



INFRAESTRUTURAS DEFENSIVAS

Aplicando Segurança em Camadas
com Firewall, WAF e SIEM



EQUIPE - PENTAGUARD IT


GABRIEL COSTA RA: 2302207
LUAN FERREIRA RA: 2102908



OBJETIVO

FOCO EM PROTEGER

aplicações e redes internas através de camadas de segurança, aplicando firewall, IDS/IPS, proxy reverso e SIEM – tudo isso de forma virtualizada.



OBJETIVO DO PROJETO

O projeto tem como objetivo proteger aplicações críticas da rede, implementando políticas de segurança e controle de tráfego com firewall, monitoramento de ataques com IDS/IPS, e visibilidade total via gerenciamento de logs com o Graylog. Toda a infraestrutura foi simulada no VirtualBox



TECNOLOGIAS UTILIZADAS

01

VIRTUALBOX

para virtualização de toda a infra

02

PFSENSE

firewall, controle de tráfego, DMZ, NAT

03

SNORT

IDS/IPS

04

GRAYLOG (SIEM)

centralização e análise de logs

05

WAF MODO SECURITY - NGINX

proteção a nível de aplicação via proxy reverso



PERÍMETRO E CONTROLE: PFSENSE

- Configuração do firewall
- Separação de redes (LAN, DMZ interna e externa)
- Regras de acesso personalizadas (BLOCK GERAL)
- Monitoramento de tráfego e alertas no PFSENSE

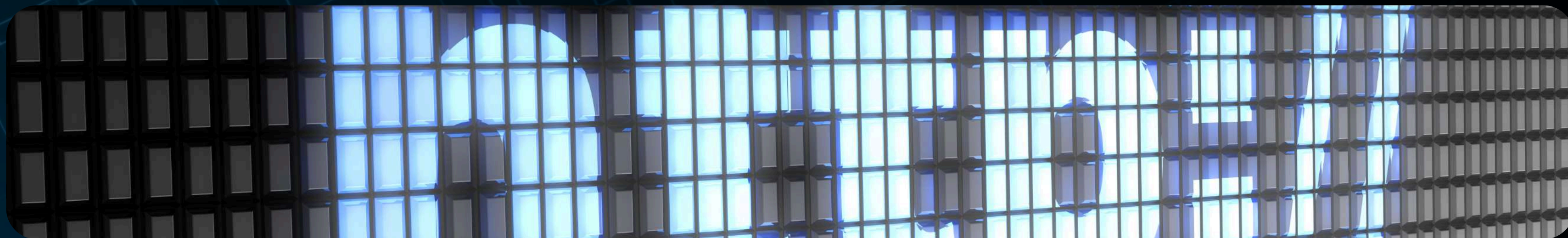




IDS E IPS

- Dentro do Firwall Ativação do IDS/IPS
- Instalação do pacote Snort e configuração
- Analise de trafego
- Respostas automatizadas ou manuais
- Logs integrados ao SIEM (GRAYLOG)





WAF E PROXY REVERSO

- Implantação de WAF como proxy reverso
- Redirecionamento de requisiçõesAnálise de tráfego
- Ocultação do IP real dos servidores
- Balanceamento de carga e mitigação de DoS



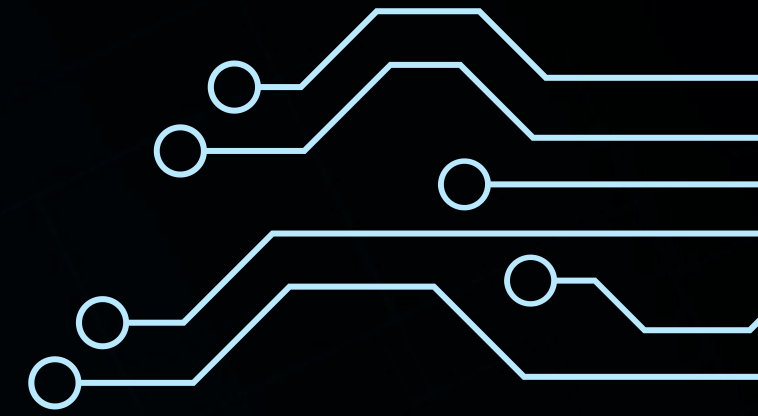


GRAYLOG (SIEM)

