INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Licenciatura em Engenharia Informática
Tópicos de Engenharia Informática

WAF – Web Application Firewall

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Beja, março de 2025

INSTITUTO POLITÉCNICO DE BEJA
Escola Superior de Tecnologia e Gestão
Licenciatura em Engenharia Informática
Tópicos de Engenharia Informática

WAF – Web Application Firewall

Martinho José Novo Caeiro - 23917
Paulo António Tavares Abade - 23919

Orientador: Professor Armando Ventura

Beja, março de 2025

Resumo

Neste relatório será abordado o processo de instalação da máquina Servidor com o uso do AlmaLinux, os pacotes instalados e a configuração de DNS, Virtual Hosts e WAF para a realização do Projeto. Este relatório foi realizado no âmbito da Unidade Curricular de Tópicos de Engenharia Informática (IPBeja, 2025).

Keywords: almalinux, putty, dns, virtual hosts, waf

Abstract

In this report, we will address the installation process of the Server machine using AlmaLinux, the installed packages and the configuration of DNS, Virtual Hosts and WAF for the completion of the Project.

Keywords: almalinux, putty, dns, virtual hosts, waf

Índice

Índice de Figuras

1 Introdução

Para a realização do projeto é necessária a configuração de duas máquina AlmaLinux, Servidor e WAF. Em seguida são configurados os serviços DNS, Virtual Hosts e WAF. Para a configuração de todos estes serviços foi utilizado o Putty (Putty, 2025) que permitiu inserir comandos mais rapidamente.

2 Introdução Teórica

2.1 DNS

O DNS (Domain Name System) é um sistema hierárquico e distribuído que permite a resolução de nomes de domínio em endereços IP, permitindo que os utilizadores acedam a sites e serviços na Internet de forma mais fácil.

2.2 Virtual Hosts

Os Virtual Hosts permitem que um único servidor Apache hospede múltiplos sites ou aplicações web, cada um com o seu próprio nome de domínio e configuração. Isto é feito através da criação de entradas de configuração específicas para cada domínio.

2.3 WAF

O WAF (Web Application Firewall) é uma solução de segurança que protege aplicações web contra ataques e vulnerabilidades. Ele atua como uma camada adicional de defesa, analisando as requisições e respostas entre o cliente e o servidor, bloqueando atividades maliciosas e garantindo a integridade e confidencialidade dos dados.

3 Configuração de Máquinas

A instalação AlmaLinux (AlmaLinux, 2025) , foi feita na máquina Servidor com o uso de um .iso fornecido pelo docente da UC. Para a instalação foi necessário a criação de um disco de 8GB de espaço com três partições cujas quais são:

- Partição /boot - 500MB em ext4
- Partição swap - 1000MB
- Partição / - Resto do Disco em ext4

Informações adicionais incluem 1MB de RAM e dois processadores de CPU e a rede está em modo 'bridge'. No instalador foi definida a palavra-passe do 'root' como '1234', KDUMP desativado e nomes de rede 'server.tei.pt' e 'waf.tei.pt' para o Servidor e WAF respetivamente.

Figura 1: Exemplo de Maquina Utilizada

4 Instalação de Pacotes

A firewall foi desativada com o comando **systemctl disable –now firewalld** e desativado o SELinux, necessitando a edição do ficheiro **/etc/selinux/config** e alteração da linha **SELINUX=enforcing** para **SELINUX=disabled**. Adicionalmente, foi necessário instalar os seguintes pacotes para a configuração dos serviços:
Servidor:

- **nano** - Para a edição de ficheiros
- **whois** - Para verificar o IP da máquina
- **bind** - Para o DNS
- **bind-utils** - Para o DNS
- **httpd** - Para as Virtual Hosts
- **mod_ssl** - Para comunicações por SSL

WAF:

- **nano** - Para a edição de ficheiros
- **httpd** - Para as Virtual Hosts
- **mod_security** - Para o WAF
- **mod_security_crs** - Para o WAF
- **mod_geoip** - Para o WAF
- **GeoIP** - Para o WAF
- **GeoIPdata** - Para o WAF

5 Configuração de Serviços

5.1 DNS

Primeiramente é inicializado o DNS com o comando **systemctl enable –now named**. Em seguida, para a configuração do DNS, foram feitas as seguintes alterações no ficheiro **/etc/named.conf** com o uso do Putty:

- Adicionado *"any;"* nas linhas de *listen-on port 53* e *allow-query*;
- Adicionadas as zonas forward e reverse.

