ORACLE

Web Application Firewall

L100

Flavio Pereira
Oracle Cloud Infrastructure
October 2019

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Objectives

After completing this lesson, you should be able to:

- Understand WAF concepts and use cases
- Describe the OCI WAF Service
- Explain OCI WAF capabilities and architecture
- Show a demo of OCI WAF

WAF Concepts and Use Cases

What is a Web Application Firewall?

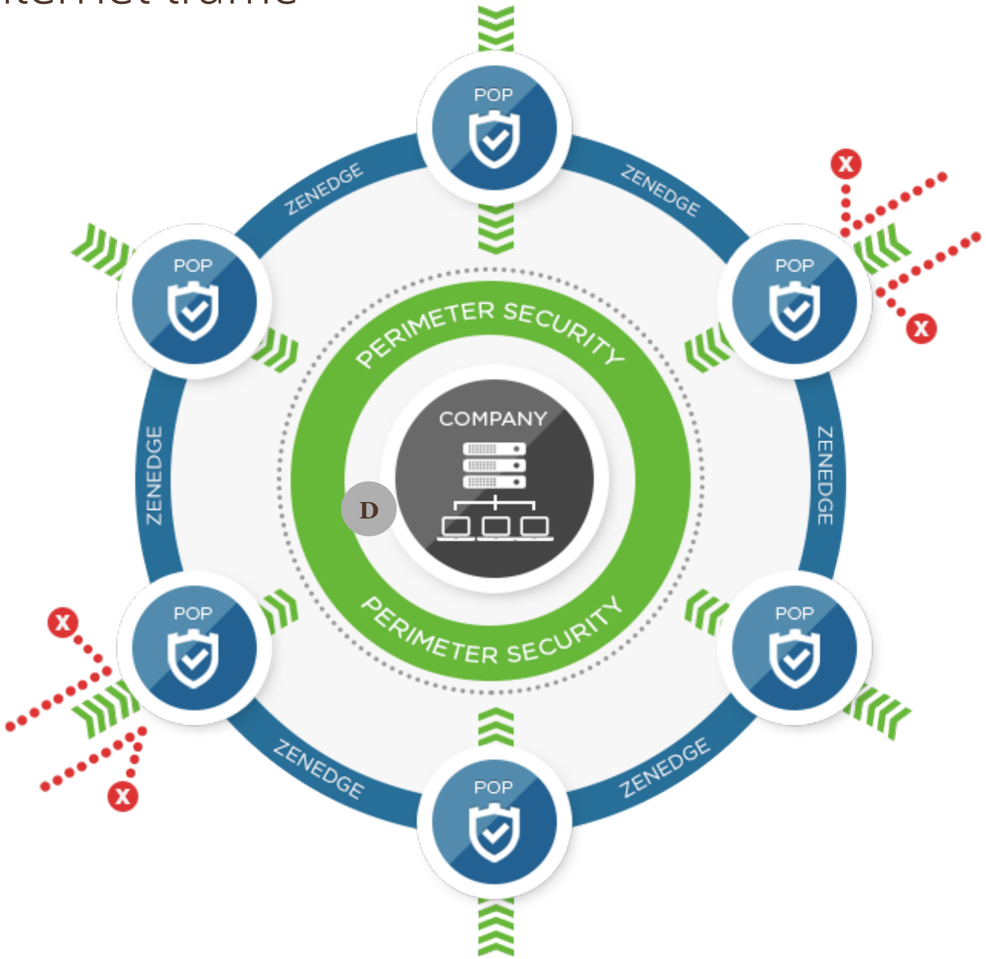
- Web Application Firewall (WAF) refers to a device, server-side plugin, or filter that applies a set of rules to HTTP/S traffic
- By intercepting HTTP/S traffic and passing them through a set of filters and rules, WAF is able to uncover and protect against attack streams hitting a web application
- Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection in addition to giving customers the ability to filter specific source IPs or bad bots
- Typical responses from WAF will either be allowing the request to pass through, audit logging the request, or blocking the request by responding with an error page.

