UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Matheus José de Moura

Uso do Sistema *pfSense* para a Coleta de Dados de Redes Sem-fio

Uberlândia, Brasil

2019

UNIVERSIDADE FEDERAL DE UBERLÂNDIA

Matheus José de Moura

Uso do Sistema *pfSense* para a Coleta de Dados de Redes Sem-fio

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito exigido parcial à obtenção do grau de Bacharel em Sistemas de Informação.

Orientador: Rodrigo Sanches Miani

Universidade Federal de Uberlândia – UFU

Faculdade de Ciência da Computação

Bacharelado em Sistemas de Informação

Uberlândia, Brasil

2019

Matheus José de Moura

Uso do Sistema *pfSense* para a Coleta de Dados de Redes Sem-fio

Trabalho de conclusão de curso apresentado à Faculdade de Computação da Universidade Federal de Uberlândia, Minas Gerais, como requisito exigido parcial à obtenção do grau de Bacharel em Sistemas de Informação.

Uberlândia, Brasil, 12 de Julho de 2019:

Rodrigo Sanches Miani
Orientador

Luís Fernando Faina
Professor

Muriel Ribeiro Alves
Técnico

Uberlândia, Brasil
2019

Agradecimentos

Primeiramente agradeço a minha família meu pai Orlando, minha mãe Raquel e irmã Florença, por todo apoio na caminhada durante minha graduação, agradeço a todos outros familiares e meus amigos que estiverem me apoiando neste período. Fica também meu agradecimento a todos meus amigos do Centro de Tecnologia da Informação da Universidade Federal de Uberlândia, para o desenvolvimento do trabalho, apoio, estudos e a amizade no qual foi fundamental para a construção deste trabalho e principalmente aos professores Rogério Ribeiro e Rodrigo Miani, que tiveram papel fundamental para meu desenvolvimento e realização do trabalho de conclusão de curso. Por fim, agradeço a Deus a oportunidade de estar podendo concluir mais uma etapa na minha vida.

"O êxito da vida não se mede pelo caminho que você conquistou, mas sim pelas dificuldades que superou no caminho."

Abraham Lincoln

Resumo

A Internet possui um papel fundamental no cotidiano das pessoas, seja para enviar uma mensagem, fazer uma ligação de vídeo ou áudio, ler notícias entre outras funcionalidades. Com esse grande volume de pessoas acessando a Internet, o número de vulnerabilidades e ataques maliciosos se tornou cada vez mais frequentes. Nesse contexto, o objetivo deste trabalho é desenvolver um ambiente computacional que simule uma rede sem fio e possibilite a coleta dos dados de usuários conectados em tal rede. O sistema *pfSense* foi utilizado como base para a elaboração desse ambiente e a validação da proposta foi feita dentro da Universidade Federal de Uberlândia. Um experimento para analisar determinados comportamentos de usuários ao se conectarem em uma rede sem fio foi proposto para validar o sistema e as configurações propostas. Os resultados obtidos no trabalho mostram que é possível usar o *pfSense* para criar, gerenciar e coletar dados de uma rede sem fio pública.

Palavras-chave: Redes de computadores, Redes sem fio, Internet, Segurança de redes de computadores, *firewall*.

Lista de ilustrações

Lista de tabelas

Lista de abreviaturas e siglas

AP	Access Point
UFU	Universidade Federal de Uberlândia
Mbits/s	Megabits por segundos
GHz	Giga Hertz
EUA	Estados Unidos da América
LAN	Local area network
IES	Instituição de Ensino Superior
ICV	Integrity Check Value
CRC	Cyclic Redundancy Check
AES	AdvancedEncryption Standard
CCMP	CounterCipherMode
VPN	Virtual Private Network
KSA	Key Scheduler Algorithm
TKIP	Temporal Key Integrity Protocol
PMK	Chave mestra dupla
PTK	Chave transiente de dupla
AES	Advanced Encryption Standard
SSH	Secure Shell
STP	Spanning Tree Protocol

Sumário

1 Introdução

Com o avanço tecnológico e a convergência das redes de computadores, novos sistemas de acesso à Internet se tornaram cada vez mais presentes no nosso cotidiano. As redes sem fio, por exemplo, são definidas pelo padrão IEEE 802.11 *(Institute of Electrical and Electronics Engineers)* e representam uma das principais formas de acesso à Internet.

Um estudo realizado abordou o crescimento das redes sem fio, a fim de investigar a utilização de redes sem fio em ambientes internos quanto externos. O trabalho fez o uso de *wardriving* como metodologia para mapear o crescimento de redes sem fio em uma região, de maneira que fosse coletado dados sobre quantidades de redes sem fio existentes e as suas potências de sinais a fim de verificar a área cobertura do sinal (PASQUALINI; MARCONDES, 2012).Desta forma foi possível verificar que teve um aumento significativo de rede sem fio nas cidades, em comparação com anos anteriores.

Segundo Rufino (2015), apesar da praticidade das redes sem-fio novos riscos surgiram. Sem o conhecimento adequado e a necessidade de acesso rápido à Internet, usuários acabam se esquecendo e deixando de lado práticas de segurança das redes sem fio, tornando-se alvos de ataques e violações. Estende-se a esses riscos redes sem fio públicas como Universidades, órgãos governamentais, prefeituras, dentre outros setores.

As universidades, visando atender as necessidades de seus professores, funcionários, terceiros e alunos, fornecem acesso a Internet por meio de infraestruturas cabeadas ou de comunicação sem fio. Em geral, essas redes fornecem serviços de alta velocidade na transmissão de pacotes, com uma boa abrangência de área de sinal para conexão sem fio. Contudo, esse tipo de serviço pode ser explorado por usuários maliciosos à partir de ataques como apresentados por (VIEIRA, 2016):

- *Port Scanning*
- *M*AC Spoofing
- *A*taques Sniffers
- *Man in the Middle*

Dentro do contexto apresentado, as seguintes perguntas direcionam o tema proposto na monografia. Qual a importância de um *firewall* em uma rede sem fio? Como estruturar uma rede com o uso do sistema *pfSense*. Em relação à segurança de redes sem fio, qual é o comportamento das pessoas, perante uma rede sem fio desconhecida?

1.1 Objetivos

Com base nas perguntas apresentadas anteriormente, o presente trabalho tem como objetivo desenvolver uma infraestrutura computacional que permita a construção de uma rede sem fio pública alternativa usando os recursos de rede da própria instituição. Essa nova rede sem fio poderá ser utilizada para analisar dados como números de acessos e duração da conexão e permitir alterações na configuração da rede (alteração do nome da rede - SSIDs e uso de *captive portal*, por exemplo) para facilitar a execução de experimentos para análise de comportamento dos usuários.

O trabalho será conduzido a partir do desenvolvimento de um *Rogue Access Point*, ou *rogue* AP, que serve como um ponto de acesso sem fio não autorizado dentro de uma rede, no qual seu principal objetivo é a captura de informações. O sistema desenvolvido será instalado e validado dentro da Universidade Federal de Uberlândia (UFU).

1.1.1 Objetivos Específicos

- Implantar uma rede sem fio do tipo *Rogue Access Point* nas dependências da UFU usando o *pfSense*;
- Usar os recursos da rede sem fio criada com o *pfSense* para avaliar o comportamento de usuários perante dois tipos de redes sem fio - redes que fornecem aviso (*banner*) antes de permitir o ingresso de novos usuários e redes sem aviso.

A Figura 1 apresenta o cenário de construção do experimento, demonstrando o fornecimento da rede e o *firewall*. O *rogue AP* será instalado em alguns locais de interesse e estará ligado diretamente a um computador com o sistema *pfSense* que irá gerenciar o acesso dos usuários. O provimento de Internet para tal AP poderá ser feito usando as seguintes fontes: a própria rede cabeada da UFU, a própria rede sem fio da UFU ou uma rede móvel de uma operadora de telecomunicações.

O presente trabalho encontra-se estruturado da seguinte forma:

- o capítulo 2 desenvolve a fundamentação teórica do trabalho, a fim de contribuir para organização e entendimento do trabalho. O capítulo também relaciona alguns trabalhos correlatos;
- o capítulo 3 apresenta a metodologia, abordando as configurações usadas para o funcionamento do *pfSense* suas configurações e regras de *firewall*;
- o capítulo 4 fornece o desenvolvimento do ambiente da rede sem fio com uso do *pfSense* e apresenta os experimentos realizados, assim como as análises construídas;

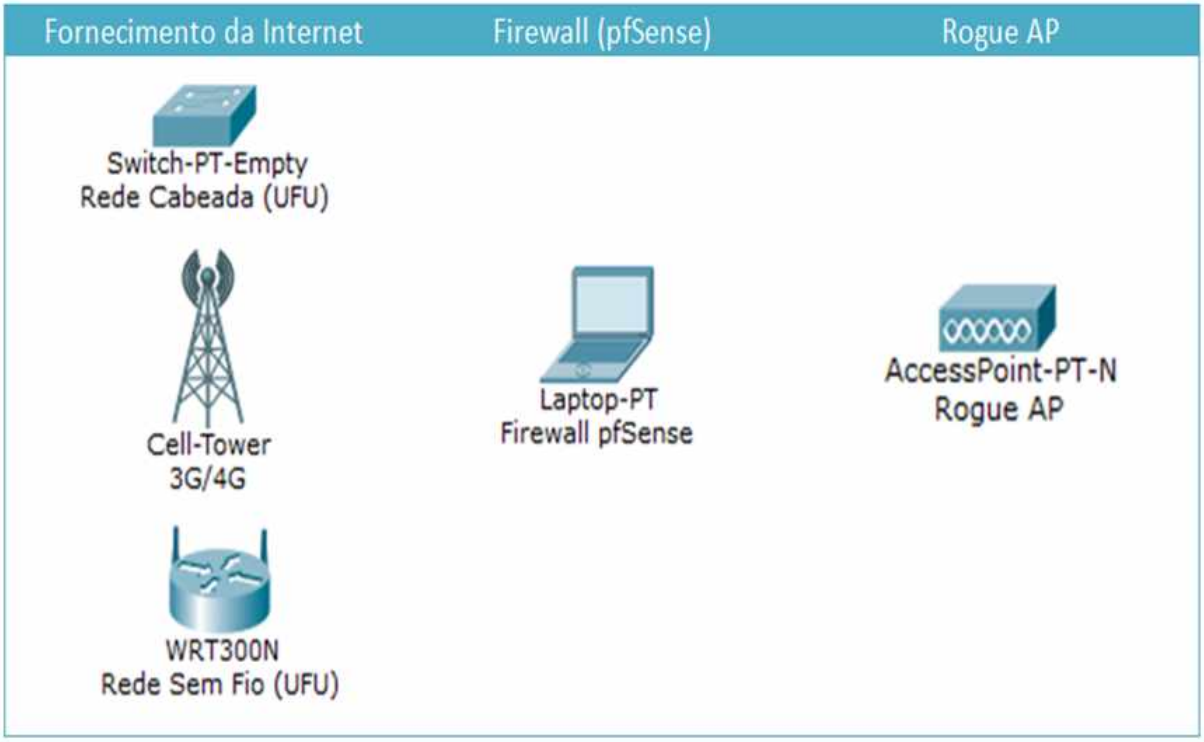

Figura 1 – Cenário do experimento

- Por fim, as conclusões e possibilidades de trabalhos futuros são discutidas no capítulo 5;

2 Fundamentação Teórica

Este capítulo descreve os fundamentos teóricos que abrangem os principais conceitos utilizados, que são necessários para a compreensão deste trabalho.

