

**PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS**  
**PUC Minas Virtual**

**Nome completo dos autores**

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**GESTÃO PARA A SEGURANÇA**

**Belo Horizonte**

**2023**

**Nome completo dos autores**

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

## **GESTÃO PARA A SEGURANÇA**

**Relatório apresentado no Eixo 4 – Gestão para a Segurança do curso superior de Tecnologia em Segurança da Informação, como requisito avaliativo.**

**Orientador: Luiz Alberto Ferreira Gomes.**

LISTA DE FIGURAS

Figura 1 - UTM - Regra 1 - Passo 1 .....	9
Figura 2 - UTM - Regra 1 - Passo 2 .....	10
Figura 3 - UTM - Regra 1 - Passo 3 .....	11
Figura 4 - UTM - Regra 1 - Passo 4 .....	12
Figura 5 - UTM - Regra 2 - Passo 1 .....	13
Figura 6 - UTM - Regra 2 - Passo 2 .....	14
Figura 7 - UTM - Regra 2 - Passo 3 .....	15
Figura 8 - UTM - Regra 2 - Passo 4 .....	15
Figura 9 - UTM - Regra 2 - Passo 5 .....	16
Figura 10 - IDS - Passo 1 .....	17
Figura 11 - IDS - Passo 2 .....	18
Figura 12 - IDS - Passo 3 .....	19
Figura 13 - IDS - Passo 4 .....	19
Figura 14 - IDS - Passo 5A .....	20
Figura 15 - IDS - Passo 5B .....	21
Figura 16 - IDS - Passo 6 .....	22
Figura 17 - IDS - Passo 7 .....	22
Figura 18 - Backup - Passo 1 .....	24
Figura 19 - Backup - Passo 2 .....	24
Figura 20 - Backup - Passo 3A .....	26
Figura 21 - Backup - Passo 3B .....	27
Figura 22 - Backup - Passo 4 .....	27
Figura 23 - Backup - Passo 5 .....	28
Figura 24 - Backup - Passo 6 .....	28
Figura 25 - Log - Passo 1 .....	30
Figura 26 - Log - Passo 2 .....	30
Figura 27 - Log - Passo 3A .....	31
Figura 28 - Log - Passo 3B .....	32
Figura 29 - Log - Passo 4 .....	32
Figura 30 - Log - Passo 5 .....	33
Figura 31 - Log - Passo 6 .....	33
Figura 32 - Log - Passo 7 .....	34
Figura 33 - Log - Passo 8 .....	34
Figura 34 - Teste de Penetração - Passo 1 .....	36
Figura 35 - Teste de Penetração - Passo 2 .....	37
Figura 36 - Teste de Penetração - Passo 3 .....	38
Figura 37 - Teste de Penetração - Passo 4 .....	39

## SUMÁRIO

<b>1 INTRODUÇÃO .....</b>	<b>6</b>
<b>2 OBJETIVOS .....</b>	<b>8</b>
2.1 OBJETIVO GERAL .....	8
2.2 OBJETIVOS ESPECÍFICOS .....	8
<b>3 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA UTM .....</b>	<b>9</b>
3.1 FERRAMENTA UTILIZADA: PFSense .....	9
3.2 REGRA 1 .....	9
3.3 REGRA 2: .....	12
<b>4 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA IDS .....</b>	<b>17</b>
4.1 FERRAMENTA UTILIZADA: PFSense. ....	17
4.2 CONFIGURAÇÃO .....	17
<b>5 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA DE BACKUP .....</b>	<b>24</b>
5.1 FERRAMENTA UTILIZADA: CARBONITE. ....	24
5.2 CONFIGURAÇÃO .....	24
<b>6 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA DE LOGS .....</b>	<b>30</b>
6.1 FERRAMENTA UTILIZADA: GRAYLOG. ....	30
6.2 CONFIGURAÇÃO .....	30
<b>7 PROCEDIMENTO PARA UTILIZAR FERRAMENTA DE TESTE DE PENETRAÇÃO .....</b>	<b>36</b>
7.1 FERRAMENTA UTILIZADA: ZED ATTACK PROXY (ZAP). ....	36
7.2 CONFIGURAÇÃO .....	36

## 1 INTRODUÇÃO

Este relatório refere-se ao projeto organizado para atender os requisitos da Etapa 2 do Projeto para estabelecer a [REDACTED] Para tanto, serão apresentadas as ferramentas para as quais foram elaborados procedimentos de utilização, considerando a realidade [REDACTED]

A primeira ferramenta escolhida foi UTM (Unified Threat Management, ou Central Unificada de Gerenciamento de Ameaças, em português) da PF Sense, uma solução gratuita e que possui vasta documentação. Esta se destaca por possuir diversas funcionalidades, sendo o firewall a mais utilizada em qualquer porte de empresa. Neste projeto, foram utilizadas as funções Firewall e IDS (Intrusion Detection System).

Na linguagem dos especialistas em Segurança da Informação, a disponibilização dos pacotes para as mais diversas funções credencia o pfSense como um UTM. São exemplos destas funções:

- firewall;
- servidor (internet, DHCP, NTP, Proxy...);
- antivírus;
- antispymware;
- antispam;
- filtragem de conteúdo;
- detecção de intrusão, entre outros.

A segunda ferramenta escolhida foi a Carbonite uma empresa americana que oferece um serviço de backup online, disponível para usuários de Windows e macOS. Em 2019, foi adquirido pela empresa canadense de software OpenText. Ele faz backup de documentos, e-mails, músicas, fotos e configurações. Além disso, este serviço possibilita fazer cópia de arquivos individuais, pastas inteiras e até mesmo de todo o sistema operacional de uma única vez.

Ele também oferece funcionalidades adicionais como recuperação de desastres, acesso remoto e compartilhamento de arquivos, tornando-se uma solução robusta para proteção de dados. Vale destacar que o Carbonite é executado continuamente, assim, sempre que algum arquivo for criado ou modificado, ele será automaticamente salvo no servidor em nuvem.

A terceira ferramenta escolhida foi a Graylog, uma plataforma web de código aberto para gerenciamento de log para coleta, indexação e análise de dados estruturados e não estruturados de quase qualquer fonte. Com esta ferramenta, evita-se tanto a perda de dados quanto possibilita a gestão dos tantos logs do projeto. Os logs são dados sigilosos e muitas vezes cruciais na hora de otimizar o tempo. Alguns exemplos de como utilizar a ferramenta:

- Analisar registros de segurança, como logs de firewall, logs de autenticação e registros de eventos de segurança, a fim de detectar atividades suspeitas ou tentativas de invasão.
- Registre logs de aplicativos e sistemas para ajudar a identificar e resolver problemas de software, como erros, exceções e comportamentos inesperados.

A última ferramenta escolhida foi a Zed Attack Proxy (ZAP), uma solução de segurança gratuita, de código aberto e das mais populares do mundo, que é mantida ativamente por uma equipe internacional dedicada de voluntários, mantida pela OWASP (Open Web Application Security Project). Enquanto aplicativos estão sendo desenvolvidos e testados, a ferramenta ajuda a detectar automaticamente uma ampla variedade de vulnerabilidades de segurança em seus aplicativos da web, como injeções SQL, cross-site scripting (XSS), cross-site request forgery (CSRF) e muitas outras.

Além disso, o ZAP oferece recursos para explorar manualmente as aplicações da web, permitindo que os testadores investiguem mais a fundo e encontrem vulnerabilidades específicas. Ele também suporta a automação por meio de APIs (Application Programming Interface), facilitando a integração com pipelines de desenvolvimento ágil.

## **2 OBJETIVOS**

### **2.1 Objetivo Geral**

- Elaboração do Plano Detecção, Mitigação e Acompanhamento de Ameaças.

### **2.2 Objetivos Específicos**

- Elaborar procedimentos de Unified Threat Management;
- Elaboração de procedimento de detecção de instrução;
- Elaboração um procedimento de backup e recuperação;
- Elaboração de procedimento de registro de análise de logs;
- Elaboração de um procedimento de testes de segurança.

### 3 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA UTM

#### 3.1 Ferramenta utilizada: Pfsense

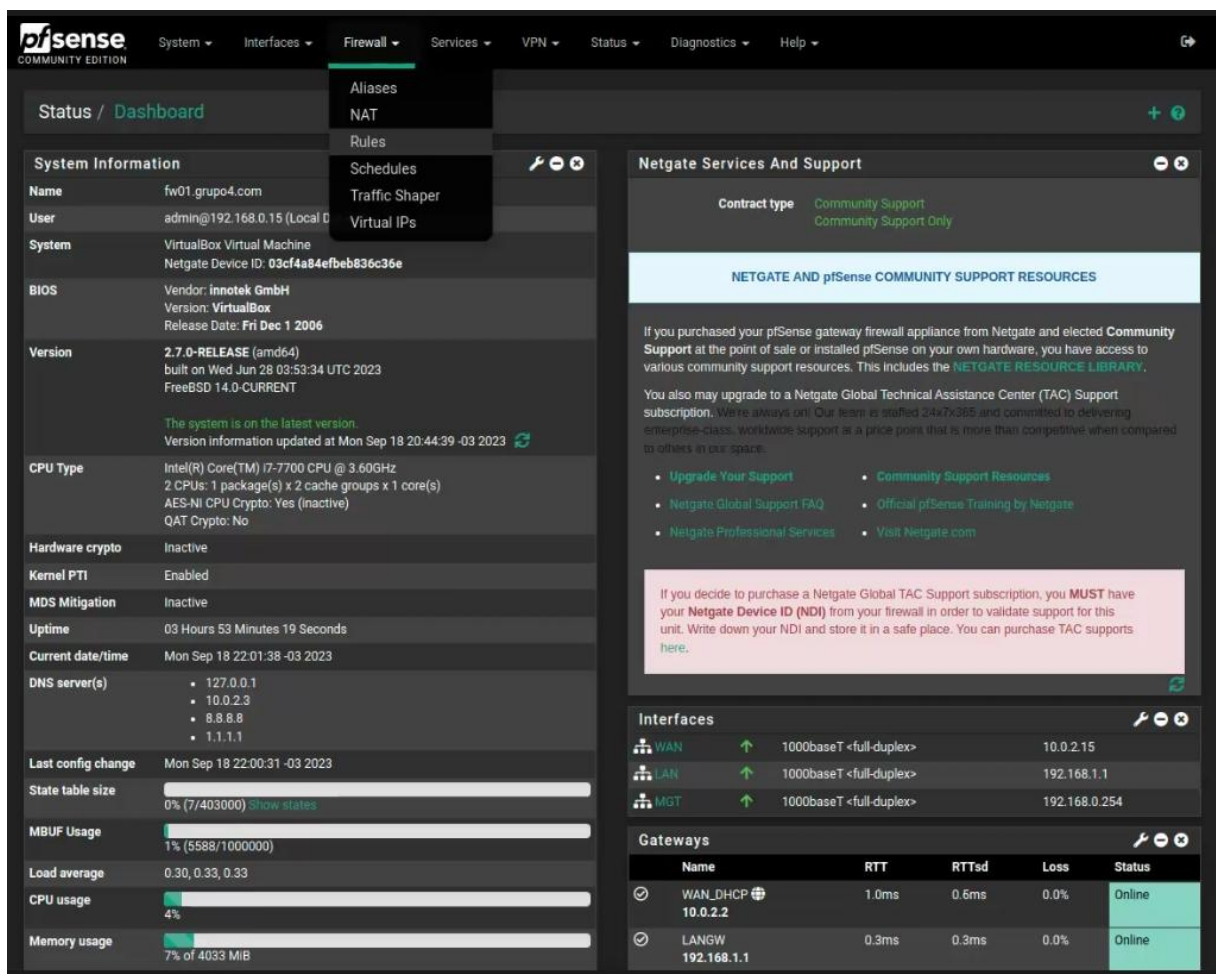
#### 3.2 Regra 1

Bloquear portas acima 1024, por serem portas dinâmicas e por algumas não terem um serviço específico que escute nestas portas.

##### Passo1:

A Figura 1 a seguir representa a tela inicial da ferramenta. No menu, clique em **Firewall** e escolha a opção **Rules** para iniciar a adição de uma nova regra.

FIGURA 1 - UTM - REGRA 1 - PASSO 1



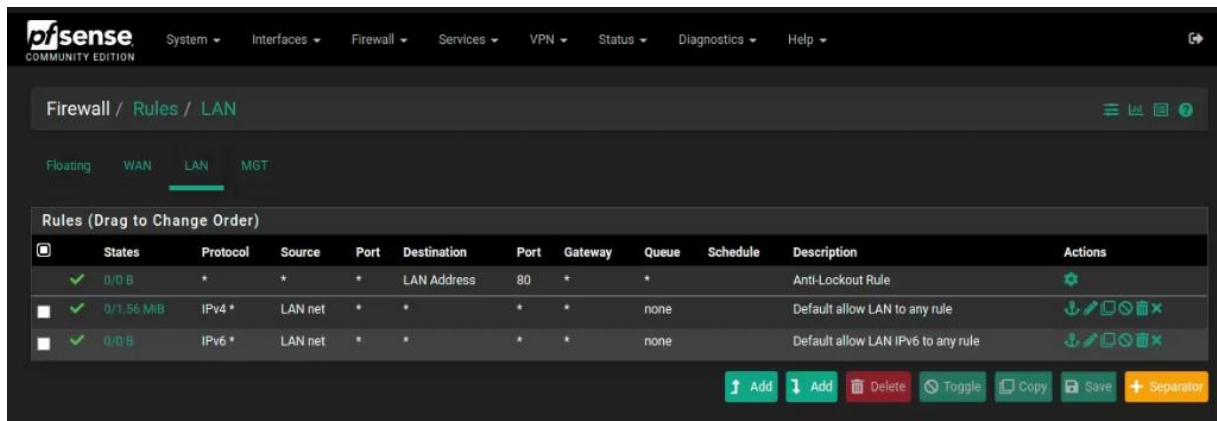
Fonte: Elaborado pelos autores, 2023



**Passo2:**

Por padrão, a tela que se abre está selecionada a opção WAN. Na Figura 2, altere a seleção para LAN e, em seguida, clique em Add para continuar.

