



8. Open, and then examine the trigger settings.

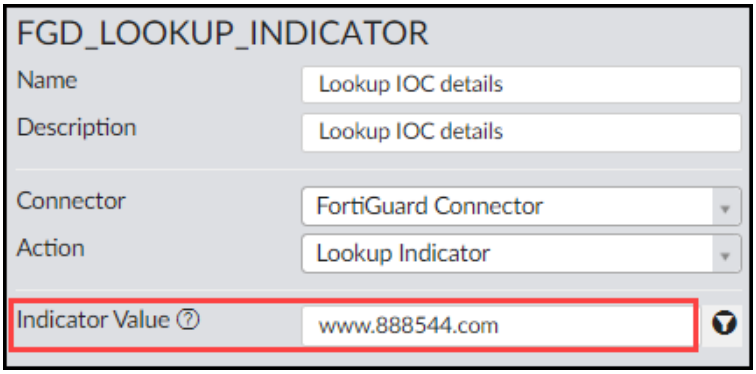


This playbook uses an **Event_Trigger** that runs when the system detects an event generated by the **Compromised Host-Detection-888544** event handler.

You created this event handler in a previous lab.

It may take a few seconds for the handler name to appear under **Value**.

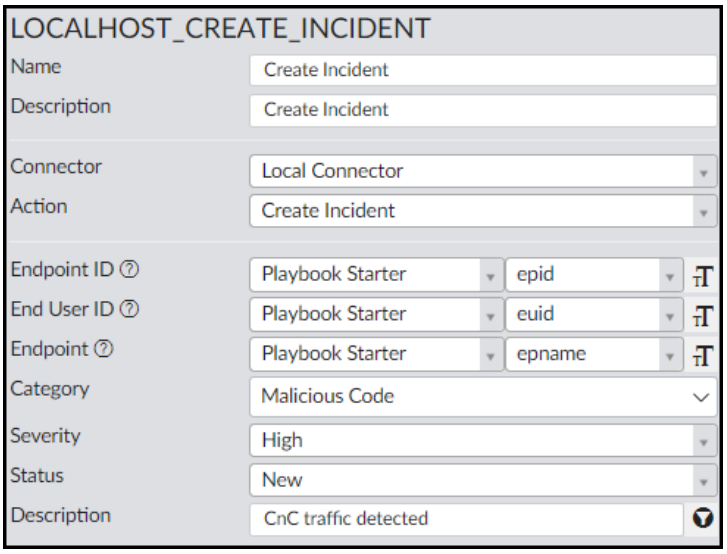
9. Click **OK**.
10. Examine the settings of the **Lookup IOC details** task.



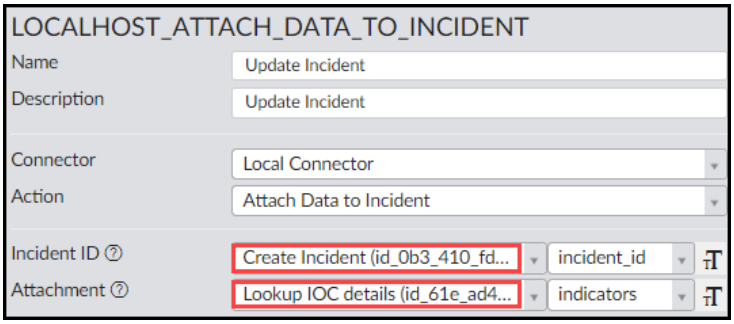
This task will look up information from FortiGuard about the indicator given by the URL **www.888544.com**.

Another task will add the information retrieved to an incident. This information will be useful to the person assigned to that incident.

11. Open the properties of the **Create Incident** task, and then verify they match the following image:



12. Click **OK**.
13. Examine the settings of the **Update Incident** task.



Stop and think!

This task adds some information to an existing incident, and uses two output variables to achieve that goal.

The incident that is updated is provided by the **Create Incident** task.

The information that is added is provided by the **Lookup IOC details** task.

14. Click **OK** to return to the playbook editor.
15. Click **Save Playbook**.
16. Wait for 5 minutes to ensure that FortiAnalyzer has enough time to parse the imported playbook.

Generate Traffic to Trigger the Playbook

You will generate some traffic to trigger the execution of the imported playbook.

