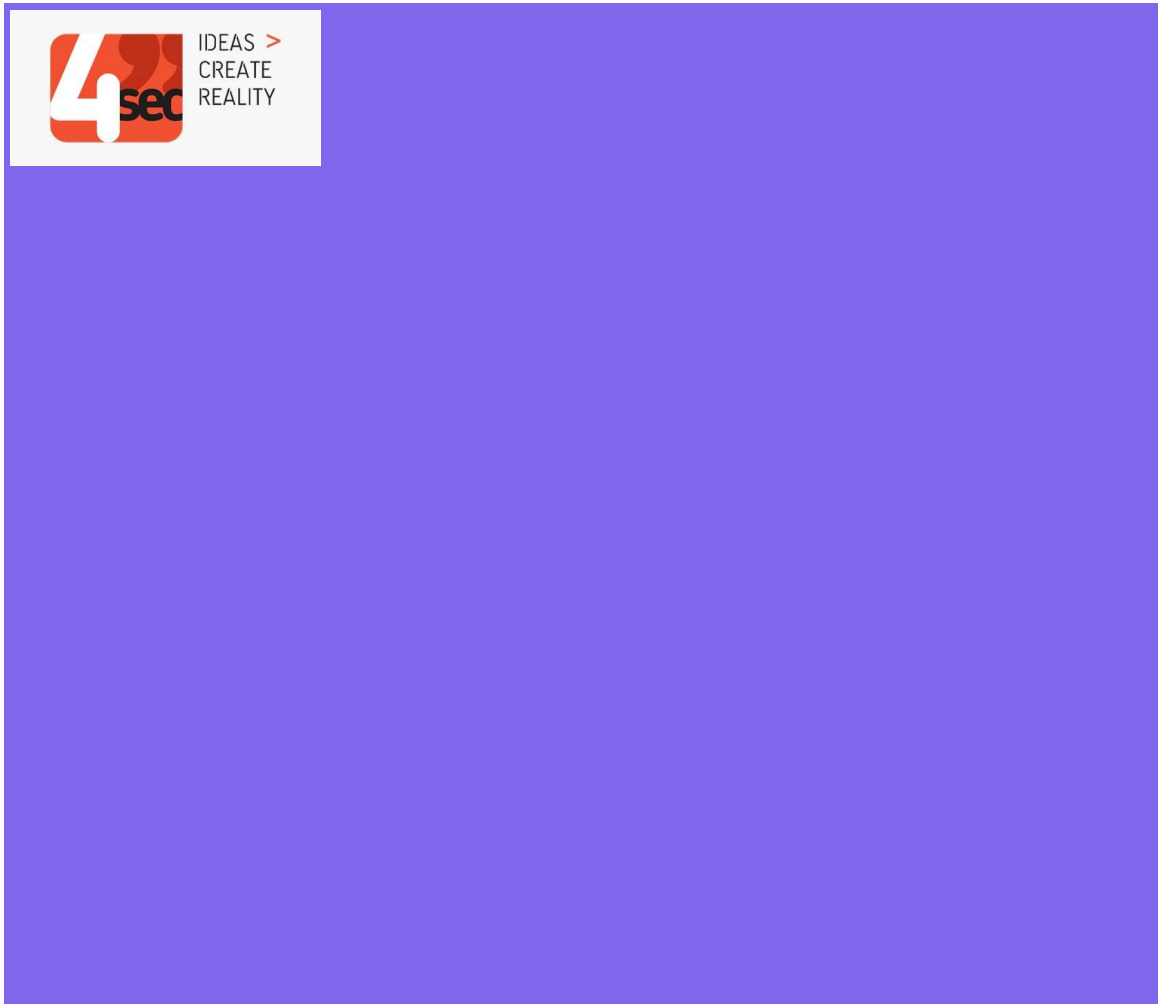


Array

ASF
Application Security Firewall

The Big Picture: Why Protect the Web Layer?

- **Front Door of Business are Web applications**
  - E-commerce, retail
  - Banks, financial services, and insurance
  - Government agencies, education, enterprises
  - Service providers
  - Application service providers and SaaS providers

- **Attacks to Web exploded: 70%+ of breaches hit the app layer**
  - Sensitive customer information becomes main target
  - SQL injection, cross-site scripting, cache overflow, CSRF, DoS are common attacks
  - More sophisticated attacks make protection more difficult

- **Compliance (PCI DSS etc)**

Why we still need WAF

- **Mission: changing the software development culture into one that produces more secure code!**

- one of the main reason for successful web attack is the lack of security checks in the code itself

Why we still need WAF

Application-Level Security

Defense-in-depth for business-critical resources and data.