Zonas Forward

```
zone "trinta.org" {
    type master;
    file "/var/named/trinta.org.hosts";
};

zone "3emfrente.eu" {
    type master;
    file "/var/named/3emfrente.eu.hosts";
};

zone "the.com" {
    type master;
    file "/var/named/the.com.hosts";
};
```

Também necessitamos criar um ficheiro de configuração com caminho dado anteriormente em cada zona, cujos quais são:

Zonas Foward

```
nano /var/named/trinta.org.hosts
$TTL 38400
@   IN  SOA server.tei.pt. admin.tei.pt. (
1165190726 ; Serial
10800      ; Refresh
3600       ; Retry
604800     ; Expire
38400 )    ; Minimum TTL

 IN NS server.tei.pt.
server IN A 192.168.30.10
@ IN A 192.168.30.5
www IN A 192.168.30.5
www1 IN A 192.168.30.10
```

```
nano /var/named/3emfrente.eu.hosts
$TTL 38400
@   IN  SOA server.tei.pt. admin.tei.pt. (
1165190726 ; Serial
10800      ; Refresh
3600       ; Retry
604800     ; Expire
38400 )    ; Minimum TTL

 IN NS server.tei.pt.
server IN A 192.168.30.10
@ IN A 192.168.30.5
www IN A 192.168.30.5
www1 IN A 192.168.30.10
```

```
nano /var/named/the.com.hosts
$TTL 38400
@   IN  SOA server.tei.pt. admin.tei.pt. (
1165190726 ; Serial
10800      ; Refresh
3600       ; Retry
604800     ; Expire
38400 )    ; Minimum TTL

 IN NS server.tei.pt.
server IN A 192.168.30.10
@ IN A 192.168.30.5
www IN A 192.168.30.5
www1 IN A 192.168.30.10
```

Após serem configurados os ficheiros, é necessário reiniciar o serviço DNS com o comando **systemctl restart named**.

Figura 2: Demonstração de funcionamento do DNS

Como podemos verificar, o DNS está a funcionar corretamente.

5.2 Virtual Hosts

Primeiramente é necessária a criação de três utilizadores **trinta.org**, **3emfrente.eu** e **the.com** com a palavra-passe **123**. É em seguida, é necessário criar o ficheiro **/etc/httpd/conf/httpd.conf** com o seguinte conteúdo:

```
NameVirtualHost 192.168.30.10:80
<VirtualHost 192.168.30.10:80>
DocumentRoot "/home/trinta.org/"
ServerName www.trinta.org
ServerAlias trinta.org
<Directory "/home/trinta.org">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```
NameVirtualHost 192.168.30.10:443
<VirtualHost 192.168.30.10:443>
DocumentRoot "/home/trinta.org/"
ServerName www.trinta.org
ServerAlias trinta.org
<Directory "/home/trinta.org">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>

NameVirtualHost 192.168.30.10:80
<VirtualHost 192.168.30.10:80>
DocumentRoot "/home/3emfrente.eu/"
ServerName www.3emfrente.eu
ServerAlias 3emfrente.eu
<Directory "/home/3emfrente.eu">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```
NameVirtualHost 192.168.30.10:443
<VirtualHost 192.168.30.10:443>
DocumentRoot "/home/3emfrente.eu/"
ServerName www.3emfrente.eu
ServerAlias 3emfrente.eu
<Directory "/home/3emfrente.eu">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>

NameVirtualHost 192.168.30.10:80
<VirtualHost 192.168.30.10:80>
DocumentRoot "/home/the.com/"
ServerName www.the.com
ServerAlias the.com
<Directory "/home/the.com">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