FIGURA 2 - UTM - REGRA 1 - PASSO 2



Fonte: Elaborado pelos autores, 2023

**Passo 3:**

Preencha os quatro blocos de informações, da Figura 3, conforme segue:

Bloco 1: Edit Firewall Rule.

Selecione a opção **Block** no campo **Action**.

Deixe o campo **Disable** desmarcado.

Mantenha o padrão **LAN** no campo interface.

Mantenha o padrão IPv4 no campo **Family Address**.

Mantenha o padrão **TCP** no campo Protocol.

Bloco 2: Source

Mantenha o check box **Invert Match** desmarcado.

Na primeira caixa de seleção, escolha a opção **Any**, para que a regra seja aplicada de forma generalizada.

A segunda caixa de seleção permanece bloqueada, em função da opção **Any** ter sido escolhida na caixa anterior.

Desconsidere o botão **Display Advanced**.

Bloco 3: Destination

Mantenha o check box **Invert Match** desmarcado.

Na primeira caixa de seleção, escolha a opção **Lan net**.

A segunda caixa de seleção permanece bloqueada, em função da opção **Lan net** ter sido escolhida na caixa anterior.

Em Destination Port Range, selecione **Other** no campo From e insira **1025** no primeiro campo Custom. Em seguida, selecione **Other** no campo To e insira **65535** no campo Custom.

Bloco 4: Extra Options.

Mantenha o check box **Log packets that is handle by this rule** desmarcado.

O preenchimento da caixa de texto Description é opcional.

Desconsidere o botão **Display Advanced**.

Clique em **Save** para salvar.

FIGURA 3 - UTM - REGRA 1 - PASSO 3

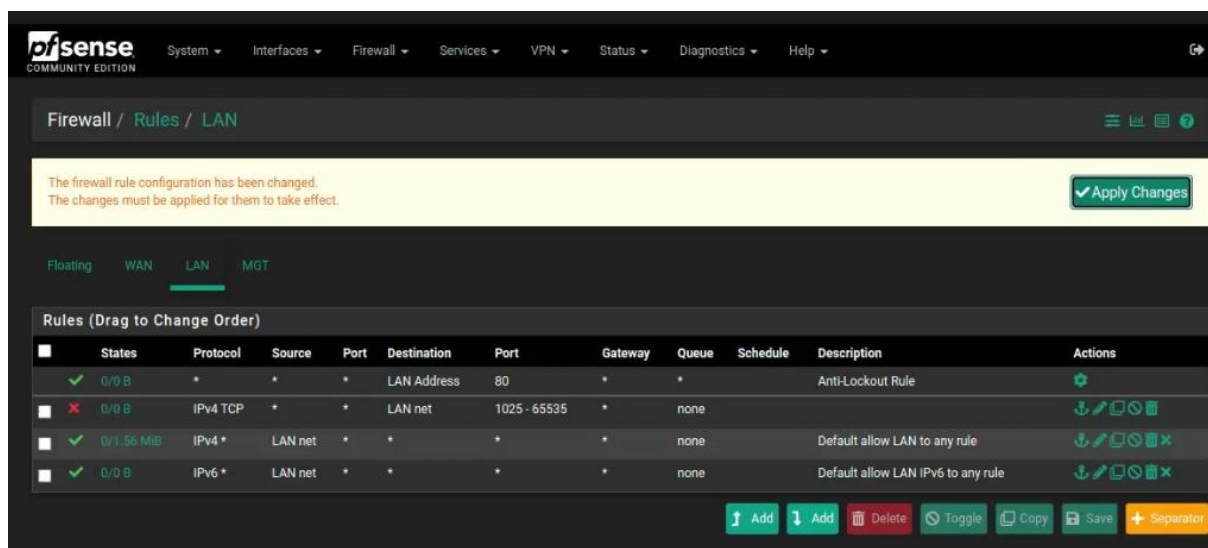
The screenshot shows the 'Edit Firewall Rule' interface in pfSense. The 'Action' is set to 'Block'. The 'Interface' is 'LAN'. The 'Address Family' is 'IPv4'. The 'Protocol' is 'TCP'. The 'Source' is 'any'. The 'Destination' is 'LAN net'. The 'Destination Port Range' is set to 'From: (other) 1025' and 'To: (other) 65535'. The 'Log' checkbox is unchecked. The 'Description' field is empty. The 'Save' button is at the bottom.

Fonte: Elaborado pelos autores, 2023

#### Passo 4:

Na Figura 4, clique em **Apply Changes** para aplicar a nova regra criada.

FIGURA 4 - UTM - REGRA 1 - PASSO 4



Fonte: Elaborado pelos autores, 2023

### 3.3 Regra 2:

Bloqueio de Mídias Sociais (Facebook, instagram, twitter...).

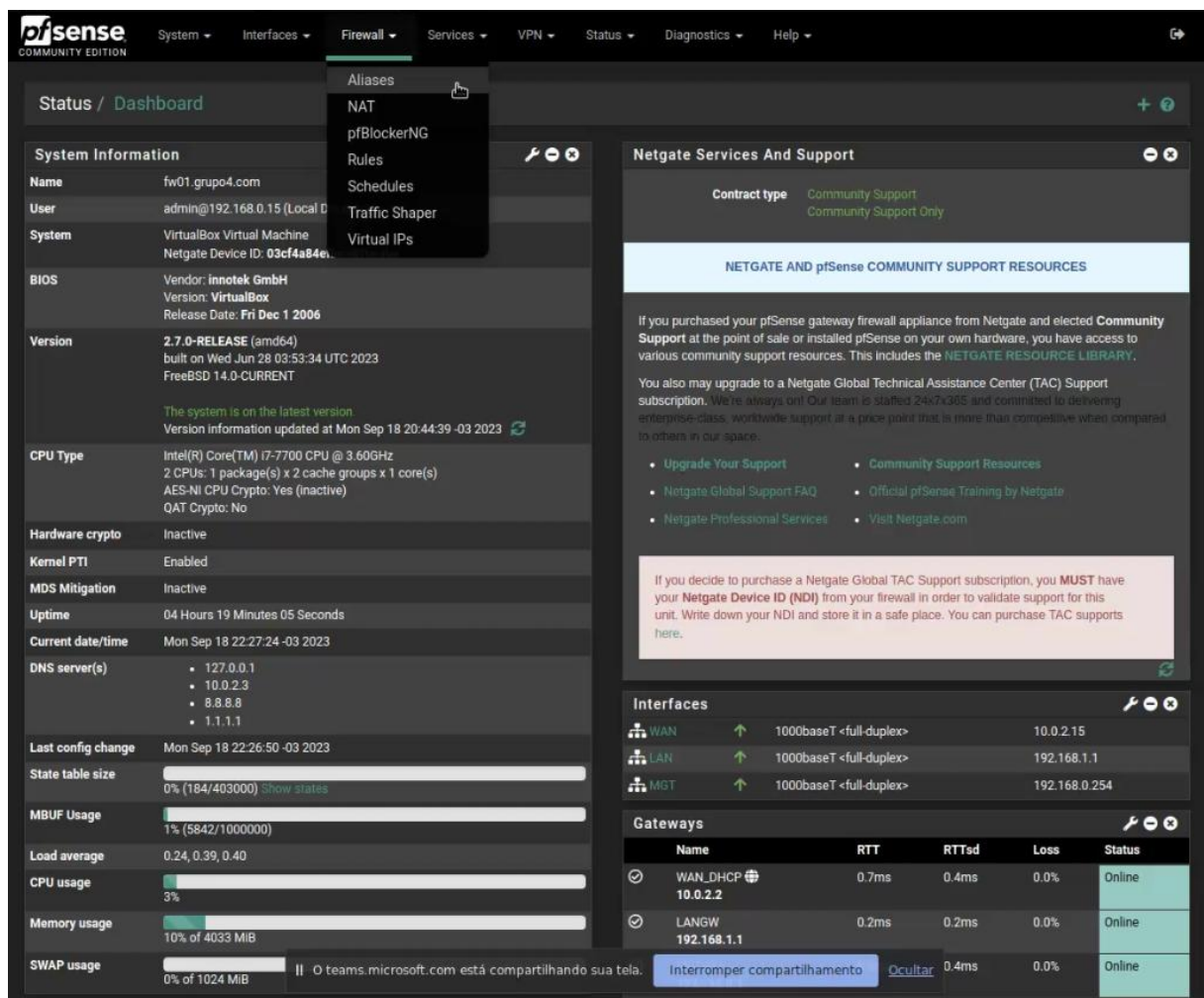
A criação desta regra na empresa é importante para aumentar a segurança e a proteção de dados, pois as redes sociais também estão cheias de links maliciosos que podem levar o usuário a instalar involuntariamente vírus, spywares e malwares nos equipamentos e na rede de computadores da empresa, o que pode ocasionar lentidão, mal funcionamento dos equipamentos ou vazamento de dados.

Para criar uma regra para Bloqueio de Mídias Sociais, primeiramente, é preciso criar um Aliases, que é opção que a ferramenta oferece de se criar um nome para um conjunto de aplicações que serão bloqueadas ao mesmo tempo. Em seguida, a regra poderá ser criada.

**Passo 1:**

No menu a Figura 5, clique em **Firewall** e escolha a opção **Aliases**.

FIGURA 5 - UTM - REGRA 2 - PASSO 1

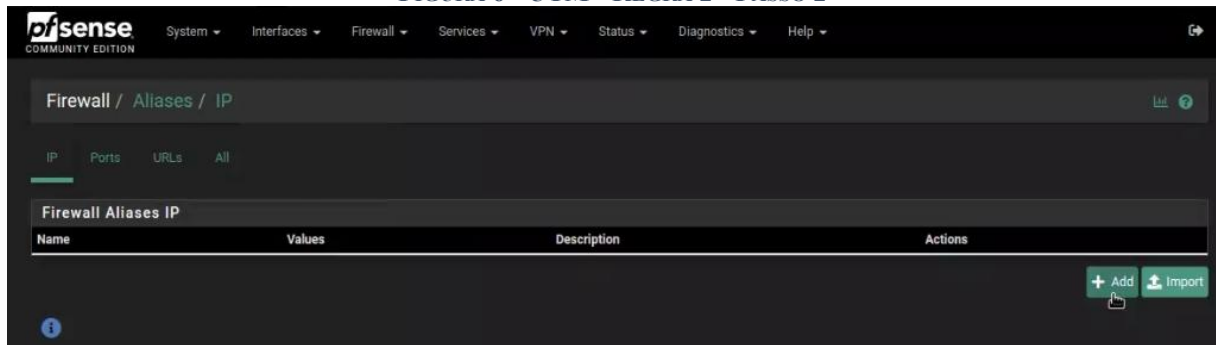


Fonte: Elaborado pelos autores, 2023

**Passo 2:**

Na Figura 6, clique em **+Add** para adicionar um novo Aliases.

FIGURA 6 - UTM - REGRA 2 - PASSO 2



Fonte: Elaborado pelos autores, 2023

### Passo 3:

Preencha os dois blocos de informações, da Figura 7, conforme segue:

Bloco 1: Properties.

Escreva **Redes\_Sociais** no campo **Name**.

Escreva **Block Redes Sociais** no campo **Description**.

Selecione a opção **Host(s)** na caixa de seleção **Type**.

Bloco 2: Host(s)

Para cada linha do **IP or FQDN (Fully qualified domain name)**, insira a URL da plataforma da rede social que deseja bloquear no primeiro campo de texto e, no segundo, alguma informação complementar .

Clique em **+Add Host** para inserir URLs de outras redes sociais.

Clique em **Save** para salvar.

FIGURA 7 - UTM - REGRA 2 - PASSO 3

pfSense COMMUNITY EDITION

System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Firewall / Aliases / Edit

**Properties**

**Bloco 1**

**Name** Rede\_Sociais  
The name of the alias may only consist of the characters "a-z, A-Z, 0-9 and \_".

**Description** Block Rede sociais  
A description may be entered here for administrative reference (not parsed).

**Type** Host(s)

**Host(s)**

**Bloco 1**

**Hint** Enter as many hosts as desired. Hosts must be specified by their IP address or fully qualified domain name (FQDN). FQDN hostnames are periodically re-resolved and updated. If multiple IPs are returned by a DNS query, all are used. An IP range such as 192.168.1.1-192.168.1.10 or a small subnet such as 192.168.1.16/28 may also be entered and a list of individual IP addresses will be generated.

