



**UNIVERSIDADE FEDERAL DO ACRE**  
**CENTRO DE CIÊNCIAS EXATAS E TECNOLÓGICAS**  
**CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO**

**UM ESTUDO DE RADIUS E CAPTIVE PORTAL COMO FERRAMENTAS  
PARA CONTROLE DE ACESSO À REDES SOB O FIREWALL  
PFSENSE**

**RIO BRANCO**  
**2019**

**PATRICK THANUS MOTA BATISTA**

**UM ESTUDO DE RADIUS E CAPTIVE PORTAL COMO FERRAMENTAS  
PARA CONTROLE DE ACESSO À REDES SOB O FIREWALL  
PFSENSE**

Monografia apresentada como exigência final para obtenção do grau de bacharel em Sistemas de Informação da Universidade Federal do Acre.

Prof. Orientador: Wilker Luiz Gadelha Maia

**RIO BRANCO**

**2019**

## **TERMO DE APROVAÇÃO**

**PATRICK THANUS MOTA BATISTA**

### **UM ESTUDO DE RADIUS E CAPTIVE PORTAL COMO FERRAMENTAS PARA CONTROLE DE ACESSO À REDES SOB O FIREWALL PFSENSE**

Esta monografia foi apresentada como trabalho de conclusão de Curso de Bacharelado em Sistemas de Informação da Universidade Federal do Acre, sendo aprovado pela banca constituída pelo professor orientador e membros abaixo mencionados.

Compuseram a banca:

---

Prof. Wilker Luiz Gadelha Maia, MsC.  
Curso de Bacharelado em Sistemas de Informação

---

Prof. André Luiz Nasserla Pires, Dr.  
Curso de Bacharelado em Sistemas de Informação

---

Prof. Jean Gonzaga Souza de Oliveira, MsC.  
Curso de Bacharelado em Sistemas de Informação

Rio Branco, 2019

*Dedico este trabalho a toda minha  
família e amigos.*

## **AGRADECIMENTOS**

Primeiro a Deus, pela vida.

Agradeço a minha família por terem me apoiado todos esses anos para que eu conseguisse alcançar esse objetivo, especialmente aos meus pais, avós, tios e irmãos.

Ao meu orientador, professor Wilker Maia pela ajuda na elaboração desse trabalho.

Aos meus grandes amigos que fiz no curso, Italo Rogério, Vitor Hugo, Matheus Vale e Salatiel Soares, agradeço vocês pela ajuda no curso, pelo convívio entre amigos e por histórias que sempre serão lembradas por nós.

E a todos que fizeram parte, mesmo que de alguma forma, da minha formação.



## RESUMO

Atualmente a segurança é imprescindível em qualquer organização, em especial as menores que precisam de uma forma barata para implementar mecanismos que tornem suas informações mais seguras. Este trabalho tem como finalidade operar pesquisas e testar ferramentas para a utilização de um *firewall* livre para controlar acessos dos usuários na rede de uma organização. Um *firewall* utiliza de regras para permitir ou bloquear acessos acarretando a prevenção de inúmeros ataques. Nesse contexto, foi modelado uma PSI, implementado um *firewall pfsense* que realiza a validação dos usuários através do protocolo RADIUS, assim como seus testes e resultados.

**Palavras-chave:** RADIUS. *Pfsense*. *Firewall*. Segurança. *Proxy*.

## **ABSTRACT**

Nowadays, the *Security* of information is extremely necessary in any organization, mainly the ones who deals with sensitive informations and needs a cheap methodology that brings more *Security* for your information. In this works were made researchs and applications that implements a free firewall to control the users access in an intern network from an organization. A firewall uses a set of rules to allow or block an access, resulting in a prevention of countless attacks. In this context, this works proposes a *Security* police for one organization, implementing a fsense firewall that performs users authentications through the RADIUS protocol.

**Key-words:** RADIUS. *Pfsense*. *Firewall*. *Security*. *Proxy*.



## Índice de figuras

Figura 1: Modelo PDCA.....	20
Figura 2: Exemplo rede PAN.....	25
Figura 3: Exemplo rede LAN.....	26
Figura 4: Exemplo rede MAN.....	27
Figura 5: Exemplo rede WAN.....	28
Figura 6: Tela <i>Kali Linux</i> .....	30
Figura 7: Tela <i>Fedora Security</i> .....	31
Figura 8: Tela <i>Parrot Security</i> .....	32
Figura 9: Tela sistema BackBox.....	33
Figura 10: VirtualBox e máquinas instaladas.....	40
Figura 11: Placa WAN .....	40
Figura 12: Placa LAN .....	41
Figura 13: Placa LAN do lubuntu.....	42
Figura 14: Tela inicial .....	43
Figura 15: Interface WEB.....	44
Figura 16: DHCP rede LAN.....	45
Figura 17: Teste DHCP rede LAN.....	46
Figura 18: Regras LAN.....	47
Figura 19: Aliase.....	48
Figura 20: Criação servidor .....	49
Figura 21: NAS.....	50
Figura 22: Interfaces RADIUS.....	51
Figura 23: Users RADIUS.....	52
Figura 24: Captive Portal autenticado.....	53
Figura 25: Página autenticação captive portal.....	54
Figura 26: Status captive portal.....	55
Figura 27: Aba General do Squid proxy.....	56
Figura 28: Autenticação Squid proxy.....	57
Figura 29: Configuração proxy no navegador.....	57
Figura 30: Configuações gerais SquidGuard.....	58
Figura 31: Common ACL.....	59
Figura 32: Groups ACL.....	60
Figura 33: Times SquidGuard.....	61
Figura 34: Teste bloqueio a sites.....	61
Figura 35: Teste acesso a sites.....	62

## SUMÁRIO

<b>1. INTRODUÇÃO.....</b>	<b>11</b>
1.1. JUSTIFICATIVA.....	12
1.2. OBJETIVOS.....	13
<b>1.2.1. Geral.....</b>	<b>13</b>
<b>1.2.2. Específicos.....</b>	<b>13</b>
1.3. METODOLOGIA.....	14
1.4. ORGANIZAÇÃO DA MONOGRAFIA.....	14
<b>2. FUNDAMENTAÇÃO TEÓRICA.....</b>	<b>16</b>
2.1. SEGURANÇA DA INFORMAÇÃO.....	16
<b>2.1.1 SGSI.....</b>	<b>18</b>
<b>2.1.2 Política de Segurança da Informação.....</b>	<b>19</b>
<b>2.1.3. Teste de Invasão.....</b>	<b>20</b>
2.2. REDES DE COMPUTADORES.....	22
<b>2.2.1. Redes pessoais ou PANs.....</b>	<b>22</b>
<b>0.0.1. 2.2.2. Redes locais ou LANs.....</b>	<b>23</b>
<b>2.2.3. Redes metropolitanas ou MANs.....</b>	<b>24</b>
<b>0.0.2. 2.2.4. Redes de longas distâncias ou WANs.....</b>	<b>25</b>
<b>2.2.5. Redes <i>wireless</i>.....</b>	<b>26</b>
2.3 LINUX.....	27
<b>2.3.1. Kali Linux.....</b>	<b>28</b>
<b>2.3.2. <i>NodeZero</i>.....</b>	<b>29</b>
<b>2.3.3. Fedora Security.....</b>	<b>29</b>
<b>2.3.4. <i>Parrot OS Security</i>.....</b>	<b>30</b>
<b>2.3.5. <i>BackBox</i>.....</b>	<b>30</b>
2.4 FIREWALL.....	31
<b>2.4.1. Filtragem de pacotes.....</b>	<b>33</b>

2.4.2. Filtro de Pacotes com Controle de Estado.....	33
2.4.3. <i>Proxy firewall</i> .....	34
2.4.4. <i>Pfsense</i> .....	34
2.5 RADIUS.....	35
<b>3. IMPLANTAÇÃO DO FIREWALL PFSENSE E RADIUS.....</b>	<b>37</b>
3.1 PREPARAÇÃO DO AMBIENTE.....	37
3.2 CONFIGURAÇÃO DO PFSENSE.....	40
3.2.1. <i>Pfsense WEB</i> .....	41
3.2.2. DHCP Server.....	42
3.2.3. Regras de Firewall.....	44
3.2.4. <i>FreeRADIUS</i> .....	46
3.2.5. Captive Portal.....	50
3.2.6. Servidor proxy.....	53
<b>4. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES.....</b>	<b>61</b>
4.1 CONSIDERAÇÕES FINAIS.....	61
4.2 RECOMENDAÇÕES.....	62
<b>REFERÊNCIAS.....</b>	<b>63</b>
<b>APÊNDICE A – POLÍTICAS DE SEGURANÇA.....</b>	<b>65</b>
1. INTRODUÇÃO.....	65
2. OBJETIVO.....	65
3. AUTENTICAÇÃO.....	65
3.1 Senhas.....	66
3.2 Acesso a internet.....	66
4. MAQUINAS DE TRABALHO.....	67
5. BOAS PRÁTICAS DE SEGURANÇA.....	67
6. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA.....	68
7. SUPORTE.....	68

## 1. INTRODUÇÃO

Uma rede é formada por um composto de computadores interligados com objetivo de trocar informações. Partindo do princípio simples, a rede é formada por quatro elementos: protocolo, placas de rede, cabo e *hub* ou *switches*. Já as redes *wireless* não precisam de um cabeamento, pois o sinal é enviado por pontos de acesso.

Internet utiliza um grande sistema de comunicação que conecta várias redes, é possível compartilhar informações com outros computadores em qualquer lugar do mundo, a internet é tão popular e essencial no mundo todo. É importante falar que enquanto um computador está preso somente a informações de seu disco rígido, com a internet é possível ter o mundo aos seus pés, fazendo isso ser uma faca de dois gumes pois os usuários têm acesso há um grande número de dados derramado pela rede.

A informação é uma peça chave em qualquer organização que queira gerar conhecimento, sendo assim peça chave para seu negócio. Nas universidades não é diferente, a informação tem um valor muito alto, e isso deve ser protegido da melhor forma. Segurança da informação está interligada com redes, onde o sistema de segurança da informação apresenta 3 princípios básicos: confidencialidade, integridade e disponibilidade, a quebra de um desses princípios acarreta a quebra

da segurança da informação, podendo assim ser chamando também de incidente de segurança da informação.

Assim, é importante que as organizações protejam da melhor forma seus dados evitando assim problemas futuros.

Segurança da informação tentar criar meios para evitar agentes externos quebrem os três princípios básicos. Uma boa forma de se proteger em uma rede é conhecendo suas fraquezas e vulnerabilidades para que possa ser melhorada e evitar um ataque que algum hacker mal-intencionado pode fazer para prejudicar uma organização.

Nesse contexto, é objetivo desse trabalho é construir conceitos e fundamentos sobre planejamento e organização de um SGSI (Sistema de Gestão de Segurança da Informação), modelar uma Política de Segurança e demonstrar ferramentas utilizadas para realizar uma simulação de ambiente onde possa ser realizado a configuração do *firewall pfsense* acompanhado do protocolo RADIUS para controlar melhor os acessos da rede.

### 1.1. JUSTIFICATIVA

Está cada vez mais fácil compartilhar informação, gerando assim conhecimento através de redes interligadas de computadores. Essas informações podem ser utilizadas de várias formas para ajudar ainda mais no potencial organizacional.

A tecnologia trouxe uma gama de infinidades para empresas e organizações fazendo assim as mesmas investirem mais em tecnologia, atualmente isso é um fator que pode levar uma empresa as alturas. Uma empresa/organização com um bom sistema de informação é essencial para sua estabilização do mercado ou no cenário que ela está inserida.

É importante manter uma informação segura, e para isso são usados mecanismos de segurança da informação, como encriptação de dados para dificultar a leitura caso a informação seja interceptada por pessoas sem autorização.

Uma PSI tenta prevenir que uma rede possa ser invadida, uma organização precisa de alternativas para evitar pessoas indevidas acessando seus dados. Com o *pfsense* instalado e configurado acompanhado do protocolo RADIUS é possível criar usuários específicos e dar suas devidas permissões tanto na rede local como na internet.

## 1.2. OBJETIVOS

Abaixo segue o objetivo geral e os objetivos específicos.

### 1.2.1. Geral

Compor um estudo apresentando distros *Linux* voltada para segurança da informação. Simular uma rede, modelar e aplicar uma Política de Controle de Acesso utilizando o *pfsense* como servidor *firewall* e o protocolo RADIUS para autenticação de usuários.

### 1.2.2. Específicos

Esse trabalho possui os seguintes objetivos específicos:

- a) Apresentar SOs *Linux*, suas distribuições especializadas em segurança da informação;
- b) Desenvolver conceitos e fundamentos sobre planejamento e organização de um SGSI;
- c) Modelar uma Política de Segurança;
- d) Simular uma rede;
- e) Configuração de servidores Proxy, DHCP e RADIUS;
- f) Integrar o Portal Capitivo com o RADIUS;
- g) Bloquear acessos a sites utilizando *proxy* autenticado.

### 1.3. METODOLOGIA

Para a realização desse trabalho será realizado os seguintes passos:

- a) Pesquisa bibliográfica;
- b) Modelagem de uma Política de Segurança;
- c) Criação de um ambiente para simulação;
- d) Execução de algumas ferramentas presentes no *pfsense* e no protocolo RADIUS;
- e) Apontar os resultados.

### 1.4. ORGANIZAÇÃO DA MONOGRAFIA

O capítulo 1 trata a Introdução, onde é apresentado o tema da monografia acompanhado do problema da pesquisa, justificativa e seus objetivos, no total são 4 capítulos.

No capítulo 2 são apresentados os conceitos que fundamentam a monografia, descrevendo Segurança da Informação, Redes, *Linux*, *Firewall* e RADIUS.

O capítulo 3 mostra a preparação do ambiente simulado, configuração do *pfsense* e suas ferramentas, assim como seus testes e resultados.

O capítulo 4 apresenta as considerações finais e sugestões para trabalhos futuros.



## 2. FUNDAMENTAÇÃO TEÓRICA

Na realização desta monografia foram utilizados conceitos relacionados à segurança da informação, redes, *Linux*, *firewall* e RADIUS. Estes conceitos permitem compreender a utilização do RADIUS e do CP, bem como servir de base para o entendimento da monografia.

As seções a seguir apresentam conceitos sobre:

- 2.1) Segurança da Informação;
- 2.2) Redes;
- 2.3) *Linux*;
- 2.4) *Firewall*;
- 2.5) RADIUS.

### 2.1. SEGURANÇA DA INFORMAÇÃO

A informação tem um significado muito grande para as organizações pois se for utilizada da maneira certa pode gerar valor para seus negócios. A informação é um elemento-chave para a geração do conhecimento, podendo influenciar diretamente na tomada de decisão em uma organização.

Uma vez que a informação representa valor, e conseqüentemente, contribui diretamente para a geração do lucro, é possível afirmar então que a informação é um bem, um ativo da organização, e como tal deve ser preservado e protegido tal qual os demais ativos da organização...  
(CAMPOS, 2007, pg.16)

Tendo em vista a importância da informação, surge a segurança da informação, que é um meio de manter a informação livre de ameaças relacionadas a três princípios: 1) confidencialidade, 2) integridade e 3) disponibilidade. Se um desses princípios for violado a informação foi quebrada.

O princípio da confidencialidade é garantido quando apenas as pessoas explicitamente autorizadas podem ter acesso à informação.  
O princípio da integridade é garantido quando a informação acessada está completa, sem alterações e, portanto, confiável.  
O princípio da disponibilidade é garantido quando a informação está acessível, por pessoas autorizadas, sempre que necessário.  
(CAMPOS, 2007, p.17-19)

Poderá ocorrer a quebra de um ou mais desses princípios da segurança da informação. Uma informação pode deixar de ser confidencial, íntegra e podendo não estar acessível no momento solicitado e isso acarretará problemas para a empresa, podendo até ser financeiros, pois como dito a informação também é considerado um ativo da empresa.

