UNIVERSIDADE PAULISTA

EDUARDO GABRIEL DOS SANTOS

ESTUDO DE CASO PARA DISPONIBILIDADE DE ACESSO DE DADOS GRATUITO EM ÁREAS PÚBLICAS.

LIMEIRA

2018

EDUARDO GABRIEL DOS SANTOS

ESTUDO DE CASO PARA DISPONIBILIDADE DE ACESSO DE DADOS GRATUITO EM ÁREAS PÚBLICAS.

Trabalho de conclusão de curso para obtenção do título de graduação em Ciência da Computação apresentado à Universidade Paulista – UNIP

Orientadores: Prof. Me.Antonio Mateus Locci; Prof. Me. Sergio Eduardo Nunes.

LIMEIRA

2018

EDUARDO GABRIEL DOS SANTOS

ESTUDO DE CASO PARA DISPONIBILIDADE DE ACESSO DE DADOS GRATUITO EM ÁREAS PÚBLICAS.

Trabalho de conclusão de curso para obtenção do título de Graduação em Ciência da Computação apresentado à Universidade Paulista - UNIP

Banca examinadora

_____

Prof. Dr.

_____

Prof. Dr.

RESUMO

Atualmente tem havido um aumento na demanda por conexões a dispositivos móveis, pois há uma facilidade de compra de aparelhos que já possuem acesso à internet, portanto vários estabelecimentos e órgãos públicos são obrigados a liberar uma conexão gratuita para atender a essa demanda , mas não estão se conscientizando que ao acabar liberando este acesso estará gerando alguns riscos tanto para o usuário quanto para aqueles que disponibilizam, sejam eles de roubo de informação ou mesmo processos, pois quem disponibiliza é parcialmente culpado por toda ação dentro de sua rede , por facilitar o acesso a esse usuário mal intencionado, o foco deste projeto não estaria apenas na segurança, mas também na estabilidade da conexão, pois dependendo da quantidade de acessos ou interferências causadas no local, este sinal pode ser lento ou ficar até mesmo indisponível. Esse TCC é destinado aos municípios devido à falta de conhecimento sobre a liberação desse sinal e ao fato de estarem sancionando leis para forçar esses órgãos a liberar tal acesso a população, uma lei já promulgada é a Lei nº 16.685 dez de julho de 2017 que foi direcionado para a cidade de São Paulo, já obrigando a liberar essa conexão e devido a essa demanda não demorou muito para ter outras leis promulgadas para outros municípios, para esse fim, um projeto foi concebido orientando os riscos de uma rede aberta, tanto para o usuário quanto para aqueles que também fornecem as etapas necessárias para construir uma rede segura e estável e também para demonstrar os equipamentos que fornece resultados e os meios para se proteger dos processos e garantir ao usuário uma conexão segura. Projeto aplicado na prefeitura municipal de araras em abril de 2017 até o presente momento novembro de 2018, sem possíveis invasões ou instabilidades relatadas, conclui-se que o projeto teve as etapas bem elaboradas e pode ser bem utilizado pelas prefeituras e também por pessoas e empresas que duvidam dos riscos e meios para implementar uma rede segura e estável.

Palavras-chave: Firewall; HotSpot; Proxy; Servidores; Wifi.

ABSTRACT

Currently there has been an increase in the demand for connections to mobile devices, as there is a facility to buy handsets that already have access to the internet, so several establishments and public agencies are required to release a free connection to meet this demand, but they are not being aware that end up releasing this access will generate some risks for both the user and those who make available, whether they are information theft or even processes, because those who make available is partially guilty of any action within their network, for facilitating access to this malicious user, the focus of this project would not only be on security but also on the stability of the connection, because depending on the amount of hits or interferences caused in the place, this signal can be slow or even unavailable. This Tcc is destined to the municipalities due to the lack of knowledge about the liberation of this signal and to the fact that they are sanctioning laws to force these organs to liberate such access to the population, a law already promulgated is the Law nº 16.685 of July 10, 2017 that was directed to the city of São Paulo, already obliging to release this connection and due to this demand did not take long to have other laws promulgated for other municipalities, for that purpose, a project was designed guiding the risks of an open network, both for the users as well as those who also provide the steps necessary to build a secure and stable network and also to demonstrate the equipment that provides results and the means to protect the processes and ensure the user a secure connection. Project applied in the municipal prefecture of macaws in April 2017 until the present time November of 2018, without possible invasions or instabilities reported, it is concluded that the project had the stages well elaborated and can be well used by the city halls and also by people and companies who doubt the risks and means to implement a secure and stable network.

Keywords: Firewall; Hot spot; Proxy; Servers; Wifi.

LSTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS

3G	Terceira Geração
AES	Advanced Encryption Standard
AP	Access Point
CPF	*Cadastro de Pessoa Física*
DNS	Domain Name System
ETH	Ethernet
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IEEE	Institute of Electrical and Electronics Engineers
IIS	Internet Information Services
IP	Internet Protocol
OSI	Open Systems Interconnection
P2P	Peer to Peer
PSK	Pre-Shared Key
SSH	Secure SHell
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WIFI	Wireless Fidelity
WIMAX	Worldwide Interoperability for Microwave Access
WPA2	Wi-Fi Protected Access 2

SUMÁRIO

INTRODUÇÃO

Atualmente à acessibilidade a informação tornou-se tão fácil quanto prática, todo e qualquer recurso estão disponíveis na palma de nossas mãos, por isso ficamos à mercê deles. Assim a conexão com a internet tem que ser prática, com essa necessidade, estabelecimentos e órgãos públicos liberam acessos à internet para atender essa demanda sem ter um conhecimento adequado para tal, desconhecendo os riscos que os usuários e até mesmo quem disponibiliza esse sinal possa passar. A partir disto foi proposto um uso de dados livre, de qualidade, através de um simples projeto de baixo custo em longo prazo direcionado a órgãos públicos, devido a ter leis que obrigam essa liberação e com o desconhecimento desses órgãos sobre os risco que geram ao disponibilizar essas redes. Neste sentido para evitar riscos para o usuário e assegurar o disponibilizador houve a realização de um projeto, começando com alguns estudos referentes a redes sem fio, foram verificados grande parte dos pontos que geram brechas e instabilidades nessas redes, para assim poder disponibilizar o melhor sinal no local desejado.

Nestas perspectivas para essa aplicação, diversas etapas foram necessárias, como: termo de uso, licenciamento, cuidados, ponto de acesso, verificação da área, estudo da largura de banda[1], cache[2], servidor de log[3], autenticação, servidor de cadastros e os resultados. O trabalho teve como base o projeto desenvolvido e aplicado pela Prefeitura Municipal de Araras sendo este disponibilizado na Praça Barão de Araras.

[1] Largura de Banda ou BandWidth é a capacidade de transmissão de uma rede, determinando a velocidade trafegada naquela rede
[2] Cache refere se a uma área que contenha uma cópia temporária de determinado dados gravados
[3] Log são eventos salvos, podendo ser sites acessados ou registros de um endereço entre outros.

1 OBJETIVO

O objetivo deste trabalho foi desenvolver uma estrutura simples e eficaz para conexões sem fio gratuitas com o intuito de minimizar os impactos causados por uma má gestão de uma rede sem fio, voltado para áreas públicas com o intuito de disponibilizar conexões gratuitas para população a rede mundial de computadores, evitando transtornos para o usuário em caso de redes sem fio inseguras, assim sendo descrito todos os passos necessários que se deve seguir para disponibilizar uma conexão estável e confiável, sendo um projeto aplicado e com resultados.

1.1 Justificativa

Devido ao crescimento exponencial da integração da população a rede mundial de computadores, a liberação de pontos de acessos à internet aumentou nos últimos tempos, tornando uma jogada de *marketing*, porém os responsáveis por liberarem esses pontos não possuem conhecimento dos riscos referente a esse acesso, com isso a uma fragilidade na segurança dessas redes sem fio, onde também não é de conhecimento do usuário a importância dessa segurança. Com o intuito de orientar e demostrar, foi elaborado um projeto exibindo os riscos e como aplicar uma rede sem fio de maneira correta, visando à segurança, confiabilidade e respaldo jurídico e civil, que possa acontecer em alguns casos, voltado a prefeituras porem também podendo ser aproveitado por empresas privadas, para sanar dúvidas em relação a preocupações e meios com resultados a serem aderidos.

1.2 Metodologia

Estudo de área analise de taxa de conexão e banda, pesquisas sobre licenciamento e processos civis e jurídicos, visando o conhecimento dessas partes para respaldos de possíveis atuações referentes à suas áreas. Definições de segurança e prevenção de possíveis ataques e indisponibilidade do serviço, orientação a métodos de autenticação e

registros de dados, como logs e informações para beneficiar o órgão público e também para respaldas.

2 PERPECTIVAS PARA O FUTURO

Com o grande crescimento das massas, várias cidades e estados veem a internet como um serviço essencial, com isso sancionam leis para a liberação obrigatória desse serviço, porem poucos deles sabem sobre a usabilidade desse acesso e seus riscos, ao obrigaram prefeituras entre outras autarquias, essas entidades se veem sem saída onde acabam errando em suas escolhas, liberando deliberadamente esse acesso para população, alguns órgãos públicos são conscientes do uso e optam pela contratação de empresas competentes para realização e instalação desse serviço, que por sua vez acaba não sendo tão barato, podendo ter custos mensais. Esse tcc visa demonstrar os pontos principais para elaboração de um projeto acessível para esses órgãos, evitando gastos desnecessários e tendo uma segurança e controle do conteúdo liberado.

Com esse crescimento está surgindo projetos de lei que obrigam esses órgãos a distribuírem esse acesso, há um projeto de lei já promulgada é o projeto de Lei nº 16.685, de 10 de julho de 2017, obrigando todos os órgãos públicos da cidade de São Paulo a liberarem acesso gratuito a população, com isso pode se perceber que não que não irá demorar muito para promulgarem outras leis com o mesmo sentido para outros municípios, tendo eles uma carência na área de informática e liberando esse acesso sem o consentimento adequado e conhecimento dos riscos que podem ter.

3 LICENCIAMENTO DO SERVIÇOS DISTRIBUÍDO

Antes de iniciar um projeto para disponibilizar acesso sem fio, há uma preocupação com a homologação na ANATEL, esse licenciamento é necessário para a autorização da disponibilização desse acesso, há alguns pontos para se preocupar em relação a isso e meios para regularizar, serão descritos logo mais os passos a serem aderidos.

3.1 Licença Serviço e Comunicação Multimídia (SCM)

Licença SCM foi criado em 2016 com o intuito de barrar empresas clandestinas que disponibilizam serviços de telecomunicação, a fim de deixar igualitária a disputa entre as empresas que disponibilizam tal serviço, sendo assim o responsável por essa rede tem que se legalizar conforme as diretrizes da ANATEL, após o licenciamento será adquirido à licença de SCM, responsável por permitir a liberação desse serviço.

Essa licença é necessária para algumas tecnologias sendo elas *WIMAX*, *3G*, *WIFI* e *MESH*, para as tecnologias *WIMAX* e *3G* é obrigatório o licenciamento tanto na frequência 2.4GHz e 5GHz, já as tecnologias *WIFI* e *MESH* são necessários apenas para as cidades com mais de quinhentos mil habitantes. Porem para esse licenciamento obrigatório, caso o responsável tenha até cinco mil usuários, ele estará isento, pois, a ANATEL aprovou dia 22 de junho de 2017, a isenção desse licenciamento.

Os equipamentos utilizados neste projeto já são homologados pela ANATEL e a tecnologia utilizada é o *MESH* responsável por disponibilizar o acesso sem fio.

Caso seja necessário retirar a licença consultar o passo a passo no apêndice deste trabalho.