OCI Web Application Firewall

OCI Web Application Firewall (WAF) is a cloud-based, PCI-compliant, global security service that protects applications from malicious and unwanted internet traffic

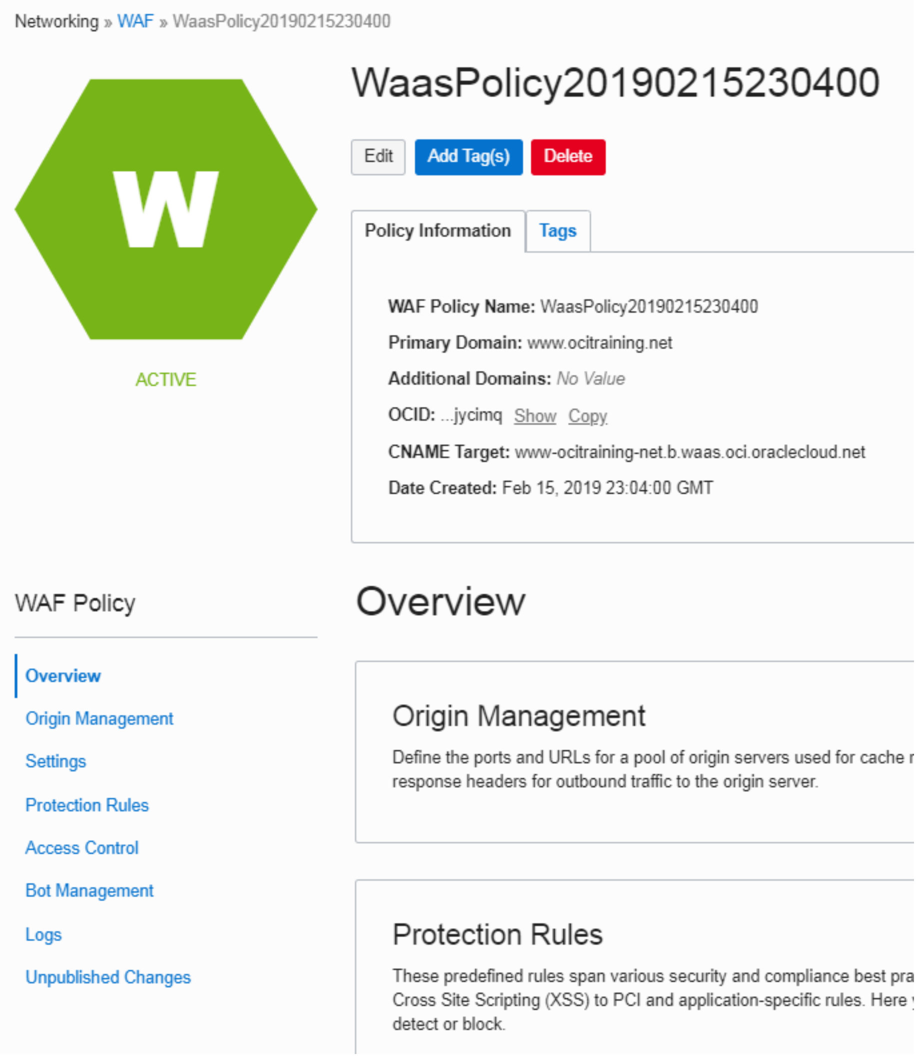
Use cases:

- Protect any internet-facing endpoint from cyberattacks and malicious actors
- Protect against cross-site scripting (XSS) and SQL injection, activities that allow attackers to gain unauthorized access to privileged information
- Bot management – dynamically blocking bad bots
- Protection against layer 7 distributed denial-of-service (DDoS) attacks
- Aggregated threat intelligence from multiple sources including Webroot BrightCloud



Key OCI WAF components

- Supports over 250 rulesets to protect against SQL injection, cross-site scripting, HTML injection, and many more threats
- JavaScript Challenge, CAPTCHA Challenge, Device Fingerprint Challenge and white listing capabilities work in conjunction with rulesets to further detect and mitigate bad bots and allow legitimate human and bot traffic
- User access controls can be configured on the basis of countries, IP addresses, URLs, and other request attributes to prohibit risky traffic
- Multi-cloud support provides WAF protection for any internet-facing application in any environment: OCI, on-premises, and across multi-cloud deployments



Networking » WAF » WaasPolicy20190215230400

WaasPolicy20190215230400

WAF Policy Name: WaasPolicy20190215230400

Primary Domain: www.ocitraining.net

Additional Domains: *No Value*

OCID: ...jycimq Show Copy

CNAME Target: www-ocitraining-net.b.waas.oci.oraclecloud.net

Date Created: Feb 15, 2019 23:04:00 GMT

Overview

Origin Management

Define the ports and URLs for a pool of origin servers used for cache r response headers for outbound traffic to the origin server.