A proteção da rede com cabo é feita por meios físicos, pois há necessidade de estar conectado com o cabo para usufruir da rede, assim com a restrição de pessoas não autorizadas à aquele ambiente é um modo de proteção. Mas para as redes *wireless* é diferente, pois é utilizado ondas de rádio para fazer a transmissão dos dados, assim uma pessoa de fora pode interceptar o sinal, sendo então necessários alguns protocolos para tentar tornar os tráfegos mais seguros, por exemplo: WEP que é um dos primeiros padrões de encriptação a ser usados nas redes *wireless*, que apesar de ser muito usado hoje em dia possui muitas falhas e vulnerabilidades; o WPA foi criado para substituir o WEP e corrigir suas falhas, permitindo assim uma melhor segurança para as redes *wireless*; e o WPA2 que foi

lançado mais recentemente e usar protocolo de criptografia diferente e é o mais seguros entre os três citados.

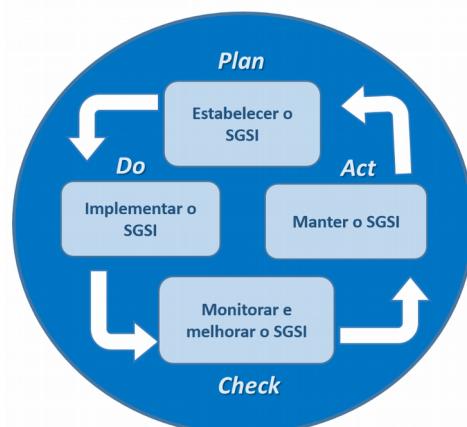
### 2.1.1 SGSI

“Um SGSI é um sistema de gestão voltado para a Segurança da Informação, que inclui toda a abordagem organizacional usada para proteger a informação empresarial e seus critérios de confidencialidade, integridade e disponibilidade.” (PALMAS, 2017).

“Estabelecer um Sistema de Gestão da Segurança da Informação é dar vida própria para a segurança da informação dentro da organização.” (CAMPOS, 2007, pg.31).

“O SGSI representa um conjunto de políticas, procedimentos e vários outros controles que definem as regras de segurança da informação em uma organização.” (KOSUTIC, 2016). A norma ISO 27001 adota o modelo PDCA (*Plan-Do-Check-Act*) para descrever a estrutura de um SGSI, segue a figura 1:

Figura 1: Modelo PDCA



Fonte: (PALMAS, 2017).

Estabelecer o SGSI: É a etapa que dá vida ao SGSI. Suas atividades devem estabelecer políticas, objetivos, processos e procedimentos para a gestão de segurança da informação. São os instrumentos estratégicos fundamentais para que a organização possa integrar suas a segurança da informação às políticas e objetivos globais da organização.

Implementar o SGSI: Consiste em implementar e operar a política de segurança, os controles / medidas de segurança, processos e procedimentos.

Monitorar e analisar criticamente o SGSI: Reúne as práticas necessárias para avaliar a eficiência e eficácia do sistema de gestão e apresentar os resultados para a análise crítica pela direção. A política de segurança é usada para comparar e desempenho alcançado com as diretrizes definidas.

Manter e melhorar continuamente o SGSI: Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente, para alcançar a melhoria contínua do SGSI.  
(KOSUTIC, 2016)

Implantar um sistema de gestão da segurança da informação não é uma tarefa fácil, é relevante que a implementação seja gerida e acompanhada por especialistas. A realização do implemento de um SGSI varia de uma organização para a outra, é necessário seguir os passos do mesmo, fazendo avaliação de riscos e analisando seus resultados com os requisitos das partes interessadas.

### **2.1.2 Política de Segurança da Informação**

Atualmente com todo esse avanço tecnológico a internet ficou essencial em toda ou qualquer organização que queira ser competitiva no mercado. Com isso, é necessário que utilizem de um sistema de rede de computadores totalmente eficaz e seguro. A informação é um bem muito precioso dentro de uma organização, é de importância que apenas pessoas autorizadas possam acessar esses dados. Uma Política de Segurança da Informação se baseia fortemente nos princípios da segurança da informação: confiabilidade, integridade e disponibilidade, sendo que a quebra de um desses princípios é considerado como uma ameaça.

A PSI é o conjunto de ações, técnicas e boas práticas relacionadas ao uso seguro de dados. Ou seja, trata-se de um documento ou manual que

determina as ações mais importantes para garantir a segurança da informação.  
(MOREIRA, 2017)

Uma PSI não é obrigatória dentro da organização, porém ela é aplicada na maioria das organizações atualmente, sendo essencial para que a mesma obtenha uma vantagem competitiva, reduzindo seus riscos e assim alcançando sucesso. É importante que os funcionários sejam orientados para maior eficiência da PSI.

Para elaborar uma PSI são levadas em considerações algumas normas relacionadas com práticas segurança da informação, a norma ISO/IEC 27001:2005 fala em práticas para que seja mantido a segurança em organizações.

Para conseguir alcançar a meta de uma boa PSI, deve ser elaborado regras que norteiem os funcionários, clientes e fornecedores com relação aos padrões pertencentes à segurança da informação, restrição de acesso somente a pessoas autorizadas, monitoramento e controle, entre outros, sendo que o objetivo principal é preservar os dados ou informações.

Com esses conhecimentos adquiridos sobre segurança da informação, foi elaborado uma PSI para uma organização podendo ser adaptada para cada caso específico, pode ser visualizada no Apêndice A.

### **2.1.3. Teste de Invasão**

Um problema atualmente relacionado a tecnologia é a invasão que pode ocorrer em determinadas organizações sejam por pessoas internas (ligadas a organização) ou pessoas externas. Um teste de penetração é uma simulação de um ataque malicioso em um sistema de computador, rede ou organização a partir de uma perspectiva interna ou externa. O objetivo não é causar danos à organização,

mas sim identificar vulnerabilidades encontradas para mostrar o risco que existe e diminui-lo.

Hoje em dia as empresas contratam o serviço Pentest como forma de se precaver dos hackers maliciosos que existem no mundo. Hacker pode ser definido com indivíduos que dedicam diariamente para conhecer e modificar programas relacionados a redes. Deixa claro que um hacker é uma pessoa habilidosa, mas que não coopera muito com a ética relacionada com convívio em sociedade.

Testes de invasão são realizados utilizando alguns modelos padrões, como:

a) Modelo Caixa Preta: Todo o teste é realizado sem necessidade de haver prévio conhecimento do ambiente ou de credenciais de acesso;

b) Modelo Caixa Branca: Neste modelo, todas as informações sobre a topologia de rede, credenciais dos sistemas e aplicações são repassadas ao analista de teste para que este possa avaliar as vulnerabilidades;

c) Modelo Caixa Cinza: Neste modelo, serve basicamente para descobrir se existem inconsistências nas permissões de acesso de usuário, como se a empresa contratada fosse um funcionário ou prestador de serviço relacionado à empresa.

Um teste de penetração pode ajudar muito para identificar vulnerabilidades em uma rede, com o teste caixa branca percebe-se que esse é um teste que simula um ataque por pessoas que tem todo acesso a rede, deixando claro que os perigos não estão apenas fora.

## 2.2. REDES DE COMPUTADORES

Uma rede tem como motivação principal trocar informações sem a obrigação do receptor estar próximo do emissor, podendo acontecer de várias maneiras, através de áudio, vídeo, texto, etc. Exemplo de rede simples é a troca de informações entre dois computadores conectados por um cabo. A rede mais utilizada e que interliga o mundo todo é a Internet, podendo com ela trocar informações com qualquer pessoa em qualquer lugar, basta que as duas estejam conectadas a rede.

A Internet é uma rede de computadores que interconecta milhares de dispositivos do mundo. Há pouco tempo esses dispositivos eram basicamente computadores de mesa, estações de trabalho *Linux*, e os assim chamados servidores que armazenam e transmitem informações, como páginas da Web e mensagens de e-mail.  
(KUROSE e ROSS, 2010, p.2)

Hoje em dia há uma grande diversidade de dispositivos que podem se introduzir nas redes, até aqueles inusitados como um forno micro-ondas, esse exemplo facilita uma pessoa a esquentar sua comida sem necessidade de estar perto da mesma, basta que a comida esteja no forno e que haja uma comunicação entre a pessoa e o forno micro-ondas, sendo válido para inúmeros outros dispositivos como TVs, videogames, lâmpadas, etc.

Rede de computadores pode ser classificada com base na sua cobertura ou localização geográfica, com isso temos:

### 2.2.1. Redes pessoais ou PANs

As redes PANs ou redes pessoais são redes de curta distância com o intuito de interligar aparelhos pessoais com o alcance de até 10 metros. Pode-se notar o exemplo da rede PAN na Figura 2.

Redes PAN, também chamadas de WPAN (wireless PAN), são redes de curtíssima distância que utilizam comunicação sem fio (canais de rádio frequência) com o objetivo de interconectar dispositivos de rede, multimídia e processamento de dados, em distâncias de poucos metros, normalmente em uma mesma sala.

(CARISSIMI, ROCHOL e GRANVILLE, 2009, p.49-50)

Figura 2: Exemplo rede PAN



Fonte: (PINTO, 2010).

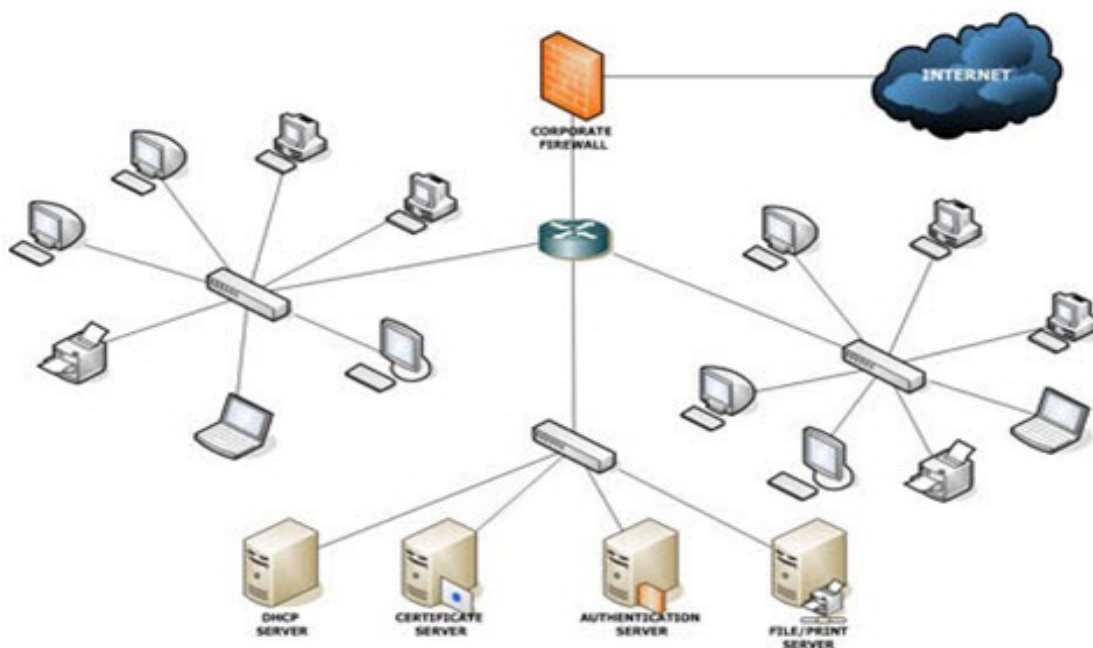
#### 0.0.1. 2.2.2. Redes locais ou LANs

É uma rede composta por diversos computadores que pertencem a mesma organização, numa área curta. “As redes locais ou LANs surgiram na década de oitenta, segundo três padrões do IEEE: IEEE 802.3, IEEE 802.4, IEEE 802.5.”



(CARISSIMI, ROCHOL e GRANVILLE, 2009, p.49-50). Pode-se notar uma rede LAN na Figura 3.

Figura 3: Exemplo rede LAN



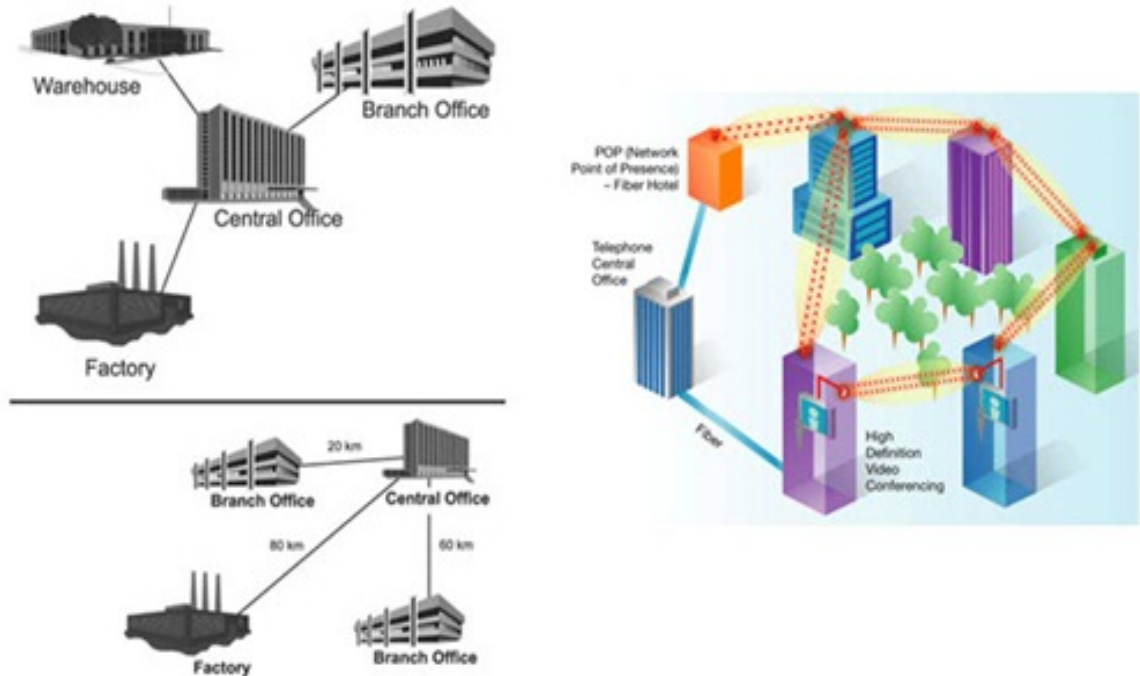
Fonte: (PINTO, 2010).

### 2.2.3. Redes metropolitanas ou MANs

São redes com alcance maior em comparação com redes locais (LAN), podendo alcançar cidades e até regiões. Pode-se notar o exemplo da MAN na Figura 4.

“As redes locais LAN e as redes metropolitanas MAN fazem parte do que se convencionou chamar de tecnologias de acesso à Internet, ou ISP.” (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.52)

Figura 4: Exemplo rede MAN



Fonte: (PINTO, 2010).

#### 0.0.2. 2.2.4. Redes de longas distâncias ou WANs

É uma rede que alcança uma distância considerável, podendo alcançar um país ou continente. Pode-se notar o exemplo da WAN na Figura 5.

“As redes WAN são suportes de telecomunicações que cobrem distâncias que vão de dezenas de milhares de quilômetros e os meios utilizados são preferencialmente as fibras ópticas.” (CARISSIMI, ROCHOL e GRANVILLE, 2009, p.52)

Figura 5: Exemplo rede WAN



Fonte: (PINTO, 2010).

#### 2.2.5. Redes *wireless*

As redes *wireless* nasceram como forma de complementar a rede cabeada. Dessa forma, uma rede *wireless* fornece a propagação de dados sem utilizar cabos, acarretando uma rápida e grande aceitação no mercado mundial.

O padrão 802.11 estabelece normas para a criação e para o uso de redes sem fio. A transmissão deste tipo de rede é feita por sinais de radiofrequência, que se propagam pelo ar e podem cobrir áreas na casa das centenas de metros. (ALECRIM, 2008)

Com a Internet no mundo todo, passou a surgir rapidamente novas tecnologias que visavam a mobilidade como um foco principal. Redes *wireless* passaram a ser utilizadas nas diversas áreas, como telecomunicações, na transferência de dados, podendo se conectar com periféricos tornando uma opção para conexões entre dispositivos.

Wi-Fi é uma rede sem cabo que permite se conectar a internet e transmitir dados pelas ondas de rádio, sendo muito popular no mundo.

Além de permitir uma implementação barata de redes locais (LANs), o Wi-Fi permite criar redes onde o cabeamento não pode ser executado. Isso é uma vantagem que faz com que a rede se popularize a cada dia, sendo uma das mais utilizadas em todo o mundo.

