# Great Firewall of Web Apps

## Risk assessment & Audit considerations around Web Application Firewall (WAF) – Sripati M S

April 8, 2025

ISACA® Muscat Chapter 25 YEARS

# What this session is about…

1. High level overview of WAF
2. Do we need it?
3. How does it work?
4. Different ways to test a WAF
5. Focus areas while auditing/ assessing a WAF
6. Before we go…

# What this session is not about…

1. Technical details of a WAF (deployment, operations, bypass, etc.)
2. Live Demo (administration, hardening, or breaking WAF). Another session, perhaps…

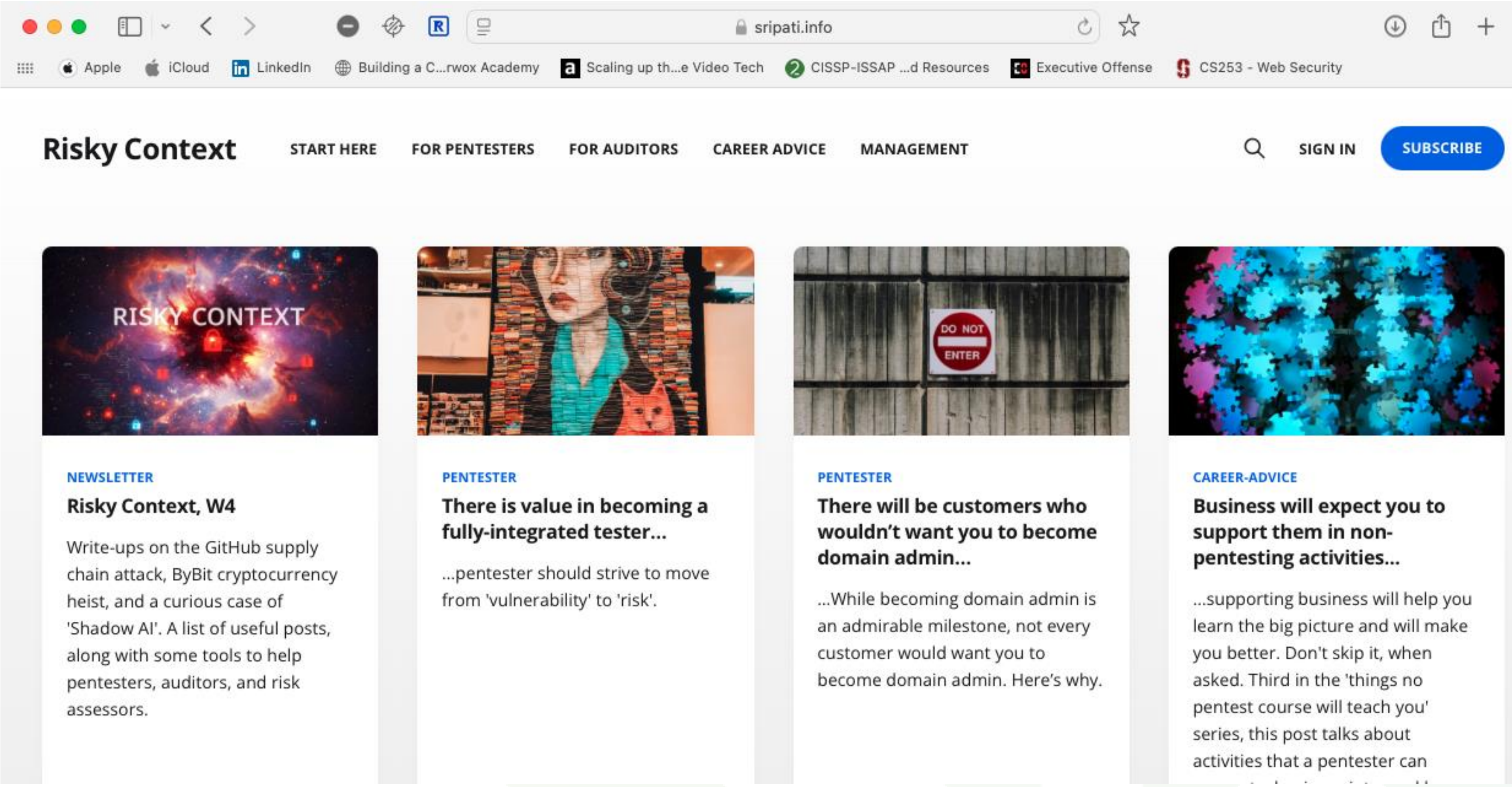
# /whoami…

Information Security risk management professional, 2 decades of experience in information security,