Protection Rules

These predefined rules span various security and compliance best pra Cross Site Scripting (XSS) to PCI and application-specific rules. Here detect or block.

OCI WAF Rulesets

- OCI WAF uses OWASP ModSecurity Core Rule Set to protect against the most common web vulnerabilities. These rules are managed and maintained by the open source community.

- OCI WAF comes pre-configured with protection against the most important threats on the Internet as defined by OWASP Top 10. These include
  - A1 – Injections (SQL, LDAP, OS, etc.)
  - A2 – Broken Authentication and Session Management
  - A3 – Cross-site Scripting (XSS)
  - A4 – Insecure Direct Object References
  - A6 – Sensitive Data Exposure
  - A7 – Missing Function-Level Access Control

- Each type of vulnerability ruleset is shown within the OCI console, with granular controls for each specific rule.

Challenges and whitelisting capabilities

- JavaScript Challenge: fast and efficient way to block a large percentage of bot attacks
  - After receiving an HTTP request, a piece of JavaScript is sent back to the browser of every client, attacker, and real user. It instructs the browser to perform an action. Legitimate browsers will pass the challenge without the user's knowledge, while bots—which are typically not equipped with JavaScript—will fail and be blocked

- CAPTCHA Challenge
  - If a specific URL should be accessed only by a human, you can control it with CAPTCHA protection.
  - You can customize the comments for the CAPTCHA Challenge for each URL

- Whitelisting: Allows you to manage which IP addresses appear on the IP whitelist
  - Requests from the whitelisted IP addresses bypass all challenges, such as DDoS policies and WAF rulesets.

Bot Management

Entity Attributes and Behavioral Detection

- Human Interaction

  Oracle WAF identifies normal usage patterns based on legitimate user behavior to the site. The WAF will challenge with CAPTCHA or block requests when it detects abnormalities or traffic exceeds defined interaction thresholds.

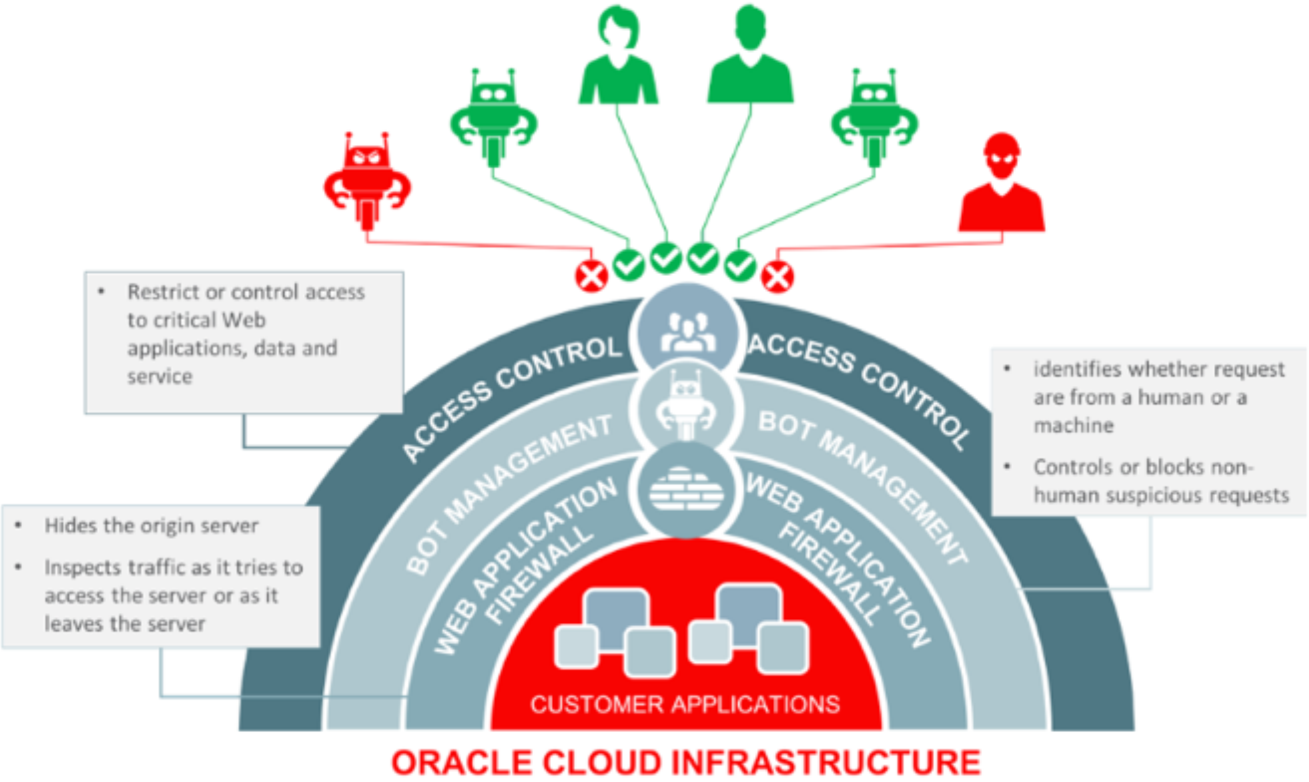
- Device Fingerprinting (available in the API)