## 2.3 LINUX

Os sistemas operacionais que utilizam o núcleo *Linux*, tem seu código fonte aberto para qualquer pessoa que queira modificar, por isso há várias versões diferentes. Originalmente inspirado no sistema Minix, o *Linux* foi desenvolvido pelo programador finlandês Linus Torvalds. Existem várias distribuições do *Linux*, nada mais é do que um núcleo com vários programas específicos de cada versão para dar um diferencial, o *Kali Linux* tem muitas ferramentas para teste de invasão pois é um sistema voltado para segurança. Já o Ubuntu é uma das distribuições *Linux* mais populares atualmente pois há um grande foco no usuário final e em usuários menos habituados com o mundo do *Linux*.

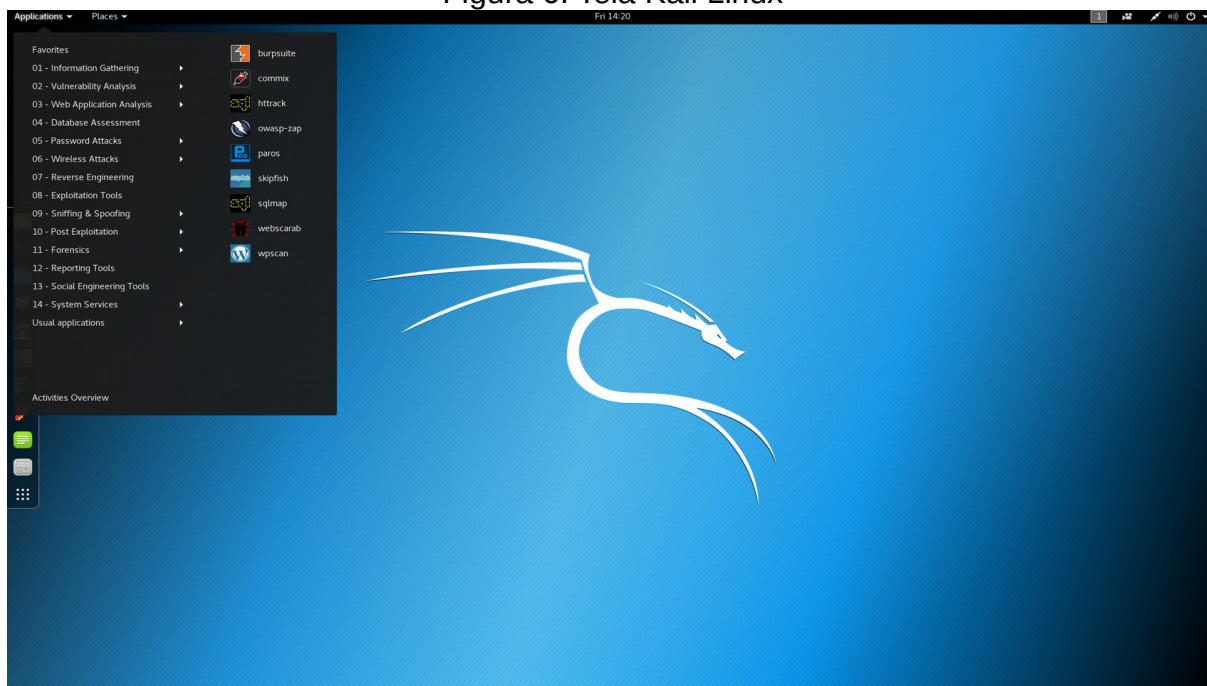
Algumas distribuições *Linux* são voltadas para a área de segurança, entre elas estão: *NodeZero Linux*, *Fedora Security*, *Parrot Security*, *BlackArch Linux*, *Pentoo*, *BackBox Linux*, *Kali Linux*, etc.

### 2.3.1. Kali Linux

“O *Kali Linux* é um SO *Linux* baseado no *Debian*, que é desenvolvido pela *Offensive Security*.” (FRAGA, 2016). Desenvolvido com o foco em fornecer várias ferramentas de *PenTest* nativas no sistema, o *Kali Linux* é um projeto open source e não é indicado para uso doméstico, é utilizado por hackers, *pentesters*, analistas e auditores de segurança da informação.

A principal vantagem do *Kali Linux* é que há uma infinidade de ferramentas exclusivamente para fazer teste de invasão. Pode ser rodado no computador como sistema principal, não é muito indicado caso o usuário não vá utilizar ferramentas para teste de invasão diariamente, pode ser instalado em um pendrive e sempre que quiser iniciar o sistema através dele, ou em uma VM. Pode-se observar a tela do *Kali Linux* na Figura 6.

Figura 6: Tela Kali Linux



Fonte: (MOZ, 2017).

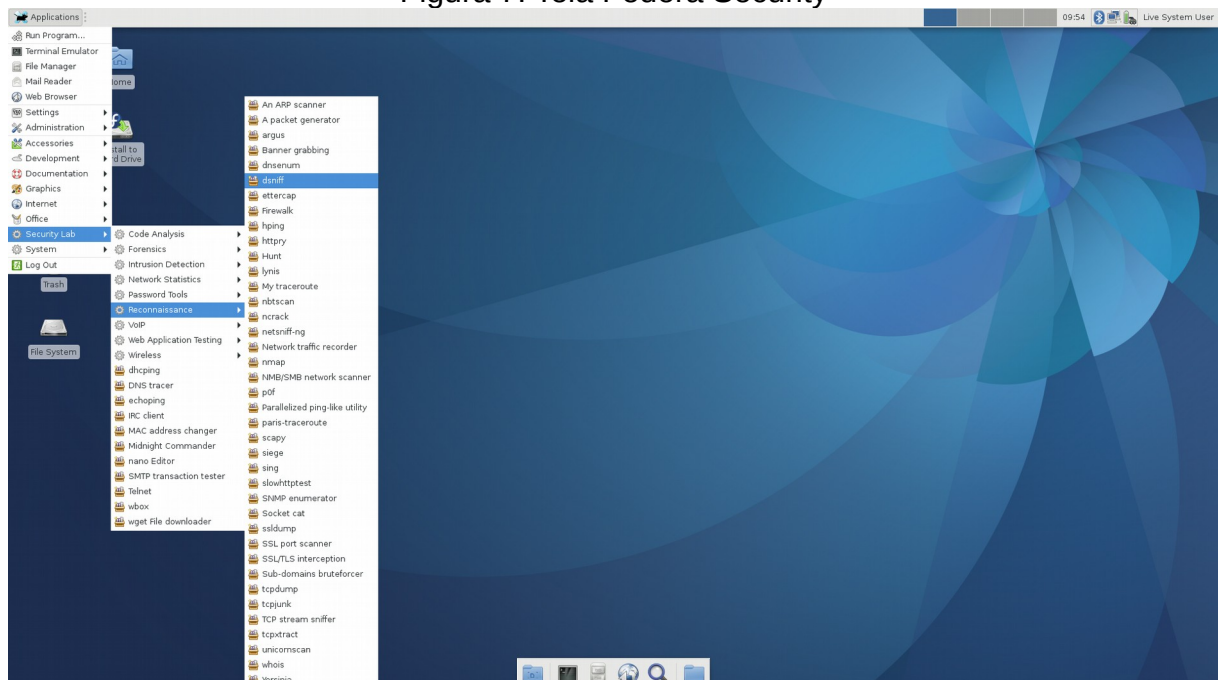
### 2.3.2. NodeZero

*NodeZero* é um SO alicerçado no Ubuntu e possui mais de 300 de tipos de ferramentas voltadas para o teste de invasão/intrusão. Um ponto negativo do *NodeZero* é que ele foi feito para ser gravado no HD do computador, diferentemente de outros como o *Kali Linux* que pode rodar com um *pen-drive*.

### 2.3.3. Fedora Security

*Fedora Security* como os outros também é voltado para segurança da informação e destinado para execução de testes de invasão/intrusão e análise forense. Vem com o *Fedora Security* várias ferramentas para serem exploradas a fim de melhorar uma rede tanto privada como principalmente nas organizações. Pode-se observar a tela do *Fedora Security* na Figura 7.

Figura 7: Tela Fedora Security



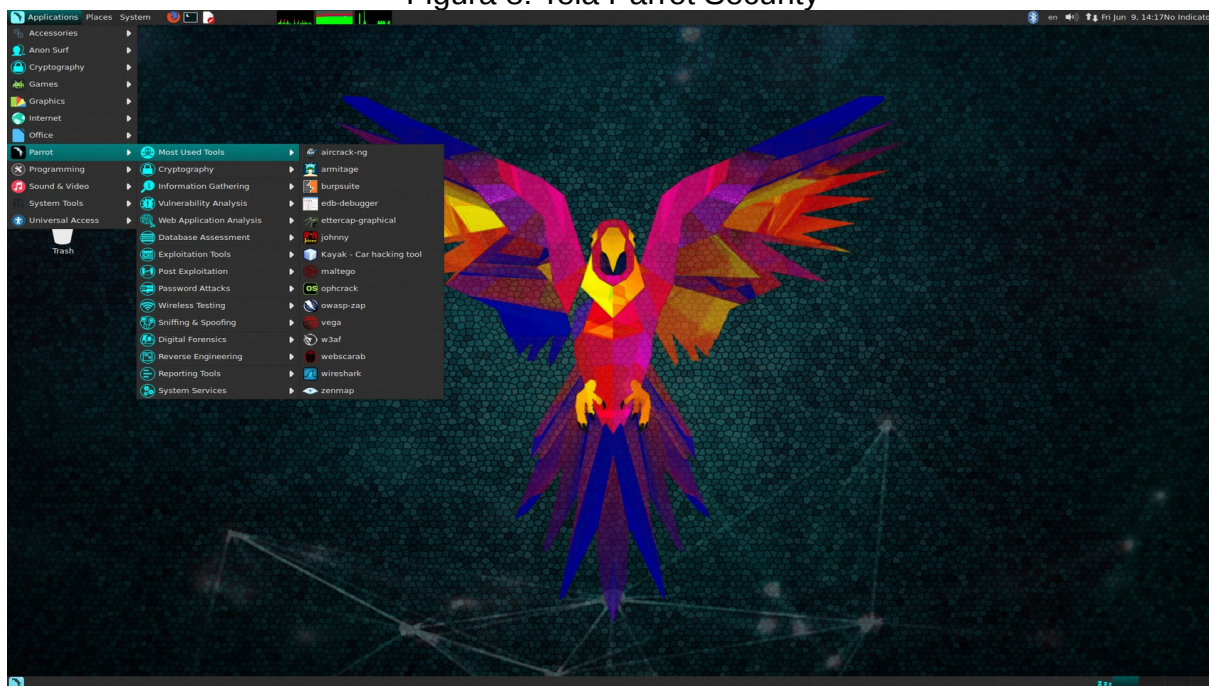
Fonte: (MOZ, 2017).



### 2.3.4. Parrot OS Security

*Parrot OS Security* foi lançado em 2013 como um sistema voltado para segurança da informação, uso geral e segurança em redes. É derivado do *Debian*, disponível para arquiteturas 32bits e 64 bits, por ser leve esse sistema é recomendado também para computadores pessoais. Esse sistema é bem didático, sua interface é similar ao *Kali Linux*. Igualmente os demais, esse sistema tem aproximadamente 500 ferramentas que facilita a vida das pessoas que trabalham com teste de invasão. Pode-se observar a tela do *Parrot OS Security* na Figura 8.

Figura 8: Tela Parrot Security



Fonte: (MOZ,2017).

### 2.3.5. BackBox

É um SO voltado para segurança baseado no Ubuntu, é ideal para realizar testes de penetração. Esse sistema vem com muitas ferramentas que deve

ser usadas para diversos fins, como análise de redes, análise de segurança, entre outros. O sistema *BackBox* é sempre atualizado e tem suas ferramentas principais sempre estáveis para que os usuários que trabalhem na área de *pentester* possam aproveitar o máximo do que o sistema tem para oferecer. Com o *BackBox* é possível fazer testes de vulnerabilidades a fim de encontrar riscos em redes de organizações ou redes privadas para que as mesmas sejam corrigidas. Pode-se observar a tela do *BackBox* na Figura 9.

Figura 9: Tela sistema BackBox



Fonte: (MOZ,2017).

## 2.4 FIREWALL

Computadores interligados com a internet abre uma gama de possibilidades positivas para o usuário, como se conectar com outras pessoas distantes fisicamente, estudar a distância, compartilhar informações, etc. Porém, a



internet também acarreta perigos aos usuários pois há pessoas prontas para fazer o mal, como roubar informações pessoais.

*Firewall* basicamente é uma parede de fogo que bloqueia acesso de conteúdo malicioso. Os *firewalls* são ferramentas que ficam no meio da internet e do computador tentando bloquear acessos indevidos a partir de regras e instruções para determinar quais operações de transmissão e recepção podem ser executadas. O *firewall* pode impedir várias ações maliciosas, como a tentativa de intrusão de um computador não autorizado e externo a rede, malware, etc.

*Firewall* é configurado inspirado em uma PCA, regras configuráveis pelo usuário. Nesse contexto, com base em (ALECRIM, 2013) um *firewall* básico deve configurado levando em consideração dois princípios: todo tráfego é bloqueado, exceto o que está explicitamente autorizado; todo tráfego é permitido, exceto o que está explicitamente bloqueado. *Firewalls* mais avançados conseguem dar uma gama maior em procedimentos para autenticação a usuários e tráfego de rede mais específico.

Cada situação se pode definir como vai ser implementado um *firewall*, partindo do mais simples há necessidade de proteger um computador pessoal, e logo os principais sistemas operacionais já tem segurança de *firewall*, assim como os antivírus.

Os três tipos de *firewalls*: Packet Filtering; Filtro de Pacotes com Controle de Estado; *Proxy firewall*.

### 2.4.1. Filtragem de pacotes

É o *firewall* mais simples, cada pacote possui várias informações sobre ele, como o IP do pacote, endereço de origem, endereço de destino, etc. Com as regras estabelecidas, o *firewall* analisará os pacotes para permitir o acesso ou negar os pacotes.

A filtragem dos pacotes pode ocorrer de maneira estática ou de maneira dinâmica, a regra estática não muda, é sempre fixa, já a maneira dinâmica vai ser mais flexível e pode mudar levando em conta o horário, dia e semana.

De um modo geral, a filtragem de pacote vai aceitar tudo que não está negado e vai negar tudo que não está autorizado pelas regras de *firewall*.

### 2.4.2. Filtro de Pacotes com Controle de Estado

Esse filtro analisa todo o tráfego da rede para encontrar padrões que serão aceitos por suas regras, não é considerado só as regras configuradas, é analisado a origem e a interação entre eles. Pode ser dizer que o filtro de pacotes com controle de estado é uma evolução da filtragem dinâmica de pacotes.

Esse *firewall* por ser mais detalhado costuma ser mais lento que o *firewall* filtragem de pacotes, sendo assim ele também exige mais recurso para o seu funcionamento e sua implementação geralmente é mais cara.

### 2.4.3. Proxy firewall

O *proxy firewall* vai agir na camada de aplicação sendo mais um meio de proteger a rede. O *proxy* vai ser um intermediário no meio do cliente local e o servidor, onde o cliente é responsável em fazer os pedidos e o servidor o responsável pelas respostas.

Nesse *firewall* todo fluxo de dados passará pelo servidor *proxy*, com isso é possível limitar a comunicação a determinados endereços utilizando regras. Por ter um IP próprio, esse *firewall* é muito seguro pois ele impede que servidores de fora tenham interação com a rede local.

### 2.4.4. Pfsense

O *pfsense* foi desenvolvido por Chris Buechler e Scott Ullrich em 2014, é um sistema gratuito baseado em FreeBSD com algumas modificações. Basicamente, tem como motivação promover conexão com internet de maneira mais segura, configurável como *firewall* ou roteador de rede.

Por ser uma opção barata para proteger a rede, o *pfsense* é utilizado não só por pequenas empresas, mas também por médias e até grandes organizações. Pode-se utilizar o *pfsense* como *firewall*, servidor (DHCP, *proxy*, internet...), antivírus, antispware, antispam, filtro de conteúdo, etc. Além dessas funcionalidades, o *pfsense* é leve então não necessita de muito recurso computacional para ser implementado.