2.1 Redes sem fio

Pontos de acesso a redes sem fios públicos estão se tornando cada vez mais comuns em hotéis, aeroportos e cafés ao redor do mundo. A maioria dos campi universitários oferece acesso sem fio espalhado por toda a parte (KUROSE; ROSS, 2003). É possível identificar alguns elementos que categorizam uma rede sem fio:

- *Hospedeiros sem fio:* os hospedeiros sem fio são os equipamentos de sistemas finais que executam uma aplicação, podendo ser um notebook, smartphone ou até um computador de mesa; estes hospedeiros podem ser móveis ou não;
- *Enlaces sem fio:* É necessário que pelo menos um hospedeiro estabeleça uma conexão com uma estação-base, ou com outro meio de enlace de comunicação sem fio. Na Figura 1, é possível verificar que os enlaces sem fio se conectam a hospedeiros que estão localizados na borda da rede com a infra-estrutura da rede de maior porte.
- *Estação-base:* A estação-base é o principal componente de uma infra-estrutura de redes sem fio. Ela é responsável pelo envio e recebimento de dados e tem como função a coordenação da transmissão de vários hospedeiros sem fio nos quais estão associados a ela. Quando dizemos que um hospedeiro sem fio está "associado" a uma estação-base, isso quer dizer que (1) o hospedeiro está dentro do alcance de comunicação sem fio da estação-base e (2) o hospedeiro usa a estação-base para retransmitir dados entre ele (o hospedeiro) e a rede maior. Torres celulares em redes celulares e pontos de acesso em LANs sem fio 802.11 são exemplos de estações-base. Nessa circunstância os raciocínios a seguir são importantes, ou seja, quando os hospedeiros estão associados a alguma estação-base, geralmente quer dizer que eles estão operando em modo de infra-estrutura, uma vez que os serviços de redes como atribuição de endereços e roteamento são fornecidos pela rede na qual as estações bases estão conectados;
- *Infraestrutura de rede:* A infraestrutura é a rede maior na qual o hospedeiro sem fio poderá solicitar uma comunicação com uma infra-estrutura criada para interligação de hospedeiros.

A Figura 2 representa os elementos de uma rede sem fio, demonstrando áreas de coberturas e de deslocamento na qual o hospedeiro não perde a interatividade com uma conexão sem fio. Também é possível notar que diferentes sub-redes se interconectam com a mesma infraestrutura.

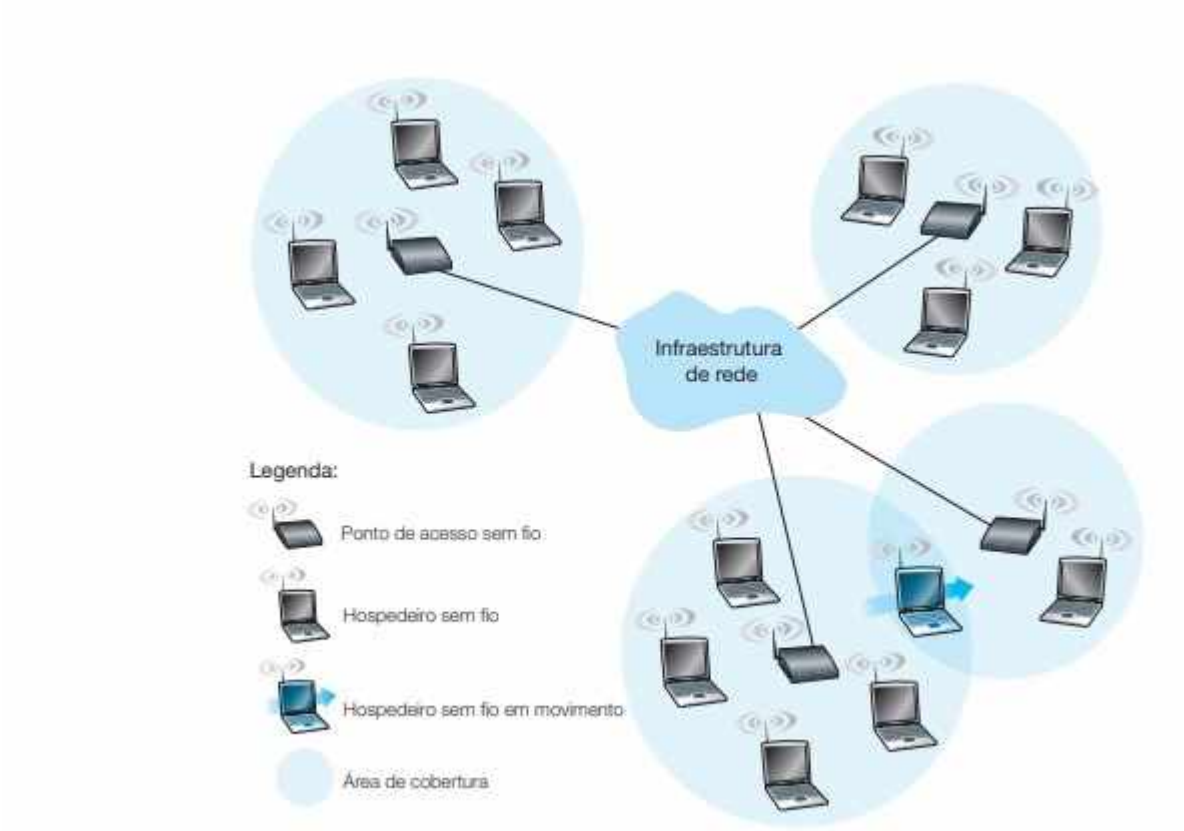

Figura 2 – Elementos de uma rede sem fio. Extraído de Kurose e Ross (2003)

2.1.1 Tecnologia Wi-Fi

As primeiras tecnologias sem fio surgiram no começo da década de 90, fazendo uso de frequência de 900 MHz e que fornecia taxa de transmissão de 1Mb/s. Já no ano de 1992, surgiram tentativas de implementações não padronizadas de produtos que operavam na faixa de 2.4 GHZ. Para uma padronização neste tipo de tecnologia, o grupo IEEE formou um grupo de trabalho denominado 802.11. No ano de 1997, o projeto foi finalizado e entregava taxas de transmissão de 1 e 2 Mb/s. Segundo Mendes (2007), com essa padronização, o grupo de trabalho foi fazendo melhorias e correções a fim de aperfeiçoar questões de desempenho e segurança, no 802.11.

Atualmente redes sem fio são encontradas em locais de trabalho, residências, instituições educacionais, aeroportos, cafés, uma vez que esta tecnologia passou a ser um importante meio de acesso à Internet. A rede sem fio IEEE 802.11, conhecida como Wi-Fi, é uma forma de acesso à rede por meio de meio de um sinal de radio frequência. A

Tabela 1, apresenta as variações de padrões da tecnologia IEEE, apresentando os padrões 802.11b, 802.11a e 802.11g e suas respectivas faixas de frequência e taxa de transferência de dados.

Tabela 1 – Tabela de Taxas dos padrões IEEE 802.11

Padrão	Faixa de frequências (EUA)	Taxa de dados
802.11b	2,4–2,485 GHz	até 11 Mbits/s
802.11a	5,1–5,8 GHz	até 54 Mbits/s
802.11g	2,4–2,485 GHz	até 54 Mbits/s

Estes padrões possuem alguns pontos em comuns, como o modo de infra-estrutura ad hoc, este tipo de rede não possui um nó ou terminal especial, é geralmente designado como ponto de acesso no qual todas as comunicações convergem para os respectivos destinos. Segundo Tanenbaum (2003), mesmo existindo pontos comuns nos padrões, há também diferenças que são importantes na implantação de uma rede sem fio, sendo elas:

1. 802.11b possui uma taxa de dados de aproximadamente 11 Mbits/s, ela opera dentro de uma faixa de frequência entre 2.4 a 537/8 Ghz. Dentro desta faixa, encontram-se espectros como telefones e microondas;

2. 802.11a tem frequências mais altas, assim entrega taxas de bits significativamente mais altas, mas o alto nível da frequência acaba que a distância de transmissão é relativamente mais curta para determinados níveis de potência, assim sofrendo propagações;

3. 802.11g opera na mesma freqüência que a 802.11b, porém trabalha com taxa de dados maiores, entregando assim ao usuário final uma melhor cobertura de sinal e taxa de dados.

2.2 Segurança da Informação

A fim de se compreender as diferentes formas na qual a segurança da informação se apresenta, é necessário definir os conceitos no qual formam sua base. A ABNT (2005), através da norma ABNT NBR ISO/IEC 17799:2005, estabelece diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação. Estas diretrizes e princípios buscam melhorar a segurança da informação, mas devido à importância que a informação possui, geri - lá de forma integra é uma tarefa difícil na qual se encontra sujeita a vários tipos de riscos e ameaças, para Marciano (2006) destaca-se:

1. Erros e falhas de natureza humana;

2. Forças da natureza (chuvas, tremores, incêndios, etc);
3. Falhas e erros provenientes de hardware ou software;
4. Atos como sabotagem, espionagem, invasão.

Em meio a estas ameaças no qual envolvem o gerenciamento da informação, os usuários buscam proteção contra estas ameaças, que podem afetar seus dados de informação. Para Dantas (2011), os pilares da segurança da informação podem ajudar na proteção dos dados, destaca três principais pilares: integridade, disponibilidade e confidencialidade.

- **Integridade:** este pilar da segurança impede a modificação não autorizada dos dados, garantindo que os dados continuem os mesmos na comunicação entre o emissor e receptor. Assim quaisquer alterações que ocorra nas informações, indiferente do nível de permissão que se tenha, são monitoradas, rastreados e documentados.
- **Disponibilidade:** este conceito garante que as informações possam ser acessadas e modificadas por qualquer pessoa autorizada a qualquer momento sem intervenção externa. De modo geral a disponibilidade consiste em proteger os serviços entregues pelo software de modo que não fiquem indisponíveis sem autorização, ou seja, afetados.
- **Confidencialidade:** um dos pilares da segurança a confidencialidade, consiste em proteger as informações sigilosas contra leitura e copia por alguém na qual não seja o proprietário ou autorizado a ter acesso à informação. Isso significa que visualização, alteração ou copia da informação só pode ser feita por pessoas autorizadas.

Mesmo apresentando os três principais pilares da segurança da informação é importante salientar que os mesmos estão sujeitos a apresentar falhas e sofrer algum tipo de ameaça, no qual possam afetar as informações. Desta forma, Dantas (2011) apresenta exemplos de riscos para cada um dos pilares:

- **Integridade:** este pilar é critico do ponto de vista operacional, pois é nele que se valida todo processo de comunicação seja ele de uma empresa, instituição ou comunidade. Um exemplo de violação de integridade pode ser visto no caso de uma empresa que possui uma rede local e usa a Internet para se comunicar com outros parceiros. Essa comunicação só é efetiva quando emissor e o receptor da informação interpretam a mensagem da mesma maneira. Quando essa informação é adulterada ou corrompida pelo caminho, demanda-se a verificação, correção e investigação, levando a empresa desperdiçar energia e recursos, podendo se traduzir em perda de dinheiro e credibilidade.

