

Visão Geral

O SecureLog FortiGate realiza o monitoramento em tempo real dos logs de autenticação enviados pelo FortiGate via protocolo Syslog para um servidor Linux.

No back-end, um script em Python processa os logs recebidos e identifica eventos como:

- Usuário inválido
- Senha incorreta
- Login bem-sucedido

Os dados são registrados em um arquivo .txt, que serve como base para exibição no front-end. O front-end é uma página HTML única que lê o arquivo de log e exibe as informações atualizadas em tempo real. O servidor Linux também executa Apache e PHP, viabilizando funções adicionais, como o botão "Deletar Logs", que limpa o arquivo de forma segura via script PHP.

1º Instale os pacotes necessários:

```
apt update && apt upgrade -y && apt install apache2 python3 python3-pip python3-venv unzip rsyslog php -y && systemctl enable apache2 && timedatectl set-timezone America/Sao_Paulo
```

2º Extraia o pacote

```
rm /var/www/html/index.html  
unzip SecureLog_FortiGate_v2.4.5_Trial.zip -d /var/www/html
```

3º Ajuste permissões

```
cd /var/www/  
chown -R www-data:www-data html/  
cd /var/www/html/
```

4º Configure o Rsyslog

Edite o arquivo:

```
vim /etc/rsyslog.conf
```

E descomente:

```
module(load="imudp")  
input(type="imudp" port="514")
```

```
module(load="imtcp")  
input(type="imtcp" port="514")
```

5º Habilite o serviço

```
systemctl enable rsyslog  
systemctl restart rsyslog
```

6º Iniciar SecureLog

```
python3 securelog.py
```

7º Configuração no FortiGate

Menu: Log & Report > Log Settings > Global Settings

- Syslog logging: Enable
- IP address/FQDN: IP_do_servidor_SecureLog
- Apply

8º Acesso ao Painel Web

- URL: 127.0.0.1
- Usuário: admin
- Senha: Secure@Log#