4 TERMO DE USO

Com a dimensão da rede global de dados, fica praticamente impossível filtrar todos os sites e acesses ilícitos, vulgares e também ofensas e agressão verbais recebidas por usuários navegantes, segundo o artigo 7 da lei do Marco Civil da Internet no Brasil as informações tem que ser claras sobre armazenamentos, uso, tratamentos e usos pessoais, sendo descritas no termo de uso. Com isso é de suma importância à elaboração concisa e bem clara de um termo de uso aos utilizadores, ele será utilizado para isentar de quaisquer mal-uso de quem estará disponibilizando. Assim tendo que deixar claro em seu termo de uso, toda e qualquer condição, quanto mais detalhada melhor, para possíveis respaldos de ações e medidas judiciais que possam prejudicar. Sendo essencial para a liberação de acesso sem fio gratuito.

5 EQUIPAMENTOS PARA O PONTO DE ACESSO

Após o licenciamento e a elaboração do termo de uso há uma necessidade em verificar a disponibilidade de um ponto de acesso capaz de suportar várias conexões simultâneas e com distância aceitável, neste projeto foi utilizado um roteador de alto desempenho *UBIQUITI UNIFI MESH PRO*, o mesmo tem um alcance de 180 metros de diâmetro e capaz de velocidades de até 450 Mbps em redes 2.4GHz e 1300Mbps em redes 5GHz.

Para este projeto foi utilizado dois desses roteadores da *UBIQUITI*, para obter ponto de acesso entre esses dois equipamentos, foi aplicado dois rádios *UBIQUITI ROCKET M5*, sendo um *AP* e uma estação, eles são responsáveis por fazer a interação entre esses roteadores e disponibilizar a conexão de internet para os usuários.

6 VERIFICAÇÃO DA ÁREA DE APLICAÇÃO

Ao definir os equipamentos para área a ser aplicada, assim para definir os pontos de instalação para um melhor desempenho desses equipamentos, foi utilizado o *UNIFICONTROLLER*, com ele é possível montar um ambiente virtual de teste, com ele pode se definir a área desejada e aplicar aparelhos de sua linha, assim tendo uma prospecção do sinal que será disponibilizado, isso torna o trabalho mais viável, sem ter a necessidade de todo o trabalho manual testando os melhores pontos, mas sempre se atentando a possíveis interferências do local, porém há uma necessidade do estudo da área para mapear os pontos que possua uma estrutura adequada, sendo ela de energia e local apropriado para fixar os equipamentos.

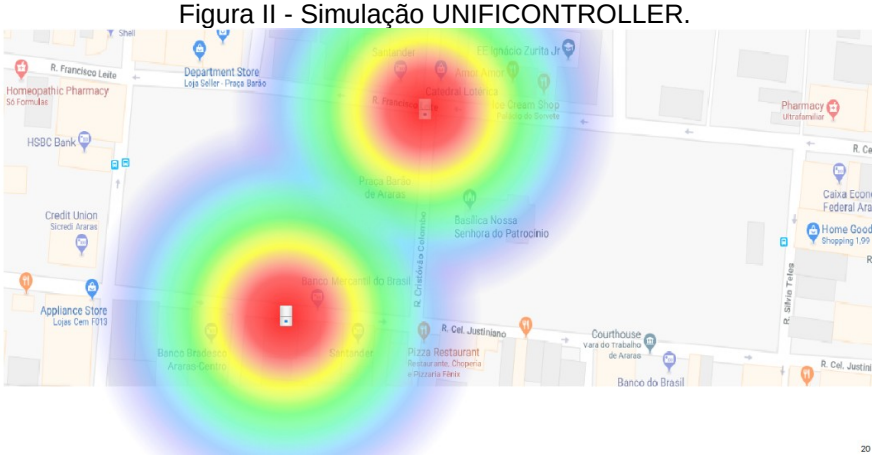
Na primeira fase do projeto foi especificada a área solicitada com maior fluxo de pessoas e direcionadas a abranger eventos no local, sendo representada na figura I.

Figura I - Área Solicitada.

Fonte: https://www.google.com.br/maps/@-22.3576232,-47.3862313,17.5z

Após saber em que a área será aplicada, foi verificado a área em qual contenha energia e local adequado para fixar os roteadores, após isso foi mapeado virtualmente com o software *UNIFICONTROLLER*, para verificar se atendia a área solicitada, assim como exibido na figura II está atendendo toda a área solicitada.

Figura II - Simulação UNIFICONTROLLER.



Fonte: https://www.google.com.br/maps/@-22.3576232,-47.3862313,17.5z

Sendo os roteadores aplicados no local exibido acima e testado abrangendo toda a área mapeada.

7 ESTUDO DO CANAL, MODO E LARGURA DA BANDA

Um estudo da banda no local a ser aplicado é necessário para buscar o melhor desempenho da rede a ser disponibilizada, tendo como foco identificar possíveis interferências relacionadas ao sinal, às mesmas causam lentidões e até mesmo indisponibilidade do serviço, devido a isso a uma necessidade desse estudo efetivo do local onde será aplicado, assim após obter esses dados é possível configurar o equipamento de forma correta minimizando as interferências que há no local.

7. 1 Interferência

Com o crescimento do uso de sinais sem fio surgiu uma preocupação, a poluição das ondas de frequências geradas pelos roteadores, onde pode se ter alguns tipos distintos de interferência, causando lentidão e às vezes indisponibilidade, assim neste projeto citamos os três tipos conhecidos e como evita-los, eles são.

7.1.1 Co-channel

Esse tipo de interferência é comum entre roteadores que trabalham no mesmo canal, assim as ondas geradas por roteadores próximos a instalação se chocam diminuindo o tempo de resposta para cada requisição feita por um utilizador, ela é bem comum porque os roteadores são pré-configurados com canais padrão, assim terá uma alta possibilidade de coincidir de estarem no mesmo canal assim sendo representado esse tipo de interferência na figura III.

Figura III - Interferência Co-Channel.

Fonte: https://www.netspotapp.com/wifi-channel-scanner.html

7.1.2 Canal adjacente

Esse tipo de interferência é causado quando possui vários equipamentos próximos, mesmo eles trabalhando em canais diferentes, pode haver a interferência de canais adjacentes, são quando causam ruídos nas faixas próximas a que foi escolhida, assim esse ruído gera um excesso nas requisições feitas para o roteador, demorando o tempo de resposta dessas requisições como podemos ver na figura IV.

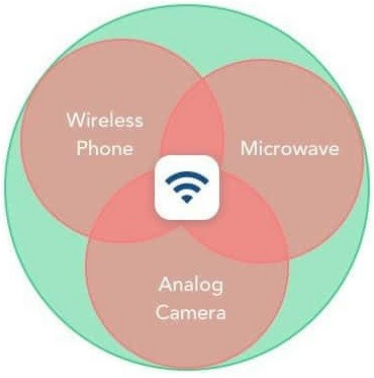
Figura IV - Interferencia Adjacent Channel.

Fonte: https://www.netspotapp.com/wifi-channel-scanner.html

7.1.3 Non Wifi

Essa interferência é causada por qualquer equipamento que utiliza a frequência de 2.4GHz, como *bluetooth*, micro ondas entre outros e também redes elétrica que pode causar instabilidade na rede sem fio distorcendo as ondas geradas, porem em áreas abertas esse tipo de interferência é mais difícil de acontecer, mas caso haja a necessidade de replicar em ambientes fechados, se atentar a esses equipamentos que trabalham na mesma frequência, exemplo na figura V.

Figura V - Interferência Non Wi-Fi.



Fonte: https://www.netspotapp.com/wifi-channel-scanner.htm

7. 2 Estudo da Largura de Banda

Atualmente os roteadores trabalham em duas larguras de banda, conhecidas como bandwidth, elas são responsáveis por determinar quantos canais estará disponíveis para seu roteador trabalhar, sendo elas 20 MHz e 40MHz, quando se escolhe a largura maior sendo de 40 MHz ela é mais veloz que a de 20 MHz porem essa largura sofre mais interferência, definir uma largura manual dependera muito do local em que está querendo aplicar, caso seja um local com pouca interferência o ideal seria usar a largura de 40MHz por ser mais rápida, caso esteja em um ambiente que sofra muita interferência o ideal será a largura de 20MHz, mesmo sendo mais lenta, seu desempenho será melhor devido a largura da banda também ser menor e sofrer menos interferência do local, fazendo com que os pacotes que são transmitidos entre utilizador e roteador sejam recebidos bem mais rápidos. Assim com esse estudo do ambiente será possível escolher sempre a melhor opção visando o desempenho de sua rede sem fio.

7.2.1 Especificações do Padrão IEEE 802.11

Toda conexão sem fio trabalha em um padrão que segue especificações, sendo ele o padrão IEEE 802.11, ele estabelece normas para criação e para o uso dessas redes sem fio. Atualmente há alguns padrões mais usados pelos equipamentos que utilizam redes sem fio, nos quais são mostrados no quadro I, demonstrando a frequência, largura da banda e velocidade que trabalham.

Tabela I - Padrão de Protocolos IEEE

Protocolo	Frequência em GHz	Largura de banda (MHz)	Velocidades de transferência (MB/s)
802.11a	5	20	54
802.11b	2.4	20	11
802.11g	2.4	20	54
802.11n	2.4/5	20 /40	300
802.11ac	5	80	1300

Fonte: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2412/1/CT_GESER_IV_2014_03.pdf

Os roteadores veem com padrão selecionado a opção auto para a escolha desses protocolos, porém caso haja um equipamento que utiliza o padrão mais inferior, à rede se nivelara nesse padrão, assim deixando alguns equipamentos instáveis e com a conexão insatisfatória.

O utilizado neste projeto é a intercalação dos padrões 802.11g, 802.11n e 802.11ac, por serem os mais rápidos e mais atuais, descartando duas primeiras opções de protocolos. Assim equipamentos que só utilizam o padrão 802.11b e 802.11a não conseguirão conectar se a rede, tendo em vista que são equipamentos obsoletos e que apenas prejudicarão a rede, sendo priorizada uma rede mais estável e rápida.

7.2.2 Estudo do Canal

Dependendo da região que estará, terá uma quantidade de canais para trabalhar, onde a região do Brasil possui 13 canais, os canais que trabalham na largura de banda de 20MHz tem sua largura de 22MHz por canal, assim tendo uma baixa taxa de dados transmitida, e os que trabalham na bandwidth de 40MHz utilizam dois canais adjacentes de 20MHz assim tendo uma maior taxa de dados para transmitir, mesmo sendo maior pode se ter também maior interferência no canal escolhido, pelo fato de usar dois canais adjacentes, assim as vezes não sendo viável o uso.

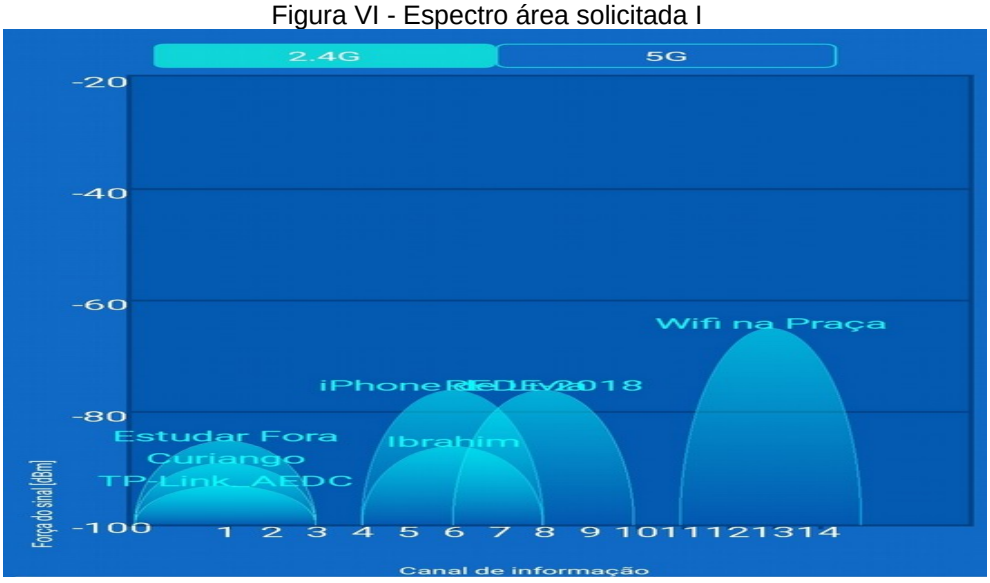
Com o desconhecimento desses canais, muito das vezes não são configurado o canal com menos interferência, assim eles trabalham em canais padrões sendo eles 1, 6 ou 11, devido a serem canais que não se sobrepõe entre os demais canais, caso selecione canais diferentes desses, mesmo que

não haja outro equipamento no mesmo canal, mas haja em canais adjacentes terá uma interferência sendo causada, assim gerando uma instabilidade na rede, para que isso seja minimizado ou sanado há uma necessidade do estudo dos canais dessas áreas.

