Corfu

Web Application Firewall (WAF)

Dr. Stylianos Karagiannis (PhD)
Ionian University, Corfu, Greece

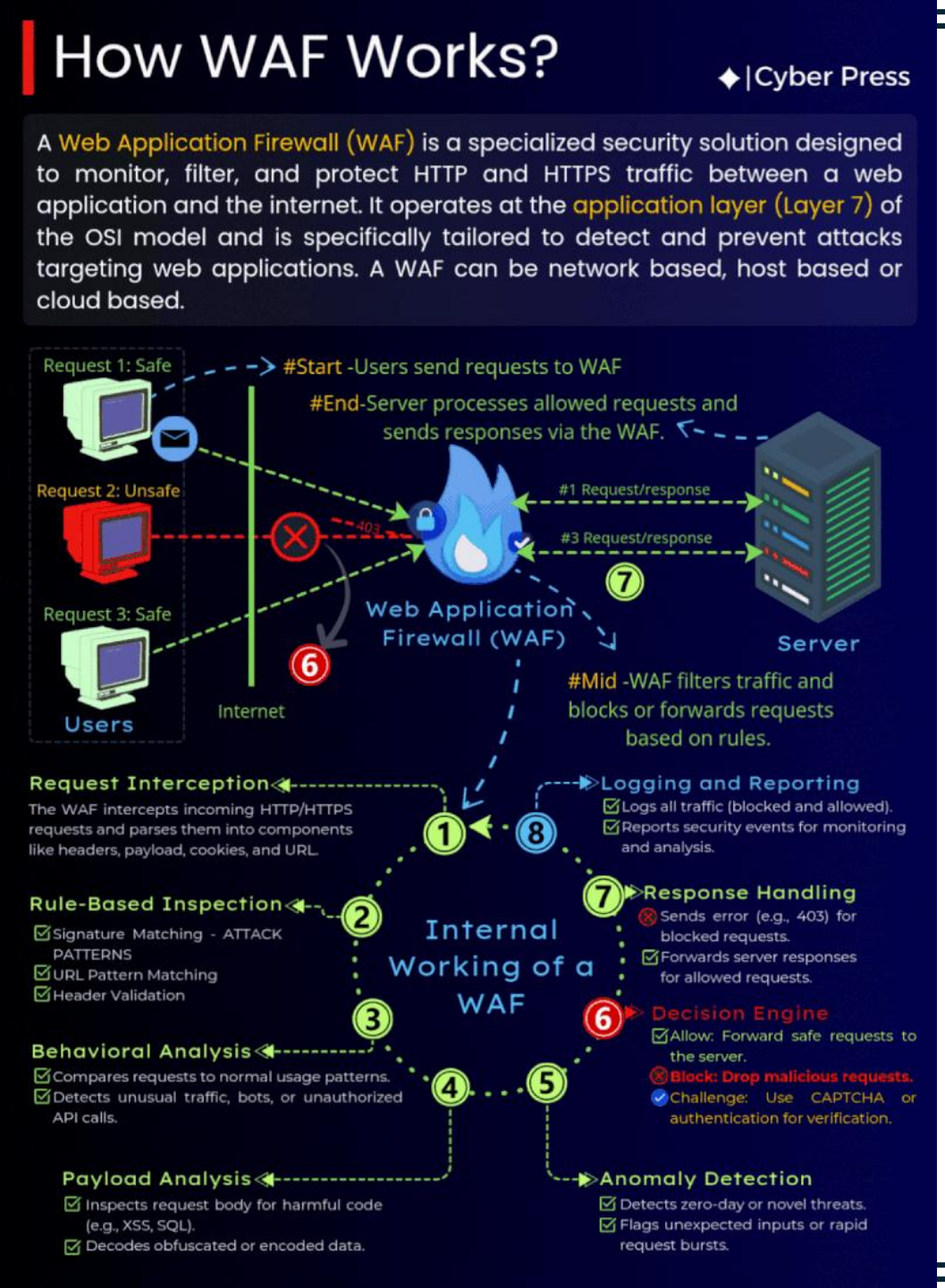
</> Stylianos Karagiannis

Corfu, Kozani, Greece Lisbon, Portugal

PhD in Cybersecurity - Post Doc @ Ionian University Department of Informatics, Corfu, Greece
Senior Researcher @ PDMFC, Lisbon, Portugal

