Ασφάλεια, Διαθεσιμότητα και Ταχύτητα για τις Web Εφαρμογές

Barracuda Web Application Firewall

Καλοχριστιανάκης Αντώνης

Διευθυντής Πωλήσεων

Digital SIMA

Ανατομία Web επίθεσης

- Οι Web επιθέσεις δε διαφέρουν ουσιαστικά από το κοινό έγκλημα
- Κάποιοι είναι θύματα από τύχη…
- … κάποιοι έχουν στοχευθεί

Επιλογή στόχου

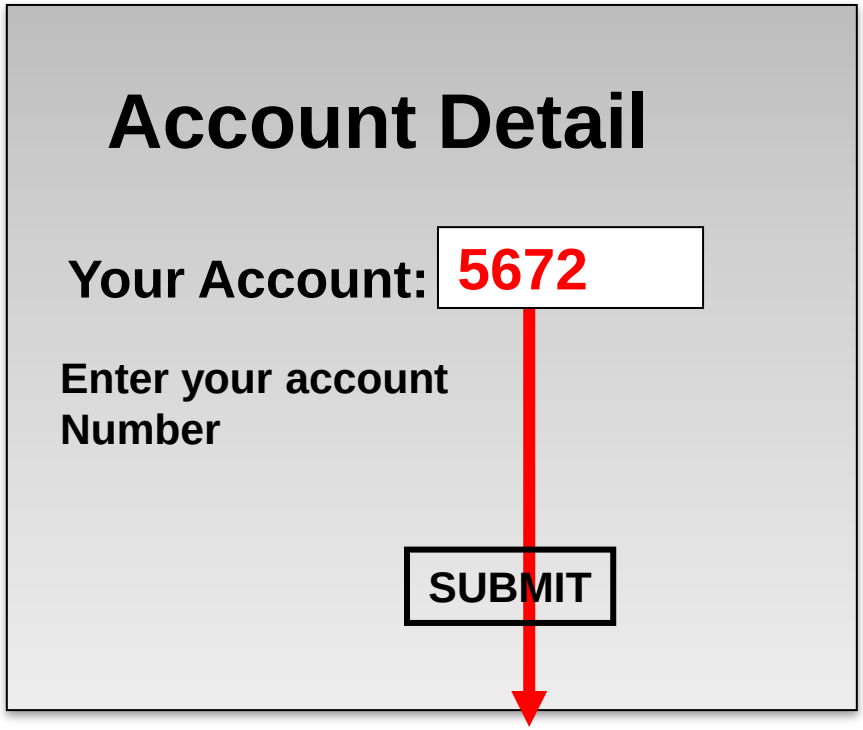
Ανάλυση ασφάλειας

Εκμετάλλευση του Προβλήματος

SQL Basics

Ο χρήστης εισάγει δεδομένα σε μία φόρμα σε μία web σελίδα

Αυτή η τιμή μετατρέπεται από την εφαρμογή σε ένα SQL statement

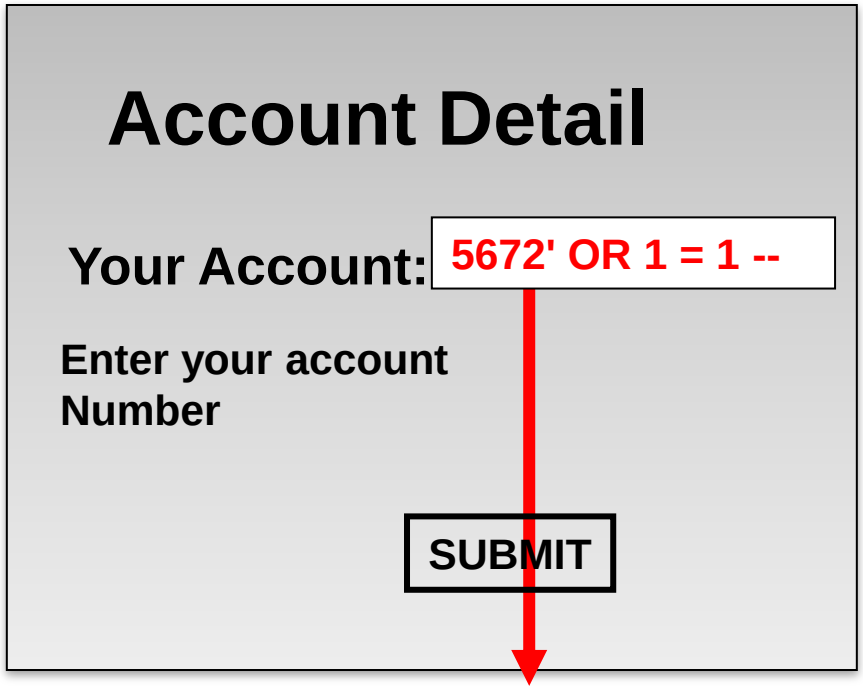


…select acct-detail from acct-master WHERE acct=‘5672’

