
AWS Networking

<https://campus.barracuda.com/doc/49743134/>

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 F-Series 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 health check to ensure that only healthy instances are used.

For more information, see [How to Configure Route 53 for F-Series 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](#).

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.