Introduction

The objective of this five-day consulting engagement is to design and implement a FortiGate VM next-generation firewall (NGFW) for your AWS environment and ensure your team is equipped with the knowledge to further enhance your security posture.

FortiGate VM integrates with many AWS services, such as Amazon GuardDuty, AWS Transit Gateway, and AWS Gateway Load Balancer. Fortinet experts will design an architecture to help you take advantage of these native integrations and automate network security capabilities. This will not only strengthen your defenses but also streamline your time to value.

Typical Engagement Includes:

Custom Architecture Build

Fortinet experts will design an architecture that adheres to AWS design best practices, including but not limited to:

- Compliance
- Resilience and fault tolerance
Maintaining consistent security posture across different AWS accounts
- High availability
- Scalability
- Cost optimization
- Shared security services

As part of this architecture service, multiple design options that leverage various AWS and Fortinet solutions and services will be presented with the pros and cons of each design discussed in detail. These designs could include:
- Active/Active (A/A) with AWS Load Balancer
- Active/Passive (A/P) cluster in Fortinet Cloud Security Services Hub integrated with AWS Transit Gateway
- FortiGate VM cluster integrated with AWS Gateway Load Balancer and ingress routing to inspect north-south and east-west traffic in a scalable and transparent fashion
- Hub-and-spoke design principles in AWS

The architecture can address east-west segmentation, north-south traffic inspection, as well as virtual private network (VPN) tunnel termination use cases. The architecture will be finalized based on your requirements, which will be discussed in detail during the engagement.

We will provide guidance on VM instance type/size in AWS based on the following criteria:
- Projected bandwidth/throughput requirement
- Predictability of the network traffic
- AWS enhanced networking

### Implementation

Fortinet will assist in the implementation and configuration of FortiGate VMs in AWS, including:
- Basic configuration to ensure traffic flows across the deployment.
- FortiGate HA configuration (A/P and/or A/A) in AWS Availability Zones. A/P deployment across two different zones can also be considered.
- Automation templates to deploy FortiGate VMs in A/A or A/P modes. All required infrastructure components will also be provisioned as part of these templates. You can choose one of the following automation frameworks:
  - HashiCorp Terraform
  - AWS CloudFormation
- Solution deployment in up to two regions.

### Transfer of Information (TOI)

This includes continuous knowledge transfer during the life of the project. We will train your engineers and architects on key AWS networking security concepts and security design best practices, such as:
- Advanced routing features, such as AWS Ingress Routing
- AWS Transit Gateway and Transit Gateway Connect
- AWS Load Balancer advanced concepts
- Transit VPC, AWS-native VPN services, and Fortinet Cloud Security Services Hub
- AWS Gateway Load Balancer and its integration with FortiGate NGFW using GENEVE encapsulation
FortiGate VM in AWS with focus on AWS-specific configurations, bootstrapping leveraging user data, and metadata server
Fortinet Fabric Connector for AWS; how to design security policies based on tags/metadata (cloud dynamic address objects) instead of ephemeral IP addresses

Documentation

We will provide you with detailed design/architecture document(s) that covers all aspects of the proposed solution in your AWS environment, including:

- Design diagrams
- Deployment guide that outlines steps necessary to deploy all components of the solution