IP or FQDN		
www.facebook.com	Para não afetar a produtividade	Delete
www.instagram.com	Para não afetar a produtividade	Delete
www.twitter.com	Para não afetar a produtividade	Delete
www.x.com	Para não afetar a produtividade	Delete

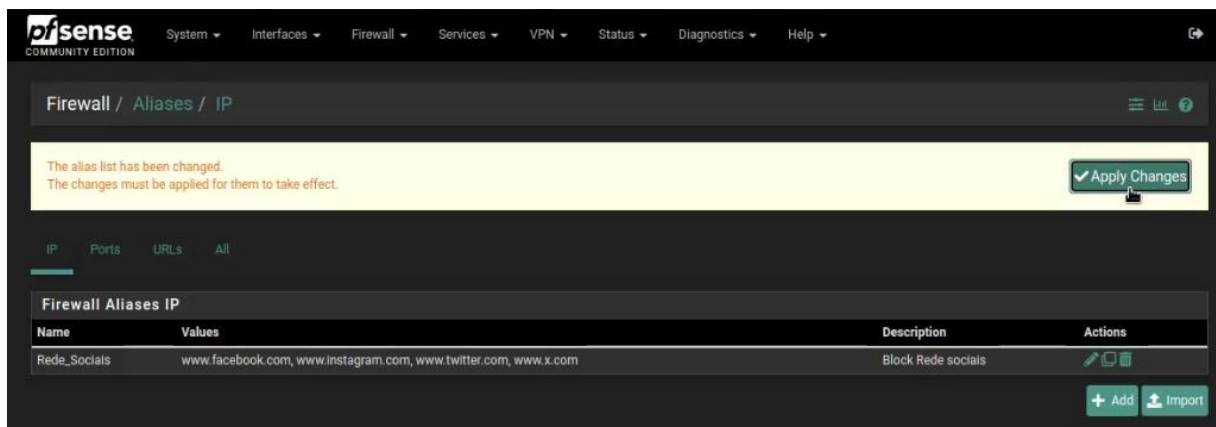
Save + Add Host

Fonte: Elaborado pelos autores, 2023

**Passo 4:**

Na Figura 8, clique em **Apply Changes** para aplicar o novo Aliases criado.

FIGURA 8 - UTM - REGRA 2 - PASSO 4

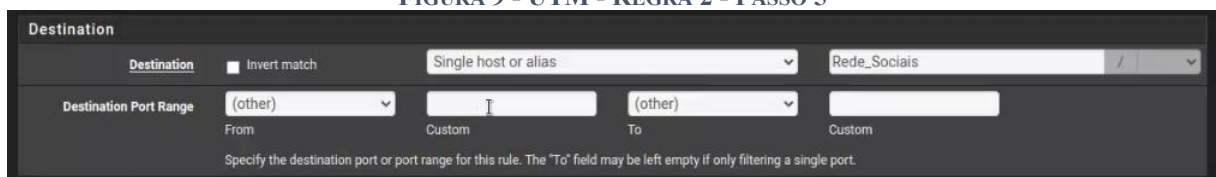


Fonte: Elaborado pelos autores, 2023

### **Passo 5:**

Após a criação do Aliases, pode-se utilizá-lo junto com uma regra de Firewall para bloquear todas as redes sociais de uma vez. Para acrescentar esta nova regra, siga os passos apresentados na regra 1 deste documento, considerando algumas diferenças no Bloco de informações **Destination**, conforme Figura 9, que utiliza o Aliases criado ao invés do Endereço IP ou Rede de destino, neste caso, **Redes\_Sociais**.

**FIGURA 9 - UTM - REGRA 2 - PASSO 5**



Fonte: Elaborado pelos autores, 2023

## 4 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA IDS

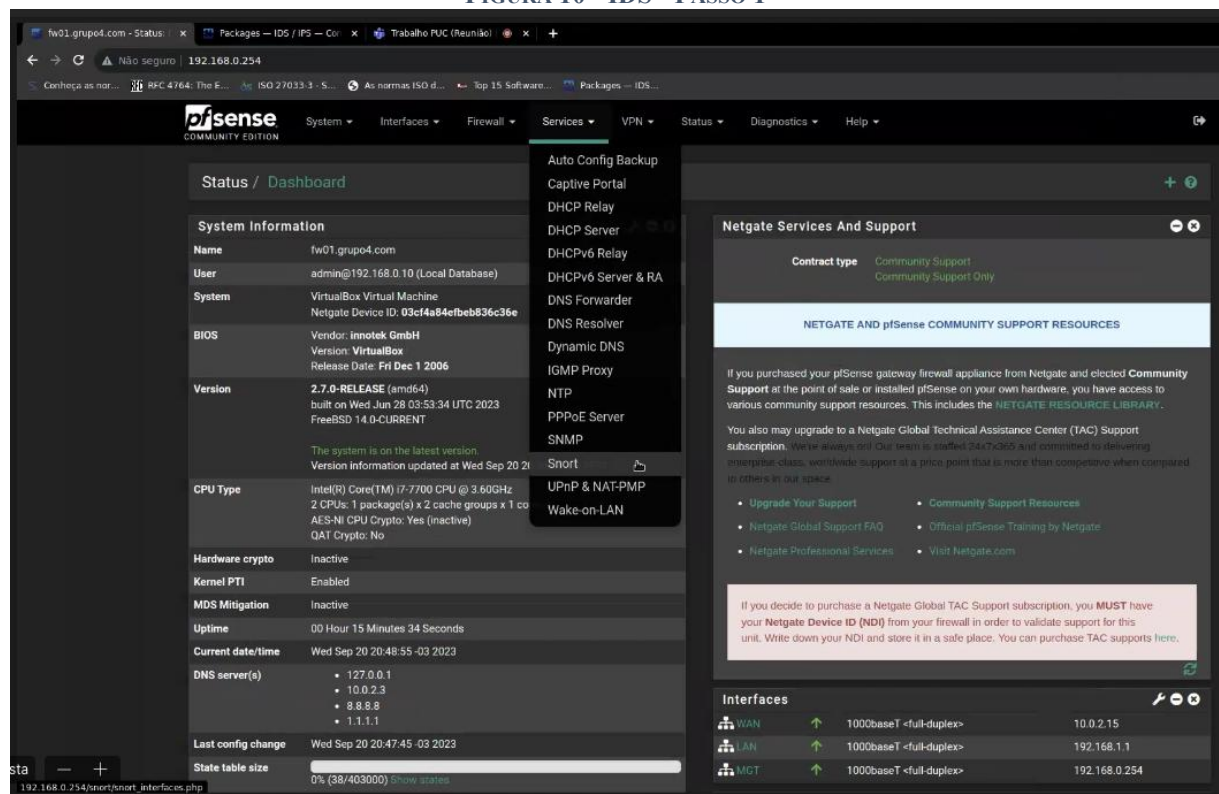
### 4.1 Ferramenta utilizada: Pfsense.

### 4.2 Configuração

#### Passo1:

A Figura 10 a seguir representa a tela inicial da ferramenta. No menu, clique em **Services** e escolha a opção **Snort** para iniciar a configuração do IDS.

FIGURA 10 - IDS - PASSO 1



Fonte: Elaborado pelos autores, 2023

#### Passo 2:

Na tela da Figura 11, clique em Global Settings e configure conforme a seguir:

Selecione o checkbox do campo **Enable Snort GPLv2**.

Selecione o checkbox do campo **Enable ET Open**.



Selecione o checkbox do campo **Enable OpenAppID**.

Selecione o checkbox do campo **Enable AppID Open Text Rules**.

Selecione a opção **12 HOURS** na caixa de seleção do campo **Update Interval**.

Digite um horário no formato 24h (ex. **00:45**) na caixa de texto do campo **Update Start Time**.

Selecione o checkbox do campo **Hide Deprecated Rules Categories**.

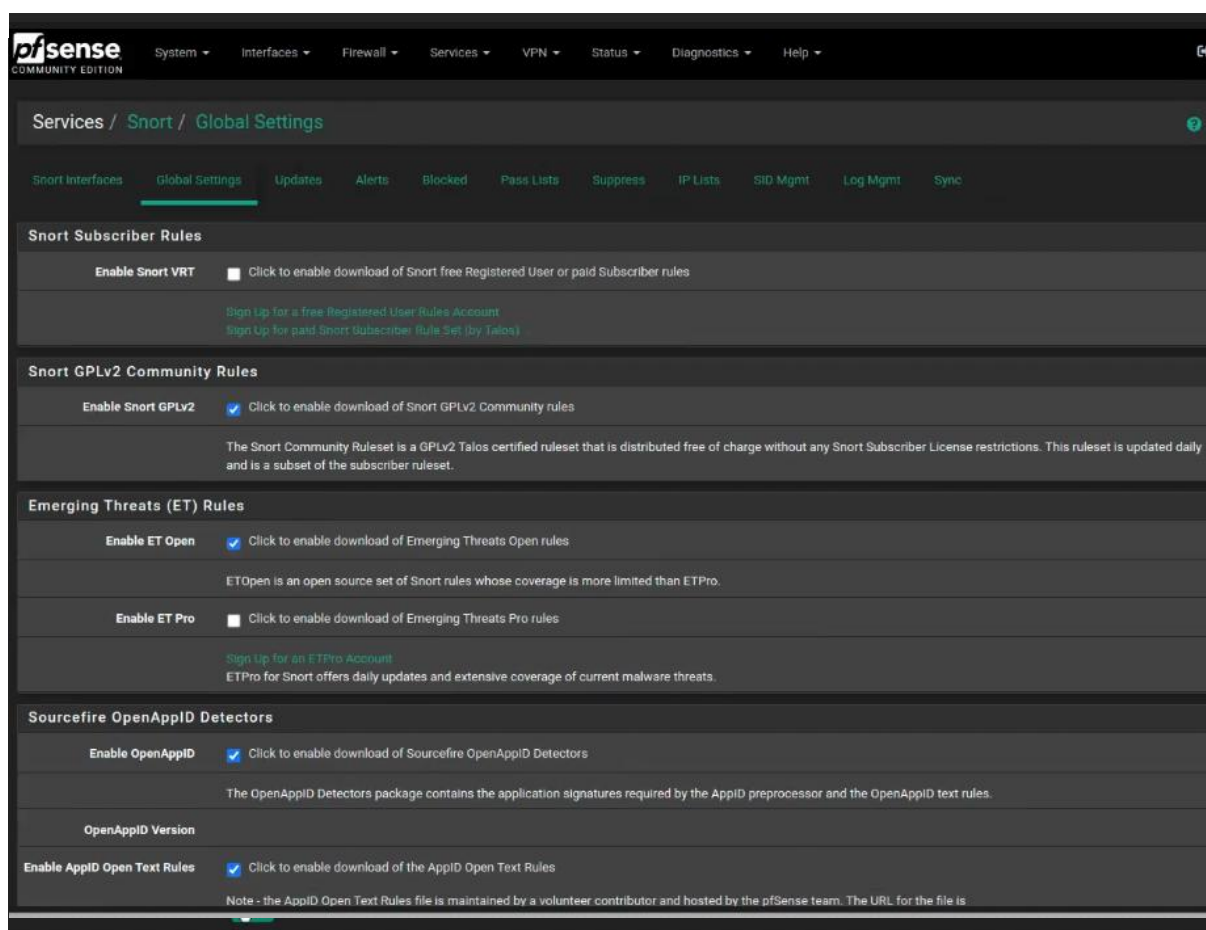
Selecione a opção **1 HOUR** na caixa de seleção do campo **Remove Blocked Hosts Interval**.

Selecione o checkbox do campo **Keep Snort Settings After Deinstall**.

Selecione o checkbox do campo **Startup/Shutdown Logging**.

Clique em **Save**.