  Oracle WAF collects unique various characteristics about a device entity, generating a hashed signature. This hashed signature is then compared to other requests to determine the same signature is being leverages across different contexts.

Access Controls

Use the access controls to restrict or control access to your critical web applications, data and services. E.g., in some cases, an offering may need to stay within a specific country. Regional access control can be used to restrict users from certain geographies.

- Control access, based on HTTP header information. Block requests if the HTTP header contains specific names or values or allow traffic with proper HTTP regular expression
- Control access based on URL address matching or partial matching or match proper URL regular expressions



- Restrict or control access to critical Web applications, data and service
- identifies whether request are from a human or a machine
- Controls or blocks non-human suspicious requests
- Hides the origin server
- Inspects traffic as it tries to access the server or as it leaves the server
ACCESS CONTROL
ACCESS CONTROL
BOT MANAGEMENT
BOT MANAGEMENT
WEB APPLICATION FIREWALL
WEB APPLICATION FIREWALL
CUSTOMER APPLICATIONS
ORACLE CLOUD INFRASTRUCTURE

Safe harbor statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions.

The development, release, timing, and pricing of any features or functionality described for Oracle’s products may change and remains at the sole discretion of Oracle Corporation.

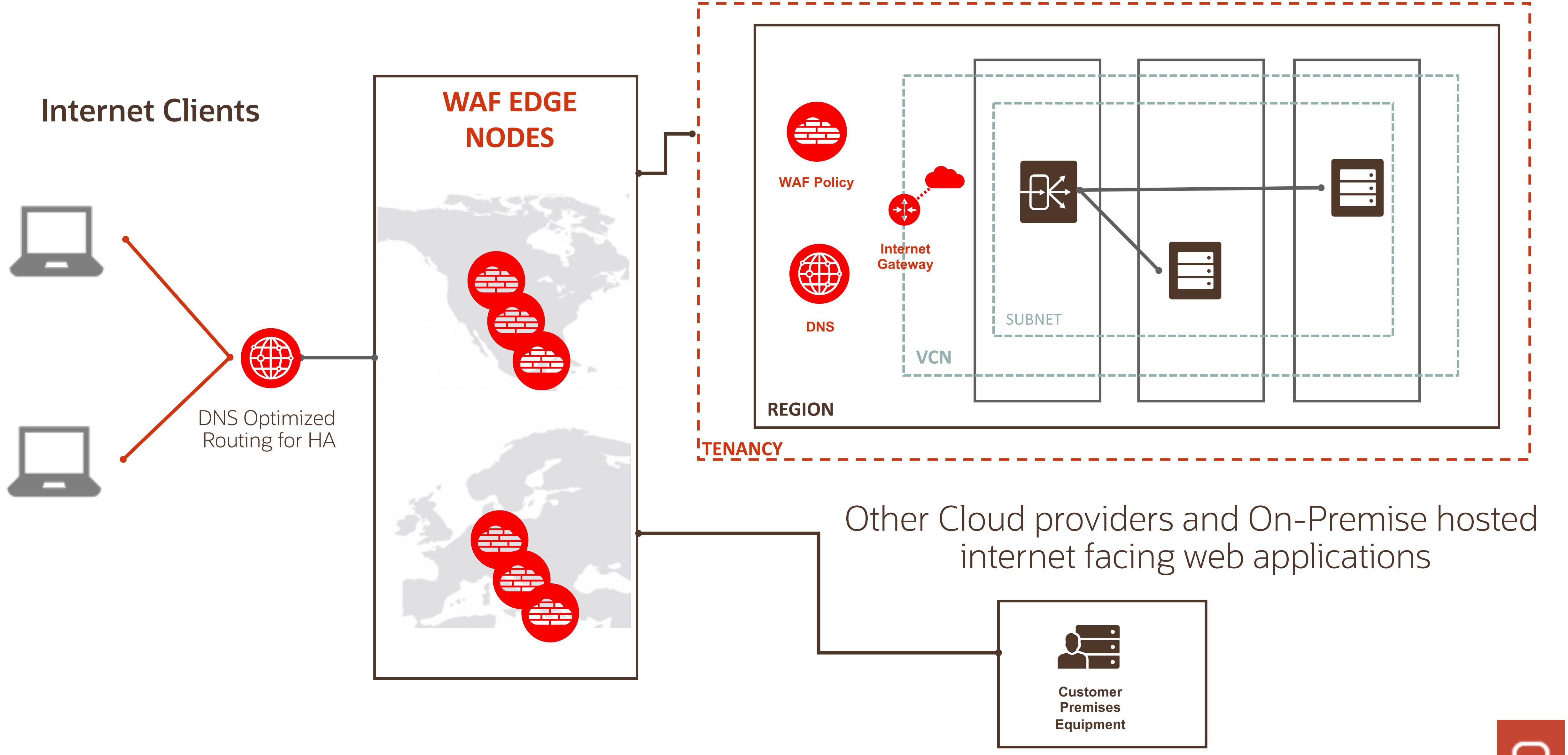
Web Application Firewall

L100

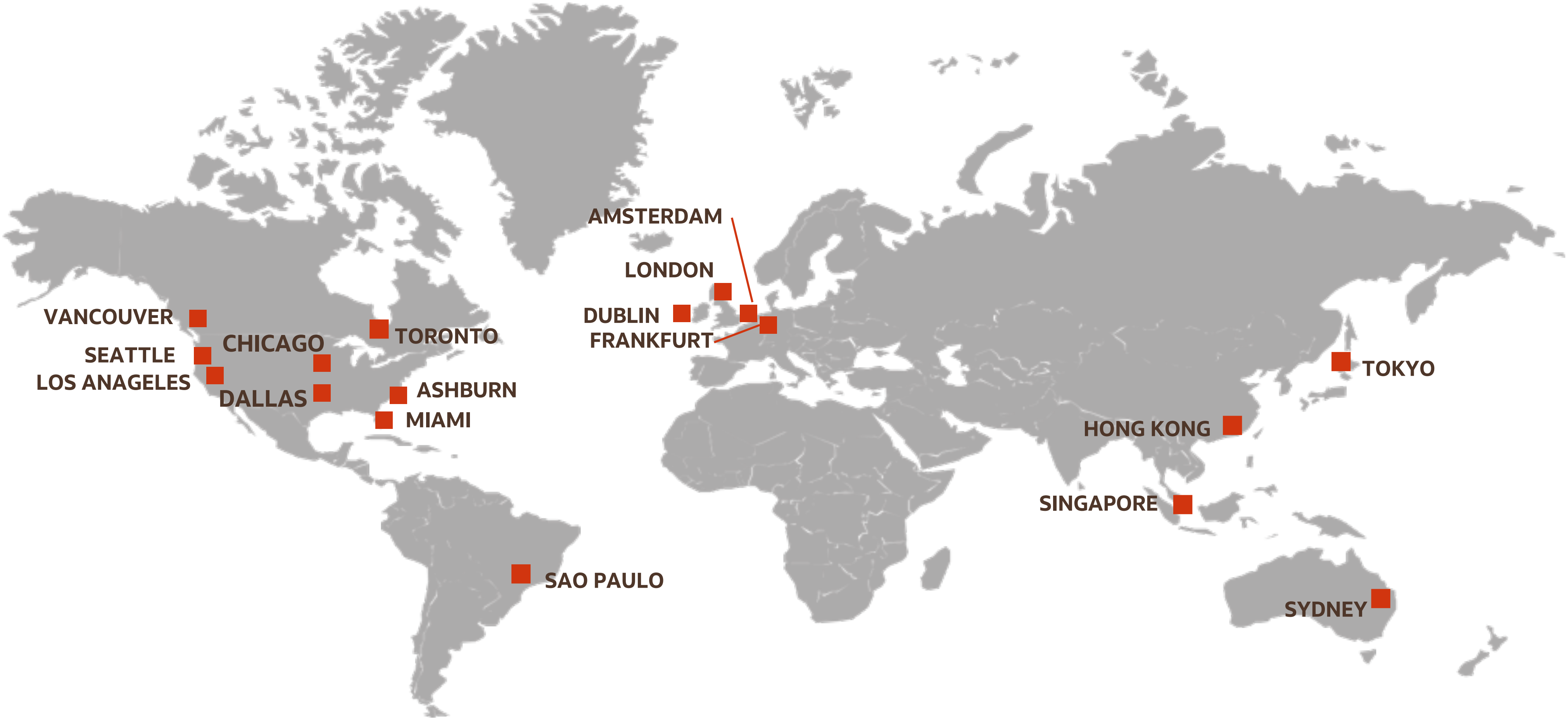
Flavio Pereira
Oracle Cloud Infrastructure
October 2019

WAF Architecture and Benefits

Oracle Cloud Infrastructure WAF Architecture



WAF Point of presences (PoPs)



Shared Responsibility Model for WAF

Responsibility	Oracle	Customer
Configure WAF on-boarding dependencies (DNS, Ingress rules, network)	No	Yes
On-board/Configure the WAF policy for the web application	No	Yes
Construct new rules based on the new vulnerabilities and mitigations	Yes	No
Review and accept new recommended rules	No	Yes
Keep WAF infrastructure patched and up-to-date	Yes	No
Monitor data-plane logs for abnormal, undesired behavior	Yes	Yes
Monitor for Distributed Denial of Services (DDoS) attacks	Yes	No
Provide High Availability (HA) for the WAF	Yes	No
Tune the WAF's access rules and bot management strategies for your traffic	No	Yes

Benefits of Oracle Cloud Infrastructure WAF

- Consolidate threat intelligence
- Push malicious traffic farther away from your orign
- Augment your Security Operations Center (SOC)
- Better Visibility into internet traffic metrics
- Consolidate governance through policies, audit, and taggin
- Off-load patching and maintenance of Web Application Firewall
- Global traffic management and optimization
- Consolidate WAF policy for OCI and non-OCI applications
- Low cost

ORACLE

Demo: Web Application Firewall

Summary

- OCI WAF is a cloud-based Web Application firewall and PCI compliant
- Offer granular access control, geo blocking and URL blocking
- Protect any internet-facing endpoint from cyberattacks and malicious actors
- All traffic flows through the OCI WAF edge nodes before arriving at your application server

Oracle Cloud always free tier:
oracle.com/cloud/free/

OCI training and certification:
oracle.com/iaas/training
oracle.com/iaas/training/certification
education.oracle.com/oracle-certification-path/pFamily_647

OCI hands-on labs:
ocitraining.qloudable.com/provider/oracle

Oracle learning library videos on YouTube:
youtube.com/user/OracleLearning