INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO PIAUÍ
CAMPUS TERESINA ZONA SUL
DIRETORIA DE ENSINO
COORDENAÇÃO DO CURSO SUPERIOR EM LICENCIATURA EM INFORMÁTICA

IMPLEMENTAÇÃO DE UMA REDE WI-FI INFRAESTRUTURADA PARA OS ALUNOS DO IFPI-CATZS

Francisco Rômulo de Oliveira Sabóia[1]
Jeanne de Souza Silva Leite[2]

RESUMO

Esta pesquisa teve por objetivo a implementação de uma rede *Wi-Fi* (*Wireless Fidelity*) infraestruturada para os alunos do Instituto Federal do Piauí – Campus Teresina Zona Sul. Para tanto, fez-se necessário a escolha da topologia utilizada, a implantação de um sistema de controle de acesso e outro de banda larga. A abordagem metodológica desenvolvida neste trabalho foi uma análise quantitativa e como procedimento técnico adotou-se a pesquisa-ação. Nos resultados foi possível definir a topologia utilizada, a implementação de um servidor *FreeRADIUS* integrado ao *Router Board Mikrotik* com a ferramenta *Hotspot* habilitada para o controle de acesso e controle de banda larga. Conclui-se que a rede infraestruturada implantada através da ferramenta *Hotspot* é eficiente para o controle de acesso, mas falha no quesito segurança, pois fornece endereço de Protocolo da Internet (IP) antes de realizar a autenticação no servidor *FreeRADIUS, e que* o controle de banda larga é de extrema importância para a instituição, pois observamos um consumo de banda larga de 5,2 gigabytes na rede implementada.

Palavras-chave: Redes *Wi-Fi*. Infraestruturada. Autenticação. Banda larga.

1 INTRODUÇÃO

As redes *Wi-Fi* têm se difundido em todos os lugares e nos campuses universitários, um grande número de acadêmicos utiliza essas redes para se conectarem a internet. Essas redes possuem algumas vantagens em relação às redes cabeadas como a mobilidade e flexibilidade, mas também possuem desvantagens e uma delas está relacionada à vulnerabilidade do seu meio de transmissão, pois seus dados trafegam pelo ar e podem ser facilmente capturados e

[1] Graduando de Licenciatura em Informática. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. romulo0788@gmail.com.

[2] Professora Me. Eixo Disciplinas Específicas do curso de Licenciatura em Informática. Instituto Federal de Educação, Ciência e Tecnologia do Piauí, Campus Teresina Zona Sul. jeanneleite@gmail.com.

acessados por pessoas mal intencionadas principalmente aquelas redes que encontram - se abertas e não possuem nenhum tipo de controle de acesso. Outra desvantagem é que as redes *Wi-Fi* instaladas para um grande número de usuários geralmente não recebem nenhum controle de banda larga podendo causar indisponibilidade do serviço de internet.

Portanto, a implementação de uma rede *Wi-Fi* infraestrutura, que segundo a autora Rodrigues (2011), são aquelas redes em que toda a comunicação deve passar por um ponto central mesmo que os equipamentos sem fio estejam em uma distância em que poderiam comunicar-se diretamente, pode solucionar esses problemas, considerando o fato de que nesses pontos centrais chamados de *EMS (Estação de Suporte à Mobilidade)* serão aplicados os protocolos de segurança para autenticação de usuários e proteção de dados, além do controle de banda larga, que consiste em limitar a velocidade de banda larga em que cada usuário poderá utilizar para navegar na internet, fazendo com que o *link* de banda larga recebido no roteador fique disponível para outros usuários.

O IFPI -CATZS, disponibiliza acesso à internet aos seus alunos por meio de redes *Wi-Fi* instaladas no campus. Enquanto aluno do Curso de Licenciatura em Informática do IFPI-CATZS e usuário dessa rede observou-se que a mesma não possui protocolos de segurança para autenticação de usuários, o que deixa os dados dos usuários conectados nessa rede vulneráveis, pois qualquer pessoa mal-intencionada que adentre no campus pode usar softwares capazes de roubar dados. Também foi percebido que a rede não possui nenhum controle de banda larga impactando na indisponibilidade do serviço de internet.

Em face do exposto, como podemos resolver os problemas de falta de controle de acesso e indisponibilidade do serviço de internet na rede *Wi-Fi* disponível para os alunos do IFPI-CATZS?

Visando solucionar os problemas apontados, este trabalho tem como objetivo geral implementar de uma rede *Wi-Fi* infraestruturada para a rede dos alunos. Para tanto, foram traçados os seguintes objetivos específicos: escolher a topologia a ser implementada; estabelecer um de controle de acesso e controlar a banda larga da rede *Wi-Fi* disponível para os alunos do IFPI-CATZS.

Durante todo o período acadêmico pôde-se observar que a rede *Wi-Fi* possui os problemas já citados anteriormente e pelo fato de o proponente deste projeto possuir conhecimentos específicos na área de administração de redes de

computadores fez com que houvesse o interesse em realizar uma pesquisa para poder contribuir com uma solução simples e barata para proporcionar uma melhor segurança e acesso à internet para os alunos da instituição.

O acesso à internet no IFPI-CATZS é de extrema importância para os alunos possibilitando a realização de pesquisas acadêmicas, acesso ao sistema de controle acadêmico entre outros serviços disponibilizados pelo instituto e necessários para o estudo acadêmico, tornando-se um facilitador de acesso à informação.

As melhorias sugeridas neste projeto podem ser implementadas com poucos custos para a instituição, pois além de já ter a maioria dos equipamentos em funcionamento na rede *Wi-Fi* atual, a mesma dispõe de um laboratório de informática Laboratório Interdisciplinar de Formações de Educadores (*LIFE)* onde se encontra computadores e um rack montado com os equipamentos necessários para a implementação de uma rede *Wi-Fi* infraestruturada.

2 REDES Wi-Fi E SEUS PROTOCOLOS DE AUTENTICAÇÃO

As redes *Wi-Fi*, são uma forma de interconectar dispositivos sem o uso de cabos usando somente hardwares transmissores de ondas de rádio para a conexão, transmissão de dados e transmissão de pacotes.

De acordo com Tanenbaum (2003, p.23), a comunicação digital sem fio não é uma ideia nova já que em 1901 um físico italiano demonstrou como funcionava um telégrafo sem fio que transmitia informações de um navio para o litoral por meio de código *morse*. A ideia das redes *Wi-Fi* modernas é a mesma, porém com um melhor desempenho e capacidade de transmissão de dados.

Com a modernização das redes *Wi-Fi* várias empresas e grupos de pesquisas resolveram trabalhar com a tecnologia, mas esbarraram na falta de padronização visto que cada grupo trabalhava de uma forma diferente, diante disso algumas empresas como a *3Com*, *Nokia*, *Lucent Technologies* (atualmente *Alcatel-Lucent*) e *Symbol Technologies* (adquirida pela *Motorola*) resolveram criar um grupo para lidar com essas questões de padronizações surgindo assim, em 1999 a *Wireless Ethernet Compatibility Alliance* (*WECA*), que passou a se chamar *Wi-Fi Alliance* em 2003 trazendo junto com essa modificação a adoção do padrão *Institute of Electrical na Eletronics Engineers* (*IEEE)* 802.11.