Provides a superior combination of Layer 3 to **Layer 7** defense, with **behavior analysis** for HTTP and HTTPS.

Monitors changes in web apps and **updates** mathematical models constantly. .

Next-Gen FW & IPS/IDS

While able to block some common Web attacks, network-layer security is blind to application-level threats.

IPS/IDS lacks Layer-7 detection, they work on layer 3 and 4 (data and network traffic), and are signature-based. It's a defense for DNS, FTP, SMTP, SSH, Telnet.

Unified Threat Management

Aimed at SMB customers, is a jack of all trades and master of none w/ security and performance deficits.

UTM does not protect against Web 2.0 threats. Creates performance bottlenecks when called on to simultaneously support multiple security services at scale.

OWASP Top 10 Web Application Security Risks

- The Open Worldwide Application Security Project
- ranks the most critical security risks to web apps, and it's truly representative of the most significant current threats because it's built from data gathered from an industry-wide survey
- every 4 years new edition

2021
A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

Why aren't Signatures Enough? SQL Injection Example

How does SQL Injection work?
When submitting input to a web application a query is formed from the application to the database

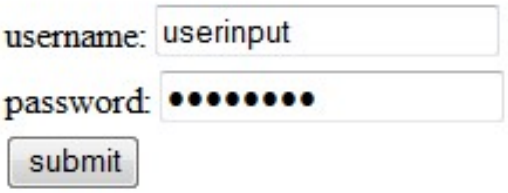
- Normal login request
  SQL query: *select * from user_table where username= ' userinput ' AND password=' userinput ';*

If the app doesn't perform input validation the attacker can manipulate the input to bypass authentication

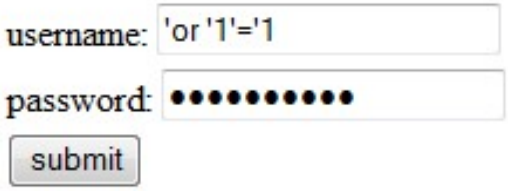
- Injection login request
  SQL query: *select * from user_table where username= ' ' OR ' 1'= ' 1' AND password= 'anything'*

Since OR 1=1 is always true, the entire WHERE statement will be true, and the database will return all rows from user table without checking the password.

What the developer intended:



What the developer didn't intend:



Why aren’t Signatures Enough?

Signatures are attack patterns that are matched against network traffic.