A ferramenta *pfsense* é boa para clientes que não querem gastar tanto na hora de implementar uma solução de *firewall* e que ao mesmo tempo não abre mão da segurança nas conexões de rede.

## 2.5 RADIUS

“Remote Authentication Dial-In User Service (RADIUS) é um sistema centralizado de autenticação para clientes. É frequentemente implementado para garantir um nível adicional de segurança em uma rede de computadores.” (RODRIGUES, 2013). Esse protocolo é baseado em pergunta e resposta, usa o protocolo de transporte UDP nas portas 1812 e 1813. “Ele tem a função principal de permitir acesso a clientes remotos e separar os acessos internos dos externos.” (RODRIGUES, 2013).

O RADIUS, Remote Authentication Dial In User Service, é um protocolo amplamente utilizado para gerenciar o acesso dos mais diversos serviços de rede. Este protocolo define um padrão para troca de informações entre um Servidor de acesso à rede (NAS, Network Access Server) e um servidor AAA para realizar a autenticação, a autorização e as operações de gerenciamento de contas. (MACÊDO, 2012).

Com o RADIUS é possível colocar em prática em rede local ou empresarial uma Política de Segurança da Informação ou uma Política de Controle de Acesso previamente definida e modelada.

O RADIUS trabalha com o modelo cliente/ servidor, sendo que o cliente do servidor é o NAS. O servidor recebe o pedido do usuário para acessar. O RADIUS possui 3 funções: autenticação, autorização e *accounting*.

A autenticação é uma referência ao procedimento que confirma a validade do usuário que realiza a requisição de um serviço. Este procedimento é baseado na apresentação de uma identidade junto com uma ou mais credenciais. As senhas e os certificados digitais são exemplos de credenciais.

A autorização é a concessão de uso para determinados tipos de serviço, dada a um usuário previamente autenticado, com base na sua identidade, nos serviços que requisita e no estado atual do sistema. A autorização pode ser baseada em restrições, que são definidas por um horário de permissão de acesso ou localização física do usuário, por exemplo.

O procedimento de *accounting* é uma referência à coleta da informação relacionada à utilização de recursos de rede pelos usuários. Esta informação pode ser utilizada para gerenciamento, planejamento, cobrança e etc. (DUQUE, 2016).

Simplificando, na autenticação é feita a checagem de permissão para o usuário acessar a rede, a autorização dá para esses usuários autenticados a permissão de diversos serviços de rede e o *accounting* representa e acompanha o uso desses serviços oferecidos pelo RADIUS.

O RADIUS apresenta várias funções que o coloca como um bom *server* de autenticação em diversas redes, e se apresenta como uma forma segura de autenticar usuários e definir o quê esses usuários poderão acessar na rede.

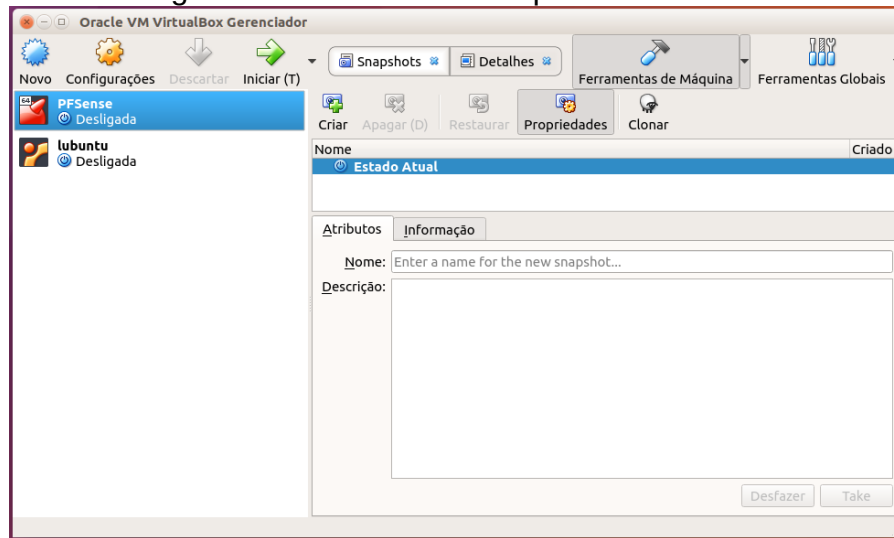
### **3. IMPLANTAÇÃO DO FIREWALL PFSENSE E RADIUS**

Será mostrado ferramentas importantes para a configuração do *pfsense*, o RADIUS será instalado dentro do *pfsense* por meio do *Freeradius3*. Essas ferramentas servirão para serem realizados os testes no ambiente, analise e mostrar os resultados.

#### **3.1 PREPARAÇÃO DO AMBIENTE**

Para a realização da configuração do *pfsense* e do *freeradius3* foram utilizados 2 máquinas virtuais criadas no *VirtualBox*, sendo mostrado na figura 10.

Figura 10: VirtualBox e máquinas instaladas

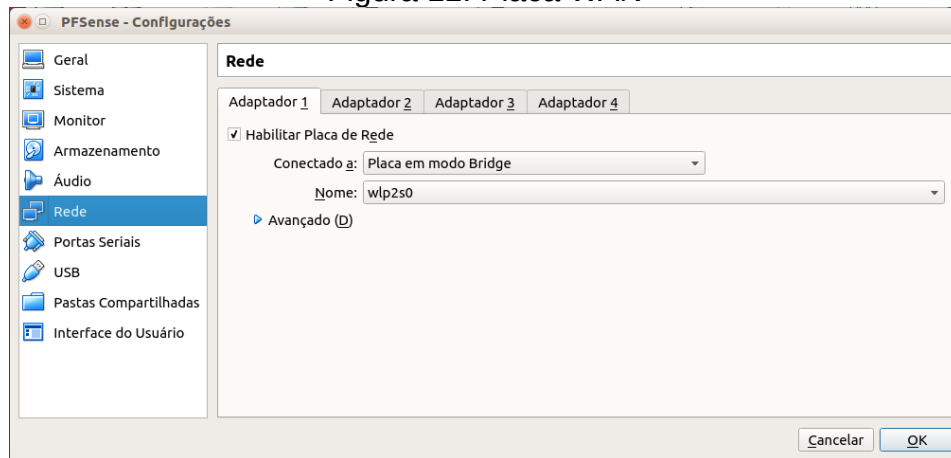


Fonte: Própria

Foram criadas 2 máquinas virtuais para representar 2 máquinas físicas, a máquina “*pfsense*” representa o servidor de *firewall pfsense*, enquanto a máquina “*lubuntu*” representa um cliente da rede interna que vai utilizar a máquina “*pfsense*” como seu servidor de *firewall*.

Na máquina virtual “*pfsense*” serão utilizados 2 placas de rede. O primeiro adaptador de rede terá a denominação “*wlp2s0*”, se pode visualizar na figura 11, será responsável pela rede WAN do *pfsense*, esse adaptador vai receber internet, aplicará seu *firewall*, configurações e restrições para que sejam conectados outros computadores por meio da rede LAN.

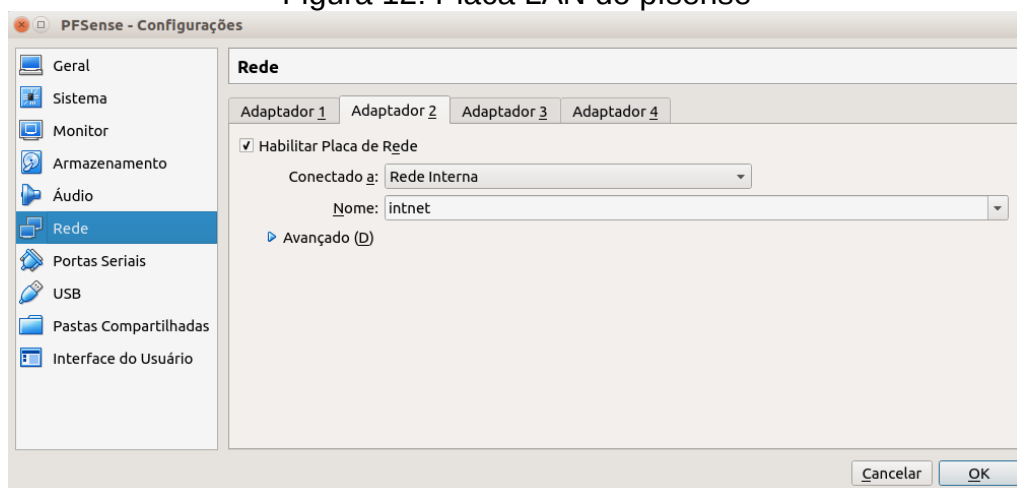
Figura 11: Placa WAN



Fonte: Própria

O segundo adaptador rede da máquina “*pfsense*” será destinado para rede LAN e terá a denominação “*intnet*”, vista na figura 12. A rede LAN será responsável pela rede interna da organização. Nesse trabalho esse segundo adaptador serve para interligar outros computadores formando uma rede interna protegida pelo *firewall* do *pfsense*.

Figura 12: Placa LAN do pfsense

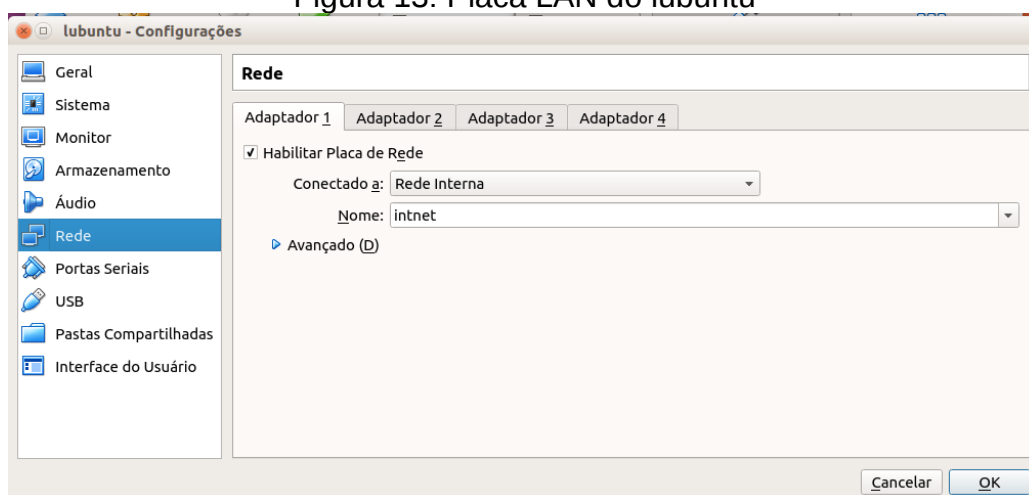


Fonte: Própria



A máquina que estará conectada a rede interna desse ambiente simulado será a máquina “lubuntu”, onde também precisa ser feita uma configuração no adaptador de rede. Na configuração no *VirtualBox*, na aba de “Redes” será habilitado 1 adaptador de rede que corresponderá a rede interna, esse receberá a denominação “intnet”, que posteriormente será conectado com o *firewall pfSense*. Podemos visualizar essa configuração feita na figura 13.

Figura 13: Placa LAN do lubuntu



Fonte: Própria

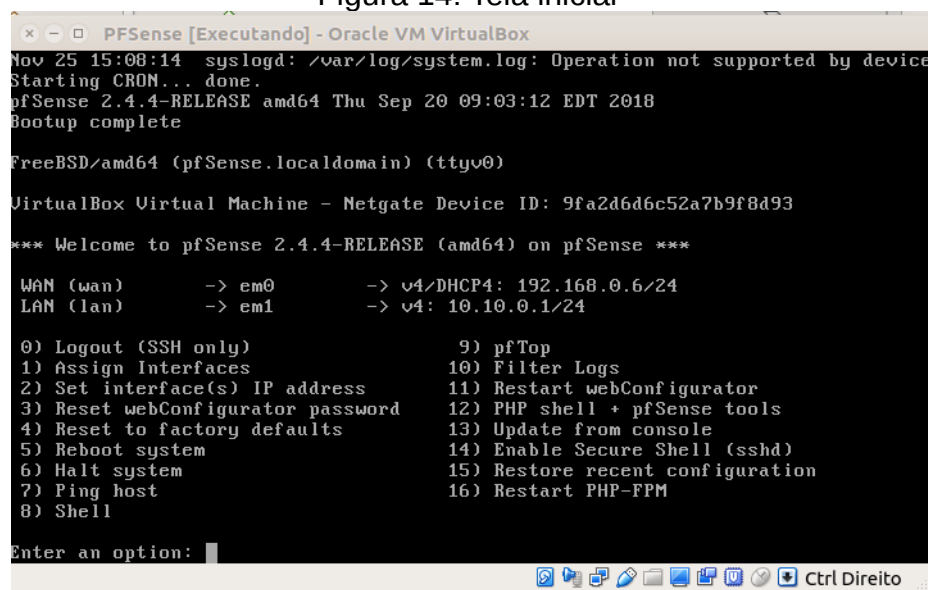
Além do computador “lubuntu”, pode-se também acessar a página do *pfSense* pelo computador real, pois na configuração o adaptador 1 da máquina “*pfSense*” está conectado em modo bridge.

Após o *pfSense* instalado de forma básica e rápida pode-se chegar a tela inicial do *pfSense* ilustrado na figura 14. A versão utilizada para esse projeto foi a *pfSense* 2.4.4 – RELEASE amd64, instalada através de uma versão ISO.

### 3.2 CONFIGURAÇÃO DO PFSENSE

A interface de rede WAN recebeu a denominação em0, essa interface terá a função de conectar o *firewall pfSense* com a rede externa. Enquanto a interface LAN recebeu a denominação em1 e será responsável por conectar a rede interna com o *pfSense*.

Figura 14: Tela inicial



```
Nov 25 15:08:14 syslogd: /var/log/system.log: Operation not supported by device
Starting CRON... done.
pfSense 2.4.4-RELEASE amd64 Thu Sep 20 09:03:12 EDT 2018
Bootup complete

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)

VirtualBox Virtual Machine - Netgate Device ID: 9fa2d6d6c52a7b9f8d93

*** Welcome to pfSense 2.4.4-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.0.6/24
LAN (lan)      -> em1      -> v4: 10.10.0.1/24

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

Enter an option: 
```

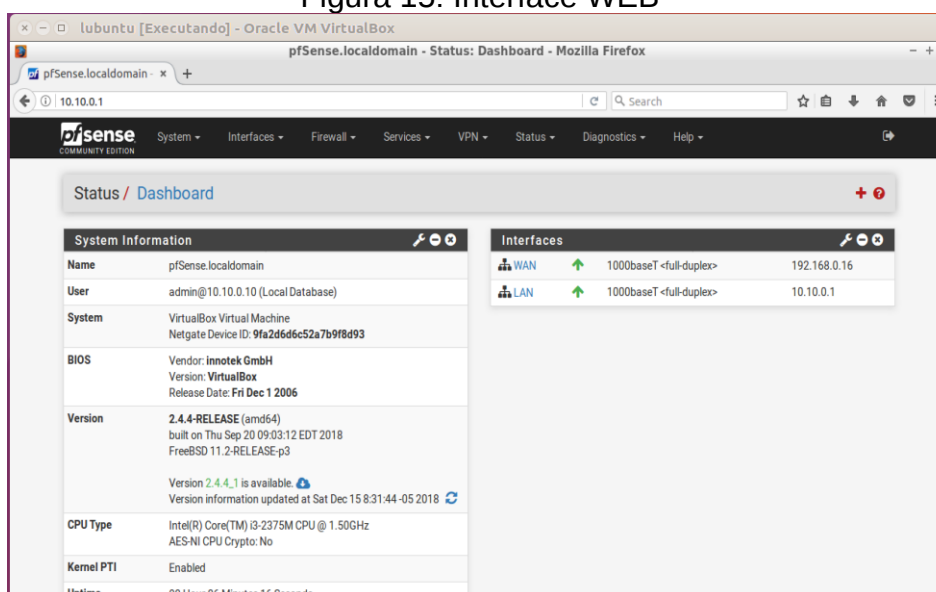
Fonte: Própria

Pode-se observar na figura 14 que a interface de rede LAN foi configurada manualmente e foi escolhido o endereço IP 10.10.0.1, a máscara de rede utilizada foi a 255.255.255.0 (/24). O DHCP para a LAN está ativado, definindo o range entre os IPs 10.10.0.10 até 10.10.0.254 da rede para que os IPs da rede possam ser definidos automaticamente pelo próprio *pfSense* ao conectar máquinas clientes na rede, não dependendo assim de IPs fixos. A interface WAN não será configurado um IP fixo, porém é possível definir fixamente o IP da WAN.