7.2.3 Realização dos estudos

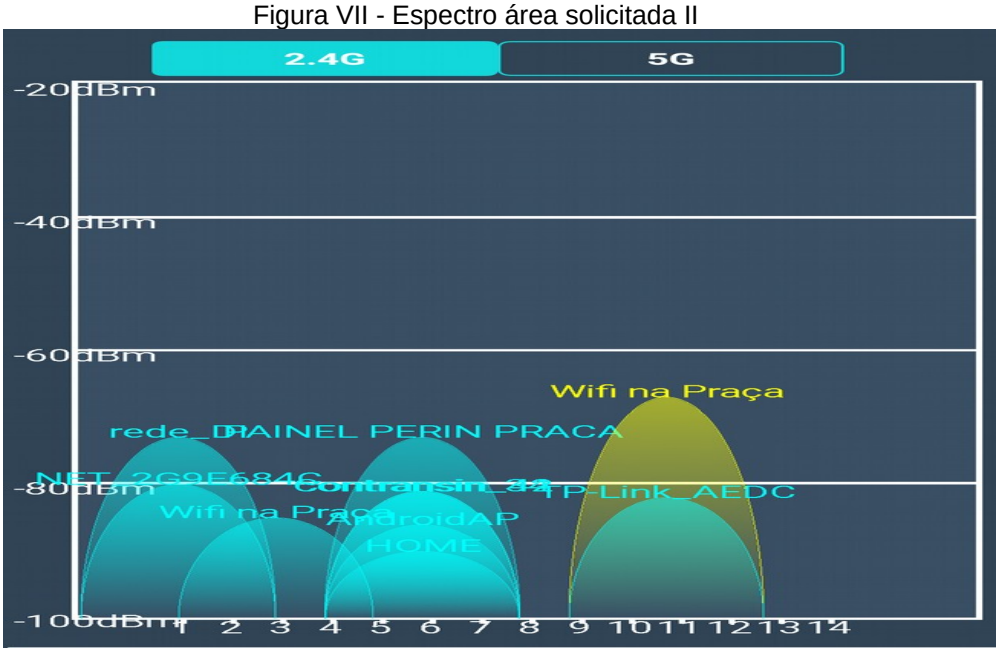
Para poder escolher o melhor cenário para o ambiente foi utilizado o aplicativo *WIFIANALAYZER* ele é responsável por mostrar todos os canais que estão ativos no momento, assim com o conhecimento de cada parte desse estudo foi possível determinar a melhor frequência, melhor largura e modo para o equipamento, assim eliminando e diminuindo grande parte da interferência causada por outros equipamentos ao redor, mantendo uma rede mais estável. Como demonstra figura VI com o espectro do local aplicado, exibindo o canal em que as redes sem fio do local está trabalhando, a do projeto aplicado é a de nome (Wifi na Praça).

Figura VI - Espectro área solicitada I



Fonte:O Autor

Figura VII - Espectro área solicitada II



Fonte:O Autor

Assim podendo verificar que na figura VI não há interferência no local e na segunda devido a quantidade de equipamentos no local, ah uma interferência como demonstrado na figura VII, assim sendo definido a largura de banda para o primeiro roteador de 40MHz e para o segundo 20MHz para minimizar as interferências sofrida no local, mesmo com a velocidade reduzida terá melhor desempenho devido a largura da banda ser menor sofrendo menos interferência e o pacote chegando mais rápido ao roteado e assim vice e versa, o canal configurado nesse projeto foi o canal 11 para o primeiro roteador e para o segundo o canal 3, o padrão 802.11g\n\ac visando uma rede mais estável e rápida.

8 SEGURANÇA

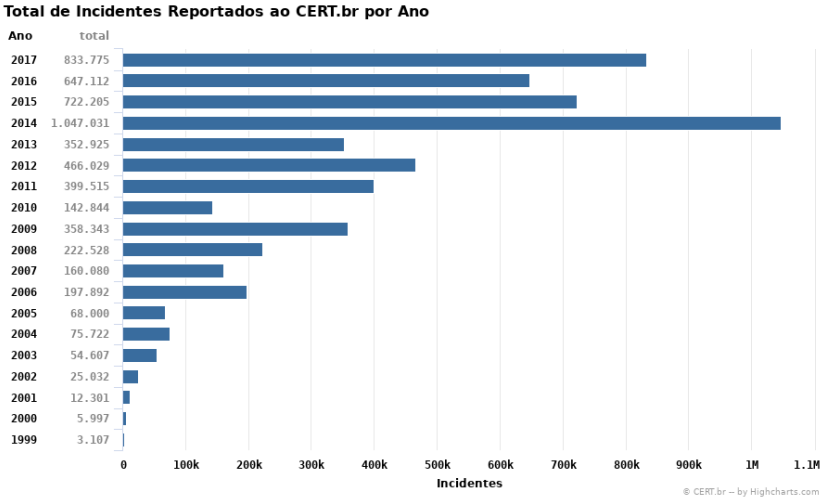
Após a aplicação dos equipamentos e sua configuração para diminuir as interferências do local outro ponto importante do projeto é a segurança da rede sem fio gratuita, pois com ela é gerada a confiabilidade, sendo responsável diretamente pela satisfação do usuário, assim caso haja uma invasão ou algo que prejudique o utilizador, essa rede perdera completamente sua confiabilidade, assim tendo uma drástica redução do uso e críticas negativas em relação ao serviço distribuído. Sendo um ponto crucial devido a facilidade dos invasores e atacantes de roubar alguma informação dos equipamentos que estão na mesa rede, pois segundo Emilio Tissato Nakamura e Paulo Lício de Geus.

> “Basta que esteja dentro da área de cobertura de cada tecnologia para que os pacotes cheguem até ele, e este possa ler, modificar ou inserir novos pacotes” (SEGURANÇA DE REDES, 2004, p.125).

Assim demostrando uma fragilidade enorme em redes sem fio, necessitando se atentar bem a segurança da rede.

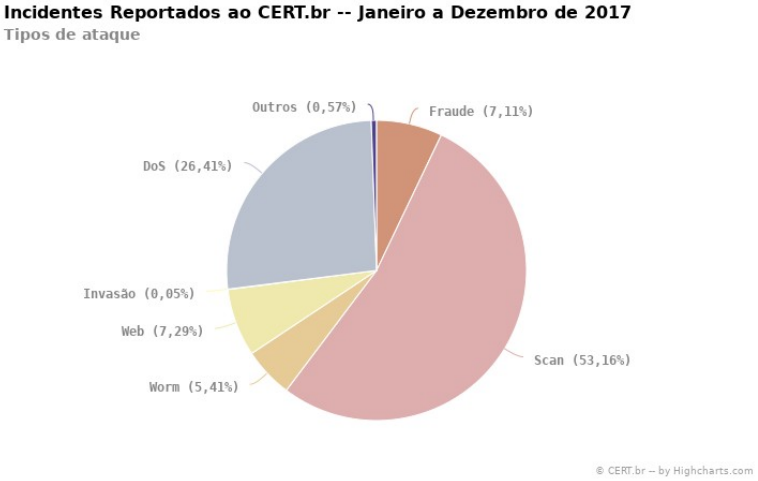
Segundo o livro segurança máxima(2001) o atacante pode comprometer qualquer sistema, podendo roubar dados pessoais, como contas bancarias, cartões de credito ou até mesmo utilizar o telefone da vítima para monitorar seus movimentos e rotinas diárias. Ao analisar as figuras do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil sendo elas as figuras IX e figura X, os incidentes de janeiro a dezembro de 2017, demostra os tipos de ataques e os ataques por portas, a figura VIII demonstra o total de invasões no período de 1999 a 2017, podendo verificar que os incidentes de invasões está cada vez maior e com isso deve se preocupar com a segurança da rede devido a esse aumento.

Figura VIII - Total de Incidentes Reportados ao CERT.br



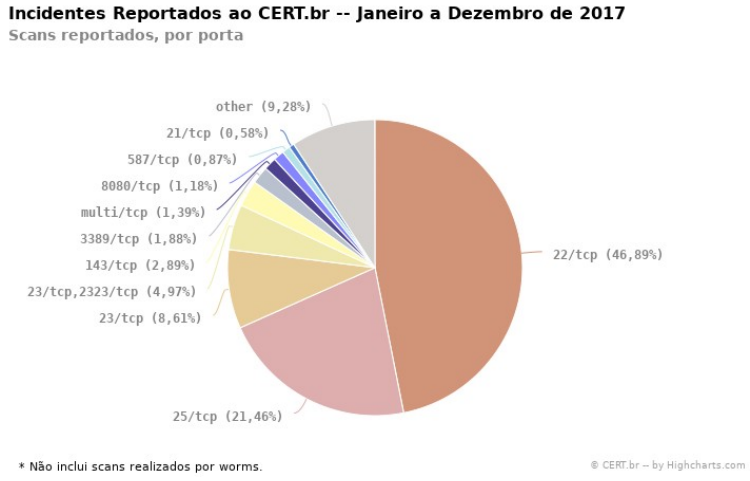
Fonte: https://www.cert.br/stats/incidentes/

Figura IX - Incidentes de Tipos de ataques reportados ao CERT.br



Fonte: https://www.cert.br/stats/incidentes/2017-jan-dec/tipos-ataque.html

Figura X - Incidentes de scans por porta reportados ao CERT.br



Fonte: https://www.cert.br/stats/incidentes/2017-jan-dec/scan-portas.html

Com os dados que foram reportados ao CERT.br é possível visualizar um aumento exponencial a cada ano, aumentando também a preocupação com a segurança da rede, assim sendo proposto neste projeto os pontos para se preocupar em relação a isso.

Mesmo com essas preocupações e aplicações de regras recentemente foi descoberto uma falha no protocolo *WPA2* tornando praticamente toda rede sem fio ainda mais insegura, apenas sendo possível minimizar o ataque de reinstalação de chaves onde com ele é possível inserir sites falsos para adquirir dados do usuário e também podendo ser inserido códigos maliciosos nos aparelhos das vítimas, a meios práticos de minimizar esse ataque, definindo a criptografia como *WPA2-PSK* com *AES* ou redes privadas *VPN*, porém não deixa a rede invulnerável. Está sendo desenvolvido um novo protocolo sendo ele *WPA3* aonde terá um nível maior de segurança, assim sanando as vulnerabilidades das redes *WPA2*, porem o protocolo será lançado apenas em 2019 pela empresa *WIFI ALLIANCE* uma organização sem fins lucrativos que promove o uso da tecnologia *WIFI* e certifica equipamentos que utiliza tal tecnologia. Assim em trabalhos futuros deste projeto será descrito como implementar o protocolo *WPA3* para sanar essa falha.

9 EQUIPAMENTO MIKROTIK

Visando uma segurança melhor para o serviço disponibilizado foi utilizado um *FIREWALL* da *MIKROTIK*, ele possui todos os recursos necessários para um *FIREWALL*, gerenciamento ponto de acesso sem fio, *LINK BACKHAUL*[4] e *HOTSPOT*[5], sendo também responsável por determinar toda regra de navegação, redirecionamento e segurança.

Seu fluxo será da seguinte maneira, sendo aplicado um *link* de internet em sua interface *ETH0* e disponibilizando uma saída *ETH1* para navegação e acesso aos servidores *PROXY*[6] e de cadastro. Alguns pontos são importantes para ser aplicado nessas regras, sendo ela o alto consumo de dados, nesta perspectiva visamos diminuir a taxa de *STREAM*[7], pois com uma taxa liberada o acesso será reduzido e insatisfatório para os usuários. Assim será descrito alguns serviços disponibilizados pelo equipamento da *MIKROTIK* e o uso dos mesmos neste projeto, toda regra utilizada neste projeto tem a necessidade de ser realizada pelo terminal do sistema do MIKROTIK para adição das mesmas.