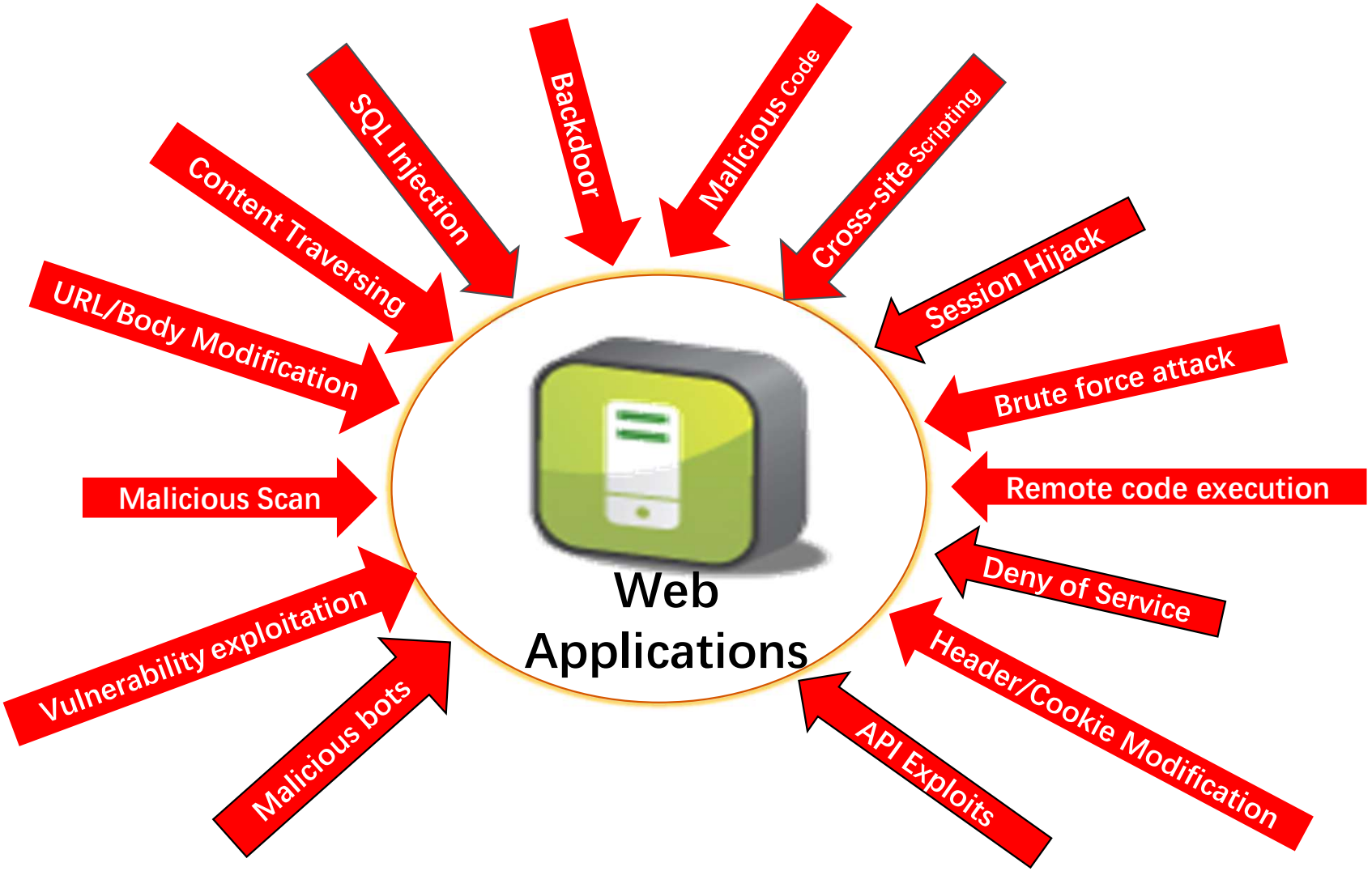
Using regular expressions can cover many of attack patterns but obviously not all.

Tightening the signatures would trigger false positives.

There would always be a possibility for signature evasion.

There must be another layer of protection to validate character input and identify threats!