### 3.2.1. Pfsense WEB

Pode ser feito algumas configurações primárias na tela inicial como foi mostrado, porém há outra forma de proferir configurações e administrar um servidor *pfsense*. Por meio do modo WEB se pode realizar configurações de maneira mais fácil e prática para o usuário, tendo uma gama de informações adicionais para ser gerenciado.

Figura 15: Interface WEB



Fonte: Própria

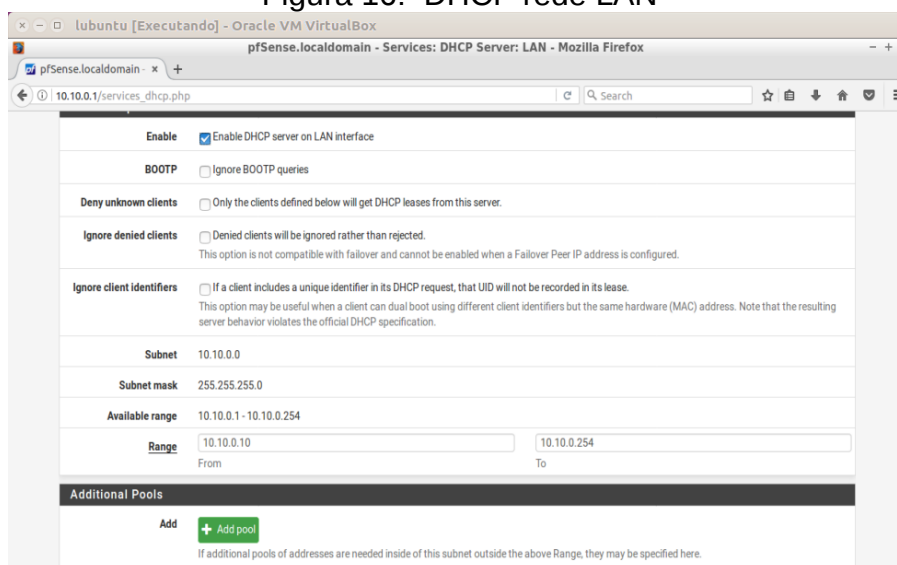
Com a figura 15 observa-se tela do *pfsense* acessado de modo WEB, onde é possível fazer mudanças no servidor de uma forma fácil e rápida. Para acessar essa interface é necessário digitar o IP da rede LAN configurada previamente (IP 10.10.0.1) e depois fazer o login com o usuário e a senha. Na tela inicial do *pfsense* já é mostrado algumas informações básicas do sistema, como: nome, usuário que está logado, sistema, BIOS, versão, tempo que o servidor está ativo, status das interfaces, etc. Com as modificações das configurações no servidor se pode adicionar mais informações na tela inicial e customizar baseado com as necessidades e preferências.

### 3.2.2. DHCP Server

O *pfSense* também pode trabalhar com o DHCP server da rede. A rede LAN já foi configurada um DHCP nas configurações iniciais pelo modo shell, mas também é possível configurar um novo DHCP sever ou modificá-lo.

Nesse projeto a rede LAN (intnet) foi definido com o IP 10.10.0.1 e o *pfSense* vai trabalhar o DHCP na rede LAN a partir do IP 10.10.0.10 até o IP 10.10.0.254, foi exposto na figura 16.

Figura 16: DHCP rede LAN

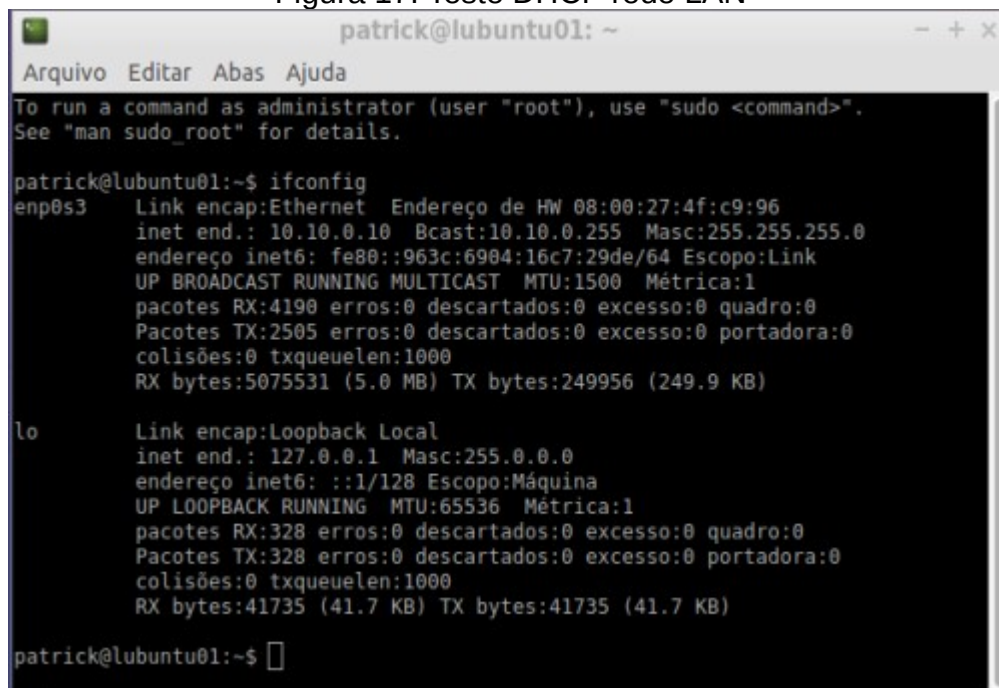


Fonte: Própria

Ainda na figura 16 é apresentado o range de IPs disponíveis para rede LAN (intnet) partindo do IP 10.10.0.1 até 10.10.0.254 sendo que a mesma é do tipo 10.10.0.0 e a máscara de IP 255.255.255.0 ou \24.

Toda vez que um computador for introduzido na rede LAN (intnet) o DHCP server lhe atribuirá um IP entre o range descrito que ainda não está sendo utilizado. Para testar podemos acessar a máquina “lubuntu” que está conectada na rede LAN e executar o comando “ifconfig” no terminal do SO.

Figura 17: Teste DHCP rede LAN



```

patrick@lubuntu01: ~
Arquivo Editar Abas Ajuda
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

patrick@lubuntu01:~$ ifconfig
enp0s3  Link encap:Ethernet  Endereço de HW 08:00:27:4f:c9:96
        inet end.: 10.10.0.10  Bcast:10.10.0.255  Masc:255.255.255.0
        endereço inet6: fe80::963c:6904:16c7:29de/64  Escopo:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Métrica:1
        pacotes RX:4190 erros:0 descartados:0 excesso:0 quadro:0
        Pacotes TX:2505 erros:0 descartados:0 excesso:0 portadora:0
        colisões:0 txqueuelen:1000
        RX bytes:5075531 (5.0 MB) TX bytes:249956 (249.9 KB)

lo      Link encap:Loopback Local
        inet end.: 127.0.0.1  Masc:255.0.0.0
        endereço inet6: ::1/128  Escopo:Máquina
        UP LOOPBACK RUNNING  MTU:65536  Métrica:1
        pacotes RX:328 erros:0 descartados:0 excesso:0 quadro:0
        Pacotes TX:328 erros:0 descartados:0 excesso:0 portadora:0
        colisões:0 txqueuelen:1000
        RX bytes:41735 (41.7 KB) TX bytes:41735 (41.7 KB)

patrick@lubuntu01:~$ 

```

Fonte: Própria

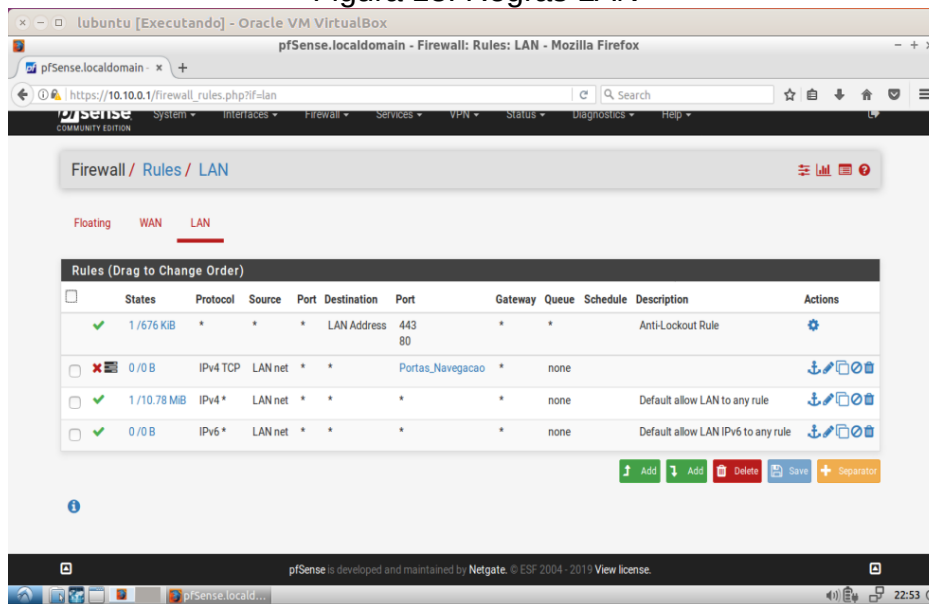
Com a figura 17 nota-se que o DHCP está funcionando corretamente. Uma máquina foi conectada e obteve o endereço IP 10.10.0.10, se uma segunda máquina fosse conectada na rede LAN a mesma receberia o IP 10.10.0.11 e assim até acabar o range de IPs.

### 3.2.3. Regras de Firewall

Essa é uma etapa bastante importante na configuração do *pfsense*, pois são as regras permitirá ou negará a passagem dos dados pela rede. Para criar as regras no *pfsense* será necessário definir em qual interface as regras atuarão, interface WAN, LAN, etc. É possível bloquear tudo em uma interface e deixar passar só o que interessa a rede, como permitir tudo menos o que estiver bloqueado.

É importante analisar com cuidado a posição de uma regra, pois a regra que estiver acima prevalece em relação as que estão embaixo.

Figura 18: Regras LAN

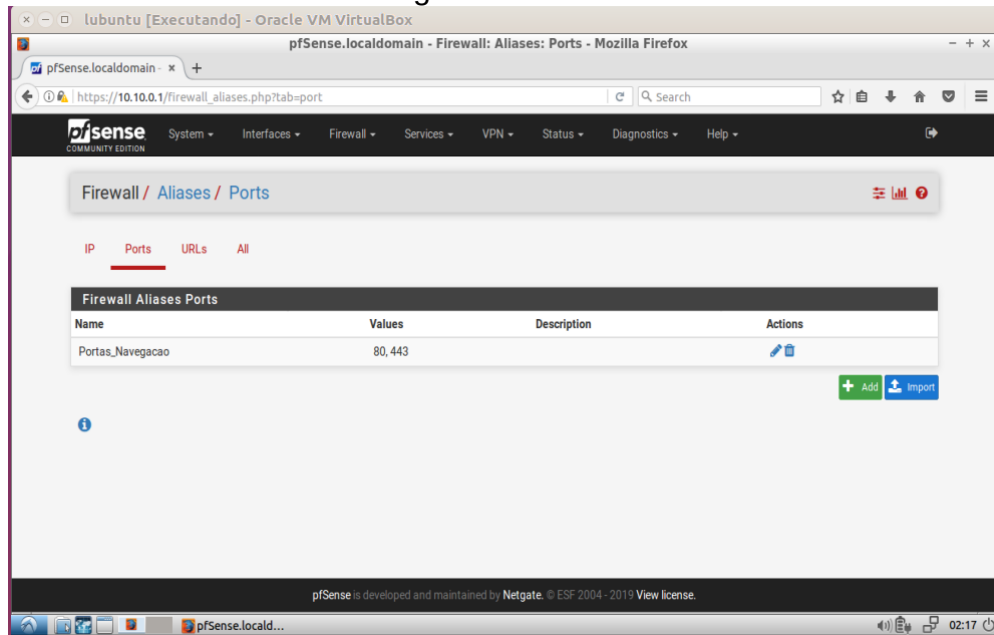


Fonte: Própria

Foi exposto com figura 18 a criação regras para a interface LAN, essas regras irão bloquear ou permitir baseado na configuração, as regras funcionam de cima para baixo na hora da leitura. A regra 1 na interface LAN é para permitir que o colaborador possa acessar a interface web, esta regra está no topo e foi criada automaticamente e não pode ser removida.

A regra 2 foi criada com objetivo de bloquear as portas de navegação na internet, o usuário não poderá utilizar a internet. Para bloquear as portas de navegação 80 e 433 foi criado uma *alias* com o nome Portas\_Navegacao, que é basicamente um grupo de portas, hosts ou rede que ajudam na criação de regras. É possível visualizar a *alias* Portas\_Navegacao na figura 19. Para elaborar uma *alias* basta ir na aba *Firewall > Aliases*, podendo ainda ser separadas por IP, Ports, URLs e All.

Figura 19: Aliase



Fonte: Própria

A regra 3 mostrada na figura 18 permitirá todo o tráfego com origem na interface LAN utilizando o IPv4. A quarta regra também irá permitir todo o tráfego com origem na interface LAN, porém essa regra vale para o protocolo IPv6.

### 3.2.4. FreeRADIUS

*FreeRADIUS* é um servidor RADIUS bastante utilizado no mundo, trabalha com autenticação, autorização e contabilidade e foi iniciado em 1999 por Alan DeKok e Miquel van Smoorenburg.

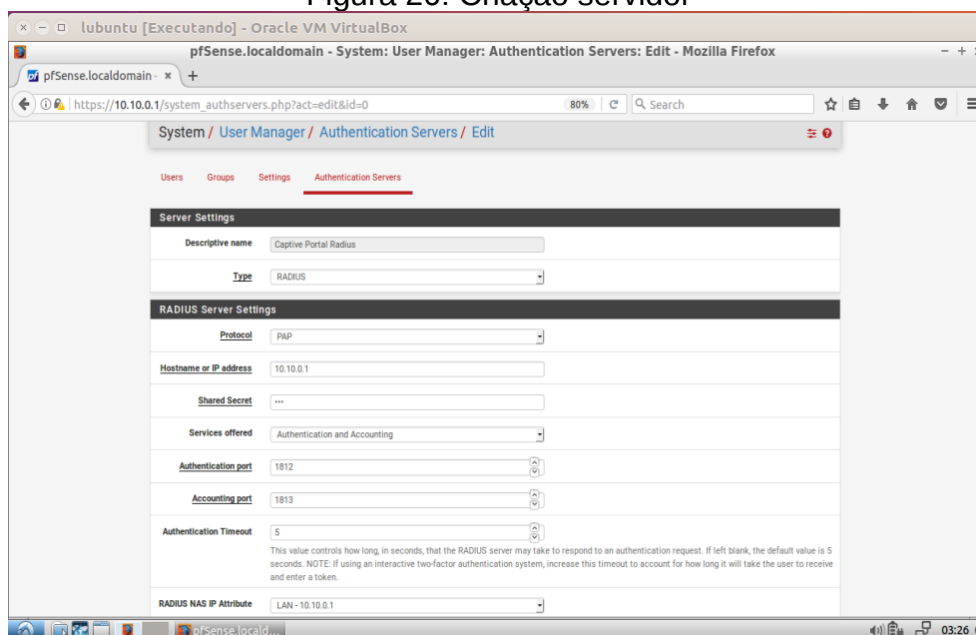
Esse trabalho utilizará o *freeradius3* que será instalado através do *pfsense*. O servidor RADIUS será utilizado para autenticar os usuários por meio do CP e assim permitir os que podem acessar a internet e os que terão o acesso à internet negado.

