



**INSTITUTO FEDERAL DE EDUCAÇÃO,  
CIÊNCIA E TECNOLOGIA DO AMAPÁ**  
Campus Macapá

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ  
CAMPUS MACAPÁ  
CURSO TECNOLOGIA EM REDES DE COMPUTADORES

LUCAS MATEUS OLIVEIRA DO CARMO  
YRLLAN BRANDÃO BRAGA

**IPS SNORT E SURICATA:** análise do impacto no desempenho da rede enquanto  
atuam inline

MACAPÁ – AP  
2022

LUCAS MATEUS OLIVEIRA DO CARMO  
YRLLAN BRANDÃO BRAGA

**IPS SNORT E SURICATA:** análise do impacto no desempenho da rede enquanto atuam inline

Trabalho de Conclusão de Curso apresentado ao Curso tecnologia em redes de computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores Orientador: Me. Thiêgo Maciel Nunes

MACAPÁ - AP  
2022

Biblioteca Institucional - IFAP  
Dados Internacionais de Catalogação na Publicação (CIP)

---

- C287i Carmo, Lucas Mateus Oliveira do  
IPS Snort e Suricata: análise do impacto no desempenho da rede enquanto atuam inline / Lucas Mateus Oliveira do Carmo, Yrllan Brandão Braga. - Macapá, 2022.  
55 f.: il.
- Trabalho de Conclusão de Curso (Graduação) -- Instituto Federal de Educação, Ciência e Tecnologia do Amapá, Campus Macapá, Curso de Tecnologia em Redes de Computadores, 2022.
- Orientador: Me. Thiêgo Maciel Nunes.
1. IPS. 2. Snort. 3. Suricata. I. Braga, Yrllan Brandão. I. Nunes, Me. Thiêgo Maciel, orient. II. Título.

LUCAS MATEUS OLIVEIRA DO CARMO  
YRLLAN BRANDÃO BRAGA

**IPS SNORT E SURICATA:** análise do impacto no desempenho da rede enquanto atuam inline

Trabalho de Conclusão de Curso apresentado ao Curso tecnologia em redes de computadores do Instituto Federal de Educação, Ciência e Tecnologia do Amapá, em cumprimento às exigências legais como requisito parcial à obtenção do título de Tecnólogo em Redes de Computadores Orientador: Me. Thiêgo Maciel Nunes

BANCA EXAMINADORA:

*Thiêgo Maciel Nunes*

---

Prof. Me. Thiêgo Maciel Nunes

*f. L. L. L.*

---

Prof. Esp. Francisco Sanches da Silva Junior

*Celso do Nascimento Rodrigues*

---

Prof. Me. Celio do Nascimento Rodrigues

Apresentado em: 21 / 11 / 2022

Conceito/Nota: 8,8

À minha falecida mãe Gizelle, que criou sozinha eu e meu irmão.

**Lucas do Carmo**

Dedico este trabalho aos meus pais e meus irmãos que sempre me apoiaram durante minha trajetória.

**Yrllan Brandão**

## **AGRADECIMENTO**

A todos nossos colegas que de algum modo ajudaram no nosso aprendizado.

Ao professor Thiêgo por ter aceitado ser nosso orientador, aos demais professores que também foram importantes na nossa jornada.

Aos nossos familiares que sempre estiveram nos apoiando mesmo nos momentos difíceis.

“Nós poderíamos ser muito melhores se não quiséssemos ser  
tão bons”

**Sigmund Freud**

## RESUMO

Quando se trata de segurança de redes, além do *firewall* que é uma ferramenta indispensável devido ao seu papel de filtragem de conteúdos externos direcionados a rede interna, existem vários outros instrumentos que atuam realizando a proteção da rede interna, como é o caso do IPS. Os sistemas de prevenção de intrusos podem contribuir significativamente com a segurança da rede, pois estes atuam realizando a leitura e análise dos pacotes que trafegam na rede e tomam determinada ação, conforme são configurados. Por atuarem realizando análises de todo o tráfego da rede, os sistemas de prevenção podem ter diferentes impactos no desempenho da mesma. Sendo assim, este estudo utiliza o sistemas de prevenção de intrusos Snort e Suricata e realiza a comparação dos efeitos de seus modo *inline* na rede, a fim de concluir qual deles ocasionou menos impacto na sua performance.

Palavras-chave: IPS; Snort; Suricata; Iperf3.



## **ABSTRACT**

When it comes to network security, in addition to the firewall, which is an indispensable tool due to its role of filtering external content directed to the internal network, there are several other instruments that act to protect the internal network, such as the IPS. Intrusion prevention systems can significantly contribute to network security, as they work by reading and analyzing packets that travel on the network and take a certain action, as they are configured. By performing an analysis of all network traffic, prevention systems can have different impacts on their performance. Therefore, this study uses the Snort and Suricata intrusion prevention systems and compares the effects of their inline mode on the network, in order to conclude which one caused the least impact on its performance

Keywords: IPS; Snort Suricata; Iperf3.

## LISTA DE FIGURAS

Figura 1 - Firewall	16
Figura 2 - Logo pFsense	17
Figura 3 - IPS em modo passivo	19
Figura 4 - IPS atuando em linha	20
Figura 5 - modelo de funcionamento iperf3	21
Figura 6 - rede base contendo apenas o firewall	26
Figura 7 - capacidade de transmissão do <i>host</i>	28
Figura 8 - Taxa de transferência média sem IPS	29
Figura 9 - Snort habilitado	30
Figura 10 - média de transmissão com Snort	31
Figura 11 - Suricata habilitado	32
Figura 12 - média de transmissão com Suricata	32
Figura 13 - média dos cenários de teste	33

## LISTA DE SIGLAS

GB	GigaByte
HIPS	Host Intrusion Prevention System
IDS	Intrusion Detection System
IOF	The Open Information Security Foundation
IPS	Intrusion Prevention System
MB	MegaByte
NBA	Network Behavior Analysis
NIPS	Network Prevention System
RAM	Random Access Memory
VPN	Virtual Private Network
WIPS	Wireless Intrusion Prevention System

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO</b>	<b>12</b>
1.1	<b>Objetivos</b>	13
1.1.1	Objetivos Gerais	13
1.1.2	Objetivos Específicos	13
<b>1.2</b>	<b>Justificativa</b>	<b>13</b>
1.3	<b>Metodologia</b>	14
<b>2</b>	<b>SEGURANÇA DE REDES</b>	<b>15</b>
<b>3</b>	<b>FERRAMENTAS</b>	<b>16</b>
3.1	<b>Firewall</b>	16
3.1.1	pfSense	16
3.2.	<b>Sistema de Prevenção de Intrusão (IPS)</b>	17
3.2.1	IPS Passivo e IPS Inline	18
3.2.2	Snort e Suricata	20
<b>3.3</b>	<b>Iperf3</b>	<b>21</b>
<b>4</b>	<b>REFERENCIAL TEÓRICO</b>	<b>23</b>
<b>5</b>	<b>DESENVOLVIMENTO</b>	<b>25</b>
5.1	<b>Teste sem IPS</b>	25
<b>5.2</b>	<b>Cenário de testes com IPS</b>	<b>29</b>
<b>6</b>	<b>CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS</b>	<b>34</b>
	<b>REFERÊNCIAS</b>	<b>35</b>
	<b>APÊNDICE A - Downloads de ferramentas</b>	<b>37</b>
	<b>APÊNDICE B - guia de instalação Pfsense</b>	<b>38</b>
	<b>APÊNDICE C - Guia de instalação IPS no firewall pfSense</b>	<b>51</b>

## 1 INTRODUÇÃO

Uma rede é um conjunto de nós interligados que podem trocar dados e compartilhar recursos uns com outros, segundo Forouzan (2007, p. 7) uma rede deve ser capaz de atender alguns critérios, dentre os mais importantes estão a segurança, desempenho e confiabilidade, No contexto moderno esses requisitos são cada vez mais necessários conforme as tecnologias avançam e os dados que circulam na *internet* se tornam alvo de pessoas mal-intencionadas, também conhecidas como cibercriminosos.

Para uma rede obter os critérios de confiabilidade e segurança, é fundamental que esta esteja protegida por mecanismos operacionais conhecidos, que geralmente fazem parte da estratégia de defesa de rede, dentre estes podemos citar o *firewall*, sistema de detecção de intrusão (IDS) e sistema de prevenção de intrusão (IPS), que segundo (Kurose; Ross, 2013), atuam na entrada e saída de tráfego de uma rede, realizando uma inspeção de segurança, no qual o tráfego pode ser registrado, descartado ou transmitido.

Ao utilizarmos ferramentas de proteção de rede devemos evitar que as mesmas acabem impactando o desempenho da rede com a geração de gargalos e problemas relacionados ao fluxo de dados, segundo (Kurose; Ross, 2013) o desempenho de aplicações da internet como navegação, *e-mail* e voz sobre ip(VoIP) é bastante afetado devido a atrasos na rede, portanto devemos levar isso em consideração quando fazemos usos de aplicações que trabalham com a análise de tráfego, pois dependendo do posicionamento, pode afetar a rede negativamente.

O bom desempenho de uma rede não depende somente dos mecanismos de segurança que a mesma possui, conforme Forouzan (2007), a performance da rede depende de vários fatores como número de usuários, meio de transmissão e capacidades de hardware, tendo isso em mente devemos encontrar um equilíbrio saudável entre segurança da rede e desempenho.

Este estudo busca verificar qual sistema de prevenção de intrusão causa menos impacto no desempenho de rede através da comparação das ferramentas Snort e Suricata, atuando em modo *inline* em uma rede composta por dois computadores e um *firewall*, ambos rodando no virtualbox. Para os testes foi utilizada a ferramenta Iperf3 que é capaz de medir o desempenho da rede.

## 1.1 Objetivos

Este trabalho apresenta os objetivos gerais descritos no item 1.1.1 e os objetivos específicos descrito no item 1.1.2

### 1.1.1 Objetivos Gerais

Realizar uma análise comparativa dos impactos dos sistemas de prevenção de intrusão Snort e Suricata em modo *inline* quando implementados em uma rede.

### 1.1.2 Objetivos Específicos

- a) Realizar testes de desempenho antes da implementação dos sistemas de prevenção de intrusão;
- b) Verificar o desempenho da rede com os sistema de prevenção de intrusão implementados;
- c) Observar e avaliar se alguma das ferramentas teve menos impacto na rede.

## 1.2 Justificativa

Para prevenir e combater invasões são necessários o uso de ferramentas e mecanismos de defesa sofisticados capazes de neutralizar as ações do invasor de forma rápida a fim de reduzir danos aos sistemas. Os mecanismos de segurança podem ser a nível de hardware e software e podem variar de acordo com a necessidade da rede e de acordo com a estratégia de segurança adotada pelo administrador da rede.

O uso do Sistema de Prevenção de Intrusão (IPS) se tornou uma das alternativas usadas pelos administradores de rede para ajudar a manter o ambiente de trabalho protegido contra possíveis invasores que tem a intenção de invadir a rede e subtrair dados na intenção de obter compensação financeira ou apenas destruir informações por motivos de represália, o último geralmente se tratando de um invasor interno.

Apesar de ser de grande importância a adoção de ferramentas eficazes na proteção da rede, é preciso também levar em consideração os problemas que estes podem causar, analisando de forma objetiva, se tal ferramenta trará mais benefícios ou malefícios quando estiver implementada na rede.

No caso do IPS, cuja principal função quando atuando ativamente na rede, é analisar todo o tráfego de pacotes que estão passando na mesma e caso ocasionalmente um venha comprometer a integridade dos dispositivos nela conectados, ele será capaz de bloqueá-lo. Entretanto, quando trabalha fazendo a análise dos pacotes que trafegam pela rede, é possível que o IPS acabe congestionando a rede fazendo com que ela fique lenta ou até mesmo que os *end points* fiquem sem se comunicar..

A importância da implementação e análise dos IPS Snort e Suricata em uma rede é o impacto causado nela quando requisitado a analisar uma grande quantidade de tráfego que foi gerado através de uma ferramenta específica, haja vista que além de ser eficaz no que se diz respeito a segurança o IPS também não deve prejudicar o bom funcionamento da rede, logo é preciso uma comparação das duas distribuições distintas para se ter um consenso de qual ferramenta se sobressai sem causar maiores transtornos para os administradores e usuários da rede.

### 1.3 Metodologia

Para verificar a hipótese levantada pelo estudo, foram realizadas análises de desempenho de uma rede com a ferramenta iperf3 levando em consideração três cenários, todos utilizando o *firewall* pfsense mas com diferenças nos sistemas de prevenção de intrusão.

No primeiro cenário foram realizadas análises em uma rede apenas com *firewall*, sem nenhum sistema de prevenção de intrusão. No segundo cenário a análise de desempenho é realizada em uma rede que possui o sistema de prevenção de intrusão Snort. Por último, no terceiro a rede possui o sistema de prevenção de intrusões da Suricata.

Com base nestes cenários espera-se concluir qual IPS menos impactou no desempenho da rede.