9. 1 Serviço de *HOTSPOT*

Uma conexão tem que ser confiável, de qualidade, estável e rápida, pois a baixa demanda gera insatisfação para os usuários, com isso deve-se haver um controle efetivo dessa banda, através de uma gestão desses dados trafegados. Com isso a serviços disponíveis para esse propósito, o utilizado nesse projeto foi o serviço de *HOTSPOT*, responsável por gerenciar toda conexão realizada, primeiramente ele bloqueia toda conexão solicitada e apenas libera após um *LOGIN* efetivo do utilizador.

Mesmo com esse serviço a alguns pontos necessários para ser analisados. O primeiro ponto, conexão ociosa, caso um usuário conectar-se na rede, mas o mesmo acabar não navegando, lesionaria possíveis

[4] LINK BACKHAUL responsável por interligar o núcleo da rede com as sub-redes.
[5] HOTSPOT refere-se a um local que possua rede sem fio e que está disponível para o uso.
[6] PROXY é um servidor intermediário, responsável por tratar as requisições dos usuários a sites.
[7] STREAM é a tecnologia que envia informações multimídias dentro de uma rede.

utilizadores, pois manterá uma sessão aberta, para resolver esse problema esse serviço disponibiliza-se da função para derrubar conexões ociosas, assim configurando um tempo médio para essas conexões sendo ela de cinco minutos cada, onde a um controle por taxa de navegação, caso não houver requisições em um período de cinco minutos, a sessão é encerrada, caso queira utilizar o serviço novamente terá que efetuar um novo *LOGIN*. O segundo ponto é o limite de tempo de acesso e de dados, o acesso por tempo indeterminado prejudica possíveis utilizadores, pois ocuparia toda banda caso haja uma grande demanda de conexões simultâneas, visando isso alguns passos foram adotados para esse controle, sendo elas, as limitações por sessões, com um período aceitável de conexão, abrangendo um número grande de usuários, o fator limitante desse projeto foi de 30 minutos por conexão ativa regularmente e um limite para os dados de download e upload, sendo eles de trinta megabits de download e dez megabits de upload, o importante é sempre utilizar 40% da banda real, para evitar possíveis gargalos de rede. Com o serviço de *HOTSPOT* é possível também abranger a área de segurança, onde é possível filtrar os acessos com os respectivos *MAC* e *IP's* dos clientes, assim podendo associar qualquer ato ilícito ao responsável.

9.2 Adicionando Endereços de Rede

Um ponto importante a ser observado, foi acerca de casos de roubo de informações dentro da rede, a vários meios para se amenizar esse problema, todo roubo de dados são feitos através de brechas na rede, onde farejadores na rede buscam máquinas ativas para começar determinado ataque, onde é aplicado na camada de rede, um meio eficaz de diminuir exponencialmente esse problema, é bloqueando a interação entres redes, porem a uma necessidade de criar vários endereçamentos para que isso seja possível, com isso foi criado onze faixas distintas, sendo elas, quatro para endereçamento de host, todas sem interação uma com a outra, visando diminuir questões como *SNIFFER* na rede, quatro para autenticações no serviço de *HOTSPOT* cada usuário receberá dois *IP's*, um para autenticar na rede e

outro para autenticar no serviço de *HOTSPOT*, mais um para identificações dos equipamentos na rede, como roteadores e rádios, um para manutenção caso haja necessidade, assim como descrito na Cartilha de Segurança para Internet(2012), desabilitar o gerenciamento via rede sem fio, apenas sendo possível através uma rede cabeada assim o usuário não terá acesso a *LOGIN* no equipamento onde está presente as configurações da rede e outro sendo para o servidor de autenticação, assim sendo conectados em portas distinta pode se fazer um bloqueio mais efetivo, fazendo uma filtragem diretamente nos dados trafegados em cada interface de rede.

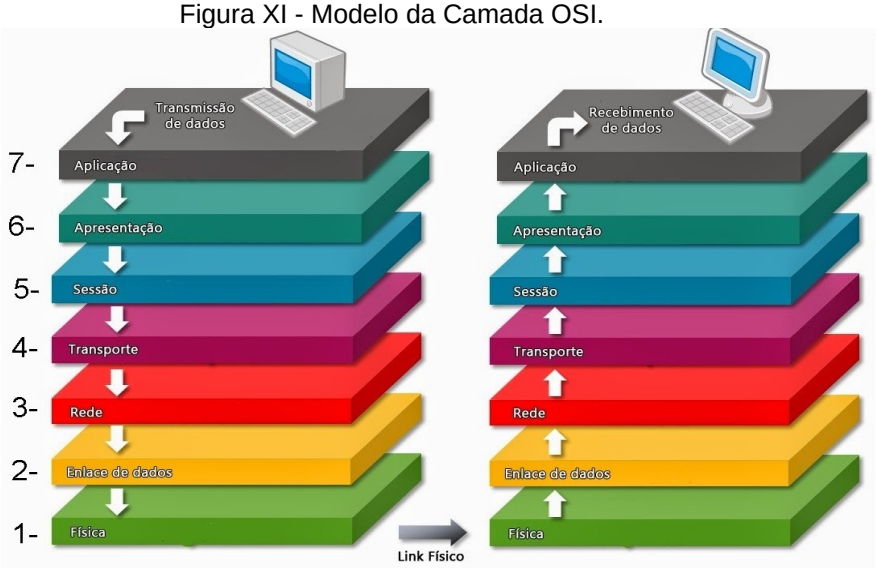
9.3 Servidor Proxy

Para ter um controle efetivo e registro dos dados navegados é necessário possuir um *PROXY* para essa filtragem, onde é necessário redirecionar as portas padrão de navegação, sendo elas a porta 80 para protocolos *HTTP* e a porta 443 para protocolos *HTTPS*, com o *PROXY* e possível filtrar os sites navegados e bloqueá-los, também podendo gerar um histórico dessa navegação, sendo ele configurado como transparente para evitar a configuração nos equipamentos dos utilizadores e também evitar a autenticação com usuários de *PROXY*, o mesmo não restringe sites com protocolos *SSL* devido a segurança do protocolo.

9.4 Camada OSI

Para entender um pouco mais como fazer um bloqueio efetivo em camadas de aplicação, aonde atinge os protocolos *SSL* é necessário saber como funciona o modelo da camada *OSI* e suas funções, são exatamente sete camadas, exibido na figura XI.

Figura XI - Modelo da Camada OSI.



Fonte: https://www.dfilitto.com.br/rede-de-computadores/modelo-osi/

Cada camada referenciara a uma aplicação direta de rede de computadores, assim cada tipo de protocolo referência se a um tipo, sendo elas:

1- Camada física: como placas de redes, modens entre outros.

2- Camada de enlace: responsável pela trafego dos dados, pelos protocolos de comunicação como *IEEE* entre outros.

3- Camada de rede: responsável pelos protocolos de comunicação e tratativa, usados para identificar os pacotes de rede e tratamento do mesmo.

4- Camada de transporte: responsável por destinar o pacote referido ao seu destino.

5- Camada de sessão: responsável pela troca de dados e a comunicação entre hosts, a camada de Sessão permite que duas aplicações em computadores diferentes estabeleçam uma comunicação.

6- Camada de apresentação: responsável pela parte de criptografia, aonde ira comprimir e descomprimir pacotes para encaminhamento ou para utilização da camada de aplicação.

7- Camada de aplicação: responsável pela apresentação, aonde terá os dados recebidos por outro usuário ou servidor, como sites entre outros.

Assim segundo o Rob Scrimger sobre a solicitação de um site pelo usuário.

> “Solicitar um site Web como www.nwcomputertraining,com no seu navegador colocará uma solicitação na camada de aplicativo para conversão do nome por meio do DNS e também uma solicitação de protocolo para o HTTP.” (TCP/IP a Bíblia, 2002, p.9).

Como Rob Scrimger disse a camada de aplicativo trata direto com o nome do site que o usuário solicitou e não depois com a requisição criptografada, assim para ter um bloqueio efetivo dos sites *HTTPS* trabalhamos na camada do aplicativo, tratando diretamente os nomes contidos no *link* do site, dando assim para bloquear esses sites que não podem ser bloqueados pelo *PROXY*.

Também há uma preocupação com conexões *P2P* devido a sua alta taxa de consumo de banda, eles também podem ser tratados na camada de aplicação, conseguindo restringir de forma eficaz o acesso a sites com protocolos seguros e a conexões *P2P* responsáveis por consumir uma grande quantidade de banda de *DOWNLOAD* e *UPLOAD* e ao bloquear protocolos *P2P* também aumentamos a segurança para o usuário porque conforme a cartilha de segurança para internet sobre programas *P2P*, “Obtenção de arquivos maliciosos: os arquivos distribuídos podem conter códigos maliciosos e assim, infectar seu computador ou permitir que ele seja invadido”(CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.44), neste projeto foi utilizada essas tratativas para disponibilizar uma conexão segura, rápida e estável.

9.5 Proteção Firewall

Essa parte é essencial para o projeto, ela será responsável por determinar toda a regra dentro da rede, sendo feita toda a tratativa de restrições e bloqueios, assim determinará as possíveis brechas que poderá estar disponível para pessoas mal intencionadas, essas pessoas tem o intuito

de roubar informações ou tornar o serviço disponibilizado indisponível, assim conforme a cartilha de segurança para internet.

> “Quando bem configurado, o firewall pessoal pode ser capaz de:
>
> - Registrar tentativas de acesso aos serviços habilitados no seu computador;
> - Bloquear o envio para terceiros de informações coletadas por invasores e códigos maliciosos;
> - Bloquear as tentativas de invasão e de exploração de vulnerabilidades do seu computador e possibilitar a identificação das origens destas tentativas
> - Analisar continuamente o conteúdo das conexões, filtrando diversos tipos de códigos maliciosos e barrando a comunicação entre um invasor e um código malicioso já instalado;
> - Evitar que um código malicioso já instalado seja capaz de se propagar, impedindo que vulnerabilidades em outros computadores sejam exploradas;”(CARTILHA DE SEUGURANÇA PARA INTERNET, 2012, p.57).

Devido a essas preocupações citadas uma boa configuração do *firewall* é essencial, sendo responsável por barrar qualquer ação maliciosa dentro da rede, assim sendo descrito logo mais os ataques mais usados e os meios necessários para se proteger de cada um, para tornar-se uma rede mais segura para o utilizador.

9.5.1 IP Spoofing

O *CRACKER*[8] usa o *SPOOFING* para mascarar seu endereço durante um ataque, assim evitando que o real atacante seja encontrado, com essa técnica é possível abrir brechas para outros ataques, já que o *IP SPOOFING* não permite que as respostas sejam obtidas, pois os pacotes são direcionados para o *IP* falso, assim ele é capaz de utilizar ataques como, Dos para negação de serviço, a fim de tornar esse acesso indisponível, ataque de homem do meio para interceptar os pacotes do utilizador e também tem a possibilidade de cria vários endereços falsos, assim causando o aumento do consumo da largura de banda e de processamento desse roteador, causando lentidões ou indisponibilidade do serviço disponibilizado, segundo Emilio

[8] CRACKER é quem pratica a quebra de segurança de uma rede de dados.

Tissato Nakamura e Paulo Lício de Geus “O *IP SPOOFING* pode ser considerado uma técnica auxiliar para outros métodos de obtenção de informação” (SEGURANÇA DE REDES, 2004, p.69), assim como citado o *IP SPOOFING* pode ser muito perigoso por facilitar outros ataques a serem realizados com sucesso, por isso demostramos como evita-lo.

5.9.1.1 Proteção contra ataques spoofing

Ativando o Reverse Path Filter é uma opção ótima para tratar *IP SPOOFING*, para ativa-lo somente entrar com a seguinte regra demonstrada na figura XII.

Figura XII - Regra para ativar Reverse Path Filter.

```
/ip settings set rp-filter= strict
```

https://wiki.mikrotik.com/wiki/Manual:IP/Settings

Assim sendo possível filtrar automaticamente *IP’s* falsos descartando os pacotes que falham na autenticação dentro da rede.