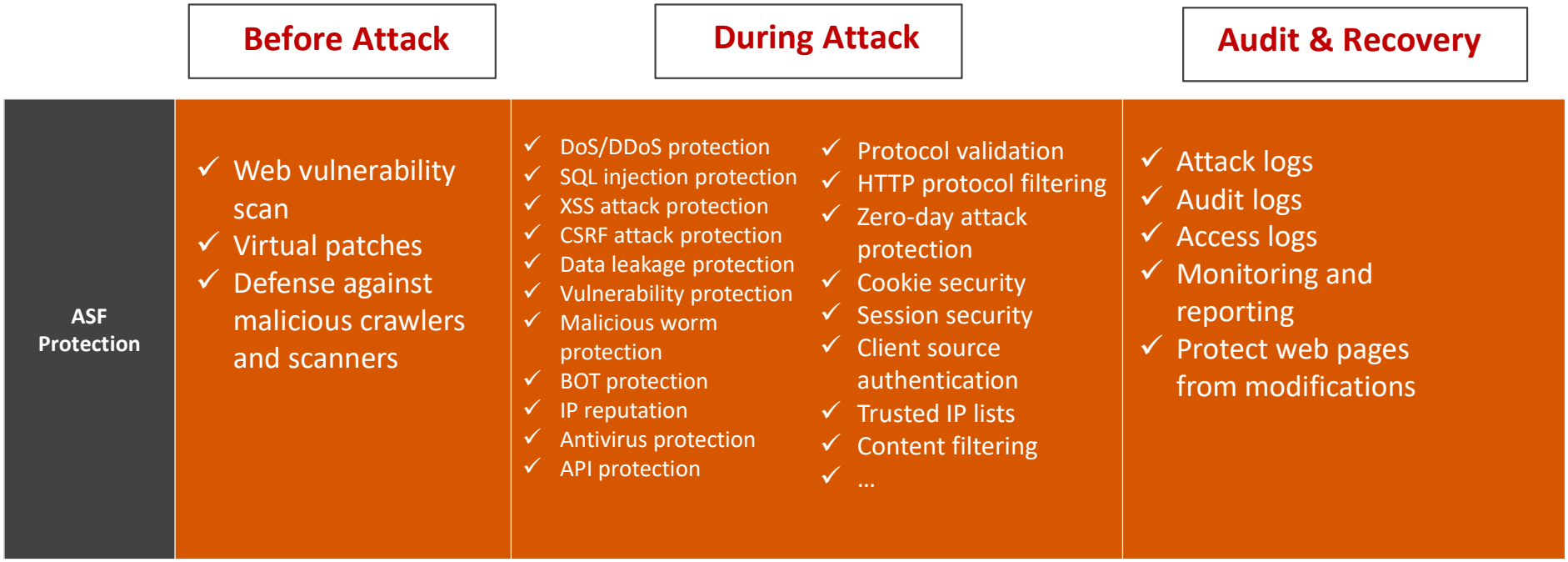
WAF Blocks Various Threats



Array WAF (ASF) Protects the Whole Cycle

	Reconnaissance	Attack	Damage
Attack cycle	☠ Reconnaissance ☠ Vulnerability scan	☠ SQL Injection ☠ Cross-site scripting ☠ Cross-site request forgery ☠ Deny of service ☠ Brute force ☠ Web page modification	☠ Loss of information ☠ Web page modification ☠ Service interruption ☠ Loss of property of fame

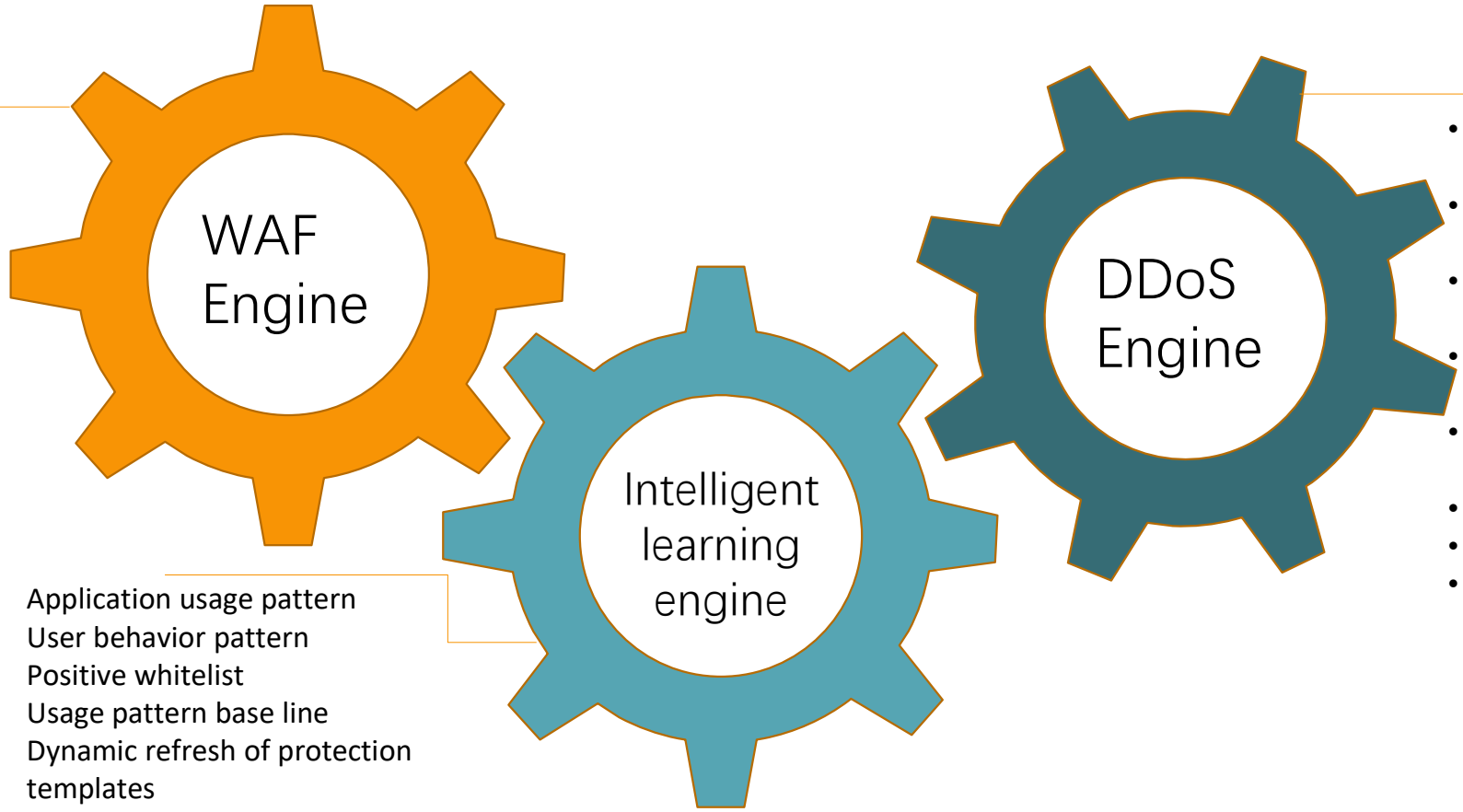
Array WAF (ASF) Protects the Whole Cycle