## 2 SEGURANÇA DE REDES

Apesar desse trabalho tratar de análise e desempenho de rede, é importante falar sobre segurança de redes visto que as ferramentas usadas no estudo também são utilizadas para melhorar a segurança da rede na qual são implementadas. Como podemos ver em Kurose e Ross (2013,p.496) nos dias de hoje, a maioria das organizações possuem redes conectadas a internet pública, com isso elas se tornam suscetíveis a ataques de invasores externos, que quando obtém sucesso na invasão podem comprometer o funcionamento de toda a rede. Deste modo, mecanismos como o *firewall* e o IPS trabalham em conjunto com os administradores da rede fazendo a proteção e a prevenção contra eventuais ataques. Para que haja os chamados três pilares da segurança da informação, é necessário confidencialidade, integridade e disponibilidade, visto que é preciso que haja segurança tanto na origem quanto no destino. Assim, além dos mecanismos de defesa já citados, também se fez necessário o uso de métodos que impossibilitem a captação de dados quando eles passam por uma rede pública, como o chamado protocolo IP de segurança, também conhecido como IPsec, que de acordo com Kurose e Ross (p.528) é responsável por prover segurança na camada de rede, protegendo os datagramas IP entre todas entidades da camada de rede, incluindo hospedeiros e roteadores. Vale citar outro método bastante utilizado que é a VPN (*Virtual Private Network*) que apesar de utilizar uma rede pública para envio dos pacotes, possui segurança devido seu uso de criptografia.



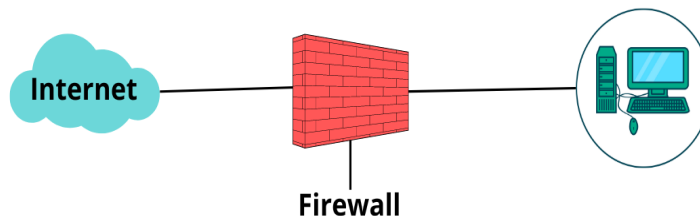
### 3 FERRAMENTAS

Este capítulo aborda ferramentas relacionadas aos objetos alvo da pesquisa.

#### 3.1 Firewall

O *firewall* atua na camada de aplicação e é um dos responsáveis pela filtragem do tráfego de determinada rede de acordo com as políticas de segurança que nela atuam. “Todo o tráfego de dentro para fora e vice-versa precisam passar pelo *firewall*” (STALLINGS,2006), ou seja: o *firewall* funciona como uma barreira que protege a rede interna de uma rede externa, conforme demonstrado na figura 1.

Figura 1 - *Firewall*



Fonte:Carmo e Braga, 2022

##### 3.1.1 pfSense

O pfSense é uma distribuição *firewall* de código aberto e gratuito, ele é o baseado no sistema *FreeBSD* e é uma solução robusta que serve para proteção de redes nos mais variados cenários, além disso, segundo (NETGATE, 2021) uma das principais funcionalidades do Pfsense é a filtragem de tráfego, analisando qual tráfego deverá passar e qual será bloqueado

Figura 2 - logo pfSense



Fonte: kindpng

### 3.2 Sistema de Prevenção de Intrusão (IPS)

O IPS (*Intrusion Prevention System*) é um conjunto de mecanismos com a função de prevenção de intrusão. Suas ações de prevenção são a detecção de invasões, emissão de alertas, bloqueio de arquivos maliciosos e bloqueio de tráfego suspeito a fim de neutralizar eventuais ameaças aos sistemas no qual o mecanismo está instalado.

O sistema de prevenção de intrusão podem ser implementado a nível de *hardware* ou *software* e esta escolha está subordinada às necessidades e orçamento das instituições, ele também pode ser classificado como HIPS (*Host Intrusion Prevention System*), WIPS (*Wireless Intrusion Prevention System*), NBA (*Network Behavior Analysis*), todos estes apenas para fins informativos e não serão abordados no trabalho. Apenas o NIPS (*Network Intrusion Prevention System*), foi utilizado em nossa pesquisa e será tratado apenas como IPS.

Segundo Vmware (s.d) o IPS utiliza alguns métodos para fazer a filtragem de pacotes que são:

- Baseado em assinatura- Esse método assim como sugere o nome, utiliza assinaturas conhecidas para fazer o bloqueio dos pacotes. Sua desvantagem é que se não obtiver as vacinas ele não reconhecerá novas assinaturas.
- Baseado em anomalias- A técnica trabalha analisando e comparando amostras obtidas aleatoriamente do tráfego da rede. Isso pode ocasionar a obtenção de falsos positivos, que é quando a ferramenta entende que pacotes legítimos podem ser danosos.

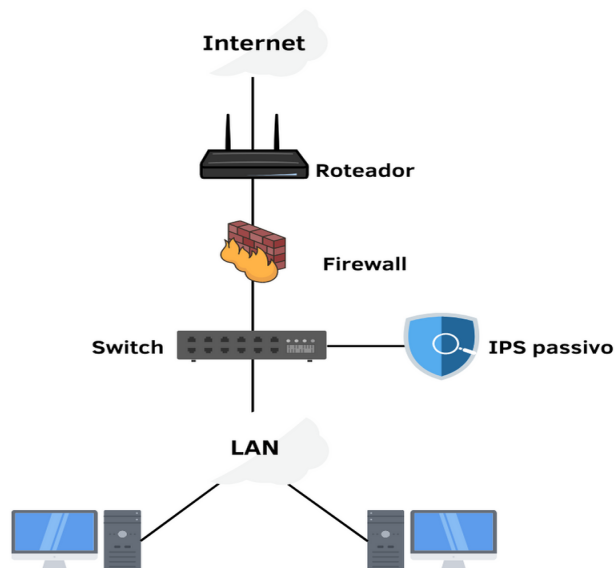
- Baseados em políticas - O administrador da rede é quem define quais políticas serão utilizadas pelo IPS para fazer a filtragem dos pacotes que trafegam pela rede.

### 3.2.1 IPS Passivo e IPS *Inline*

Quando implementamos um sistema de prevenção de intrusão na rede podemos optar por o utilizarmos em seu modo passivo, também conhecido como IDS, que segundo (JEYASHANKAR, 2021) atua recebendo um cópia dos dados que circulam na rede para analisá-los em paralelo ao tráfego real, deste modo ele é capaz de analisar e gerar alertas para o administrador mas não tomar medidas para realizar o bloqueio do tráfego.

Na figura 3 podemos verificar o IPS passivo posicionado de forma que ele irá receber uma cópia dos dados, analisar e alertar o administrador em caso de tráfego suspeito para que sejam feitas ações a fim de evitar que o tráfego suspeito possa causar algum dano na rede. O IPS passivo também pode ser configurado para reiniciar a conexão do invasor, mas o ataque já pode ter sido bem sucedido antes da ação do IDS ou do administrador da rede.

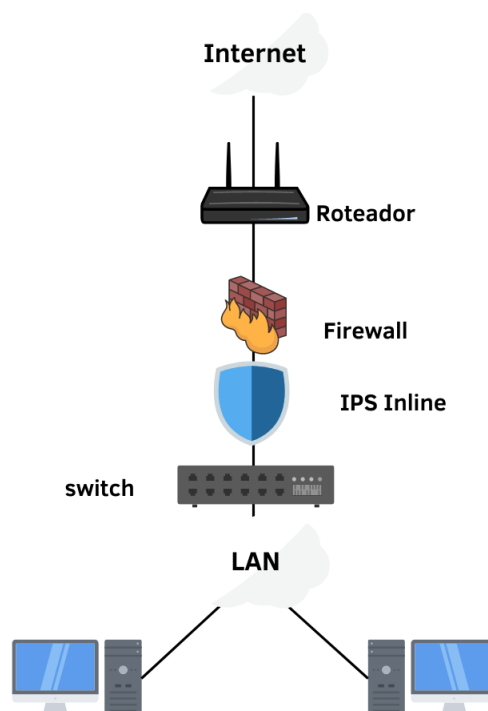
Figura 3 - IPS em modo passivo



Fonte: Carmo e Braga, 2022

Além do seu modo passivo, podemos configurar o IPS em modo *inline* ou modo em linha, que trata-se da forma como o IPS estará posicionado na rede e como tratará o tráfego, podemos verificar na figura 4 um exemplo de IPS *inline* posicionado de forma com que o tráfego original obrigatoriamente seja analisado antes que chegue ao destino, segundo (JEYASHANKAR, 2021) trabalha analisando o tráfego ao vivo e, portanto, pode bloquear ativamente os pacotes antes que eles cheguem ao seu destino

Figura 4 - IPS atuando em linha



Fonte: Carmo e Braga, 2022

### 3.2.2 Snort e Suricata

O Snort é um sistema de prevenção de intrusão de código aberto (*open-source*) que utiliza conjunto de regras que contribuem com a proteção da rede a medida em que define como os dados que trafegam na rede deverão ser tratados, o Snort é o IPS mais implementado no mundo, possuindo cerca de 5 milhões de instalações e uma base de 600.000 usuários cadastrados (SNORT, 2018).

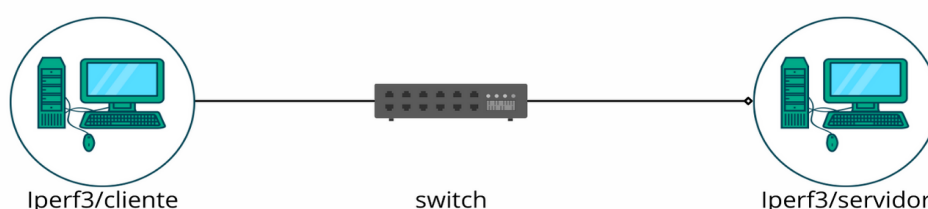
Para realizar a análise do tráfego em rede o Snort faz uso de conjuntos de regras para definir como agir, os conjuntos de regras são divididos em regras para assinantes (*Snort Subscriber Rules*), que segundo (SNORT, 2015) são desenvolvidas, testadas e aprovadas pela Cisco Tales. E as regras da comunidade (*Snort GPLv2 Community Rules*) que estão disponíveis para todos gratuitamente, ao utilizarmos qualquer um desses conjuntos podemos fornecer melhor proteção para a rede.

Suricata é uma solução IPS de alta performance que atua na proteção da rede, segundo (SURICATA, 2021) a ferramenta é capaz de realizar a análise de diversos gigabits de tráfego com uma única instância, a ferramenta pode inspecionar o tráfego em busca de anomalias com metodologia de assinatura, que contribui para reconhecer assinaturas conhecidas e violações de políticas de segurança, assim como outros sistemas de prevenção e detecção, o suricata pode ser integrado com outras aplicações de segurança.

### 3.3 Iperf3

O IPerf3 é uma ferramenta *open-source* e multiplataforma desenvolvida pela ESnet, esta ferramenta é utilizada para medição de largura de banda e utiliza a arquitetura cliente-servidor para medir a capacidade de transmissão da rede, na figura 5 podemos ver o modelo cliente-servidor no qual o host configurado como cliente transmitirá tráfego para o servidor a fim de verificar quantos pacotes chegaram ao destino, o servidor por sua vez recebe o tráfego e relata a largura de banda, perda e outros parâmetros que podem ser configurados.

Figura 5 - modelo de funcionamento iperf3



Fonte:Carmo e Braga, 2022

O iPerf3 é uma ferramenta bastante versátil e pode ser configurada de várias formas conforme a necessidade dos testes, para isso devem ser utilizados parâmetros que ajudam a obter resultados precisos, na tabela 1 são demonstradas algumas das opções de comandos que foram utilizados durante os testes.

Tabela 1- Comandos do iperf3 que foram utilizados

COMANDOS DO IPERF3 QUE FORAM UTILIZADOS	
Opção de linha de comando	Descrição
-c , --cliente host	Execute o iPerf no modo cliente, conectando-se a um servidor iPerf em execução no host .
-n , --num n[KM]	O número de buffers a serem transmitidos. Normalmente, o iPerf envia por 10 segundos. A opção -n substitui isso e envia uma matriz de len bytes num vezes, não importa quanto tempo isso demore.
-D , --daemon	Executa o servidor em segundo plano como um daemon.
-s , --servidor	Execute o iPerf no modo servidor. (Isso permitirá apenas uma conexão iperf por vez)

Fonte: iperf.fr

## 4 REFERENCIAL TEÓRICO

A comunicação em redes ocorre entre dois pontos que utilizam protocolos em comum para troca de dados, segundo Forouzan (2007) os protocolos são conjuntos de regras responsáveis por tornar possível a conexão entre duas entidades, isso ocorre porque as entidades que fazem parte da comunicação devem saber o que será comunicado, quando e o como será comunicado.

Com o avanço tecnológico de comunicações de dados, além dos cuidados com a segurança da rede, também torna-se cada vez mais necessário darmos atenção no desempenho da rede, haja vista a importância da velocidade na troca de informações e as possíveis perdas que atrasos podem causar.

As pesquisas em comunicações de dados e redes resultaram em novas tecnologias. Um dos objetivos é estar apto a trocar dados como texto, áudio e vídeo de todas as partes do planeta. Queremos acessar a Internet para fazer download e upload de informações de forma rápida e precisa e a qualquer momento. (Forouzan, 2007).