O padrão *IEEE* 802.11 foi criado em 1990 pelo *IEEE* que é uma organização profissional sem fins lucrativos fundada em 1963 nos Estados Unidos, eles passaram a apostar nessa nova tecnologia *Wi-Fi* e definiram um grupo de pesquisa para criar padrões abertos que pudessem tornar a tecnologia *Wi-Fi* uma realidade, criando assim o projeto denominado padrão *IEEE 802.11* que define basicamente uma arquitetura para as redes *Wi-Fi*.

De acordo com Torres (2019, p.35) as arquiteturas de redes são um conjunto de camadas e protocolos que definem a transmissão física de dados, ou seja, como os dados são transmitidos. Nas redes *Wi-Fi* a arquitetura é definida com a utilização de cinco camadas do modelo *Open System Interconnect (OSI),* sendo a camada física, camada de enlace de dados, camada de rede, camada de transporte e camada de aplicação.

A seguir está descrito as duas camadas que servem como base para o padrão *IEEE* 802.11:

A camada física é subdividida em outras duas subcamadas o Procedimento de Convergência do Meio Físico (*PLCP*) que tem a função de interface entre a camada de controle de acesso ao meio e a segunda subcamada da camada física, denominada Dependente do Meio Físico (*PMD*) onde ela é responsável por converter os sinais elétricos em ondas de rádio.

A camada de enlace de dados recebeu duas subdivisões Controle do *Link* Lógico (*LLC*) onde através dessa subcamada a máquina receptora de pacote tem como saber para qual protocolo de alto nível ela deve entregar os dados de um quadro que ela acabou de receber e Controle de Acesso ao Meio (*MAC*) onde ela monta o quadro de dados a ser transmitido pela camada física e criptografa os dados protegendo-os de acessos não autorizados que se tornou um problema das redes *Wi-Fi* sem segurança.

A criação de redes *Wi-Fi* seguras surgiu com o aumento exponencial das redes de computadores onde os dispositivos se conectavam nessas redes sem nenhum tipo de controle de acesso e tinham seus dados acessados sem autorização, devido a esses problemas foram criados os protocolos de autenticação (MORAIS, 2017).

Segundo Morimoto (2011, p.243) o primeiro protocolo de autenticação criado foi o *Wired Equivalent Privacy (WEP)*, que trazia como promessa um nível de segurança equivalente ao de redes cabeadas, o que logo se mostrou falso já que

sua criptografia utiliza o algoritmo de criptografia *RC4* (*Alleged RC4*). Voitechen (2015) diz que o protocolo *RC4* é um algoritmo de cifra de fluxo de chave compartilhada que utiliza uma mesma chave simétrica para criptografia e descriptografia que pode ser quebrada facilmente apesar de utilizar chaves de 64 e 128 *bits*.

Outro grande problema deste protocolo é que ele é baseado no uso de vetores de inicialização onde eles utilizam uma chave fixa configurada no cliente que sempre estará se repetindo quando o cliente estiver se comunicando. Essas vulnerabilidades do protocolo *WEP* fez com que fosse criado emergencialmente o protocolo de autenticação *Wired Protect Acess* (*WPA)*, que surgiu em 2002 com algumas melhorias como a utilização do algoritmo *RC4* de forma mais segura dentro do protocolo de criptografia *Temporal Key Intregrity Protocol* (*TKIP)* (PAIM, 2011).

O protocolo *TKIP* trabalha com conceito de chave dinâmica em que essa chave é utilizada por um período de tempo e depois é gerada outra chave dinâmica que faz que cada pacote seja encriptado com uma chave diferente, essa chave tem uma base de 128 bits denominada *Temporal Key (TK)*, que é combinada com o endereço *MAC* do transmissor sendo gerada outra chave denominada *Temporal and Transmitter Address Key* (*TTAK)*, também conhecida como chave da “primeira fase”. Na “segunda fase” a chave *TTAK* é combinada com o IV do *RC4* para gerar diferentes chaves para cada pacote, logo depois dessas melhorias lançaram o protocolo de segurança *WPA2* (SILVA, 2011).

No *WPA2* a autenticação possui dois métodos: a primeira denominada Pessoal, onde é usada uma chave compartilhada (*WPA-Pre Shared Key ou WPA-PSK*) entre o ponto de acesso e os clientes da rede sem fio. A segunda é denominada Corporativo, onde se utiliza um servidor de autenticação, por exemplo, um servidor *Remote Authentication Dial-In User Service* (*RADIUS)*, *Lightweight Directory Access Protocol* (*LDAP)*. Esse método utiliza um protocolo de comunicação 802.1x entre o Ponto de Acesso e o servidor de autenticação em conjunto com algum tipo de *Extensible Authentication Protocol* (*EAP)* (RUFINO, 2005).

De acordo com Silva (2011) *EAP* é um protocolo que permite várias técnicas de autenticação que é definido pela *RFC* 3478 utilizados em redes Wi-Fi possuindo os seguintes padrões *EAP-MD5*, *EAP Transport Layer Security (EAP-TLS*), *EAP-Tunneled Transport Layer Security (EAP-TTLS)* e *Protected Extensible*

Authentication Protocol (PEAP) que é utilizado nos servidores *Remote Authentication Dial-In User Service (RADIUS)*. O *RADIUS* foi criado pela *Livingston Enterprises, Inc*. no início da década de 90, sua função era permitir acesso dos usuários aos servidores de autenticação por meio de protocolos (MORAIS, 2017).

Para Medeiros (2017) *RADIUS* é um servidor remoto para autenticação de usuários e contas em que ele é responsável por receberem pedidos de conexões de usuários, autenticando-os e retornando toda configuração necessária para o cliente, esses servidores dispõem de soluções pagas para Windows e versões *open source* para sistemas *Unix* que tem o *FreeRADIUS* como o mais utilizado.

O servidor *FreeRADIUS* é um serviço para *Unix* que permite configurar um servidor do protocolo *RADIUS*, o qual permite ser usado para autenticação e contagem de vários tipos de acesso à rede. Para usar o servidor é necessário configurar corretamente o cliente, isso permitirá que possam se comunicar, incluindo servidores terminais, *Switches Ethernet*, pontos de acesso sem fio ou um computador com um aplicativo que emula a função de *RADIUS* cliente (MEDEIROS, 2017).

O *FreeRADIUS* é um pacote *RADIUS* modular de alto desempenho e rico em recursos incluindo servidor, cliente *radius*, bibliotecas de desenvolvimento e várias outras funcionalidades como o balanceamento de carga e tolerância a falhas, importantes para uma rede *Wi-Fi* infraestruturada, (*FREERADIUS*, 2015). Segundo Levy (2015) o *FreeRADIUS* é utilizado em ambientes empresariais em conjunto com um *RouterOS Mikrotik* com a finalidade de otimizar e garantir a disponibilização de conectividade e um controle mais amplo da rede *Wi-Fi*.

Segundo a documentação oficial de sua desenvolvedora *Mikrotik*, site *wiki.mikrotik.com* (2019), o *RouterOS Mikrotik* é um sistema operacional baseado em *Linux* que é instalado em um microcomputador ou em seu próprio hardware proprietário (*Routerboard*), ele é um poderoso servidor de rede que possui várias ferramentas, tais como, servidor *DHCP*, *Hotspot*, limitador de banda, *Firewall*, *WebProxy*, *VPN*, entre outros.