- **Disponibilidade:** a empresa Amazon, depende que seus servidores estejam no ar durante 24 horas nos 365 dias do ano, pois é um serviço disponível à partir da Internet. Os usuários que contratam serviços da Amazon esperam que os recursos contratados estejam sempre prontos para produção. Uma vez que a Amazon fique fora do ar mesmo que por poucos minutos, pode representar um grande prejuízo financeiro tanto para a Amazon quando para o contratante do serviço.
- **Confidencialidade:** um exemplo a citar são bancos e instituições financeiras, que por lei, são obrigadas a proteger os dados pessoais e financeiros de seus clientes, ocorrendo qualquer tipo de vazamento, são eles os responsáveis por danos causados.

2.3 Segurança em redes sem-fio

Com a popularização da rede sem fio, foi necessária a criação de protocolos para segurança em rede, os mais conhecidos e utilizados são o WEP e WPA, usados, por exemplo, em *access points* residenciais e de trabalho. As definições descritas por Paim (2014), apresenta as principais características dos três protolocos WEP, WPA e o WPA2:

- **WEP (*Wired Equivalent Privacy*)**
  Este protocolo é o primeiro em proteção a redes sem fio, tendo sido lançado como um padrão de segurança no ano de 1997. O seu funcionamento é dividido em duas partes, a de autenticação e encriptação/descriptação das mensagens que estão sendo trafegadas na rede. O protocolo baseia na troca de quadros encriptados pelo algoritmo RC4 que utiliza de chaves simétricas, este algoritmo possui duas funcionalidades básicas: a geração de um código que será usado para encriptar e descriptar *(key-scheduling)* conhecida como KSA *(key-scheduling) (onde gera uma permutação pseudo-aleatória do conteúdo de uma chave secreta)* e outra para criptografar a mensagem. O WEP mesmo sendo considerado obsoleto no quesito de segurança continua sendo usado no mundo todo, em residências e empresas, sendo um reflexo da falta de informação dos usuários de redes sem fio e da constante insistência de fabricantes de aparelhos de distribuição de rede sem fio, no qual ainda permitam o uso deste padrão.
- **WPA (*Wi-Fi Protected Access*)**
  O protocolo foi criado em 2002, como postulante substituto do WEP, no seu desenvolvimento foi dado um enfoque no qual buscava correções de falhas presente no seu antecessor. Dentre melhorias propostas, a mais significativa foi o uso do RC4 dentro do protocolo TKIP *(Temporal Key Integrity Protocol)*, no qual é responsável pela

encriptação da mensagem transmitida. O funcionamento do WPA funciona a partir de uma chave secreta contendo entre 32 e 512 bits, no qual gera uma chave mestra dupla PMK *(Pairwise Master Key)*, onde gera uma chave transiente de dupla PTK *(Pairwise Transient Key)*, através de parâmetros obtidos durante a conexão, sendo compartilhada entre o computador e o ponto de acesso. Mesmo sendo um protocolo no qual existem falhas de segurança, ainda é bastante usado em aparelhos de distribuição rede sem fio.

- **WPA-2 (*Wi-Fi Protected Access* II)**
  Em 2004 o protocolo WPA2 foi lançado, após descoberta de falhas de segurança presentes no TKIP, assim tentando resolver o problema ele foi substituído pelo protocolo CCMP, que faz uso do algoritmo de criptografia simétrico AES. O AES é considerado uma cifra de bloco, no qual operam em bloco de tamanho fixo, fazendo uso da mesma chave para cifrar e decifrar. O WPA2 utiliza o AES junto com o TKIP com chave de 256 bits, sendo assim considerada uma ferramenta de criptografia muito segura. Mesmo sendo conhecido como um dos protocolos mais seguros e utilizado em dispositivos de redes sem fio, os pesquisadores Vanhoef et al. (2018) apresentaram vulnerabilidades encontradas no protocolo, dando o nome de *Key Reinstallation Attacks*, que ficou conhecida como KRACK, onde atua na ligação entre a rede sem fio WPA2 e o aparelho que se conecta na rede, a falha encontrada permite que pessoas maliciosas interceptem a rede quando um dispositivo é conectado, alterando a chave de registro que vincula o aparelho e a rede sem fio, obtendo acesso a todo trafego feito no dispositivo, permitindo o roubo de credencias e senhas. Mesmo com a vulnerabilidade encontrada o WPA2 ainda é considerado o protocolo mais seguro a se usar na escolha de proteção em uma rede sem fio.

A Figura 3 apresenta comparações entre os protocolos WEP, WPA e WPA2, a fim de apresentar características existentes em cada protocolos.

2.4 Trabalhos Correlatos

Nesta seção, será apresentada uma visão geral de trabalhos já expostos à comunidade cientifica no qual relaciona estudos sobre o comportamento de usuários em redes sem-fio em locais públicos, utilização de *banners* e experimentos em cenários com redes sem-fio apresentando vulnerabilidades de segurança.

Figueiredo (2017), descreve uma abordagem semelhante ao trabalho aqui proposto. O trabalho realizada por ele tem como objetivo analisar, por meio de teste de penetração

	WEP	WPA	WPA2
The main Purpose	Security is provided in contrast to wired networks	Implementation of major IEEE802.11i standards with WEP without requiring new hardware	Complete IEEE 802.11i standards are implemented with new enhancements of WPA
Data Privacy (Encryption)	Rivest Cipher 4 (RC4)	Temporal Key Integrity Protocol (TKIP)	Authentication is provided through chipper blocks with CCMP and AES.
Authentication	WEP-Open and WEP-Shared	WPA-PSK and WPA-Enterprise	WPA2-Personal and WPA2-enterprise
Data Integrity	CRC-32	Data integrity is provided through Message Integrity Code.	Cipher block chaining message authentication code (CBC-MAC)
Key Management	Key management is not provided	The 4 way handshaking mechanism is used to provide for key management	The 4 way handshaking mechanism is used to provide for key management
Compatibility in terms of Hardware	Possible to deploy on current hardware infrastructure	Possible to deploy on both current and previous hardware	Older Network Interface Cards are not supported. Only the 2006 and newer.
Vulnerability	Vulnerable against Chopchop, Bittau's fragmentation and DoS attacks including variety of DoS attacks.	Vulnerable against Chopchop, Ohigashi-Morii, WPA-PSK, and Dos attacks.	Vulnerable against DoS attacks due to unprotected control frames and MAC spoofing
Deployment in terms of complexity	Easy to deploy and configure		WPA-2 requires complicated setup with WPA enterprise.
Replay attack protection	No protection against replay attacks	Implements sequence counter for replay protection	Implementation of 48-bit datagram/packet number protects against replay attack

Figura 3 – Comparação entre WEP, WPA and WPA2. . Extraída de Sari (2016)

(Pentesting), as vulnerabilidades e ameaças que estão presentes nas redes sem fio das IES (Instituições de Ensino Superior) de Belo Horizonte. Inicialmente, Figueiredo (2017) fez levantamentos, por meio de pesquisas bibliográficas para saber a evolução do padrão de rede IEEE 802.11 e seus mecanismos de segurança e as principais vulnerabilidades presentes na arquitetura.

Figueiredo (2017) realizou testes de penetração em redes sem fio de 12 Instituições de Ensino Superior (IES). A partir dos dados coletados ele identificou que a infra-estrutura das redes sem fio de algumas IES encontram-se vulneráveis e podem estar sujeitas a ataques de usuários maliciosos. A fim de comprovar a possibilidade de capturar pacotes para analisar as vulnerabilidades na rede sem fio, ele fez a instalação do sistema *Red Hat* 9, para fazer a captura de pacotes, porem o modulo original do *kernel* não envia informações sobre os frames de gerenciamento das redes sem fio, assim a fim de contornar o problema ele a utilizou a ferramenta *libpcap*, que é uma interface de programação de aplicativos para capturar o tráfego de rede.

Lacerda (2007) utiliza uma metodologia diferente da exposta por Figueiredo (2017). O trabalho apresentada por Lacerda (2007), tem o objetivo de analisar as principais falhas de segurança da rede sem fio 802.11 e apresentar estratégias de assegurar e defender ameaças e falhas. Em sua pesquisa ele apresenta os padrões atuais das redes sem fio 802.11(b/a/g/i/n), a maneira no qual funciona o endereçamento MAC e os protocolos usados para criptografar e autenticar WEP, WPA, WPA2. Após um levantamento dos

fundamentos Lacerda (2007), apresenta técnicas e ferramentas de ataque:

- Técnicas: *ARP Poisoning*, *MAC Spoofing*, associação maliciosa, vulnerabilidades nos protocolos WEP e WPA.
- Ferramentas: Airtraf, Netstumbler, Kismet, AirJack, Ferramentas para quebra de chaves WEP.

Para elaboração do experimento, Lacerda (2007) pontuou estratégias de defesa a redes sem fio, com uso de *firewalls*, certificados digitais e ferramentas de detecção de ataques e monitoramento. A partir das estratégias pontuadas ele fez a realização de testes experimentais usando equipamentos de distribuição de rede sem fio (roteadores e Access point), no qual foi possível apresentar falhas de segurança em redes sem fio que eram configurados com protocolos vulneráveis (WEP e WPA). Ao termino do trabalho ele apresentou a partir dos experimentos, maneiras de detecção de ataques e monitoramentos como, Garuda, *Kismet*, *Snort-Wirelles* e wIDS, a fim de melhorar a segurança na rede sem fio.

A pesquisa conduzida por Maimon et al. (2014) possui características semelhantes em relação ao trabalho aqui proposto. Os autores desenvolveram experimentos para analisar o comportamento de usuários ao se conectarem a um terminal SSH sem *banner* e com o uso de banner (aviso). Os pesquisadores usaram uma infraestrutura computacional baseada em honeypots para a configuração dos terminais SSH e dos avisos. Os autores analisaram a frequência e duração de uma invasão nos dois casos (SSH com *banner* e sem *banner*). No outro experimento os autores definiram diferentes configurações do sistema de tal maneira que fosse possível avaliar o efeito do *banner* sobre a duração da invasão do sistema. No final dos experimentos foi possível verificar que quando um atacante se depara com o *banner* acaba não efetuando o acesso, diferente do cenário sem *banner* no qual ele persiste com o ataque.

No trabalho apresentado por Sobesto, Cukier e Maimon (2012), é realizado um estudo a fim de avaliar ameaças de ataque a computadores, onde o trabalho tem como base focar em crimes cometidos por atacantes que obtém acesso a um terminal SSH, fazendo a coleta de informações durante um período de 30 dias.

Para a realização do experimento foi um criado um ambiente controlado (*Honeypot*), que tem a função proposital de simular falhas de segurança em um sistema e colher informações sobre o invasor. Dentro do ambiente os computadores criados eram configurados a fim de receber um ataque sendo totalmente exposto, assim após a invasão a um dos computadores esta maquina era monitorada durante 30 dias. Durante este período de tempo foi feito o monitoramento e coleta do trafego de rede e criado um /textit keylogger software cuja finalidade é registrar tudo que é digitado.

