Automating Application Security on Microsoft Azure

Barracuda CloudGen WAF, Barracuda Vulnerability Remediation Service, and Puppet

White Paper

Introduction

Organizations like yours are adopting Infrastructure-as-Code in order to be more agile in responding to shifting business requirements. At the same time, the threats posed by advanced malware have been growing exponentially. This poses a challenge: How to accelerate proven security best practices so that they enhance—rather than impede—the agility of the application-development lifecycle while continuing to support optimal security.

The Barracuda CloudGen WAF includes powerful built-in security-automation features, and leverages configuration automation solutions such as those developed by Puppet. As a result, it can serve as an important element of your strategy to accelerate the overall application-development process by bringing security up to agile speed, especially when implemented in public-cloud environments such as Microsoft Azure.

Puppet has been a pioneer in the development of configuration-automation solutions, and has a proven track record for automating the configuration and management of enterprise workloads. Puppet Forge is a hub for publicly available Puppet modules.

Automating the Provisioning of Barracuda CloudGen WAF Virtual Machines on Microsoft Azure

The Puppet module for Microsoft Azure makes it easier for you to eliminate potential bottlenecks by using code to automate the process of provisioning CloudGen WAF instances in Azure. Using the "azure_resource_template" resource type—included in Puppet's module—you can customize solution templates to create and configure virtual machines, along with such needed resources as the resource group, storage account, network security group, and network interface card.

REST API for the Barracuda CloudGen WAF

The REST API framework, which enables remote administration, can also be used to automate the configuration of the Barracuda CloudGen WAF. Almost all CloudGen WAF configuration tasks can be achieved with API calls. Here's an sample API call to create a service:

curl http://<systemip>:<mgmt-port>/restapi/v1/virtual_services -u 'token:' -X POST -H Content-Type:application/json -d '{"name": "demo_service", "ip_address": "<ipaddr>", "port": "80", "type":"http", "address_version":"ipv4", "vsite":"demo_vsite", "group":"demo_vsite_group"}'

In that example, the call to the virtual_service API is sent as a POST request, with a JSON body containing the required parameters and their values to create a service. Please note that this example is for REST APIv1. In the WAF Firmware version 9.1, there is support for an enhanced RESTAPI framework. The new version number is v3.

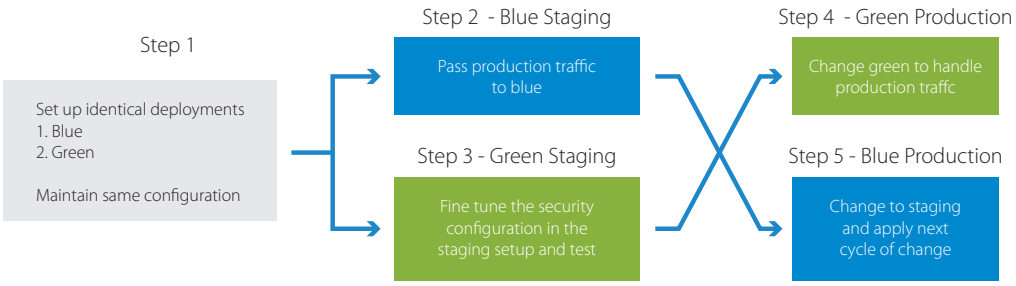
Application Security Automation Workflow Model

The Blue-Green testing framework is a proven deployment design pattern to achieve foolproof configuration management with minimal or no downtime.

With a Blue-Green deployment methodology, you can set the Blue environment as the default

production environment. In that case, the Green environment serves as the idle staging environment in which the Puppet Agent executes the Puppet catalog to create the workflow.

A schematic diagram to show the Blue Green deployment methodology is shown below:

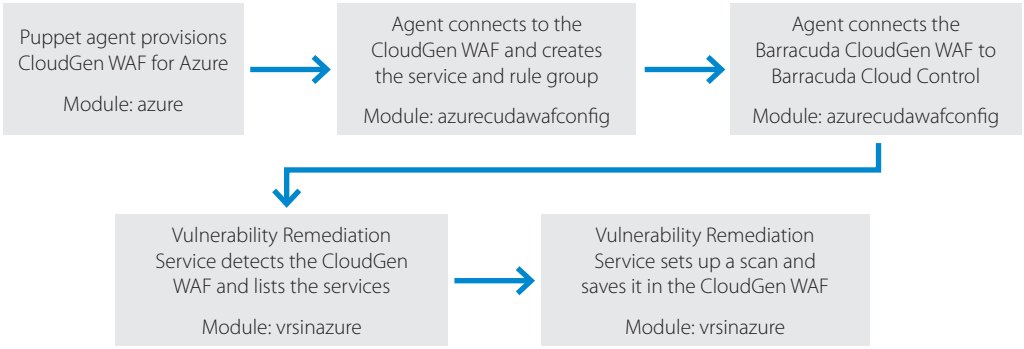


Notes:
Configuration can be synced between green and blue environments periodically.
Iterations to swap the environments are performed as per change requirements.