Hotspot é uma ferramenta em que oferece o serviço de internet, sejam eles pagos ou gratuitos e controle de autenticação, essa ferramenta geralmente é mais utilizada em locais públicos onde se tem muitos acessos. O *Hotspot* contido no *Routerboard Mikrotik* oferece várias maneiras de autenticação de acesso e uma

delas é a possibilidade de usar um servidor externo de autenticação, o *FreeRadius*, Levy (2015).

No trabalho de Medeiros (2017) denominado “Implementação de um modelo de segurança rede sem fio WPA2-EAP”, na qual foi implementado um servidor *FreeRadius*, os resultados mostraram que a partir da implementação do protocolo *RADIUS* se pode ter um melhor gerenciamento do controle de acesso. Morais (2017) descreve em seu trabalho os tipos de criptografia e faz o uso da aplicação *FreeRADIUS* para gerenciar o controle de acesso do usuário, neste mesmo trabalho ele cadastrou vários usuários em que eles se conectavam na Rede Wi-Fi a partir de uma senha criada para cada usuário e cadastrada no servidor.

No trabalho de Levy (2015) denominado “Gerenciamento de uma rede pública utilizando a ferramenta *Hotspot* do sistema operacional routeros”, ele faz o uso do servidor *FreeRADIUS* em conjunto com um *Routerboard Mikrotik* em um ambiente acadêmico*,* no *Routerboard* ele habilitou a função *Hotspot* com a finalidade de aplicar um melhor controle de autenticação, assim como, um controle de banda larga.

Todos os trabalhos citados acima serviram de fundamentação e referência para este projeto, onde pretendemos contribuir para solucionar os possíveis problemas detectados na Rede Wi-Fi disponível para os alunos do IFPI-CATZS.

3 ASPECTOS METODOLÓGICOS DA PESQUISA

A metodologia aplicada neste trabalho compreende uma pesquisa-ação com abordagem qualitativa, porém os resultados foram expressos de forma quantitativa. Através da pesquisa foram identificados problemas na rede *Wi-Fi* disponível para os alunos do IFPI-CATZS, que serviu de objeto de estudo para este trabalho.

Conforme Thiollent (2011) uma pesquisa-ação é um tipo de pesquisa social que é concebida e realizada em estreita associação com uma ação ou com a resolução de um problema coletivo. Nas pesquisas qualitativas, segundo Deslauriers (1991, p. 58), "o objetivo da amostra é de produzir informações aprofundadas e ilustrativas: seja ela pequena ou grande, o que importa é que ela seja capaz de produzir novas informações" (DESLAURIERS apud GERHARDT e SILVEIRA, 2009, p. 32).

Segundo Richardson (1999), a pesquisa quantitativa caracteriza-se pelo emprego de quantificação, em que a coleta de dados de dados enfatiza números em que permitam verificar a ocorrência ou não das consequências e aceitar ou não as hipóteses.

Para a coleta de dados utilizamos um notebook da marca *Asus*, modelo *A42F Series,* com configuração de 6 *Gb* de memória *RAM*, processador *Intel® Core™* i5-460M e HD (*hard disk*) de 500GB e nele instalamos os softwares *Winbox* 3.2(*64bit*), *Mikrotik Sys Log Daemon* ambos fornecidos gratuitamente pela fabricante do *RouterBoard* e o *Gestor Log Mikrotik* que foi desenvolvido pela empresa *Bylltec* e fornecido gratuitamente na internet.

A coleta de dados feita no software *Winbox* 3.2(*64bit*) de consumo de banda larga e tempo de conexão de usuários foram registrados através de logs de dados gerados na própria ferramenta e foram apresentados através de capturas de tela e gráficos, na ferramenta *Gestor Log Mikrotik* os dados foram gerados em conjunto com o software *Mikrotik Sys Log Daemon* que é responsável por registrar as requisições de acesso ao servidor *FreeRADIUS* e o acesso a páginas *web* que foram apresentados por meio de captura de telas e gráficos. Posteriormente a coleta desses dados foi realizada a análise dos dados obtidos.

Esta pesquisa foi realizada em 3 etapas, descritas nas seções 3.1, 3.2 e 3.3, sendo que as etapas 3.1 e 3.2 foram baseadas nos métodos utilizados pelo autor Levy (2015) que fez sua pesquisa em um campus universitário, onde primeiramente fez uma análise da topologia que estava sendo utilizada para posteriormente realizar sua implementação de controle de acesso, enquanto etapa 3.3 foi desenvolvida pelo proponente deste projeto. Todas as etapas da pesquisa foram realizadas no Laboratório Interdisciplinar de Formações de Educadores *(LIFE)* do IFPI-CATZS no período de setembro 2019 a janeiro de 2020.

3.1 ETAPA 1 - DEFINIR TOPOLOGIA

Para a definição da topologia que foi utilizado na implementação da rede *Wi-Fi*, foi feito um levantamento da topologia que está sendo utilizada atualmente na rede disponível para os alunos e para isso utilizamos o software gratuito *network mapping*, com este software podemos mapear todos os dispositivos que estão sendo utilizados para o funcionamento da rede *Wi-Fi* atual e a partir dos resultados obtidos

definimos qual a melhor topologia para ser implementada sem que haja muitas mudanças na estrutura atual para que não houvesse custos excessivos e desnecessários.

3.2 ETAPA 2 - IMPLEMENTAR A REDE WI-FI COM CONTROLE DE ACESSO

Para a implementação da rede *Wi-Fi* infraestruturada utilizamos 01 rack de 36 u's para acondicionamento dos equipamentos, 01 *Access Point* da marca *TP-LINK* modelo *AC1750*, 01 computador da marca Positivo com *Intel® Core™* i5 - 3300 3º geração, memória de 8GB de *RAM* e *hard disk* de 1TB que foi suficiente para a instalação do sistema operacional *Linux Debian* 9.0 e o software aplicativo *FreeRADIUS*, que segundo Medeiros (2017) são softwares gratuitos e de código fonte aberto transformando-se uma alternativa de baixo custo de implementação (todos os equipamentos acima citados encontram-se no laboratório de informática "*LIFE*" do IFPI-CATZS). Também foi utilizado um *RouterBoard Mikrotik* RB 750 de baixo custo responsável por realizar o controle de banda larga, nele habilitamos também a ferramenta *Hotspot* que foi responsável por receber as requisições de autenticação à rede *Wi-Fi* com usuário e senha e levando-as ao servidor *FreeRADIUS* para autenticação, o *RouterBoard* foi fornecido pelo proponente deste projeto para o período de testes e recolhido posteriormente após a coleta dos dados.

Após a implementação do controle de acesso foi cadastrado no servidor *FreeRADIUS* o usuário e senha de um grupo de 10 acadêmicos do curso de licenciatura em informática do IFPI-CATZS, os alunos escolhidos foram todos da turma 826 pois estes utilizam frequentemente o laboratório onde a rede *Wi-Fi* foi implementada. A rede *Wi-Fi* esteve disponível para o acesso dos alunos durante um período de 10 dias e recebeu o *Service Set Identifier (SSID)* "ALUNOSTESTE".

3.3 ETAPA 3 - IMPLEMENTAR CONTROLE DE BANDA LARGA

Nesta etapa utilizamos um notebook da marca *Asus*, modelo *A42F Series,* com configuração de 6 Gb de memória *RAM*, processador *Intel® Core™* i5-460M e *hard disk* de 500GB e nele instalamos os softwares *Winbox* 3.2(*64bit*) que é responsável por acessar as configurações do *RouterBoard Mikrotik* em que foi feito o

controle de banda larga disponibilizado para os usuários uma velocidade de 2048*kpbs* para navegação com a internet.

