A starter guide to getting FortiAnalyzer up and running on AWS

Networks are constantly evolving due to threats, organizational growth, or new regulatory/business requirements. Traditional analysis products focus on recording and identifying company-wide threats through logging, analysis, and reporting over time. FortiAnalyzer offers the features to identify these threats and provides flexibility to evolve along with your ever-changing network. FortiAnalyzer minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns.

FortiAnalyzer platforms integrate network logging, analytics, and reporting into a single system, delivering increased knowledge of security events throughout your network. The FortiAnalyzer family minimizes the effort required to monitor and maintain acceptable use policies, as well as identify attack patterns to help you fine-tune your policies.

The FortiAnalyzer is ideal for organizations of all sizes. The virtual appliances can collect, correlate, and analyze geographically and chronologically diverse security data. Aggregate alerts and log information from Fortinet appliances and third-party devices in a single location provide a simplified, consolidated view of your security posture. In addition, FortiAnalyzer platforms provide detailed data capture for forensic purposes to comply with policies regarding privacy and disclosure of information security breaches.

Why FortiAnalyzer for AWS?

Available as a VM on AWS Marketplace, the FortiAnalyzer VM is ideal for keeping track of and protecting both public cloud and hybrid deployments. It is available on AWS through the BYOL model.
1. First, create a VPC. In AWS console, go to Services -> VPC. On dashboard, select “Start VPC Wizard.”

2. Select VPC with Public and Private Subnets.

3. Create public subnet 10.0.0.0/24 and private subnet 10.0.1.0/24. Before creation, click to “Use a NAT instance instead.” VPC creation can take a few minutes to accomplish.
4. Select Subnets on the left menu and check the results of the VPC Wizard.

5. Create an EC2 instance with FortiAnalyzer. Click Services -> EC2. On dashboard, select “Launch Instance.”

6. Choose AWS Marketplace and find FortiAnalyzer.
7. Click Select. The default setting for instance size can stay unchanged.
8. Click “Configure Instance Details,” then set proper VPC and add second interface in private subnet (10.0.1.18).
Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click Launch to assign a key pair to your instance and complete the launch process.

⚠️ Improve your instance's security. Your security group, Fortinet FortiAnalyzer-VM-v5-2-2-AutogenByAWSMP-, is open to the world.
Your instance may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
You can also open additional ports in your security group to facilitate access to the application or service you’re running, e.g., HTTP (80) for web servers. Edit security groups.

⚠️ Your instance configuration is not eligible for the free usage tier
To launch an instance that’s eligible for the free usage tier, check your AMI selection, instance type, configuration options, or storage devices. Learn more about free usage tier eligibility and usage restrictions.

AMI Details
FortiAnalyzer-VM

Fortinet FortiAnalyzer-VM
AMIRx467P6B (4.2.2) Release
Root Device Type: ebs
Virtualization type: paravirtual

Hourly Software Fees: $0.00 per hour on m3.2xlarge instance
Software charges will begin once you launch this AMI and continue until you terminate the instance.

By launching this product, you will be subject to this software and agree that your use of this software is subject to the pricing terms and the seller’s End User License Agreement.

Instance Type

<table>
<thead>
<tr>
<th>Instance Type</th>
<th>vCPUs</th>
<th>Memory (GB)</th>
<th>Instance Storage (GB)</th>
<th>EBS-Optimized Available</th>
<th>Network Performance</th>
</tr>
</thead>
<tbody>
<tr>
<td>m3.2xlarge</td>
<td>256</td>
<td>30</td>
<td>2 x 80</td>
<td>Yes</td>
<td>High</td>
</tr>
</tbody>
</table>
10. Select existing key pair or create new key pair and click “Launch Instance.” When instance ID shows up, collect it for future steps.
11. Assign public IP address to interface in Public subnet. In EC2 service, click on “Elastic IPs” -> Allocate New Address -> Confirm by clicking “Yes, Allocate.” Then select new public IP and assign it to instance ID from previous step.

12. Within the AWS Console, go back to EC2 Service -> “Instances.” Search for FortiAnalyzer-VM instance. Create URL https://<Public DNS>/admin and open it in new web browser tab. Instance ID is also default password. Copy it and go to tab with login screen.

13. Log in to FortiAnalyzer using “admin” as username and the instance ID as password.
14. Click on the option to enter the license.

15. Download license from https://support.fortinet.com. After login, go to “Asset” -> “Manage Products” and select license for FortiAnalyzer VM.
16. Enter the correct IP Address as seen on the FortiAnalyzer VM (in this case, 10.0.0.18) and generate the license.

17. Click on “License File Download.” The file with the license will be saved locally.

18. Choose the selected License file from the FortiAnalyzer UI and select ok.

19. This should bring up your FortiAnalyzer and you should now be able to access and configure it.
Support

For more use cases on Fortinet products and support, please visit www.fortinet.com/aws and Fortinet cloud security solution.