```
NameVirtualHost 192.168.30.10:443
<VirtualHost 192.168.30.10:443>
DocumentRoot "/home/the.com/"
ServerName www.the.com
ServerAlias the.com
<Directory "/home/the.com">
Options Indexes FollowSymLinks
AllowOverride All
Order allow,deny
Allow from all
Require method GET POST OPTIONS
</Directory>
</VirtualHost>
```

Finalmente, é necessário criar as diretorias para cada um dos sites, com os seguintes comandos:

```
mkdir /home/trinta.org/public_html
mkdir /home/3emfrente.eu/public_html
mkdir /home/the.com/public_html
```

Após a criação das diretorias, é necessário criar um ficheiro **index.html** em cada um dos diretórios com o seguinte conteúdo:

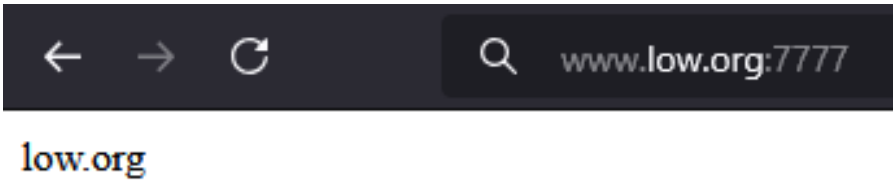

Figura 3: Demonstração dos Virtual Hosts

Como podemos verificar, após realizar os comandos **systemctl restart named** e **systemctl restart httpd** os sites já se encontram funcionais.

6 WAF

Para a configuração do WAF, foram feitas as seguintes alterações no ficheiro /**etc/httpd/conf.d/modsecurity.co**

```
SecRuleEngine On
SecAuditEngine On
SecAuditLog /var/log/httpd/modsec_audit.log
IncludeOptional modsecurity.d/*.conf
IncludeOptional modsecurity.d/activated_rules/*.conf
```

Na diretoria /**etc/modsecurity.d**/ foi adicionada a pasta **activated.rules**. Em seguida foi copiado o conteúdo da pasta /**usr/share/modsecurity-crs/base.rules/*** para a pasta **activated.rules**.

Finalmente, foram feitas as seguintes alterações no ficheiro /**etc/httpd/conf/httpd.conf**:

```
<VirtualHost *:80>
    ServerName www.trinta.org
    ProxyPreserveHost On
    ProxyPass / http://192.168.30.10:80/
    ProxyPassReverse / http://192.168.30.10:80/
</VirtualHost>

<VirtualHost *:80>
    ServerName www.3emfrente.eu
    ProxyPreserveHost On
    ProxyPass / http://192.168.30.10:80/
    ProxyPassReverse / http://192.168.30.10:80/
</VirtualHost>

<VirtualHost *:80>
    ServerName www.the.com
    ProxyPreserveHost On
```

```
    ProxyPass / http://192.168.30.10:80/
    ProxyPassReverse / http://192.168.30.10:80/
</VirtualHost>
```

7 Conclusão

Todos os serviços foram implementados com sucesso, dado que a sua maioria foi semelhante ao Laboratório 2 da Unidade Curricular de Administração de Sistemas. Este projeto permitiu adquirir conhecimentos sobre este Tópico e as diferentes possibilidades de manter os serviços seguros. Além disso, a configuração de WAF é essencial para garantir a segurança das aplicações web, protegendo-as contra ataques e vulnerabilidades.

Bibliografia

AlmaLinux. (2025). *Repositorio AlmaLinux* [Instalador AlmaLinux]. Obtido maio 19, 2025, de https://repo.almalinux.org/almalinux/8.10/isos/x86_64/AlmaLinux-8.10-x86_64-minimal.iso

IPBeja. (2025). *Disciplina: Tópicos de Engenharia Informatica / IPBeja* [Página TEI]. Obtido maio 19, 2025, de https://cms.ipbeja.pt/course/view.php?id=2775

Putty. (2025). *Download PuTTY: latest release (0.83)* [Instalador Putty]. Obtido maio 19, 2025, de https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html