9.5.2 Man in the Middle

O ataque *MAN IN THE MIDDLE* é utilizado para roubar informações dos usuários dentro de uma rede, onde intercepta a comunicação de servidor e cliente, podendo atingir no momento do *HANDSHAKE*[9], assim o atacante consegue interceptar os dados do utilizador, a fim de descobrir senhas de acesso.

Ao possuir uma rede sem fio sem autenticação, abre uma brecha para pessoas mal intencionadas ao criarem pontos de acessos falsos, parecendo que aquele acesso está sendo realmente sendo disponibilizado por tal local, assim esse atacante é capaz de capturar toda informação que passa em sua rede, por ter o controle dela, gerando transtornos para os utilizadores, esses

[9] HANDSHAKE é a negociação entre o cliente e servidor, ou utilizador e roteador, para estabelecer os protocolos de comunicação.

pontos de acessos falsos são bem utilizados para o ataque *MAN IN THE MIDDLE*, por já ser uma rede direcionada para captura de dados.

9.5.2.1 Proteção contra ataque man in the middle

Essa proteção é feita através dos bloqueios de ataques *SPOOFING*, sendo ele responsável por abrir uma brecha para que aja o ataque *MAN IN THE MIDDLE* e também a orientação aos usuários sempre verificar se a rede que esta conectando é realmente a verdadeira disponibilizada pelo local.

9.5.3 Brute Force

Conforme descrito na cartilha de segurança para internet.

> “Um ataque de força bruta, ou brute force, consiste em adivinhar, por tentativa e erro, um nome de usuário e senha e, assim, executar processos e acessar sites, computadores e serviços em nome e com os mesmos privilégios deste usuário” (CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.20).

Assim com ataques de força bruta é utilizado a fim de conseguir acesso a um equipamento que exija senha, na rede sem fio de quem disponibiliza esse invasor faz esse tipo de ataque para conseguir acesso ao roteador ou ao firewall da rede, tendo acesso a todas as configurações e estará livre para fazer diversos ataques, tendo a possibilidade de interceptar os pacotes e redireciona-los para o dispositivo do invasor, ou até mesmo para tornar a conexão indisponível.

9.5.3.1 Proteção contra Brute Force

Para bloquear ataques de *BRUTE FORCE*, têm que tratar as tentativas de conexão via *FTP* e *SSH*, as regras para limitar até 10 respostas incorretas caso tenha uma tentativa via *FTP*, assim esse ip ira para uma *BLACK LIST*, as regras para o bloqueio *FTP* está descrita na figura XIII:

‘

Figura XIII - Adição a Black List de Ips com logins incorreto pelo FTP.

```
/ip firewall filter add chain=input protocol=tcp dst-port=21
src-address-list=ftp_blacklist action=drop \
comment="drop ftp brute forcers"

/ip firewall filter add chain=output action=accept protocol=tcp
content="530 Login incorrect" dst-limit=1/1m,9,dst-address/1m

/ip firewall filter add chain=output action=add-dst-to-address-
list protocol=tcp content="530 Login incorrect" \
address-list=ftp_blacklist address-list-timeout=3h
```

Fonte: https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

E para bloqueio de *SSH* restringindo a pessoa por um determinado tempo até sua liberação, sendo a definida neste projeto para um dia, as regras estão descritas na figura XIV.

Figura XIV - Adição a Black List de Ips com logins incorreto pelo SSH.

```
/ip firewall filter add chain=input protocol=tcp dst-port=22 src-address-
list=ssh_blacklist action=drop \
comment="drop ssh brute forcers" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage3 action=add-src-to-address-list address-
list=ssh_blacklist \
address-list-timeout=10d comment="" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new \
src-address-list=ssh_stage2 action=add-src-to-address-list address-
list=ssh_stage3 \
address-list-timeout=1m comment="" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new
src-address-list=ssh_stage1 \
action=add-src-to-address-list address-list=ssh_stage2 address-list-timeout=1m
comment="" disabled=no

/ip firewall filter add chain=input protocol=tcp dst-port=22 connection-state=new
action=add-src-to-address-list \
address-list=ssh_stage1 address-list-timeout=1m comment="" disabled=no
```

Fonte: https://wiki.mikrotik.com/wiki/Bruteforce_login_prevention

Assim minimizando ataques de *BRUTE FORCE* evitando que o invasor tenha acesso as configuração do roteador

9.5.4 Interceptação de Tráfego (Sniffers)

Visto que na cartilha de segurança para internet (2012), interceptação de tráfego ou *SNIFFING*, é uma técnica que capturar informações trafegadas na rede para inspeciona-los, podendo ser utilizado de duas formas, uma de forma legitima sendo utilizada para monitorar a rede e detectar problemas ou de forma maliciosa a fim de conseguir senhas números de cartão de credito ou conteúdo dos arquivos trafegados naquela rede.

9.5.4.1 Proteção contra ataques Sniffers

Para bloquear possíveis ameaças de *SNIFFERS* na rede. Primeiro você cria uma *ADDRESS LIST*, nela conterá os *IP'S* que estão tentando farejar sua rede, após isso adicionara uma regra para bloquear esses *IP*, com a propriedade *PSD* que detecta varredura na rede dos protocolos *TCP* e *UDP*, assim quando detecta-los adicionara na *BLACK LIST*, regra exibida na figura XV.

Figura XV - Varredura de rede para encontrar sniffers.

```
/ip firewall filter add chain=input protocol=tcp psd=21,3s,3,1 action=add-src-to-address-list address-list="port scanners" address-list-timeout=2w comment="Port scanners to list " disabled=no
```

Fonte: https://wiki.mikrotik.com/wiki/Drop_port_scanners

Após adicionar a rede de varredura, terá também que adicionar as regras dos sinalizadores *TCP*, eles são responsáveis por essas etapas.

- ack - reconhecendo dados
- cwr - janela de congestionamento reduzida
- ece - sinalizador ECN (notificação explícita de congestionamento)

- Aleta - conexão próxima
- psh - função push
- primeiro - soltar conexão
- syn - nova conexão
- urg - dados urgentes

Assim com esses sinalizadores é possível após detectar os *IP's* que estão a farejar a rede, adiciona-los a uma *BLACK LIST*, a regra para adicionar esses endereços está exposta na figura XVI.

Figura XVI - Regra de utilização de Sinalizadores para identificar sniffers.

```
/ip firewall filter add chain=input protocol=tcp tcp-flags=fin,!syn,!rst,!psh,!ack,!urg
action=add-src-to-address-list address-list="port scanners" address-list-
timeout=2w comment="NMAP FIN Stealth scan"

/ip firewall filter add chain=input protocol=tcp tcp-flags=fin,syn action=add-src-to-
address-list address-list="port scanners" address-list-timeout=2w
comment="SYN/FIN scan"

/ip firewall filter add chain=input protocol=tcp tcp-flags=syn,rst action=add-src-to-
address-list address-list="port scanners" address-list-timeout=2w
comment="SYN/RST scan"

/ip firewall filter add chain=input protocol=tcp tcp-flags=fin,psh,urg,!syn,!rst,!ack
action=add-src-to-address-list address-list="port scanners" address-list-
timeout=2w comment="FIN/PSH/URG scan"

/ip firewall filter add chain=input protocol=tcp tcp-flags=fin,syn,rst,psh,ack,urg
action=add-src-to-address-list address-list="port scanners" address-list-
timeout=2w comment="ALL/ALL scan"

/ip firewall filter add chain=input protocol=tcp tcp-flags=!fin,!syn,!rst,!psh,!ack,!urg
action=add-src-to-address-list address-list="port scanners" address-list-
timeout=2w comment="NMAP NULL scan"
```

Fonte: https://wiki.mikrotik.com/wiki/Drop_port_scanners

[9] SYN é o envio de pacote de dados de um host para um servidor, assim que aceito começa a o envio de dados.
[10] ACK mensagem de reconhecimento do host estabelecendo uma conexão entre cliente servidor.

Assim que esses endereços estiverem nessa *BLACK LIST* com a regra da figura XVII é possível bloqueá-los, evitando possíveis ataques *SNIFFER*.

Figura XVII - Regra para bloqueio da Black List de sniffers.

```
add chain=input src-address-list="port scanners" action=drop comment="dropping
port scanners" disabled=no
```

Fonte: https://wiki.mikrotik.com/wiki/Drop_port_scanners

Com esse bloqueio é possível evitar e o atacante não consiga capturar pacotes dentro da rede de outros usuários e também com a configuração do *HOTSPOT* ajuda na efetividade do bloqueio de *SNIFFER*, pois ele isola todos os clientes na rede, bloqueando toda iteração entre esses dispositivos conectados à rede e também para minimizar esses ataques podem se dividir as faixas de rede como descrito mais acima no título *ADDRESS*.

9.5.5 Negação de Serviço (DoS e DDos)

Como na descrição da Cartilha de Segurança para Internet, negação de serviço é.

> “Negação de serviço, ou Dos (Denial of Service), é uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conecta à internet.”(CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.21).

Isso significa que o atacante tem o intuito de deixar um tipo de serviço indisponível, podendo ser direcionada para redes sem fio, assim tornando essas redes inutilizáveis, eles podem ser atrás de um ataque distribuído sendo ele *DDos* (Distributed Denial of Service), sendo várias maquinas acessado simultaneamente a conexão assim o roteador não consegue responder a todas essas solicitações, até mesmo a ataques de inundações *SYN*[9], toda a vez que um utilizador se conecta a uma rede, ele manda um sinal *SYN* e o roteador retorna um sinal *SYN-ACK*[10] autorizando a utilizar a

[9] SYN é o envio de pacote de dados de um host para um servidor, assim que aceito começa a o envio de dados.
[10] ACK mensagem de reconhecimento do host estabelecendo uma conexão entre cliente servidor.

rede, assim a pessoa mal intencionada que usa esse tipo de ataque, envia várias solicitações *SYN* falsas consumindo todo o processamento do roteador, assim não conseguindo retornar todas essas mensagens tornando a rede indisponível para os demais utilizadores.

9.5.5.1 Proteção contra ataques DDos

Para se proteger de ataques *Dos* pode se fazer a filtragem dos pacotes, assim poderá descarta-lo ou salva-lo. A regra a ser adiciona está descrita na figura XVIII:

Figura XVIII - Regra para limite de solicitações SYN.

```
/ip firewall filter add chain=input protocol=tcp connection-limit=LIMIT,32  \
action=add-src-to-address-list  address-list=blocked-addr address-list-timeout=1d

/ip firewall filter add chain=input protocol=tcp src-address-list=blocked-addr \
connection-limit=3,32 action=tarpit

/ip firewall filter add chain=forward protocol=tcp tcp-flags=syn connection-
state=new \
action=jump jump-target=SYN-Protect comment="SYN Flood protect"
disabled=yes

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn limit=2000
connection-state=new \
action=accept comment="" disabled=no

/ip firewall filter add chain=SYN-Protect protocol=tcp tcp-flags=syn connection-
state=new \
action=drop comment="" disabled=no
```

Fonte: https://wiki.mikrotik.com/wiki/DoS_attack_protection

Configurando um total de 2000 conexões assim caso exceda esse número as novas conexões serão descartadas e também com essa regra caso aja um ip com muitas conexões ela é descartada. Com isso é possível evitar ataques *Dos*.

9.6 Servidor de log e de cache

Após os cuidados com a segurança um serviço de cache é essencial pois ele é responsável por armazenar toda a navegação, assim após um site for carregado por completo, o próximo usuário a solicitar o mesmo site, terá um carregamento da página mais rápido que o convencional, mas também há uma preocupação, com erros de cache podendo deixar a conexão de alguns sites impossível, com isso foi aplicado uma rotina para limpeza desses *CACHE*. Outra parte e a mais importante é o servidor de *LOG*, ele faz um armazenamento continuo dessas navegações, segundo o artigo 18 da lei do Marco Civil da Internet do Brasil, descreve que qualquer ato referente a conteúdos gerados por terceiros não seja responsabilidade de quem disponibiliza, porem segundo o artigo 13 da lei do Marco Civil da Internet tem que armazenar o registro desses utilizadores por no mínimo um ano, assim caso não tenha nenhum registro que identifique quem gerou esse ato, quem disponibiliza essa rede será responsável pelo ato, essas informações será necessária para identificar possíveis atos ilícitos efetuados dentro da rede como descrito na cartilha de segurança para internet.

