Palo Alto Networks AWS Autoscale Documentation

Release 2.0

Palo Alto Networks

Jul 22, 2021

Contents:

CHAPTER 1

Palo Alto Networks Lambda Functions for ELB AutoScale Deployment

The Lambda Functions implemented and published by Palo Alto Networks are meant to work in conjunction with the ELB Auto Scaling Deployment on AWS.

At a high level, the goal of the lambda functions is to perform the initial setup and the plumbing necessary to allow traffic from the internet (untrust subnet) to the backend web tier (trust subnet) via the Palo Alto Networks Next Generation Firewall. The policies on the PAN NGFW determine the traffic that will be permitted to pass between the untrust and trust subnets. Additionally, the lambda functions also handle the various actions required when various events, such as autoscaling, occur which require the manipulation of the firewalls.

1.1 Use Cases

1. Deploy Palo Alto Networks Next Generation Firewall in an auto scale configuration to handle unpredictable traffic patterns (spikes etc).
2. Deploy best practice architectures to secure multi-tier applications on AWS with Palo Alto Networks Next Generation Firewalls.

1.2 AWS Specific Deployment Options

1. Palo Alto supports the ELB architecture to be deployed with NAT Gateways fronting back end infrastructure. The advantage of this configuration is to not require publicly routable IP addresses for various instances in the absence of the NAT gateway.

1.3 Lambda function objectives

- Deploy ASG's and Bootstrap the Firewalls.
- Deploy Lambda Functions to monitor the private or public IPs on the NLB.

- Program the NAT rules on the PAN FW
- Handle Auto Scale Events and take the necessary actions.
- Handle the de-licensing of Firewalls when they are deleted.
- Handle de-registration of Firewalls from Panorama if Panorama is used.

1.4 Theory of Operation

There are 3 main lambda functions that get deployed:

- init
- fw_init
- sched_evt1

The two lambda functions that get deployed by the CFT are the first two listed above.

Init Lambda Function

> The InitLambda lambda function is responsible for the following functions: - deployment and configuration of the `sched_evt1` lambda function - handling creation, update and delete of the cloud formation template - validating the AMI-ID's of the PAN FW specified by the user
>
> When the init lambda function is triggered it validates that the AMI-ID of the PAN FW is valid and then proceeds to deploy the `sched_evt1` lambda function with all the required parameters. It should also be noted that the `sched_evt1` lambda function is configured to be triggered every minute. The rationale for the frequency is provided in the next section.

Sched_evt1 Lambda Function

> The primary objective of this lambda function is to read messages of NLB IP addresses published by NLB template, and for each and every IP address added ensure that there is a corresponding NAT rule configured on all firewall instances deployed. Conversely, for each and every IP address removed due to the removal of NLB, the lambda function will delete the NAT rule from all firewall instances.

Fw_init Lambda Function

> The `fw_init` lambda function gets invoked by a life-cycle hook trigger. The lambda function gets triggered when an instance in an ASG either launches or terminates. When handling an instance launch life-cycle hook action, the lambda function creates and attaches ENI's for the management and trust subnets.

1.5 Availability Zones

The ELB Autoscale Deployments require two availability zones to be deployed into. Consequently, the lambda functions will spin up two auto scale groups in the specified availability zones.

1.6 Auto Scaling Parameters

Autoscaling on AWS occurs by defining and advertising the parameters that will be used by the AWS framework to make auto scaling decisions. The parameters currently defined are:

- DataPlaneCPUUtilizationPct

- panSessionActive
- panSessionUtilization
- panSessionSslProxyUtilization
- panGPGatewayUtilizationPct
- panGPGWUtilizationActiveTunnels
- DataPlanePacketBufferUtilization

The AWS requires users to specify a `high` threshold and a `low` threshold for each parameters. When one of the parameters breaches the high threshold mark, a scale out event is triggered. Consequently, when one of the parameters breaches the low threshold mark, a scale in event is triggered.

1.7 Panorama

The use of a Panorama is optional along with the autoscaling deployment. However, it is possible to associate a firewall with the Panorama. Panorama configuration parameters such as the IP among others can be specified in the `init-cfg` file.

1.8 Logging

The logs from the lambda functions are available as Cloud Watch Logs. Log groups are created on cloud watch, which are prepended with the stack name. Debug logging can be enabled through template parameter when creating stack or updating stack.