- Integração com firewall, IDS, WAF
- Visualização centralizada de logs
- Geração de alertas e relatórios



BENEFÍCIOS DA INFRAESTRUTURA CRIADA



- Segurança em camadas
- Balanceamento de carga via proxy reverso
- Prevenção de ataques DoS
- Controle e visibilidade total do tráfego
- Segmentação de rede com DMZ
- Monitoramento proativo com SIEM
- Estrutura escalável e adaptável
-

CONSIDERAÇÕES FINAIS

Através desse projeto, a equipe Pentaguard IT demonstrou como é possível montar uma infraestrutura robusta de defesa cibernética utilizando soluções de código aberto, com foco em controle, prevenção e monitoramento de ameaças, mesmo em ambientes virtualizados.

Com isso, mostramos a importância de pensar segurança como um todo, e não apenas como ferramenta isolada


```
firewall [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

INTERNET (wan) -> em0 -> v4/DHCP4: 192.168.0.7/24
INTRANET (lan) -> em1 -> v4: 192.168.56.10/24
DMZ (opt1) -> em2 -> v4: 172.100.1.10/24
DMZEXT (opt2) -> em3 -> v4: 172.100.2.10/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces          10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults 13) Update from console
5) Reboot system             14) Disable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell

Enter an option: █
```

```
WAF [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Debian GNU/Linux 11 server tty1

server login: root
Password:
Linux server 5.10.0-16-amd64 #1 SMP Debian 5.10.127-1 (2022-06-30) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun  5 14:17:57 -03 2025 on tty1
root@server:~#
```

```
Graylog [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
    valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
    valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 08:00:27:d3:71:b0 brd ff:ff:ff:ff:ff:ff
inet 172.100.1.101/24 brd 172.100.1.255 scope global enp0s3
    valid_lft forever preferred_lft forever
inet6 fe80::a00:27ff:fed3:71b0/64 scope link
    valid_lft forever preferred_lft forever
root@graylog:~# ss -tnl
State      Recv-Q    Send-Q      Local Address:Port      Peer Address:Port
UNCONN     0          0
*:1514     *:*
```

