FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA
Curso Técnico em Redes de Computadores
Parecer SEC/CEED 487/2014
Rua Dr. Flores 396 - Centro - POA/RS

RELATÓRIO FINAL DE ESTÁGIO

FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA: IMPLANTAÇÃO DE CONTROLE DE ACESSO À REDE WIRELESS UTILIZANDO O LOGIN DO FACEBOOK COMO MÉTODO DE AUTENTICAÇÃO

GÉRSON DOS SANTOS TORRES

Porto Alegre / RS
Fevereiro / 2020

FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA
Curso Técnico em Redes de Computadores
Parecer SEC/CEED 487/2014
Rua Dr. Flores 396 - Centro - POA/RS

GÉRSON DOS SANTOS TORRES

FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA: IMPLANTAÇÃO DE CONTROLE DE ACESSO À REDE WIRELESS UTILIZANDO O LOGIN DO FACEBOOK COMO MÉTODO DE AUTENTICAÇÃO

Relatório de Estágio Curricular apresentado à disciplina Estágio Supervisionado do Curso Técnico em Redes de Computadores da Faculdade e Escola Técnica Alcides Maya, como requisito parcial para obtenção do título de Técnico em Redes de Computadores.

Orientador: João Padilha Moreira
Direção da Escola Alcides Maya: Devanir Oss Emer Eizerik
Empresa: Faculdade e Escola Técnica Alcides Maya
Período: 12/09/2018 a 31/07/2019

Porto Alegre / RS
Fevereiro / 2020

T693f TORRES, Gérson dos Santos

FACULDADE E ESCOLA TÉCNICA ALCIDES MAYA: IMPLANTAÇÃO DE CONTROLE DE ACESSO À REDE WIRELESS UTILIZANDO O LOGIN DO FACEBOOK COMO MÉTODO DEAUTENTICAÇÃO / Gérson dos Santos Torres. – Porto Alegre, 2020. 39 f. : il

Orientador: João Padilha Moreira.
Trabalho de Conclusão de Curso Técnico (Técnico em Redes de Computadores) -- Faculdade e Escola Técnica Alcides Maya, 2020.

1. Redes de Computadores. 2. Redes Wireless. 3. Controle de Acesso à Internet. 4. Login Social. I.Moreira, João Padilha. II. Título.

CDD 004.678
CDU 004.738

Ficha Catalográfica elaborada e modificada pelo autor por meio do
Sistema de Geração Automática de Ficha Catalográfica da UFBA.

APROVAÇÃO

_____

Direção Geral da Escola Alcides Maya

_____

João Padilha Moreira - Orientador Estágio

_____

Gérson dos Santos Torres - Estagiário

Aos professores deste país que não valoriza a educação.
Corrigindo.
Aos professores deste país, aos que merecem.

AGRADECIMENTO

Acredito que este seja o pior dos tópicos de um Trabalho de Conclusão, não pela falta das pessoas a quem devamos ser gratos, mas o contrário, ao término desta etapa muitas são as pessoas a quem agradecer.

Amigos, colegas, professores, familiares são tantas as pessoas que pode ser difícil enumerá-las, muitos são os merecem, entretanto alguns podem acabar nem sendo lembrados, afinal foram quase dois anos.

Sendo assim, peço desculpa por optar em não fazer esta lista. Sei que todos entenderão, mesmo assim quero que saibam que sou muito grato, por toda ajuda que me foi dada ao logo desta jornada.

Concomitantemente, gostaria de agradecer a uma pessoa em especial, pois sem ela está jornada poderia nem mesmo ter começado. Alguém a quem devo todos os agradecimentos, por todo apoio, incentivo, compreensão não somente neste período, mas ao logo dos anos.

Às vezes na vida acabamos não agradecendo às pessoas que nos cercam e nos ajudam em todas as horas, seja nos momentos fáceis ou nos difíceis.

Todavia, é preciso reconhecer que nem sempre conseguiríamos chegar aonde queremos sem estas pessoas.

Sendo assim, gostaria de agradecer a está pessoa. Gostaria de agradecer a minha IRMÃ.

“Bear in mind that the wonderful things you learn in your schools are the work of many generations... All this is put into your hands as your inheritance in order that you may receive it, honour it, add to it, and one day faithfully hand it on to your children.”
(Albert Einstein)

LISTA DE ABREVIATURAS E SIGLAS

API	Application Programming Interface
BOOTP	Bootstrap Protocol
CA	Certificate authority
CIDR	Classless Inter-Domain Routing
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
IEEE	Institute of Electrical and Electronics Engineers
ID	Identity
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
LAN	Local Area Network
SGCE	Sistema de Gestão de Certificados Eletrônicos
SSID	Service Set Identifier
SSL	Secure Sockets Layer
VPN	Virtual Private Network
WAN	Wide Area Network
WMM	Wi-Fi Multimedia
WPS	Wi-Fi Protected Setup

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

Este Trabalho de Conclusão de Curso tem como objetivo apresentar uma melhoria a Faculdade e Escola Técnica Alcides Maya, assim como descrever as atividades desenvolvidas ao longo do estágio curricular obrigatório realizado nesta mesma instituição.

Nos últimos anos houve um crescimento significativo de pessoas com acesso à Internet tanto no mundo como no Brasil. Entretanto, uma maior demanda representa também um aumento dos problemas de segurança.

E a aprovação do Marco Civil da Internet, trouxe a obrigação de manter os registros de acesso à Internet, por um determinado tempo.

Uma alternativa para cumprir com esta nova obrigação é a utilização do login social para controlar o acesso à Internet.

Sendo assim, através de um laboratório foi realizada uma simulação demonstrando a implementação de uma solução utilizando o login do Facebook como controle de acesso a rede wireless para esta instituição de ensino.

2 DADOS DE IDENTIFICAÇÃO DA EMPRESA

Criada no Ano de 1967 a Escola Alcides Maya começou apenas como um Curso de Alfabetização de Jovens e Adultos.

Ao longo dos anos devido a sua qualidade de ensino e seu crescimento foi lançado o primeiro Curso Técnico da Instituição, mantendo a excelência de ensino que tornaria a marca Alcides Maya referência em cursos na Área de Informática.

Com o advento dos anos 2000 a até então Escola Técnica Alcides Maya tornou-se a Faculdade e Escola Técnica Alcides Maya, oferecendo à comunidade além dos tradicionais cursos Técnicos os cursos de Graduação na Área de Informática com a mesma qualidade que sempre selou por oferecer.

Sua Identidade Organizacional, definida através do tripé Missão, Visão e Valores Organizacionais, podem ser vistos como o norte desta Instituição.

Sua MISSÃO:

Promover conhecimento, inovação, formação acadêmica e desenvolvimento profissional em atividades de ensino, extensão e pesquisa na área de Tecnologia da Informação.

Sua VISÃO:

Até 2020, ser reconhecida pela comunidade e pelo mercado de trabalho como instituição de referência em qualidade de ensino, inovação, sustentabilidade e formação profissional na área de Tecnologia da Informação.

Seus VALORES ORGANIZACIONAIS:

Ética: buscar sempre a verdade, a transparência e o senso de justiça.

Responsabilidade: incentivar a responsabilidade no exercício dos direitos e no cumprimento das obrigações.

Solidariedade: estabelecer princípios de dedicação e comprometimento, priorizando a cooperação.

Sustentabilidade: garantir a formação integral do educando, a docência competente e moderna, buscar a infra-estrutura apropriada e a inovação para alcançar o crescimento sustentado e garantir o futuro da instituição.

Dialogicidade: oferecer educação como prática de liberdade, gerar ciclos de novas possibilidades de desenvolvimento acadêmico e profissional bem como promover a empregabilidade, crescimento pessoal e institucional.

Cidadania: incentivar a consciência social e a responsabilidade pessoal a serviço da comunidade.

Desta forma, representando tudo o que esta Escola acredita, zela e almeja.

3 REFERENCIAL TEÓRICO

A disponibilização de pontos de acesso wireless para clientes aumentou consideravelmente nos últimos anos. Novos dispositivos têm ganhado função wireless e assim cada vez mais os clientes buscam lugares onde há o serviço de wi-fi gratuito, fazendo com que lojas, restaurantes, escolas e outros tipos de empresas invistam em hotspots[1] como um atrativo.