FIGURA 11 - IDS - PASSO 2

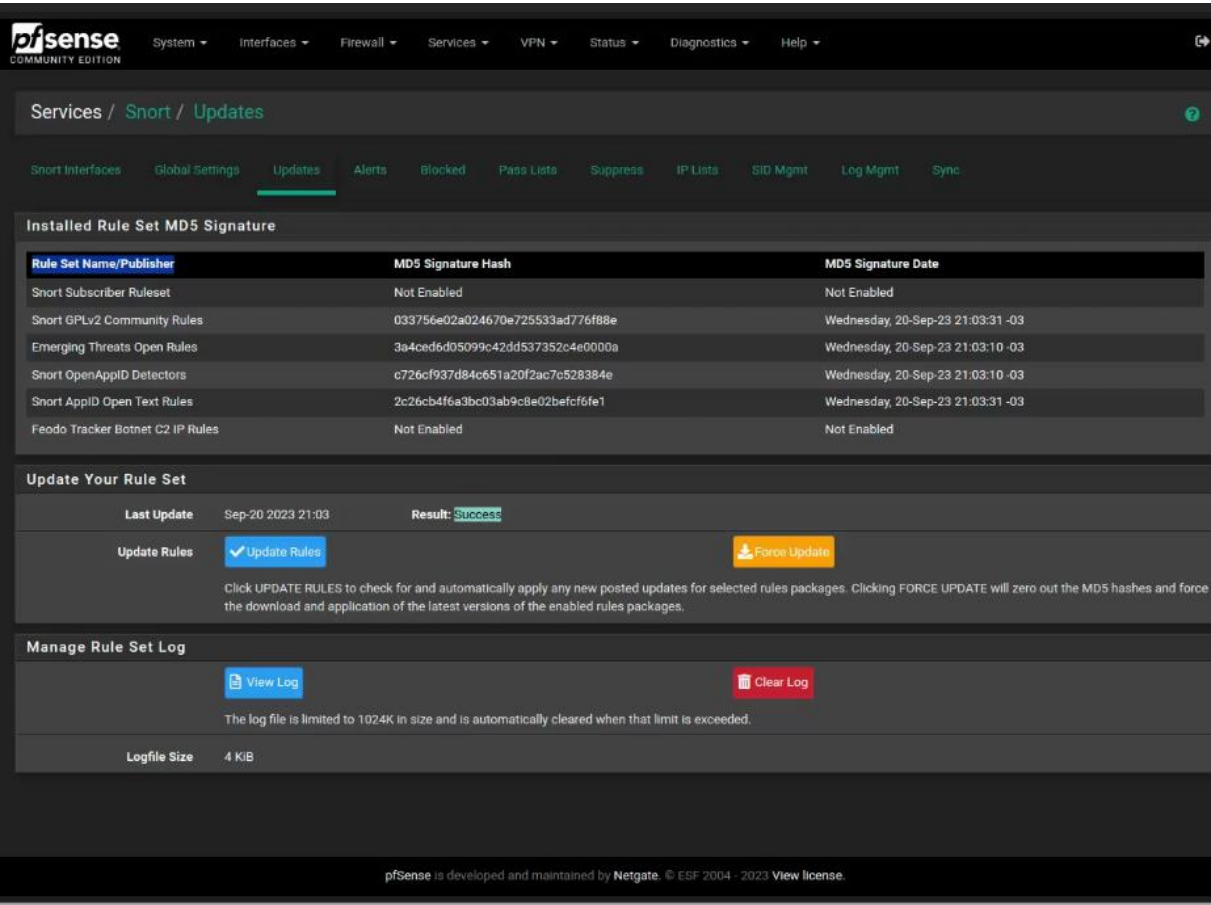


Fonte: Elaborado pelos autores, 2023

**Passo 3:**

Na Figura 12, selecione a guia **Updates** e clique em **Update Rules** e aguarde que no campo **Result** apareça **Success** ou **Fail**.

FIGURA 12 - IDS - PASSO 3

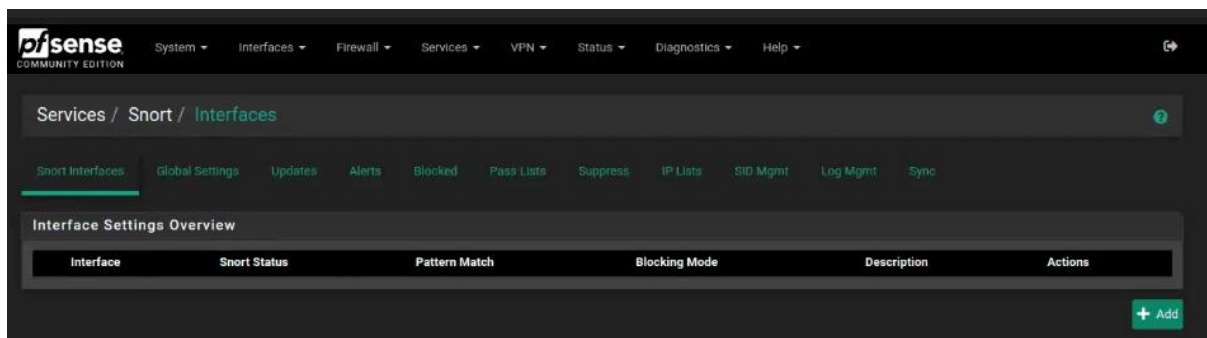


Fonte: Elaborado pelos autores, 2023

**Passo 4:**

Na Figura 13, selecione a guia **Snort Interface** e clique em **Add**.

FIGURA 13 - IDS - PASSO 4



Fonte: Elaborado pelos autores, 2023

### Passo 5:

Na Figura 14, com a guia **WAN Settings** aberta, marque o checkbox do campo **Enable**.

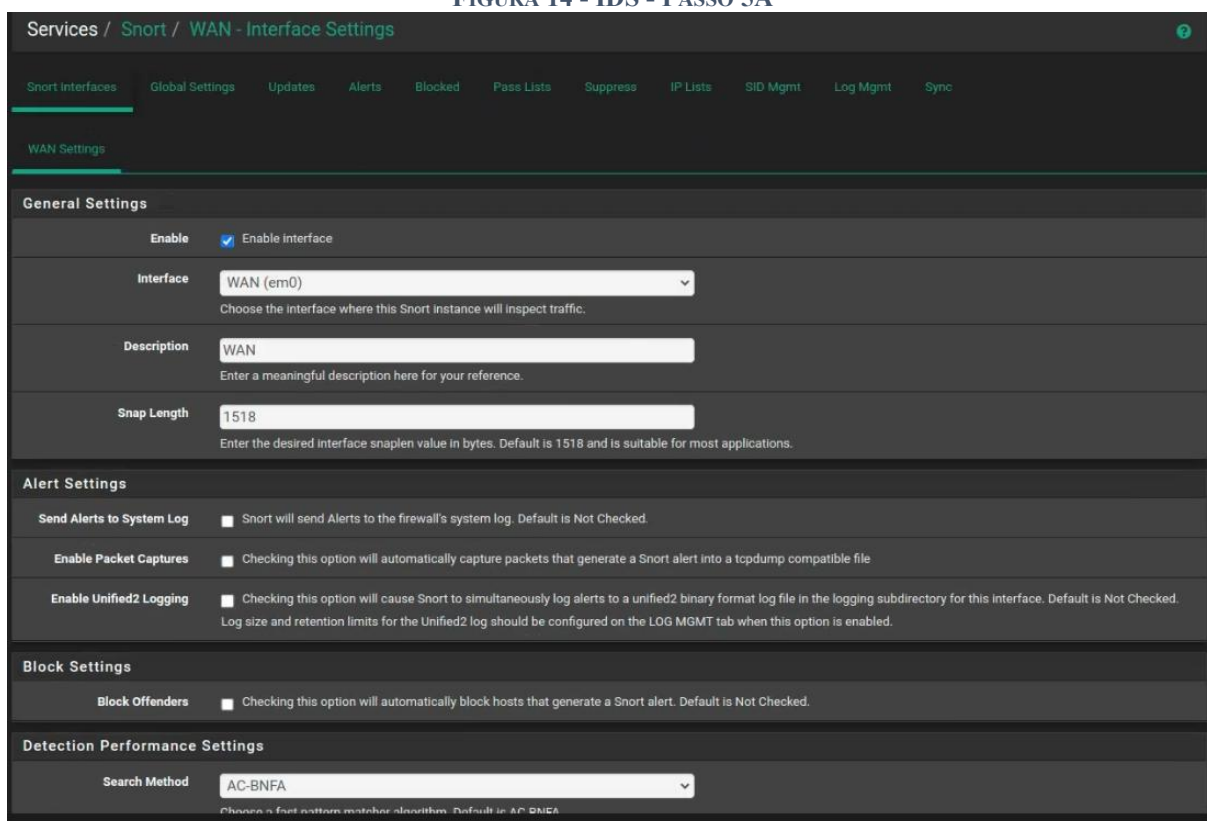
Selecione a opção **WAN (em0)** na caixa de seleção do campo **Interface**.

Escreva uma descrição sobre a interface (ex. **WAN**) no campo **Description**.

Escreva **1518** no campo **Snap Length**.

Deixar os demais campos no default.

FIGURA 14 - IDS - PASSO 5A



Fonte: Elaborado pelos autores, 2023

A Figura 15 é continuidade da tela da Figura 14.

**FIGURA 15 - IDS - PASSO 5B**

**Detection Performance Settings**

**Search Method**    
 Choose a fast pattern matcher algorithm. Default is AC-BNFA.

**Split ANY-ANY** ☐ Enable splitting of ANY-ANY port group. Default is Not Checked.

**Search Optimize** ☐ Enable search optimization. Default is Not Checked.

**Stream Inserts** ☐ Do not evaluate stream inserted packets against the detection engine. Default is Not Checked.

**Checksum Check Disable** ☐ Disable checksum checking within Snort to improve performance. Default is Not Checked.

**Choose the Networks Snort Should Inspect and Whitelist**

**Home Net**  [View List](#)   
 Choose the Home Net you want this interface to use.   
 Default Home Net adds only local networks, WAN IPs, Gateways, VPNs and VIPs.   
 Create an Alias to hold a list of friendly IPs that the firewall cannot see or to customize the default Home Net.

**External Net**  [View List](#)   
 Choose the External Net you want this interface to use.   
 External Net is networks that are not Home Net. Most users should leave this setting at default.   
 Create a Pass List and add an Alias to it, and then assign the Pass List here for custom External Net settings.

**Choose a Suppression or Filtering List (Optional)**

**Alert Suppression and Filtering**  [View List](#)   
 Choose the suppression or filtering file you want this interface to use.

**Custom Configuration Options**

**Advanced Configuration Pass-Through**   
    
 Enter any additional configuration parameters to add to the Snort configuration here, separated by a newline

[Save](#)

Fonte: Elaborado pelos autores, 2023

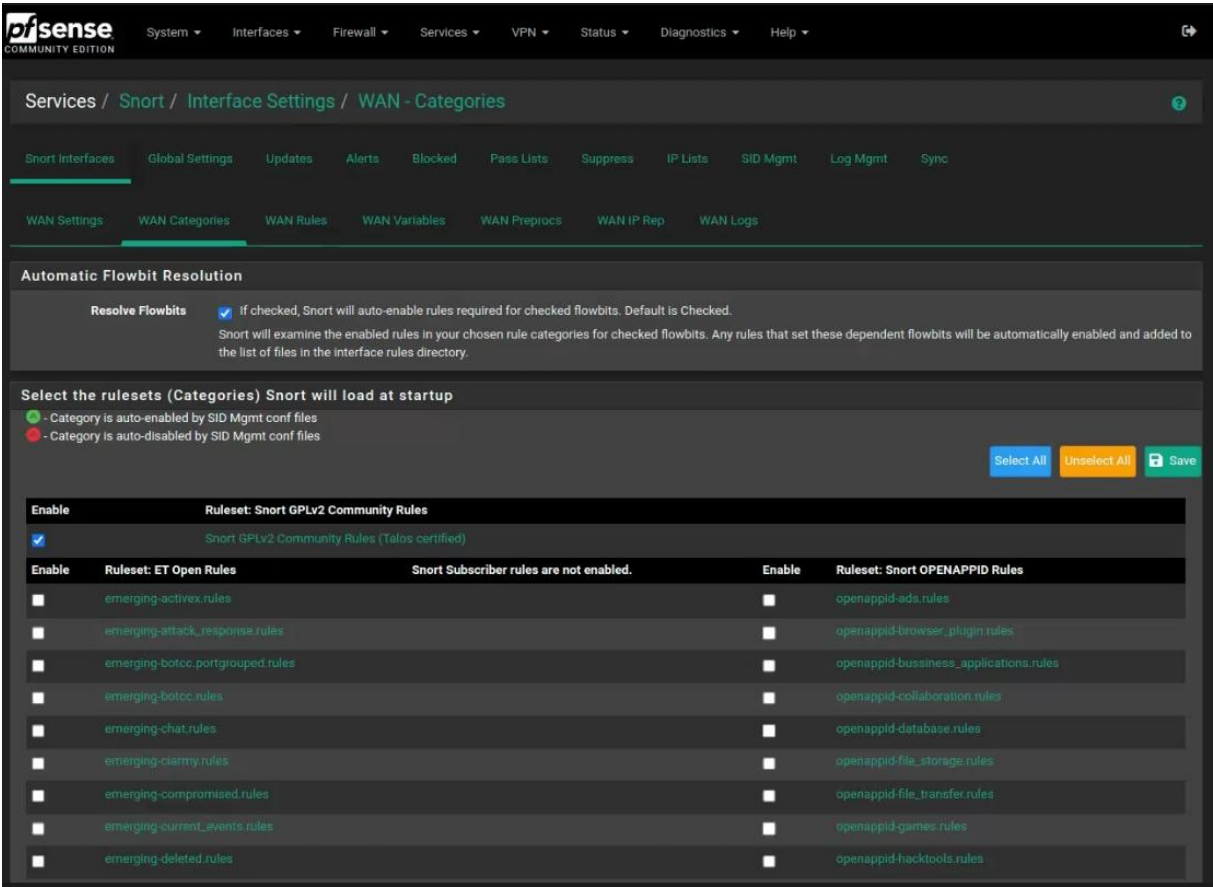
### **Passo 6:**

Na Figura 16, selecione a guia WAN Categories

Marque o checkbox do campo **Ruleset: Snort GPLv2 Community Rules**.

Clique em **Save**.