* Many diferrent security measures available in each cycle period

Protection with Multiple Engines

- Detection of attack signatures
- Data leakage Protection
- Content key word filtering
- Virtual patches
- HTTP protocol filtering
- Prevention of web page modification



- Application usage pattern
- User behavior pattern
- Positive whitelist
- Usage pattern base line
- Dynamic refresh of protection templates

- Network DDoS protection
- HTTP DDoS attack protection
- HTTPS DDoS attack protection
- Abnormal packet detection
- ACL(access control list)
- Black/whitelist
- IP credibility
- Access based on geo regions

Integration of Positive and Negative Security Models

Positive Security Model

- **Learning of application usage pattern**
- **Dynamic modeling – Hidden Markov model (machine learning)**
- **Positive whitelist creation**
- Automatic protection template refresh
- DDoS baseline learning and baseline formation
- DDoS template real-time refresh
- **Zero-day attack protection**

Negative Security Model

- **Attack protection based on signatures (built in library-ASL)**
- **Data leakage protection**
- Content key word filtering
- Virtual patches
- Protocol compliance check
- Source authentication and session monitoring
- Trusted IP address data base
- Advanced access control
- Static/dynamic white/blacklist
- DoS and DDoS attack protection
- **Abnormal packet detection**

Work /Deployment modes

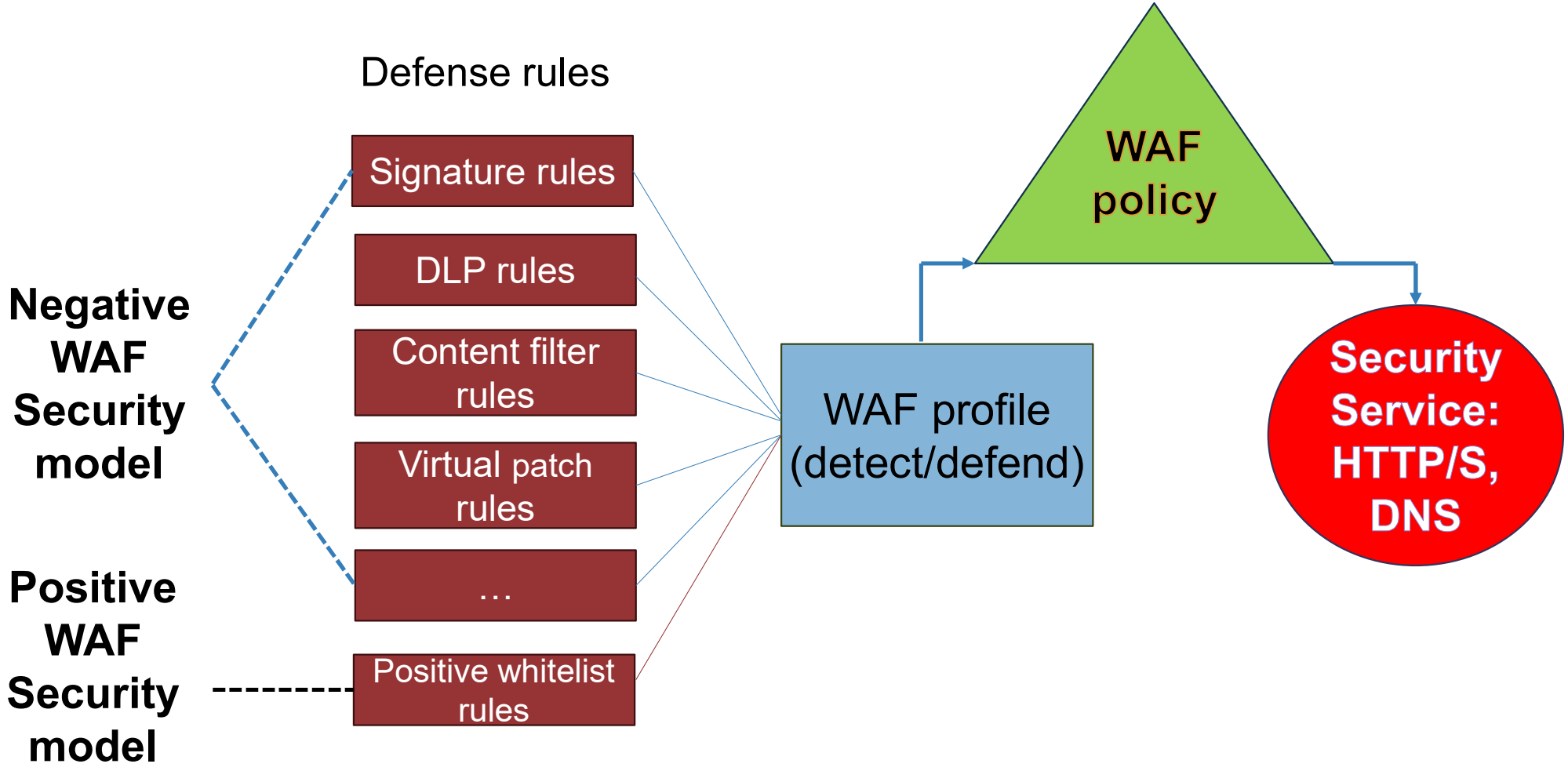
- Transparent
- Reverse proxy (Change source & Keep source)

