

Advantages of Web Application Firewall on Distributed Environment



..... dincersalih.kurnaz@medianova.com 

Web Application Nedir?

Bir web tarayıcısı yada mobil uygulama üzerinden erişilebilen ve **web teknolojilerini kullanarak çalışan bir yazılımdır**. Web uygulamaları, kullanıcılar arasında bilgi paylaşımı, iş süreçleri otomasyonu, e-ticaret, eğitim, haberleşme ve daha birçok alanda çeşitli işlevleri yerine getirebilir.

Sunucu tarafında genellikle bir **programlama** dili (örneğin Python, Java, PHP, Ruby) kullanırlar.



Web uygulamalarının güvenlik **zorlukları** ve **ihtiyaçları**.

Developerların **Güvenli Kod** geliřtirmeleri gerek.

Kullanılan programlama dili, kütüphaneleri, 3.parti API'lerin zafiyetleri **Internet üzerinden gelen ve sadece atak olan isteklerin tespit ve engellenmesi** F/P leri yönetmek

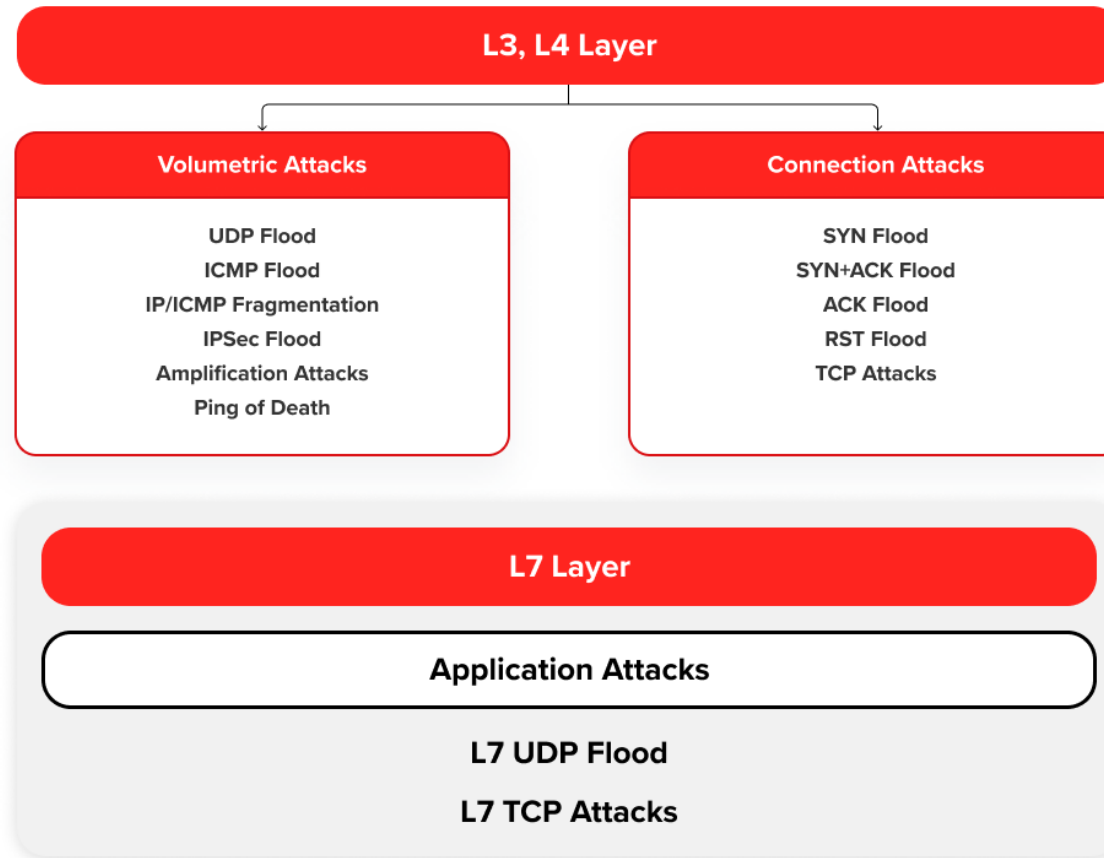


WAF Nedir?

- Web uygulamalarının güvenliğini artırmak için kullanılan bir tür güvenlik duvarıdır. WAF, web uygulamalarına yönelik saldırıları engeller ve koruma sağlar.