> ...hotspots podem ser utilizados como hospitalidade enquanto propõem a oferta de pontos de conexão, sejam diretos, onde um cliente contrata um serviço e tem acesso a conexão por pontos pré-definidos, ou no caso da distribuição da conexão gratuitamente por estabelecimentos específicos que firmam parcerias ou arcam com as despesas de maneira a oferecer diferenciais para seus clientes...(ROCHA, 2016, p.6)

Conforme Tanenbaum e Wetherall (2011), pontos de acesso wireless assim como outros dispositivos tendem a utilizar o padrão IEEE 802.11 para se conectarem.

Este padrão começou a ser definido em 1990 pelo “Institute of Electrical and Electronics Engineers” (IEEE), e a partir de então sofreu modificações gerando outros padrões baseados nele, como por exemplo: 802.11b, 802.11g e 802.11n que são os mais encontrados em aparelhos atualmente.

Para que cada equipamento seja localizado em uma rede, seja esta uma rede local ou até mesmo na Internet, é necessário um endereço que o identifique, para que isso ocorra um número é atribuído a este equipamento, sendo chamado de IP. Conforme Tanenbaum e Wetherall (2011), o endereço “Internet Protocol” (IP) é um número de 32 bits, capaz de identificar o equipamento de forma única.

Além do IP é necessária uma máscara de sub-rede que também possui 32 bits, este número associado ao IP consegue fornecer duas informações: qual é a rede e qual é o host[2].

Este endereço segue algumas regras. Segundo Kurose e Ross (2013), atualmente existem dois Protocolos de Internet o IPV4 e o IPV6 sendo que o primeiro ainda é o mais usado atualmente.

Para realizar a atribuição de endereços IP antigamente utilizava-se o protocolo “Bootstrap Protocol” (BOOTP) que distribuía de forma manual, ou seja,

[1] Hotspot é um determinado local onde uma rede sem fio está disponível.
[2] Host é definido como qualquer equipamento dentro de uma rede.

estática os endereços de IP. Desenvolveu-se então protocolo “Dynamic Host Configuration Protocol” (DHCP) baseado no BOOTP para que fosse capaz de fazer esta distribuição tanto de forma dinâmica, como estática utilizando o BOOTP.

“O Dynamic Host Configuration Protocol (DHCP) por sua vez, é o protocolo que provê um meio para alocar estes endereços dinamicamente.” (PEDROZO, 2014, p.32).

Quando o equipamento é iniciado e não possui um IP ele envia um pacote chamado DHCP DISCOVER para o IP de broadcast[3] quando este pacote chegar ao servidor DHCP será atribuído um IP e será enviado um pacote DHCP OFFER para o host com o IP correspondente e outras configurações necessárias para a comunicação.

Em redes domésticas ou de pequeno porte, na maioria dos casos o próprio roteador se encarrega de fazer o papel do servidor DHCP. Contudo, é comum que empresas que possuam uma rede maior utilizem um servidor para realizar esta função, normalmente rodando uma distribuição Linux ou o Windows Server, mas em alguns casos a empresa pode optar por um firewall como o pfSense, que além de atuar como um servidor DHCP, pode fornecer inúmeras outras funções de segurança.

A segurança de uma rede quando a conectamos à Internet é uma grande preocupação, não apenas de grandes empresas. Quando conectada à Internet, o equipamento responsável por interligar as redes também se torna uma porta de entrada para crackers e diversos tipos de pragas digitais como: malwares, trojans, spywares, keyloggers, ransomwares entre outros. Uma das formas de reduzir estas vulnerabilidades causadas pela conectividade é a utilização de antivírus e firewalls.

> “Os firewalls são apenas uma adaptação moderna de uma antiga forma de segurança medieval: cavar um fosso profundo em torno do castelo. Esse recurso forçava todos aqueles que quisessem entrar ou sair do castelo a passar por uma única ponte levadiça, onde poderiam ser revistados por guardas.” (TANENBAUM e WETHERALL, 2011, p.513).

[3] Broadcast é o último endereço de uma rede, sendo utilizado para enviar dados a todos os equipamentos da rede.

Segundo Kurose e Ross (2013), os firewalls são responsáveis por monitorar o tráfego das comunicações entre redes, para poder informar qualquer atividade suspeita.

Através de um firewall, podemos criar regras de acesso que aumentem a segurança da rede. Pode-se, por exemplo: impedir que usuários tenham acesso a sites potencialmente perigosos ou que usuários através da Internet consigam acessar uma rede interna.

Um dos mais utilizado é o pfSense, que é um sistema operacional destinado a ser um firewall e um roteador, criado em 2004 por Chris Buechler e Scott Ullrich é baseado no FreeBSD e desenvolvido pela Netgate. Além de ser um firewall e roteador, possui muitos outros recursos como: servidor DHCP, VPN, Proxy, controle de acesso via Captive Portal entre outros, com a vantagem de poder ser gerenciado através de uma interface Web.

O pfSense pode ser utilizado para realizar a liberação de acesso através do Captive Portal, que é uma ferramenta de gerenciamento de acesso, assim o pfSense é capaz de autorizar o acesso à Internet apenas a determinados usuários.

> “Um captive portal é comumente utilizado como uma camada adicional de segurança nas redes sem fio corporativas para acesso à Internet. O captive portal permite forçar a autenticação, ou seja, quando um usuário se conecta a rede sem fio e tenta abrir uma página Web, o captive portal intercepta a tentativa de acesso e, direciona o usuário para uma tela de autenticação, o acesso à Internet só será liberado se o usuário possuir login e senha válidos.” (FRANCO, 2015, p.27).

A autenticação em uma rede pode ser feita mediante alguns métodos: cadastro de usuários, vouchers, utilizando o login de alguma rede social entre outros. Sendo que, a autenticação por uma rede social traz a vantagem de não necessitar cadastro prévio de usuários por parte do administrador do ponto de acesso. Em uma rede social “...o fluxo de informações é controlado pelos relacionamentos que as pessoas declaram umas às outras.” (TANENBAUM e WETHERALL, 2011, p.5).

A escolha da rede social a ser utilizada, deve ser feita com base no alcance que ela tem. Utilizar o Facebook como método de autenticação é uma das melhores, senão a melhor opção, pois atualmente quase 1/3 (um terço) da

população mundial faz parte, e aproximadamente 60% (sessenta por cento) da população brasileira a utiliza[4].

Contudo, mesmo após a autenticação e liberação de acesso para que possamos acessar uma página da Internet outro protocolo é de extrema importância. Cada vez que acessamos um site não digitamos seu endereço de IP, seria algo muito difícil ter que decorar dezenas de endereços de IP para podermos acessar sites do dia a dia. É neste momento que o Protocolo “Domain Name System” (DNS) é utilizado, pois ele é capaz de, partindo de um nome de domínio ser capaz de determinar o endereço de IP correspondente.

Cada vez que digitamos um domínio é enviada uma solicitação ao servidor DNS e este retorna com o respectivo endereço de IP e o navegador localiza e exibe a página solicitada.

A falta de um sistema de controle de acesso pode acabar se tornando um grande inconveniente às empresas que oferecem wi-fi. A evolução da Internet fez necessária a criação de regras claras sobre a sua utilização, sendo assim diversos governos criaram leis sobre o assunto, como é o caso do Brasil que aprovou o chamado de Marco Civil da Internet, a Lei Nº 12.965 estabelece que:

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. (BRASIL, 2014)

Segundo Filho (2005), juridicamente podemos dizer que um provedor de acesso é aquele que faz a ligação entre o usuário e à Internet, utilizando-se de equipamentos e programas responsáveis pela execução do “Internet Protocol”.

Assim podemos considerar qualquer pessoa, seja física ou jurídica que forneça acesso à Internet para os clientes ou não clientes, de forma gratuita ou não como sendo um provedor de acesso, estando então sujeito ao Artigo 13 da Lei supracitada.

Tendo em vista a exigências da guarda de registros, torna-se necessário a adequação dos pontos de acesso. Por este motivo, sugiro o controle de acesso através da utilização de um roteador wireless ligado ao firewall pfSense, utilizando o Captive Portal e tendo como método de autenticação o login no Facebook. Para que assim seja possível a geração dos registros de acesso à rede.

---

[4]Disponível em: <https://canaltech.com.br/redes-sociais/facebook-chega-a-127-milhoes-de-usuarios-mensais-no-brasil-118358/>. Acesso em: 15 dez. 2019.

4 ATIVIDADES DE ESTÁGIO

Durante o período de estágio, foram desenvolvidas atividades de manutenção preventiva e corretiva nos computadores dos laboratórios, entre outras.