Conforme Kurose e Ross (2013, p.26), o trajeto dos pacotes começa em um sistema final (origem) passam por vários roteadores para chegar a outro sistema final (destino), Entretanto enquanto o pacote viaja de um nó para outro ele pode sofrer diversos tipos de atraso. Tais atrasos ocorrem por uma série de fatores que envolvem desde largura de banda até congestionamento no tráfego da rede devido ao uso de ferramentas de segurança que fazem a análise dos pacotes recebidos, como por exemplo o IPS.

O uso de ferramentas de detecção e prevenção de intrusões em redes de computadores é considerada uma área em grande expansão e constante evolução, novas técnicas surgem a todo tempo, tanto as utilizadas por invasores quanto as usadas por administradores de redes, para fazer a proteção de seus dados.

O mundo da segurança, seja pensando em violência urbana ou em hackers, é peculiar. Ele é marcado pela evolução contínua, no qual novos ataques têm como resposta novas formas de proteção, que levam ao



desenvolvimento de novas técnicas de ataques, de maneira que um ciclo é formado.( Nakamura; Geus, 2007,p 25).

Segundo Sousa (2016), ocorreu um aumento no número de tentativas de invasões a redes por programas mal intencionados, fazendo com que surgisse a necessidade de novas tecnologias de segurança capazes de fazer frente a estas tentativas de invasão, sendo capazes de detectar e bloquear eventos que possam comprometer a segurança da rede.

De acordo com Nakamura e Geus (2007,p 293) quando atua em modo *inline* o IDS fica caracterizado como IPS baseado em rede (NIPS). Isto se deve ao fato de que o IPS passa a atuar no front, filtrando todo o tráfego que passará pela rede, fazendo que além da sua capacidade de detectar ataques, também seja capaz de preveni-los.

É correto dizer que ele serve como proteção reforçada para os sistemas onde é implementado, para Dos Santos (2010, p.5) "As soluções de IPS utilizam múltiplas metodologias de detecção. Essas metodologias podem ser isoladas ou integradas a fim de proporcionar uma detecção mais exata".

## 5 DESENVOLVIMENTO

Neste capítulo será mostrado a montagem dos ambientes de testes conforme visto no último parágrafo da introdução. Os estudos foram feitos utilizando um computador com as seguintes especificações: processador *core i7* de nona geração, 16GB de memória ram, placa de vídeo integrada GeForce 940MX, os cenários foram criados dentro do *software* VirtualBox pela facilidade em restaurar as máquinas testes ao seu estados de origem a fim de realizarmos novas configurações, com o intuito de obtermos um resultado mais correto possível, foram configuradas máquinas virtuais com as seguintes configurações:

PC1 - processador Intel(R) Core™ i7-9700 CPU @ 3.00GHz × 2, 2GB de memória ram. Sistema operacional linux mint 21. Softwares instalados: iperf3.

PC2 -processador Intel(R) Core™ i7-9700 CPU @ 3.00GHz CPU @ 2.70GHz × 2, 2GB de memória ram. Sistema operacional linux mint 21. Softwares instalados: iperf3.

*Firewall* - processador Intel(R) Core™ i7-9700 CPU @ 3.00GHz × 2, 1GB de memória ram. Sistema operacional pfSense. Softwares instalados: Snort e Suricata.

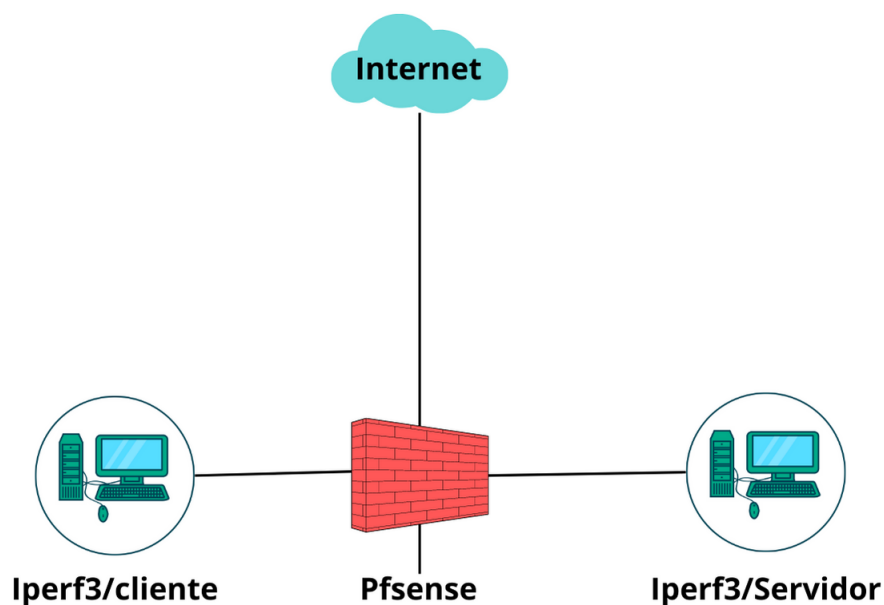
Este capítulo está dividido em três cenários, o primeiro cenário é demonstrado na seção 5.1.1 e aborda um rede composta de dois computadores e um *firewall*, esse cenário serve como base para os outros dois cenários, no segundo cenário, que será apresentado no item 5.2 temos o uso do primeiro cenário com o acréscimo do IPS snort em modo *inline*. Por fim, no último cenário, que também está presente no item 5.2 utilizamos o primeiro cenário como base mas com a diferença que foi implementado o IPS Suricata em modo *inline*.

### 5.1 Teste sem IPS

Antes de iniciarmos os testes de desempenho é fundamental obter a capacidade de transmissão dos *hosts* que serão utilizados durante o teste, a rede que será utilizada em todo o teste foi composta de dois computadores para atuação como cliente-servidor e o *pfSense* atuando como *firewall* conforme podemos observar na figura 6 o modelo de rede que será utilizada neste estudo, este modelo de rede é compatível com o funcionamento da ferramenta iPerf3, que utiliza o

modelo cliente-servidor, nesta etapa foram realizados testes para verificarmos a largura de banda dos *hosts*, que segundo Forouzan(2007) é elemento de desempenho de uma rede.

Figura 6 - rede base contendo apenas o firewall



Fonte:Carmo e Braga, 2022

A ferramenta iperf3 foi instalada utilizando o comando a seguir:

```
$ sudo apt install iperf3
```

Após a instalação foi escolhido um *host* para verificarmos a largura de banda, tendo em vista que ambos os hosts possuem as mesma configurações foi considerado a largura de banda para ambos, para iniciarmos a medição da largura de banda foram abertos dois terminais na mesma máquina, logo em seguida configuramos o primeiro terminal em modo servidor através do seguinte comando:

```
$ iperf3 -s
```

O comando `iperf3 -s` é responsável por deixar o *host* disponível em rede fazendo com que seja possível receber pacotes vindo de outros nós a fim de medir a quantidade de tráfego que chegou ao destino.

O segundo terminal `iperf3` foi configurado no modo cliente e se conecta ao próprio *host* através do endereço padrão 127.0.0.1, tendo cliente e servidor ativos na rede é iniciado a transmissão de pacotes para o servidor a fim de verificar a largura de banda utilizando o comando:

```
$ iperf3 -c 127.0.0.1
```

Depois de configurarmos cliente e servidor, foram realizadas transmissões de pacotes durante o intervalo de 10 segundos a fim de constatar a largura de banda do dispositivo, após este intervalo foi constatado que a capacidade de transmissão média do *host* é de 42.6 Gigabits por segundo, este resultado é demonstrado na figura 7, nela podemos verificar as transmissões realizadas pela máquina cliente, o total de pacotes transmitidos e a taxa de transmissão suportada pelo *host*.

Figura 7 - capacidade de transmissão do *host*

```

-----
Server listening on 5201
-----
Accepted connection from 127.0.0.1, port 50198
[ 5] local 127.0.0.0 port 5201 connected to 127.0.0.1 port 50200
[ ID] Interval      Transfer    Bitrate
[ 5]  0.00-1.00    sec  4.62 GBytes 39.7 Gbits/sec
[ 5]  1.00-2.00    sec  4.84 GBytes 41.6 Gbits/sec
[ 5]  2.00-3.00    sec  5.13 GBytes 44.1 Gbits/sec
[ 5]  3.00-4.00    sec  4.81 GBytes 41.3 Gbits/sec
[ 5]  4.00-5.00    sec  4.88 GBytes 41.9 Gbits/sec
[ 5]  5.00-6.00    sec  4.63 GBytes 39.7 Gbits/sec
[ 5]  6.00-7.00    sec  5.22 GBytes 44.8 Gbits/sec
[ 5]  7.00-8.00    sec  5.02 GBytes 43.1 Gbits/sec
[ 5]  8.00-9.00    sec  5.23 GBytes 44.9 Gbits/sec
[ 5]  9.00-10.00   sec  5.17 GBytes 44.4 Gbits/sec
[ 5] 10.00-10.00   sec  5.38 MBytes 34.3 Gbits/sec
-----
[ ID] Interval      Transfer    Bitrate
[ 5]  0.00-10.00   sec  49.6 GBytes 42.6 Gbits/sec
-----
receiver

```

Fonte: Carmo e Braga, 2022

A etapa foi dividida em 5 testes contabilizando 49.6 GBytes por cada transmissão, para recebermos os dados fornecidos pelo Iperf3 colocamos um host em modo servidor com o comando:

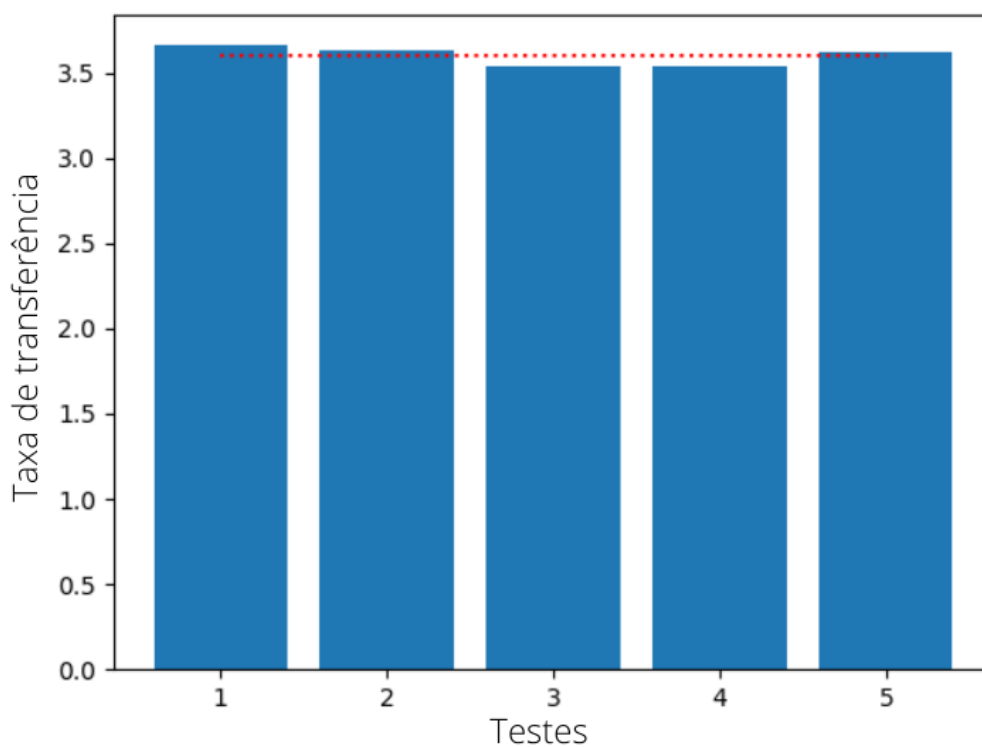
**\$ iperf3 -s**

em seguida para enviarmos dados com tamanho personalizado para o servidor utilizamos no *host* cliente o comando a seguir:

**\$ iperf3 -c 192.18.1.100 -n 51200MB**

Após realizarmos todos os 5 testes de desempenho, os resultados podem ser visualizados na figura 8.

Figura 8 - Taxa de transferência média sem IPS



Fonte: Carmo e Braga, 2022

Podemos verificar as taxas de transmissões de dados por teste e a média de transmissão, cada barra azul no gráfico representa 1 teste e a linha tracejada representa a média geral que foi 3,598 Gbits/s. este resultados serão úteis para compararmos com os resultados após a implementação dos IPS na rede.


## 5.2 Cenário de testes com IPS







Para os sistemas de prevenção de intrusos Snort e Suricata foram utilizadas na interface de rede LAN as seguintes regras:

- *Snort Subscriber Rules*
- *Snort GPLv2 Community Rules*
- *Emerging Threats Open Rules*

As regras 1 e 2 foram discutidas no item 3.2.2, a regra 3(Emerging threats Open Rules) são regras mantidas pela comunidade que utilizam diversas abordagens para identificação de ameaças como varreduras e busca por padrões de ataques contra alguns protocolos, a ação realizada pelo IPS após uma detecção de anomalia foi configurado para *DROP MODE*, ou seja, o IPS irá descartar todo o tráfego suspeito antes que chegue ao destino, na figura 9 podemos verificar que o IPS Snort está configurado para atuar em linha, filtrando e analisando todos os pacotes antes que eles cheguem ao destino, evitando que pacotes maliciosos passem antes de uma ação de segurança, por parte do IPS.