To generate traffic and watch for new events

1. On the Local-Client VM, open PuTTY, and then connect to the FIT saved session (connect over SSH).
2. Log in with the username `student` and password `password`.
3. Enter the following command to run a script that changes the default route of FIT to send traffic through the ISFW FortiGate (see Network Topology on page 5):
   ```
   $ sudo ./default3
   ```
4. When prompted, enter the password again.
5. Enter the following command to check the default route:
   ```
   $ ip route
   ```
   You should see the default route through `10.0.3.254`.
6. Enter the following commands:
   ```
   # cd FIT
   # ./fit.py all --repeat
   ```
   Traffic will begin to generate, and the script will repeat each time it completes.
7. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate.
8. Click **FortiSoC** > **Event Monitor** > **All Events**.
9. Filter the view to the **Last 30 Minutes**, and then change the refresh rate to 10 seconds.

10. Verify that new events are appearing—pay close attention to the **Event** column, and look for a `www.888544.com` entry.
11. Once you see that entry, return to the PuTTY session, and then press `Ctrl+Z` to stop the script.

Verify the Successful Execution of the Playbook

After a few seconds, the traffic generated in the previous step should trigger the playbook. You will verify the execution of the playbook.

To verify the successful execution of the playbook

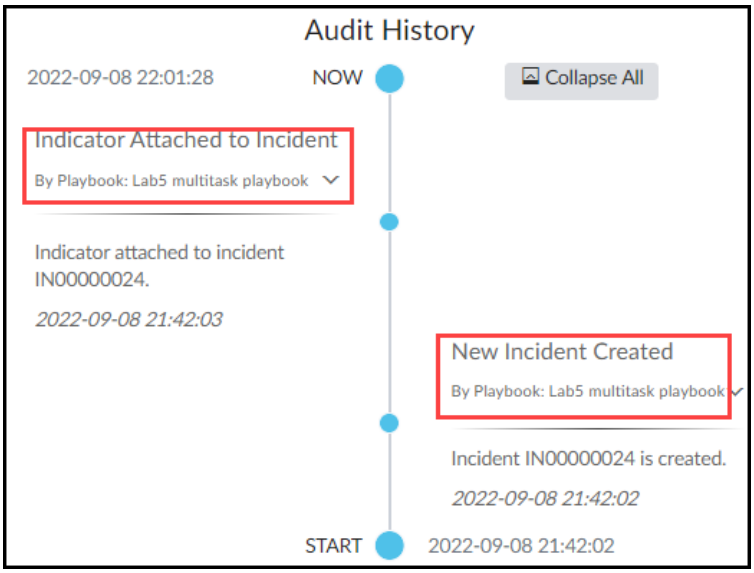
1. Return to the **Playbook Monitor**, and then verify that FortiAnalyzer successfully executed the playbook.

Playbook	Trigger	Start Time	End Time	Status	Details
Lab 5 multitask playbook	event (202209	2022-09-01 21:53:23	2022-09-01 21:53:26	Success (Scheduled:0/Running:0/Success:3/Failed:0)	

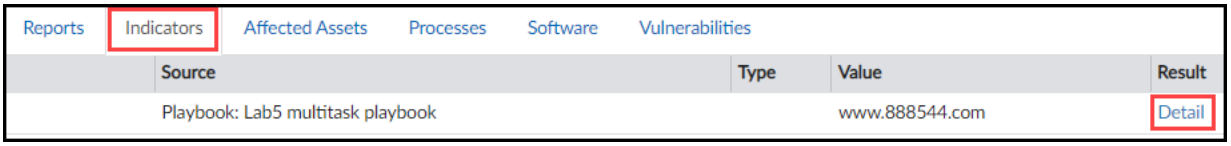
This indicates that the three tasks were successfully completed.

If at least one task fails, the playbook is considered to have failed its execution. Click **Details** to check which task failed .

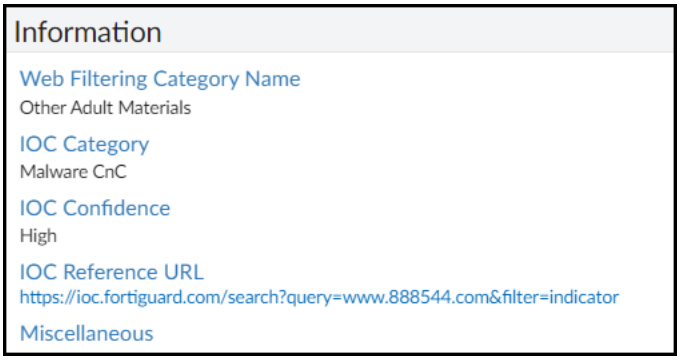
2. Click **Incidents** to verify that the playbook created a new incident.
3. Double-click the new incident to open its analysis page.
4. Examine the **Audit History** pane.
   It should look similar to the following image:



5. Continuing on the analysis page, examine the **Indicators** tab.
   You should see one entry with the name of the playbook and the value of the URL.