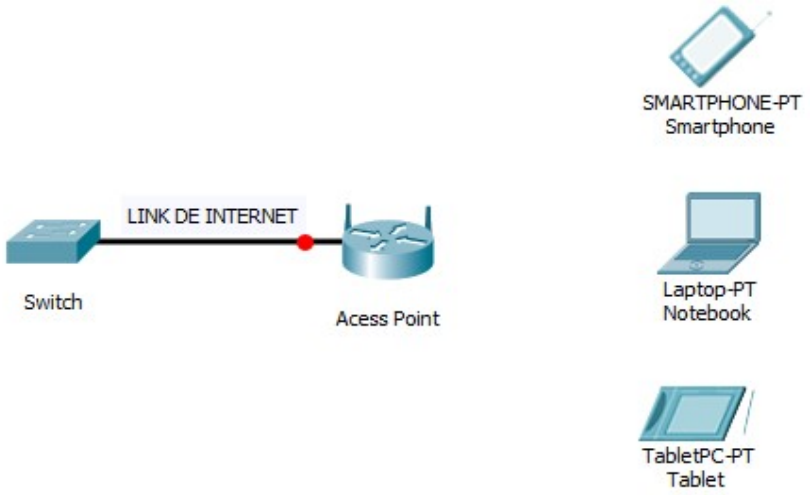
4 RESULTADOS E DISCUSSÕES

Nesta seção são apresentados e discutidos os resultados obtidos após aplicação das etapas propostas nesta pesquisa, para tanto iremos discursar sobre a definição da topologia, a implementação da Rede *Wi-fi* com controle de acesso através da análise da comunicação *Hotspot* e FreeRadius e dos usuários cadastrados, o controle de Banda Larga a partir da captura de Logs de dados da rede e outros resultados que foram alcançados na pesquisa.

4.1 DEFINIÇÃO DA TOPOLOGIA

A topologia e o *SSID* utilizados atualmente na rede *Wi-Fi*, disponível para os alunos do IFPI-CATZS são demonstrados nas Figura 1 e Figura 2. Segundo a autora Rodrigues (2011) o *SSID (Service Set Identifier),* identifica os pontos de acesso em uma rede Wi-Fi e diferencia uma rede *Wi-Fi* de outra e geralmente recebe o mesmo nome de uma empresa ou instituição para facilitar sua identificação.

Figura 1 – Topologia Rede atual

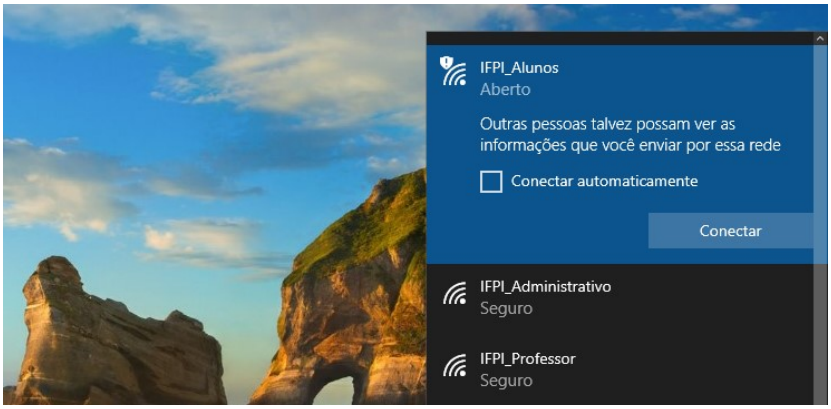


Fonte: Próprio autor (2019)

A figura 1 demonstra a topologia utilizada na rede atualmente do IFPI, onde um *switch* através de um *link* de internet fornece um ponto de acesso que pode fica disponível para ser acessado por smartphones, notebooks e tablets. A rede atual

que está disponível para os alunos encontra-se aberta sem nenhum controle de acesso e de banda larga, sendo vulnerável a ataques maliciosos.

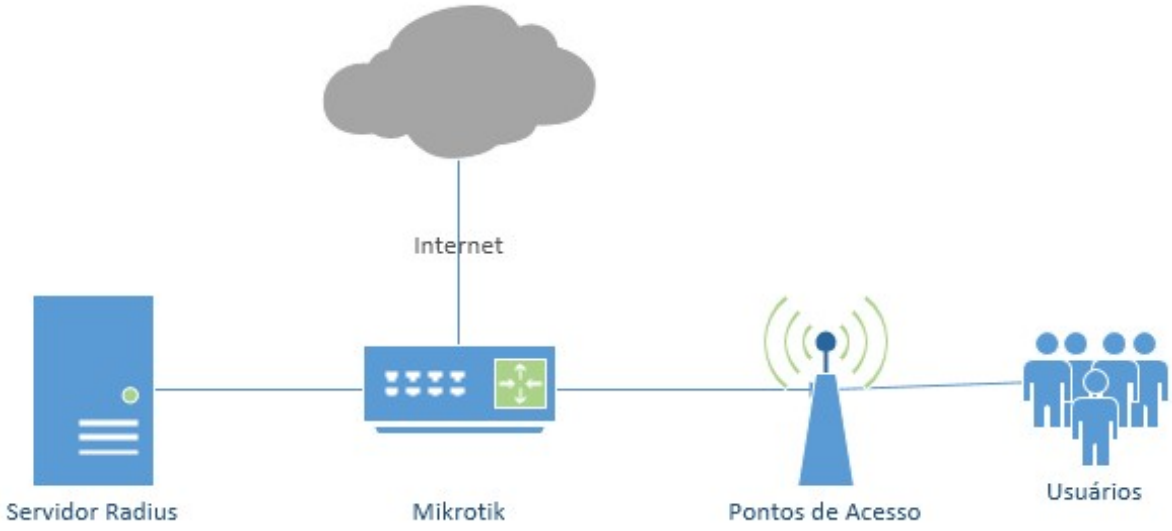
Figura 2 – SSID rede *Wi-Fi* Alunos



Fonte: Próprio autor (2019)

A Figura 2 mostra que a rede recebeu o *SSID* “IFPI_Alunos” e se encontra aberta o que possibilita que todos os usuários se conectem e consigam navegação com à internet até mesmo pessoas que passam em frente à instituição, causando um grande tráfego inútil na rede. Segundo Levy (2015) esses tipos de rede perdem consideravelmente o desempenho, pois sem nenhum gerenciamento ocasionará uma lentidão na rede e muitas vezes os usuários não conseguem conexão com à internet.

