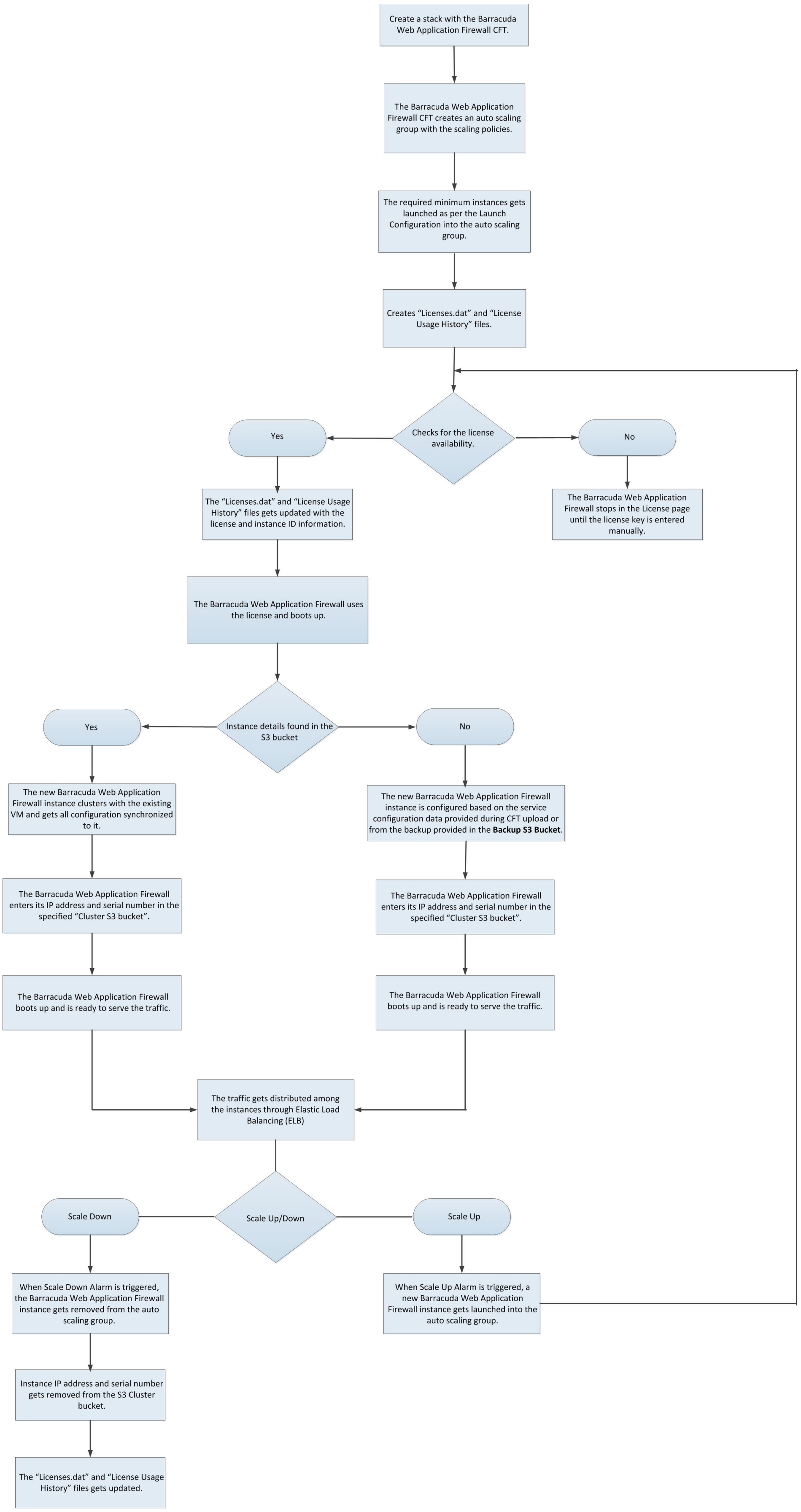
How the Barracuda CloudFormation Template Works in Bring-Your-Own-License (BYOL) instance

https://campus.barracuda.com/doc/73007167/

The following flowchart explains how the Barracuda CloudFormation Template works:


Create a stack with the Barracuda Web Application Firewall CFT.
The Barracuda Web Application Firewall CFT creates an auto scaling group with the scaling policies.
The required minimum instances gets launched as per the Launch Configuration into the auto scaling group.
Creates "Licenses.dat" and "License Usage History" files.
Checks for the license availability.
Yes
No
The "Licenses.dat" and "License Usage History" files gets updated with the license and instance ID information.
The Barracuda Web Application Firewall stops in the License page until the license key is entered manually.
The Barracuda Web Application Firewall uses the license and boots up.
Instance details found in the S3 bucket
Yes
No
The new Barracuda Web Application Firewall instance clusters with the existing VM and gets all configuration synchronized to it.
The new Barracuda Web Application Firewall instance is configured based on the service configuration data provided during CFT upload or from the backup provided in the Backup S3 Bucket.
The Barracuda Web Application Firewall enters its IP address and serial number in the specified "Cluster S3 bucket".
The Barracuda Web Application Firewall enters its IP address and serial number in the specified "Cluster S3 bucket".
The Barracuda Web Application Firewall boots up and is ready to serve the traffic.
The Barracuda Web Application Firewall boots up and is ready to serve the traffic.
The traffic gets distributed among the instances through Elastic Load Balancing (ELB)
Scale Down
Scale Up/Down
Scale Up
When Scale Down Alarm is triggered, the Barracuda Web Application Firewall instance gets removed from the auto scaling group.
When Scale Up Alarm is triggered, a new Barracuda Web Application Firewall instance gets launched into the auto scaling group.
Instance IP address and serial number gets removed from the S3 Cluster bucket.
The "Licenses.dat" and "License Usage History" files gets updated.

With regard to the flowchart, the following steps describe how a Barracuda CloudFormation Template works:

1. A CloudFormation Template (CFT) is uploaded and a stack is created on Amazon Web Services. With this:
2. The Barracuda Web Application Firewall instance(s) will be deployed and provisioned in the Virtual Private Cloud (VPC) specified while creating the stack.
3. Creates “License.dat” and “License Usage History” files.
4. After the Barracuda Web Application Firewall VM(s) is/are up and ready to serve the traffic:
5. It checks for license availability,
    1. If the license file is available with unused licenses:
        1. The “License.dat” and “License Usage History” files gets updated with the license and instance ID information.
        2. The instance uses an unused license key and boots up.
    2. It checks the **Cluster S3 bucket** for any other existing VM(s) in this Auto Scaling group.
        1. If there is no VM data available in the Cluster S3 bucket, the VM is configured based on the service configuration data provided during CFT upload or from the backup file provided as the input in the CFT.
        2. If there is an existing Barracuda Web Application Firewall instance information available in the Cluster S3 bucket, the new instance clusters with the existing instance and gets all configuration synchronized to it.
    3. Adds its information to the Cluster S3 bucket specified while creating the stack. The Cluster S3 bucket stores instance data, serial number and primary IP address (i.e., WAN IP address) of the deployed Barracuda Web Application Firewall instance(s).
    4. The Barracuda Web Application Firewall is now ready to serve the traffic to the configured services.
    5. If the instance encounters high traffic flow and triggers any of the created alarms, such as high bandwidth utilization, CPU usage, etc., then:
        1. A new Barracuda Web Application Firewall instance gets initiated automatically.
        2. Looks at the Cluster S3 bucket created in step 1 (a) and clusters with it.
        3. Adds its information to the Cluster S3 bucket, and is ready to serve the traffic.
        4. Traffic gets distributed among the instances through ELB.
6. If the license file or unused license keys are not available, the Barracuda Web Application Firewall for AWS stops in the license page until the key is manually entered.
7. If the traffic flow returns to normal, the **Scale Down** alarm is triggered.
    1. The added Barracuda Web Application Firewall instance gets removed from the auto scaling group.
    2. Instance IP address and serial number details gets removed from the Cluster S3 bucket.
    3. The License.dat and License Usage History files gets updated.

Next Step

Continue with the Importing the Barracuda Web Application Firewall BYOL CFT and Deploying the Instance article to import the CFT and deploy the instance.

Figures