Απλή SQL Injection

Καθώς το 1=1 είναι πάντα αληθές, όλες οι εγγραφές του acct-master επιλέγονται και ανακτώνται

“- - ” δηλώνει σχόλιο στην SQL



...select acct-detail from acct-master WHERE acct=‘5672' OR 1 = 1‘

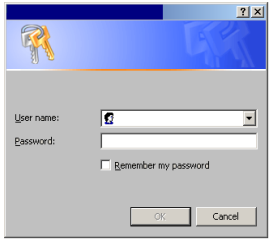
Επίθεση Cross-Site Scripting (XSS)

1 Ο Hacker τοποθετεί ένα κακόβουλο script σε ένα POST που αποθηκεύεται στη web σελίδα του server

Web Server

2 Όταν ο ανυποψίαστος χρήστης επισκέπτεται τη σελίδα, κατεβάζει το script το οποίο εκτελείται στο browser

3 Το Script συλλέγει credentials ή εμπιστευτικές πληροφορίες τις οποίες στέλνει στο hacker



Επίθεση Slow Client

Ο Hacker στέλνει πολλά ημιτελή αιτήματα HTTP

Τα αιτήματα μένουν ανοικτά μέσω πολύ αργού keepalive traffic

HTTPrequest

Κατηγορίες επιθέσεων σε Layer 7

Input Injection

- SQL patterns, scripts, metacharacters
- Virus, Malware

Session Attacks

- Cookie attacks, Cross Site Request Forgery (CSRF)

Denial of Service

- Length violations, buffer overflows
- Traffic based

Forceful Browsing

- Accessing unauthorized resources
- Hidden parameter violations

DIGITAL SIMA

T10 OWASP Top 10 Application Security Risks – 2013

A1 – Injection	Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
A2 – Broken Authentication and Session Management	Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.
A3 – Cross-Site Scripting (XSS)	XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
A4 – Insecure Direct Object References	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

www.owasp.org

Το Web Application Firewall της **Barracuda** προστατεύει συνολικά από απειλές σε Layer 7

DIGITAL SIMA

IPS και Network Firewalls σε Layer7

Ασφάλεια	IPS/FW
1. Injection attack protection (XSS, SQL)	Περιορισμένη
2. Normalize Encoded Traffic	ΟΧΙ
3. Inspect HTTPS traffic	ΟΧΙ
4. Session tampering/hijacking/riding protection	ΟΧΙ
5. Forceful Browsing Prevention	ΟΧΙ
6. Data Theft protection, Cloaking	ΟΧΙ
7. Brute-force protection	ΟΧΙ
8. Web Services Projection	ΟΧΙ
9. Application Layer DDoS Protection	ΟΧΙ
10. Rate Control Protection	ΟΧΙ

WAF & Network Firewall: συμπληρωματική προστασία DDoS

	Αντιμετώπιση Application DDoS Web Application Firewall		Αντιμετώπιση Network DDoS Network Firewall
√	Protocol anomaly detection (HTTP)	√	Protocol anomaly detection
√	HTTP GET, POST Floods	√	Packet flood mitigation - TCP, UDP, SIP, ICMP
√	HTTP "Slow Attacks" – Slowloris, R-U-Dead-Yet (RUDY), Slow Read Attack	√	SYN Flood Protection
√	LOIC, HOIC Protection	√	UDP Flood Protection
√	JS Challenges	√	ICPM Ping Floods, Smurf Protection
√	CAPTCHA Challenges	√	DNS Protection
√	Geo-location controls	√	Virtual Partitioning
√	Filtering anonymous proxies	√	Geo-location ACLs
√	SSL Inspection without exporting private keys off-site	√	Granular Inspection, Out of state filtering
√	IP Reputation feed	√	Granular layer 3 and 4 filtering
√	Building Excess Capacity	√	Defeating Bots by Blocking C&C communication
√	Session Rate Tracking		