1. Risk Management
2. Auditing
3. Governance and Compliance
4. Security Service Delivery

Write for pentesters, auditors, risk assessors on https://sripati.info

Run a newsletter ‘Risky Context’ on my website.



NEWSLETTER

**Risky Context, W4**

Write-ups on the GitHub supply chain attack, ByBit cryptocurrency heist, and a curious case of 'Shadow AI'. A list of useful posts, along with some tools to help pentesters, auditors, and risk assessors.

PENTESTER

**There is value in becoming a fully-integrated tester...**

...pentester should strive to move from 'vulnerability' to 'risk'.

PENTESTER

**There will be customers who wouldn't want you to become domain admin...**

...While becoming domain admin is an admirable milestone, not every customer would want you to become domain admin. Here's why.

CAREER-ADVICE

**Business will expect you to support them in non-pentesting activities...**

...supporting business will help you learn the big picture and will make you better. Don't skip it, when asked. Third in the 'things no pentest course will teach you' series, this post talks about activities that a pentester can

# A WAF protects a web application…

1. if configured properly,
2. by intercepting traffic silently and transparently (if deployed inline)
3. by analyzing web traffic, weeding out attacking payloads

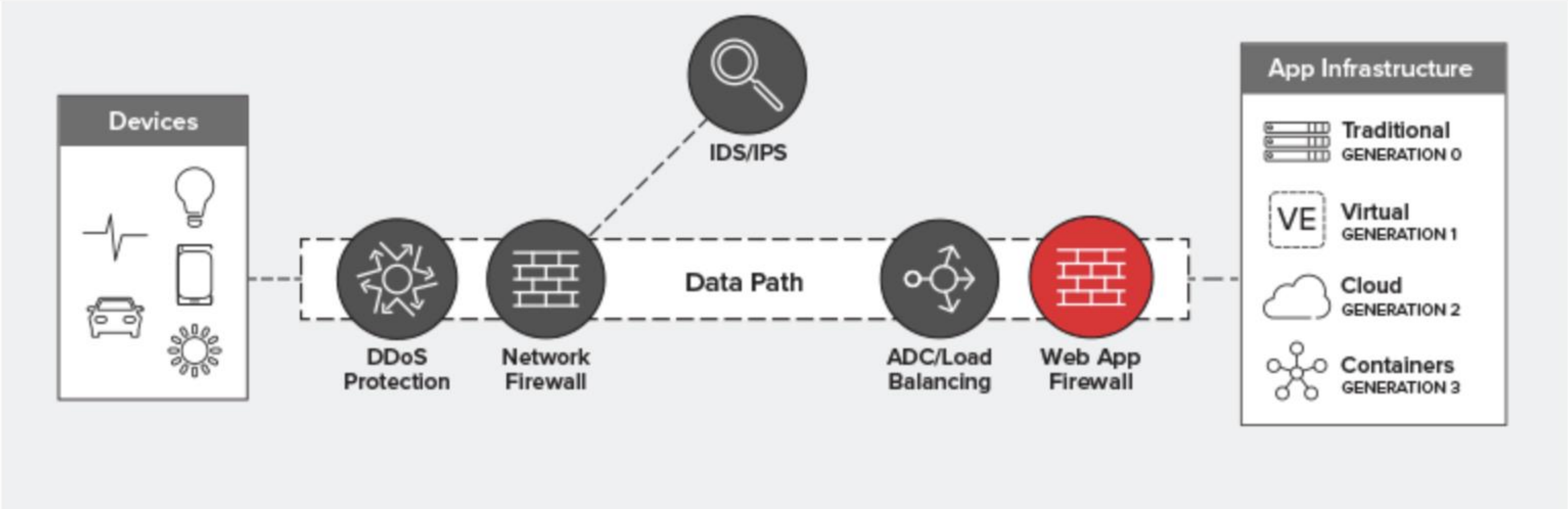


Image credit – F5, https://www.f5.com/company/blog/where-does-a-waf-fit-in-the-data-path