O freeradius3 foi instalado por meio da aba *Sytem > Package Manager > Available Packages*, basta buscar o nome “freeradius3”, logo em seguida é preciso clicar em *Install*.

Com o *freeradius3* instalado, para a criação do servidor de autenticação será necessário entrar na aba *System > User Manager > Authentication Servers* e clicar em *Add*.

Foi exposto com a figura 20 a criação do servidor com a denominação “Captive Portal Radius”, utilizando o protocolo PAP com o IP 10.10.0.1, o IP do servidor de autenticação RADIUS vai ser o mesmo IP do servidor *pfsense*. Foi definido um segredo (secret) que vai comparar com o segredo do NAS.

Figura 20: Criação servidor

The image is a screenshot of a web browser window displaying the pfSense configuration interface. The browser's address bar shows the URL 'https://10.10.0.1/system\_authservers.php?act=edit&id=0'. The page title is 'pfSense.localdomain - System: User Manager: Authentication Servers: Edit - Mozilla Firefox'. The breadcrumb navigation shows 'System / User Manager / Authentication Servers / Edit'. The main content area is titled 'Authentication Servers' and contains a form for editing a server. The 'Server Settings' section includes a 'Descriptive name' field with the value 'Captive Portal Radius' and a 'Type' dropdown menu set to 'RADIUS'. The 'RADIUS Server Settings' section includes a 'Protocol' dropdown set to 'PAP', a 'Hostname or IP address' field with the value '10.10.0.1', a 'Shared Secret' field with a masked value, a 'Services offered' dropdown set to 'Authentication and Accounting', an 'Authentication port' spinner set to '1812', an 'Accounting port' spinner set to '1813', and an 'Authentication Timeout' spinner set to '5'. A note below the timeout field explains its function. At the bottom, the 'RADIUS NAS IP Attribute' dropdown is set to 'LAN - 10.10.0.1'. The browser's status bar at the bottom shows the time as 03:26.

Fonte: Própria

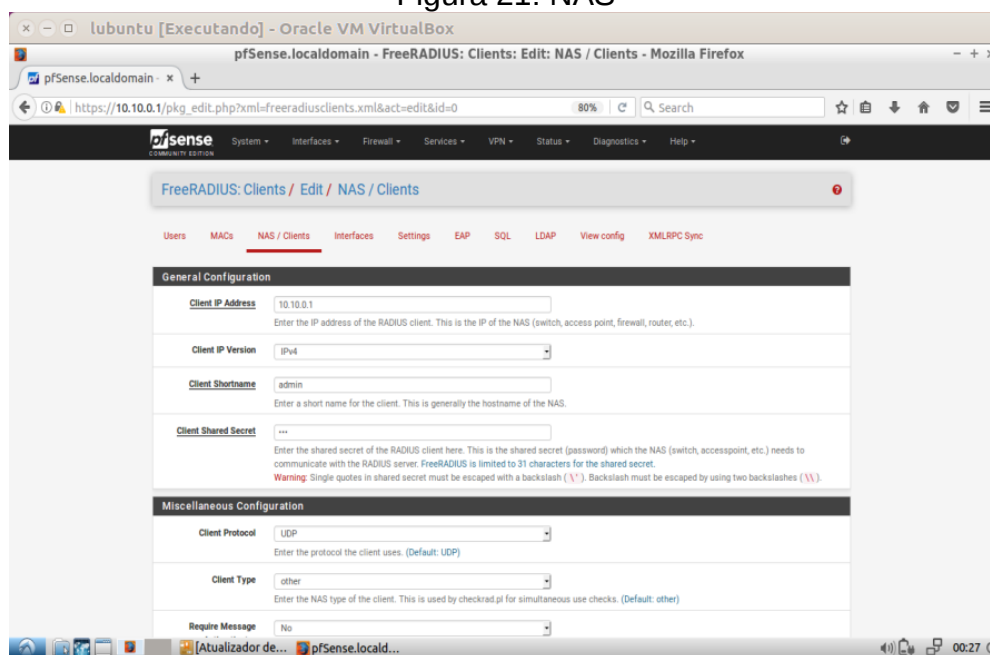
Na criação do servidor é definido as portas de trabalho do servidor, a porta de autenticação é a 1812, que é uma porta padrão para autenticar usuários por meio do RADIUS.



O próximo passo é fazer a configuração do servidor. Na aba *Services* > *FreeRADIUS* pode criar usuários, configurar o *NAS/Clients*, definir as interfaces, etc.

É possível visualizar na figura 21 que na aba *NAS\Clients* foi criado um NAS para poder receber as solicitações dos clientes e fazer a autenticação junto com o servidor. Um NAS é criado com o IP do servidor que foi configurado anteriormente (10.10.0.1), é o IP da interface LAN onde o Captive Portal será configurado, também é necessário informar o segredo do servidor. Na descrição foi colocado Captive Portal NAS.

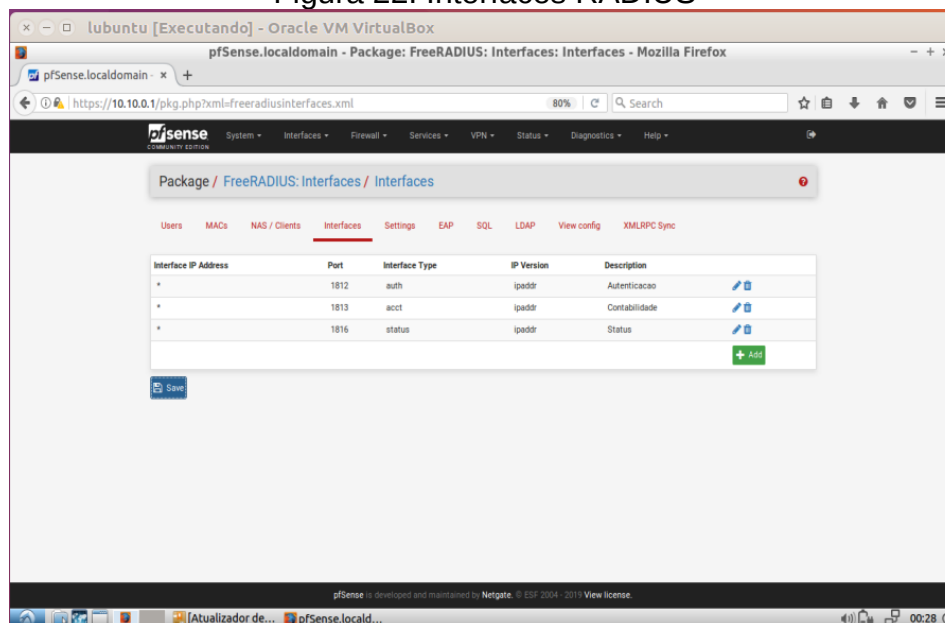
Figura 21: NAS



Fonte: Própria

Ainda a aba do *FreeRADIUS* é necessário criar as interfaces, para isso basta ir em *Interfaces*. A figura 22 expoe que foram criados três interfaces, a primeira vai ter a função de autenticação e vai utilizar a porta 1812, a segunda vai ter a função de contabilização e vai utilizar a porta 1813 e a terceira vai ser a interface para status com porta 1816, é possível observar isso na figura 22.

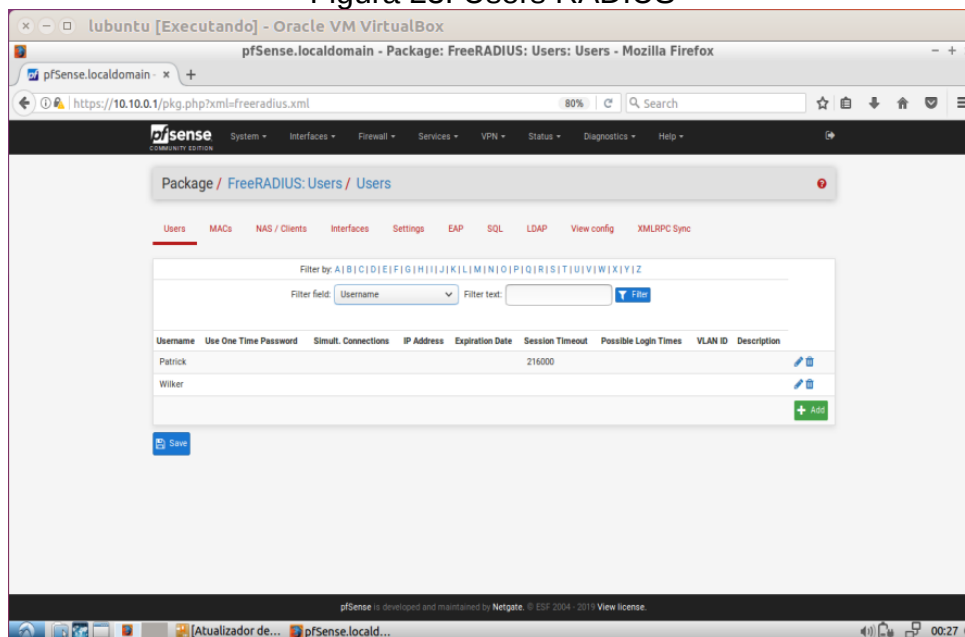
Figura 22: Interfaces RADIUS



Fonte: Própria

Na aba de *Users* é onde pode criar os usuários, foram criados dois usuários para exemplos e testes, como revela a figura 23. Cada usuário vai ter uma senha diferente do outro para uma maior segurança. A aba *Users* tem importância pois nela pode ser definidas configurações para cada usuário, é possível direcionar para um site específico após o usuário logar no CP, o admin da rede pode definir uma data para expiração do usuário, assim como a velocidade de internet que cada usuário pode usar e outras funções.

Figura 23: Users RADIUS



Fonte: Própria

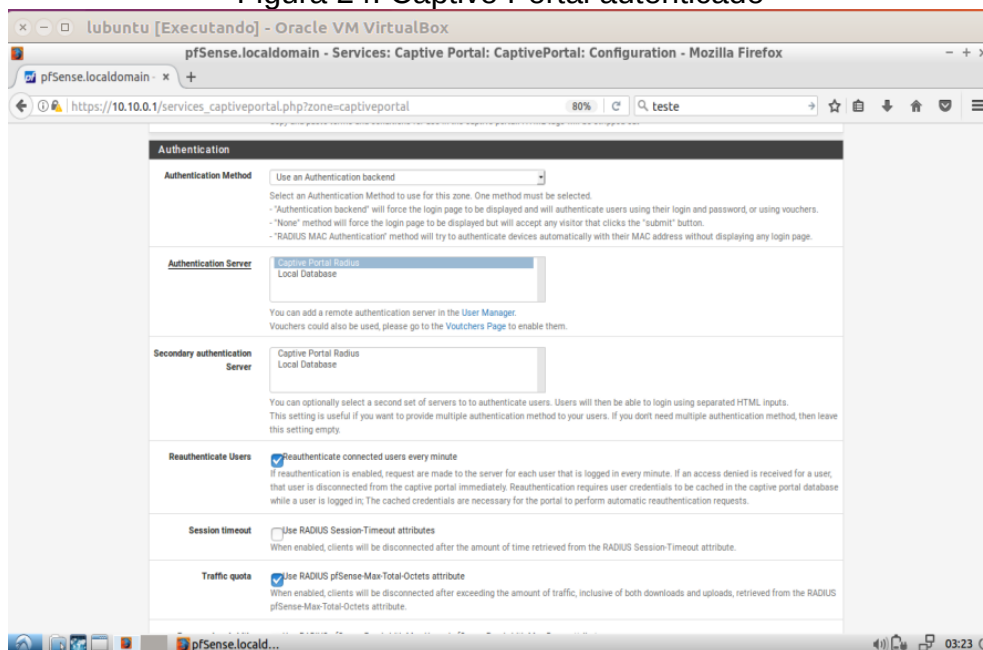
### 3.2.5. Captive Portal

Captive Portal tem o foco de controlar a navegação. Os usuários que utilizam o Captive Portal podem acessar a internet desde que eles sejam autenticados. No *pfSense* essa autenticação pode ser feita de algumas formas, através de vouchers, autenticação local pelos usuários no próprio *pfSense* e autenticação por um servidor RADIUS. Ainda no Captive Portal é possível definir endereços de IP ou de MAC que estarão autorizados ou bloqueados automaticamente.

Para adicionar um CP é necessário entrar na *Services > Captive Portal* e depois adicionar um novo. É importante definir a interface que o Captive Portal vai atuar, é muito comum utilizar nas redes *wireless*.

Foi definido que o Captive Portal atuará na interface LAN, logo vai ser solicitado uma autenticação para todo usuário que utilizar a rede LAN. Se pode visualizar com figura 24 que o campo *Authetication Server* foi selecionado *Captive Portal Radius*, é o servidor que foi criado anteriormente.

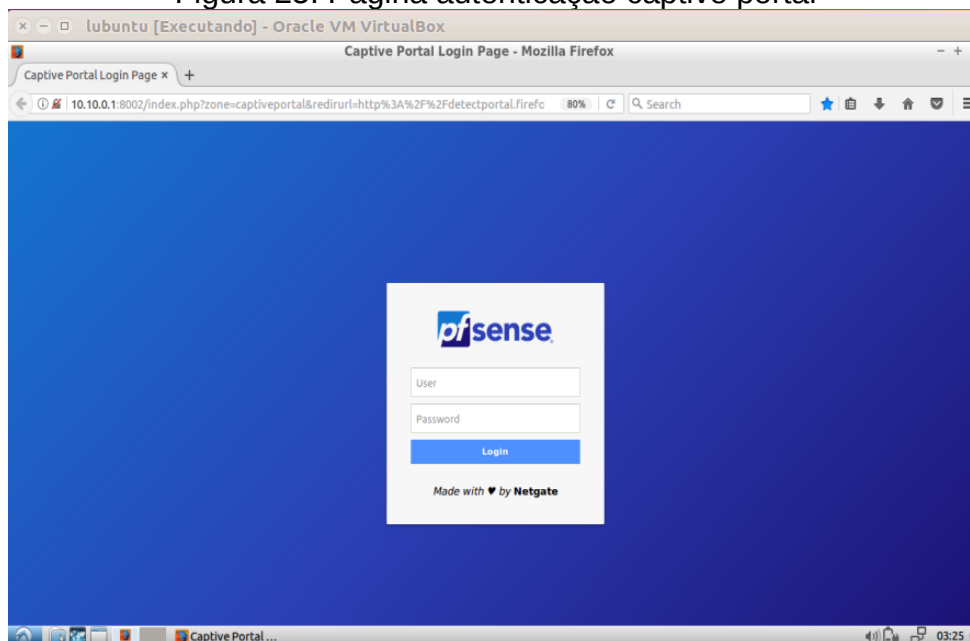
Figura 24: Captive Portal autenticado



Fonte: Própria

Pronto, agora o RADIUS está autenticando por meio do CP as pessoas que estão conectadas na rede LAN e que solicitam utilizar a internet. Para acessar basta entrar no navegador que automaticamente será redirecionado para a página de login do Captive Portal, após o login o usuário será direcionado para a página pré definida pelo administrador podendo ser o site da organização ou qualquer outro. A figura 25 apresenta a página de login do CP após as configurações.