6. Click **Details** to see a summary of the information obtained from FortiGuard.



   Click the reference URL to view the FortiGuard website, which displays full details and statistics.
7. Keep the session in FortiAnalyzer open for the next exercise.

Exercise 4: Using FortiOS Connectors

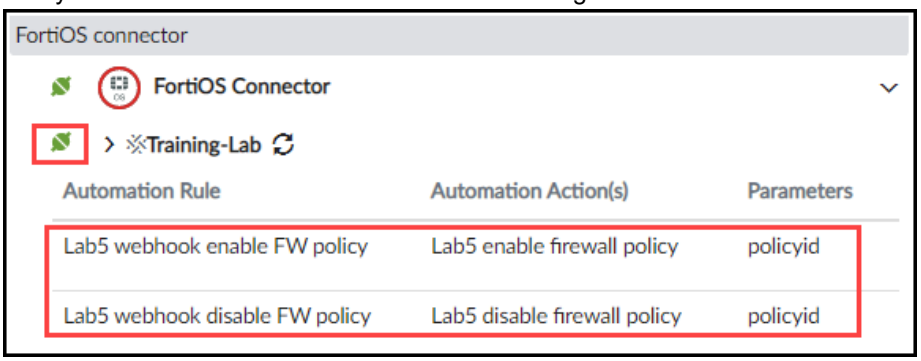
In this exercise, you will explore the use of FortiOS connectors. You will add a new task to an existing playbook. When the playbook is executed, the new task instructs FortiGate to run a simple script.

Examine the Existing FortiOS Connector

Before you start this exercise, you must verify that the FortiOS connector is ready for FortiAnalyzer to use.

To examine the availability of the FortiOS connector

1. Log in to the FortiAnalyzer GUI with the username `admin` and password `password`.
2. Click **ADOM1**.
3. Click **FortiSoC**.
4. Click **Automation** > **Connectors**.
5. Verify that the indicator for the FortiOS connector is green and shows two automation rules.



The automation rules for this exercise are preconfigured on Local-FortiGate.

Each rule consists of a CLI script that will be executed when FortiGate receives a webhook call from FortiAnalyzer during the execution of a playbook.

One script disables a firewall policy, and the other script enables it. The **policyid** parameter determines the affected policy.

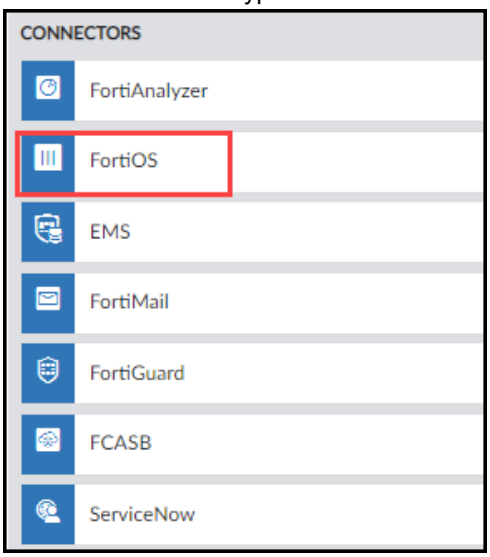
Add a Playbook Task that Disables a Firewall Policy

You will edit one of the existing playbooks to include a task that disables a firewall policy.

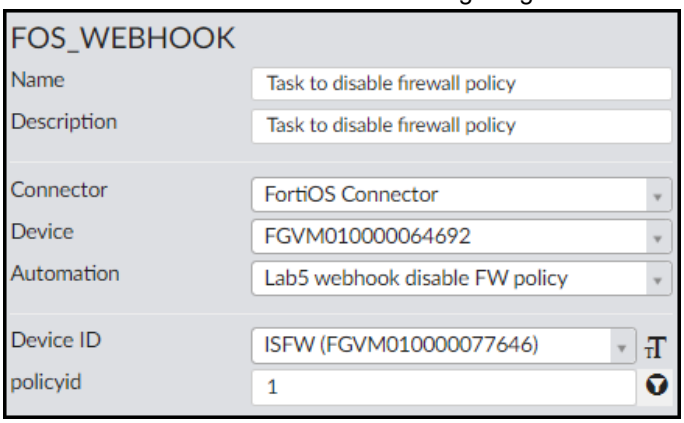
To add a new task to an existing playbook

1. Click **Automation** > **Playbook**.
2. Double-click the playbook named **Lab 5 multitask playbook** to edit its settings.
3. Drag one of the connectors in the trigger to an empty area in the playbook editor.

