FORTIWEB QUICKSTART GUIDE

A starter guide to getting FortiWeb up and running on AWS

The Fortinet FortiWeb Web Application Firewall on AWS provides the specialized, layered application threat protection for medium and large enterprises that customers have come to expect, while housed on flexible, cloud-based infrastructure on AWS with multiple pricing models to suit specific budgetary needs. Using advanced techniques to provide bidirectional protection against malicious sources, application layer DoS attacks, and sophisticated threats like SQL injection and cross-site scripting, FortiWeb platforms help you prevent identity theft, financial fraud, and denial of service. It delivers the technology you need to monitor and enforce government regulations, industry best practices, and internal policies.

Why FortiWeb for AWS?

Baseline AWS security provides a good first level of protection, but for more fine-tuned firewall control it is necessary to utilize a third-party web application firewall. FortiWeb provides enterprise-grade firewall security to protect workloads running on cloud infrastructure and communicating with outside networks, either on-premises data centers or interacting with the public Internet. FortiWeb is also available in flexible hourly, annual, or BYOL pricing models.
Here are step-by-step instructions to get FortiWeb up and running on AWS:

1. Log in to AWS and go to VPC to create new VPC.

2. Go to Subnets and create new two subnets: public and private.
Create Subnet

Use the CIDR format to specify your subnet’s IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

- Name tag: Private-FortiWeb
- VPC: vpc-b38cf0d7 (10.0.0.0/16) | FortiWebVPC
- Availability Zone: No Preference
- CIDR block: 10.0.1.0/24
3. Log in to AWS and click “Launch Instance.”
4. From the left column, select AWS Marketplace and in search label put “FortiWeb,” then select “Fortinet FortiWeb-VM (BYOL).”
5. Continue.
6. Choose an Instance Type and click Review and Launch.

7. Select Configure Instance and configure VPC and Subnets.
8. Create a new security group.


10. Click Next.
11. Click Launch.

Important information:

12. Select an existing key pair or create a new key pair and confirm check box and click Launch Instances.
13. Rename Instance.

14. Go to Elastic IPs and add Associate Address for 10.0.0.31.
15. Open VPC menu and select Route Tables. In Routes tab, add value shown below.
And in Subnet Associations, select Private subnet.

17. Open HTTPS session with public DNS address. To hostname add: https://xxxx.eu-central-1.compute.amazonaws.com
18. Log in.
   
   **Login:** admin
   **Password:** It is your Instance-ID
19. Go to Network -> Interface.
20. Go to Status and go to the Console on page shown below.

Put: execute ping 10.0.0.1

Put: execute ping 10.0.1.1
Support

For more use cases on Fortinet products and support, please visit [www.fortinet.com/aws](http://www.fortinet.com/aws) and Fortinet cloud security solution.