Dentre as manutenções preventivas podem-se destacar: atualização do Sistema Operacional assim como dos softwares utilizados nas aulas, checagem de cabos.

No campo de manutenção corretiva podemos destacar: substituição de HDs, reinstalação de Sistema Operacional e programas, clonagem de HDs, substituição de baterias, substituição e limpeza de fontes, crimpagem de cabos de rede, configuração de roteadores wireless, auxilio na implantação do Sistema de Gestão de Certificados Eletrônicos (SGCE), auxilio na criação de usuários, criação de disciplinas e respectiva inscrição de alunos na Plataforma Sagah.

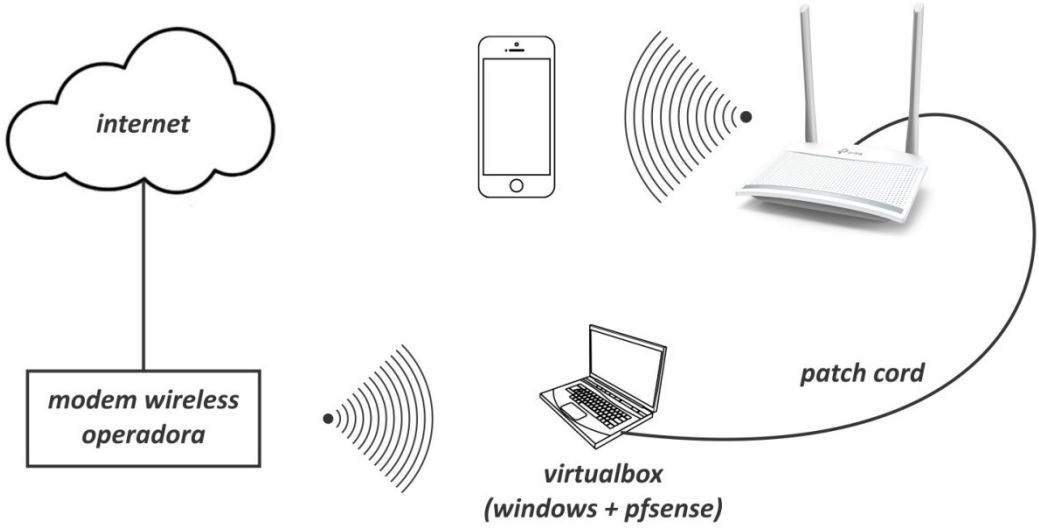
Por solicitação da empresa, por medidas de segurança, não foram anexadas fotos do setor de Suporte Técnico, muito menos foi detalhada sua infra-estrutura.

5 IMPLEMENTAÇÃO

A proposta é implantar o acesso a rede wireless utilizando o login do Facebook como método de autenticação. Para tanto, recomenda-se a utilização de um servidor pfSense com duas placas de rede, uma ligada diretamente ao modem da operadora e a segunda ao roteador wireless.

Para criar uma plataforma de testes, utilizou-se: um notebook com 6GB de memória, processador Intel Core i3 M 330, com Windows 10 Home, VitualBox versão 6.1.2 r135662 (Qt5.6.2), pfSense versão 2.4.4-p3, um roteador wireless TL-WR820N da TP Link rodando o firmware versão 1.0.2 Build 190905 Rel.42436n, e um celular com o Sistema Operacional Android para realização de testes, como pode ser visto na Figura 1.

Figura 1 – Esquema de implementação.



Fonte: Compilação do autor[5]

Como o foco deste trabalho não é a instalação do Sistema Operacional, esta etapa pode ser vista no Apêndice A, assim como a instalação do pfSense em uma máquina virtual pode ser vista no Apêndice B.

Este projeto foi dividido em cinco partes para facilitar a sua implementação, na primeira parte descreveu-se a configuração do roteador wireless, na segunda

[5] Montagem a partir de imagens coletadas nos sites: <https://www.gratispng.com/png-wuslif/>, <https://www.gratispng.com/png-mywh1t/> e <https://www.tp-link.com/br/home-networking/wifi-router/tl-wr820n/>. Acesso em: 10 fev. 2020.

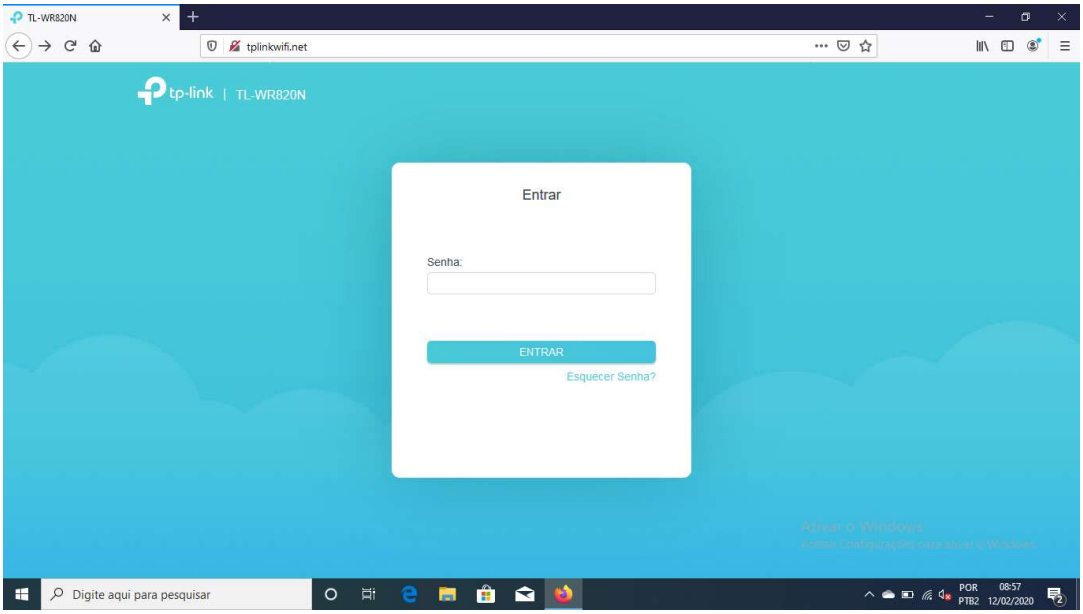
realizou-se a configuração dos adaptadores de rede dentro do Windows, na terceira parte a criação da API do Facebook, na quarta parte realizou-se as configurações básicas do pfSense assim como a instalação dos módulos adicionais necessários para a implantação do projeto e a quinta e última parte foi destinada a realização de testes.

5.1 Configuração do Roteador Wireless

Após a instalação do Windows 10 Home e instalação do VirtualBox, realizou-se as configurações do roteador wireless.

Conectou-se a placa de rede do notebook a entrada LAN do roteador wireless, acessou-se então a página de configuração do roteador através do endereço “http://tplinkwifi.net” como pode ser visto na Figura 2.

Figura 2 – Página de configuração do roteador wireless.



Fonte: O autor (2020)

Para utilizar o roteador wireless como um hotspot em conjunto com o pfSense, realizou-se algumas alterações sendo elas: as configurações da LAN, as configurações Wireless e a desativação do DHCP.

Para a configuração da LAN utilizou-se os seguintes parâmetros: endereço estático, com o IP 192.20.0.4 e máscara de sub-rede 255.255.252.0.