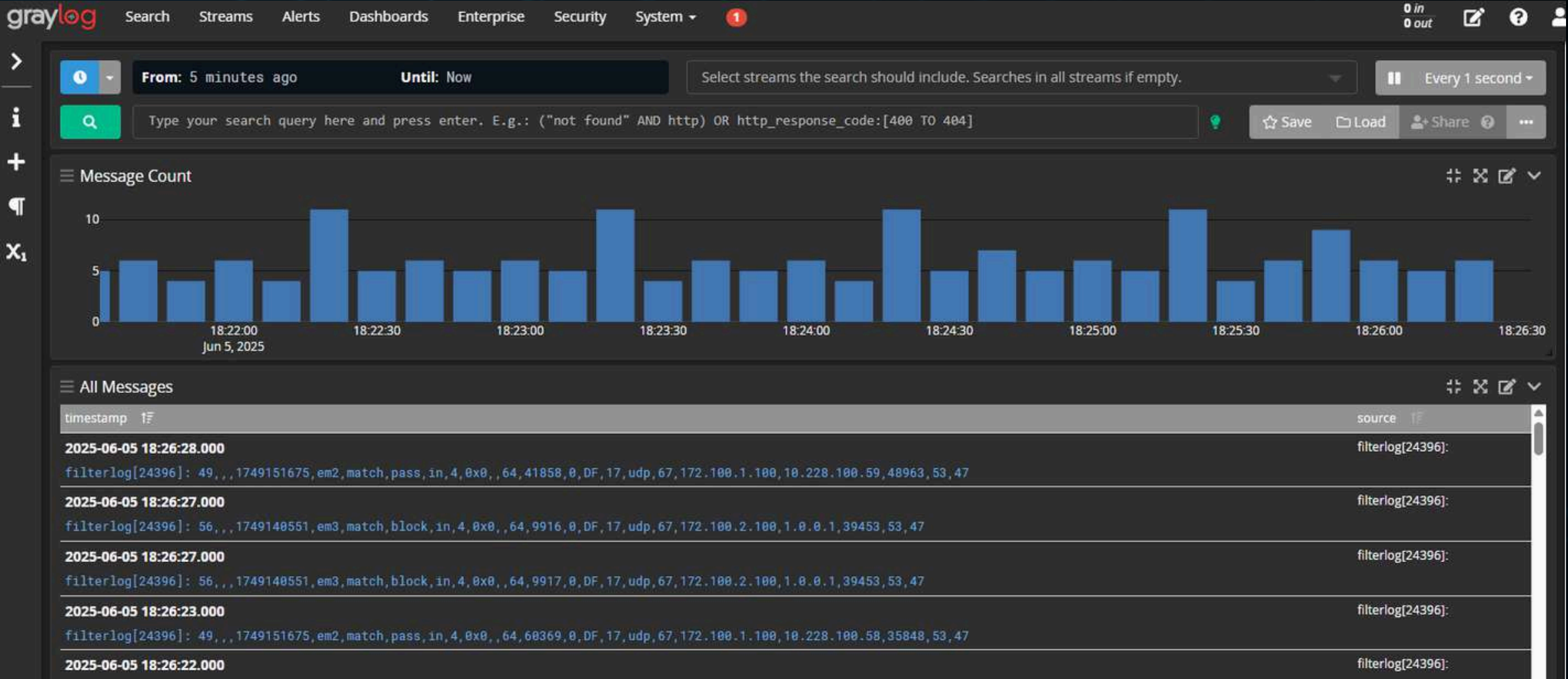
```
server [Executando] - Oracle VirtualBox
Arquivo Máquina Visualizar Entrada Dispositivos Ajuda

Debian GNU/Linux 11 server tty1

server login: root
Password:
Linux server 5.10.0-15-amd64 #1 SMP Debian 5.10.120-1 (2022-06-09) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jun  5 13:35:49 -03 2025 on tty1
root@server:~#
```

All Messages

timestamp	source
2025-06-05 18:26:49.000	filterlog[24396]:
filterlog[24396]: 49,,,1749151675,em2,match,pass,in,4,0x0,,64,253,0,DF,17,udp,67,172.100.1.100,10.228.100.59,52717,53,47	
<div><div><div></div><div>c9a97490-4253-11f0-948f-080027d371b0</div></div><div>PermalinkShow surrounding messagesTest against streamCopy ID</div></div>	
<div><div><div><div>Timestamp</div><div>2025-06-05 18:26:49.000</div></div><div><div>Received by</div><div>SYSLOG 1514 on 53102f8e / graylog.lab</div></div><div><div>Stored in index</div><div>graylog_0</div></div><div><div>Routed into streams</div><div><div>All messages</div></div></div></div><div><div><div>facility</div><div>local0</div></div><div><div>facility_num</div><div>16</div></div><div><div>level</div><div>6</div></div><div><div>message</div><div>filterlog[24396]: 49,,,1749151675,em2,match,pass,in,4,0x0,,64,253,0,DF,17,udp,67,172.100.1.100,10.228.100.59,52717,53,47</div></div><div><div>source</div><div>filterlog[24396]:</div></div><div><div>timestamp</div><div>2025-06-05 18:26:49.000</div></div></div></div>	
2025-06-05 18:26:48.000	filterlog[24396]:
filterlog[24396]: 56,,,1749140551,em3,match,block,in,4,0x0,,64,44759,0,DF,17,udp,67,172.100.2.100,1.0.0.1,54119,53,47	
2025-06-05 18:26:48.000	filterlog[24396]:
filterlog[24396]: 43,,,1657762948,em0,match,block,in,4,0xc0,,1,47975,0,DF,2,igmp,36,192.168.0.1,224.0.0.1,datalength=12	