# WAF usually are of 3 types…

1. Network based WAF, appliances (usually)
2. Host based WAF, sits on the web-server (e.g., ModSecurity)
3. Cloud based WAF (e.g., AWS WAF)

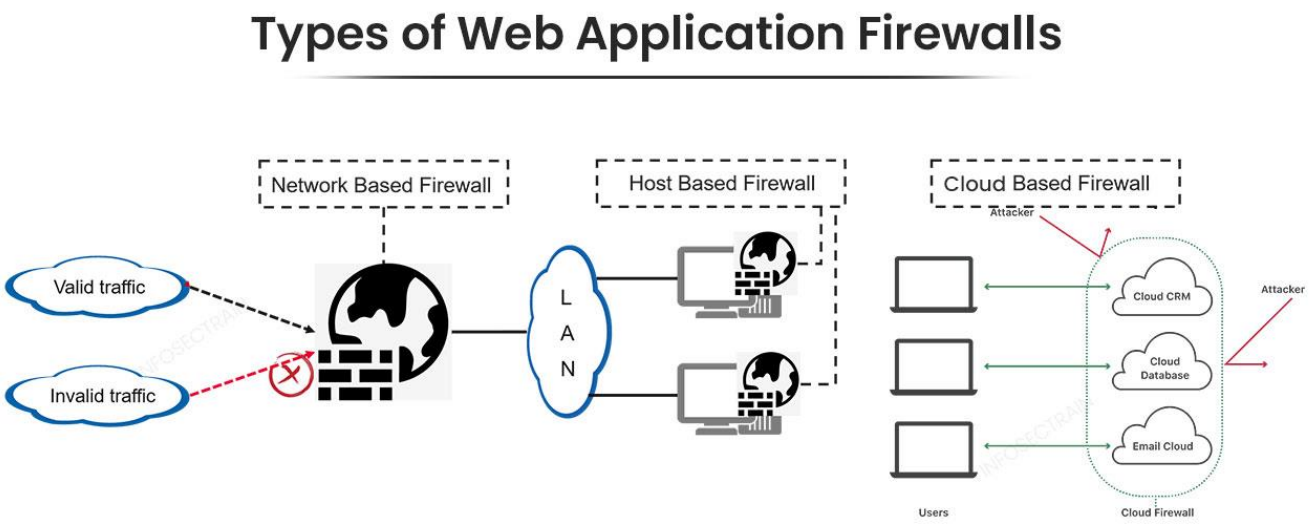


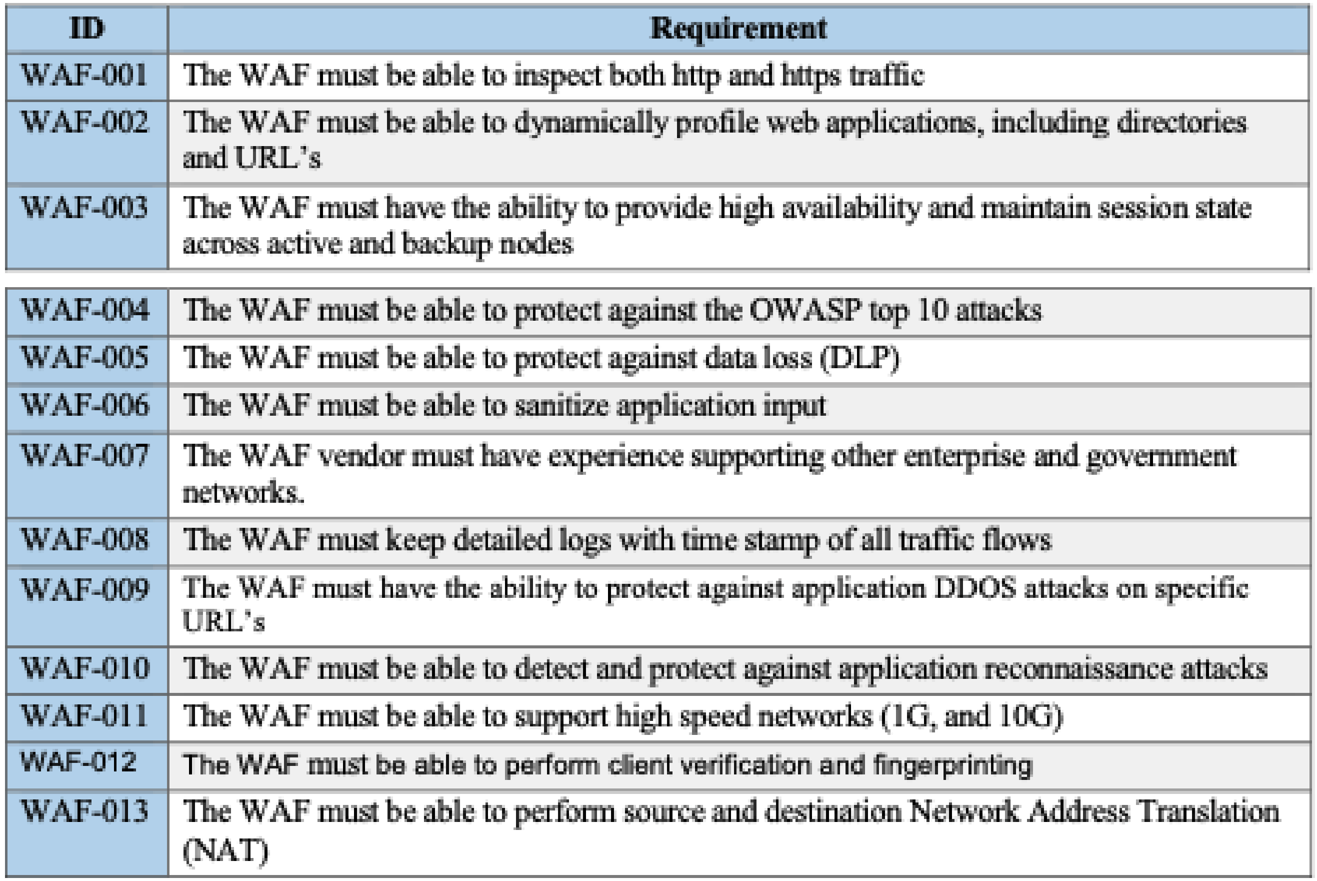
Image Credit – Infosec Train, https://www.infosectrain.com/blog/what-is-waf-and-its-types/

# WAF is needed if…

1. One is required to implement it as part of regulation (e.g., Government Network Security Architecture Framework, by ITA Oman, mandates WAF at Maturity Level II for government networks)…
2. It is industry or domain specific best practice (e.g., every bank uses a WAF)…
3. Cost of not implementing is bigger (e.g., insurance won’t pay after website defacement if it turns out that WAF wasn’t deployed)…

# WAF selection criteria by ITA…

https://www.ita.gov.om/itaportal_ar/Data/SiteImgGallery/202210291044579/تعميم%20رقم%206-2015%20حول%20إطار%20التصاميم%20الامنية%20للشبكات%20الحكومية.pdf