Figura 25: Página autenticação captive portal

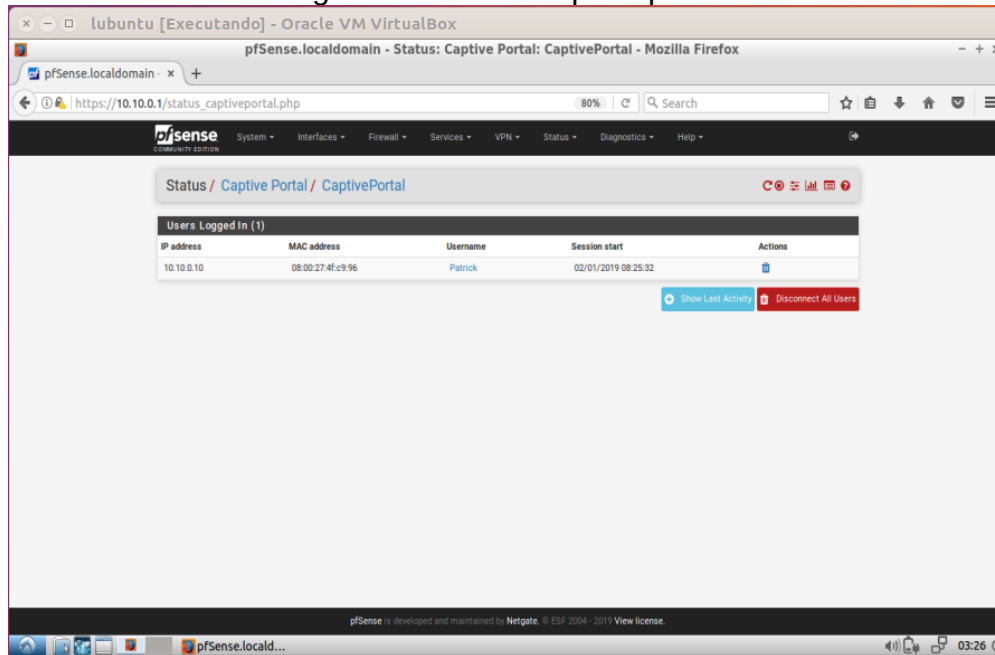


Fonte: Própria

Assim que o colaborador coloca seu nome e senha e o login é efetuado com sucesso, o *pfsense* salva os *logs*, assim fica fácil saber qual usuário está acessando determinado conteúdo como também os horários, isso é fundamental para saber se a Política de Segurança da empresa/organização está sendo respeitada, evitando assim futuros problemas.

Na aba *Status* > Captive Portal é possível saber quais usuários estão logados e utilizando a internet, como revela a figura 26.

Figura 26: Status captive portal



Fonte: Própria

### 3.2.6. Servidor proxy

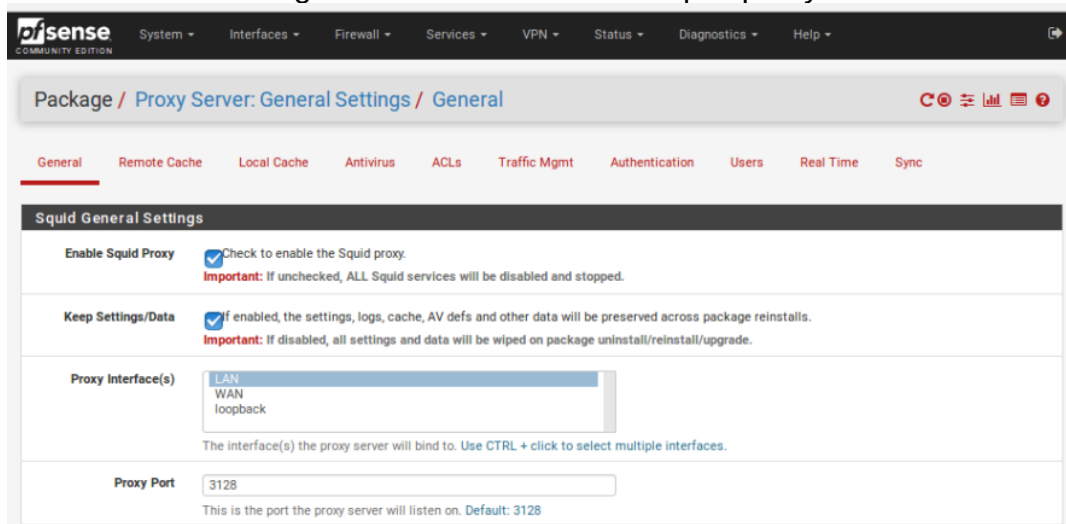
A parte final desse trabalho consiste na instalação e configuração de um servidor *proxy* que tem como função de receber requisições de clientes para utilizar serviços, o *proxy* vai fazer a intermediação do cliente de um serviço, com isso o cliente não terá acesso direto com a internet.

Para a realização do servidor *proxy*, foi utilizado o Squid *proxy*, sendo ele um software livre e que suporta os protocolos HTTP, HTTPS e FTP. A instalação do Squid *proxy* é feita de maneira semelhante as outras já mostradas, basta entrar a aba *System* > *Package Manager* e depois em *Available Packages* e procure pelo nome *squid*.

É a hora fazer a configuração, para usar o *Squid* é necessário entrar na aba *Services* > *Squid proxy Server*. O Squid tem muitas funções e pode ser

adequado baseado com cada necessidade, na aba General é preciso definir a interface onde o *proxy* atuará, foi definido a LAN e foi definido como a porta de acesso 3128, sendo a padrão. Para gerar relatórios é necessário marcar a opção de logs. A aba General tem sua ilustração com a figura 27.

Figura 27: Aba General do Squid proxy



Fonte: Própria

A definição da porta do *proxy* é relevante pois posteriormente será necessário utilizar a configuração da porta do *proxy* no navegador. Como anteriormente na parte de configurar as regras foram bloqueadas a porta de HTTP e HTTPS a navegação na internet ficou restrita ao *proxy*. É importante configurar as opções de cache na aba *Local Cache*, sendo definido o tamanho de memória que será disponibilizado para o cache, os IPs que não será preciso ser salvo em cache, etc.

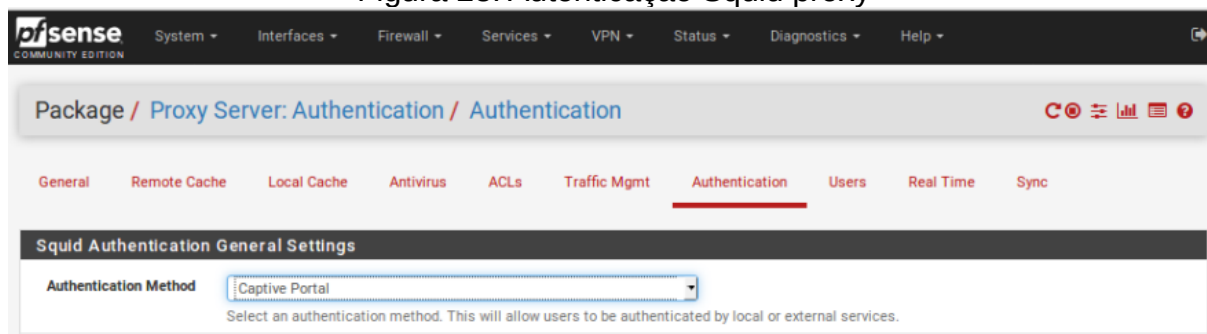
Na aba *ACLs*, é possível fazer rápidos bloqueios de sites na opção Blacklist. A aba *ACLs* também é interessante para definir quais IPs não passarão pelo filtro do *proxy*.

O *Squid proxy* tem a opção de utilização do *proxy* transparente, não é necessário colocar a porta no navegador, porém esse *proxy* não bloqueia o protocolo HTTPS. Outra opção de *proxy* é o autenticado, esse tem maior segurança

em relação ao *proxy* transparente, pois será necessário uma autenticação para navegar. Foi abordado a utilização do *proxy* autenticado.

Para configurar o *proxy* autenticado é necessário entrar aba *Authentication*, ilustrado na figura 28.

Figura 28: Autenticação Squid proxy

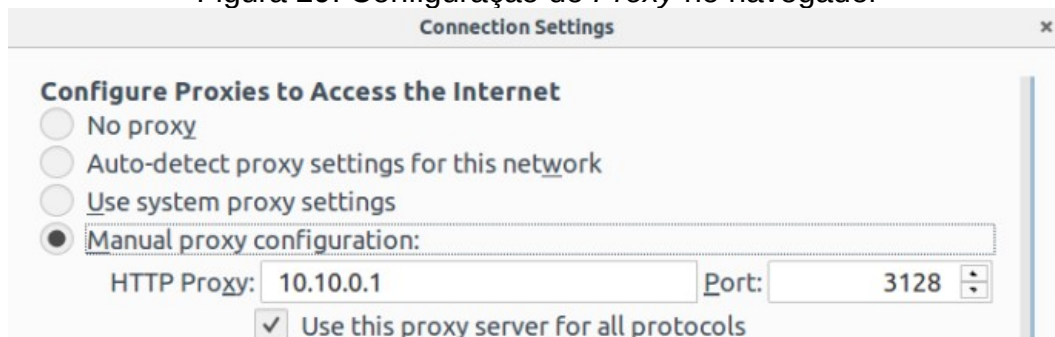


Fonte: Própria.

Como já foi ajustado um CP com a autenticação feita pelo RADIUS, foi selecionado o Captive Portal. Os usuários que foram criados para autenticação no RADIUS, irão ser utilizados para validar o CP, e o CP autenticará o *proxy*.

Após o método de autenticação estar configurado é necessário realizar a configuração do *proxy* no navegador informando o endereço do servidor e a porta, assim, o Squid *proxy* funcionará, como ilustra a figura 29.

Figura 29: Configuração do Proxy no navegador



Fonte: Própria

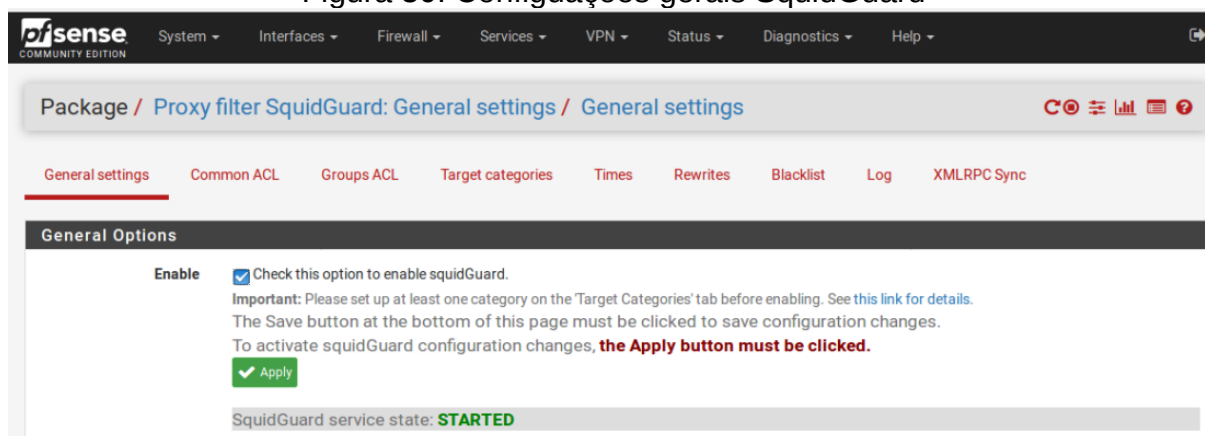


Para complementar o *Squid proxy* é utilizando o *SquidGuard*, pois ele tem a capacidade de bloquear inúmeros sites classificados por categorias, como: jogos, notícias, pornografia, etc. O *SquidGuard* utiliza uma lista para bloquear todos os tipos de site, isso deixa a segurança da empresa muito mais completa.

O processo de instalação do *SquidGuard* é feito de maneira simples, basta acessar a aba *System > Package Manager* e depois em *Available Packages* e procure pelo nome *squidguard*. Após a instalação é necessário elaborar as configurações com base em cada situação.

A aba *General settings* é importante para ativar *SquidGuard*. O botão *Apply* vai ser muito utilizado, pois a cada modificação feita é necessário aplicá-la com o botão *Apply*. O botão pode ser visto na figura 30.

Figura 30: Configurações gerais SquidGuard

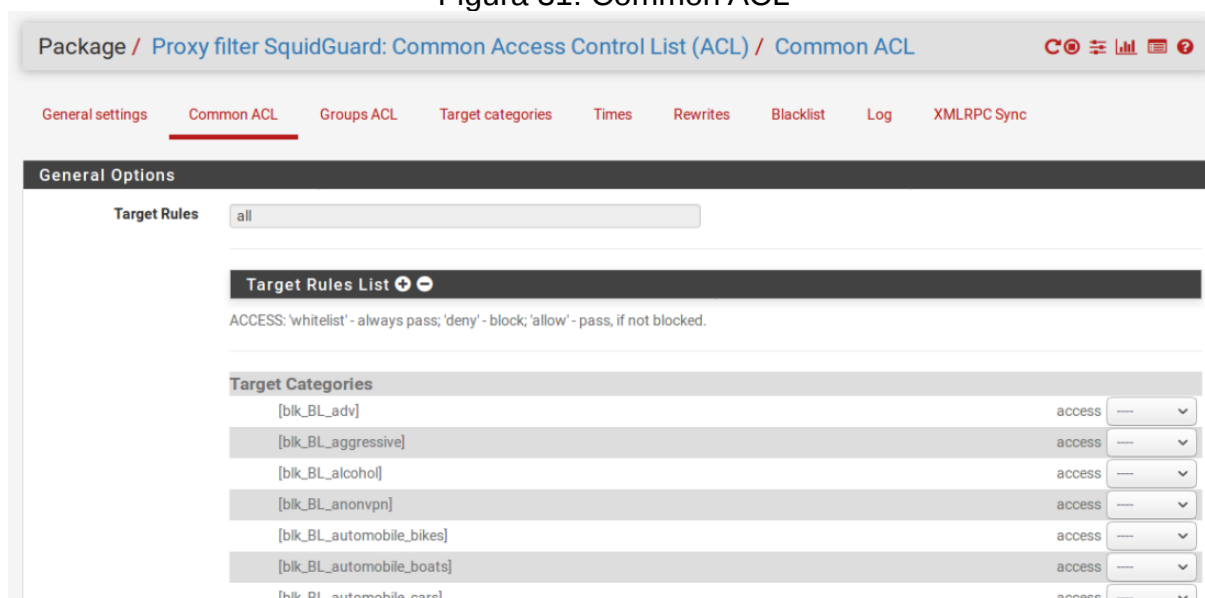


Fonte: Própria

Ainda na aba *General settings* é importante deixar marcado as opções de *log* do *SquidGuard*. Mais abaixo tem a opção de *Blacklist URL* que foi preenchido com uma URL de uma blacklist do site *Shalla Secure Services*. Essa *blacklist* é livre e bem completa, porém para uso comercial tem algumas restrições. Para baixar de fato a lista negra informada na URL, tem que acessar a aba *Blacklist* e realizar o *download*. Com uma lista negra o trabalho do *proxy firewall* fica bem mais fácil, é importante analisar muito bem a política de informação para efetuar as restrições de acesso.

Na figura 31 fica claro que de maneira geral, na aba *Common ACL* é possível realizar uma configuração padrão para todos os usuários do *proxy*.

Figura 31: Common ACL

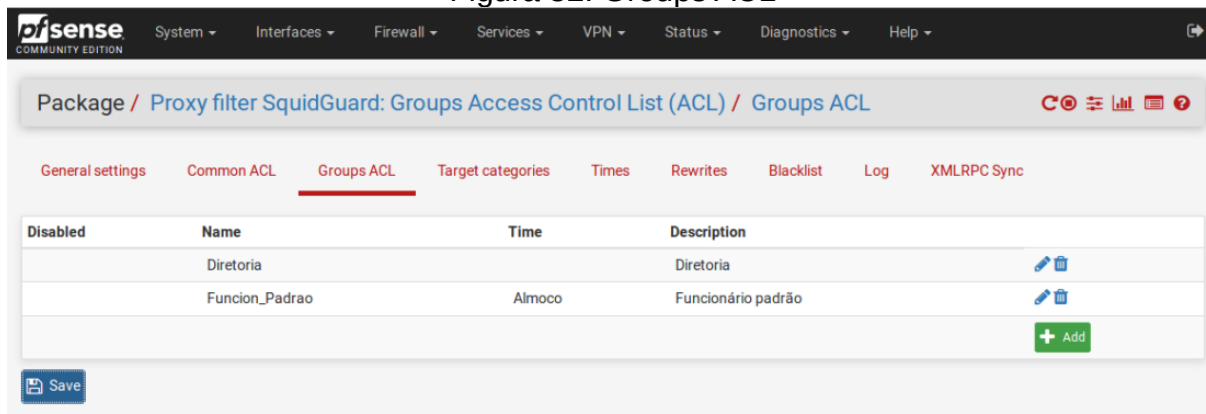


Fonte: Própria

Com a listra negra é possível liberar ou negar acesso a determinadas categorias, a figura 31 aborda apenas algumas delas. Vale ressaltar para definir quais sites devem ser acessado no horário de trabalho de uma organização varia muito da sua Política de Segurança, pode ser visto um modelo de documento no Apêndice A.