A Figura 4, apresenta a implementação do cenário do experimento, desde a criação dos computadores a serem atacados, a captura das informações e acesso a Internet dentro do ambiente.

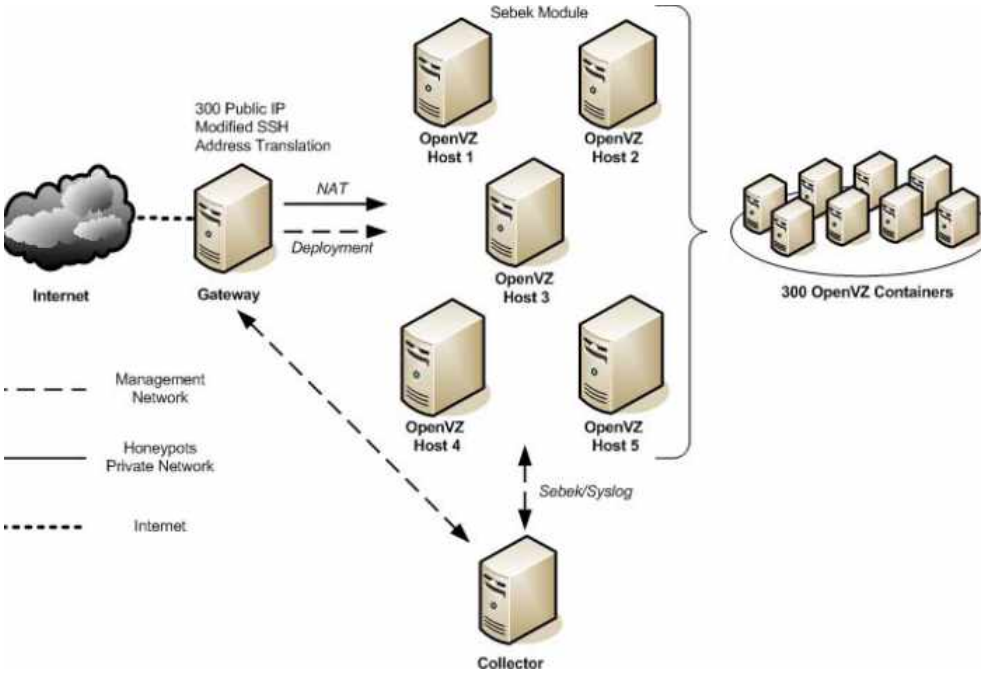

Figura 4 – Ambiente criado para testes de 30 dias. Extraída de (SOBESTO; CUKIER; MAIMON, 2012)

3 Metodologia

O propósito deste capítulo é discutir e apresentar a metodologia utilizada no desenvolvimento do trabalho. Nele será apresentado um entendimento de tópicos como, *Firewall* e *pfSense* a fim de um detalhamento mais técnico mostrando o papel de cada um destes tópicos. Na ultima seção deste capítulo é mostrado a implementação do *pfSense*, de acordo com o que é tratado no trabalho.

3.1 *Firewall*

A definição de *Firewall* apresentado por Nakamura e Geus (2007), descreve que o *Firewall* é um ponto entre duas ou mais redes, onde podem ser um componente ou um conjunto de componentes, no qual passa todo o trafego, permitindo assim o controle, autenticação e registro de todo o trafego. O *Firewall*, não é apenas utilizado para proteção de uma rede privada ou publica não confiável, suas aplicações também podem ser empregadas em um ambiente corporativo para a separação de grupos de trabalho ou sub-redes. Na Figura 5, pode se observar que o *Firewall*, serve como meio de proteção para troca de dados entre as redes, fazendo controle de acesso, registro de trafego e autenticação. Nakamura e Geus (2007), destaca que quando utilizado mais componentes, cada um destes assume uma função que esta ligada diretamente ao nível de segurança da rede em que esta sendo desenvolvido. Para Kurose e Ross (2003), os *Firewalls* podem ser classificados em três categorias, são elas: filtros de pacote, filtros de estado e *gateway*s de aplicação.

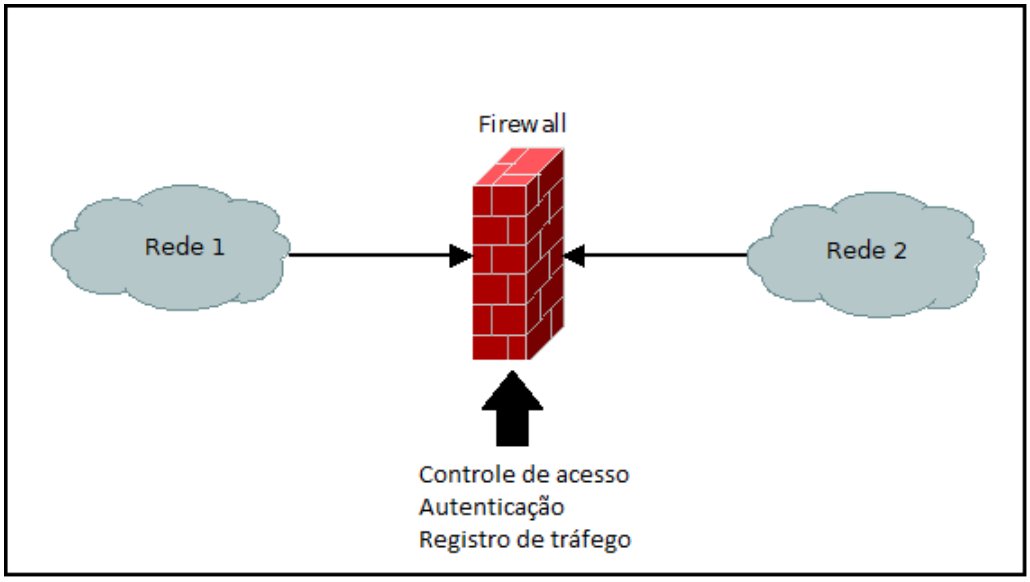

Figura 5 – Estrutura de *Firewall*. Adaptado de Nakamura e Geus (2007)

- Filtro de pacote: cada pacote é verificado individualmente e então sua passagem é verificada a fim de ser negada ou liberada, com base em regras que são especificadas pelo administrador.
- Filtro de estado: este filtro trabalha de forma mais eficiente que o filtro de pacote, onde ele analisa o trafego de dados e verifica se os padrões utilizados estão de acordo com as regras especificadas.
- *Gateway* de aplicação: é um servidor de aplicação, no qual controla todos os dados, tendo vantagens sobre a maneira que permite o trafego direto aos servidores. Quando combinados o *gateway* de aplicação e roteadores de filtragem de pacotes, podem-se obter níveis mais altos de segurança e flexibilidade.

No *Firewall*, cada componente acrescentado possui uma funcionalidade que é ligada diretamente ao nível de segurança da rede. Nakamura e Geus (2007), apresentam as funcionalidades que compõe um *Firewall*, pontuando características de cada componente, são eles: filtros, *proxy*, *bastion hosts*, zona desmilitarizada, *Network Address Translation* (NAT), rede privada virtual, autenticação e balanceamento de carga.

Na seção a seguir será apresentado o sistema (*pfSense*) que implementa boa parte das funcionalidades de um *firewall*.

3.2 *pfSense*

O *pfSense* é um software livre de distribuição do *FreeBSD*, adaptado para ser usado como *firewall* e roteador, no qual possui sua forma de gerenciar via terminal e interface WEB. Dentro de seus recursos como *Firewall* e roteamento, ele também oferece uma grande lista de recursos que podem ser adicionadas e criados a partir da necessidade do usuário. Este projeto do *FreeBSD*, começou no ano de 2004, se diferenciando do projeto *m0n0wall*, por ser um modelo de projeto no qual pode ser instalado completamente em um computador. Neves, Machado e Centenaro (2014) apresenta recursos presentes no *pfSense*:

- *Firewall*
- *DHCP Server and Relay*
- Tabela de estados
- NAT
- *Dynamic DNS* (DNS Dinâmico)

- Alta Disponibilidade
- *Load Balancing* (Balanceamento de carga)
- VPN
- *Reporting e Monitoring* (Relatório e Monitoramento)
- *PPPoE Server*
- *Captive portal*

Entre os recursos apresentados por Neves, Machado e Centenaro (2014), destaca-se o uso de três dentro do projeto, NAT, *captive portal* e captura de pacotes.

O NAT é o mecanismo de tradução de endereços, feito para resolver o problema de pouca oferta de endereços IP. Com isto, o princípio de NAT consiste em usar uma ponte estreita de conexão à Internet, como pode ser vista na Figura 6. Assim, existe pelo menos uma interface de rede conectada à rede interna, e outra interface de rede conectada a Internet com um endereço roteável para poder conectar todos os computadores da rede. Desse modo essa ponte estreita poderá fazer uma tradução de pacotes que são provenientes da rede interna para a externa. O NAT possui dois tipos de tradução: estática e a dinâmica.

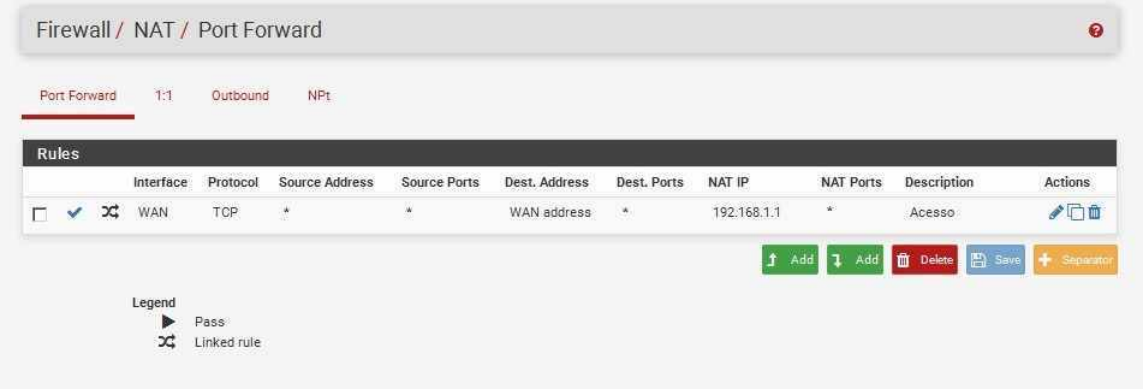

Figura 6 – Recurso NAT do *pfSense*. Imagem retirada da interface WEB do *pfSense*.

NAT estático é a associação de um endereço de IP público a um endereço IP privado interno à rede. Desta forma, o roteador permite que possa associar um IP privado a um IP público roteável na Internet, fazendo a tradução nos dois sentidos, alterando consequentemente o endereço no pacote IP.

Já o NAT dinâmico permite que um endereço IP possa ser compartilhado e concomitantemente encaminhado entre vários computadores sem endereço privado. Desta forma, os computadores da rede interna irão possuir virtualmente, visto de fora, o mesmo endereço IP. Este é o chamado *IP Masquerade*, usado para a tradução do endereço dinâmico, compartilhando os vários endereços IP em um ou mais endereços IP roteáveis.