Deployment	Transparent	Reverse proxy
Bridge	Yes	Yes
Routing	Yes	Yes
TAP	Yes	No

High Availability – Clustering (up to 32 hardware or virtual appliance)

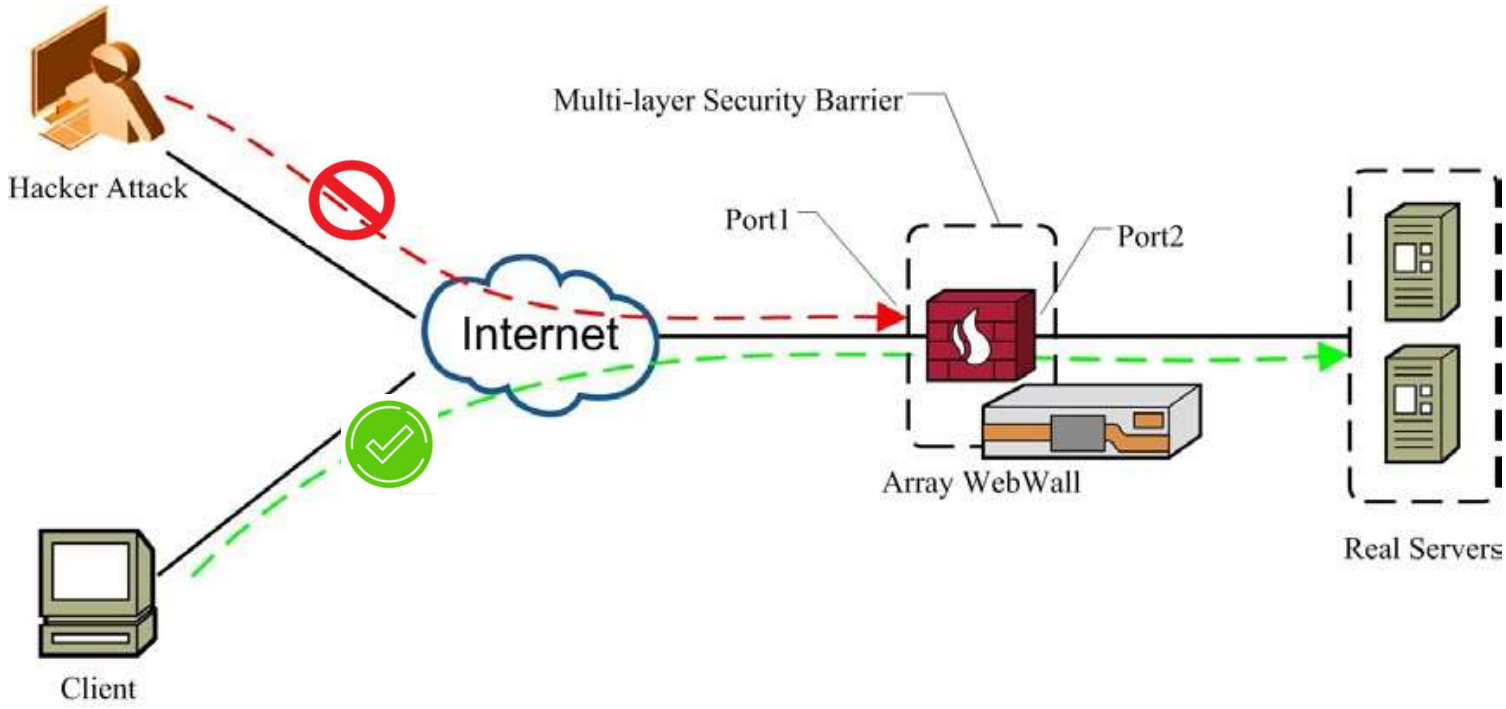
- Active-Active, Active-Standby
- Configuration sync, VRRP
- software and hardware bypass function

