Getting Started Guide:
Fortinet Managed Rules for AWS WAF – Complete OWASP Top 10 Solution
The Fortinet Managed Rules for AWS WAF – Complete OWASP Top 10 Solution offers the following key benefits:

- Ease of use
- Compliance
- Web application protection
- Continuous updates
Step 1  Locate Fortinet Managed Rules for AWS WAF – Complete OWASP Top 10 solution in the AWS Marketplace.

Step 2  Click the Continue to Subscribe button.

Step 3  Click the Subscribe button

Steps 4-5 of 27
**Step 4**

You will then see a message that you are now subscribed. Select the **Set Up Your Account** button.

**Step 5**

You will then be taken to a page, with your marketplace subscriptions and you will see the **Fortinet Managed Rules for AWS WAF** solution listed.
After subscribing to the **Fortinet Managed Rules for AWS WAF – Complete OWASP Top 10 Solution**, please perform the following steps.

**Step 6**

Log into your AWS account console.

**Steps 7-8 of 27**
Under the Security, Identity, & Compliance column, select the **WAF & Shield** option.

Select the **Go to AWS WAF** button.
Step 9  
Next, select **Web ACLs** on the left-side.

Step 10  
Click the **Create Web ACL** button.

Step 11  
Next, enter a name for your access control list in the **Web ACL name** box. This should also populate the **CloudWatch metric name** box.

Steps 12-13 of 27
Step 12  
Next, select your **Region**. In our video demonstration, we are going to select the **Global** option, but you will want to select the Region appropriate for your organization.

**Note:** Based on the Region you select, you may see resources under that Region. You can set up your rules for those individual resources, but we will not cover that in this demonstration.

Step 13  
Click the **Next** button.

Step 14  
of 27
Step 14

On the **Create Conditions** page, scroll to the bottom and select the **Next** button.
Step 15  In the **Select a rule** box, click and then choose the **Fortinet Managed Rules** solution.

Step 16  Next, click the **Add Rule to Web ACL** button to add the solution.
Step 17. Next, we can either block or allow all incoming requests that don’t match our ACL rule set. For this demonstration, we will allow the requests.

Step 18. Click the **Review and Create** button.
Step 19  You will be given one more review screen to make any needed changes. If everything looks good, click the Confirm and Create button.

Step 20  Congratulations! You have created your first ACL.

Steps 21-24 of 27
Now, let’s pretend that we needed to make a change to our ruleset.

Select the ACL you just created.

Click the **Edit Web ACL** button on the top-right of the screen.

Under the **Rule Group Exceptions** column, you can set exceptions to the ACL. This could be used, if you notice that the traffic your organization needs is being blocked.
Step 25  Select the two arrows at the bottom-right to expand out the Rule Group Name area.

Step 26  Next, you will see a box to add a Rule Identifier. The Rule Identifier can be found in your logs for the ACL you have implemented.

Step 27  Click the Update button to save any changes.

Complete
Thank you.

For more information, visit amzn.to/2KWkmcx