Nas configurações do NAT no *pfSense*, é possível trabalhar com diversas opcões como *port forward*, 1:1, *outbound*, NPt, etc. Com isso, é possível configurar o NAT de acordo com os requisitos da rede que será criada.

O *captive portal* é um recurso do *pfSense* responsável por gerenciar e controlar o acesso à navegação em redes públicas. Seu funcionamento pode ocorrer de maneiras diferentes, como se conectar a uma rede sem fio ou ser direcionado para a página de acesso da rede. A interface na qual é direcionado sempre solicitará uma autenticação; sendo assim, necessário algum privilégio de acesso a rede ou uma permissão de um administrador da rede. Na Figura 7 é apresentada a topologia da rede quando se é colocado um *captive portal*, mostrando que ao fazer um acesso com o *access point*, é redirecionado para a pagina de autenticação.

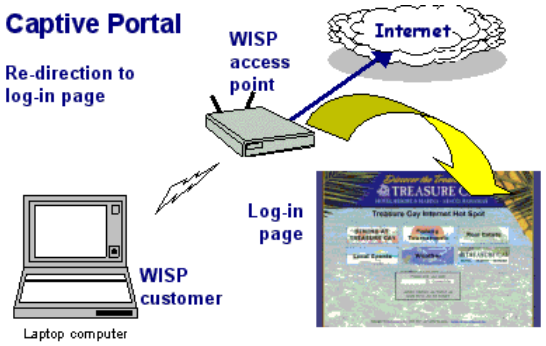

Figura 7 – Topologia de um *captive portal*. Imagem adaptada de Wegner (2016).

O *captive portal* do *pfSense* pode ser configurado para que funcione pela interface WAN ou LAN, dependendo de como foi feito a configuração da aplicação. Dentro de seus recursos é possível configurar páginas de acesso com autenticação de usuários, validação por *vouchers*, ou apenas um redirecionamento sem autenticação.

A captura de pacotes do *pfSense* é uma ferramenta usada para a captura de pacotes da interface desejada dependendo da configuração ou opção de tráfego que deseja obter a captura dos pacotes, seja essa captura pela WAN ou LAN. Com o filtro de captura de pacote é possível filtrar a quantidade de pacotes, porta na qual os pacotes estão trafegando, protocolos da camada de transporte, tamanho do pacote, filtrar entre IPV4 e IPV6. Isto possibilita que o administrador da rede possa verificar se existe algum tipo de pacote que não deveria trafegar na rede, e poder analisar e resolver problemas. A Figura 8, apresenta o recurso dentro do *pfSense* de captura de pacotes (*packet capture*) e a escolha de interface no qual deseja ser feito a captura na WAN ou LAN.

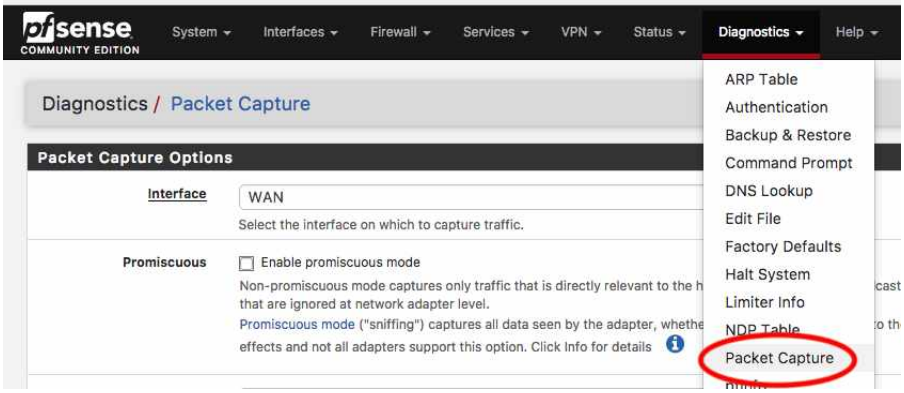

Figura 8 – captura de pacotes do *pfSense*. Imagem retirada da interface WEB do *pfSense*.

3.3 Implantação do *pfSense*

Para implantação do *pfSense*, esta seção aborda os passos da instalação do *pfSense* utilizados na realização deste trabalho. Os dispositivos utilizados para elaboração do trabalho, consistem em, um roteador sem fio da TP-Link e um notebook que se encontra com sistema operacional *Windows* 7. Para a instalação do *pfSense* foi usada a documentação presente no Netgate Forum (FREEBSD/PFSENSE,) no qual apresenta a instalação do produto, hardwares compatíveis e detalhamento de configuração dos recursos presentes no *pfSense*.

A implementação do *pfSense* seguiu os seguintes passos:

- instalação do sistema operacional *Windows* 7 no notebook;
- instalação do software de virtualização *Virtual Box;*
- configuração da maquina a ser criada, levando em consideração as recomendações básicas da documentação do *pfSense* para que possa ser feito a instalação;
- antes da instalação do *pfSense*, foi selecionada uma rede para disponibilizar a Internet (rádio, sem fio ou cabeada), a escolha para o trabalho foi uma rede sem fio;
- a placa de rede da máquina virtual foi configurada como modo bridge;
- após o processo de configurações do recurso da máquina no *Virtual Box* e escolha da rede, o *pfSense* foi instalado;
- foram escolhidas as interfaces de rede em0 e em1, para definição de acordo com a rede na qual será montada;
- no roteador TP-Link, foi configurado o DHCP no qual vai ser operado dentro do equipamento, escolhendo uma faixa de endereços para distribuição;

- com as configurações anteriores realizadas, o *pfSense* foi habilitado via terminal para o uso do modo da interface web, de modo que processos como NAT, *captive portal* e captura de pacotes, possam ser configurados;

- apos a interface web já configurada, é criado um NAT, para que possa ocorrer a comunicação entre a rede interna e externa, uma vez que a rede usada para fornecimento da navegação na Internet é a rede sem fio da UFU, e a rede do *pfSense* é outra distinta;

- próximo passo foi configurar o *captive portal*, colocando a página na qual foi direcionado e qual maneira de autenticação foi feita, seja por usuário, sem autenticação ou *vouchers*;

- com a habilitação do *captive portal* e o NAT, foi habilitado a captura de pacotes no qual pode se escolher em qual interface vai capturar, LAN ou WAN, e que tipo de filtragem deva ser feito;

- ao ter todos os requisitos anteriores já executados, é possível realizar testes e coletas de dados para o trabalho.

4 Desenvolvimento

O objetivo do capítulo é discutir o desenvolvimento do trabalho, detalhando cada etapa realizada. Inicialmente, será apresentado o ambiente de consideração do sistema *pfSense*, como apresentado no capítulo anterior. Posteriormente, serão apresentados os experimentos feitos e desenvolvidos. Também são discutidas algumas análises referentes ao experimento para validação do *pfSense*.

4.1 Ambiente

Para configuração do *pfSense*, foi usado como referências o roteiro de estudos IRAWAN e a documentação freeBSD/pfsense (). Assim para a criação da máquina virtual na qual vai ser instalado o sistema *pfSense* 2.3.5. Para os requisitos mínimos de instalação, é necessária uma máquina com 256 MB de RAM e armazenamento de 1GB. Como é um sistema *FreeBSD*, na instalação usa-se configurações do tipo BSD. Para a máquina virtual criada para o trabalho, foram usados 2GB de memória e um espaço de 20GB de armazenamento.

A escolha de uma rede de acesso para o fornecimento de Internet pode ser por meio de uma rede sem fio ou cabeada, podendo utilizar das próprias redes da Universidade Federal de Uberlândia ou de outro tipo de Internet, como 4G, redes públicas, etc.. Como o foco do trabalho foi desenvolvido dentro de um cenário universitário, foi utilizado dessa maneira, a rede sem fio da universidade.

A placa de rede da máquina precisa estar em modo bridge, de modo que o adaptador faça uma ponte entre a interface “real” do host, conectando-se diretamente a rede deste. Deste modo passa a ter mais um computador na rede do host, obtendo IP dinamicamente, tendo assim uma rede entre host, e todos os equipamentos que se encontram na rede.

Na documentação do *pfSense* freeBSD/pfsense (), existem varias opções no modo de instalação. A escolhida foi o modo *Quick/Easy Install*”, isto é, de maneira fácil e rápida, pois não requer nenhuma personalização ou alteração de configuração. Na opção *Rescue config. xml* recupera as configurações de uma outra instalação, podendo reutilizar cópias de outras máquinas já instaladas.

Com o processo de instalação concluído é necessário configurar as interfaces. Para o trabalho, foi configurado para que a interface WAN (em0) seja a proveniente e que forneça a Internet por meio de uma rede sem fio ou uma rede cabeada. Como demonstrado na Figura 9, a interface LAN (em1) foi configurada de maneira que funcione como a interface

gráfica do *pfSense*, sendo fixado o endereço 192.168.1.1, assim quando colocado o endereço em algum navegador será direcionado para a pagina do *pfSense*.

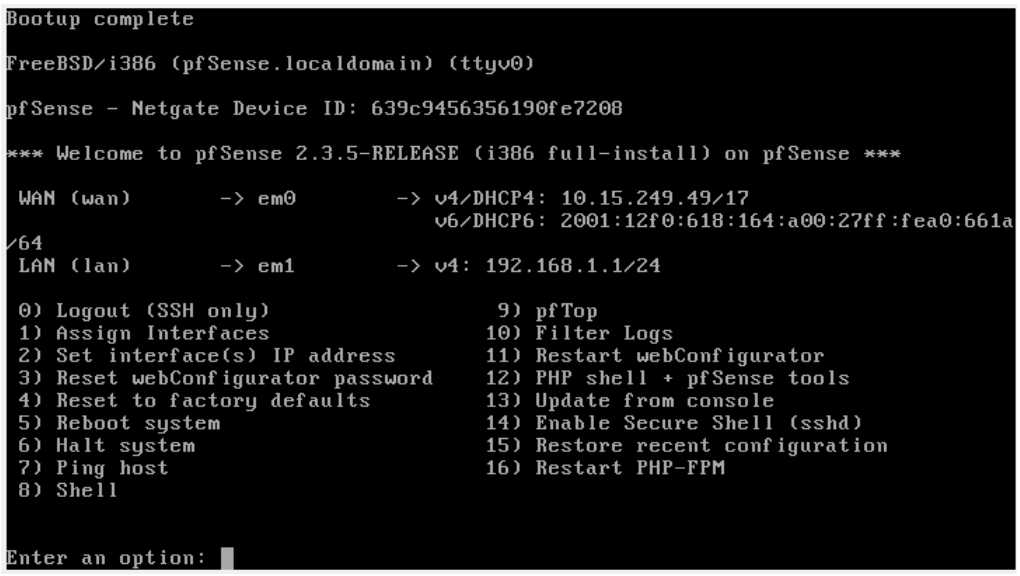

Figura 9 – Configurações WAN e LAN.Imagem retirada no momento da configuração do ambiente do trabalho.

Dentro do ambiente, é necessário um ponto de acesso no qual deve fornecer e distribuir IP's bem como a rede de navegação no qual os usuários poderão se conectar. O equipamento utilizado foi o roteador TP Link Wr940n de 300 mbps, no qual é necessário habilitar o DHCP, uma padronização para ser deixado à classe C para gama de endereços 192.0.0.0, tornando o bloco de endereços como uma rede privada. Foi feito troca de DNS tirando do modo automático no qual vem configurado e colocando o padrão do Google 8.8.8.8 e 8.8.4.4.