Katmanlı Koruma



WAF Temelleri:

- **Application Security (OSI 7)**
- WAF'in temel işlevleri ve nasıl **çalıştığı**.
- **HTTP** protokolünün WAF tarafından nasıl işlendiği.
- WAF'in çeşitli güvenlik kontrolleri ve saldırı tespit mekanizmaları. (**OWASP** Top 10)



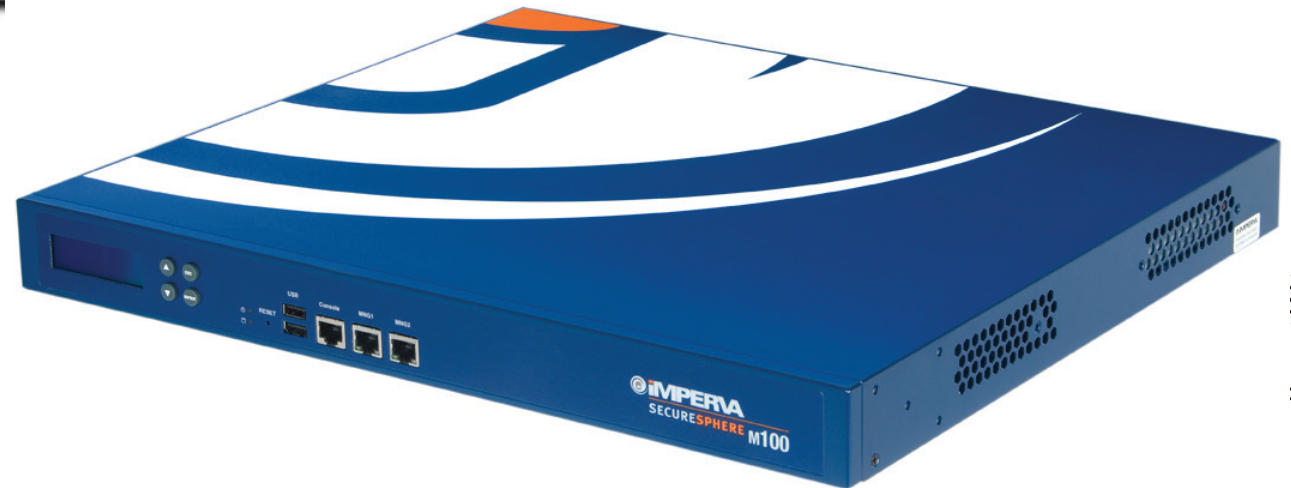
WAF Kullanım Senaryoları:

- SQL enjeksiyonu, XSS, RCE gibi yaygın saldırı türlerini **engelleme**.
- **Uygulama** katmanında güvenlik açıklarının kapatılması. WordPress, Drupal, Magento, OpenCart vb.