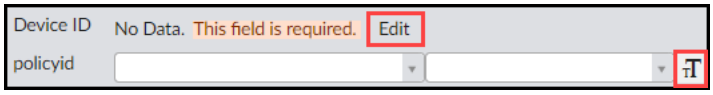
4. Select the connector type labeled **FortiOS** for the new task.



5. Edit the new task as shown in the following image:

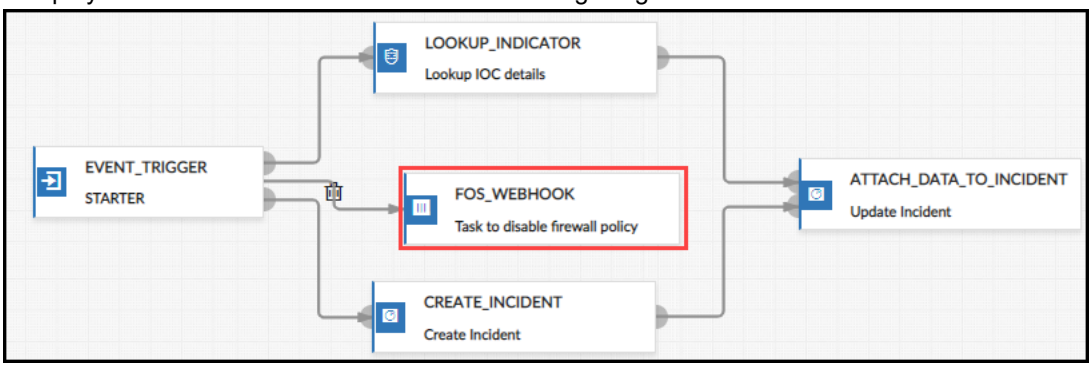


You must click **Edit** to configure the **Device ID** parameter, and then click the convert to text button to configure the **policyid**.



This task disables the **Full_Access** firewall policy on the ISFW FortiGate.

6. Click **OK**.
7. The playbook should now look similar to the following image:



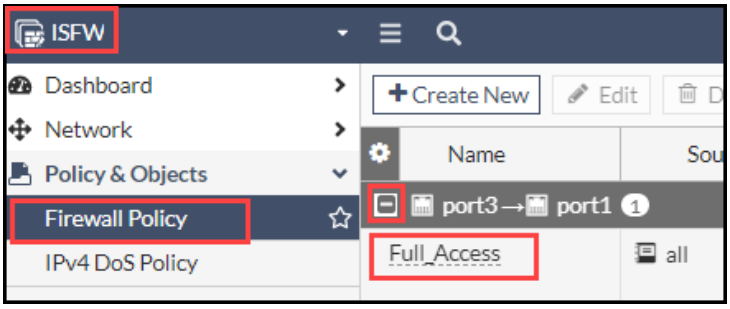
8. Click **Save Playbook**, and then click **Automation** > **Playbook**.

Verify the FortiGate Configuration Before Running the Playbook

Before proceeding to the next step, you must verify the configuration of the FortiGate that the playbook will modify.

To verify the current FortiGate configuration

1. On the Local-Client VM, open a browser, and then log in to the ISFW FortiGate GUI at `10.0.1.200` with the username `admin` and password `password`.
2. In the left panel, click **Policy & Objects**, and then click **Firewall Policy**.
3. Click **+** to expand the policies from port3 to port1, and then verify that **Full_Access** is enabled.



Generate Traffic to Trigger the Playbook

As in previous exercises, you will generate some traffic to trigger the playbook.

To generate traffic that will trigger the playbook

1. On the Local-Client VM, open PuTTY, and then connect to the FIT saved session (connect over SSH).
2. Log in with the username `student` and password `password`.
3. Enter the following command:

```
#cd FIT
#./fit.py all --repeat
```

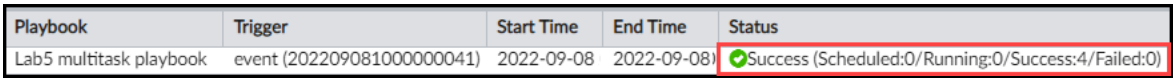
4. Leave the PuTTY session open (you can minimize it), so that traffic continues to generate.

Verify the Effect of Running the Playbook

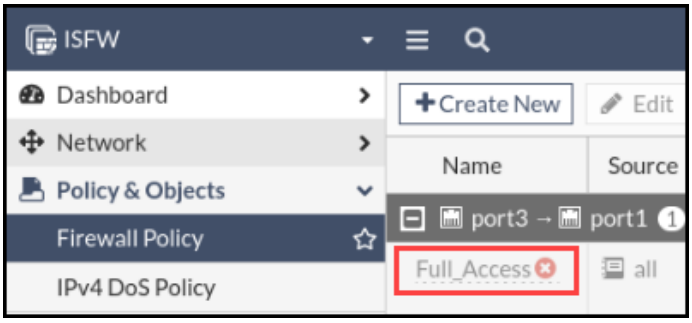
After the successful execution of the playbook, the firewall policy you examined before should now be disabled. You will verify that the firewall policy is disabled.