1.9 Inputs to the Lambda Functions

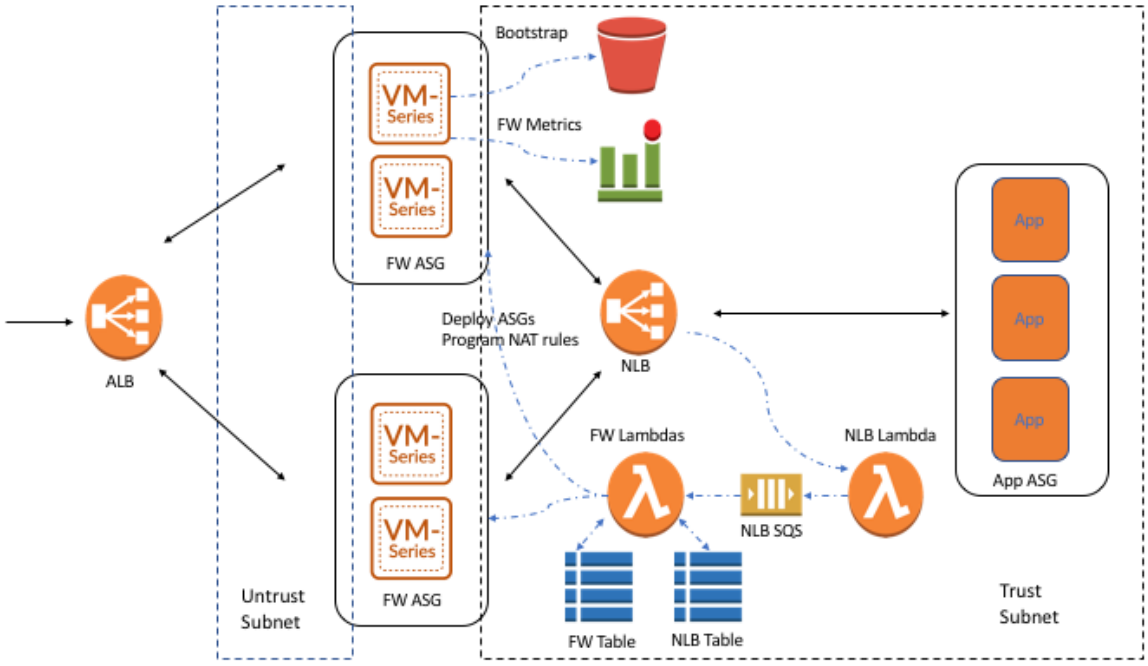
Identify the various deployment artifacts such as:

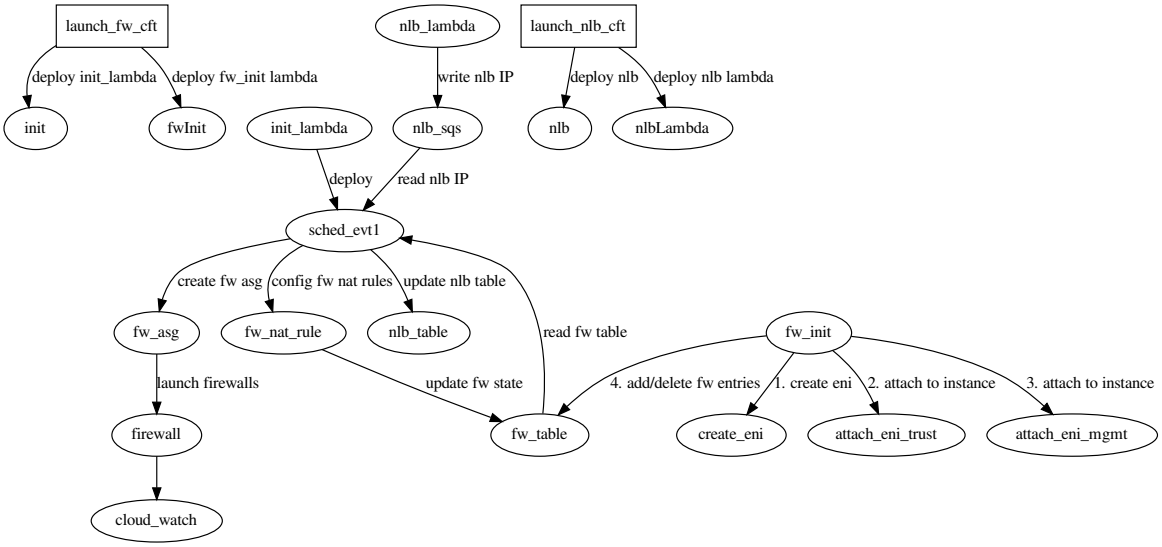
- "ServiceToken"
- "StackName"
- "Region"
- "VpcId"
- "SubnetIDMgmt"
- "SubnetIDUntrust"
- "SubnetIDTrust"
- "MgmtSecurityGroup"
- "UntrustSecurityGroup"
- "TrustSecurityGroup"
- "VPCSecurityGroup"
- "KeyName"
- "ELBName"
- "ELBTargetGroupName"

- "FWInstanceType"
- "SSHLocation"
- "MinInstancesASG"
- "MaximumInstancesASG"
- "ScaleUpThreshold"
- "ScaleDownThreshold"
- "ScalingParameter"
- "ScalingPeriod"
- "ImageID"
- "LambdaENISNSTopic"
- "FirewallBootstrapRole"
- "LambdaExecutionRole"
- "ASGNotifierRole"
- "ASGNotifierRolePolicy"
- "BootstrapS3Bucket"
- "LambdaS3Bucket"
- "PanS3KeyTpl"
- "KeyPANWFirewall"
- "KeyPANWPanorama"
- "SubnetIDNATGW"
- "SubnetIDLambda"
- "FwInit"
- "InitLambda"
- "KeyDeLicense"
- "LambdaENIQueue"
- "Debug"
- "NetworkLoadBalancerQueue"

CHAPTER 2

Architecture of the Palo Alto CFT Lambda Functions




launch_fw_cft
nlb_lambda
launch_nlb_cft
deploy init_lambda
deploy fw_init lambda
write nlb IP
deploy nlb
deploy nlb lambda
init
fwInit
init_lambda
nlb_sqs
nlb
nlbLambda
deploy
read nlb IP
sched_evt1
create fw asg
config fw nat rules
update nlb table
read fw table
fw_asg
fw_nat_rule
nlb_table
fw_init
launch firewalls
update fw state
4. add/delete fw entries
1. create eni
2. attach to instance
3. attach to instance
firewall
fw_table
create_eni
attach_eni_trust
attach_eni_mgmt
cloud_watch

CHAPTER 3

Indices and tables

- genindex
- modindex
- search