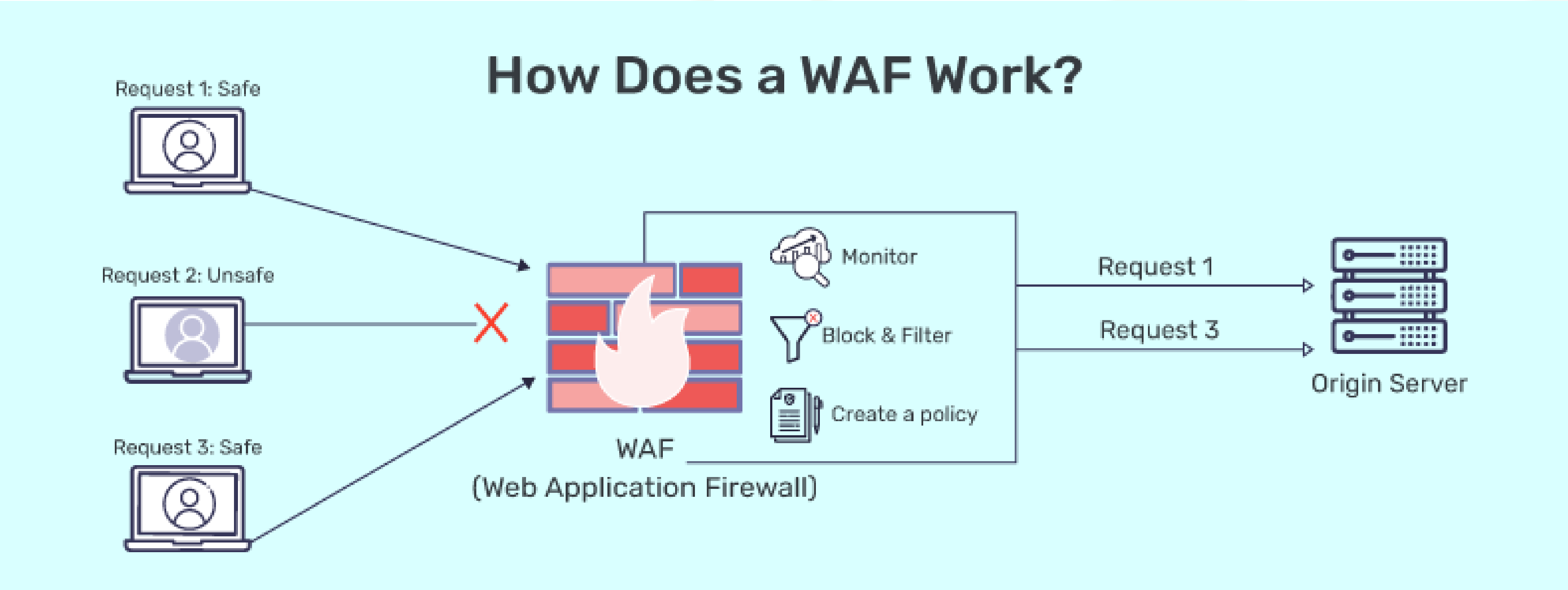
| ID | Requirement |
|---|---|
| WAF-001 | The WAF must be able to inspect both http and https traffic |
| WAF-002 | The WAF must be able to dynamically profile web applications, including directories and URL's |
| WAF-003 | The WAF must have the ability to provide high availability and maintain session state across active and backup nodes |
| WAF-004 | The WAF must be able to protect against the OWASP top 10 attacks |
| WAF-005 | The WAF must be able to protect against data loss (DLP) |
| WAF-006 | The WAF must be able to sanitize application input |
| WAF-007 | The WAF vendor must have experience supporting other enterprise and government networks. |
| WAF-008 | The WAF must keep detailed logs with time stamp of all traffic flows |
| WAF-009 | The WAF must have the ability to protect against application DDOS attacks on specific URL's |
| WAF-010 | The WAF must be able to detect and protect against application reconnaissance attacks |
| WAF-011 | The WAF must be able to support high speed networks (1G, and 10G) |
| WAF-012 | The WAF must be able to perform client verification and fingerprinting |
| WAF-013 | The WAF must be able to perform source and destination Network Address Translation (NAT) |

# WAF features (example)…

1. Threat intelligence with machine learning (building application expertise)
2. Capability to secure GraphQL REST/JSON, XMLS, and GWT APIs
3. Behavioral analytics for L7 DoS detection and mitigation
4. Defenses for OWASP Top 10
5. Protects against stolen credentials (combines threat intelligence)
6. Bot defense
7. Capability to import scanning results from DAST and SAST tools to help update signatures
8. Rate limiting, CAPTCHA, etc.
9. Geography based traffic controls

# How does a WAF work…

1. Attack signature databases
2. Traffic pattern analysis
3. DDoS protection
4. Bot protection
5. Rate Limiting
6. Load Balancing



Ref - https://www.indusface.com/blog/how-web-application-firewall-works/

# WAF can be tested by…

1. Penetration tests
   1. Test the web application reachability, bypassing WAF (finding out origin IP)
   2. Test various attacks on web application, see if they are flagged by WAF
2. Configuration Review
   1. Whether WAF is configured in ‘log’ mode, ‘learning’ mode, or ‘block’ mode?
   2. How current is the attack and signature database, against those by OEM?
   3. WAF configuration (session timeout, admin defaults, integration with SIEM, type of alerts that goto SIEM, type of HTTP verbs captured, etc.)
3. Audit/ Risk Assessment
   1. People, process, technology

While its absence gets flagged as a risk or an audit finding, many facets to consider before you get value out of a WAF.