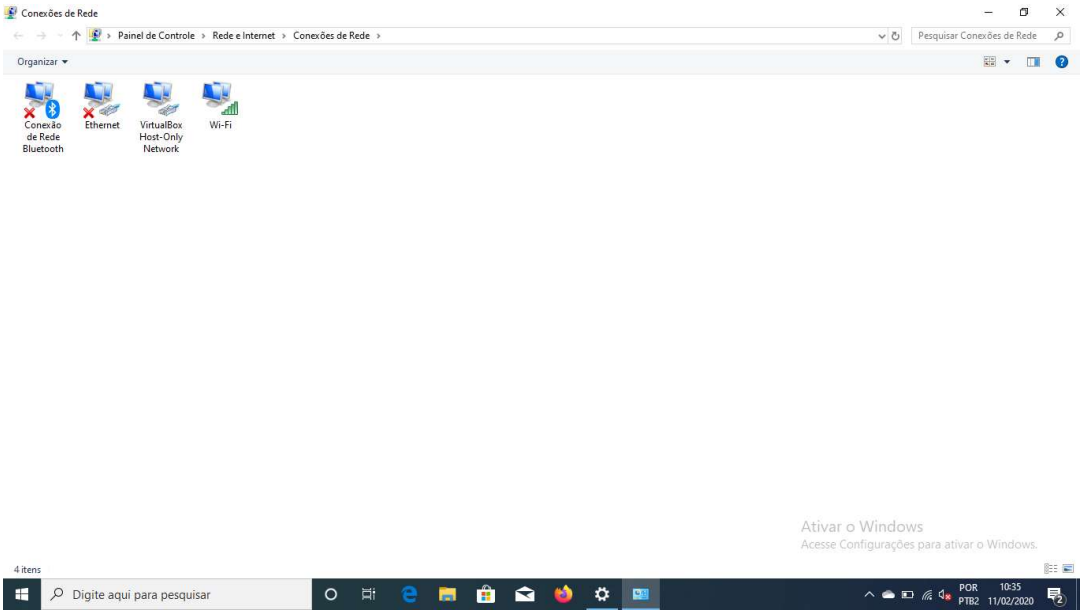
Criou-se em seguida uma rede wireless com as especificações: SSID Visitantes, sem segurança, pois o pfSense deve ser o responsável por esta parte e desabilitou-se as opções WMM e WPS, as configurações restantes foram deixadas com os padrões de fábrica.

Os últimos passos foram desabilitar o servidor DHCP do roteador wireless e reiniciá-lo para que as configurações fossem aplicadas.

5.2 Configuração dos adaptadores de rede

Realizou-se as configurações dos adaptadores: Ethernet e VirtualBox Host-Only Network. Que foram acessados pelo Painel de Controle, selecionando-se a categoria Rede e Internet em seguida Central de Rede e Compartilhamento, por fim alterou-se as configurações do adaptador, como se pode ver na Figura 3.

Figura 3 – Adaptadores de rede.



Fonte: O autor (2020)

Neste momento configurou-se o adaptador Ethernet, atribuindo um endereço de IP estático, com os seguintes parâmetros: IP 192.20.0.3, máscara de sub-rede 255.255.252.0, gateway 192.20.0.1 e servidor DNS 192.20.0.1.

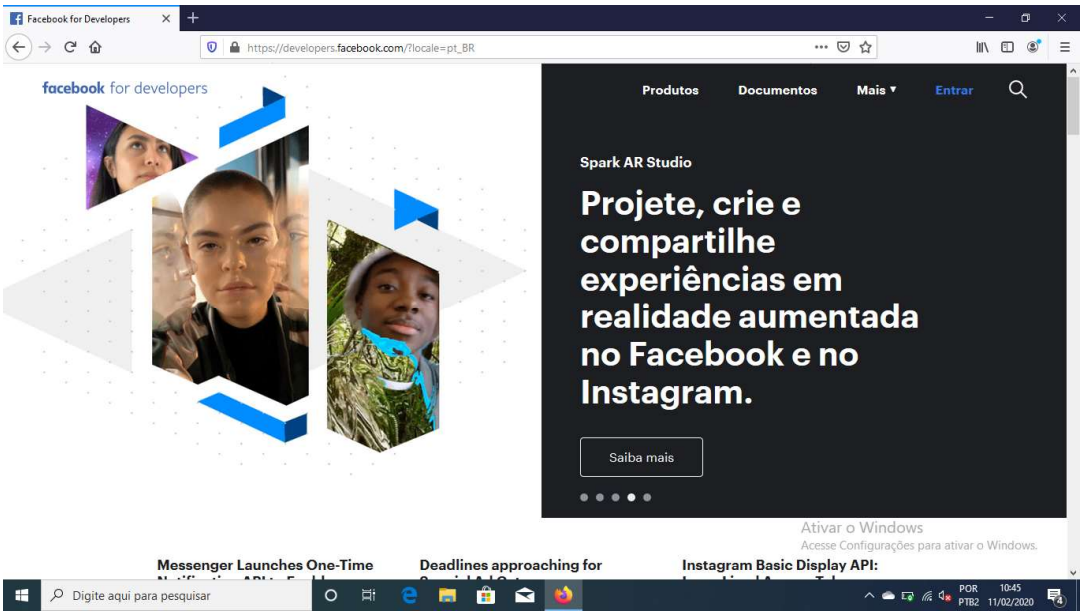
Da mesma forma foi configurado o adaptador VirtualBox Host-Only Network utilizando endereço de IP estático, com estas configurações: IP 192.20.0.2, máscara de sub-rede 255.255.252.0, gateway 192.20.0.1 e servidor DNS 192.20.0.1.

Após a configuração dos adaptadores, criou-se uma conexão ponte entre eles e posteriormente foi atribuiu-se um endereço estático com os seguintes parâmetros: IP 192.20.0.5, máscara de sub-rede 255.255.252.0, gateway 192.20.0.1 e servidor DNS 192.20.0.1.

5.3 API do Facebook

Procedeu-se a criação de uma API no Facebook, através do site Facebook Developers, que podemos ver na Figura 4.

Figura 4 – Página do Facebook Developers.



Fonte: Página do Facebook Developers[6].

Ao criar uma API, informou-se o nome da API e o email de contato, o Facebook fornece diversas opções de produtos para adicionar a uma API, neste caso o produto utilizado foi o Login do Facebook com a plataforma Web, a “Uniform Resource Locator” (URL) do site informado foi o endereço do Captive Portal, neste caso “https://192.20.0.1/cp/index.php”.

Para a utilização deste produto é necessário informar duas URLs válidas: a URL da Politica de Privacidade e a URL dos Termos de serviços, de acordo com as politicas da empresa. Para este trabalho, criou-se um texto básico e publicou-se em um blog do google.

Por fim, alterou-se o modo do API para publicado e copiou-se a ID do API.

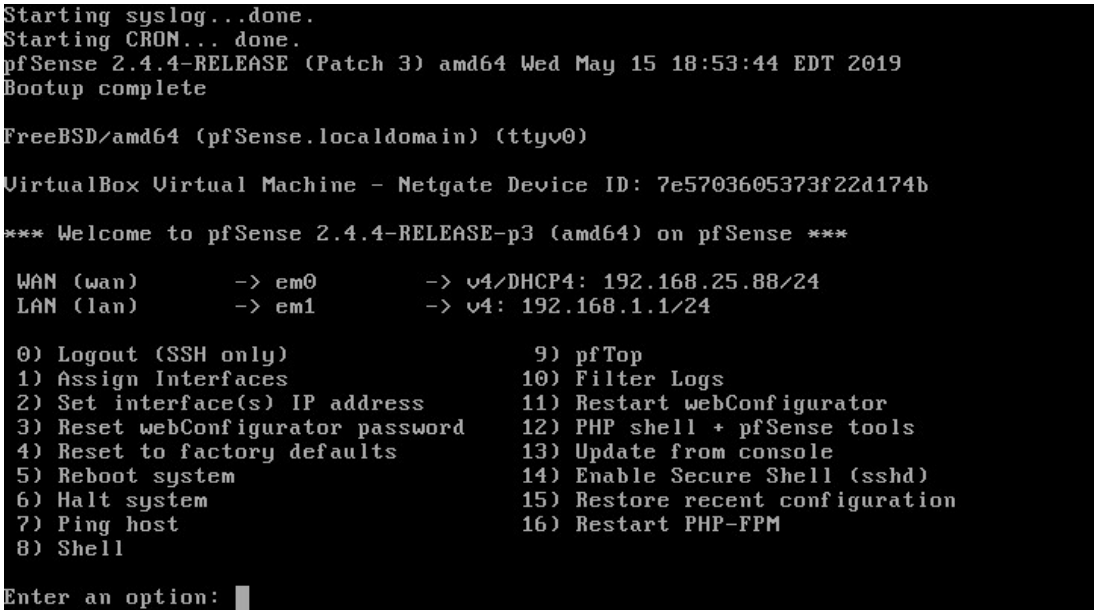
[6] Disponível em: <https://developers.facebook.com/?locale=pt_BR>. Acesso em: 11 fev. 2020.

5.4 Configuração do pfSense

Com a conclusão da API do Facebook, realizou-se as configurações iniciais do pfSense seguida da instalação dos módulos adicionais, assim como a suas respectivas configurações.

Iniciada a máquina virtual do pfSense, vizualizou-se uma tela com as informações básicas e a lista de opções, como pode ser visto na Figura 5.

Figura 5 – Tela inicial do pfSense.