Research Interests: Cybersecurity, Privacy, Capture The Flag (CTF) Challenges, Cyber Ranges
Gamification, Incident Handling, Virtual Labs, Game-Based Learning
Social Constructivism, Learning Theories

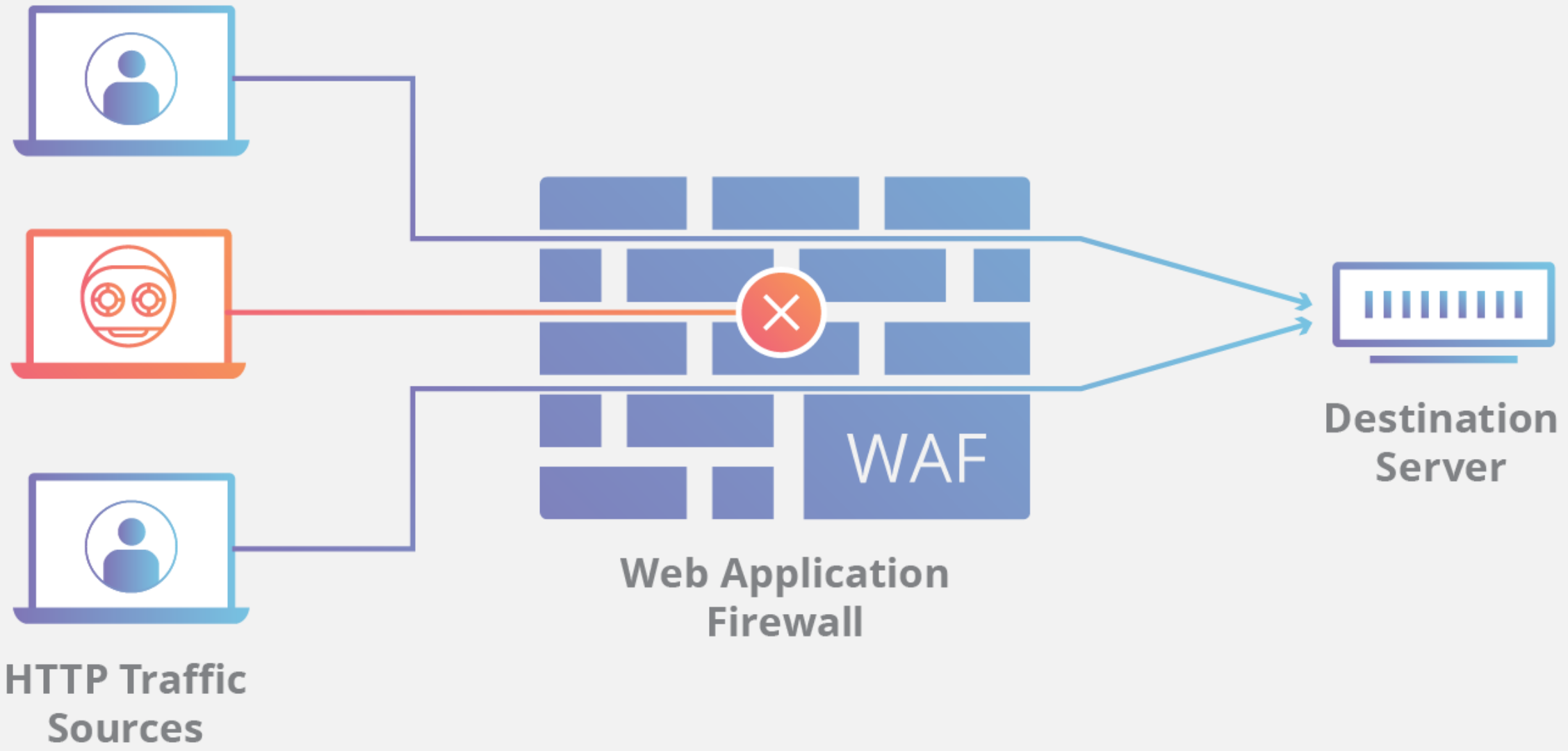
Email: skaragiannis@ionio.gr, LinkedIn, NMSLab