DIGITAL SIMA

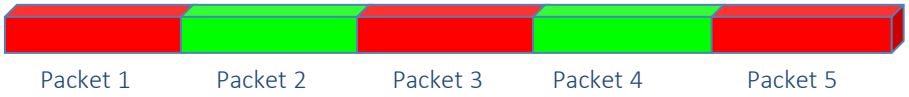
Τυπική Εγκατάσταση

Και στις δύο υλοποιήσεις μπορούμε να έχουμε δύο συσκευές σε Υψηλή διαθεσιμότητα

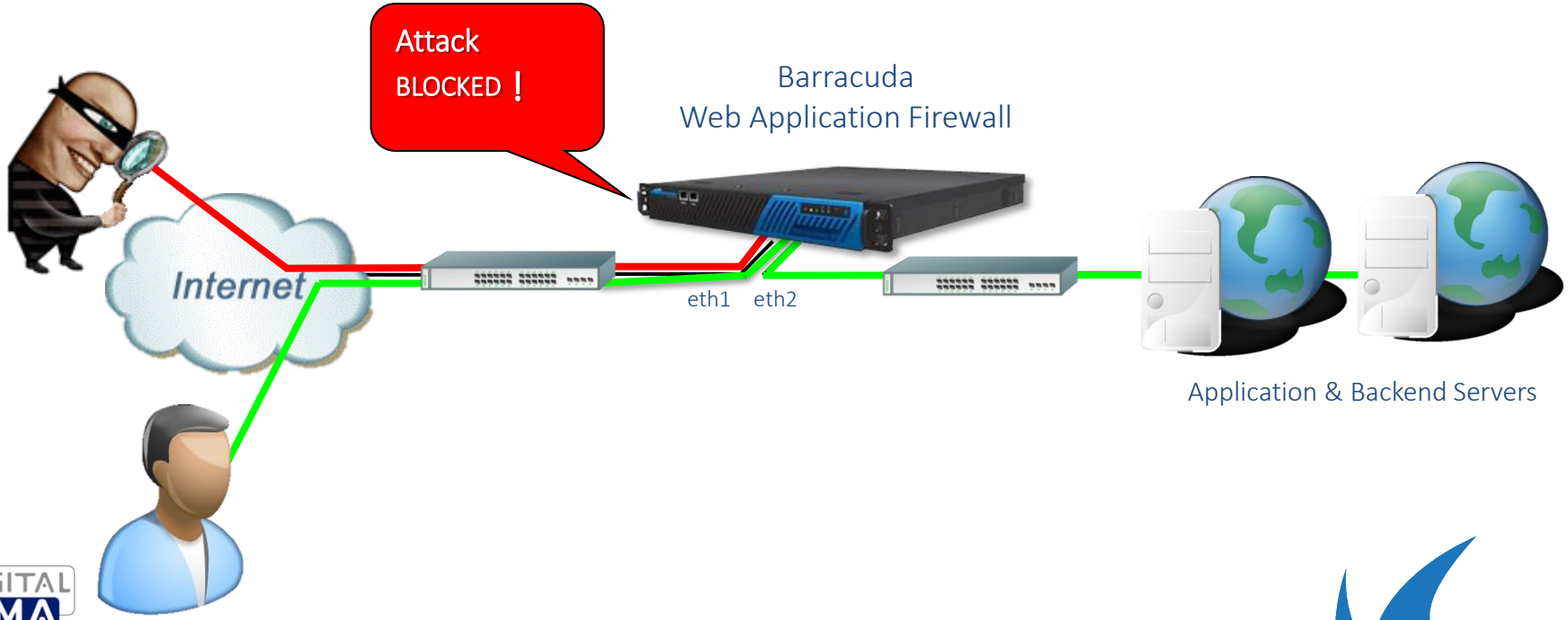
Inline μεταξύ του firewall και των servers σε Proxy ή Bridge mode