> “Logs são essências para notificações de incidentes, pois permitem que diversas informações importantes sejam detectadas, como por exemplo: a data e o horário em que uma determinada atividade ocorreu, o fuso horários do log, o endereço IP de origem da atividade, as portas envolvidas e protocolo utilizado ataque (TCP, UDP, ICMP, etc.), os dados completos que foram enviados para o computador ou rede e o resultado da atividade(se ela ocorreu com sucesso ou não)”(CARTILHA DE SEGURANÇA PARA INTERNET, 2012, p.54).

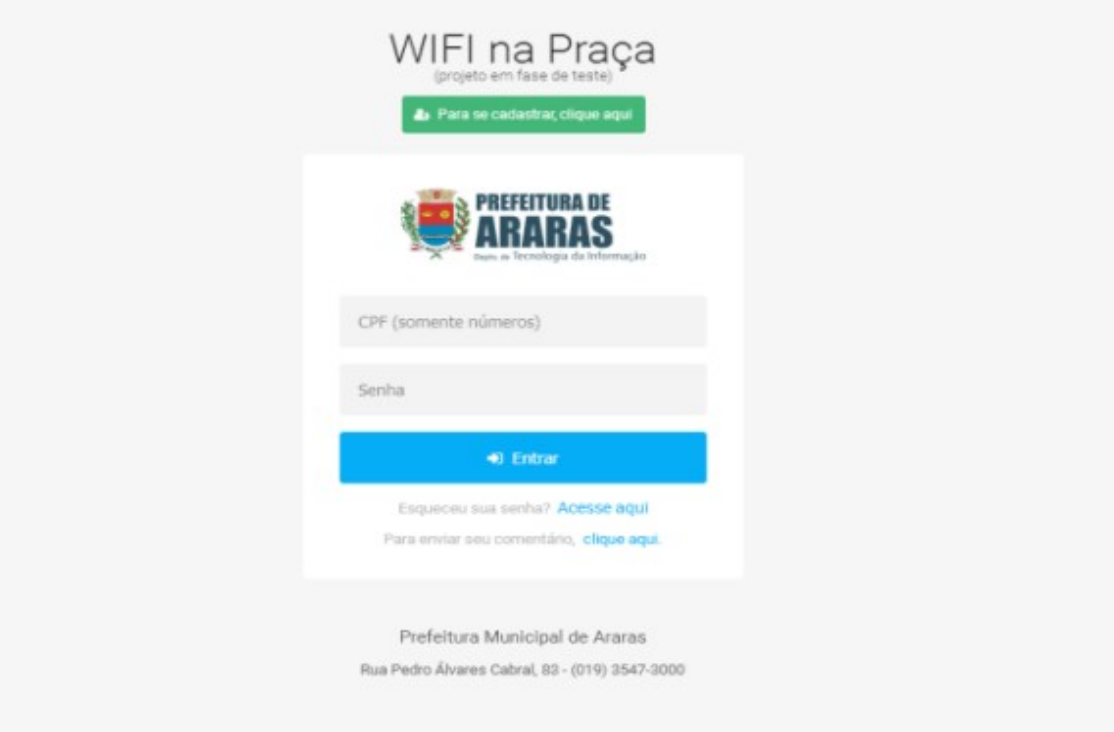
Sendo essencial para identificação de possíveis ataques na rede, sendo possível minimizar ou evitar esses ataques ou até mesmo ter respaldos para ocorrências dentro da rede.

Assim o aplicado para este projeto foi o *PROXYLIZER*, um programa em Linux capaz de se comunicar com o *MIKROTIK*, assim toda informação navegada será automaticamente gravada nesse servidor, onde constara o *IP* e *MAC* e sites acessados por esses mesmos.

10 AUTENTICAÇÂO

Após a disponibilização desse serviço, haverá a autenticação do usuário, ela pode ser definida com uma página personalizada com uma interface para logar, foi utilizado neste cenário o serviço de *HOTSPOT* do *MIKROTIK*, o mesmo já possui uma página pré-configurada para o LOGIN, assim terá que apenas alterar o layout conforme necessidade, a alteração deste projeto está demonstrada na figura XIX.

Figura XIX - Área de login.



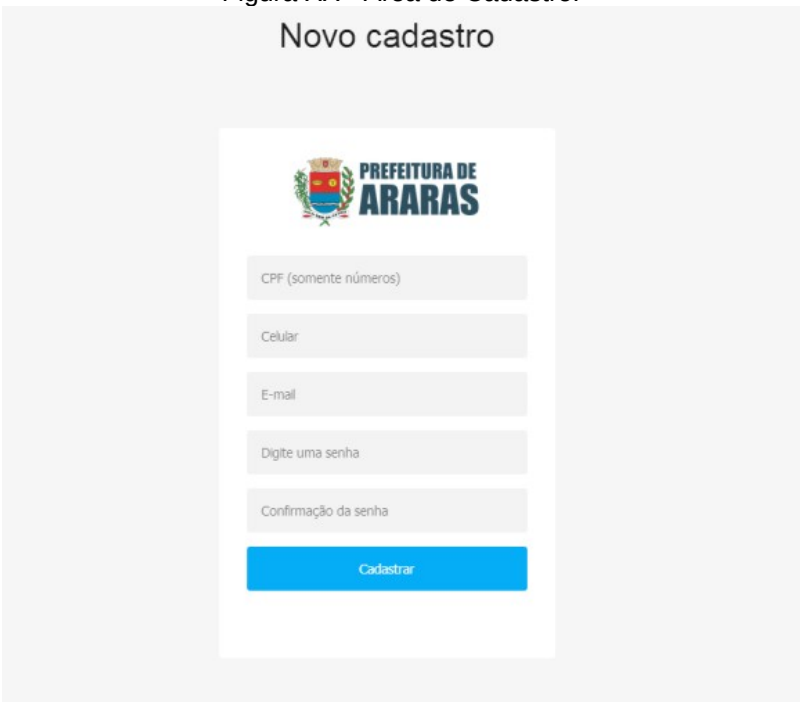
Fonte: O Autor

O *LOGIN* de cada usuário ficou restrito ao *CPF* do navegante, isso viabiliza a questão de duplicidade de usuário e também para um melhor controle, o serviço utilizado não disponibiliza de um servidor de cadastro, para isso terá que ser configurado para poder efetuar os cadastros.

11 SERVIDOR DE CADASTRO

Para que possa ter um controle efetivo e evitando clonagem dos dados e tendo um controle melhor, pode-se obter isso ao criar um servidor de cadastro, onde necessitara de um banco de dados e uma aplicação emulada para plataforma *WEB*. O servidor web será utilizado para emular as páginas criadas, para que possam ser visíveis ao usuário. O banco utilizado para este projeto foi *POSTGRESQL* visando o custo, o mesmo é grátis, nele receberá as informações cadastradas para o controle dos usuários. A linguagem utilizada foi *C-SHARP* onde foram criados os seguintes campos, *CPF* que será usado como usuário para o *LOGIN*, os outros foram, celular, e-mail, senha e confirmar a senha, nele será conectado com o banco, assim se caso houver um usuário já cadastrado, será informado que já possui um cadastro com esses dados, a tela de cadastro deste projeto está exibida na figura XX.

Figura XX - Área de Cadastro.



Fonte: O Autor

Ao pensar que um utilizador esqueça a senha, precisara também de uma tela para a redefinição de senha, mas para isso o usuário terá que inserir o *CPF* cadastrado junto a seu celular e e-mail, caso foi feito um cadastro

[11] SUBMIT método que envia dados de um formulário para um local especifico.

irregular não será possível para o mesmo redefinir a senha, ficando da seguinte maneira como demonstrado na figura XXI.

Figura XXI - Área Recuperar Senha.

Fonte: O Autor

O serviço de *HOTSPOT* reconhece apenas uma linguagem própria e linguagem web, sendo assim existe uma necessidade de inserir um código para o *SUBMIT*[11], para que essas informações digitadas possam ser gravadas no *MIKROTIK* o código fica o seguinte na figura XXII.

Figura XXII - Envio dos dados do Login

```
functiondoLogin() {document.sendin.username.value =
document.login.username.value; document.sendin.password.value =
hexMD5('$(chap-id)' + document.login.password.value + '$(chap-challenge)');
document.sendin.submit();return false.
```

Fonte:O Autor

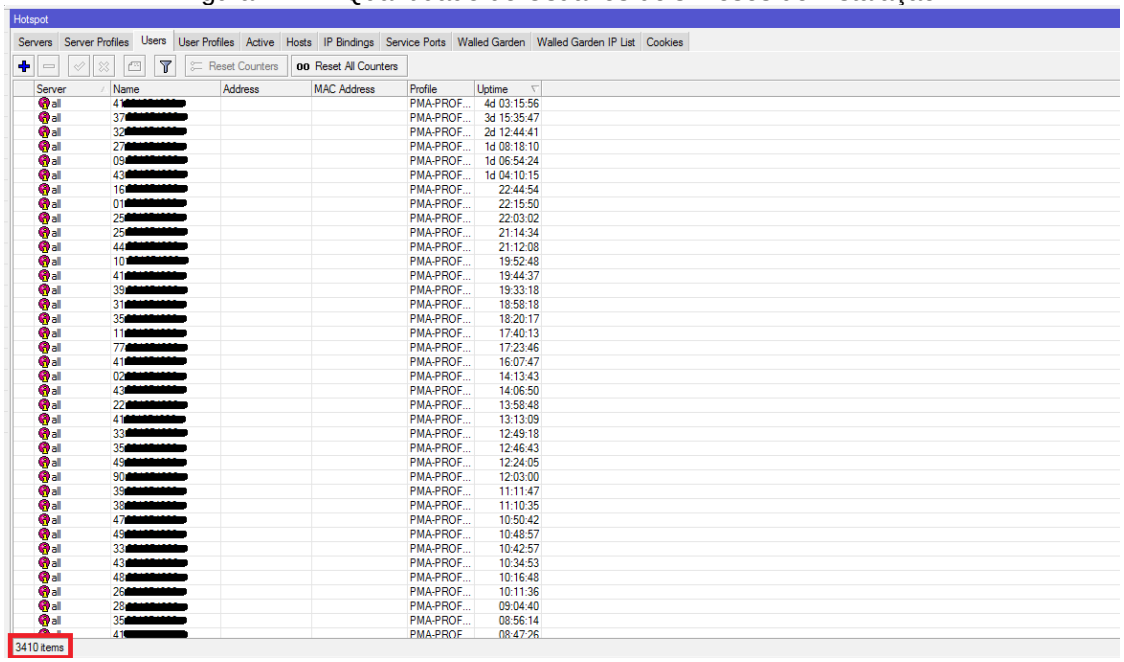
Ele receberá apenas o valor do campo *CPF* e senha e enviara para cadastrar o novo usuário, assim finaliza a parte de cadastro e *LOGIN*.

[11] SUBMIT método que envia dados de um formulário para um local especifico.

12 RESULTADOS

Após finalizar o projeto foram coletadas diversas informações para demonstrar a eficácia do projeto em si. Como demostrado na imagem a seguir podemos ver que temos 3410 usuários cadastrados em um período de dois meses, como demonstrado na figura XXIII.