FIGURA 16 - IDS - PASSO 6

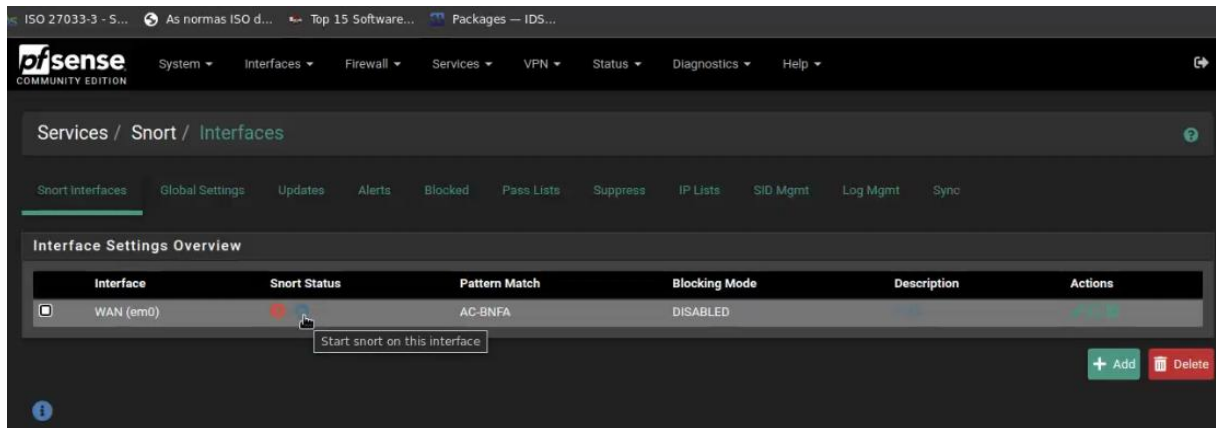


Fonte: Elaborado pelos autores, 2023

**Passo 7:**

Clique no ícone azul da coluna Snort Status, conforme Figura 17 abaixo.  
Aguarde o IDS inicializar e aguarde o ícone ficar verde.

FIGURA 17 - IDS - PASSO 7



Fonte: Elaborado pelos autores, 2023

## 5 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA DE BACKUP

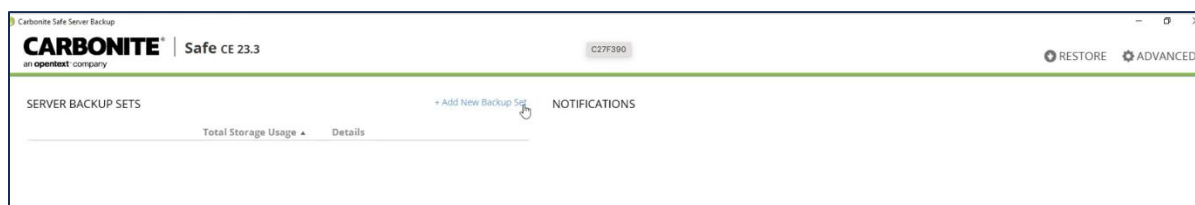
### 5.1 Ferramenta utilizada: Carbonite.

### 5.2 Configuração

#### Passo 1:

Na Figura 18, clique em **+Add New Backup Set**.

FIGURA 18 - BACKUP - PASSO 1

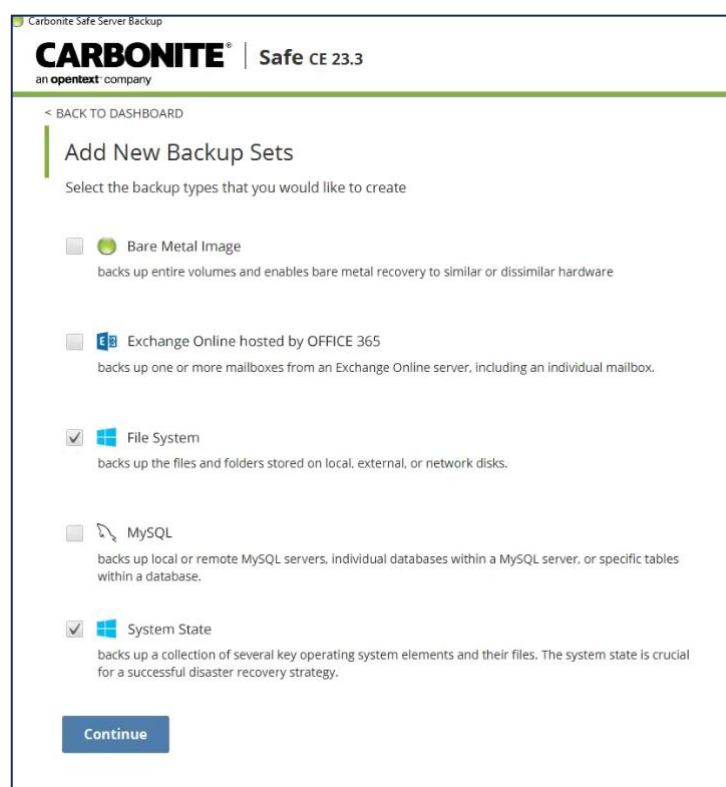


Fonte: Elaborado pelos autores, 2023

#### Passo 2:

Na Figura 19, mantenha os itens selecionados por padrão (**File System** e **System State**).

FIGURA 19 - BACKUP - PASSO 2



Fonte: Elaborado pelos autores, 2023

### **Passo 3:**

A Figura 20 refere-se à configuração de backup do tipo **Windows File System** e a Figura 21 refere-se ao tipo **Windows File State**. Em ambos há campos que são similares, com exceção da estrutura de diretório, presente no primeiro tipo e que não aparece no segundo, pois o que será contemplado no backup é padrão.

Insira um nome para a tarefa de backup no campo **Backup Name** (ex. **Windows File System**). Em **Local Backup Location**, clique em **Edit** e defina um local no disco para armazenar o backup.

No campo **Cloud Backup Location**, opcionalmente, selecione um país onde a nuvem está localizada e marque o checkbox **Back up to cloud**.

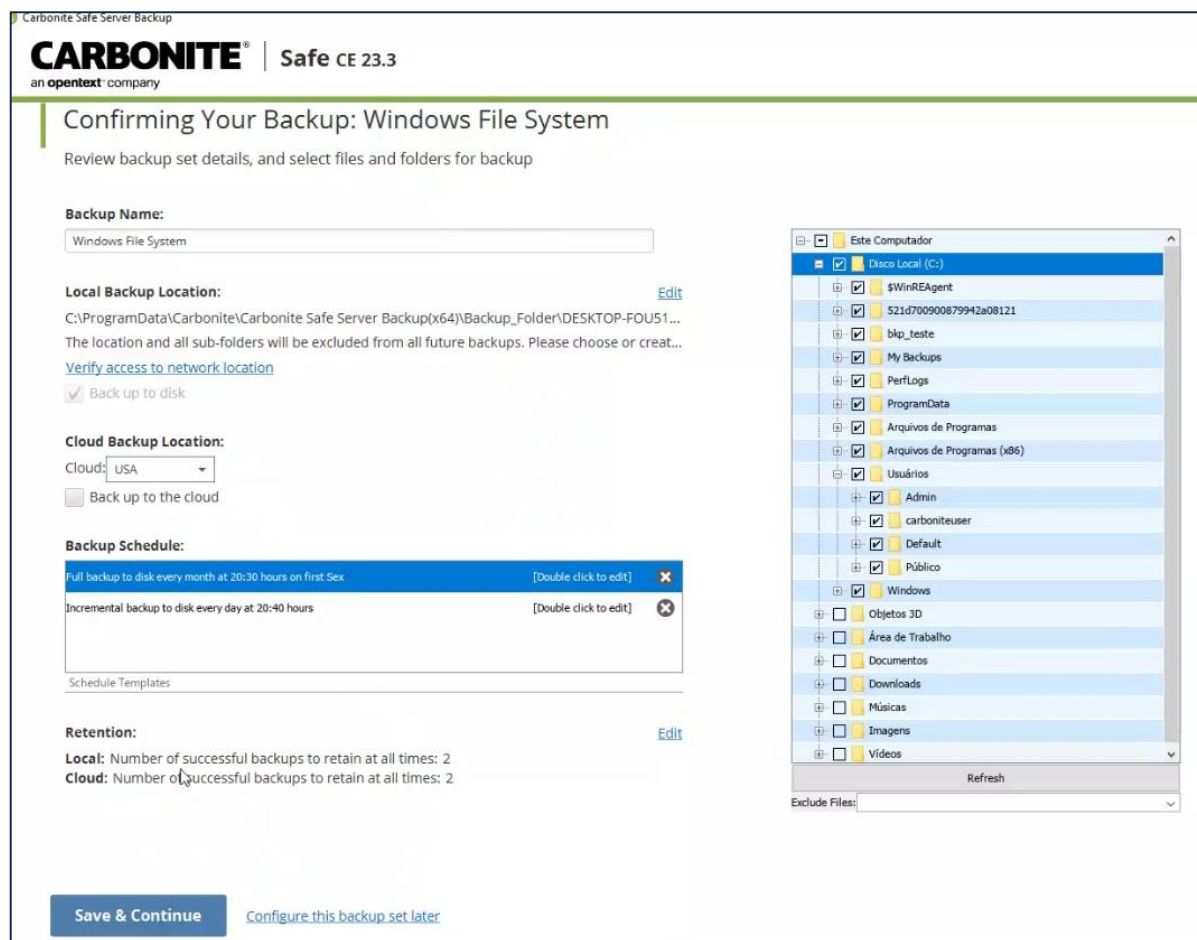
O campo **Backup Schedule** traz algumas opções predefinidas de tipo de backup e agendamento. Clique em **Double click to edit** para alterar estes parâmetros, se necessário.

No campo **Retention**, clique em **Edit** para definir a quantidade de backups com sucesso que devem ser mantidos ou definir um período de retenção.

Na estrutura de diretório à direita da figura, selecione as pastas que serão contempladas nas rotinas de backup.

Clique em **Save & Continue**.





**FIGURA 20 - BACKUP - PASSO 3A**  
Fonte: Elaborado pelos autores, 2023

A Figura 21 é a continuação da tela apresentada na Figura 20.

FIGURA 21 - BACKUP - PASSO 3B

Carbonite Safe Server Backup  
**CARBONITE**® | Safe CE 23.3  
an **openText** company

### Confirming Your Backup: Windows System State

Review backup set details, and select files and folders for backup

**Backup Name:**  
Windows System State

**Local Backup Location:** [Edit](#)  
C:\ProgramData\Carbonite\Carbonite Safe Server Backup(x64)\Backup\_Folder\DESKTOP-FOU51...  
The location and all sub-folders will be excluded from all future backups. Please choose or creat...  
[Verify access to network location](#)  
☒ Back up to disk

**Cloud Backup Location:**  
Cloud: USA  
☐ Back up to the cloud

**Backup Schedule:**  
Full backup to disk every week at 20:00 hours on Sex [Double click to edit] ✕  
Schedule Templates

**Retention:** [Edit](#)  
Local: Full: 2 Months  
Cloud: Full: 2 Months

[Save & Continue](#) [Configure this backup set later](#)

The System State backup type allows you to backup and restore all of the items listed below. System State does not include user files, folders, databases, or application information.

When used in conjunction with other backup types, System State also enables total recovery of a server to the same version of Windows on similar hardware.

System State differs from Bare Metal Image backups, which back up an entire system and allow complete recovery to different hardware.

Backup of:

- Boot files
- System files
- IIS
- COM+ database
- Registry
- Active Directory
- Certificate Server

Fonte: Elaborado pelos autores, 2023

#### **Passo 4:**

A Figura 22 é a tela de confirmação da configuração.

Clique em **Continue**.

FIGURA 22 - BACKUP - PASSO 4

Carbonite Safe Server Backup  
**CARBONITE**® | Safe CE 23.3  
an **openText** company

### Your backup set configuration is complete

- File System**  
backs up the files and folders stored on local, external, or network disks.
- System State**  
backs up a collection of several key operating system elements and their files. The system state is crucial for a successful disaster recovery strategy.

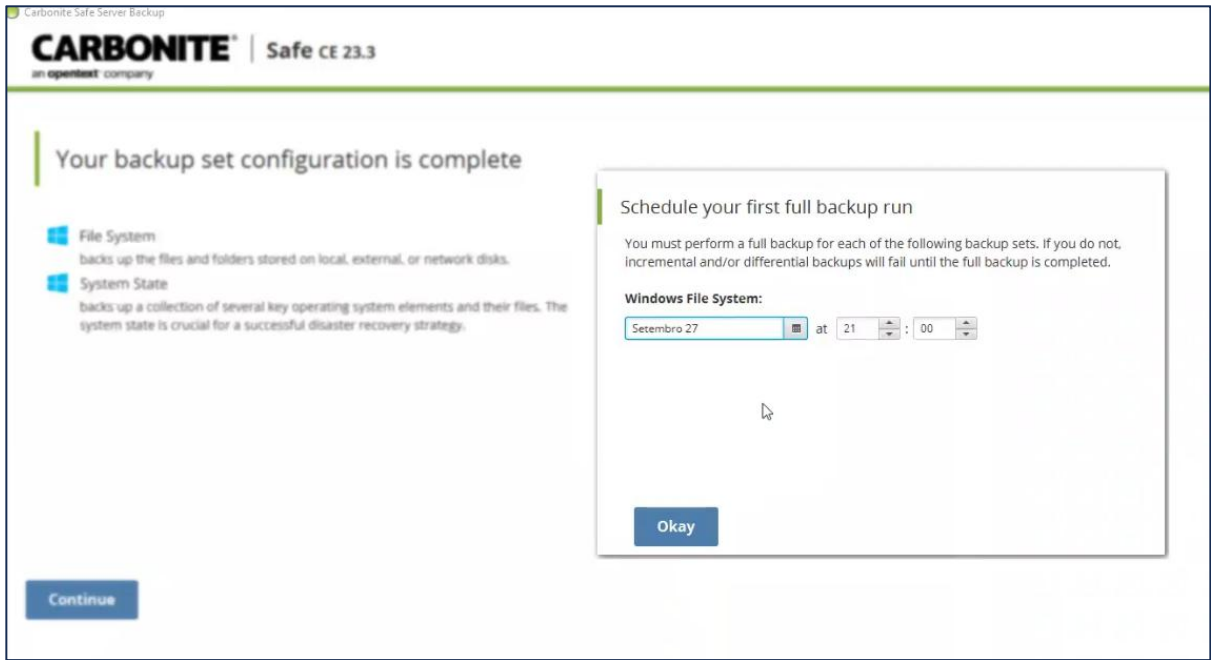
[Continue](#)

Fonte: Elaborado pelos autores, 2023

**Passo 5:**

Na Figura 23 pode aparecer uma janela para definir o primeiro agendamento do backup. Insira as informações e clique em **Okay**.