Fonte: O autor (2020).

A placa de rede WAN foi configurada em modo bridge, sendo assim ela recebeu por DHCP, um IP da mesma rede ao qual a placa wireless do notebook está conectada.

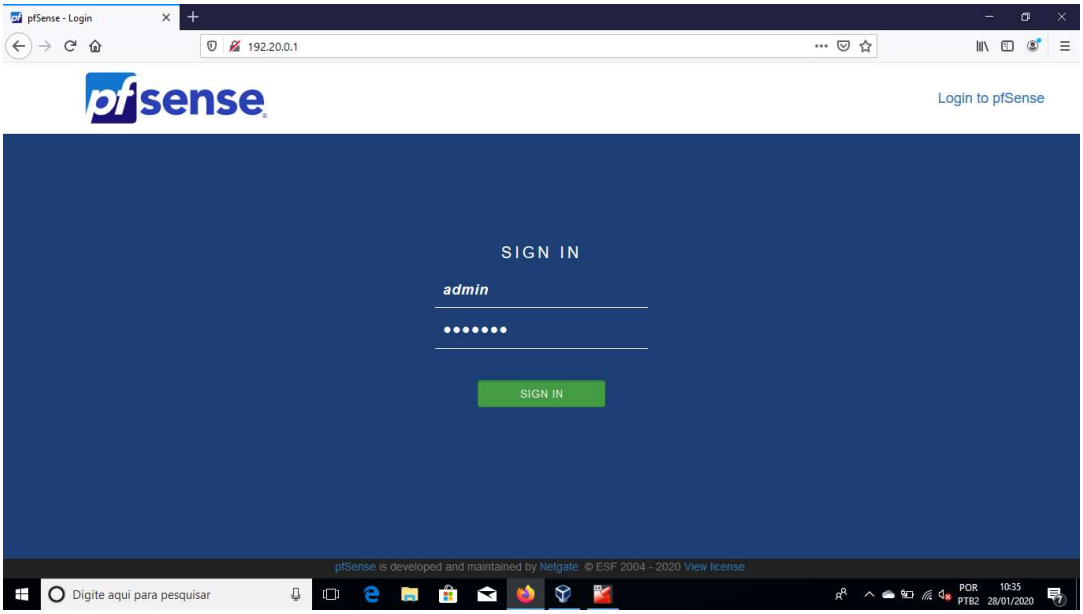
A placa LAN foi configurada no VirtualBox como Virtual Host-only e o modo promíscuo definido em permitir tudo, e como não havia sido configurada recebeu um IP dado pelo próprio pfSense.

Realizou-se então a configuração desta placa com os seguintes parâmetros: o IP estático 192.20.0.1, a máscara de sub-rede, que no pfSense é informada utilizando a notação “Classless Inter-Domain Routing” (CIDR), que informa a quantidade de bits que representa a rede, este número é precedido pelo símbolo entre aspas “/”. Neste caso optou-se pela mascara de sub-rede /22, que na notação usual é 255.255.252.0, desta forma garantindo até 1022 hosts.

Ativou-se o servidor DHCP para a interface LAN com o intervalo de IPs 192.20.0.6 à 192.20.3.254.

Em seguida foi habilitado o webconfigurator, desta forma as demais configurações do pfSense foram feitas utilizando-se outra máquina que estava na mesma rede através do navegador, utilizando o endereço de IP da placa LAN, como pode ser visto na Figura 6.

Figura 6 – Tela de acesso ao pfSense utilizando um navegador.



Fonte: O autor (2020).

Para realizar a instalação dos módulos adicionais foi preciso adicionar os repositórios destes pacotes, tendo em vista que são repositórios não oficiais.

Executou-se o comando responsável por habilitar os repositórios não oficiais.

fetch -q -o /usr/local/etc/pkg/repos/Unofficial.conf https://raw.githubusercontent.com/marcelloc/Unofficial-pfSense-packages/master/Unofficial.conf[7]

Em seguida, executou-se o comando que habilita o repositório do módulo do UserAuth.

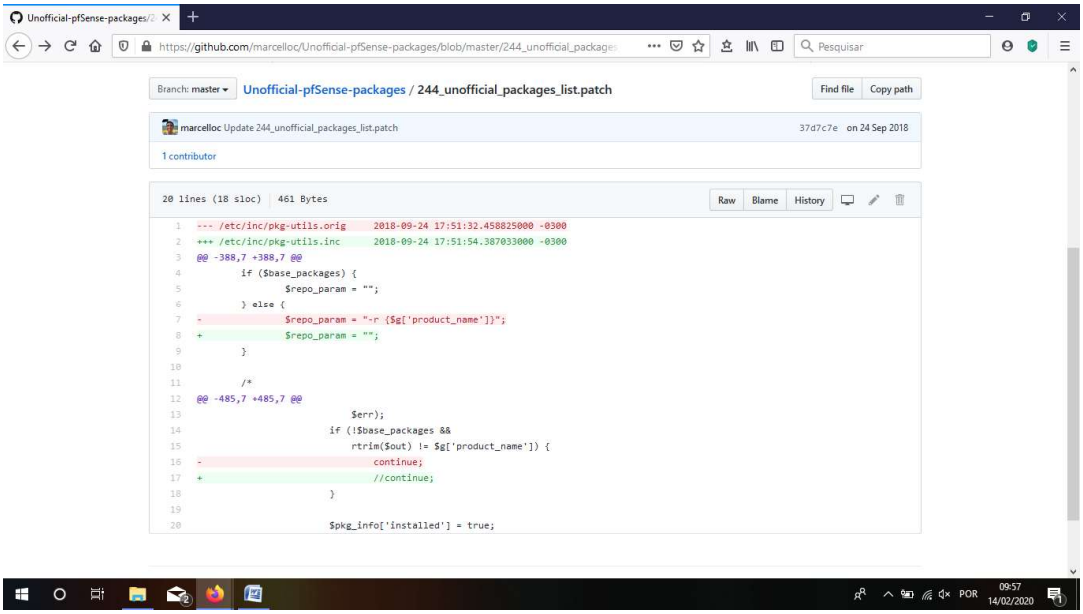
fetch -q -o /usr/local/etc/pkg/repos/wmi.conf https://e-sac.websiteseguro.com/wmi/wmi.txt[8]

[7] *Disponível em: < https://github.com/marcelloc/Unofficial-pfSense-packages>. Acesso em: 15 dez. 2019.*

[8] *Disponível em: < https:// https://jack.eti.br/userauth/>. Acesso em: 15 dez. 2019.*

Como se utilizou a versão 2.4.4 do pfSense, foi preciso a instalação do pacote System_Patches e rodar o patch que pode ser visto na Figura 7, para fazer uso dos repositórios não oficias.

Figura 7 – Patch que permite utilização de pacotes não-oficiais.



Fonte: Página de Marcello Coutinho no Github[9].

Instalaram-se então os módulos: E2guardian5 Versão 0.5.3.3, SourceGuardian Versão 0.1.8, UserAuth Versão 3.1_2.

Criou-se e exportou-se uma “Certification Authority” (CA), que foi exportada e instalada no navegador Firefox e no Windows.

Em seguida criou-se um certificado do tipo Servidor e utilizando esse certificado, configurou-se o pfSense habilitando o protocolo “Hyper Text Transfer Protocol Secure” (https).

Realizou-se a configuração do módulo E2Guardian, para isso utilizou-se as seguintes especificações: configurou-se para escutar na LAN e no loopback, limitou-se o número máximo de conexões em 1010, e habilitou-se os seguintes serviços: o Proxy transparente na LAN, o suporte ao “Secure Sockets Layer” (SSL) utilizando-se do certificado criado anteriormente, a autenticação “Domain Name System” (DNS) possibilitando então a interação com o módulo UserAuth para ocorrer o redirecionamento para o Captive Portal enquanto o usuário não realizar a autenticação.