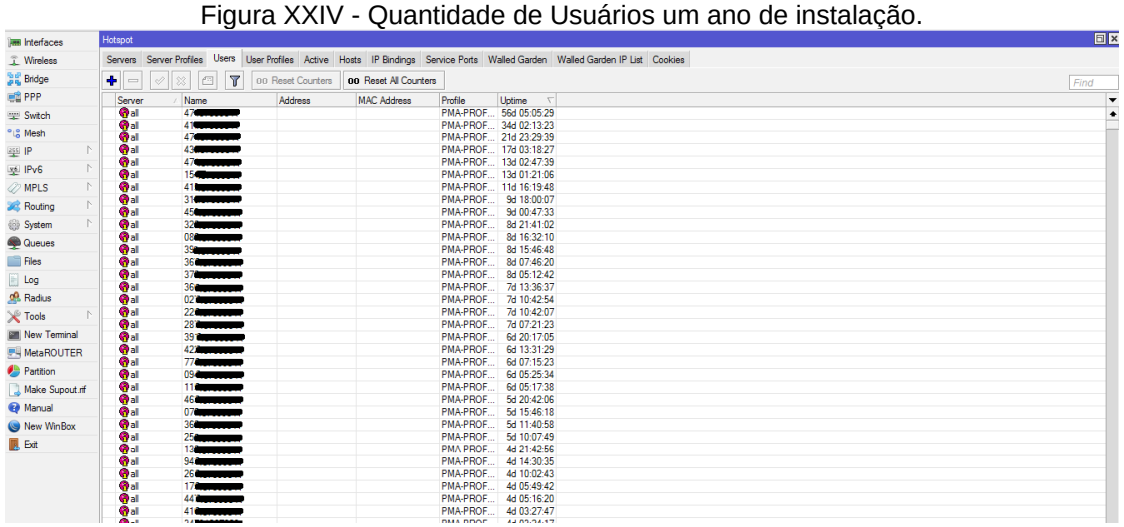
Figura XXIII - Quantidade de Usuários dois meses de instalação.



Fonte: O Autor

Após um ano de projeto temos 12424 usuários cadastrados, como demonstrado na figura XXIV.

Figura XXIV - Quantidade de Usuários um ano de instalação.



Fonte: O Autor

Figura XXV - Quantidade de Usuários mês de setembro de 2018.

UniFi 5.8.24

SÍTIO ATUAL: Default | NOME DE UTILIZADOR: admin

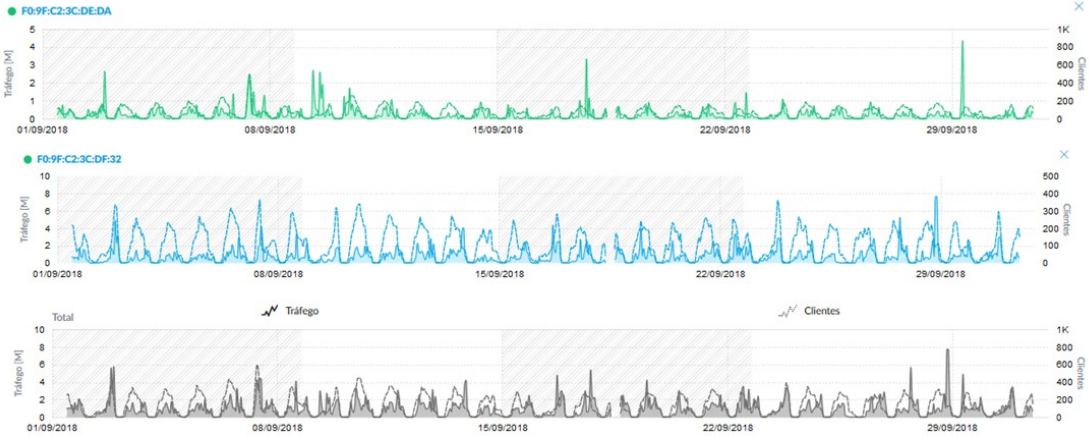
LIGAÇÕES PASSADAS | 01/09/2018 - 01/10/2018 | TODOS (8991) | UTILIZADORES (8991) | CONVIDADOS (0) | Pesquisa

NOME/ENDEREÇO MAC	UTILIZ./CONVIDADO	ASSOCIADO	DURAÇÃO ↓	DOWN	UP	ENDEREÇO IP	ÚLTIMO AP/PORTA
Galaxy-A7-2017	Utilizador	11/09/2018 6:21	5d 16h 34m 34s	6.82 KB	15.5 KB	192.168.3.36	f0:9f:c2:3c:de:da
Galaxy-A7-2017	Utilizador	11/09/2018 6:21	3d 8h 57m 15s	0 B	0 B		f0:9f:c2:3c:df:32
Galaxy-A7-2017	Utilizador	11/09/2018 6:21	2d 3m 33s	8.32 KB	52.9 KB	192.168.2.104	f0:9f:c2:3c:df:32
android-826ee86b1931b3	Utilizador	17/09/2018 16:11	1d 16h 17m	5.05 KB	9.24 KB	192.168.3.8	f0:9f:c2:3c:de:da
android-826ee86b1931b3	Utilizador	17/09/2018 11:45	21h 22m 1s	100 B	136 KB	192.168.2.137	f0:9f:c2:3c:de:da
android-d65b889e039e7aaf	Utilizador	04/09/2018 19:25	13h 8m 6s	28.8 MB	9.28 MB	192.168.2.51	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	10/09/2018 22:56	13h 7m 10s	72.1 MB	9.61 MB	192.168.3.1	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	07/09/2018 21:49	10h 57m 15s	24.9 MB	7.11 MB	192.168.2.88	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	31/08/2018 22:14	10h 28m 24s	14.4 MB	5.47 MB	192.168.2.51	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	01/09/2018 21:25	9h 56m 29s	12 MB	4.86 MB	192.168.2.51	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	09/09/2018 22:35	9h 55m 23s	25 MB	23.2 MB	192.168.2.151	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	16/09/2018 22:43	9h 42m 15s	75 MB	15.3 MB	192.168.3.83	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	13/09/2018 20:11	9h 27m 4s	18.1 MB	3.58 MB	192.168.3.83	f0:9f:c2:3c:df:32
android-423e44df316804a0	Utilizador	09/09/2018 1:04	9h 19m 36s	21 MB	4.59 MB	192.168.3.86	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	28/09/2018 15:23	8h 18m 9s	231 MB	114 MB	192.168.2.205	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	21/09/2018 16:17	8h 15m 25s	203 MB	79.8 MB	192.168.2.198	f0:9f:c2:3c:df:32
android-384994fb2d83d09f	Utilizador	12/09/2018 7:02	8h 11m 33s	5.24 MB	9.57 MB	192.168.3.111	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	05/09/2018 16:02	8h 21s	373 MB	180 MB	192.168.3.70	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	22/09/2018 22:48	7h 57m 52s	1.01 MB	1.75 MB	192.168.3.83	f0:9f:c2:3c:df:32
android-c5aa5201222a4d8e	Utilizador	11/09/2018 8:18	7h 56m 59s	161 KB	318 KB	192.168.2.196	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	01/09/2018 16:24	7h 33m 24s	159 MB	101 MB	192.168.2.53	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	29/09/2018 16:19	7h 32m 53s	194 MB	103 MB	192.168.3.29	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	06/09/2018 0:51	7h 32m 28s	29.6 MB	6.98 MB	192.168.2.51	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	11/09/2018 16:04	7h 31m 34s	276 MB	123 MB	192.168.2.181	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	26/09/2018 16:11	7h 27m 41s	173 MB	86.6 MB	192.168.3.188	f0:9f:c2:3c:df:32
android-d65b889e039e7aaf	Utilizador	20/09/2018 22:52	7h 24m 46s	12.5 MB	3.36 MB	192.168.3.83	f0:9f:c2:3c:df:32
d0:77:14:68:b6:eb	Utilizador	10/09/2018 16:32	7h 20m 10s	638 MB	150 MB	192.168.2.167	f0:9f:c2:3c:df:32
android-423e44df316804a0	Utilizador	04/09/2018 23:47	7h 13m 14s	439 KB	940 KB	192.168.2.218	f0:9f:c2:3c:df:32

Fonte: O Autor

Como exibido na figura XXV é exibido o período de navegação, sendo ele alto para vários usuários. No período de instalação no mês de abril de 2018 até o mês de setembro de 2018 houve várias tentativas de intrusão, todas elas não obtiveram sucesso e também durante esse período teve uma media de 46 horas de navegação por usuário, podendo concluir que esta rede é estável e segura, a tornando também bem utilizada.

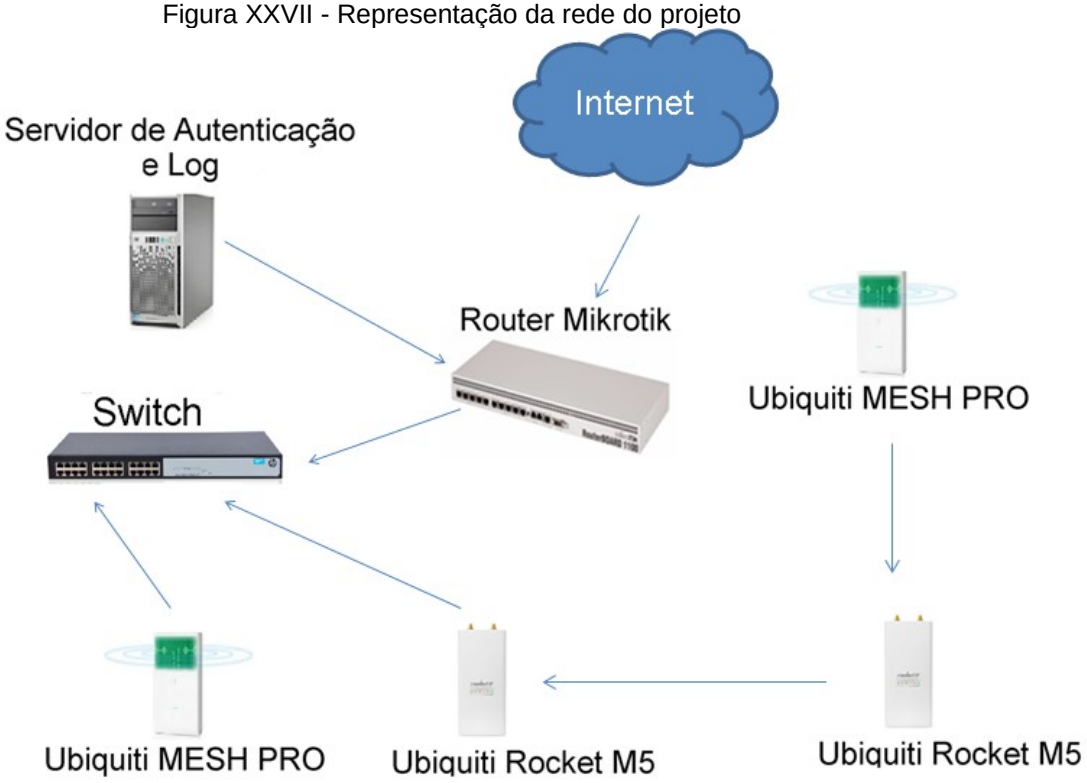
Figura XXVI - Resumo do uso mês de setembro de 2018.



Fonte: O Autor

Com a análise da figura XXVI podemos verificar que no mês de setembro de 2018, teve uma quantidade considerável de utilizadores e picos estáveis de rede sendo calculados por megabits transferidos no momento, assim concluindo que não houve gargalos ou instabilidade na rede, sempre sendo constate a taxa de navegação, assim tendo um acesso eficaz e estável. A topologia da rede ficou conforme exibido na figura XVII.

Figura XXVII - Representação da rede do projeto



Fonte: O autor

Após esses resultados podemos ter uma conclusão sobre o assunto abordado.

CONCLUSÃO

Após os resultados demonstrados podemos concluir que houve milhares de cadastros em poucos meses, e períodos de navegações longas, sendo bem utilizado, com as ferramentas certas foi possível elaborar um projeto eficiente, com analises de campo e testes em diferentes partes, assim atingindo todos os pontos citados, tornando uma conexão segura, rápida e estável, minimizando casos de indisponibilidade, este tipo de projeto pode ser aplicado e qualquer área não apenas em áreas públicas, sendo elas direcionadas ao público e a uma boa relação entre prestador de serviço e cliente, assim também sanando algumas dúvidas referentes à disponibilização de sinais sem fio, sabendo o que é necessário e equipamentos que darão resultados ao utiliza-los, podendo ser também utilizados por pessoas jurídicas ou físicas, tendo um bom rendimento ao serem aplicados, também sendo possível ter o controle dos dados trafegados para segurança de quem disponibiliza e a orientação dos riscos de uma rede aberta tanto para quem utiliza como para quem disponibiliza, deixando claros esses pontos e conscientizando todas as pessoas que tem o interesse de disponibilizar um acesso sem fio e também para quem quer utilizar uma rede gratuita.