FIGURA 23 - BACKUP - PASSO 5

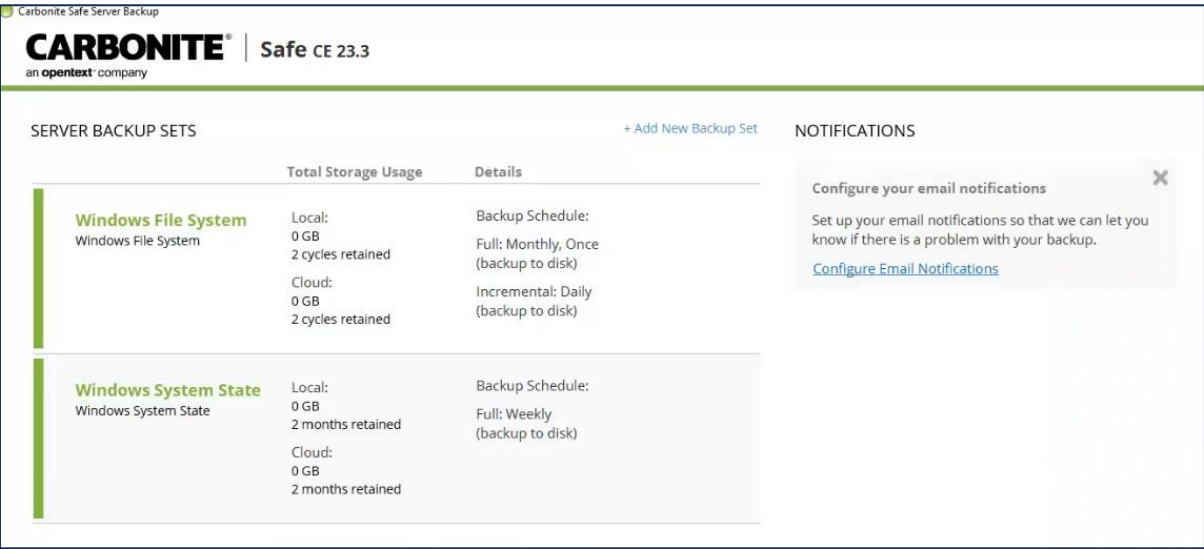


Fonte: Elaborado pelos autores, 2023

**Passo 6:**

A Figura 24 apresenta a tela final, demonstrando o backup configurado.

FIGURA 24 - BACKUP - PASSO 6



Fonte: Elaborado pelos autores, 2023

Conforme demonstrado na Figura 24, é sempre importante manter uma política de backup full uma vez por mês ou semana, além de realizar backups incrementais semanalmente ou diários. Estas estratégias visam garantir a disponibilidade dos dados o mais rápido possível, caso ocorra perda, alteração ou inacessibilidade aos dados utilizados no dia a dia. E o backup incremental visa garantir as atualizações, uma vez que possui um intervalo de tempo menor que o completo (full).

## 6 PROCEDIMENTO PARA UTILIZAÇÃO DE FERRAMENTA DE LOGS

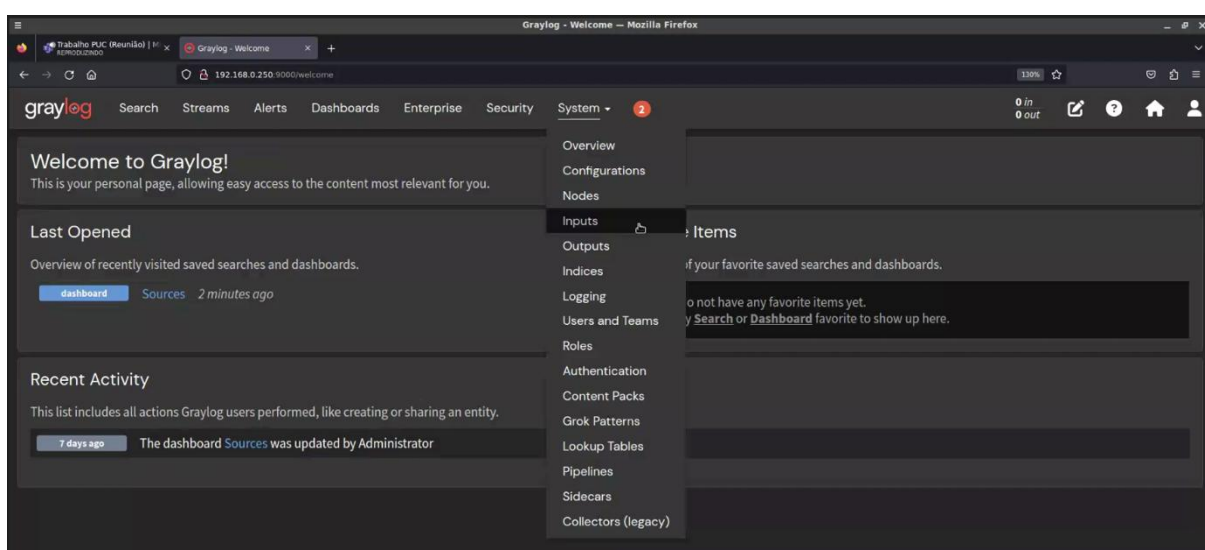
### 6.1 Ferramenta utilizada: Graylog.

### 6.2 Configuração

#### Passo 1:

Na Figura 25, no menu principal, selecione **System** e depois **Inputs**.

FIGURA 25 - LOG - PASSO 1



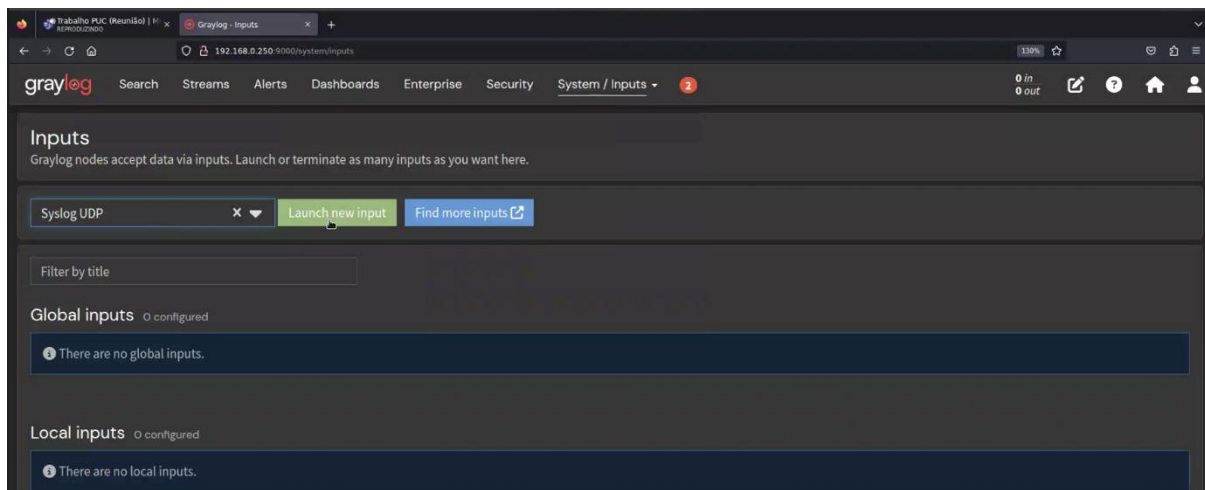
Fonte: Elaborado pelos autores, 2023

#### Passo 2:

Na Figura 26, selecionar **Syslog UDP** na caixa de seleção.

Clique em **Launch new input**.

FIGURA 26 - LOG - PASSO 2



Fonte: Elaborado pelos autores, 2023

### **Passo 3:**

Na Figura 27, marque o checkbox **Global**.

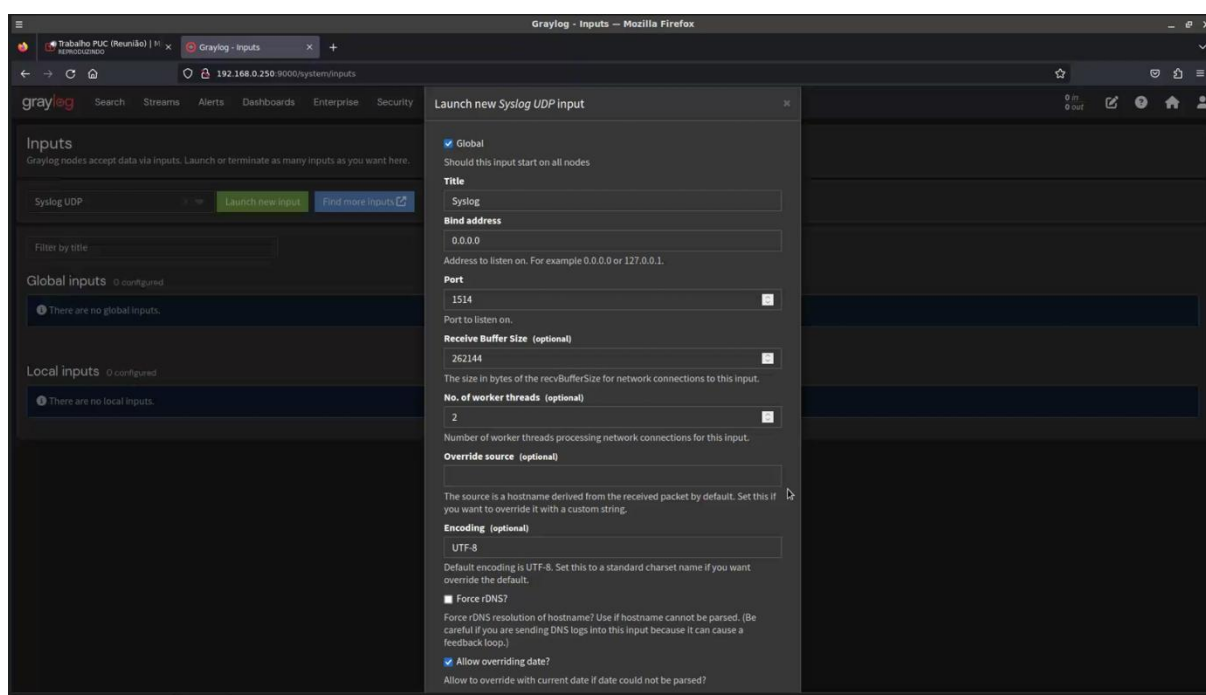
Escreva um título para identificação da origem dos dados (ex. **Sylog**) na caixa de texto **Title**.

Informe a porta no campo de texto **Port** (ex. **1514**).

Marque o checkbox **Store full message**.

Manter os demais campos com as informações default da própria ferramenta.

**FIGURA 27 - LOG - PASSO 3A**



Fonte: Elaborado pelos autores, 2023

A Figura 28 é a continuação da tela apresentada na Figura 27.