Figura 9 - snort habilitado

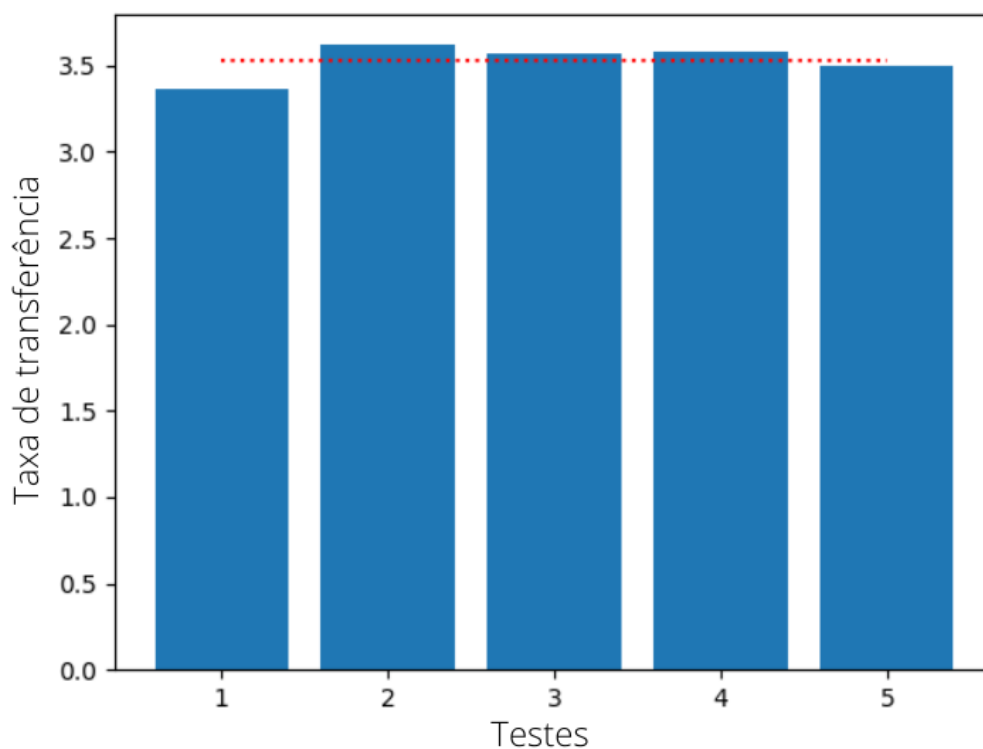


Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
<input type="checkbox"/> LAN (em1)	  	AC-BNFA	INLINE IPS	LAN	  

Fonte:Carmo e Braga, 2022

Após a finalização da configuração do Snort, foram iniciados os testes, enviando 50 Gbytes de dados a cada teste, os resultados podem ser visualizados na figura 10.

Figura 10 - média de transmissão com Snort



Fonte: Carmo e Braga, 2022

Na figura 9 podemos observar os testes realizados, representados pelas barras azuis e a taxa de transmissão média representada pela linha horizontal pontilhada, que equivale a média de 3.526 Gbits/s, esta média representou uma redução de 2% de desempenho em relação ao resultado sem IPS.

O IPS Suricata, também foi configurado em modo *inline* e habilitado na interface LAN, conforme pode ser observado na figura 11 o IPS Suricata já habilitado e com seu modo de atuação funcionando para bloqueio em linha após restaurarmos o pfSense para o modo inicial.



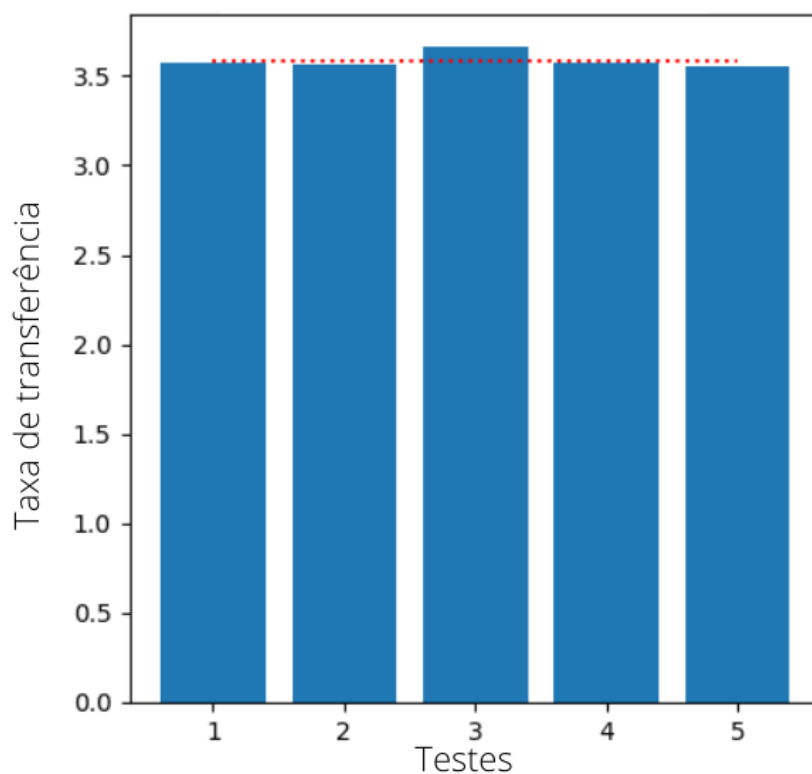
Figura 11 - Suricata habilitado

Interface Settings Overview					
Interface	Suricata Status	Pattern Match	Blocking Mode	Description	Actions
LAN (em1)		AUTO	INLINE IPS	LAN	

Fonte: Carmo e Braga, 2022

Para medição de desempenho com Suricata foram realizados 5 testes utilizando 50 Gbytes de dados por teste e foi realizado o cálculo mediano conforme feito com o Snort e também no teste sem o uso de IPS, os resultados de desempenho com o Suricata instalado podem ser observados na figura 12, nele podemos observar o gráfico de transmissões utilizando o Suricata, e seu valor médio que é de 3.582 Gbits/s.

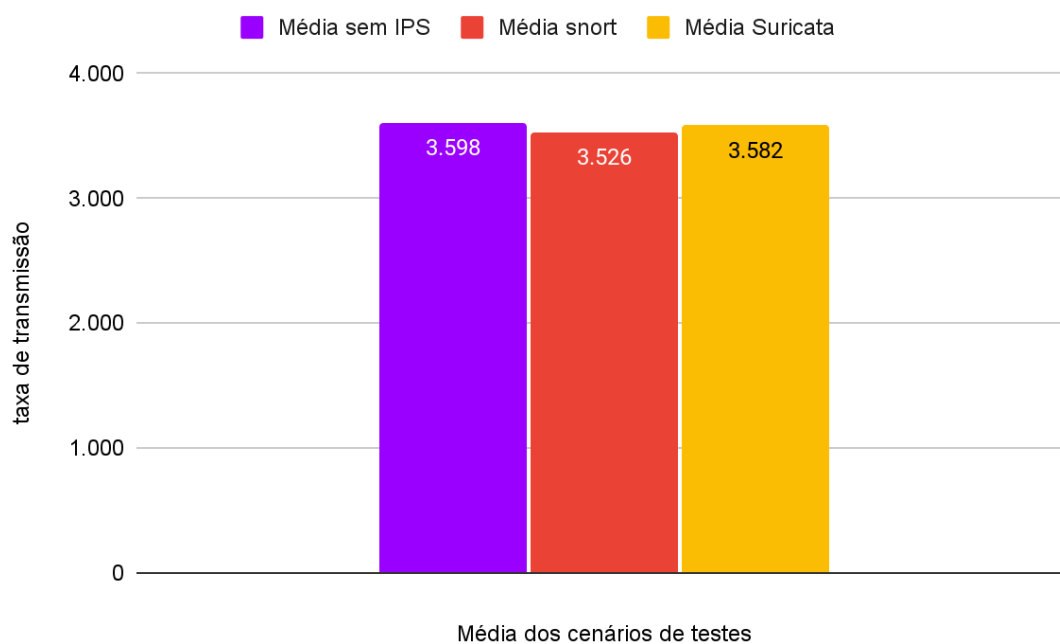
Figura 12 - média de transmissão com Suricata



Fonte: Carmo e Braga, 2022

Após finalizarmos os testes é possível verificarmos variações mínimas de desempenho em cada um dos cenários, na figura 13 podemos verificar a média de transmissão na rede nos cenários sem IPS, com Snort e com o suricata, respectivamente.

Figura 13 - média dos cenários de testes



Fonte: Carmo e Braga, 2022

Ao verificarmos a média de transmissão de cada cenário foi possível notar que a média de transmissão utilizando o IPS suricata teve uma redução de desempenho de 0.4% em relação aos testes sem IPS e uma vantagem de 1.5% de desempenho em relação ao Snort. O IPS Snort, por sua vez, apresentou uma redução de desempenho de 2.0% em relação ao cenário de teste sem IPS e uma desvantagem de 1.5% em relação ao Suricata.

## 6 CONSIDERAÇÕES FINAIS E TRABALHOS FUTUROS

Os Sistemas de prevenção de intrusos são atores importantes quando se trata de segurança de redes e contribuem significativamente com a manutenção dos princípios de segurança da informação, portanto o seu uso se torna imprescindível para ambientes que levam a segurança dos dados a sério, apesar dos inúmeros benefícios que a implementação de um IPS pode trazer para um rede, é necessário alguns cuidados para que eles não acabem por diminuir o desempenho da mesma, pensando nisso, este trabalho foi desenvolvido visando respostas em relação ao impacto individual no desempenho da rede causado por ferramentas que se propõe a lidar com a análise de dados de forma eficiente e segura.

Conforme o andamento do desenvolvimento do trabalho, fomos capazes de alcançar os objetivos estabelecidos durante o aperfeiçoamento da pesquisa, ao analisarmos os resultados e compararmos uns aos outros, pudemos verificar que a ferramenta Suricata se sobressaiu em relação ao Snort, entretanto é válido salientar que ambas ferramentas possuem formas de otimizar o processo de atuação das mesma e com isso, em outros cenários distintos, podem ou não divergirem dos resultados obtidos nesta pesquisa.

Desta forma o trabalho conseguiu obter resultados satisfatórios de acordo com nossos objetivos, entretanto nós sugerimos para trabalhos futuros sejam realizados testes utilizando outros conjuntos de regras, testes utilizando outras soluções IPS diferente de Snort e Suricata e testes utilizando o *firewall*, IPS e outras ferramentas de segurança da informação atuando em conjunto com as soluções anteriores.

## REFERÊNCIAS

AGRAWALN, R.; MUDZINGWA, D. **A study of methodologies used in intrusion detection and prevention systems (IDPS)**. 2012. Disponível em: <[https://www.researchgate.net/profile/Rajeev-Agrawal-3/publication/234082442\\_A\\_study\\_of\\_methodologies\\_used\\_in\\_intrusion\\_detection\\_and\\_prevention\\_system\\_IDPS/inks/542039120cf241a65a1b3c77/A-study-of-methodologies-used-in-intrusion-detection-and-prevention-system-IDPS.pdf](https://www.researchgate.net/profile/Rajeev-Agrawal-3/publication/234082442_A_study_of_methodologies_used_in_intrusion_detection_and_prevention_system_IDPS/inks/542039120cf241a65a1b3c77/A-study-of-methodologies-used-in-intrusion-detection-and-prevention-system-IDPS.pdf)>. Acesso em 12 de out. 2022.

**CARACTERÍSTICAS - Suricata**. 2021. Disponível em: <https://suricata.io/features/>. Acesso em: 23 ago. 2022.

Cisco, **Quais são os ataques virtuais mais comuns?**. Disponível em: <[https://www.cisco.com/c/pt\\_br/products/security/common-cyberattacks.html#~ty pes-of-cyber-attacks](https://www.cisco.com/c/pt_br/products/security/common-cyberattacks.html#~ty pes-of-cyber-attacks)>. Acesso em 10 de out. 2021.

DOS SANTOS, H. **Implantação de política de segurança e Sistemas de Detecção e Prevenção de Intrusos IDS/IPS**. 2010.a Disponível em: <<https://www.ppgia.pucpr.br/~jamhour/RSS/TCCRSS09A/Humberto%20dos%20Santos%20-%20Artigo.pdf>>. Acesso em 12 de out. 2022.

EMERGING THREATS. E. *In: The Open Information Security Foundation and Suricata*. [21--]. Disponível em: <<https://doc.emergingthreats.net/>>. Acesso em: 20 out. 2022.

FOROUZAN, Behrouz A.. **Comunicação de Dados e Redes de Computadores**. 4. ed. [S.I.]: Amgh, 2007. 1134 p.

GEUS, P. L.; NAKAMURA, E. T. **Segurança de redes em ambientes cooperativos**. Editora Novatec, 2007. Disponível em: <[https://books.google.com.br/books?id=AamSIJuLc34C&dq=info:UB1pfCvYYSUJ:scholar.google.com/&lr=&hl=pt-BR&source=gbs\\_navlinks\\_s](https://books.google.com.br/books?id=AamSIJuLc34C&dq=info:UB1pfCvYYSUJ:scholar.google.com/&lr=&hl=pt-BR&source=gbs_navlinks_s)>. Acesso em 12 out. 2022.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2008.