REFERÊNCIAS

ANÔNIMO. **Segurança máxima: o guia de um hacker para proteger seu site da internet e sua rede**. Tradução [da 3ª ed. original] de Edson Furmankievicz. Rio de Janeiro: Campus, 2001.

BARBOSA, Gracieiny A. et al. **Estudo de caso: Vunerabilidade em rede wirelles**. Revista gestão em foco, edição nº 9, 2017, p. 555-574. Disponível em: <http://unifia.edu.br/revista_eletronica/revistas/gestao_foco/artigos/ano2017/057_estudo10.pdf> Acesso em: 11.jul.2018.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil,** Brasília, DF, 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 21.jul.2018.

BRASIL. Lei nº 16.685, de 10 de julho de 2017. **Dispõe sobre o Programa Wi-Fi Livre Sampa, gratuito, em todos os espaços e prédios públicos municipais e dá outras providências**, São Paulo, SP, 2017. Disponível em: <https://www.radarmunicipal.com.br/legislacao/lei-16685>. Acesso em:

BRASIL, CERT.br. **Cartilha de segurança para internet: versão 4.0**. São Paulo: Comitê gestor de internet no Brasil, 2012.

CIANET. **Passo a passo para obter a licença SCM online em poucos dias**. Cianet, publicado em: 17/05/2016. Disponível em: <https://www.cianet.com.br/passo-a-passo-para-obter-licenca-scm-online-em-poucos-dias/> Acesso em: 01.set.2018.

Eliardsson, P.; Wiklundh, K.; Axell, E. e Stenumgaard, P**., "Mitigation of co-channel interference by transmit power control",** 2015 IEEE International Symposium on Electromagnetic Compatibility (EMC), Dresden, 2015, pp. 189-193. Disponível em: <https://ieeexplore.ieee.org/document/7256156/> Acesso em: 03.set.2018.

FARAH, Rafael. **Estabelecimento que fornece internet de graça deve estar atento aos riscos**. Conjur. Publicado em: 22/08/2015 às 09:15. Disponível em: <http://www.conjur.com.br/2015-ago-22/patricia-peck-fornecimento-internet-gratis-requer-cuidados> Acesso em 08.jul.2017.

FILITTO, Danilo. **Modelo OSI**. Dfilitto, publicado em: 28/08/2014. Disponível em: <https://www.dfilitto.com.br/rede-de-computadores/modelo-osi/>. Acesso em: 08.jul.2018.

GOGONI, Ronaldo. **Falha severa torna todas as redes Wi-Fi inseguras; saiba como reduzir os danos.** Meiobit, 2017. Disponível em: <https://meiobit.com/373917/krack-falha-torna-todas-redes-wi-fi-wpa2-vulneraveis-a-ataques-saiba-o-que-fazer/>. Acesso em: 20.abr.2018.

GEUS, Paulo Lício de; NAKAMURA, Emilio Tissato. **Segurança de redes em ambientes coorporativos**. 2ª ed. São Paulo: Futura, 2003.
JORDÂO, Fábio. **Wi-Fi 802.11ac: as redes sem fio de alta velocidade vêm aí**. Tecmundo, publicado em: 22/05/2012 às 15:00. Disponível em: <https://www.tecmundo.com.br/wi-fi/23964-wi-fi-802-11ac-as-redes-sem-fio-de-alta-velocidade-vem-ai.htm>. Acesso em: 16.mai.2018.

MIKROTIK. **DoS attack protection**. Página editada pela última vez em: 25/03/2014 às 15:44. Disponível em: <https://wiki.mikrotik.com/wiki/DoS_attack_protection>. Acesso em: 01.nov.2017.

MIKROTIK. **Drop port scanners**. Página editada pela última vez em: 24/07/2009 às 21:47. Disponível em: <https://wiki.mikrotik.com/wiki/Drop_port_scanners>. Acesso em: 01.nov.2017.

MULLER, Leonardo. **Menina de 7 anos consegue hackear WiFi público em menos de 11 minutos**. Tecmundo, publicado em: 29/01/2015 às 12:48. Disponível em: <https://www.tecmundo.com.br/ataque-hacker/73321-menina-7-anos-consegue-hackear-wifi-publico-11-minutos.htm>. Acesso em: 11.nov.2017.

NASCIMENTO, Luciano**. Anatel não vai exigir outorga para provedores de internet com até 5 mil clientes**. Agência Brasil. Publicado em: 22/06/217 às 20:45. Disponível em: <http://agenciabrasil.ebc.com.br/geral/noticia/2017-06/anatel-nao-vai-exigir-outorga-para-provedores-de-internet-com-ate-5-mil> Acesso em 08.jul.2017

NETSPOT. **Increase your Wi-Fi speed with the help of NetSpot — choose the best WiFi channel**. Netspot, 2018. Disponível em: <https://www.netspotapp.com/wifi-channel-scanner.html>. Acesso em: 12.nov.2018.

PREFEITURA MUNICIPAL DE ARARAS, SECOM. **Prefeitura disponibiliza internet de graça na Praça Barão de Araras**. Publicado em: 11/07/2017 às 15:33. <Disponível em http://araras.sp.gov.br/noticias/19096>. Acesso em: 12.jul.2017.

REDAÇÂO, Dfndr blog. **Os 3 maiores riscos para quem utiliza wi-fi público**.Dfndr blog. Publicado em: 04/05/2015. Disponível em

<http://www.psafe.com/blog/os-3-maiores-riscos-para-quem-utiliza-wi-fi-publico/>. Acesso em: 12.jul.2017.

SIMÕES, Helton Gomes**. Emprestou a senha do wi-fi? Cuidado, você pode ser processado na Justiça**.UOL, publicado em: 18/10/2018 às 04:00. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/10/18/emprestou-a-senha-do-wi-fi-cuidado-voce-pode-ir-parar-na-justica.htm>. Acesso em: 24.out.2018.

SILVA, Josmar Queiroz. **Estudo de redes wireles**s. Fórum Oficial do Técnico Reparador Brasileiro, 2018. 30f. Disponível em: <http://www.jqs.eti.br/arquivos/Livro_wireless/wirelessLivro.pdf> Acesso em: 28.out.2018.

SCRIMGER, Rob ... [et al.]. **TCP/IP, a bíblia**. Tradução Edson Furmankievicz, Doc Traduções Técnicas. 3 ª Reimpressão, Rio de Janeiro: Elsevier,2002.

VENTURA, Felipe. **As redes Wi-Fi ficarão mais seguras com o novo padrão WPA3**. Tecnoblog, 2018. Disponível em: <https://tecnoblog.net/248716/wi-fi-seguranca-wpa3-pronto/>. Acesso em: 12.set.2018.

APÊNDICE I

Passo a passo para obter a licença SCM online

1º passo: Cadastro no SEI (Sistema Eletrônico de Informações)

Para começar é preciso que o usuário que irá solicitar a licença SCM se cadastre junto à Anatel como pessoa física, por meio do SEI. Ele se tornará, assim, um usuário externo da Anatel e poderá ter acesso ao sistema Mosaico. Depois de preenchido o formulário de cadastro acessar este link < https://sei.anatel.gov.br/sei/controlador_externo.php?acao=usuario_externo_enviar_cadastro&acao_origem=usuario_externo_avisar_cadastro&id_orgao_acesso_externo=0>, um e-mail automático será enviado com orientações para a aprovação do login do usuário externo. Será necessário comparecer a uma das unidades da Anatel e apresentar cópia e original de comprovante de residência, cópia do RG e CPF, além do Termo de Declaração de Concordância e Veracidade preenchida e assinada.

Alternativamente, poderão ser entregues por terceiro ou enviadas por Correios às cópias autenticadas dos documentos acima indicados e o Termo acima com reconhecimento de firma em cartório. A correspondência por Correios deve ser endereçada ao Protocolo Sede da Anatel (SAUS Quadra 6, Bloco F, Brasília/DF, CEP: 70070-940).

2º passo: Acesso ao sistema Mosaico

Uma vez obtidos login e senha do SEI, é necessário acessar o sistema Mosaico no link <http://sistemas.anatel.gov.br/se/portal/b/login.php>. Usuários que já possuem acesso aos sistemas interativos da Anatel só precisam inserir login e senha. Usuários que ainda não possuem acesso devem clicar em “Não sou cadastrado” e seguir os passos descritos. Após acessar o sistema, é preciso clicar em “Outorga - Pedidos de Outorga” para ter acesso aos pedidos já iniciados. Para novos pedidos, clique em “Nova Outorga”.

3º passo: Preenchimento da solicitação da licença SCM

O preenchimento da solicitação de Serviço de Comunicação Multimídia segue basicamente três passos:

- Formulário
- Anexos
- Termos e condições

Em “+ Nova Outorga”, selecione o serviço desejado, informe os dados do Representante Legal, que deve possuir acesso aos sistemas interativos da Anatel. Confira as informações enviadas. O e-mail informado deve ser o mesmo cadastrado no SEI. Clique em “Enviar Código” e acesse seu e-mail para verificar e copie e cole o código recebido no campo “Validação de e-mail”.

Na seção “Entidade”, preencha o CNPJ e clique em “Buscar”. O sistema irá consultar os dados da empresa na Receita Federal e preencher automaticamente alguns campos do formulário.

Na seção “Endereço Correspondência”, preencha para onde devem ser enviadas as correspondências geradas no processo.

Na seção “Qualificação dos Diretores ou Responsáveis”, preencha quem serão os responsáveis pelo processo na empresa.

Continue preenchendo o formulário de acordo com o que for pedido. Ao final, clique em “Validar” e “Salvar Aplicação”. Você será direcionado para a lista de solicitações. Clique na lista ao lado da solução recém-criada e selecione “Enviar”.

4º passo: Cadastro de documentos

Continuando a solicitação da licença SCM, clique na lista de ações ao lado da solicitação criada e selecione “Anexar Documentos”. Será

apresentada uma lista de documentos que precisam ser anexados ao processo. Leia a descrição de cada um deles e os requisitos a serem atendidos antes de anexá-los. Caso seja apresentado o campo “Data de Expiração” para algum documento, informe a data de validade daquele documento. Após carregar todos os documentos obrigatórios, clique em “Enviar”. Se todos os documentos obrigatórios foram carregados apropriadamente, o sistema irá cadastrar os documentos e o usuário será redirecionado para a tela que lista suas solicitações. Clique na lista de ações ao lado da solicitação recém-criada selecione “Enviar” e clique no botão de execução da ação. Em seguida, sua solicitação estará na fase: “Em Cadastramento de Termos e Condições”. Clique na lista de ações ao lado da solicitação desejada e selecione “Termos e Condições”. Leia as declarações apresentadas na tela, e caso concorde, selecione a caixa “Atesto a veracidade das declarações acima” e clique no botão “Enviar”.

5° passo: Acompanhamento

Na tela que lista as solicitações do usuário, aparecerão duas linhas:

- Aguardando análise Técnica
- Aguardando análise Jurídica

Em ambos os casos, o interessado tem acesso ao número do processo criado no sistema SEI e pode consultá-lo diretamente por ali. A seguir, a Anatel envia um e-mail para que o usuário acesse o Mosaico e vá em “Ver exigências”. A partir desse acesso, começa a contar o prazo para a obtenção da licença SCM, que é de 10 dias. Se o usuário não acessar, a Anatel tentará o contato pelo envio de um ofício, que também o guiará a entrar no Mosaico para ver as exigências. Em uma terceira e última tentativa, o analista responsável pelo processo tentará entrar em contato com o interessado.

Se restar qualquer dúvida, a Gerência de Outorga e Licenciamento de Estações da Anatel disponibilizou um e-mail para que os usuários possam entrar em contato sobre a licença SCM: orle@anatel.gov.br.