Out of line ως one armed proxy

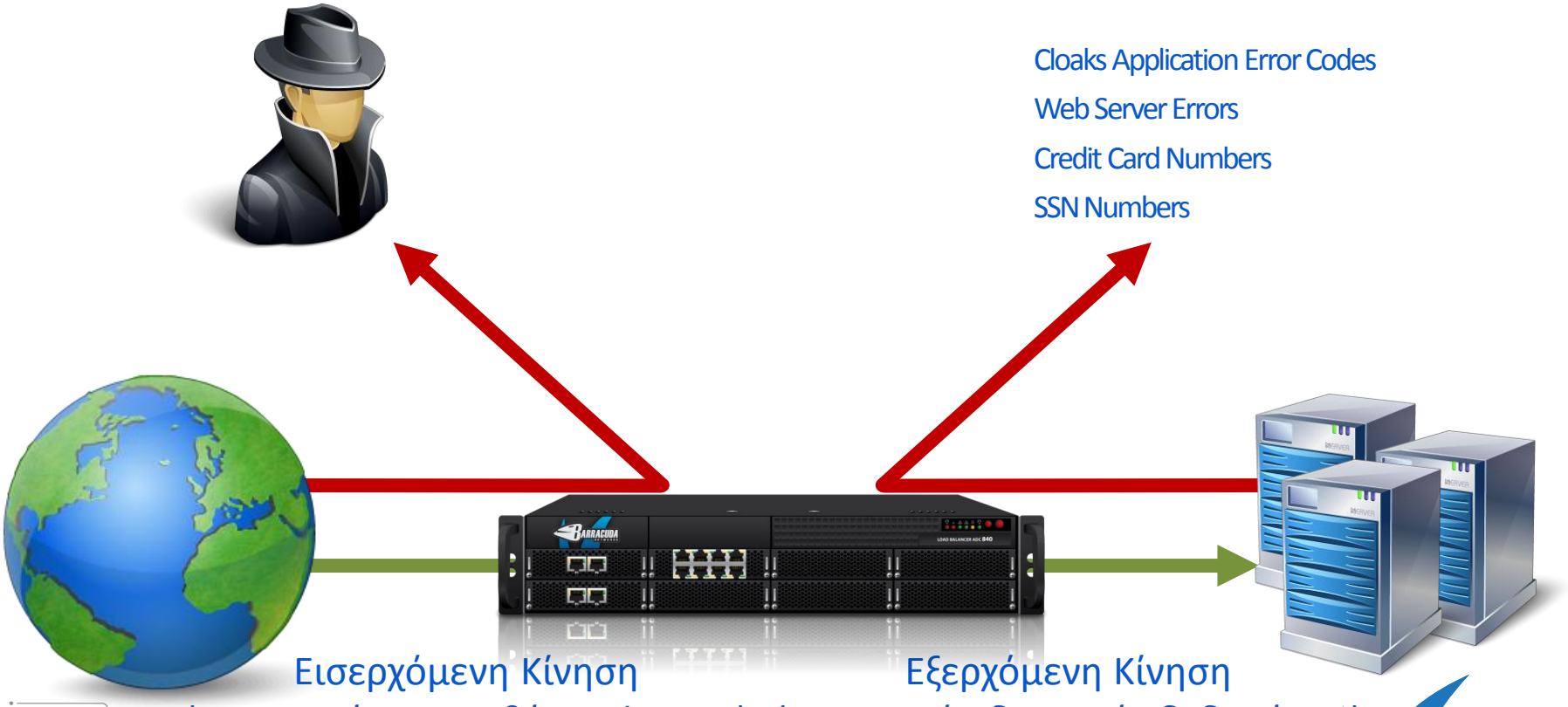
Πως λειτουργεί το Barracuda WAF



Το stream τερματίζεται, τα πακέτα ανασυντίθενται και ελέγχονται πριν προωθηθούν



Έλεγχοι ασφάλειας σε Layer 7



DIGITAL SIMA

Ενσωματώνονται 4 μηχανισμοί

Application Security

- OWASP Top 10 and beyond
- XML firewall, Cookie Security
- Positive Security Model
- DDoS and Bot protection
- Integrated Anit Virus
- Vulnerability scanner integration

Acceleration

- SSL-Offloading
- TCP-Pooling
- Caching
- Compression
- Rate Control
- Connection Multiplexing

Identity and Access Management

- Authentication & Authorization
- Single Sign On
- SSL Client Certificates
- One Time Passwords
- LDAP/AD, Kerberos, CA-Siteminder
- RADIUS, RSA SecureID

Traffic Management

- Load Balancing
- Session Persistence
- Health Monitors
- Content Routing
- Content Rewrite
- Instant SSL