IPERF - **The ultimate speed test tool for TCP, UDP and SCTP**. [S. I.]. Disponível em: <<https://iperf.fr/iperf-doc.php>>. Acesso em: 20 out. 2022.

JEYASHANKAR, A. **IDS vs IPS: Key Differences , Rule Structure , Pros and Cons**. , 2021. Disponível em: <https://www.socinvestigation.com/ids-vs-ips-key-differences-rule-structure-pros-and-cons/>. Acesso em: 22 ago. 2022.

KUROSE, Jim; ROSS, Keith. **Redes de computadores e a Internet: uma abordagem top-down**. 6. ed. [S. I.]: Pearson Universidades, 2013. 656 p.

MELL, P.; SCARFONE, K. **Guide to intrusion detection and prevention systems (IDPS)**. NIST. 2007 Disponível em: <<https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-94.pdf>>. Acesso em 12 out. 2022.

NETGATE, **FIREWALL | Documentação do pfSense**. 2021. Disponível em: <<https://docs.netgate.com/pfsense/en/latest/firewall/index.html>>. Acesso em: 23 ago. 2022.

SOUSA, Givanildo Almeida de. **Sistema de prevenção e detecção de intrusões de rede utilizando a ferramenta IPS-SNORT**. 2016. 63 f. Monografia (Especialização em Rede de Computadores com ênfase em Segurança) - Instituto CEUB de Pesquisa e Desenvolvimento, Centro Universitário de Brasília, Brasília, 2016 Disponível em: <<https://repositorio.uniceub.br/jspui/handle/235/12393>>. Acesso em 20 out. 2022.

STALLINGS, William. **Criptografia e Segurança de Redes: Princípios e Práticas**. 4. ed. [S. l.]: Pearson Universidades, 2007. 502 p.

UFRJ, **Conceitos de IDS, IPS e IDPS**. 2012. Disponível em: <[https://www.gta.ufrj.br/grad/12\\_1/ids/ConceitodeIDS.html](https://www.gta.ufrj.br/grad/12_1/ids/ConceitodeIDS.html)>. Acesso em 10 de ago. 2022.

VMWARE, **What is an intrusion prevention system?**. 2022. Disponível em: <<https://www.vmware.com/topics/glossary/content/intrusion-prevention-system.html>>. Acesso em: 20 out. 2022.

## APÊNDICE A - Downloads de ferramentas

Este apêndice apresenta o link de todas as ferramentas neste estudo

### 1) Sistemas operacionais:

a) Linux mint: <https://www.linuxmint.com/download.php>

b) Pfsense: <https://www.pfsense.org/download/>

### 2) Outras ferramentas

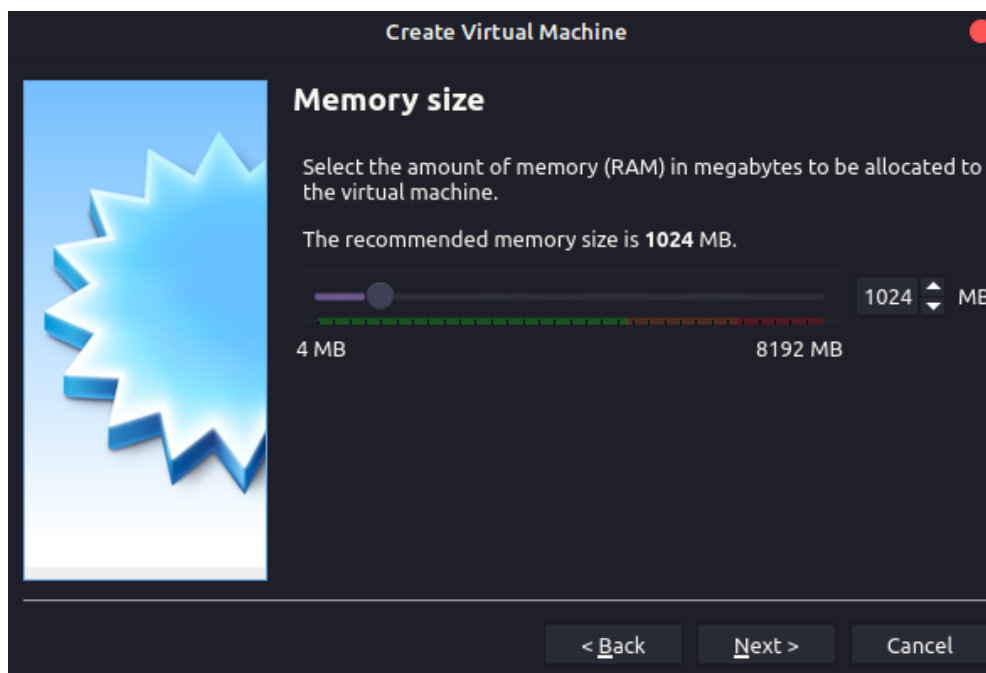
a) VirtualBox: [https://www.virtualbox.org/wiki/Linux\\_Downloads](https://www.virtualbox.org/wiki/Linux_Downloads)

## APÊNDICE B - guia de instalação Pfsense

- 1) Com o Virtualbox iniciado clique em *new* e insira um nome para a máquina virtual, em diretório, deixe a opção padrão, em *type* selecione a opção BSD e em *version* selecione FreeBSD (64-bit) e clique em *next*.



- 2) Agora selecione 1024MB de memória ram e clique em *next*.



- 3) Mantenha selecionada a opção *Create a virtual hard disk now* e clique em *create*.



4) Mantenha a opção VDI marcada e clique em *next*.

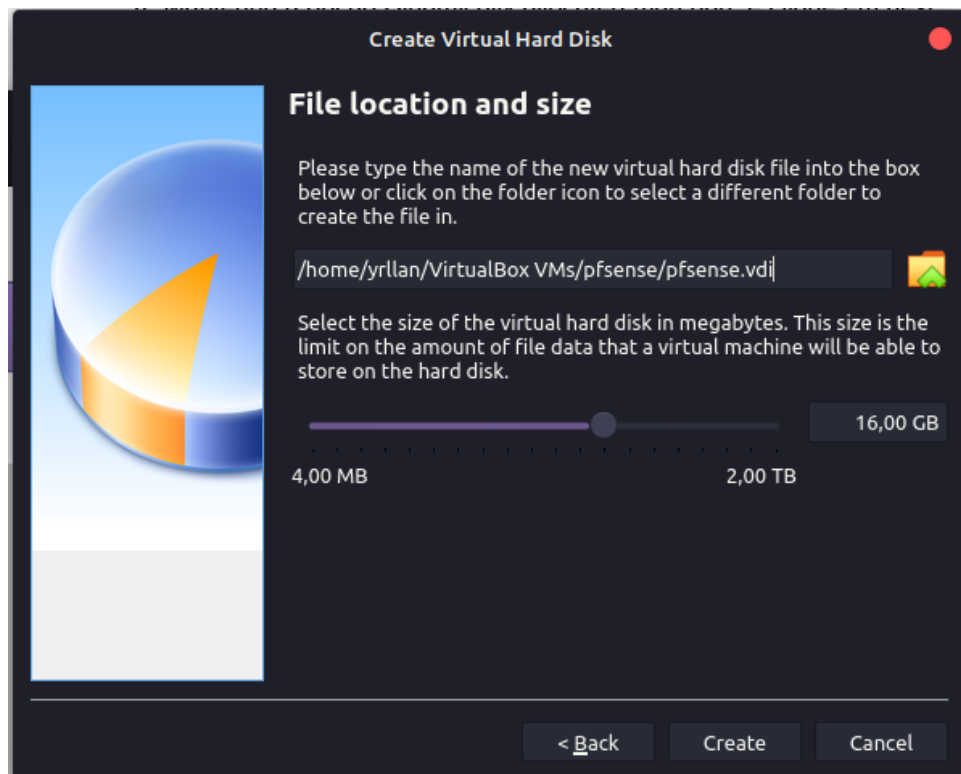




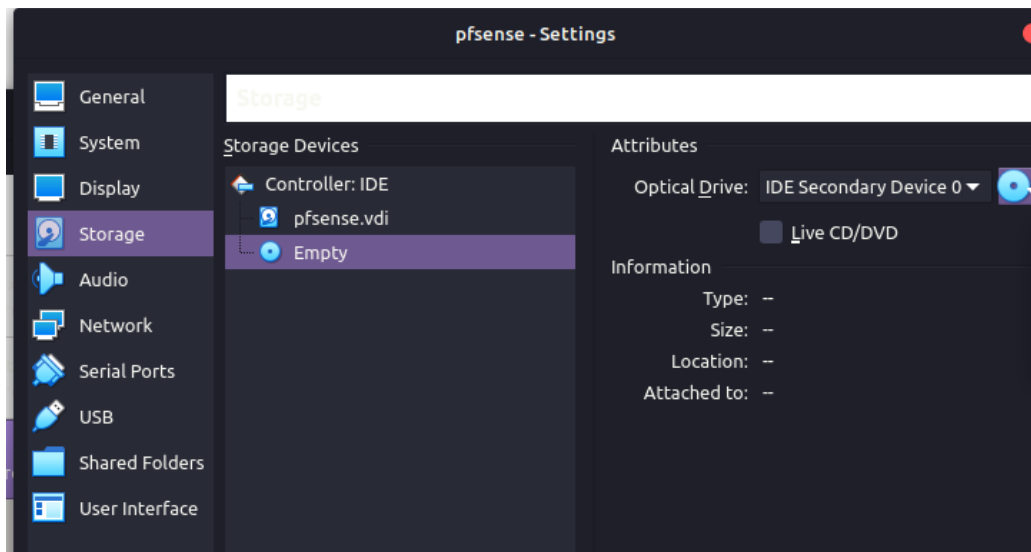
5) Mantenha a opção *Dinamically allocated* marcada e clique em *next*.



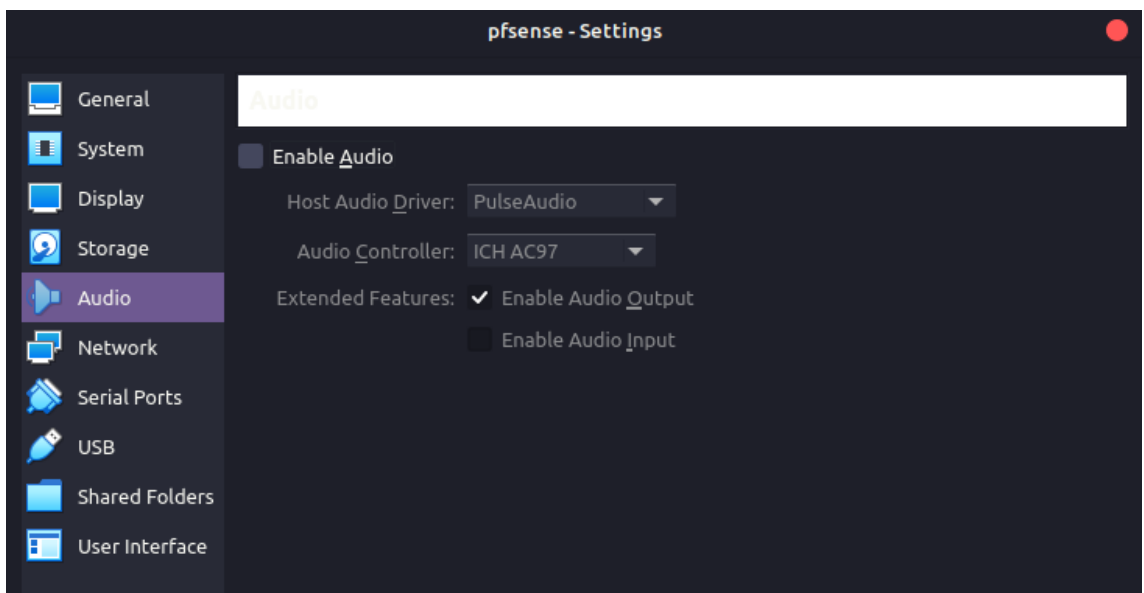
6) Seleccione o espaço em disco desejado e clique em *create*.