Com o *Tabela* instalado, é necessário configurar o modo de interface web no qual é possível se utilizar dos recursos presentes, no que serão importante para o trabalho. Para acessar a interface web, ao iniciar a máquina é necessário informar a LAN da máquina para que seja informado o IP no qual foi usado o mesmo do *gateway* 192.168.1.1.

Uma vez configurada a interface web, é necessário via *browser* (navegador) abrir a interface gráfica do *pfSense* usando o IP configurado, onde se é apresentado a página de acesso como apresentado na Figura 10. Para acessar, é necessário informar usuário e senha, que por padrão é "admin" e "*pfSense*", como descrito na documentação freeBSD/pfsense (), após o primeiro acesso é redirecionado para uma nova pagina que por questão de segurança vai solicitar a redefinição de senha.

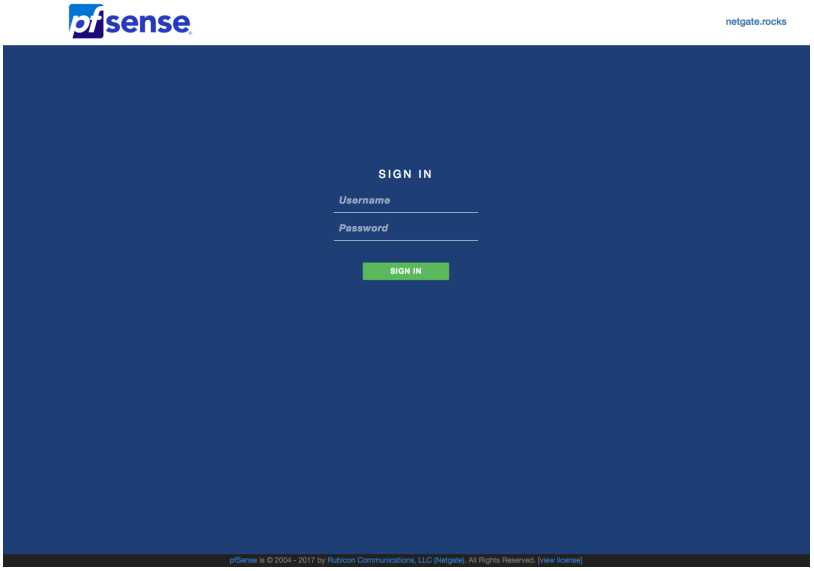

Figura 10 – Login de acesso a interface web do *pfSense*. Imagem retirada do primeiro acesso, no desenvolvimento do trabalho.

Ao iniciar a página web do *pfSense*, deve ser criado uma regra do tipo *Forward*, pois este tipo permite que um administrador controle os pacotes, para que sejam roteados em uma rede, assim como mostrado na Figura 11. Esta rede se encontra na em0 na rede WAN, que se encontra conectado a uma rede sem fio da UFU; assim, vamos direcionar os pacotes na rede.

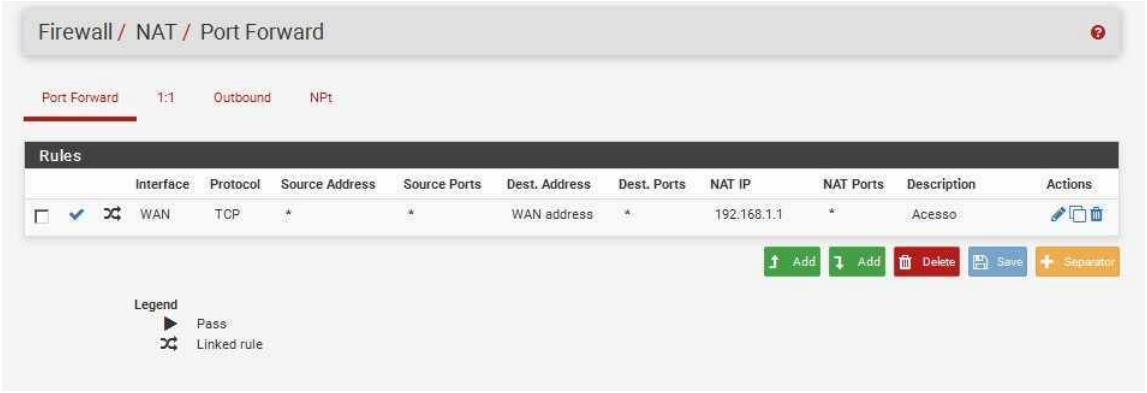

Figura 11 – Recurso *Firewall*/NAT/*Forward* da interface web do *pfSense*.Imagem retirada do antes da criação da regra, no desenvolvimento do trabalho.

A abordagem para a criação do *captive portal* segue modelos relativos aos experimentos de IRAWAN, no qual é feito a criação de uma zona de acesso, para que seja criado uma página web, onde todo acesso a rede será direcionado para este endereço. É possível que esse acesso seja por meio de uma página na qual contenha um login, *vouchers* ou apenas uma página na qual contem algum conteúdo, no qual posteriormente dentro de um período de tempo direcione a pessoa para outra página e a navegação.

No *pfSense* a interceptação dos pacotes pode ser feita de duas maneiras, pelo terminal ou via interface web. No trabalho foi usado o método de captura de pacotes própria do sistema, pois nele é possível escolher qual o tráfego de rede, que deseja monitorar a WAN ou LAN, tipos de protocolos a serem capturados, entre outros recursos. A Figura 13 apresenta como é a interface web do recurso de captura de pacotes, sendo possível escolher qual trafego será monitorado, tipo de protocolo que deseja ser coletado, tipo de porta, entre outras ferramentas dispostas neste recurso.

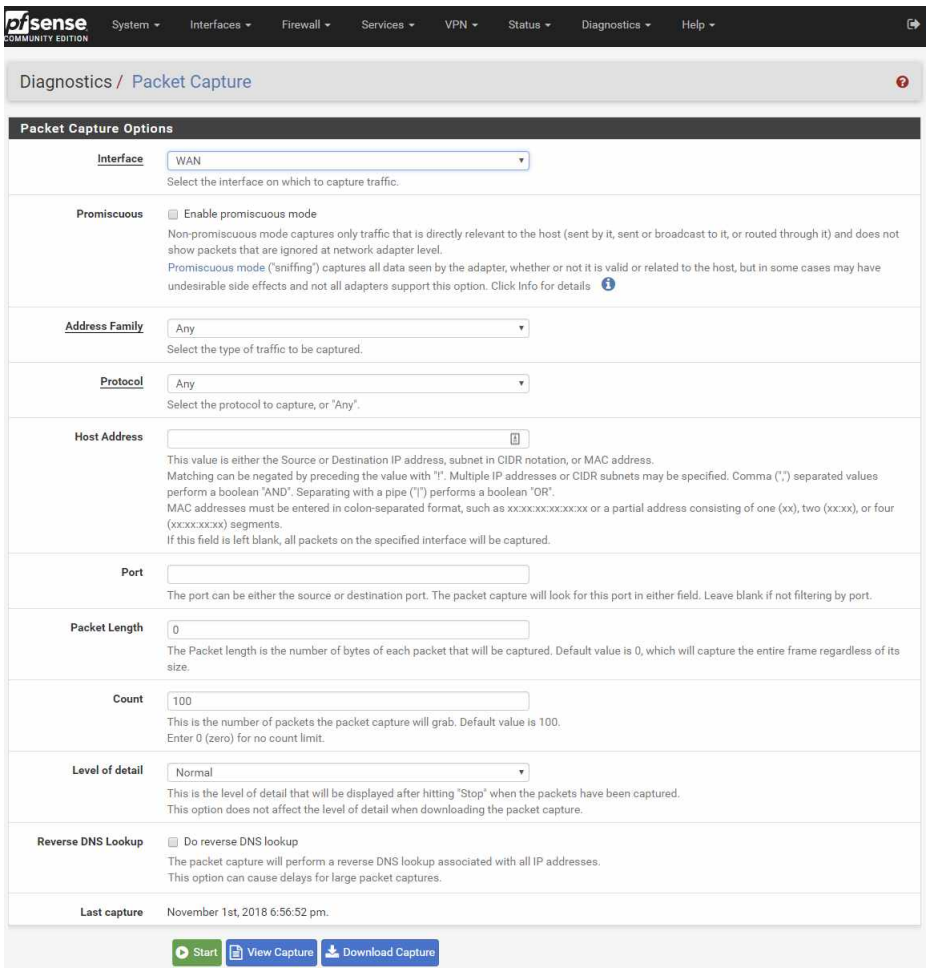

Figura 12 – Recurso de captura de pacotes.Imagem adaptada de freeBSD/pfsense ()

É importante destacar que esta coleta de pacotes só acontece quando ocorre um acesso direto à Internet. Durante a autenticação de acesso, a captura de pacotes não está habilitada. O serviço de captura pode ser encerrado manualmente ou desligando a máquina. Os dados capturados são salvos localmente e o *download* da captura dos pacotes pode ser feito, o que permite uma análise no tráfego da rede.

Nesta seção, foi demonstrado a maneira na qual foi desenvolvido o ambiente da rede e do *pfSense*. O trabalho tem como objetivo analisar a utilização do *pfSense* dentro de redes públicas. Desta forma nas seções seguintes será abordado o experimento realizado a as análises levantadas.

4.2 Vulnerabilidades

Após o levantamento do ambiente e a escolha da proposta a ser apresentada no experimento, foi feito a analise das vulnerabilidades existente dentro da infraestrutura de redes da Universidade Federal de Uberlândia.

Para a classificação das vulnerabilidades foram realizados testes na rede da UFU, os testes foram conduzidos antes da realização do experimento a fim de que fosse possível criar um cenário de experimento no qual explorasse vulnerabilidades na rede da universidade.

O primeiro teste realizado teve como foco o uso da rede sem fio a fim de saber se ao criar uma nova rede sem fio com o uso de um roteador, os *access points* por frequências de canais o bloquearia ou emitiria algum alerta para a controladora alertando uma possível rede sem fio suspeita na rede. Porém ao final do teste foi possível constatar que não é feito nenhum tipo de bloqueio em relação a outras redes sem fios presentes dentro do campus.

Segundo teste visou explorar o uso de redes cabeadas, neste cenário explorou a interrupção da rede em blocos da UFU fazendo um *loop* na própria rede. Com o *loop* criado a rede do bloco ficaria interrompida sendo possível então a criação de uma nova rede, após testes foi verificado que alguns blocos possuem *switchs* no qual possuem o protocolo STP (*Spanning Tree Protocol*), no qual este protocolo permite resolver problemas de loop em redes cuja topologia introduza anéis nas ligações, auxiliando na melhor performance da rede e evitando este tipo de problema. Em blocos nos quais os equipamentos não apresentavam o protocolo STP foi possível a paralisação da rede, até que o problema seja alertado ao administrador da rede.

Ao final dos testes de vulnerabilidade foi possível apontar falhas dentro da rede da Universidade Federal de Uberlândia, falhas como a não detecção de outras redes de frequências diferentes e equipamentos de redes sem protocolos nos quais permite que brechas como loop na rede possam acontecer. A partir destes testes será explorada dentro do experimento a vulnerabilidade na rede sem fio, sendo criada uma nova rede.