Here are 5 important focus areas related to WAF…

# Does WAF cover everything that is public…

1. Master list of application
   1. if there is a master list of applications available with some function/department (usually IT),
   2. If that master list is properly controlled (i.e., any updates, additions, removals, etc. need to be reviewed and approved before they happen, periodic review of that list is in place, etc.), and
   3. If criticality/sensitivity of information in an application is pointed out via a controlled, internal process.
2. Protection Coverage
   1. Ensure all ports of those application are configured at WAF
      1. Usually, you will need to configure WAF for each port that is used by application.
      2. if an application uses 4 ports (e.g., 9001, 8443, 443, and 80), the WAF administrator need to configure WAF for each port, as part of policy.
   2. Ensure it is not possible to reach that application:port directly

# How is PII/ sensitive information managed within WAF

1. Once SSL is offloaded, all sorts of information gets captured into WAF (passwords, access tokens, transaction payloads, etc.) in plaintext.
2. Usually, leading WAF give mechanisms to,
   1. Mark PII/ sensitive info and
   2. Hide/ mask that info.
3. However, one needs to configure it, for each application and sensitive area (within that application).
4. It is a tedious job, that many people tend to skip on, unless explicitly asked.

# Whether WAF is in ‘learning’ or ‘blocking’ mode

1. When deployed, WAFs are always in learning mode. They inspect traffic, analyze it, and flag any unusual behaviour for manual inspection. Once a human inspects and flags it, WAF knows how to handle that pattern. This goes on for a while, till humans decide that WAF is ready for action.
2. Then they put it on block mode. No more flagging and inspection after that. WAF takes action as commanded (block, usually).

1. Issue is – sometimes the learning mode never stops.
2. You can bet that not all requests for manual inspection will be looked at, beyond a point.

# Log monitoring, backup

1. No integration with SIEM (Security Incident and Event Management)

1. We have a dedicated administrator who looks at WAF console, day in and day out. What do we need SIEM for?
2. Issue is - WAF is handled by first line (IT), whereas SIEM is 2nd line (InfoSec). As a rule of thumb, your SIEM should catch all pertinent issues highlighted by your first line tools. Not integrating WAF with your SIEM is a recipe for disaster.

2. Insufficient integration with SIEM

1. Only WAF alerts go to SIEM, but not the GET, POST requests. So you have nothing to check the false positives against (especially if the alert is more than 2 days' old - see last point). You say your SOC completes all alerts in the same day?
2. Do you get alert on SIEM if someone removes an application or a profile from WAF, or makes changes to the settings? You say your WAF is handled in-house and all staff signs NDA/SLA.

3. Insufficient backup (of traffic).

# No HA (High Availability) for WAF or Human

1. Even if you project the WAF in DR (Disaster Recovery) site as HA, it is Ok. No organization can have all security controls with redundancy. You make with what you have, so long as the intention is right. However, HA means,

1. Settings (policies, profiles, etc.) must sync between the appliances that are connected in HA mode. You need to check whether that actually happens (hint: it doesn't always sync in real-time).
2. There is a configuration somewhere that says - route traffic through WAF2 if I (WAF1) breaks and vice-versa. Look for proof of that configuration. Also, check if it manual or automatic. If manual, whether that manual switch-over is tested as part of BCP/DR drill. No drill, no dice.

2. Compensating controls (if HA is not present)

1. Backup of WAF config, policies, backed up.
2. Contract with WAF OEM who provides us manpower. DR/ BCP drills to prove.
3. Above controls documented in SOP.

# QnA

ISACA
Muscat Chapter 25 YEARS

ISACA®

Muscat Chapter 25 YEARS