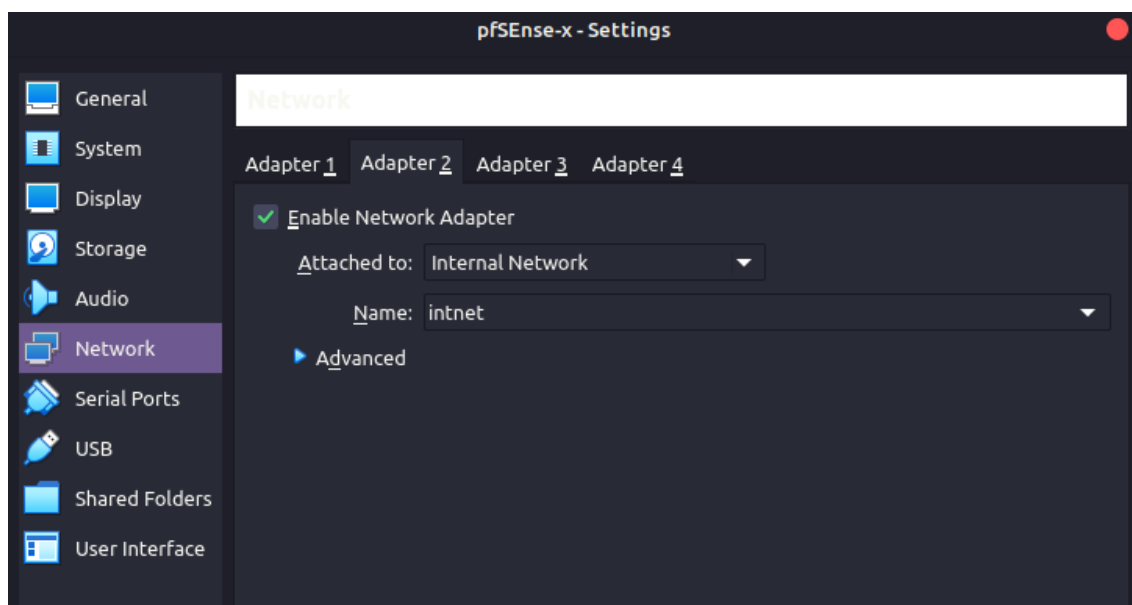
- 7) Clique na aba *Storage* > *Empty* > *Optical Drive* > clique no ícone de cd azul e selecione a iso do Pfsense > ok.



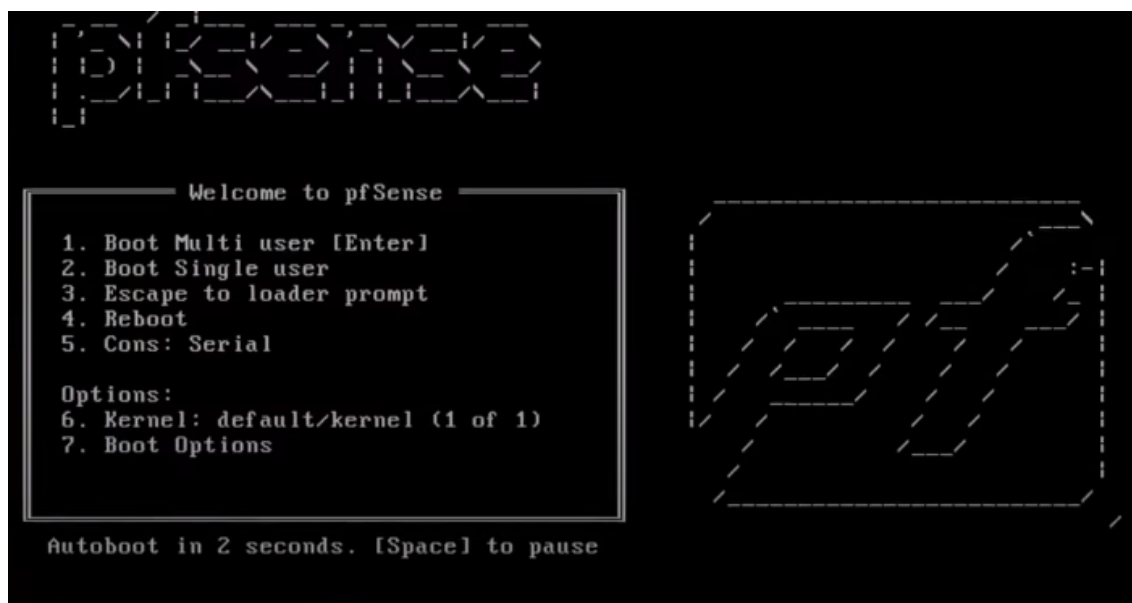
- 8) Selecione a máquina virtual > *settings* > aba *audio* > desmarque a opção *Enable Audio*.



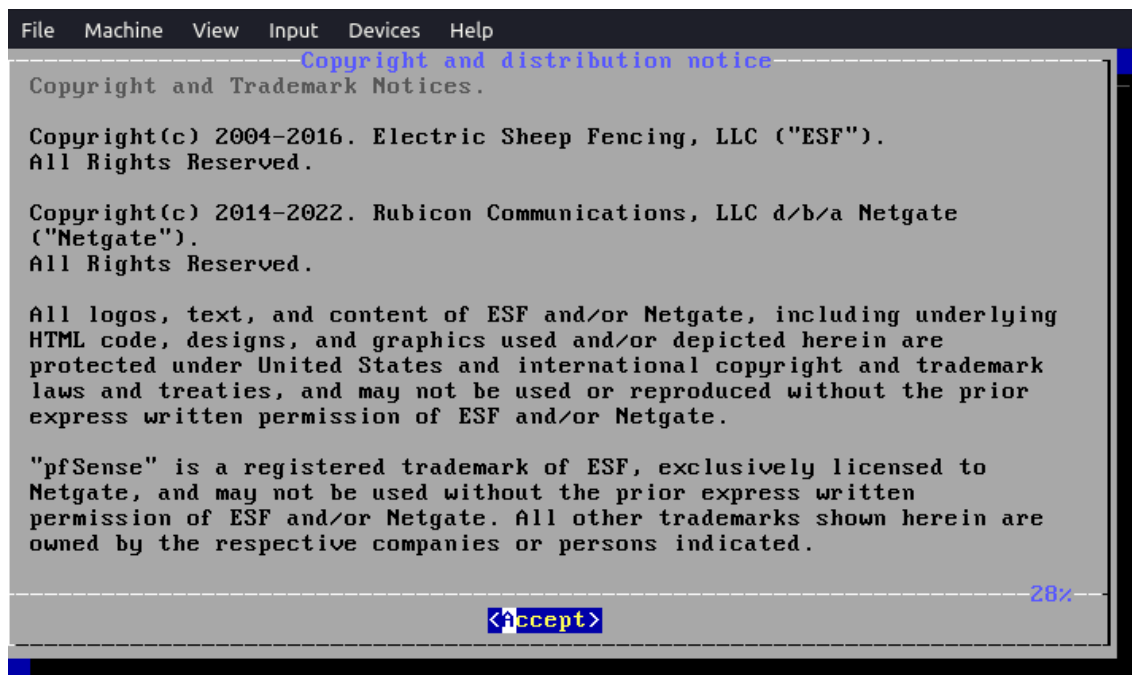
- 9) Clique em *Network* > *adapter 2* > *ative a opção Enable network Adapter* > *Attached to* > *internal network* > *ok*.



- 10) Agora inicie a máquina virtual clicando em *start*.



11) Após a inicialização pressione a tecla *Enter*.



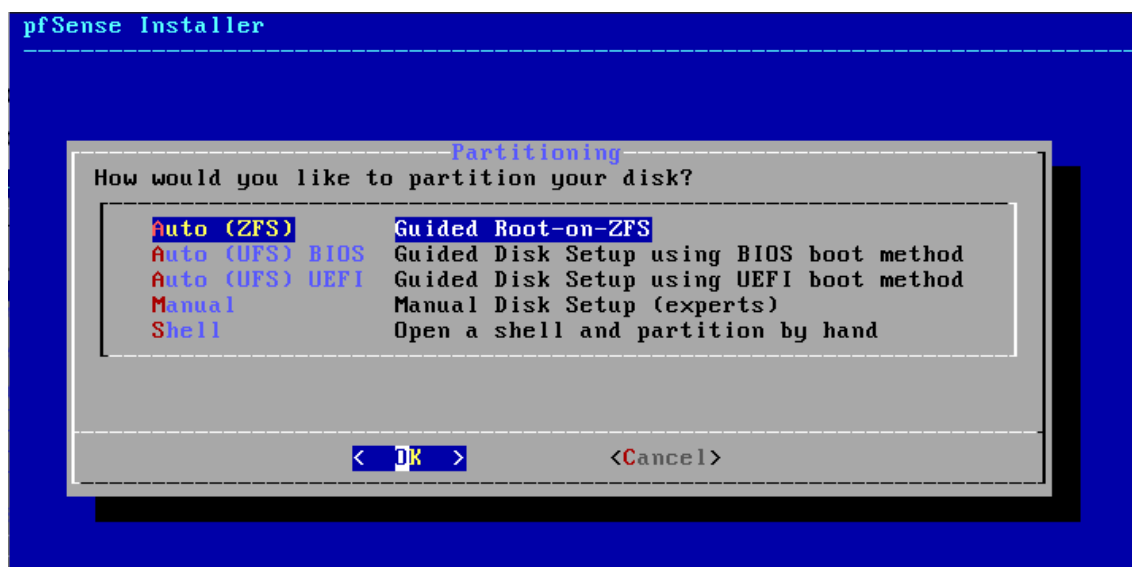
12) Nesta tela escolha a opção *install* e pressione *Enter*.



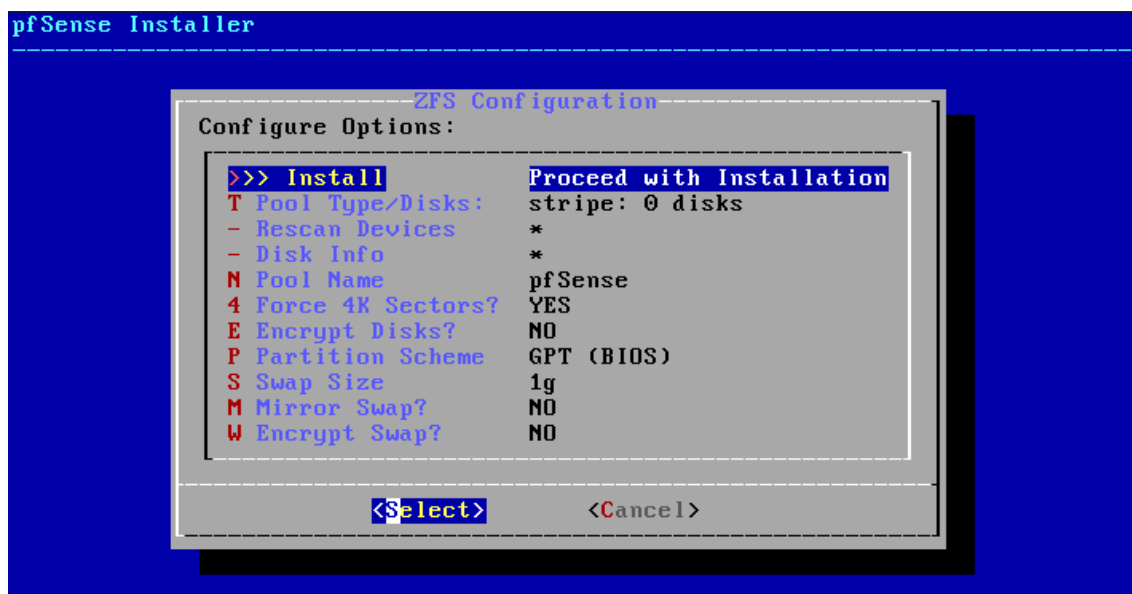
- 13) Nesta tela você pode escolher o formato do seu teclado, entretanto apenas utilizamos o teclado padrão pressionado *Enter*.



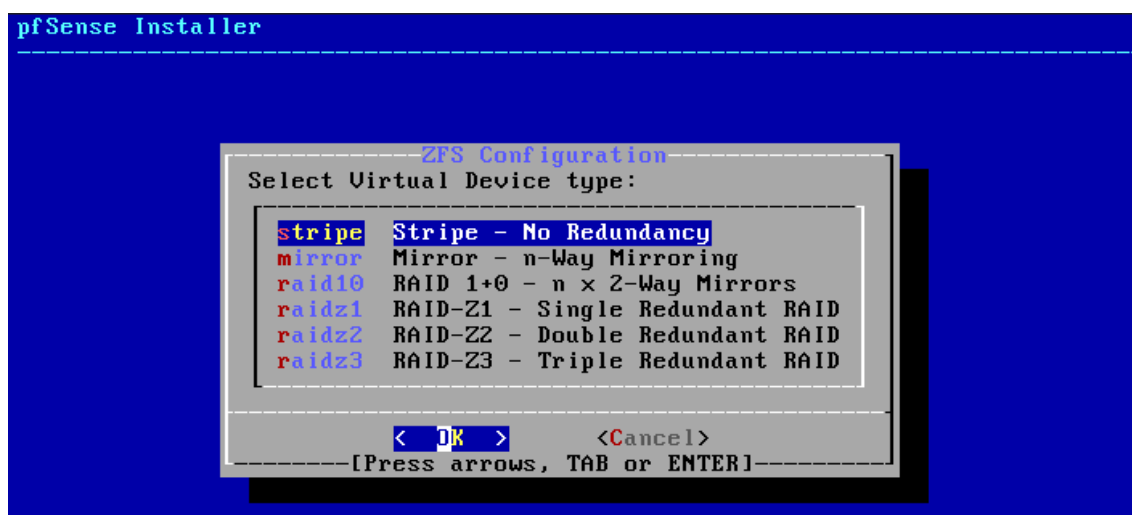
- 14) Nesta tela selecione a opção de partição *Auto* (ZFS) e pressione *Enter*.



- 15) Em configuração ZFS seleccione *install* e pressione *Enter*.