Figura 3 – Topologia rede implementada



Fonte: Próprio autor (2019)

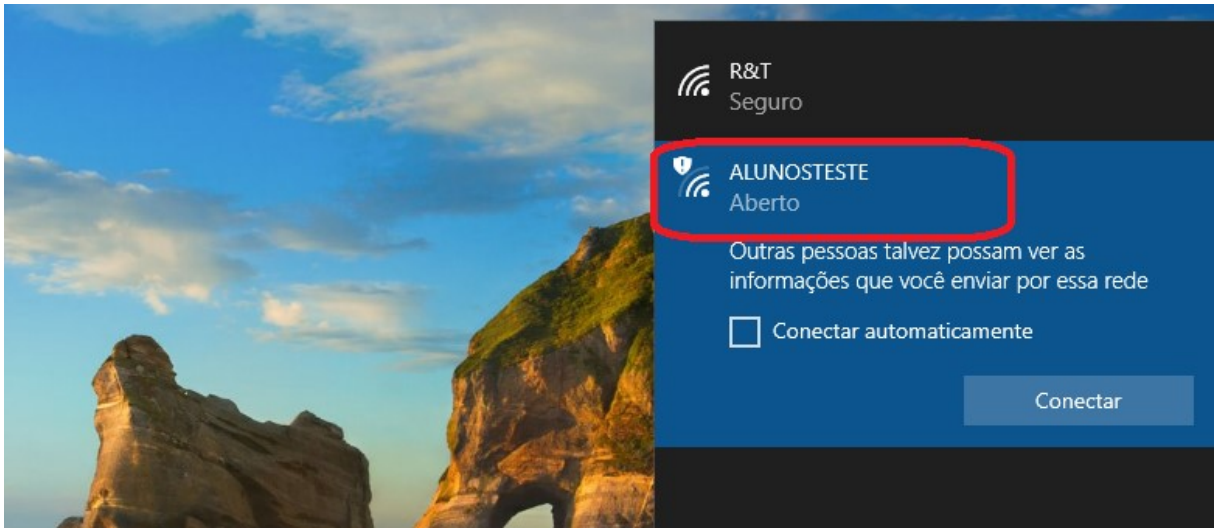
Após a verificação dos erros existentes na atual rede buscamos uma proposta de implementação em que os usuários pudessem ser autenticados através de um servidor externo e a instalação de um *Routerboard* para estar limitando a banda larga utilizada pelos usuários, resultando em um melhor gerenciamento do link de internet recebido e o tornando acessível para todos.

Esse tipo de rede foi escolhido para ser implementado no nosso projeto porque oferece controle de acesso e controle de banda larga, tornando a rede mais segura.

4.2 IMPLEMENTAÇÃO DA REDE WI-FI COM CONTROLE DE ACESSO

Para implementação da rede *Wi-Fi* acessamos o access point via web e configuramos o SSID da rede como “ALUNOSTESTE”, demonstrado na figura 4. Após essa configuração instalamos o software aplicativo FreeRADIUS no *linux debian 9.0,* digitando o seguinte comando no terminal “*apt install freeradius freeradius-utils*”, ao terminar a instalação configurei o arquivo “*/etc/freeradius/3.0/radiusd.conf*”, esse arquivo é responsável por toda a configuração do aplicativo como definição de portas de comunicação e senha de administração.

Figura 4 **–** SSID da rede implementada

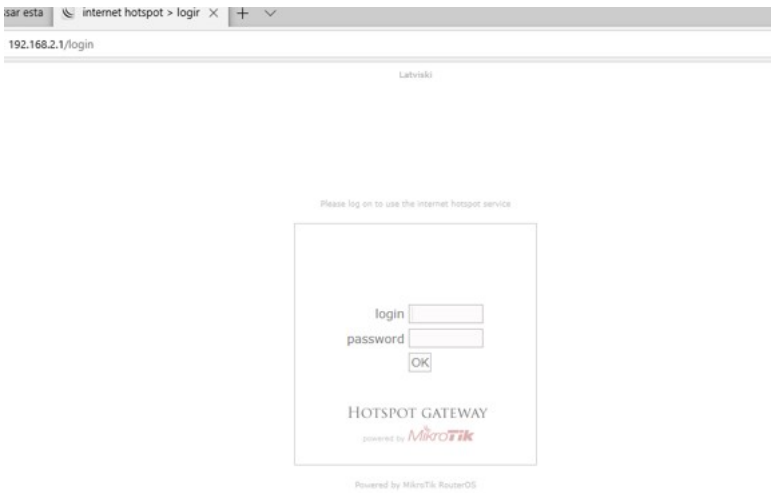


Fonte: Próprio autor (2019)

Podemos verificar que a rede *Wi-Fi* implementada também está aberta, mas ao tentar se conectar o aluno é redirecionado há uma página *Hotspot* de

autenticação e terá que preencher seu usuário e senha, assim como demonstrado na figura 5.

Figura 5 – Página de autenticação



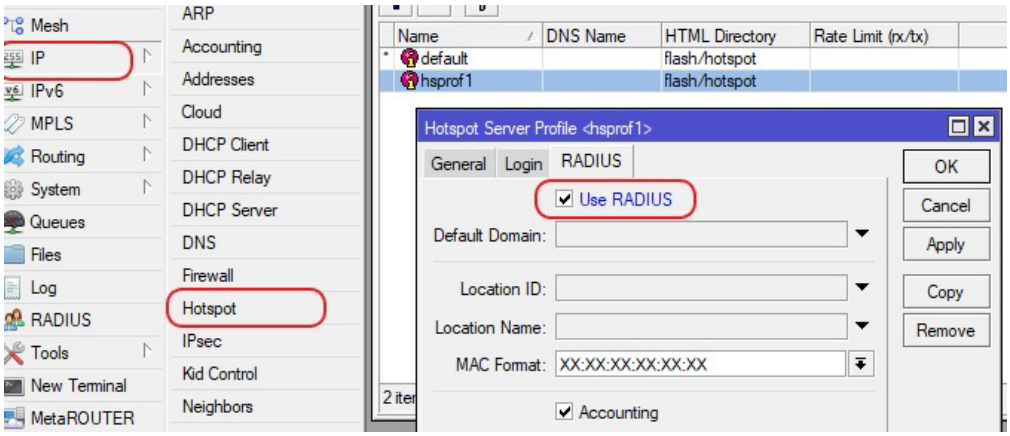
Fonte: Próprio autor (2019)

Após o preenchimento das informações requisitadas, o *Hotspot* envia essas informações para o servidor *FreeRadius* para verificar se as informações estão corretas e se corretas o usuário é autenticado e liberado seu acesso à internet.

4.2.1 Comunicação *Hotspot* e FreeRadius

As figuras 6 e 7 mostram como foi feita a comunicação entre o *Hotspot* e o servidor *FreeRADIUS* possibilitando o envio de informações para autenticação dos usuários e liberação do acesso.

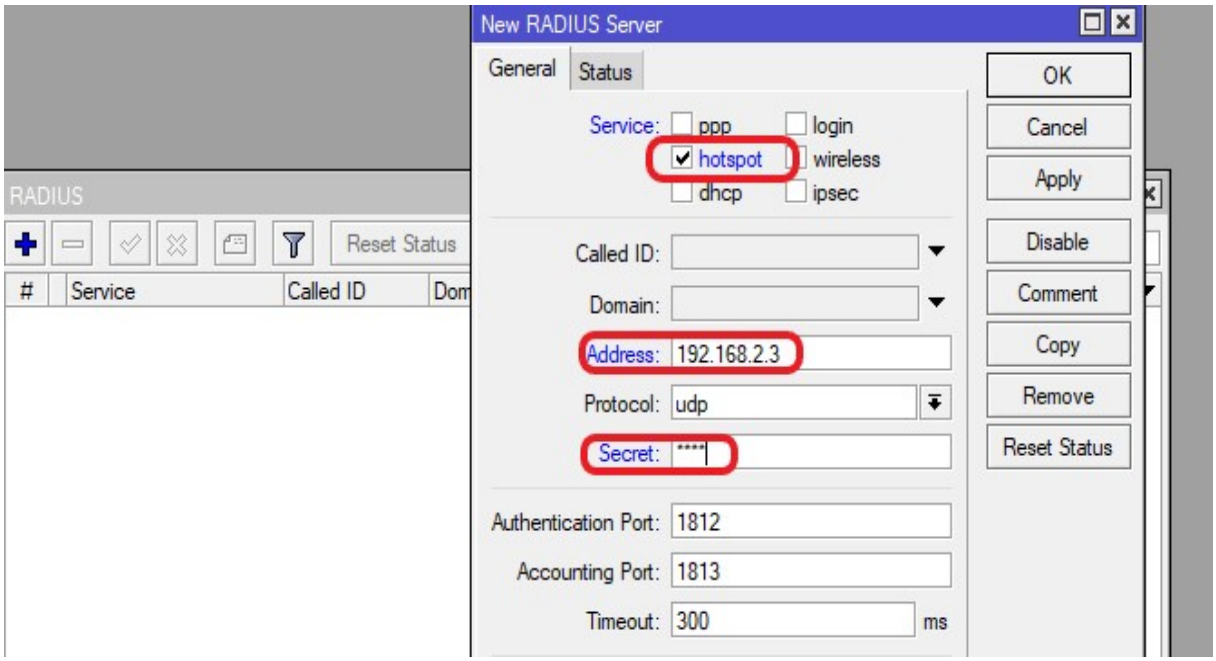
Figura 6 – Comunicação *Hotspot* com *FreeRADIUS*