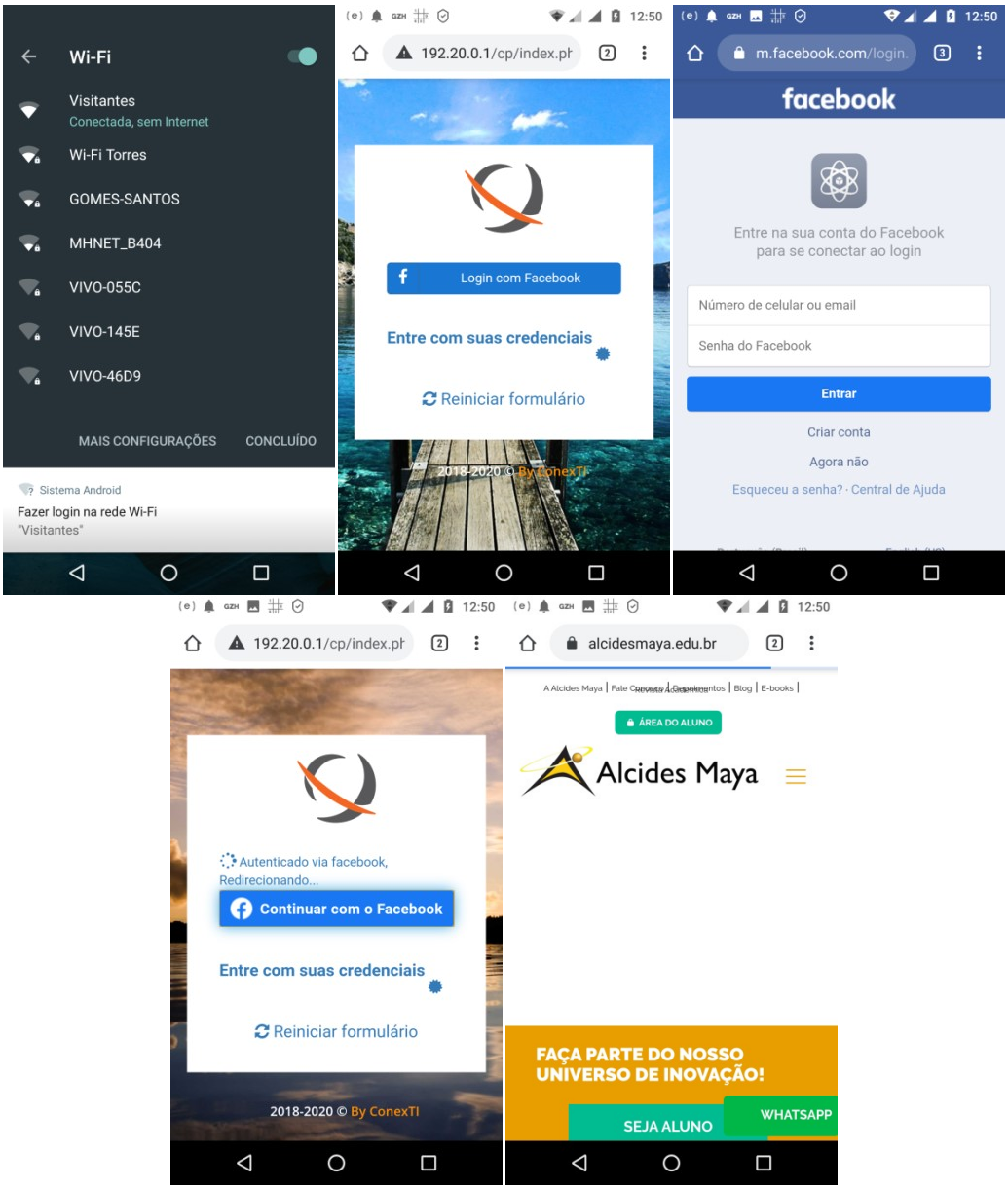
[9] Disponível em: <https://github.com/marcelloc/Unofficial-pfSense-packages/blob/master/244_unofficial_packages_list.patch>. Acesso em: 15 dez. 2019.

As configurações utilizadas no módulo UserAuth foram definir: o tempo máximo de conexão em 1 hora, o Facebook como forma de autenticação, o endereço que será encaminhado o tráfego como sendo “http://192.20.0.1”, o endereço completo do Captive Portal como sendo “http://192.20.0.1/cp/index.php” e por último informar a ID da API do Facebook.

5.5 Realização de Testes

Após todas as configurações realizadas utilizou-se um celular com o sistema operacional android, foram realizados primeiramente testes de conexão, como podemos ver na Figura 8,

Figura 8 – Sequência do teste de conexão.



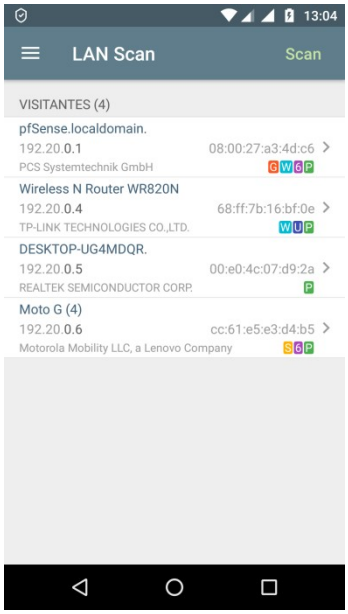
Fonte: Compilação do autor (2020)[10].

Realizada a conexão e feito o redirecionamento para o site escolhido, foram realizados testes utilizando a ferramenta Net Analyzer. Primeiramente foi feita uma

[10] Montagem a partir de imagens coletadas através de captura de tela do celular de teste.

varredura na rede onde foi possível ver quatro conexões: a LAN do pfSense, a conexão ponte no Windows, o roteador wireless e o celular de testes, como pode ser visto na Figura 9.

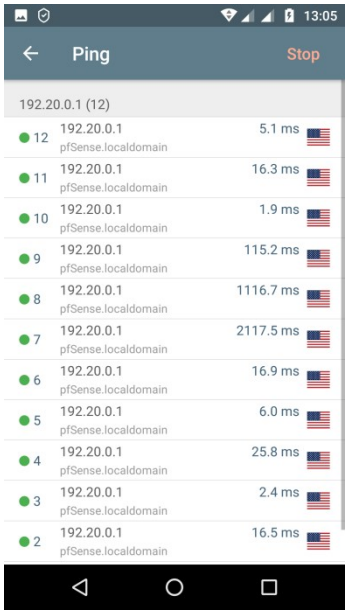
Figura 9 – Varredura da rede.



Fonte: O autor (2020).

Em seguida executamos o comando ping no endereço “192.20.0.1” que corresponde a LAN do pfSense , o resultado pode ser visto na Figura 10.

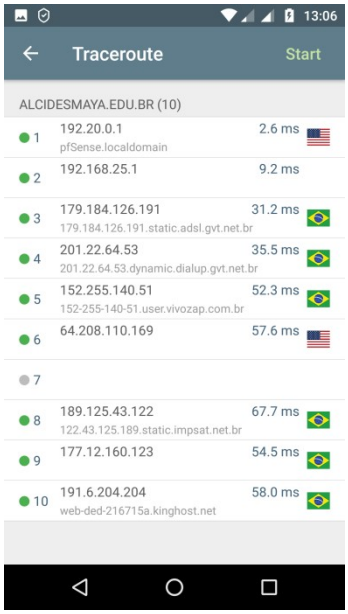
Figura 10 – Ping.



Fonte: O autor (2020).

E no último teste executou-se o comando de traceroute para o endereço “www.alcidesmaya.edu.br” cujo resultado pode ser visto na Figura 11.

Figura 11 – Traceroute.



Fonte: O autor (2020).

Como podemos ver com a sequência de testes, foi possível estabelecer uma conexão, navegar em sites, e utilizando a ferramenta Net Analyzer foi possível realizar testes de ping e traceroute, todos efetuados com sucesso.

6 CONCLUSÃO

No decorrer deste trabalho, foram apresentadas as informações sobre o estágio obrigatório realizado na Faculdade e Escola Técnica Alcides Maya, assim como uma sugestão de melhoria baseada na observação feita no decorrer do estágio.

Após ser verificada a necessidade de realizar o controle de acesso à Internet nos hotspots desta instituição e detalhado os motivos. Apresentou-se uma solução para este problema, utilizando o login do Facebook como método de autenticação.

Através de um laboratório montado foi possível demonstrar a implementação desta solução, assim como os resultados. A opção de utilizar o firewall pfSense foi feita levando-se em conta a existência de módulos capazes de promover sua integração com o Facebook.

Elencando-se a principal vantagem deste método de autenticação, como sendo o fato de não necessitar cadastro prévio de usuários por parte da instituição de ensino.

A criação de relatórios com as informações de acesso, como previsto em Lei não foi alvo deste trabalho. Porém, com utilização de um módulo adicional para o pfSense estes relatórios podem ser obtidos de forma simples.