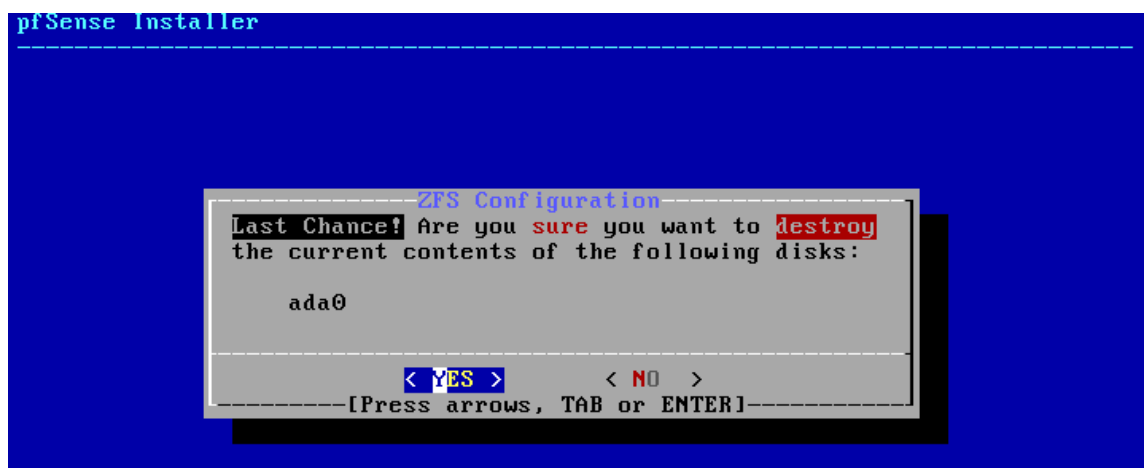
- 16) Nesta tela seleccione a opção *stripe* e pressione *enter*.



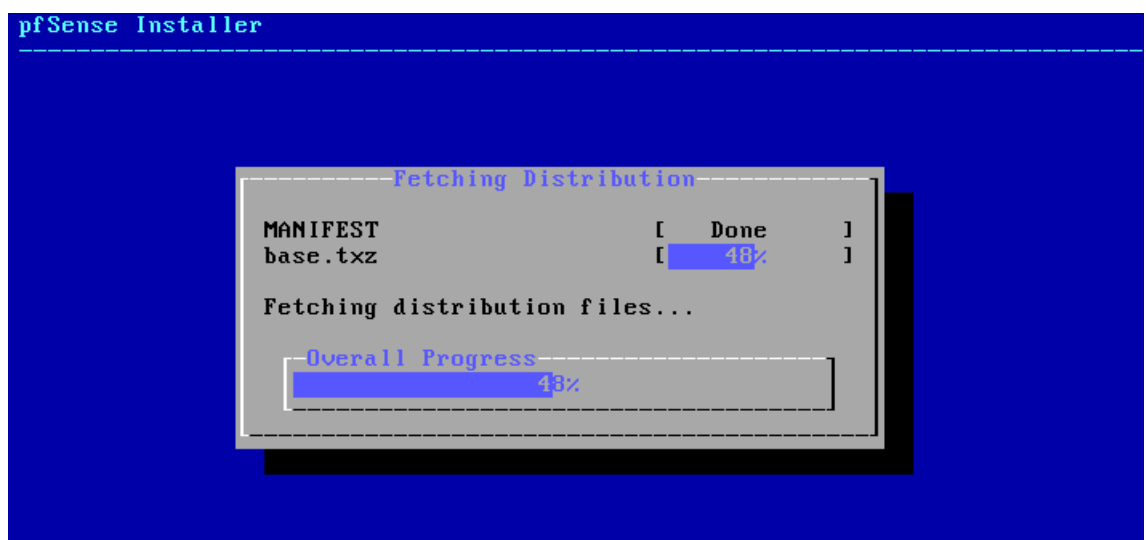
- 17) Nesta tela apenas pressione o botão espaço para marcar a única opção disponível, após marcar pressione a tecla *Enter*.



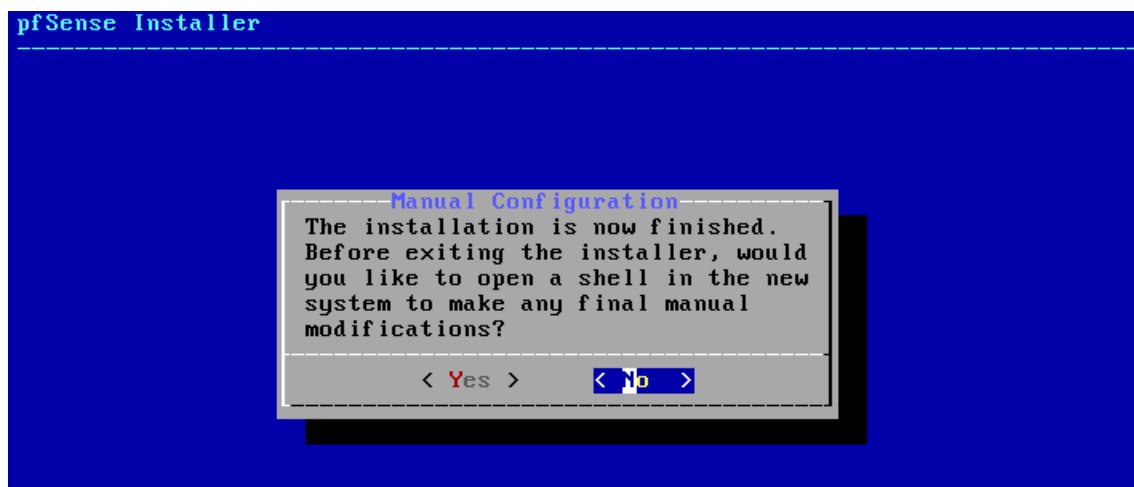
- 18) Nesta etapa você receberá um aviso que os dados do disco serão apagados, selecione a opção *yes* e pressione *Enter*.



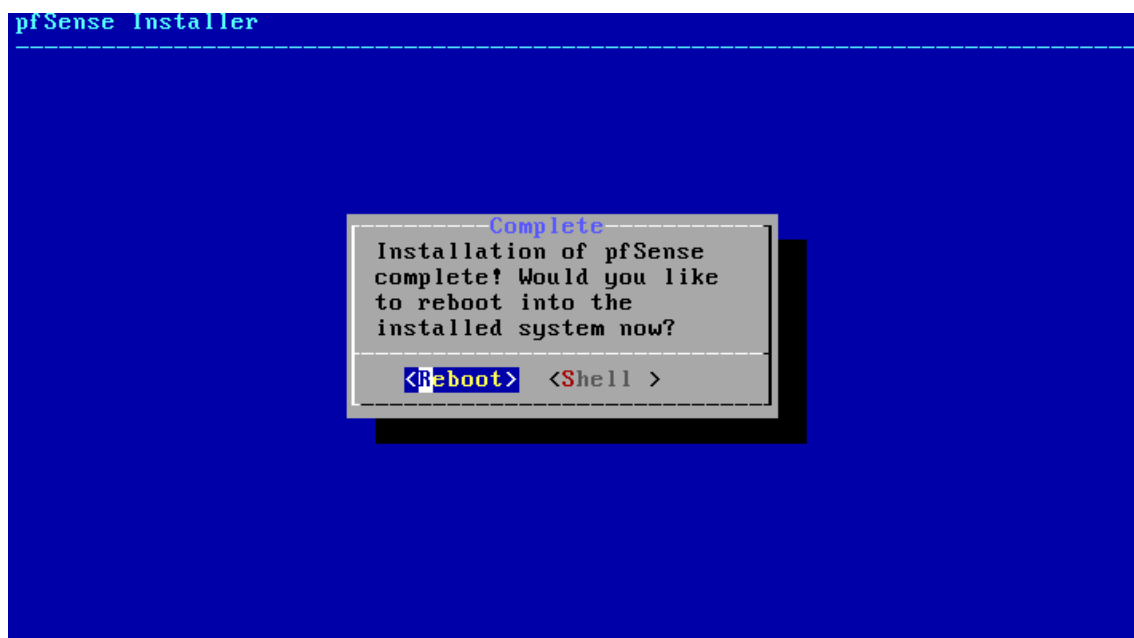
- 19) Aguarde alguns segundos até a conclusão da instalação.



20) Após a finalização da instalação, selecione a opção *no* e pressione *Enter*.

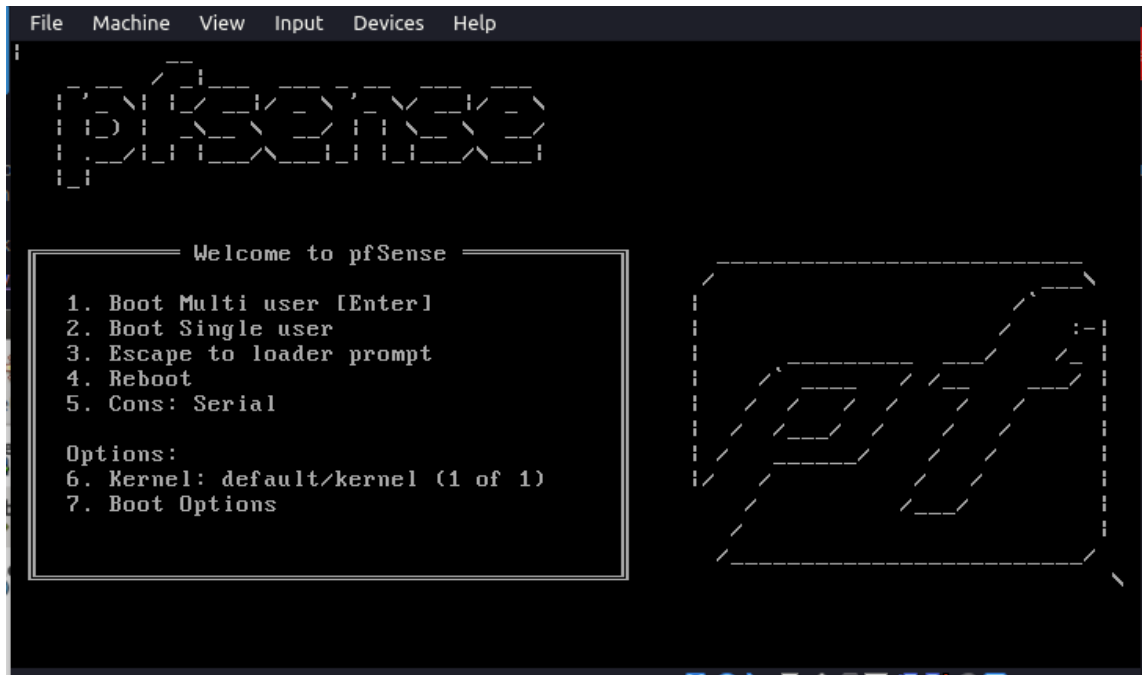


21) Agora selecione a opção *Reboot* e pressione *Enter*.

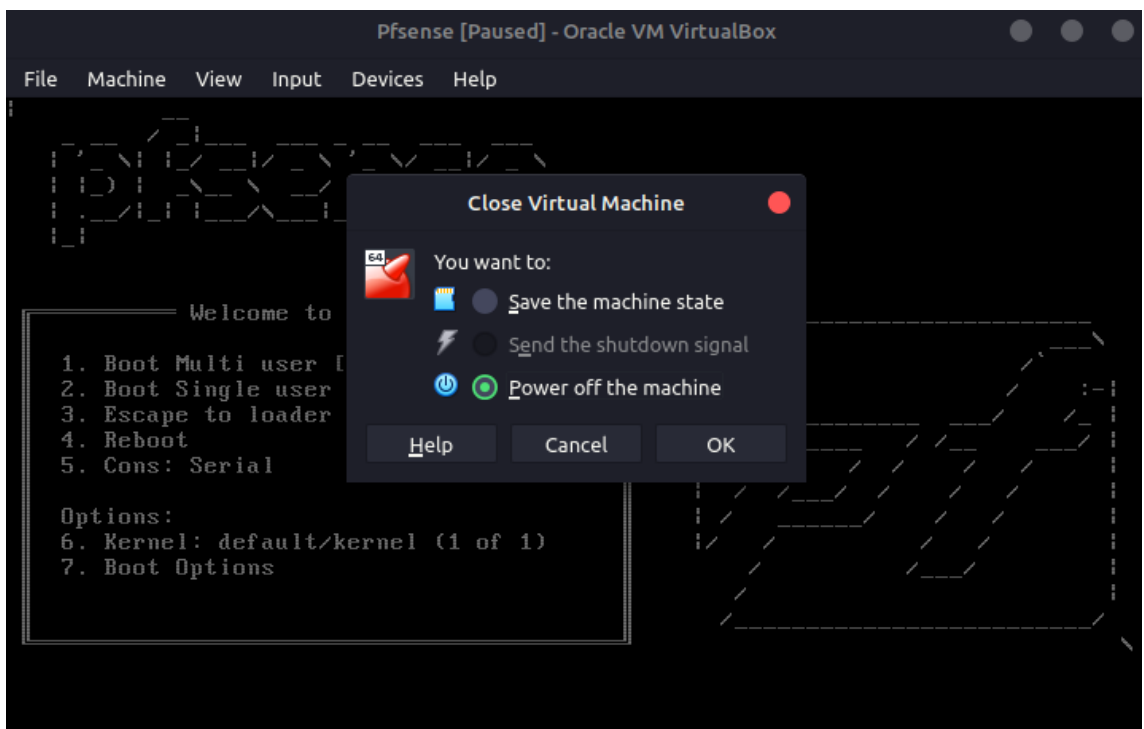




22) Aguarde a reinicialização e aparição da tela do pfSense.