Na aba *Groups ACL* é possível determinar grupos, sendo que eles podem ser compostos por IPs, usuários, etc. Cada grupo pode ter sua personalização de acesso. Na figura 32 mostra que foram criados dois grupos: Diretoria e Funcion\_Padrao. Os usuários do grupo da diretoria terão acesso liberado para mais categorias em relação aos usuários que estiverem no grupo de funcionário padrão. O usuário Wilker foi adicionado no grupo da diretoria, logo ele vai ter privilégios de acesso em relação ao usuário Patrick que foi adicionado no grupo dos funcionários padrões.

Figura 32: Groups ACL



Fonte: Própria

Com a figura 32 se pode perceber que na opção Time está escrito Almoco no grupo Funcion\_Padrao. No *SquidGuard* é possível definir um horário para que as regras de acesso possam ser flexibilizadas, nesse caso a hora do almoço. Na prática foi definido que o grupo Funcion\_Padrao não pode acessar as redes sociais no horário normal de trabalho, porém na hora do almoço será possível acessar as redes sociais. O grupo Diretoria não precisa de um Time, pois já foi definido que eles poderão acessar as redes sociais a qualquer momento.

Para elaborar um período de tempo para a flexibilização das regras de acesso, é necessário entrar na aba Times do *SquidGuard*. Com a figura 33 é possível observar que o tempo Almoco foi determinado para todos os dias da semana, com o horário entre as 12:00 horas e as 13 horas e 59 minutos, esse período é denominado de “hora do almoço” e nesse período de tempo foi feita uma flexibilização na regra de acesso com base na política de controle.

Caso a *blacklist* baixada não tenha todos os sites necessários, é possível criar uma categoria na aba *Target categories*.

Figura 33: Times SquidGuard

Proxy filter SquidGuard: Times / Edit / Times

General settings Common ACL Groups ACL Target categories **Times** Rewrites Blacklist Log XMLRPC Sync

**General Options**

**Name** Almoco  
Enter a unique name of this rule here.  
The name must consist between 2 and 15 symbols [a-Z\_0-9]. The first one must be a letter.

**Values** Weekly all 12:00-13:59  
Time type Days Date or Date range Time range

**Add** + Add

**Description**  
You may enter any description here for your reference.  
**Note:**  
Example for Date or Date Range: 2007.12.31 or 2007.11.31-2007.12.31 or \*.12.31 or 2007.\*.31  
Example for Time Range: 08:00-18:00

**Save**

Fonte: Própria

Após o término das configurações no *SquidGuard*, é necessário aplicá-las na aba *General settings*. Pode-se perceber na figura 34, o usuário Patrick que está associado ao grupo *Funcion\_Padrao* tentou acessar o *facebook* em horário diferente do almoço, logo não é permitido acessar as redes sociais no horário normal. É possível perceber na mesma figura que é indicado qual categoria da lista negra se encaixa aquele bloqueio, *facebook* e *twitter* estão na categoria *socialnet*, também é indicado qual grupo de ACL o usuário faz parte. Também não foi possível o acesso ao *Spotify* que está na categoria *music*.

Figura 34: Teste bloqueio a sites

SquidGuard Table		SquidGuard Logs		
Date-Time	ACL	Address	Host	User
10.02.2019 10:43:18	Request(Diretoria/blk_BL_porn/-)	www.xvideos.com:443	10.10.0.10/10.10.0.10	wilker
10.02.2019 10:40:52	Request(Funcion_Padrao/blk_BL_hobby_games-misc/-)	www.twitch.tv:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:40:31	Request(Funcion_Padrao/blk_BL_music/-)	www.spotify.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:40:21	Request(Funcion_Padrao/blk_BL_socialnet/-)	twitter.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:50	Request(Funcion_Padrao/blk_BL_socialnet/-)	twitter.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:45	Request(Funcion_Padrao/blk_BL_socialnet/-)	www.facebook.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:44	Request(Funcion_Padrao/blk_BL_socialnet/-)	tr.snapchat.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:40	Request(Funcion_Padrao/blk_BL_socialnet/-)	connect.facebook.net:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:40	Request(Funcion_Padrao/blk_BL_socialnet/-)	platform.twitter.com:443	10.10.0.10/10.10.0.10	patrick
10.02.2019 10:37:20	Request(Funcion_Padrao/blk_BL_socialnet/-)	pt-br.facebook.com:443	10.10.0.10/10.10.0.10	patrick

Fonte: Própria

Ainda analisando a figura 34 é possível observar o usuário Wilker do grupo *Diretoria* tentou acessar um site pornográfico e também foi negado. Porém a figura 35 mostra que o colaborador Wilker está navegando no *Spotify* e no *YouTube*,

a configuração do *Squid proxy* juntamente ao *SquidGuard* funcionou, cada grupo pode acessar conteúdos específicos na internet. Como a Diretoria tem privilégios, foi definido que os usuários que fazem parte desse grupo poderão acessar sites de músicas, vídeos e redes sociais em qualquer horário.

Figura 35: Teste acesso a sites

Squid Access Table					
Squid - Access Logs					
Date	IP	Status	Address	User	Destination
10.02.2019 10:57:00	10.10.0.10	TCP_TUNNEL/200	www.spotify.com:443	Wilker	104.154.127.47
10.02.2019 10:56:57	10.10.0.10	TCP_TUNNEL/200	www.youtube.com:443	Wilker	216.58.202.14
10.02.2019 10:56:44	10.10.0.10	TCP_TUNNEL/200	cm.g.doubleclick.net:443	Wilker	216.58.202.162
10.02.2019 10:56:44	10.10.0.10	TCP_TUNNEL/200	match.adsrvr.org:443	Wilker	34.192.39.141
10.02.2019 10:56:44	10.10.0.10	TCP_TUNNEL/200	r.dlx.addthis.com:443	Wilker	54.85.112.149
10.02.2019 10:56:42	10.10.0.10	TCP_TUNNEL/200	pixel.tapad.com:443	Wilker	107.178.246.49
10.02.2019 10:56:39	10.10.0.10	TCP_TUNNEL/200	bat.bing.com:443	Wilker	204.79.197.200
10.02.2019 10:56:38	10.10.0.10	TCP_TUNNEL/200	pixel.advertising.com:443	Wilker	18.208.9.84
10.02.2019 10:56:38	10.10.0.10	TCP_TUNNEL/200	insight.adsrvr.org:443	Wilker	35.170.199.226
10.02.2019 10:56:36	10.10.0.10	TCP_TUNNEL/200	syndication.twitter.com:443	Wilker	104.244.42.136

Fonte: Própria

O *SquidGuard* integrado ao *Squid proxy* é uma ferramenta muito poderosa, com ela é possível fazer inúmeras configurações baseadas nas opções de cada cliente.

## 4. CONSIDERAÇÕES FINAIS E RECOMENDAÇÕES

### 4.1 CONSIDERAÇÕES FINAIS

Não é de hoje como a informação vêm se tornando peça-chave em uma organização, com isso, várias formas de tentar roubar essas informações são implementadas diariamente. A internet é uma grande ferramenta para busca do conhecimento, comunicação ou trabalho, então apesar dos riscos, é inviável uma empresa ou organização ficar sem utilizá-la.

Dada a importância ao assunto, torna-se necessário buscar meios para tornar uma rede de uma empresa/organização com menos poder aquisitivo mais segura. O CP com o RADIUS se mostrou uma forma muito eficiente.

Para chegar aos objetivos iniciais, foi realizado um estudo com base em segurança da informação, redes e *firewall*. Logo após, foi criado um ambiente para simular uma rede, e foi apresentado algumas ferramentas do software *pfsense* acompanhado do protocolo RADIUS para controlar acessos na LAN.

Este trabalho apresentou uma maneira barata e segura para modelar e aplicar uma Política de Segurança na rede interna em organizações usando o

RADIUS e o CP. O ponto inicial é definir bem a PSI pra depois implementar a teoria na prática.

## 4.2 RECOMENDAÇÕES

É possível listar algumas recomendações para trabalhos futuros, são elas:

- a) Administração e gerenciamento de bilhetagem e controle de logs de usuários;
- b) Implementação do serviço de relatórios detalhados sobre o uso da rede pelos clientes;
- c) Descrever atividades de gestão para melhorias de novas implementações nas Políticas de Controle de Acesso (PCA);
- d) Apresentar novas ferramentas para controle de PCAs implementada sob componentes de controle de acesso usando biometria;

## REFERÊNCIAS

Campos, André. **Sistema de Segurança da Informação: Controlando riscos**. 2. ed. Florianópolis: VisualBooks, 2007.

PALMA, Fernando. **Sistema de Gestão de Segurança da Informação (SGSI)**, 2017. Disponível em: <<https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>>. Acesso em: 05 set. 2017.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. Ed. Campus, 2003. 160p.

KOSUTIC, Dejan. **O que é um Sistema de Gestão de Segurança da Informação (SGSI) de acordo com a ISO 27001?**, 2016. Disponível em: <<https://advisera.com/27001academy/pt-br/blog/2016/05/30/o-que-e-um-sistema-de-gestao-de-seguranca-da-informacao-sgsi-de-acordo-com-a-iso-27001/>>. Acesso em: 05 set. 2017.

MOREIRA, Esdras. **O que é a Política de Segurança da Informação (PSI)?**, 2017. Disponível em: <<http://introduceti.com.br/blog/o-que-e-a-politica-de-seguranca-da-informacao-psi/>>. Acesso em: 14 de nov. 2018.

PINTO, Pedro. **LAN, MAN, WAN, PAN, SAN ... Sabe a diferença?**, 2010. Disponível em: <<https://pplware.sapo.pt/tutoriais/networking/lan-man-wan-pan-san-%E2%80%A6-sabe-a-diferenca/>>. Acesso em: 14 de nov. 2018.

ALECRIM, Emerson. **O que é firewall? - Conceito, tipos e arquiteturas**, 2013. Disponível em: <<https://www.infowester.com/firewall.php>>. Acesso em: 06 de dez. 2018.

DUQUE, Luciano. **Banda Larga: Autenticação Radius**, 2016. Disponível em: <[http://www.teleco.com.br/tutoriais/tutorialblcdr/pagina\\_2.asp](http://www.teleco.com.br/tutoriais/tutorialblcdr/pagina_2.asp)>. Acesso em: 06 de dez. 2018.



CARVALHO, Hugo. **Radius**, 2008. Disponível em: <[https://www.gta.ufrj.br/grad/08\\_1/radius/index.html](https://www.gta.ufrj.br/grad/08_1/radius/index.html)>. Acesso em: 06 de dez. 2018.

OLIVEIRA, Paulo. **O que é e por que usar um firewall pfsense pra sua rede?**, 2016. Disponível em: <<https://www.escolaLinux.com.br/blog/o-que-e-e-por-que-usar-um-firewall-pfsense-pra-sua-rede>>. Acesso em: 06 de dez. 2018.

Shalla Secure Services, **Shalla's Blacklists** 2018. Disponível em: <<http://www.shallalist.de/>>. Acesso em: 05 de fev. 2019.

MACÊDO, Diogo. **RADIUS**, 2012. Disponível em: <<https://www.diegomacedo.com.br/radius/>>. Acesso em: 13 de fev. 2019.

RODRIGUES, Carlos. **Radius**, 2013. Disponível em: <[https://www.projetoderedes.com.br/artigos/artigo\\_radius.php/](https://www.projetoderedes.com.br/artigos/artigo_radius.php/)>. Acesso em: 13 de fev. 2019.

ALECRIM, Emerson. **O que é Wi-Fi (IEEE 802.11)?**, 2008. Disponível em: <<https://www.infowester.com/wifi.php>>. Acesso em: 13 de fev. 2019.

CARISSIMI, A.; ROCHOL, J.; GRANVILLE, L. Z. **Redes de Computadores**. Porto Alegre: Bookman, 2009.

## **APÊNDICE A – POLÍTICAS DE SEGURANÇA**

### **1. INTRODUÇÃO**

Atualmente a informação é o bem mais precioso em uma instituição ou organização, por isso é necessário ter um cuidado a mais na hora de proteger essas informações. Sendo assim é importante que as empresas ou organizações com regras e boas práticas reforce a segurança na rede. É importante que todos os funcionários ou colaboradores da empresa ou organização sigam essa PSI.

### **2. OBJETIVO**

Essa Política de Segurança tem como foco deixar um documento genérico para que as empresas e/ou organizações possam definir para todos os colaboradores de forma clara e simples suas regras e condutas permitidas para cada indivíduo, assim como boas práticas de segurança da informação.

### **3. AUTENTICAÇÃO**

A validação dos colaboradores para poderem navegar na rede da empresa será feita através de usuário e senha para que tenha um melhor controle sobre quem acessa o quê, e definir exatamente quem pode acessar determinado conteúdo. Os usuários serão incluídos em grupos, em cada grupo será definido regras de acesso específicas. Exemplo, os usuários do grupo Diretoria tem mais liberdade de acesso em relação aos usuários do grupo RH.

-Controle de acesso de usuários à rede

### **3.1 Senhas**

Na hora da criação da senha pelos colaboradores da empresa é vital que seja utilizado senhas fortes para reduzir ao mínimo os riscos de alguma outra pessoa tente descobrir a senha e assim deixar brechas para invasão.

-Não é apropriado e seguro o colaborador utilizar senhas óbvias ou fáceis de serem descobertas, como nome do usuário, “123”, etc.

-É recomendado criar uma senha com 6 caracteres ou mais, e que misturem letras maiúsculas com minúsculas. Exemplo de uma senha forte: “poieHKJk76”. Uma senha forte é necessária, mas vale o aviso de memorizar bem a senha para não esquecer.

-Os colaboradores devem ficar ciente de que eles tem que ter cuidado pois tudo estará logado e vai ser possível determinar o que o colaborador faz na rede.

### **3.2 Acesso a internet**

-A internet deve ser usada para buscar de conhecimento ou como ferramenta para trabalho, com exceções na hora do almoço que será liberado redes sociais.

-No horário do expediente a internet será utilizada para fins de trabalho.

-Para acessar a internet o colaborador deve logar no Captive Portal pelo navegador.

-Não tem como navegar sem o proxy devidamente configurado, sempre será acessado pelo proxy da organização.

-Sites de músicas, redes sociais não poderão ser acessados no expediente de trabalho, porém será liberado na hora do almoço (12hrs:00min às 13hrs:59min).

-Sites acesso a sites pornográficos estará bloqueado.

- Todo acesso a sites está sendo monitorado.
- Download de arquivos será proibido. (adaptar a realidade específica)
- Youtube e serviços de stream será bloqueado para não comprometer a banda de internet ou desviar o foco.

#### 4. MAQUINAS DE TRABALHO

- É obrigatório efetuar o desligamento do computador sempre que acabar sua utilização para que outras pessoas não acessem o mesmo.
- Para usar notebooks pessoais e afins deve ser feito antes uma verificação pelas pessoas responsáveis.
- Caso esteja utilizando notebook próprio para fins de trabalho, é necessário que o mesmo seja protegido com uma senha no SO.
- Não é permitido instalação de softwares no computador da empresa, no caso do notebook é necessário tomar muito cuidado com programas maliciosos.
- Sempre deve manter o antivírus atualizado.

#### 5. BOAS PRÁTICAS DE SEGURANÇA

- Necessário atenção e cuidado com e-mails maliciosos para não comprometer informações.
- Não é aconselhável anotar as senhas em lugares como papel, computador, etc. Cada usuário deve decorar sua senha para ter uma maior segurança.
- Evite usar o notebook do trabalho em redes públicas.
- Não introduza CDs, DVDs ou pen-drivers de fora em computadores da empresa.

-É de suma importância o treinamento dos funcionários e colaboradores, assim como mostrar os riscos de segurança.

-Não comentar sobre senhas ou coisas sigilosas do trabalho com outras pessoas ou amigos

## 6. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA

Caso haja a violação de qualquer item da política de segurança a pessoa infratora deve ser notificada e avaliada pelas pessoas responsáveis.

## 7. SUPORTE

Se houver alguma sugestão, orientação ou reclamação é importante entrar em contato com e dar o feedback.

Telefone: xx xxxxx-xxxx

E-mail: [xx@xx.com](mailto:xx@xx.com)