



Application Security	S07 T03	
	Deploying application firewalls	
<p>یکی از جنبه‌های مهم امنیت نرم‌افزارها در سرورهای لینوکسی، استفاده از دیوارهای آتش برنامه‌ای یا Web Application Firewalls (WAF) است. WAF ها ابزاری قدرتمند برای محافظت از برنامه‌های وب در برابر انواع حملات هستند. در این مقاله به معرفی مفهوم WAF ، اهمیت استفاده از آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.</p>		Understanding common application vulnerabilities
	بعد از	
		User and group security
	قبل از	
پیاده سازی عملی: <b>خیر</b>	پژوهشی: <b>بله</b>	راهنمای عملی: <b>بله</b>

## استقرار دیوارهای آتش برنامه‌ای (WAF) در لینوکس

یکی از جنبه‌های مهم امنیت نرم‌افزارها در سرورهای لینوکسی، استفاده از دیوارهای آتش برنامه‌ای یا Web Application Firewalls (WAF) است. WAF ها ابزاری قدرتمند برای محافظت از برنامه‌های وب در برابر انواع حملات هستند. در این مقاله به معرفی مفهوم WAF ، اهمیت استفاده از آن و روش‌های پیاده‌سازی آن در لینوکس می‌پردازیم.

## دیوار آتش برنامه‌ای (WAF) چیست؟

دیوار آتش برنامه‌ای (WAF) یک نوع دیوار آتش است که به طور خاص برای محافظت از برنامه‌های وب طراحی شده است. WAF با فیلتر کردن و مانیتورینگ ترافیک HTTP/HTTPS ورودی و خروجی، از برنامه‌های وب در برابر حملات رایج مانند SQL Injection ، Cross-Site Scripting (XSS) و حملات DDoS محافظت می‌کند.

## اهمیت استفاده از WAF

۱. **محافظت در برابر حملات رایج وب:** WAF ها می‌توانند به طور موثری از حملات رایج وب مانند تزریق SQL ، XSS و CSRF جلوگیری کنند.
۲. **مانیتورینگ و تحلیل ترافیک وب:** WAF ها به مدیران سیستم امکان می‌دهند تا ترافیک ورودی و خروجی برنامه‌های وب را مانیتور کنند و فعالیت‌های مشکوک را شناسایی کنند.
۳. **افزایش امنیت لایه‌ای:** استفاده از WAF به عنوان یک لایه اضافی امنیتی، می‌تواند به طور قابل توجهی امنیت کلی برنامه‌های وب را افزایش دهد.
۴. **حفاظت از داده‌های حساس:** WAF ها با جلوگیری از حملات مخرب، به حفاظت از داده‌های حساس کاربران و اطلاعات مالی کمک می‌کنند.

## روش‌های پیاده‌سازی WAF در لینوکس

### 1. ModSecurity:

ModSecurity یکی از محبوب‌ترین و پرکاربردترین WAF ها برای سرورهای وب است که با سرورهای وب آپاچی (Apache) و Nginx سازگار است. این ابزار قابلیت‌های گسترده‌ای برای فیلتر کردن و مانیتورینگ ترافیک وب ارائه می‌دهد.

#### ○ نصب ModSecurity در Apache

```
sudo apt-get install libapache2-mod-security2
```

سپس فایل پیکربندی ModSecurity را فعال کنید:

```
sudo a2enmod security2
```

```
sudo systemctl restart apache2
```

#### ○ نصب ModSecurity در Nginx

```
sudo apt-get install libnginx-mod-security
```

سپس تنظیمات ModSecurity را در فایل پیکربندی Nginx اضافه کنید:

```
http {  
  
    ...  
  
    include /etc/nginx/modsecurity/modsecurity.conf;  
  
    modsecurity on;  
  
    modsecurity_rules_file /etc/nginx/modsecurity/rules.conf;  
  
    ...  
  
}
```

## 2. NAXSI:

NAXSI (Nginx Anti XSS & SQL Injection) یک WAF سبک و قدرتمند برای Nginx است که به طور خاص برای جلوگیری از حملات XSS و SQL Injection طراحی شده است.

### ○ نصب NAXSI

```
sudo apt-get install nginx-naxsi
```

سپس تنظیمات NAXSI را در فایل پیکربندی Nginx اضافه کنید:

```
http {  
    ...  
    include /etc/nginx/naxsi_core.rules;  
    ...  
}  
  
server {  
    ...  
    location / {  
        include /etc/nginx/naxsi.rules;  
        ...  
    }  
}
```

### 3. Cloud-based WAF:

برخی از ارائه‌دهندگان خدمات ابری مانند Cloudflare و AWS WAF ، خدمات WAF مبتنی بر ابر ارائه می‌دهند. این خدمات نیاز به پیکربندی پیچیده ندارند و می‌توانند به سرعت برای محافظت از برنامه‌های وب استفاده شوند.

## نتیجه‌گیری

استقرار دیوارهای آتش برنامه‌ای (WAF) یکی از مهم‌ترین اقدامات برای افزایش امنیت برنامه‌های وب در سرورهای لینوکسی است. با استفاده از WAF ها می‌توان از حملات رایج وب جلوگیری کرد، ترافیک وب را مانیتور کرد و امنیت کلی برنامه‌های وب را بهبود بخشید. آشنایی و پیاده‌سازی صحیح این ابزارها به مدیران سیستم کمک می‌کند تا از داده‌های حساس خود محافظت کرده و از عملکرد بهینه سرورهای خود اطمینان حاصل کنند.

## منابع و ارجاعات

- <https://roadmap.sh/linux>
- <https://roadmap.sh/r/general-linux-server-hardening>