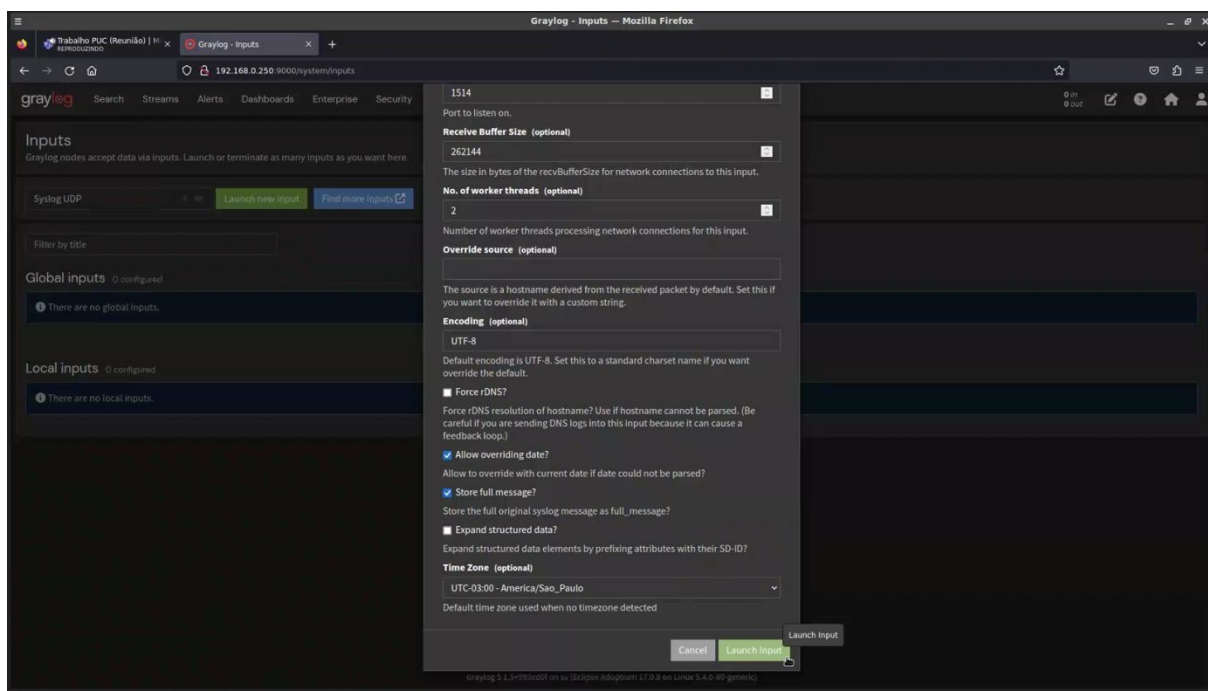


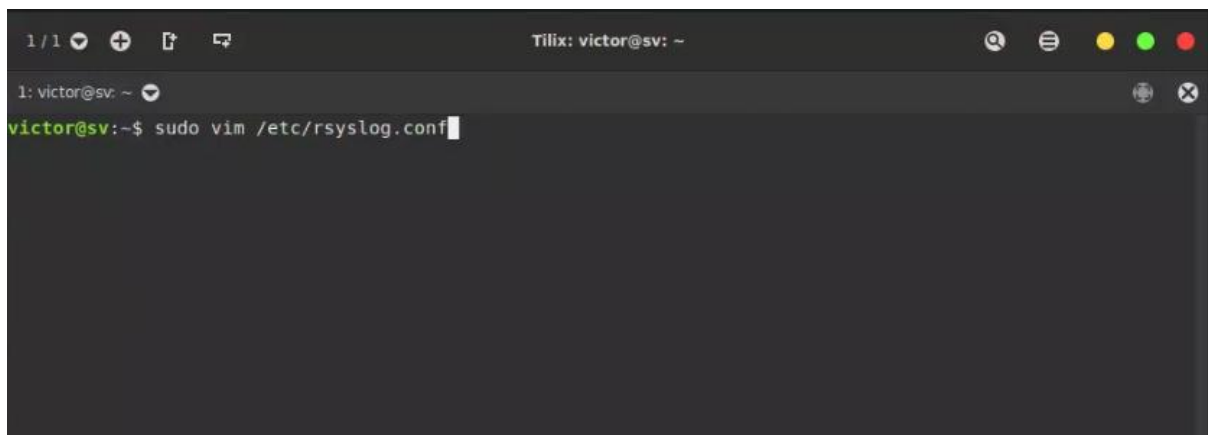
FIGURA 28 - LOG - PASSO 3B

Fonte: Elaborado pelos autores, 2023

**Passo 4:**

Na Figura 29, no servidor Linux, abra o arquivo **rsyslog.conf**.

FIGURA 29 - LOG - PASSO 4

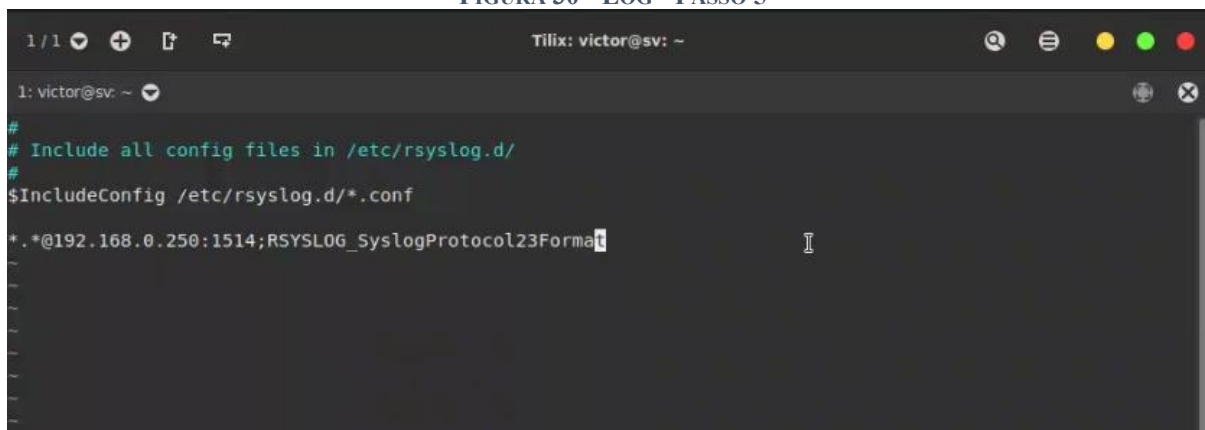


Fonte: Elaborado pelos autores, 2023

**Passo 5:**

Na Figura 30, escreva **\*.\*@192.168.0.250:1514;RSYSLOG\_SyslogProtocol23Format** e salva.

FIGURA 30 - LOG - PASSO 5



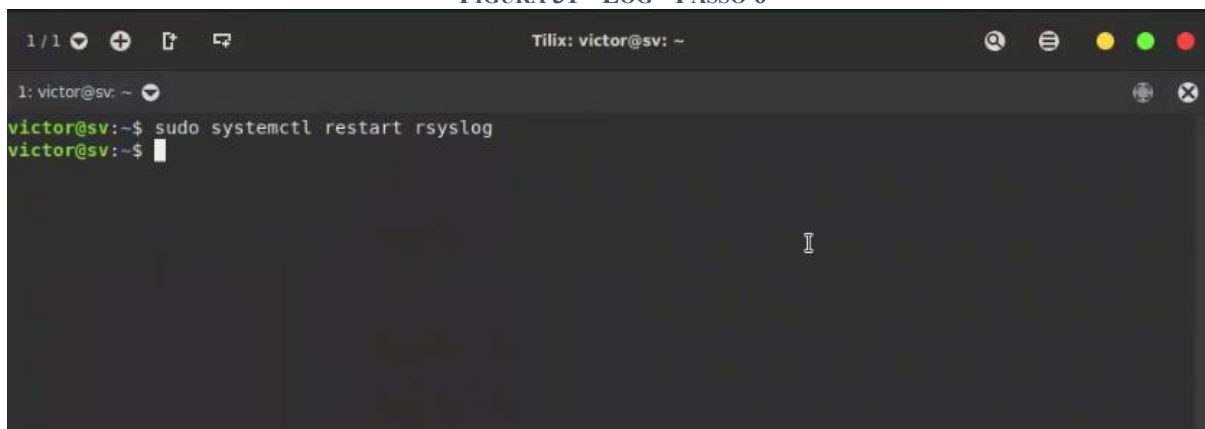
```
1 / 1  [icons]  Tilix: victor@sv: ~
1: victor@sv: ~
#
# Include all config files in /etc/rsyslog.d/
#
$IncludeConfig /etc/rsyslog.d/*.conf
*.*@192.168.0.250:1514;RSYSLOG_SyslogProtocol23Format
```

Fonte: Elaborado pelos autores, 2023

**Passo 6:**

Na Figura 31, reinicie a aplicação **rsyslog**.

FIGURA 31 - LOG - PASSO 6



```
1 / 1  [icons]  Tilix: victor@sv: ~
1: victor@sv: ~
victor@sv:~$ sudo systemctl restart rsyslog
victor@sv:~$
```

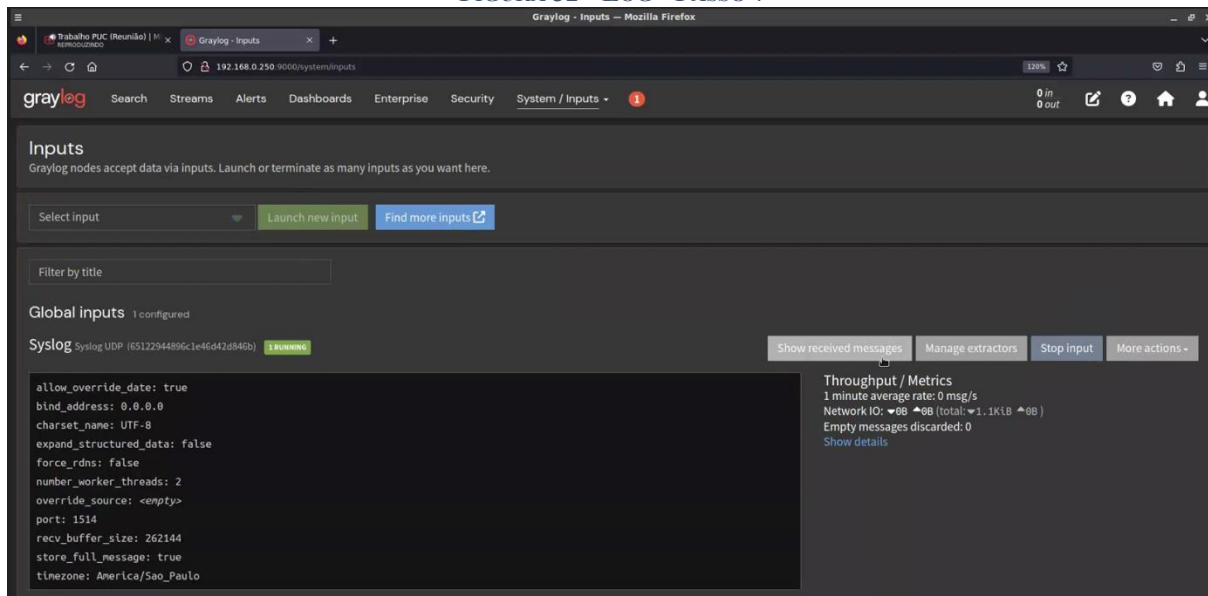
Fonte: Elaborado pelos autores, 2023



### Passo 7:

Na Figura 32 a seguir, clique em **Show received messages**.

FIGURA 32 - LOG - PASSO 7

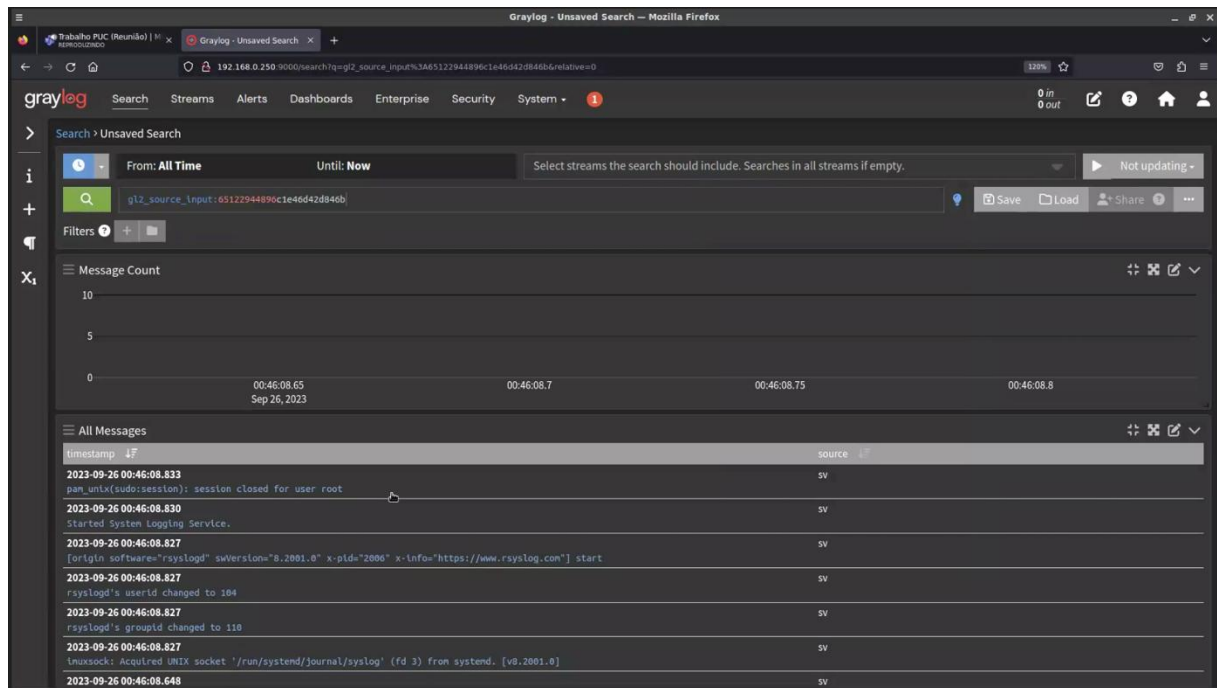


Fonte: Elaborado pelos autores, 2023

### Passo 8:

A Figura 33 apresenta as mensagens de log que estão sendo identificadas nas aplicações.