Fonte: Próprio autor (2019)

Ao acessar o painel de administração do roteador *mikrotik*, naveguel até a aba IP > *Hotspot*, no serviço *Hotspot* marcamos a caixa de seleção Use *RADIUS,* desta forma estaremos informando ao roteador que iremos utilizar um servidor externo para autenticação de usuários, após isso faremos com que o roteador encontre o servidor *RADIUS* na rede para estar realizando as autenticações, como mostra a figura 7.

Figura 7 **–** Direcionamento de informações



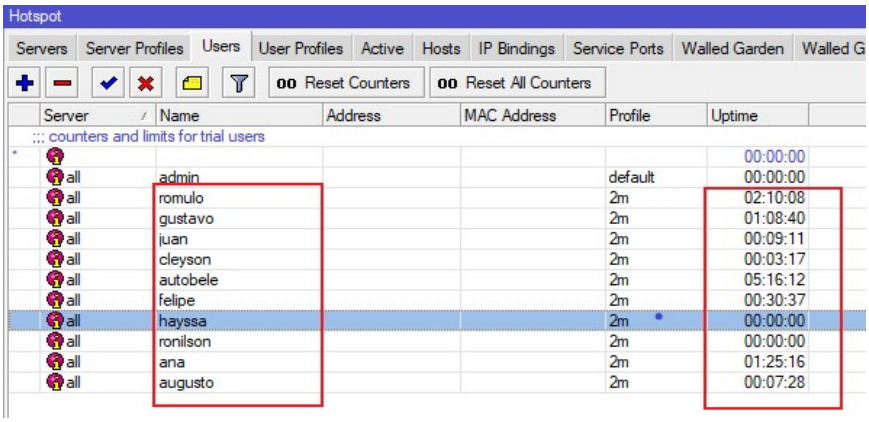
Fonte: Próprio autor (2019)

Na aba *RADIUS* marcamos o serviço *hotspot* informando para o servidor *FreeRADIUS* que esse serviço lhe enviará informações e depois em *Address* e *Secret* informaremos o IP e a senha do servidor *FreeRADIUS* na rede para que o *Routerboard* o encontre e possa estar realizando as autenticações de acesso.

4.2.3 Usuários cadastrados

A Figura 8 e o Gráfico 1 mostram os dez (10) usuários cadastrados para utilização da rede *Wi-Fi* e o tempo médio em que cada usuário esteve conectado, esses usuários foram cadastrados no *RouterBoard Mikrotik* e enviados para o servidor *FreeRadius*.

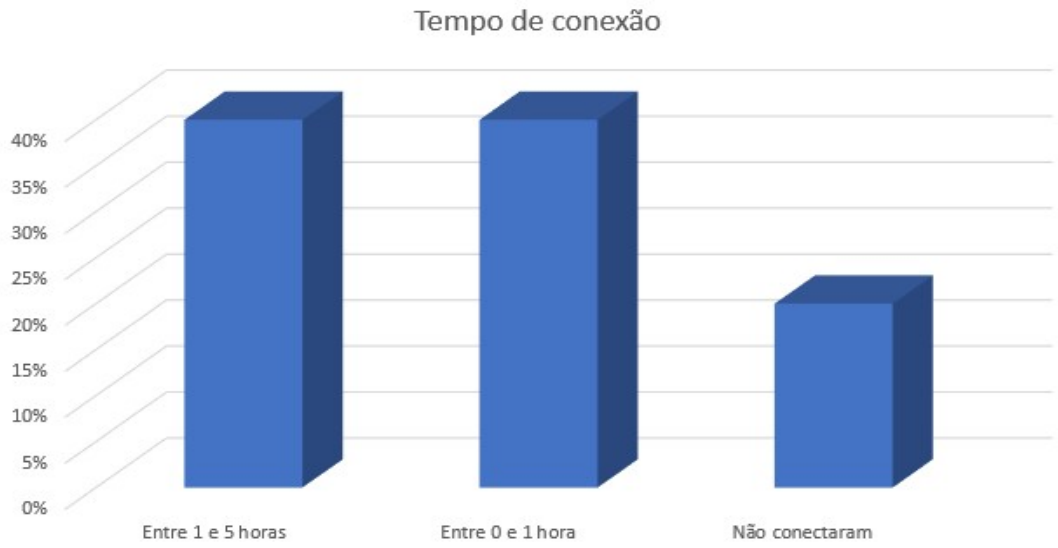
Figura 8 – Usuários cadastrados



Fonte: Próprio autor (2019)

Os dez usuários cadastrados tiveram um tempo total de conexão de 10 horas 19 minutos e 2 segundos. Desse somatório geral, 40% dos alunos tiveram um tempo de conexão entre 1 e 5 horas, 40% entre 0 e 1 hora e 20% não acessaram à internet. Todo esse tempo de conexão impactou em um consumo controlado de banda larga, como demonstrado abaixo.

Gráfico 1 – Tempo de conexão dos usuários



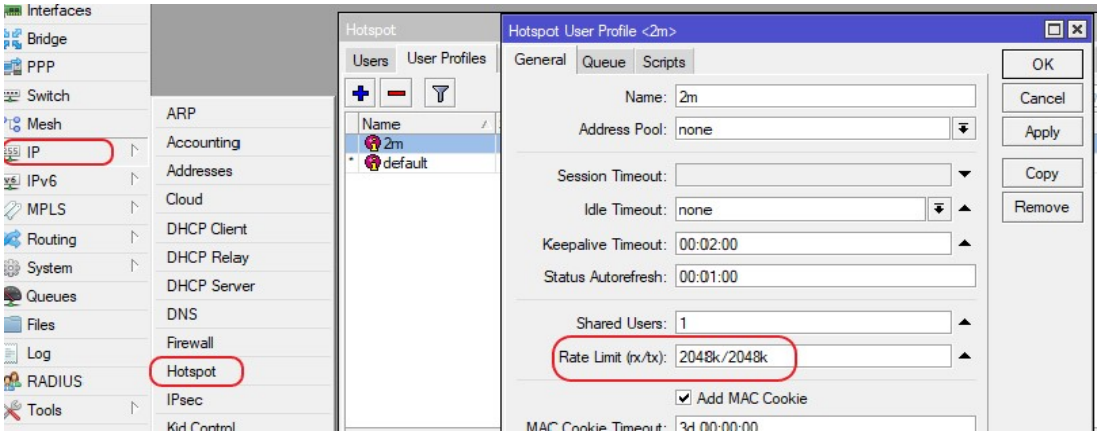
Fonte: Próprio autor (2019)

4.3 CONTROLE DE BANDA LARGA

O controle de banda larga é habilitado no *RouterBoard Mikrotik* acessando a aba *IP>Hotspot* e na aba *User Profiles* na opção *Rate Limit (rx/tx)* definimos a velocidade de banda larga em 2048kbps que foi utilizada pelos alunos, como mostra

a figura 9. Com essa velocidade os alunos geraram um consumo de banda larga mostrado no gráfico 2.