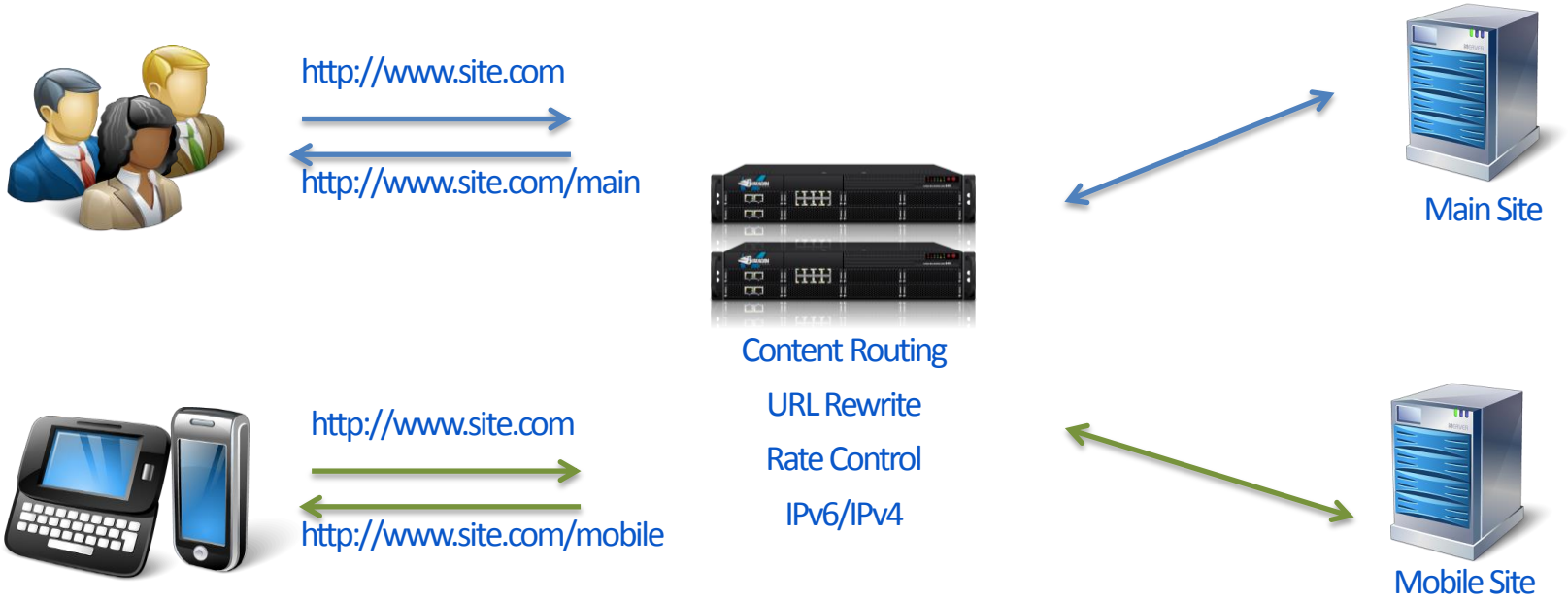
DIGITAL SIMA

WAF Models

MODEL COMPARISON	360	460	660	860	960
CAPACITY					
Backend Servers Supported	1-5	5-10	10-25	25-150	150-300
Throughput	25 Mbps	50 Mbps	200 Mbps	1 Gbps	4 Gbps
HARDWARE					
Form Factor	1U Mini	1U Mini	1U Fullsize	2U Fullsize	2U Fullsize
Dimensions (in)	16.8 x 1.7 x 14	16.8 x 1.7 x 14	16.8 x 1.7 x 22.6	17.4 x 3.5 x 25.5	17.4 x 3.5 x 25.5
Weight (lb)	12	12	26	46	52
Data Path Ports	2 x 10/100	2 x GbE	2 x GbE	2 x GbE[1]	2 x 10GbE[1]
Management Port	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100	1 x 10/100
AC Input Current (amps)	1.2	1.4	1.8	4.1	5.4
ECC Memory			●	●	●

WAF Features

MODEL COMPARISON	360	460	660	860	960
FEATURES					
Response Control	●	●	●	●	●
Outbound Data Theft Protection	●	●	●	●	●
File Upload Control	●	●	●	●	●
SSL Offloading	●	●	●	●	●
Authentication and Authorization	●	●	●	●	●
Vulnerability Scanner Integration	●	●	●	●	●
Protection Against DDos Attacks	●	●	●	●	●
Network Firewall	●	●	●	●	●
High Availability	Active/Passive	Active/Passive	Active/Active	Active/Active	Active/Active
Caching and Compression		●	●	●	●
LDAP/RADIUS Integration		●	●	●	●
Load Balancing		●	●	●	●
Content Routing		●	●	●	●
Advanced Routing			●	●	●
Adaptive Profiling			●	●	●
Antivirus for File Uploads			●	●	●
XML Firewall			●	●	●

DIGITAL SIMA

Customize Experience based on Client and Devices