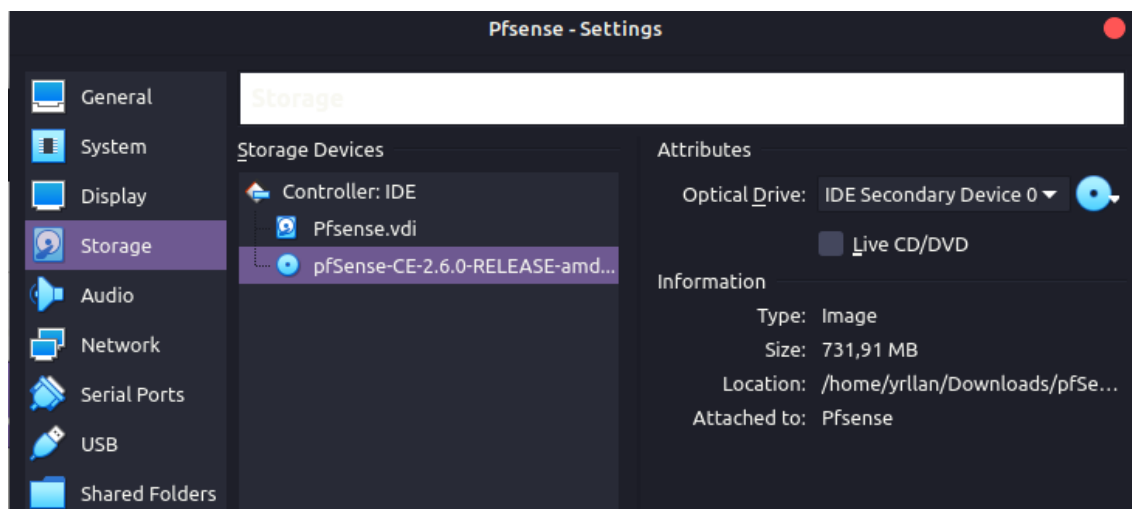


23) Clique no botão de fechar a máquina virtual e desligue a máquina.



24) Selecione a máquina virtual do pfSense e vá em *Settings > storage >* selecione a iso do pfSense e clique com o botão direito do mouse e clique em

Remove attachment > remove e ok.



25) Inicie o pfSense clicando em *Start* e aguarde toda a inicialização.

```
File Machine View Input Devices Help
5) Reboot system          14) Enable Secure Shell (sshd)
6) Halt system           15) Restore recent configuration
7) Ping host             16) Restart PHP-FPM
8) Shell

Enter an option: 1

Valid interfaces are:

em0      08:00:27:6c:09:09   (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      08:00:27:4e:bc:58   (up) Intel(R) Legacy PRO/1000 MT 82540EM

Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.

Should VLANs be set up now [y/n]?

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a):
```

26) Selecione as duas placas de rede em0 e em1.

```
Enter the WAN interface name or 'a' for auto-detection
(em0 em1 or a): em0

Enter the LAN interface name or 'a' for auto-detection
NOTE: this enables full Firewalling/NAT mode.
(em1 a or nothing if finished): em1

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1

Do you want to proceed [y/n]?
```

27) Digite a letra "y" e pressione *Enter*.

```
Do you want to proceed [y/n]? y
```

28) Agora o pfSense foi instalado e já está com o ip da LAN disponível, caso opte por escolher uma outra faixa de ip, basta digitar o número 2 ou escolher outras opções.

```
WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.15/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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) Enable Secure Shell (sshd)
6) Halt system               15) Restore recent configuration
7) Ping host                 16) Restart PHP-FPM
8) Shell
```

## APÊNDICE C - Guia de instalação IPS no *firewall* pfSense

Para instalação dos pacotes Snort e Suricata utilizaremos a interface gráfica do pfSense que pode ser acessada utilizando um navegador através do endereço inicial da rede, que neste caso é **192.168.1.1**, para acessarmos a página inicial do pfSense é necessário que o *host* esteja na mesma faixa de ip do pfSense, para máquina virtual basta utilizarmos a placa de rede do host em modo rede interna, assim como o segundo adaptador do pfSense.

- 1) acesse o navegador e digite o ip da página inicial do pfSense.



- 2) Você receberá uma mensagem de alerta, entretanto não se assuste, clique em avançar > aceitar o risco e continuar.



### Alerta: Potencial risco de segurança à frente

O Firefox detectou uma potencial ameaça de segurança e não seguiu para 192.168.1.1. Se você visitar este site, invasores podem tentar roubar suas informações, como senhas, endereços de email ou detalhes de cartões de crédito.

[Saiba mais...](#)

[Voltar \(recomendado\)](#)

[Avançado...](#)

O servidor 192.168.1.1 usa um certificado de segurança inválido.

O certificado não é confiável porque é autoassinado.

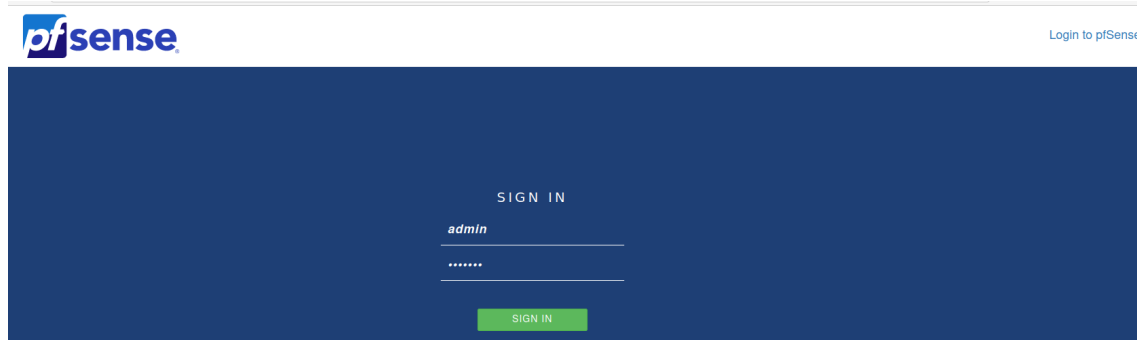
Código do erro: [MOZILLA\\_PKIX\\_ERROR\\_SELF\\_SIGNED\\_CERT](#)

[Ver certificado](#)

[Voltar \(recomendado\)](#)

[Aceitar o risco e continuar](#)

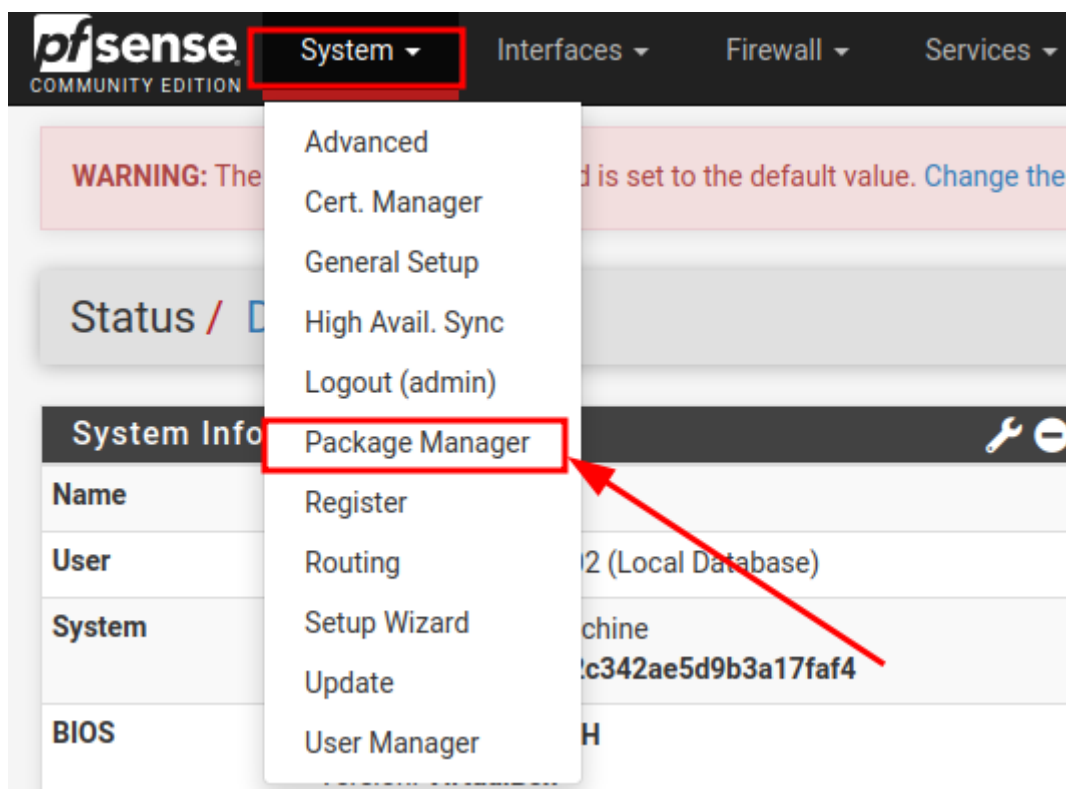
- 3) Agora você irá visualizar a página de login do pfSense, agora basta inserir o usuário **admin** e a senha **pfSense** e clicar no botão **sign in**.



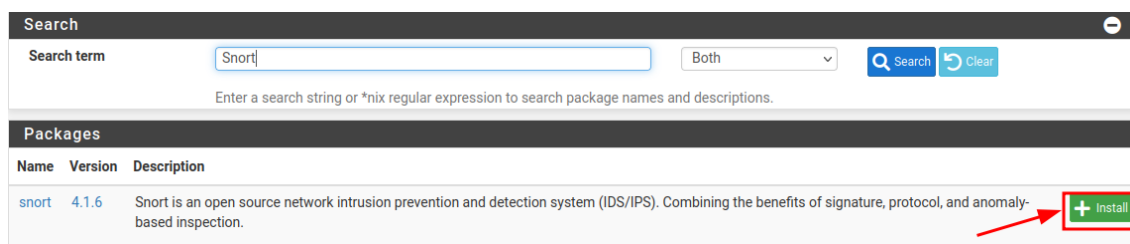
- 4) Clique na logo do pfSense para ir para a página inicial da interface gráfica, é aconselhável alterar a senha padrão, mas em nosso caso apenas iremos prosseguir com a instalação das ferramentas.



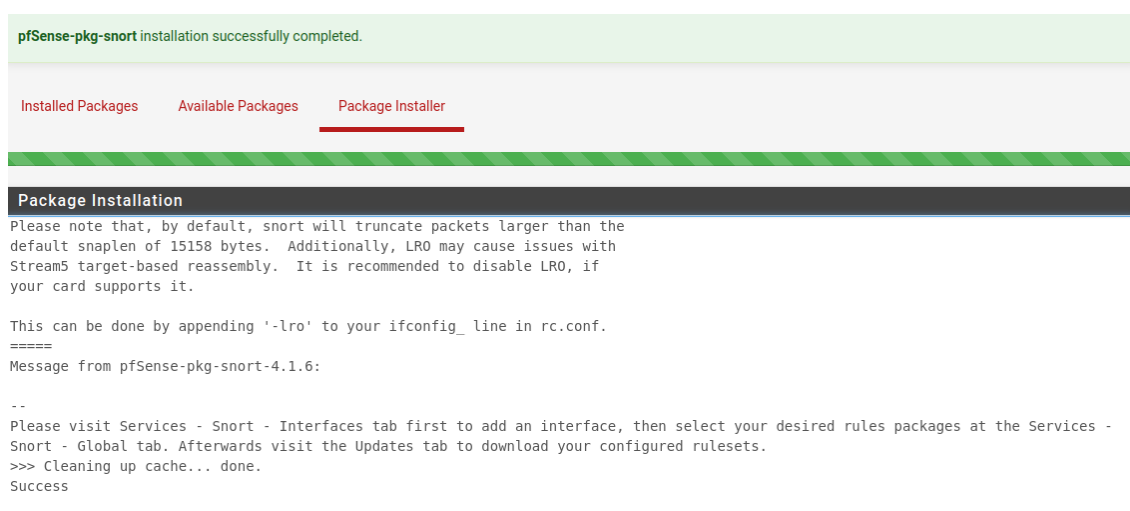
- 5) Na página inicial clique em *system* > *package manager*.



- 6) Agora clique em *Available Packages* e pesquise pelo nome do IPS, após aparecer os pacotes disponíveis basta clicar no botão *install*.



- 7) Agora clique em *confirm* para iniciar a instalação, após isso será iniciado o download e será realizada a instalação.



- 8) Para instalar o Suricata ou outras ferramentas, basta realizar o mesmo processo.