7 REFERÊNCIAS

BIAR, Emmanuel. **A responsabilidade civil e à Internet: uma abordagem expositiva sobre a posição da jurisprudência pátria e breves considerações sobre o direito comparado**. Revista Sjrj, Rio de Janeiro, n. 26, p.221-236, 2009. Disponível em: https://www.jfrj.jus.br/sites/default/files/revista-sjrj/arquivo/40-156-2-pb.pdf. Acesso em: 10 dez. 2019.

BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei n° 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso dà Internet no Brasil. **Portal da Legislação**, Brasília, abr. 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12773.htm. Acesso em: 10 dez. 2019.

CASTRO FILHO, S. O. **Da responsabilidade do provedor de Internet nas relações de consumo**. In: BRASIL. Superior Tribunal de Justiça. Doutrina: Edição Comemorativa - 15 anos. Brasília: Brasília Jurídica, STJ, 2005. p. 157-174. Disponível em: https://ww2.stj.jus.br/publicacaoinstitucional/index.php/Dout15anos/article/view/3499/3622. Acesso em: 10 dez. de 2019.

CORRÊA, J. L. **Introdução ao pfSense: implementando um firewall**. 1. Ed. Campinas: Embrapa Informática Agropecuária, 2016. E-*book*. Disponível em: https://ainfo.cnptia.embrapa.br/digital/bitstream/item/145014/1/Doc139.pdf. Acesso em: 12 dez. 2019

EDITORA IGP. **Índice para Catalogação - CDD**. Disponível em: http://editoraigp.com.br/publicandosonhos/indice-cdd. Acesso em: 20 fev. 2020.

FELICIANO, Otoniel. **Cutter's Online**. Disponível em: https://cuttersonline.com/app/. Acesso em: 20 fev. 2020.

FERREIRA C. D. Facebook chega a 127 milhões de usuários mensais no Brasil. **Canaltech**. 19 jul. 2018. Disponível em: https://canaltech.com.br/redes-sociais/facebook-chega-a-127-milhoes-de-usuarios-mensais-no-brasil-118358/. Acesso em: 15 dez. 2019.

FRANCO, B. S. D. **Gerenciamento de uma rede sem fio com pfSense**. 2015. Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas). Universidade Tecnológica Federal do Paraná. Departamento Acadêmico de Informática, Ponta Grossa, 2015. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/6445/1/PG_COADS_2015_2_09.pdf. Acesso em: 15 dez. 2019.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e à Internet: uma abordagem top-down**. 6. ed. São Paulo: Pearson Education do Brasil, 2013.

NEVES, F. C.; MACHADO, L. A.; CENTENARO, R. da F. **Implantação de firewall pfSense**. 2014. Trabalho de Conclusão de Curso (Tecnologia em Sistemas de Telecomunicações). Universidade Tecnológica Federal do Paraná. Departamento Acadêmico de Eletrônica, Curitiba, 2014. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3968/1/CT_COTEL_2014_2_02.pdf. Acesso em: 10 dez. 2019.

PEDROZO, R. M. **Implantação de uma rede utilizando os padrões do protocolo IPv6**. 2014. Trabalho de Conclusão de Curso (Tecnologia em Redes de Computadores). Universidade Federal de Santa Maria. Colégio Técnico Industrial de Santa Maria, Santa Maria, 2014. Disponível em: https://www.ufsm.br/cursos/graduacao/santa-maria/tecnologia-em-redes-de-computadores/wp-content/uploads/sites/495/2019/05/2014-Raissa_Monego.pdf. Acesso em: 10 dez. 2019.

ROCHA, M. A. **O papel dos hotspots na experiência turística moderna**. 2016. Trabalho de Conclusão de Curso (Bacharelado Interdisciplinar em Ciências Humana). Universidade Federal de Juiz de Fora. Instituto de Ciências Humanas, Juiz de Fora, 2016. Disponível em: http://www.ufjf.br/bach/files/2016/10/MATHEUS-AMORIM-ROCHA.pdf. Acesso em: 15 dez. 2019.

TANENBAUM, A. S.; WETHERALL, D. **Redes de computadores**. 5. Ed. São Paulo: Pearson Prentice Hall, 2011.

UDC CONSORTIUM. **UDC Summary**. Disponível em: http://www.udcsummary.info/php/index.php?tag=0&lang=pt. Acesso em: 20 fev. 2020.

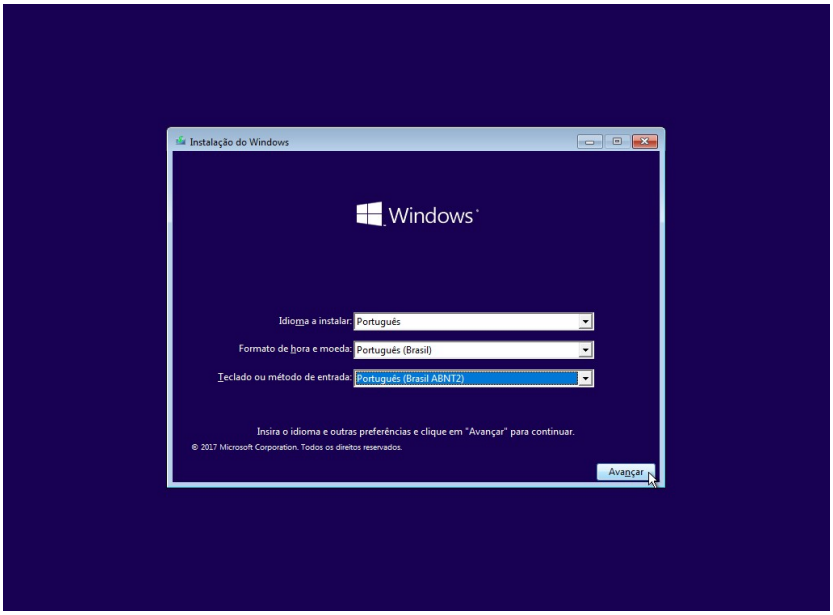
UNIVERSIDADE FEDERAL DA BAHIA. **Ficha Catalográfica**. Disponível em: http://www.sibi.ufba.br/node/55#overlay-context=. Acesso em: 20 fev. 2020

APÊNDICE A – INSTALAÇÃO DO WINDOWS 10 HOME

Para realizar a instalação do Windows 10 Home, o primeiro passo foi colocar a mídia de instalação no computador e em seguida dar o boot utilizando esta mídia.

Informou-se então o idioma, o formato de hora e moeda e o tipo de teclado, como pode ser visto na Figura 12.

Figura 12 – Tela inicial de instalação do Windows.



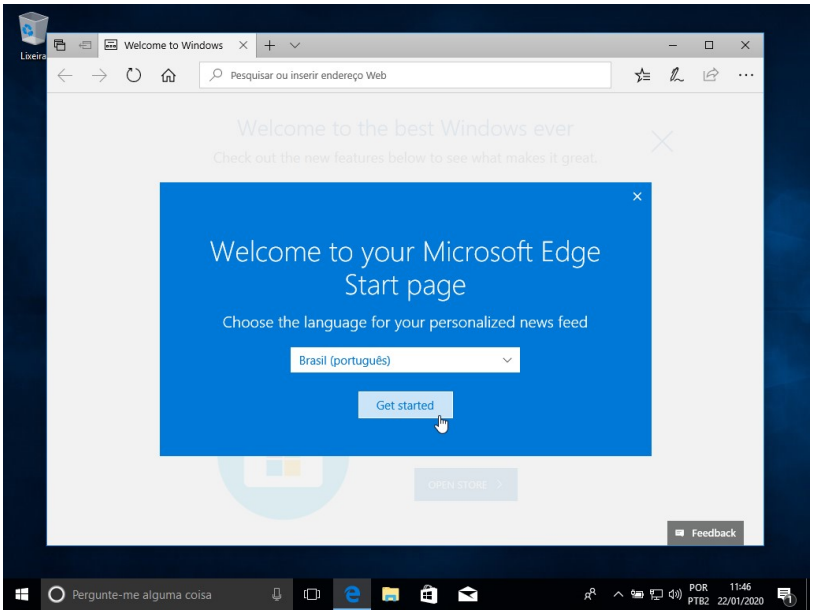
Fonte: O autor (2020).

Por se tratar de uma instalação e não de uma atualização, escolheu-se a opção de instalar apenas o Windows.