Networks, Multimedia, Security and Privacy Laboratory | Ionian University

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

- Το WAF (web application firewall) προστατεύει τις web εφαρμογές φιλτράροντας και παρακολουθώντας την HTTP κίνηση μεταξύ της εφαρμογής και του Διαδικτύου.
- Συνήθως προστατεύει από επιθέσεις όπως:
  - cross-site request forgery (CSRF)
  - cross-site scripting (XSS)
  - file inclusion
  - SQL injection
  - και άλλους τύπους επιθέσεων.
- Το WAF λειτουργεί στο επίπεδο 7 του μοντέλου OSI και δεν έχει σχεδιαστεί να αντιμετωπίζει όλους τους τύπους επιθέσεων.
- Χρησιμοποιείται ως μέρος ενός συνόλου εργαλείων που παρέχουν ολιστική άμυνα απέναντι σε διαφορετικά vectors επιθέσεων.
- Τοποθετώντας ένα WAF μπροστά από μια web εφαρμογή, δημιουργείται ένα «τείχος προστασίας» ανάμεσα στην εφαρμογή και το Διαδίκτυο.
- Σε αντίθεση με έναν proxy server που προστατεύει τον client, το WAF είναι μορφή reverse-proxy που προστατεύει τον server, καθώς όλη η κίνηση περνά πρώτα από αυτό.
- Το WAF λειτουργεί με κανόνες/πολιτικές (policies) που φιλτράρουν κακόβουλη κίνηση και προστατεύουν από ευπάθειες της εφαρμογής.
- Μεγάλο πλεονέκτημα του WAF είναι η ευκολία και ταχύτητα τροποποίησης πολιτικών για άμεση αντίδραση σε νέους τύπους επιθέσεων.
- Σε περίπτωση επίθεσης DDoS, μπορεί γρήγορα να εφαρμοστεί rate limiting μέσω κατάλληλης αλλαγής των WAF policies.


WAF
Destination Server
Web Application Firewall
HTTP Traffic Sources

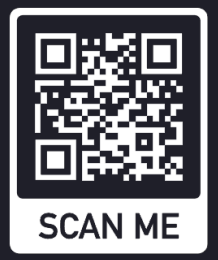
Διαφορά μεταξύ blocklist και allowlist WAFs

- Ένα WAF που λειτουργεί με **blocklist** (μοντέλο αρνητικής ασφάλειας) προστατεύει από **γνωστές επιθέσεις**.
  - Παράδειγμα: σαν έναν πορτιέρη σε κλαμπ που δεν επιτρέπει την είσοδο σε όσους δεν τηρούν τον ενδυματολογικό κώδικα.
- Ένα WAF που βασίζεται σε **allowlist** (μοντέλο θετικής ασφάλειας) επιτρέπει **μόνο την προεγκεκριμένη κίνηση**.
  - Παράδειγμα: σαν τον πορτιέρη σε ένα αποκλειστικό πάρτι που επιτρέπει είσοδο μόνο σε όσους βρίσκονται στη λίστα.
- Και τα δύο μοντέλα έχουν **πλεονεκτήματα και μειονεκτήματα**.
- Πολλά WAFs χρησιμοποιούν ένα **υβριδικό μοντέλο**, το οποίο εφαρμόζει και blocklists και allowlists για καλύτερη προστασία.

NMSLab

Ευχαριστώ για την Προσοχή σας!

Dr. Stylianos Karagiannis, PhD



https://nmslab.di.ionio.gr