Status / Dashboard



System Information



Name	lab.local
User	admin@192.168.56.1 (Local Database)
System	KVM Guest Netgate Device ID: 396ca86824b59eeb5707
BIOS	Vendor: innotek GmbH Version: VirtualBox Release Date: Fri Dec 1 2006
Version	2.6.0-RELEASE (amd64) built on Mon Jan 31 19:57:53 UTC 2022 FreeBSD 12.3-STABLE Version 2.7.0 is available. Version information updated at Thu Jun 5 16:49:53 -03 2025
CPU Type	Intel(R) Core(TM) i5-6300U CPU @ 2.40GHz AES-NI CPU Crypto: Yes (inactive) QAT Crypto: No
Hardware crypto	
Kernel PTI	Enabled
MDS Mitigation	Inactive
Uptime	01 Hour 38 Minutes 32 Seconds
Current date/time	Thu Jun 5 18:27:30 -03 2025

Interfaces

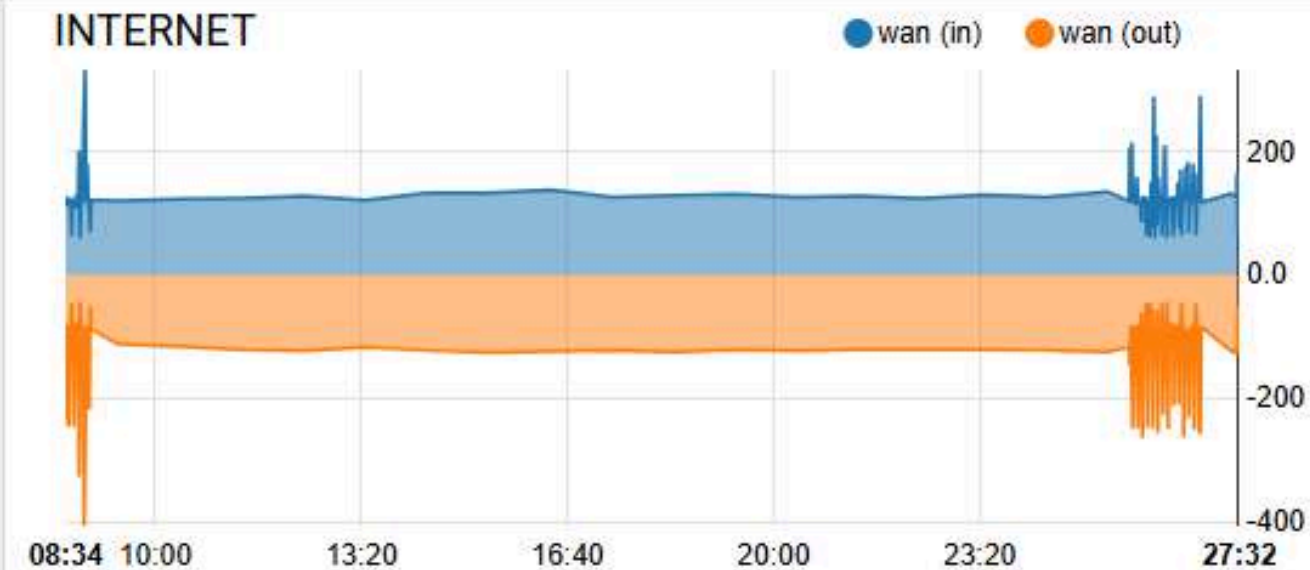


INTERNET	↑	1000baseT <full-duplex>	192.168.0.7
INTRANET	↑	1000baseT <full-duplex>	192.168.56.10
DMZ	↑	1000baseT <full-duplex>	172.100.1.10
DMZEXT	↑	1000baseT <full-duplex>	172.100.2.10

Traffic Graphs



INTERNET



INTRANET