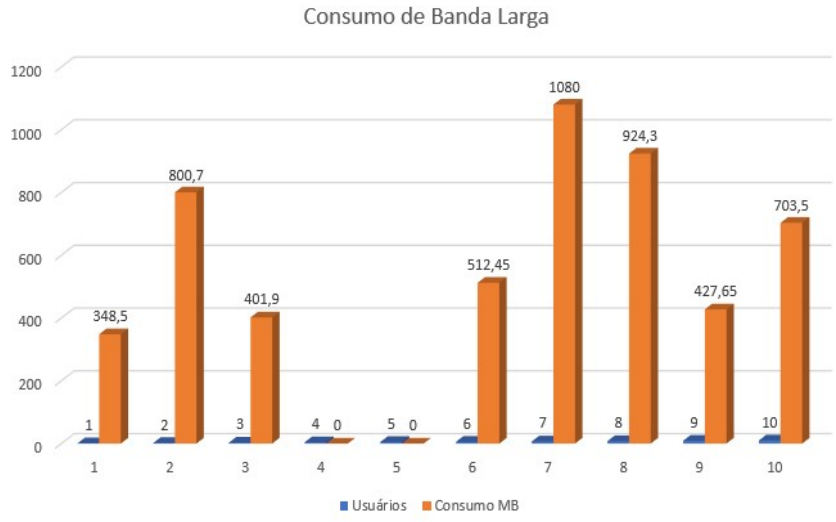
Figura 9 – Controle de banda larga



Fonte: Próprio autor (2019)

Os dez usuários consumiram um total de 5.2 gigabytes de banda larga levando em consideração o envio e recebimento de dados, essa distribuição por usuário pode ser observada no gráfico abaixo.

Gráfico 2 – Consumo de banda larga



Fonte: Próprio autor (2019)

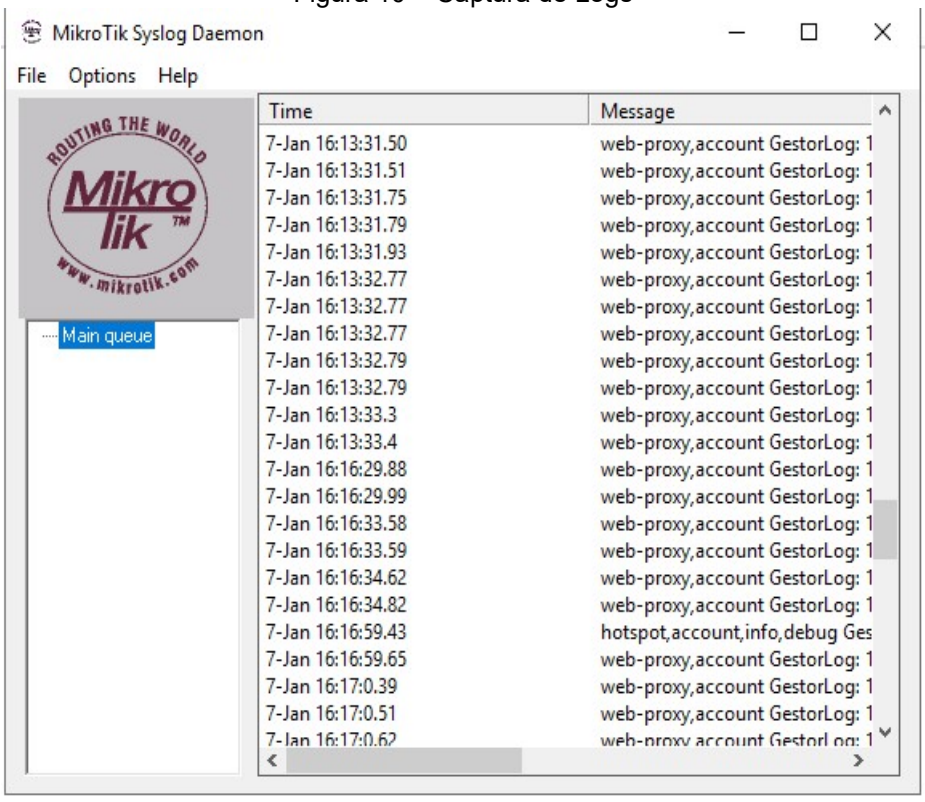
O Gráfico 2 mostra o que cada usuário consumiu no período em que esteve conectado, sendo assim o usuário 1 consumiu um total de 348,5MB; o 2 utilizou 800,7MB; o 3 consumiu 401,9MB; o 4 e o 5 não contabilizaram consumo; o 6 contabilizou 512,45MB; o 7 usou 1080GB; o 8 com 924,3MB; o 9 utilizou 427,65MB

e o 10 acessou utilizando 703,5MB. Todo esse consumo gerou um tráfego total de 7.490.618 pacotes na rede, tendo em média 936.327 pacotes trafegados por dia.

4.3.1 Capturando Logs de dados da rede

O *Routerboard Mikrotik* é capaz de registrar várias informações quando está sendo utilizado e entre elas estão as informações dos usuários cadastrados. Ao habilitar essa função temos a possibilidade de enviar essas informações para um servidor remoto de registros de log, o software Mikrotik Syslog Daemon criado pela própria fabricante do roteador. A Figura 10 demonstra parte dos logs gerados durante a implementação da rede.

Figura 10 – Captura de Logs



Fonte: Próprio autor (2019)

A Figura 11 mostra a ferramenta GestorLog que é uma página web responsável por organizar as informações colhidas no Mikrotik SysLog Daemon, ela demonstra a quantidade de logs gerados e quantitativo em que que cada página foi acessada.

Figura 11 – GestorLog

Fonte: Próprio autor (2019)

Durante o período de implementação foram gerados 56715 logs que contém informações de páginas acessadas, requisições de autenticação e desautenticação de usuários. No gráfico 3 estão os cinco sites mais acessados pelos usuários.

Gráfico 3 – Top 5 dos sites mais acessados

Fonte: Próprio autor (2019)

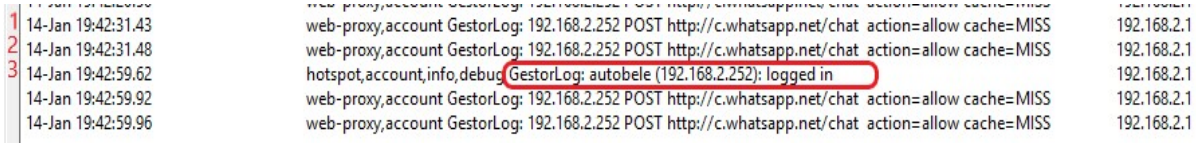
Na Figura 13 podemos observar que o site www.google.com obteve 544 acessos o que representa 20,91% do total acessado, já o site www.whatsapp.com obteve 540 acessos representando 20,75% do total, em seguida temos o site

www.youtube.com com 378 acessos ficando com um percentual de 14,52%, os sites www.globo.com e www.uol.com.br foram os que tiveram menos acessos contabilizando 362 e 242 visitas respectivamente representando um percentual de 13,91% e 9,3% do total, juntos os 5 representam 78,58% do que ~~se~~ foi acessado na rede durante o período disponível.