4.3 Experimento

Nesta seção, serão apresentados os procedimentos do experimento e quais pontos foram abordados para realizar o trabalho.

Como já abordado em seções anteriores, o foco do trabalho é a utilização do *pfSense* em uma rede de ambiente público. Assim, foi proposta a criação de um ambiente onde seja possível o desenvolvimento de um serviço de rede sem fio no qual seja controlado e configurado a partir do *pfSense*.

O experimento abordado para análise de funcionamento do sistema *pfSense* foi a

elaboração e configuração de uma rede sem fio, fazendo em alguns momentos o uso de um *captive portal* e outras vezes não. O nome dado a esta rede foi “Wi-Fi UFU”, a fim de simular um nome parecido com as redes fornecidas pela universidade. Na rede sem fio criada, foram inseridas mensagens de avisos (*banners*) nas páginas de redirecionamento de navegação (*captive portal*), conforme as Figuras 14 e 15. Como já apresentado em seções anteriores estas páginas são um meio no qual o usuário precisa se identificar para que seja assim liberado o acesso a navegação e feito o redirecionamento de pagina web.

Os *banners* criados nas páginas de autenticação buscam fazer um levantamento sobre o comportamento de usuários em redes sem fio em locais públicos, a fim de poder traçar perfis diferentes de pessoas. A idéia de criação dos *banners* é uma adaptação do trabalho de Maimon et al. (2014), mais neste contexto os *banners* são usados em *captive portal* de redes sem fio. Os avisos colocados nas páginas contêm frases com intuito de poder causar desconfiança as pessoas que tentam se conectar a rede, informando riscos e ameaças nas quais eles podem vir a sofrer caso continue navegando.

A partir do desenvolvimento das mensagens de aviso, foi elaborado um experimento que durou cinco dias no período entre 22/10/2018 à 26/10/2018. Essa data aconteceu o evento "Vem pra UFU"que tem como objetivo apresentar os cursos de graduação da UFU para alunos de ensino médio. A data foi escolhida visto que várias pessoas não vinculadas a Universidade Federal de Uberlândia estariam presentes e posteriormente não utilizariam a rede sem fio fornecida pela universidade, por não possuírem cadastro de acesso.

As experimentações foram subdivididas entre os dias 22 à 26 de outubro de 2018, de acordo com o tipo de rede sem fio que será apresentada ao usuário:

- Dias 22 e 23 de outubro: não foi gerado nenhum *banner* para acesso a rede, o intuito nestes dias era apenas verificar se algum usuário acessaria a rede mesmo que fosse uma desconhecida.
- Nos dias 24 e 25 de outubro: foi inserido um *captive portal* contendo um *banner* (Figura 11), apresentando um alerta sobre a continuação da navegação. O *banner* era apresentado a pessoa que se conectava na rede sem fio e, após 10 segundos, o usuário era direcionado para o site institucional da UFU. O objetivo aqui era avaliar se a pessoas se desconectariam ou não da rede ao ver o aviso.
- Dia 26 de outubro: no último dia do evento foi alterada a página do portal contendo o mesmo aviso, só que para liberar o acesso é necessário dar um check como mostra a Figura 14. Este cenário foi elaborado para analisar se além do aviso, exigir uma interação direta do usuário (concordar com os riscos) influencia no acesso a rede.

Na próxima é apresentado as análises sobre o experimento e feito o levantamento de dados coletados. Também descreve a maneira de como os dados foram analisados.

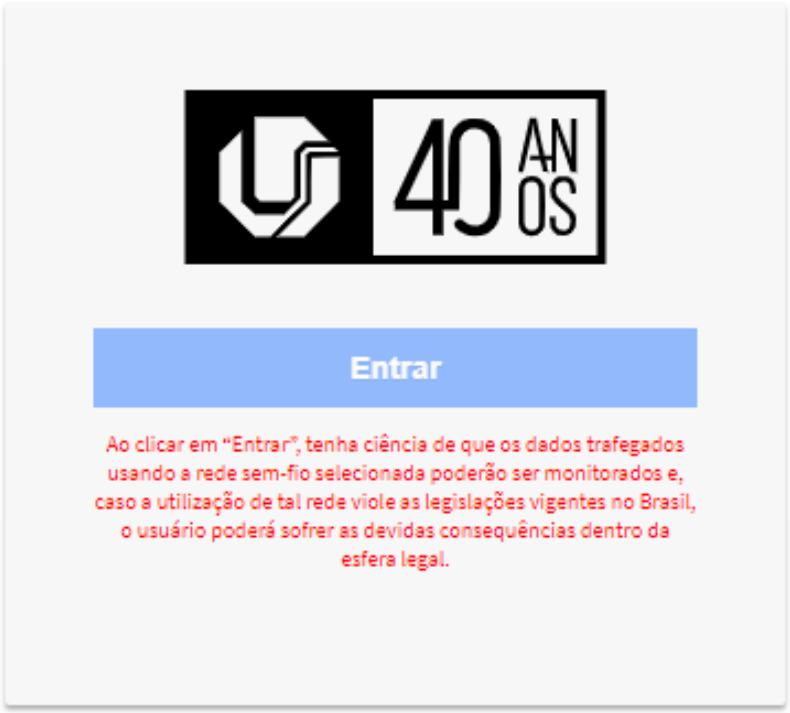

Figura 13 – *Banner* dias 24 e 25. Imagem retirada do experimento do trabalho.

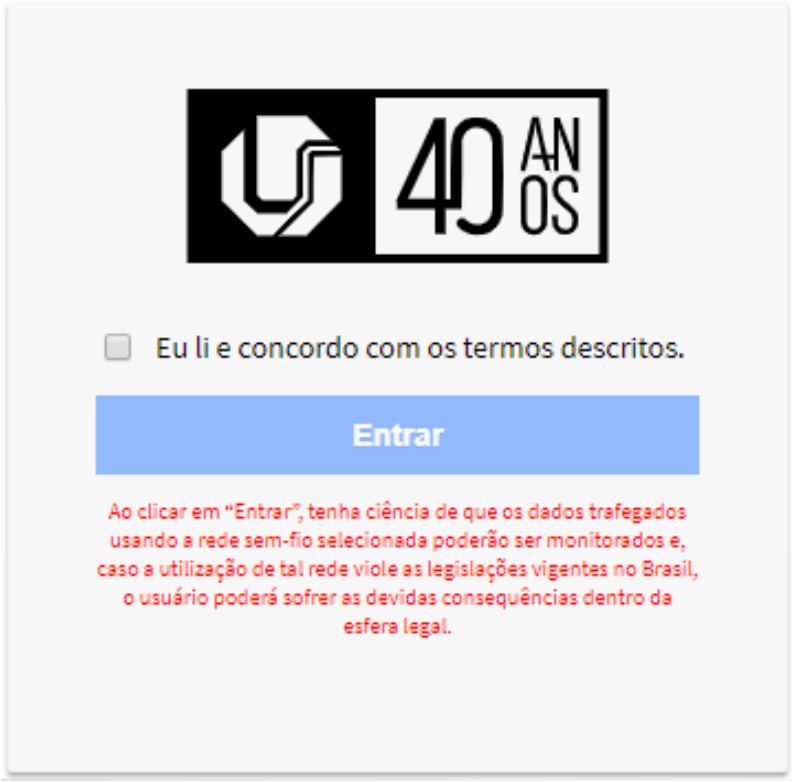

Figura 14 – *Banner* dia 26. Imagem retirada do experimento do trabalho.

4.4 Análises

Durante o período de realização do experimento, foi feito a coleta de dados. As informações dos dados coletados foram obtidos a partir do próprio *pfSense*. Para o recolhimento destes dados, foram utilizadas as ferramentas de captura de pacotes e *System Monitoring*.

A captura de pacotes auxiliou na captura de pacotes do tráfego de rede a fim de analisar as seguintes métricas: i) número de acessos a rede sem fio e ii) tempo médio de navegação no dia. Essa coleta era feita sempre ao fim de cada experimento, juntamente com um relatório de todo trafego gerado pelos usuários da rede sem fio.

Ao término de cada dia, esses dados eram analisados e inseridos em uma Tabela semelhante a Tabela 2, mostrando se o experimento aconteceu com ou sem portal de acesso e a quantidade de acessos. Para análise do tempo médio de navegação, foi feito em cada dia uma média do tempo de todos os pacotes trafegados na rede, não levando em consideração a variação de tempo que cada usuário utilizou de navegação. Na Tabela 3 apresenta-se os resultados obtidos.

Para uma análise gráfica, foi utilizado o System Monitoring, ferramenta na qual é utilizada para mostrar um gráfico interativo, apresentando dados diários da rede sem fio, como dados processos, utilização do sistema, tempo de interrupção na navegação, entre outros. Nas Figuras 15, 16, 17 e 18, é possível verificar usuários utilizando o sistema, picos de interrupção, a utilização de sistema *pfSense* e os processos gastos.

Tabela 2 – Tabela de Acessos

Dia	*Banner*	Quantidade de acessos
22-10	Sem *Banner*	4
23-10	Sem *Banner*	3
24-10	*Banner* 1	4
25-10	*Banner* 1	3
26-10	*Banner* 2	2
-	Total Acesso:	16

A primeira análise a se apresentar em relação ao uso do *pfSense* é como uma infraestrutura que possibilita a criação e gerenciamento de uma rede sem fio. É possível afirmar que o *pfSense* conseguiu atender os requisitos estabelecidos no trabalho. Comparando com outros sistemas semelhantes como por exemplo *OPNsense*, *NG Firewall* e *ClearOS*, foi possível notar que o *pfSense* se sobressai em relação a eles devido a presença de recursos como *captive portal*, NAT e coleta de trafego nativa. Um dos principais obstáculos com o *pfSense* foi a incompatibilidade com softwares de virtualização (*Hyper-V* e *VMLite-Workstation*) para instalação de um sistema *freeBSD*.

Tabela 3 – Tabela tempo médio de navegação

Dia	*Banner*	Tempo Médio
22/10	Sem *Banner*	14 minutos.
23/10	Sem *Banner*	21 minutos.
24/10	*Banner* 1	18 minutos.
25/10	*Banner* 1	7 minuots.
26/10	*Banner* 2	12 minutos.
	Media total:	14 minutos.

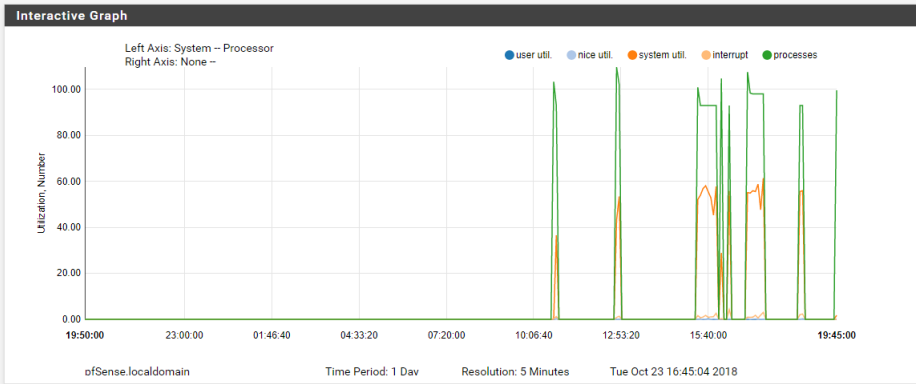

Figura 15 – Utilização de recursos do Pfsense nos dias 22 e 23 de Outubro.