Typically, you will use the staging environment to automate all these stages of the deployment process:

Introduction of the security policy upon the application	Barracuda CloudGen WAF supports security policies that are fine-tuned for different types of application. Creating a service ensures that the security policy is bound to the service. REST API calls can be made to the CloudGen WAF for automating this process.
Seamless access to the application through the security layer	Minimal or no work is involved if the service is configured correctly.
Penetration testing through the security layer	The CloudGen WAF lets you use Barracuda Vulnerability Remediation Service to scan the application through and to ensure that policy fixes are available. This can be automated through REST API calls to the Vulnerability Remediation Service.
Fine-tuning the security layer	Policy fixes on the Barracuda CloudGen WAF are authorized by the administrator, and can be initiated from the Vulnerability Remediation Service console.
Go to production	Barracuda Vulnerability Remediation Service can be scheduled to run updated scans on a periodic basis to maintain optimum security.

Puppet has set up a sample environment that automates all these aspects of deployment. You can download it at https://github.com/barracudanetworks/waf-automation/tree/master/waf-puppet/azureinfra.



Deployment Automation Workflow

Provisioning the Barracuda CloudGen WAF

This is the Puppet manifest for creating the Barracuda CloudGen WAF using the ARM template:

```
azure_resource_template { 'waf-on-azure':
 ensure => 'present',
 resource_group => 'wafresourcegroup',
 content => file('azure/wafpayg.template'),
 params => {
'adminPassword' => '1234567a!',
'addressPrefix' => '10.0.0.0/16',
'subnetPrefix' => '10.0.0.0/24',
'vmSize' => 'Standard_D2',
'location' => 'South Central US',
'vmName' => 'waf-on-azure',
'storageAccountName' => 'waf_puppet',
'storageAccountType' => 'Standard_RAGRS',
'publicIPAddressName' => 'CloudGen WAF-ip',
'dnsNameForIP' => 'wafpublicpuppet',
'vNETName' => 'prod',
'subnetName' => 'default',
 },
}
```

Barracuda CloudGen WAF Configuration

Once the Barracuda CloudGen WAF is provisioned on Azure, the "azurecudawafconfig" module is used to configure the CloudGen WAF. REST API calls are used in a ruby script to connect to the CloudGen WAF and configure the service and the rule groups.

The sample script available in the module performs the following operations:

1. Accepts the EULA
2. Authenticates with the CloudGen WAF admin username and password and gets a REST API access token
3. Connects to the REST API and creates two service groups
4. Creates a certificate for use with the HTTPS service
5. In each of the service groups, creates two services, one each for HTTP and HTTPS
6. Connects the Barracuda CloudGen WAF to Barracuda Cloud Control

Barracuda Vulnerability Remediation Service

Barracuda Vulnerability Remediation Service is a complementary service to the Barracuda CloudGen WAF. It lets you automatically scan, remediate, and maintain your application security posture.

The solution supports REST API calls for all the critical aspects of the product, such as listing the services on the CloudGen WAF, configuring and running a scan operation, etc. The sample script available in the module creates a scan for a service mentioned by the administrator.

The script can also be extended to automatically create a scan every time a service is added on the CloudGen WAF.

What Next?

Once the Puppet agent run is complete, your application infrastructure includes a functional CloudGen WAF with a scanning service that's fully configured to keep your applications secure. Barracuda Cloud Control provides a simple, powerful, centralized interface for comprehensive administration and management.

Code Revision and Versioning

Since there is no manual intervention in the process except for the Puppet agent settings, the Puppet environment code can be uploaded to Continuous Integration (CI) services such as GitHub or Bitbucket.

Summary

Agility in developing, deploying, and updating applications is critical in today's fast-moving business environment. That same agility must extend to the deployment and configuration of application security solutions. Automating these security processes delivers that agility, and makes it easier to pivot rapidly when business needs shift.

Barracuda CloudGen WAF delivers optimal application security and exceptional ease of use, and its advanced automation frameworks help you boost productivity and stay ahead of the competition by accelerating your development cycles.

About Barracuda Networks, Inc.

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications, and data regardless of where they reside. These powerful, easy-to-use, and affordable solutions are trusted by more than 150,000 organizations worldwide, and are delivered in appliance, virtual appliance, cloud, and hybrid configurations. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network security and data protection. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks Inc.
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com