To verify that the playbook disabled the firewall policy

1. On FortiAnalyzer, click **Automation** > **Playbook Monitor**.
2. Wait for the playbook to run until its status changes to **Success**.



3. Return to the ISFW FortiGate GUI, and then verify that the firewall policy is disabled.



Stop and think!

You successfully configured FortiAnalyzer to instruct a FortiGate to change its configuration based on a detected event.

Although this is a very simple example, it should give you a good idea of the power of using playbooks to automate tasks.

4. Return to the PuTTY session, and then press `Ctrl+Z` to stop the script.

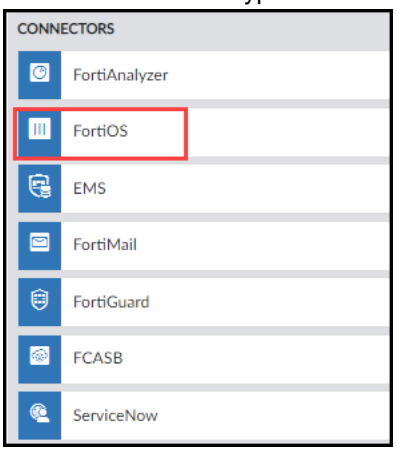
Create a Playbook to Enable a Firewall Policy

To enable the firewall policy again, you will create a new playbook to be executed on demand.

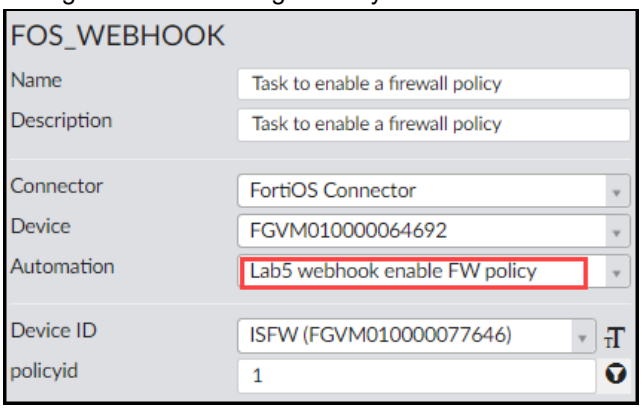
To create a playbook that enables a firewall policy

1. On FortiAnalyzer, click **Automation** > **Playbook**.
2. Click **Create New**, and then select **New Playbook created from scratch**.
3. Select **On_Demand** to choose that trigger type.
4. Drag one of the connectors to an empty area in the playbook editor.

5. Select the connector type labeled **FortiOS** for the new task.

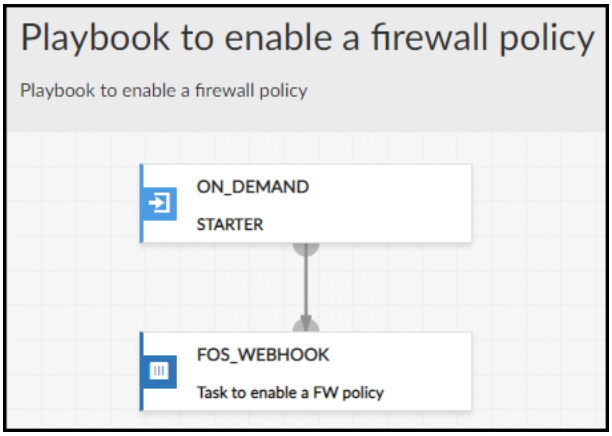


6. Configure the task settings exactly as shown in the following image:



When executed, this task enables the same policy that was disabled in the previous section.

7. Click **OK**.
8. Change the name and description of the playbook as shown in the following image:



9. Click **Save Playbook**.

Do not run the playbook immediately.

Remember, it takes about 5 minutes for FortiAnalyzer to finish parsing a new playbook.

10. Run the playbook.
11. Click **Automation** > **Playbook Monitor**.
12. Wait for the playbook to run until its status changes to **Success**.
13. Return to the ISFW FortiGate GUI, and then verify that the firewall policy is now enabled.
14. Log out of the ISFW FortiGate.
15. Keep the session in FortiAnalyzer open for the next exercise.

FORTINET