Barracuda®

Solution Brief

Accelerate the Deployment of Application Security on Amazon Web Services

Key Benefits

1. Consistently deploy AWS security best practices
2. Automate web application security with Puppet and Barracuda CloudGen WAF
3. Maintain continuous compliance with Barracuda CloudGen WAF and Puppet

Businesses must be able to innovate rapidly to remain competitive. This makes it important to accelerate the application lifecycle and increase the frequency of new features and new applications. DevOps automation tools including Puppet, and AWS services like Cloud Formation Templates help organizations implement agile development practices. Provisioning security services for applications typically lags compute resource provisioning, causing longer application deployment cycles.

Barracuda, Puppet and AWS have worked together to provide an end-to-end solution that enables organizations to accelerate the secure deployment of web applications. This is done by enabling the automation of various stages of the software development process such as builds, testing and deployment while introducing application security at each level with the Barracuda Application Security suite for ensuring complete protection. These solutions provide organizations with everything needed to automatically deploy application-level security into an AWS well-architected framework.

Barracuda and Puppet on AWS

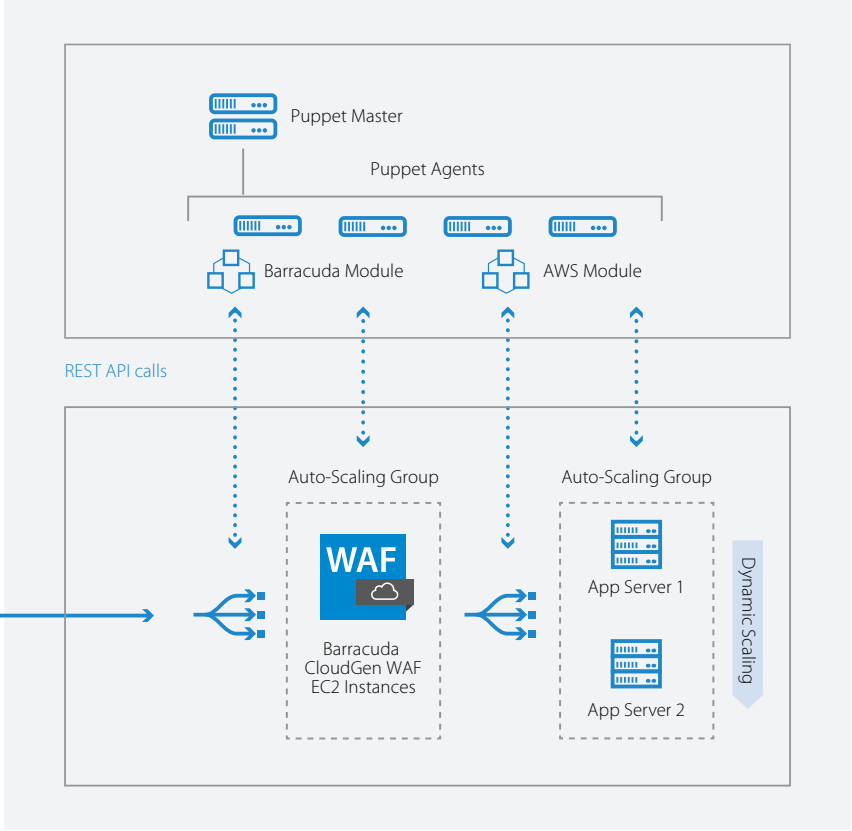
Puppet provides a configuration automation software suite that can be used to provision and configure AWS resources. This capability can be used to orchestrate well-architected deployments. Barracuda CloudGen WAF augments this by providing the application security protection for the deployment by enabling the configuration of the application security controls through its REST API framework. The puppet ecosystem can be used to configure Barracuda CloudGen WAF instances through the Puppet DSL (Domain Specific Language) using a Puppet module designed by Barracuda Networks.

Here's How It Works

Provisioning and configuration tasks are written using Puppet DSL and saved as Puppet manifest files on the Puppet Master. The manifest files are created in accordance with the Puppet modules that are imported into the Puppet Master for the intended configuration tasks.

A purpose-built Barracuda CloudGen WAF Puppet module that supports the REST API endpoints would be one such module on the Puppet Master. When the agent connects to the Master, it sends its system information as "facts" based on which the Puppet master compiles and sends a JSON construct called a catalog to the agent. This catalog contains the list of configurations tasks as well as the module level dependencies to bring the resources including the Barracuda CloudGen WAF's configuration to the desired state as declared in the manifest files. Once the Puppet agent configures the CloudGen WAF using the catalog, it also monitors and maintains the achieved state by connecting to the Puppet Master at periodic intervals to check if there have been any changes to the declared state of the resources. By using Puppet to consistently manage their CloudGen WAF devices, organizations can avert redundant efforts and ensure reliability of the configurations, thus saving a significant amount of time and human resources.

Automatically deploy AWS best practice architecture with Puppet



Use Cases

Automate application security

Securing vulnerabilities in web applications is an ongoing process that requires testing the application for new vulnerabilities every time an update or change is made. The combined solution enables end-to-end automation of the application testing and security implementation process and consistent deployment of AWS security best practices.

Enable blue-green testing

As organizations expand and their infrastructure grows, it all too often happens in ad hoc ways which cause configuration drift. Today's agile practices focus on minimizing infrastructure downtime due to failovers and when releasing new changes. Blue-green deployment methodology is one way to reduce any potential downtime and risk by running two identical environments: blue and green. The blue environment can be the default production environment, and the green environment can be the idle staging environment in which the Puppet agent can execute the Puppet catalog to create the workflow. Once the Barracuda CloudGen WAF is fine-tuned for optimum configuration, the application URL can be changed to the production URL and the site can go live.

Ensure secure lifecycle management

In the software development lifecycle, application software is routinely built, tested and destroyed. When security is introduced into this lifecycle, manual processes often cause delays in the process. Automating the Barracuda CloudGen WAF with Puppet can vastly accelerate this by seamlessly integrating security at every stage of the lifecycle – from development to production.