WAF Profile, Rule and Policy



Packet Filtering

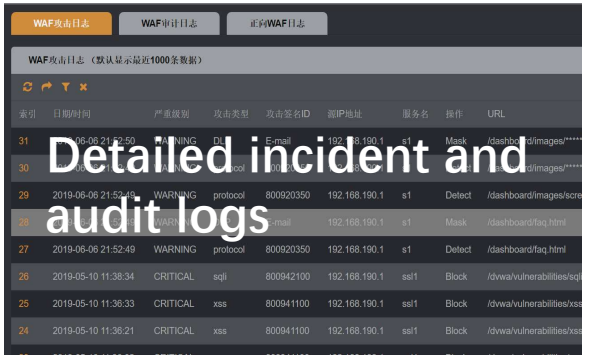
- **permit/deny rules** to filter packets passing through your network infrastructure
- filtering of **TCP, UDP and ICMP** packets that are using the **IPv4 or IPv6** address
- by default, the packet filtering function is disabled on every interface



Array Signature Library (ASL)

- ASL contains the **signatures of latest attacks**, including predefined signatures of negative and positive WAF.
- Array Security Center (ASC) will regularly release ASL versions in the form of ASL images.
- Manual/automatic download is possible with the subscription license of security update services. The ASL update is independent from the system update.

Data Visualization



Deployment Options

Software

WAF virtual appliances with support for popular hypervisors including VMware, Hyper-V and KVM. Available as permanent or subscription licenses.

Cloud

Available natively on industry-leading cloud platforms including AWS, Azure and Google Cloud. Supports utility consumption and BYOL license options.

Hardware

High availability appliances with Hardware SSL acceleration Multi-tenant network hyper-converged infrastructure for flexibility with performance.

Why Customers Choose ASF Series

Client-side Attack Prevention

DOM-based XSS
CSRF
Malicious script execution

Manual Attack Prevention

Probing parameters
Injecting data
Extracting data

Server-side Attack Prevention

Injection and scripting
RCE, OS command execution
API-based attacks

Automated Attack Prevention

Scanners and BOTS
Interceptors and proxies
Attack frameworks

Price-Performance & Value

Deploy in conjunction with Array load balancing for superior app delivery and security with best-in-class return on investment.

Array Networks At-a-Glance

Headquarters
Milpitas, CA

Technology
30+ Patents

Solutions
Web App & API Protection
SSL Visibility & Inspection
SSL VPN Remote Access
Load Balancer / Traffic Broker

Global Operations
Americas, Europe, India, Japan +

Markets
Enterprise, Service Providers,
Public Sector

Customers
6000+ Worldwide

amdocs
IBM Cloud
ORACLE
eClinicalWorks
bank hapoalim
UK2 a THG company
HITACHI Inspire the Next
MEDITECH
CBRE
Lilburn GEORGIA
DELTA DENTAL
Cathay Bank
icims
Beth Israel Deaconess Medical Center
LUTRON
DALLAS SYMPHONY ORCHESTRA
TRANSCORE
Peraton

IDEAS > CREATE REALITY

Thank You