Neste momento o instalador solicitou que fosse informado em qual partição seria feita a instalação. Optou-se por clicar em avançar, desta forma o próprio instalador realizou automaticamente o particionamento conforme as necessidades do Windows 10 Home e seguiu com a instalação, que quando concluída reinicializou o computador.

Sendo necessário apenas definir algumas configurações simples para a conclusão e inicialização do Sistema Operacional como se pode ver na Figura 13.

Figura 13 – Tela inicial do Windows.

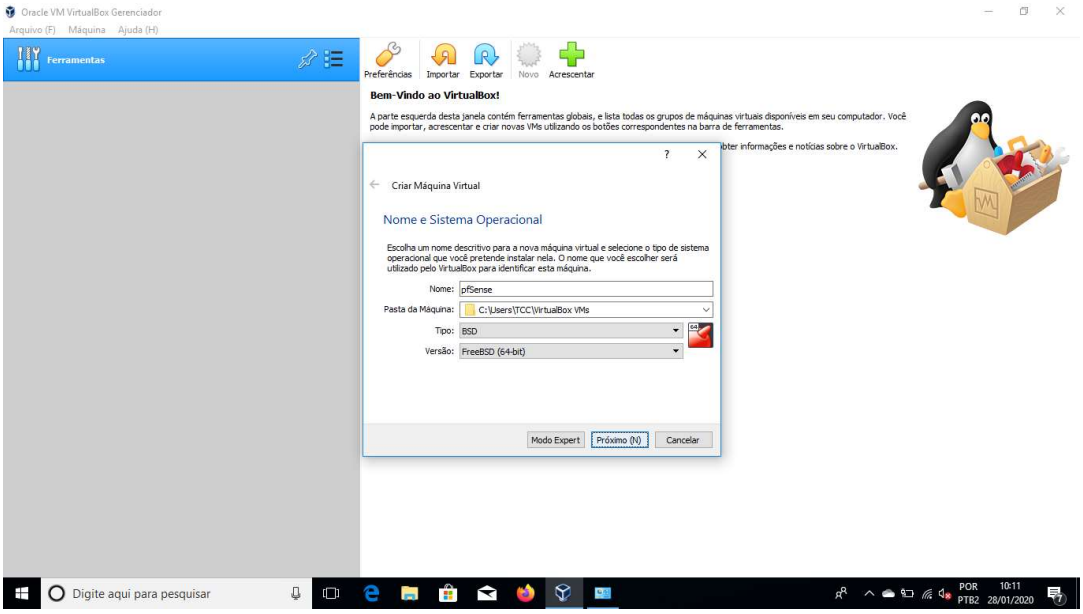


Fonte: O autor (2020).

APÊNDICE B – INSTALAÇÃO DO PFSENSE

Para realizar a instalação do pfSense no Virtualbox criou-se uma máquina virtual, como pode ser visto na Figura 14.

Figura 14 – Criação de uma máquina virtual.



Fonte: O autor (2020).

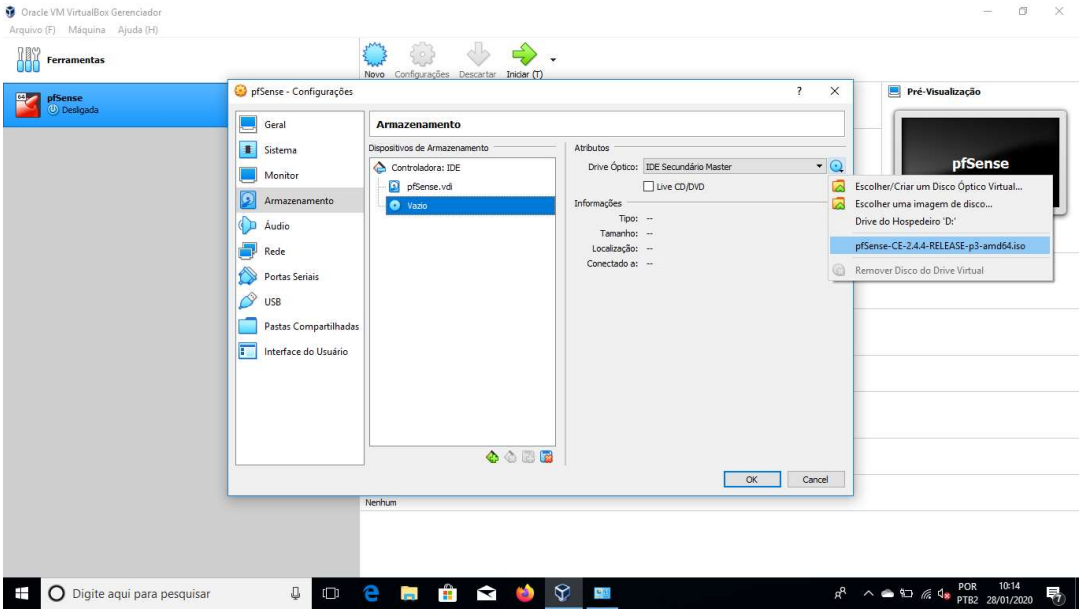
Utilizou-se as seguintes especificações: tipo BSD, versão FreeBSD (64-bit), 2,5 GB de memória e 50GB de HD dinamicamente alocado. Tanto a memória quanto HD foram dimensionados de acordo com a capacidade do notebook utilizado, sendo possível a utilização de outros valores de acordo com o equipamento utilizado.

Com máquina virtual criada, foi necessário apenas realizar algumas configurações antes de iniciá-la.

Alterou-se o número de CPUs para 2, configurou-se duas placas de rede, uma como Bridge e outra como Virtual Host-only, com o modo promíscuo em permitir tudo.

Por último, selecionou-se a imagem do pfSense, conforme a Figura 15, para que quando iniciarmos a máquina virtual ela seja inicializada.

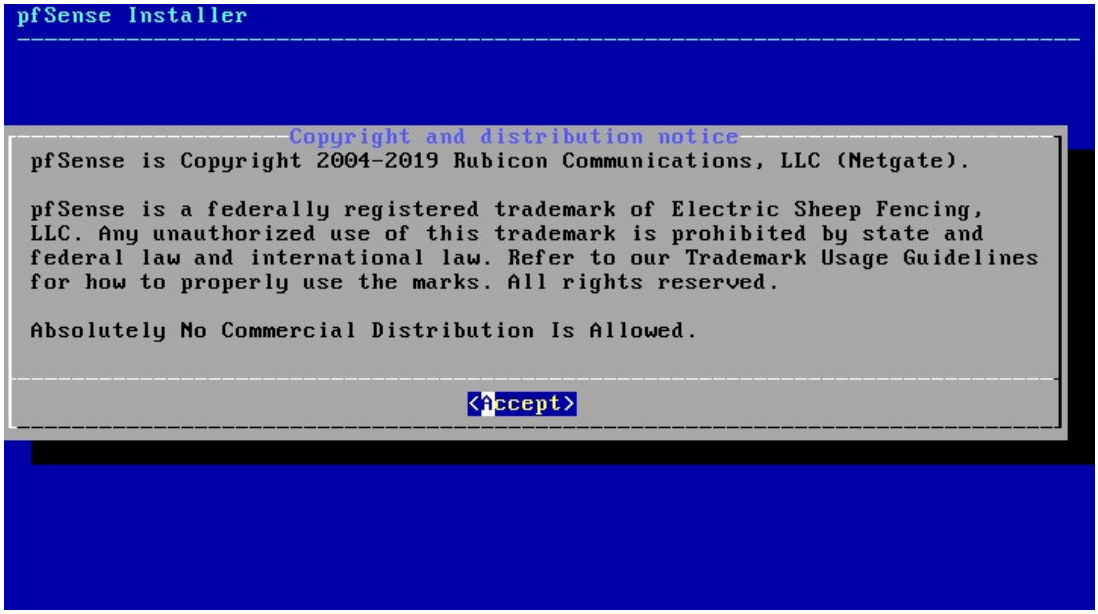
Figura 15 – Configuração de uma máquina virtual.



Fonte: O autor (2020).

O próximo passo foi iniciar a máquina virtual, como pode ser visto na Figura 16.

Figura 16 – Tela de instalação do pfSense.



Fonte: O autor (2020).

Escolheu-se como forma de particionamento, a opção Auto (UFS), desta forma o próprio instalador realizou o particionamento de acordo com as necessidades do pfSense e prosseguiu com a instalação, ao término do processo foi solicitada a reinicialização da máquina virtual, para concluir a instalação.