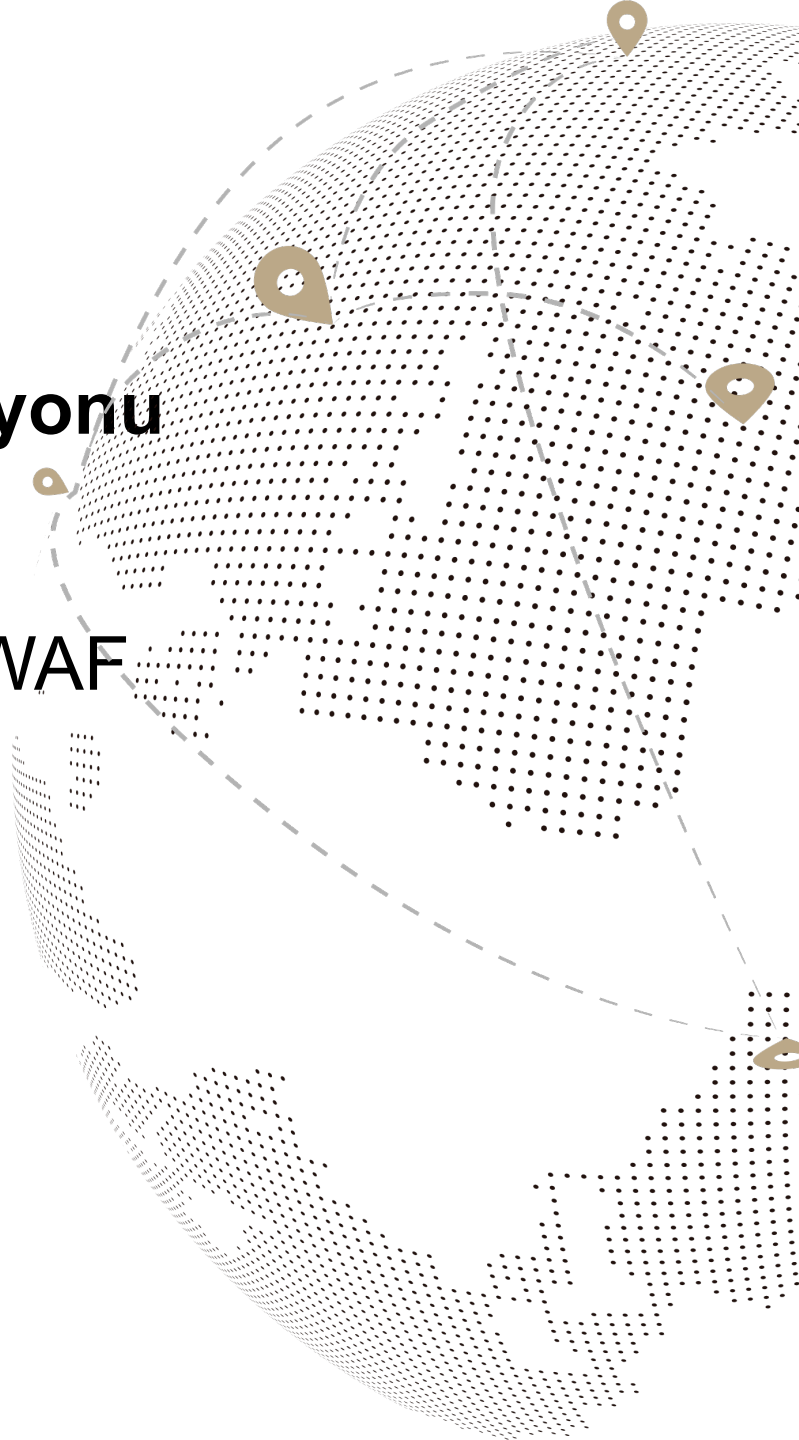
Traditional Methods

(Hardware Appliances)



WAF Yönetimi:

- WAF'in nasıl entegre edilebileceği, **konfigürasyonu** ve politika yönetimi.
- Saldırı imzalarının (Rules) **güncellenmesi** ve WAF politikalarının ayarlanması Lisans takibi.
- Yedeklilik ve **kapasite** yönetimi.
- Sistemin **7/24** monitor edilmesi



Distributed WAF (Cloud-based) peki nasıl?:

- Anycast DNS
- GSLB - Geo IP
- Advanced Load Balancer
- Edge computing
- Origin Shield

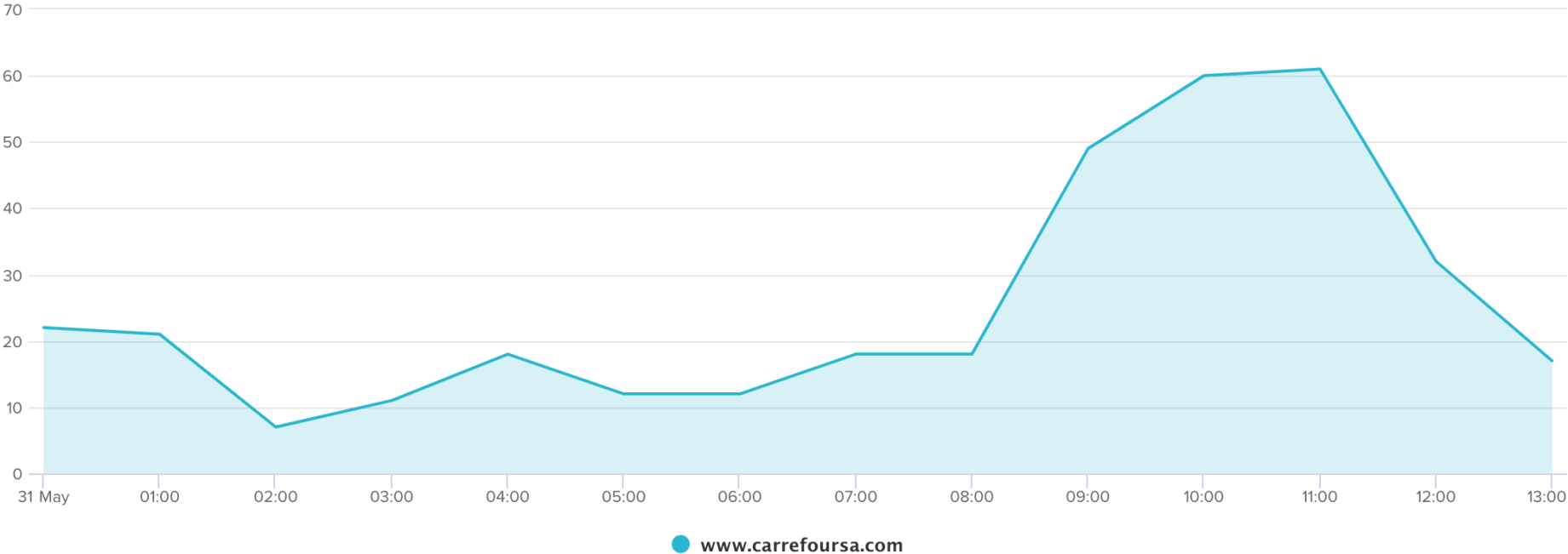


Distributed WAF Avantajları:

- **Entegrasyon Kolaylığı**
- Ölçeklenebilirlik ve Performans
- **Maliyet**
- Güncelleme ve Bakım



Attack Histogram



 Overview

 Analytics >

 CDN >

 Stook Object Storage

 **Security** v

☐ WAF

 MN Admin >

WAF

Every HTTP/HTTPS request will be checked against a set of rules. If the check succeeds, the HTTP request will be sent to the website in order to obtain the content. The event will be logged, if the check fails. In the "Monitor only" mode, no other actions will be performed. In the "On" mode, an error code will be sent in the HTTP response.

WAF Mode

On v

Rule name

When incoming requests match...

Field

Operator

Value

User Agent v

contain v

e.g. name=value

And

Choose an action

Block v

Add Rule

Submit

Sorular?

Teşekkürler.



dincersalih.kurnaz@medianova.com