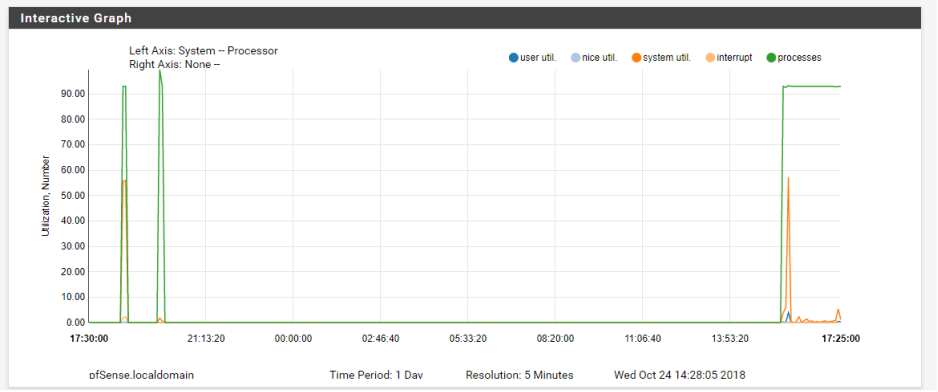

Figura 16 – Utilização de recursos do Pfsense no dia 24 de Outubro.

Sobre o experimento, o objetivo principal era somente validar o ambiente computacional proposto. Um objetivo secundário seria discutir o impacto de diferentes tipos de aviso no comportamento dos usuários de redes sem fio públicas. O baixo número de usuários que se conectaram no *rogue AP* durante o experimento impede que qualquer conclusão, do ponto de vista estatístico, seja formada. Os resultados mostram que outras áreas da universidade devem ser exploradas para a instalação do *rogue AP* assim como a duração do experimento, que deve ser prolongada. O ambiente computacional e as configurações propostas neste trabalho permitem que novos experimentos sejam executados para investigar com maior nível de profundidade o comportamento de usuários em redes

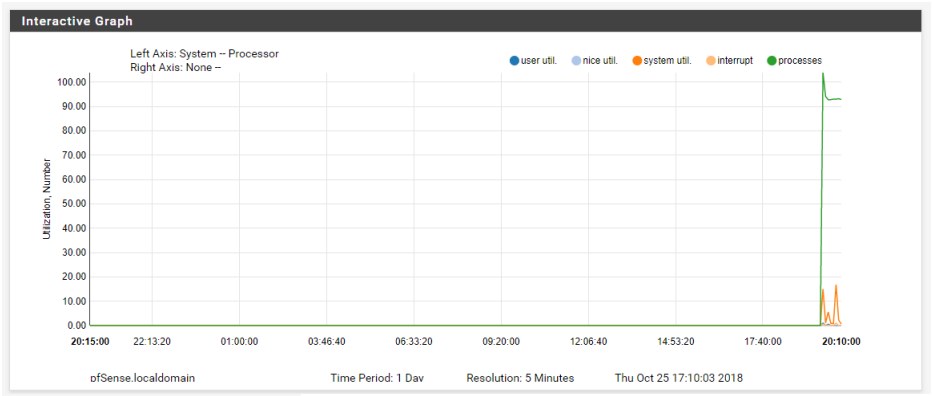

Figura 17 – Utilização de recursos do Pfsense no dia 25 de Outubro.

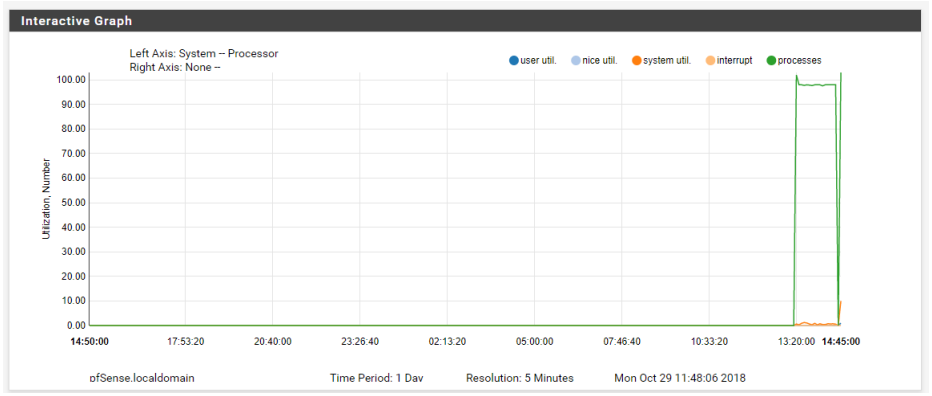

Figura 18 – Utilização de recursos do Pfsense no dia 26 de Outubro.

sem fio públicas.

5 Conclusão

As ferramentas para segurança de redes se tornam indispensáveis para evitar, ataques maliciosos. Este trabalho apresentou uma analise detalhada do funcionamento do *pfSense* e seus recursos disponíveis, a fim de gerir uma rede sem fio.

Neste contexto, a fim de se demonstrar o objetivo do trabalho, foi elaborado um ambiente experimental descrito na seção 4.2. Tal ambiente ilustra o funcionamento do *pfSense* e mostra como usar seus recursos para analisar comportamentos de usuários perante redes sem fio desconhecidas em ambientes públicos.

A análise a se fazer em relação ao tema proposto no trabalho, leva a enfatizar que o *pfSense* é um sistema de *Firewall* gratuito que fornece diversos recursos para o desenvolvimento e o gerenciamento de uma rede sem fio. Ferramentas como NAT, *captive portal* e captura de pacotes fornecem a base para o desenvolvimento de trabalhos experimentais sobre o comportamento de usuários de redes sem fio públicas.

Em um trabalho futuro, espera-se ampliar o experimento descrito neste trabalho - aumentar o número de APs e a duração, conduzirem novos experimentos (variar o nome da rede e as taxas de download/upload) e investigar novas métricas como o tipo de tráfego gerado pelo usuário. Outro ponto a se discutir em um trabalho futuro é apresentar maneiras de prevenções contra ataques de *cybercriminosos*, trazendo técnicas de defesa e apresentando informações a usuários para que não seja vitimas de ataques de *cybercriminosos*.

Referências

ABNT, A. B. D. N. T. A. N. I. *Tecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação*. [s.n.], 2005. ISBN 9788507006480. Disponível em: <https://books.google.com.br/books?id=Hl4DaAEACAAJ>. Citado na página 15.

DANTAS, M. L. Segurança da informação: uma abordagem focada em gestão de riscos. *Recife: Livro Rápido-Elógica*, 2011. Citado na página 16.

FIGUEIREDO, D. A. Análise de vulnerabilidades e ameaças presentes em redes wi-fi (ieee 802.11) de instituições de ensino superior de minas gerais. *Projetos e Dissertações em Sistemas de Informação e Gestão do Conhecimento*, v. 5, n. 2, 2017. Citado 2 vezes nas páginas 18 e 19.

FREEBSD/PFSENSE. *pfSense Documentation*. Disponível em: <https://docs.netgate.com/pfsense/en/latest/general/index.html>. Acesso em: jan. 2019. Citado 5 vezes nas páginas 6, 26, 28, 29 e 31.

IRAWAN, D. Mempercepat koneksi akses internet dengan membangun lusca proxy server menggunakan linux pfsense pada universitas muhammadiyah metro. *Jurnal Informatika*, v. 12, n. 2, p. 190–197, 2014. Citado 2 vezes nas páginas 28 e 30.

KUROSE, J.; ROSS, K. *Redes de computadores e a Internet: uma nova abordagem*. PEARSON BRASIL, 2003. ISBN 9788588639102. Disponível em: <https://books.google.com.br/books?id=AJc8AgAACAAJ>. Citado 4 vezes nas páginas 6, 13, 14 e 22.

LACERDA, P. d. S. Análise de segurança em redes wireless 802.11 x. *Universidade Federal de Juiz de Fora*, v. 49, 2007. Citado 2 vezes nas páginas 19 e 20.

MAIMON, D. et al. Restrictive deterrent effects of a warning banner in an attacked computer system. *Criminology*, Wiley Online Library, v. 52, n. 1, p. 33–59, 2014. Citado 2 vezes nas páginas 20 e 33.

MARCIANO, J. L. P. Segurança da informação: uma abordagem social. 2006. Citado na página 15.

MENDES, D. R. Redes de computadores. *Editora Novatec*, 2007. Citado na página 14.

NAKAMURA, E.; GEUS, P. de. *Segurança de Redes em Ambientes Cooperativos*. Novatec, 2007. ISBN 9788575221365. Disponível em: <https://books.google.com.br/books?id=AamSIJuLc34C>. Citado 3 vezes nas páginas 6, 22 e 23.

NEVES, F. C. d.; MACHADO, L. A.; CENTENARO, R. d. F. *Implantação de Firewall PfSense*. Dissertação (B.S. thesis) — Universidade Tecnológica Federal do Paraná, 2014. Citado 2 vezes nas páginas 23 e 24.

PAIM, R. R. Wep, wpa e eap. *Acesso em Março de*, 2014. Citado na página 17.

PASQUALINI, A. L.; MARCONDES, C. A. C. Estudo do crescimento das redes wireless 802.11–2.4 ghz em ambiente urbano–caso rio claro-sp. *Revista TIS*, v. 1, n. 2, 2012. Citado na página 10.

RUFINO, N. de O. *Segurança em Redes sem Fio – 4ª edição: Aprenda a proteger suas informações em ambientes Wi-Fi e Bluetooth*. NOVATEC, 2015. ISBN 9788575224137. Disponível em: <https://books.google.com.br/books?id=_zsaBgAAQBAJ>. Citado na página 10.

SARI, A. Comparison between wep, wpa and wpa2. 2016. Citado 2 vezes nas páginas 6 e 19.

SOBESTO, B.; CUKIER, M.; MAIMON, D. Are computer focused crimes impacted by system configurations? an empirical study. In: IEEE. *Software Reliability Engineering (ISSRE), 2012 IEEE 23rd International Symposium on*. [S.l.], 2012. p. 191–200. Citado 3 vezes nas páginas 6, 20 e 21.

TANENBAUM, A. *Redes de computadores*. CAMPUS - RJ, 2003. ISBN 9788535211856. Disponível em: <https://books.google.com.br/books?id=0tjB8FbV590C>. Citado na página 15.

VANHOEF, M. et al. Operating channel validation: Preventing multi-channel man-in-the-middle attacks against protected wi-fi networks. In: ACM. *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*. [S.l.], 2018. p. 34–39. Citado na página 18.

VIEIRA, L. *TIPOS DE ATAQUE WIRELESS*. 2016. Disponível em: <https://www.contractti.com.br/tipos-de-ataque-wireless/>. Citado na página 10.

WEGNER, P. Why is a captive portal important for wireless guest access? 2016. Citado 2 vezes nas páginas 6 e 25.