AWS Networking

https://campus.barracuda.com/doc/96025973/

For your firewall VM to be integrated into the AWS network, you must configure routing and other AWS networking features.

AWS Enhanced Networking

Firewalls running on AWS instances with enhanced networking support must enable this feature when updating the firmware to version 6.2.0 or higher. Firewall VMs deployed using the 6.2.0 (or higher) HVM image from the marketplace do not need to enable enhanced networking; it is automatically enabled if the instance supports enhanced networking.

For more information, see How to Enable Enhanced Networking in AWS.

Elastic Load Balancer

The Elastic Load Balancer (ELB) is a managed layer 4 load balancer used to distribute traffic to all healthy instances associated with the ELB. The ELB can be deployed as a public-facing load balancer or internally in your VPC. The load balancer continuously checks the health of the instances and takes unhealthy instances out of rotation.

For more information, see How to Configure an AWS Elastic Load Balancer for CloudGen Firewalls in AWS.

Route 53

Use Route 53 if you are using UDP-based services or need to load balance multiple deployments in different regions. Routing policies allow you to define how traffic is distributed and which IP address is returned for a particular record set. Each record set can be associated with a heath check to ensure that only healthy instances are used.

For more information, see How to Configure Route 53 for CloudGen Firewalls in AWS.

Additional Elastic Network Interfaces

By default, the firewall is deployed with one network interface. In some cases, such as if you want to

deploy a segmentation firewall, more than one network interface is needed. The network interface must be attached to the AWS instance and then added to the firewall configuration.

For more information, see How to Add AWS Elastic Network Interfaces to a Firewall Instance.

AWS Route Tables for Multi-NIC Firewalls

When using multiple network interfaces, you must add AWS route tables for each private subnet. The default route is then changed to send all traffic, except the internal VPC traffic, over the network interface.

For more information, see How to Configure AWS Route Tables for Firewalls with Multiple Network Interfaces.

IPv6 for CloudGen Firewalls in AWS

AWS supports IPv6 in selected regions for EC2 instances running in VPCs. IPv6 must be enabled for the VPC, the subnets, and the ENI attached to the firewall instance. The firewall can then retrieve the IPv6 IP address via SLAAC and DHCPv6 from AWS.

For more information, see How to Configure IPv6 for CloudGen Firewalls in AWS.

Multiple IP Addresses on a Network Interface in AWS

Depending on the instance type you can add additional private IP addresses to the ENI network interface of your firewall. Associate the private IPs with Elastic IP addresses to use multiple public IP addresses.

For more information, see How to Add Multiple IP Addresses to a Firewall in AWS.