4.4 OUTROS RESULTADOS

Durante a captura de *logs* foi percebido que o usuário recebe IP antes de realizar a autenticação no servidor *FreeRadius,* nas linhas 1 e 2 da Figura 12 observa-se que ele começa a enviar informações, mas somente na linha 3 que é realizado a autenticação.

Figura 12: Log de conexão



Fonte: Próprio autor (2019)

Essa demora na autenticação se torna um problema, pois ao receber um IP antes de se autenticar um usuário que não é credenciado pode executar qualquer software de captura de informações prejudicando à segurança dos dados dos alunos.

5 CONSIDERAÇÕES FINAIS

Esta pesquisa teve por objetivo a implementação de uma rede *Wi-Fi* infraestruturada para os alunos do IFPI-CATZS visando a correção dos problemas encontrados. Para isso tivemos que definir a topologia que mais se adequa a instituição, implementar um controle de acesso e de banda larga.

Os principais resultados encontrados durante a análise da rede *Wi-Fi* foram: a rede disponível para os alunos encontra-se aberta sem nenhum controle de acesso e de banda larga, deixando - a vulnerável a ataques e com um grande tráfego de dados desnecessários que impactam na indisponibilidade de internet.

A implementação do controle de acesso com o *FreeRADIUS* integrado ao *RouterBoard Mikrotik* com a ferramenta *Hotspot* habilitada mostrou - se eficiente no controle de acesso à internet e ineficiente na segurança da rede pois ao se conectar na rede Wi-Fi o usuário recebe um endereço de IP antes mesmo de realizar a autenticação no servidor FreeRADIUS, podendo executar qualquer ferramenta de captura de dados. O controle de banda larga feito no *RouterBoard Mikrotik* fez com que os usuários cadastrados tivessem um bom acesso à internet com um consumo total de 5,2 gigabytes de dados.

Além da implantação de uma rede *Wi-Fi* infraestruturada para os alunos do IFPI, esta pesquisa teve como contribuição a elaboração de um Manual com todas as configurações feitas na implementação que está disponível no Laboratório LIFE do IFPI-CATZS.

Para trabalhos futuros sugerimos que a rede *Wi-Fi* disponível para os alunos seja implantada com o servidor de autenticação *FreeRADIUS* sem a ferramenta *hotspot* e com a habilitação da ferramenta *Web Proxy* contida no *RouterBoard Mikrotik*, pois com essa ferramenta podemos bloquear o tráfego de dados que possuam conteúdos de caráter ofensivo à instituição.

IMPLEMENTATION OF AN INFRASTRUCTURED WI-FI NETWORK FOR IFPI - CATZS STUDENTS

Abstract

This research aimed to implement an infrastructure Wi-Fi network for IFPI-CATZS students. For that, it was necessary to choose the topology used, the implementation of an access control system and another of broadband. The methodological approach developed in this work was a quantitative analysis and as a technical procedure, action research was adopted. In the results it was possible to define the topology used, the implementation of a FreeRADIUS server integrated to the RouterBoard Mikrotik with the Hotspot tool enabled for access control and broadband control. It is concluded that the infrastructure network deployed through the Hotspot tool is efficient for access control but fails in the security aspect as it provides an IP address before performing authentication on the FreeRADIUS server, and that broadband control is extremely important for the institution, as we observed a bandwidth consumption of 5.2 gigabytes in the implemented network.

Keywords: Infrastructure Wi-Fi networks. Authentication. Broadband.

REFERÊNCIAS

FREERADIUS. **Overview and Features**. 2015. Disponível em: <https://wiki.freeradius.org/Overview-and-Features>. Acesso em: 27 jun. 2021.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de pesquisa**. 1 ed. [S.l.]: Plageder, 2009.

LEVY. Guilherme. **Gerenciamento de uma rede pública utilizando a ferramenta hotspot do sistema operacional Routeros**. 2015. Disponível em: <http://200.150.122.211:8080/jspui/bitstream/23102004/86/1/TCC%20Tads%20-%20Guilherme%20Levy.pdf>. Acesso em: 27 jun. 2021.

MEDEIROS, Roger C. **Implementação de um modelo de segurança para rede sem fio WPA2-EAP**. 2017. Disponível em: <http://bibliodigital.unijui.edu.br:8080/xmlui/bitstream/handle/123456789/4574/Roger%20Casagrande%20de%20Medeiros.pdf?sequence=1>. Acesso em: 27 jun.2021.

MIKROTIK. **Documentation**. Disponível em: <http://wiki.mikrotik.com/wiki/Main_Page>. Acesso em: 27 jun. 2021.

MORAIS, Giovane. **Segurança da informação através de autenticação centralizada por IEEE 802 1x baseada em protocolo RADIUS e base de dados LDAP aplicada à redes sem fio**. 2017. Disponível em: <https://www.aedb.br/seget/arquivos/artigos16/3024238.pdf>. Acesso em: 27 jun. 2021.

MORIMOTO, Carlos E. **Redes Guia Prático**. 2ª Ed. Porto Alegre RS: Sul Editores, 2011. 243 p.

PAIM, Rodrigo R. **Wep, Wpa e Eap**. 2011. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/trabalhos_vf_2011_2/rodrigo_paim>. Acesso em: 27 jun. 2021.

RICHARDSON, R. J. **Pesquisa social**: métodos e técnicas. São Paulo: Atlas, 1999

RODRIGUES, Ligia P. **Análise e desempenho de redes de acesso sem fio**. 2011. Disponível em: <https://www.feis.unesp.br/Home/departamentos/engenhariaeletrica/pos-graduacao/287-dissertacao_ligia_rodrigues_pretel.pdf>. Acesso em: 27 jun. 2021.

RUFINO, Nelson. **Segurança em redes sem fio**. 2005. Disponível em: <https://s3.novatec.com.br/capitulos/capitulo-9788575222430.pdf>. Acesso em: 27 jun. 2021.

SILVA, Eduardo S. **Pesquisa e análise dos protocolos de segurança nas implementações de redes utilizando o padrão IEEE 802.11**. 2011. Disponível em:

<http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/402/1/CT_GESER_1_2011_10.pdf>. Acesso em: 27 jun. 2021.

TANEMBAUM, Andrew S. **Redes de Computadores**. 4 ed. Rio de Janeiro RJ: Elsevier, 2003. 23 p.

THIOLLENT, Michel. **Metodologia da Pesquisa-Ação**. 18 ed. São Paulo: Cortez, 2011.

TORRES, Gabriel. **Redes de Computadores**. Vila Isabel RJ: Novaterra, 2019. 35 p.

VOITECHEN, Daianara A. **Análise e comparação de algoritmos para criptografia de imagens**. 2015. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/6438/1/PG_COADS_2015_2_03.pdf>. Acesso em: 27 jun. 2021.