FIGURA 33 - LOG - PASSO 8



Fonte: Elaborado pelos autores, 2023

## 7 PROCEDIMENTO PARA UTILIZAR FERRAMENTA DE TESTE DE PENETRAÇÃO

### 7.1 Ferramenta utilizada: Zed Attack Proxy (ZAP).

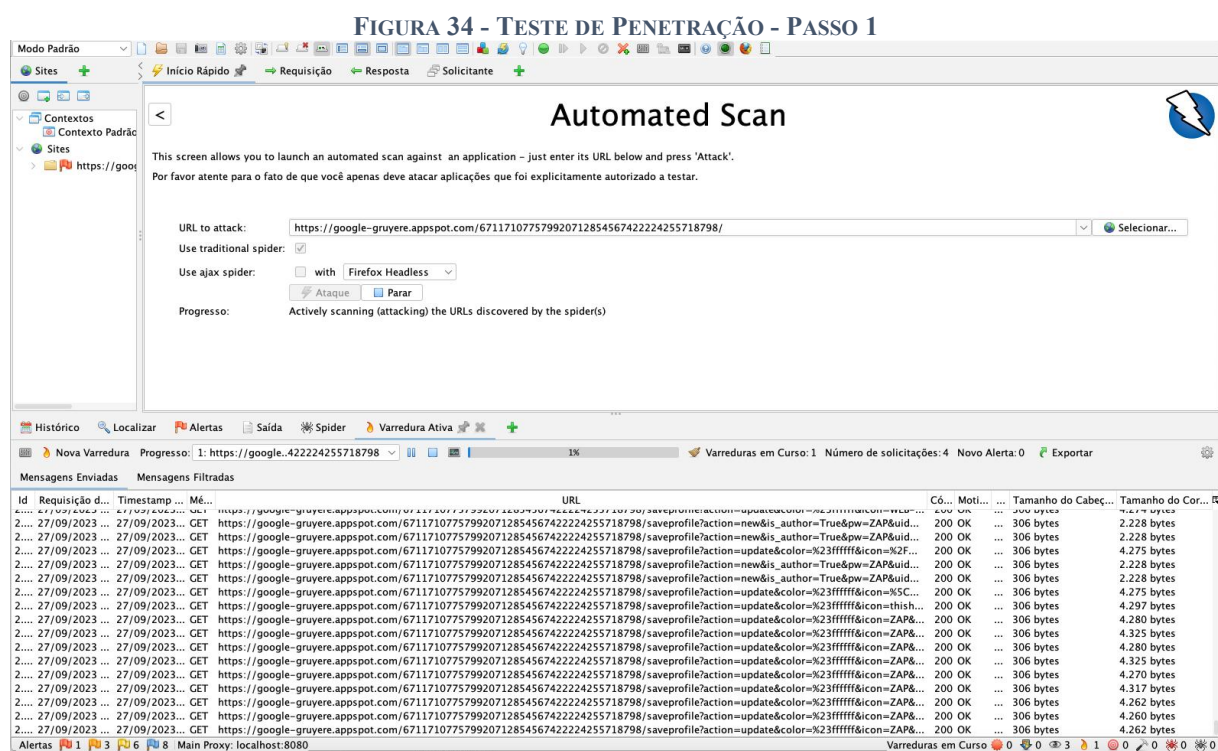
### 7.2 Configuração

#### Passo 1:

Na Figura 34, insira a URL do site Google Gruyere no campo **URL to attack**.

Clique no botão **Ataque** para iniciar o teste de segurança.

A varredura é demonstrada na parte inferior da Figura.



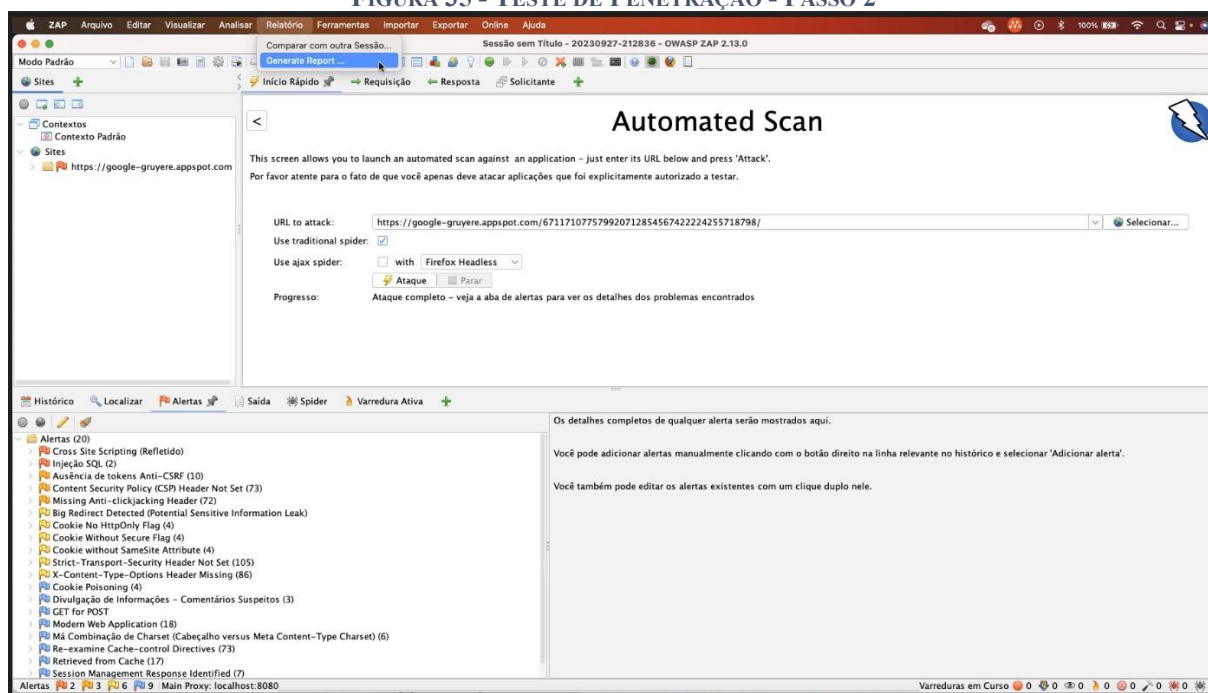
Fonte: Elaborado pelos autores, 2023

## Passo 2:

Após a conclusão da varredura, o resumo dos alertas será apresentado no canto inferior direito, conforme Figura 35.

No menu principal da ferramenta, clique no item **Relatório** e, em seguida, clique em **Generate Report** para gerar um relatório do teste.

FIGURA 35 - TESTE DE PENETRAÇÃO - PASSO 2



Fonte: Elaborado pelos autores, 2023

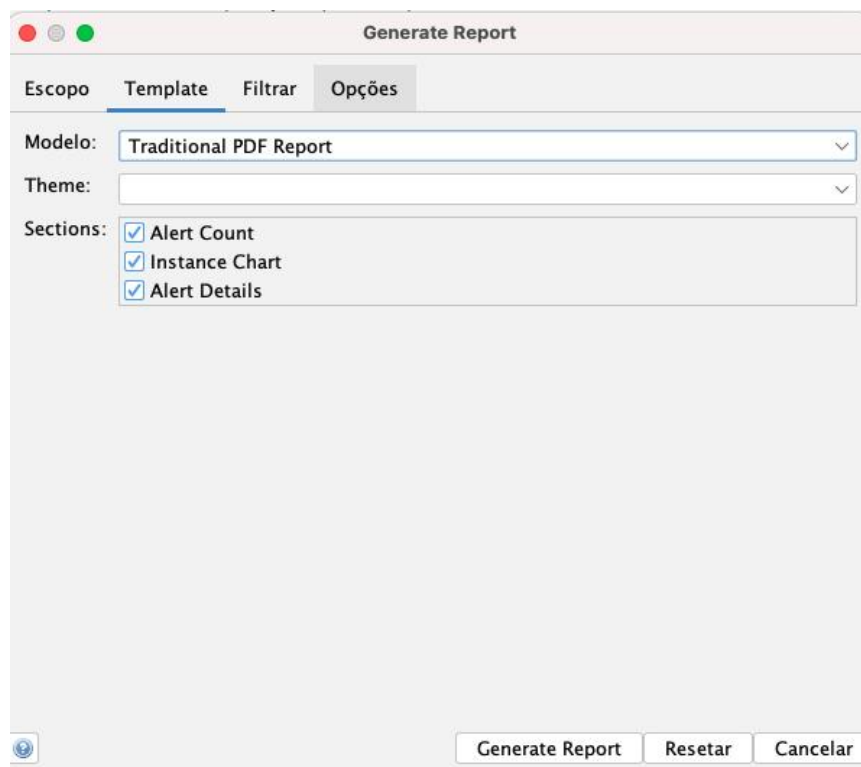
**Passo 3:**

Na Figura 36, selecione a guia **Template**.

No campo Modelo, selecione um de modelo (ex. **Traditional PDF Report**).

Clique em **Generate Report**.

FIGURA 36 - TESTE DE PENETRAÇÃO - PASSO 3



The image shows a 'Generate Report' window with four tabs: 'Escopo', 'Template', 'Filtrar', and 'Opções'. The 'Template' tab is active. It contains the following fields:

- Modelo:** A dropdown menu showing 'Traditional PDF Report'.
- Theme:** An empty dropdown menu.
- Sections:** A list of three items, each with a checked checkbox:
  - ☒ Alert Count
  - ☒ Instance Chart
  - ☒ Alert Details

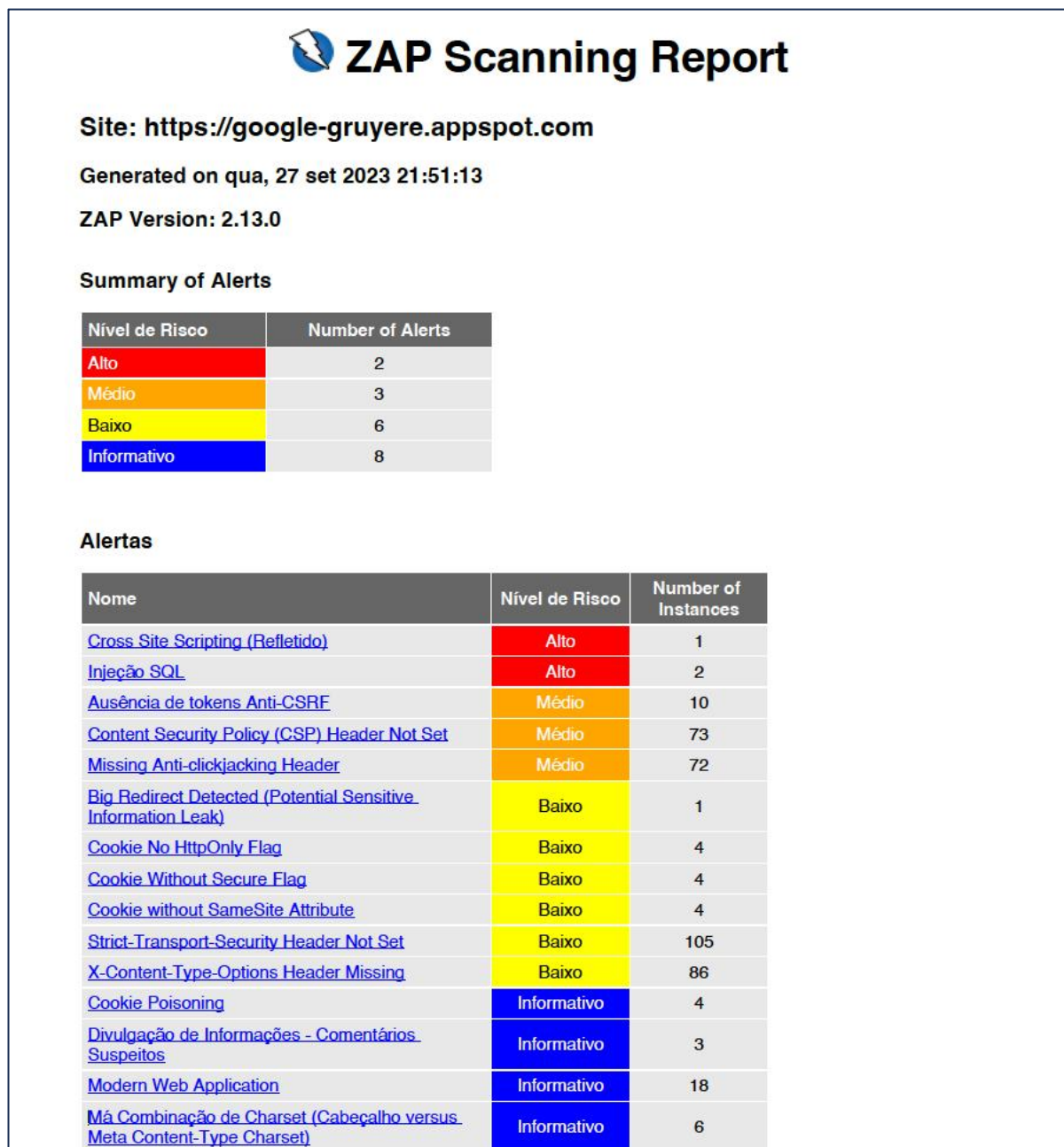
At the bottom right, there are three buttons: 'Generate Report', 'Resetar', and 'Cancelar'.

Fonte: Elaborado pelos autores, 2023

**Passo 4:**

A Figura 37 apresenta um exemplo de relatório gerado.

FIGURA 37 - TESTE DE PENETRAÇÃO - PASSO 4



Fonte: Elaborado pelos autores, 2023