CONTROLE DE ACESSO A REDE WIRLESS EM AMBIENTE MUTIPLATAFORMA

Autor
Patrick Cohenn Resende Marques Fernandes
patrickcohenn@gmail.com

Orientador
Edilberto Pereira Teixeira
Edilbeto.teixeira@uniube.br

Resumo
Com o crescente número de aparelhos tecnologia suficiente para ter acesso à internet vem crescendo também o ponto de acessos à rede sem fio com isso vem surgindo à necessidade de gerar segurança para ambas as partes que utilizam este tipo de conexões, pois uma rede sem fio não tem como limitar o seu alcance com facilidade igual podemos realizar com a rede cabeada. Com o passar do tempo muitas pesquisas foram realizadas e delas surgiram alguns protocolos de segurança na atualidade, não traz muita segurança com isso vem surgindo alguns Software para auxiliar os protocolos e alguns deles são gratuitos e de fácil customização. Alguns deste Software é o PfSens, Active Directory e o RADIUS que serão utilizados neste artigo.

Palavras-chave: Pfsense. RADIUS. Wi-Fi. Captive Portal.

Abstract
With the increase in the number of high-tech devices for access to the Internet with wireless access points also increasing, there is a need to generate security for the parties that use this type of connection, since a wireless network. How to limit your reach with equal ease, we can perform with the wired network. Over time, many searches have been carried out and have arisen from security protocols at the present time, it does not bring much security with that comes some Software to assist the protocols and some of them are free and easy to customize. Some of this software will be the PfSens, Active Directory, and RADIUS that are used in this article.

Keywords: Firewall. Pfsense. RADIUS. Wi-Fi. Captive Portal.

Lista De Ilustrações

Lista De Gráficos

Lista De Abreviaturas, Siglas E Acrônimos

LAN	Local Area Network
WLAN	Wireless Local Area Network
IEEE	Institute of Electrical and Eletronics Engineers
UTM	Unified Threat Management
AD	Active Directory
WAP	WiFi Protected Acess Version
WAP2	WiFi Protected Acess Version 2
AD	Active Directory
RADIUS	Remote Authentication Dial In User Service

1. INTRODUÇÃO

Com o avanço das pesquisas sobre as ondas de rádio cada vez mais crescente na atualidade, e com isto trazendo muitas vantagens para transmissão de dados, pois cada vez mais podemos transmitir informações como maior distância e qualidade e com isso não demorou muito para ser utilizada na transmissão de informações computacionais, com este tipo de conexão nos permite uma maior flexibilidade e podendo gerar rede entre grandes distâncias. Como este tipo de transmissão pode-se ultrapassar muitas barreiras físicas como paredes, moveis entre outras, mesmo que venha gerar uma queda de qualidade em seu sinal de transmissão ele pode chegar a lugares não desejados, e por este motivo isso se tornou um grande problema.

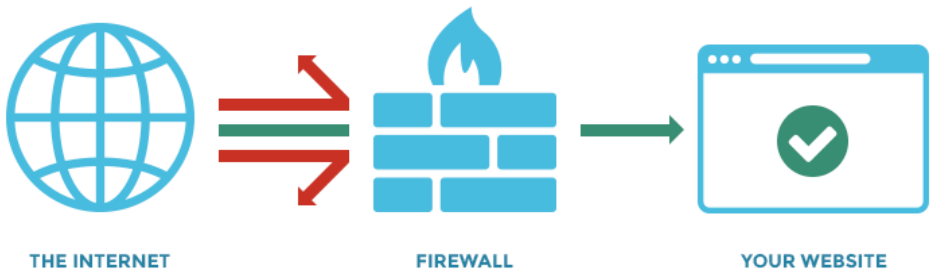
Uma conexão em rede de computadores é quando dois ou mais computadores autômatos estão interconectado, com isso podem compartilhar informações entre eles por um meio físico ou não de comunicação. Os meios são compostos por fios (cobre), fibra óptica, microondas entre outras e não possuem mestre ou escravo entre eles segundo TANEMBAUM (1981).

A conexão sem fio conhecida também como Wireless e é uma Local Area Network ou conhecida somente por LAN, porém ela recebeu o nome de WLAN para que seja diferenciada da rede local cabeada. Uma conexão WLAN nada mais que um sistema que converte o pacote de dado gerado por um dispositivo em onda de rádio e envia para outro dispositivo ou para outra rede.

Na atualidade o tipo de conexão WLAN tem como padronização IEEE 802.11 no qual tem alguns problemas de segurança e com o decorrer do tempo ele vem sofrendo alterações para que sejam corrigidos esses problemas com isso surgiu o WEP significa Wired Equivalent Privacy, no entanto não foi o suficiente e continuou com muita vulnerabilidade mesmo com um algoritmo RC4 e com chave compartilhada segundo TEWS (2007). Em 2004 chegou emenda IEEE 802.11i ou WAP2 (WiFi Protected Acess Version 2) com melhoria na confiabilidade, integridade e autenticidade. Porém em 2009 foi criada última emenda IEEE 802.11w.

Um Firewall é uma solução que pode ser hardware ou software no qual o software são os mais comuns que, eles possuem um conjunto de instruções e regras, e sem falar que ele irá analisar o tráfego de rede e determinar quais sãos as informações que podem passar ou não por ele. A sua tradução livre é "Parede de fogo", no qual já deixa bem claro a sua função na rede. A sua função principal é funcionar como uma barreira deixando passar ou não conforme são suas regras.

Figura 1 Representação básica de um firewall



Fonte: Danielle. **What is a Firewall, and Why Do You Need It?** : Disponível em > https://www.powderkegwebdesign.com/what-is-a-firewall/ Acessado em maio de 2017

O RADIUS é nada mais que um protocolo que possui como arquitetura conexão entre servidor e cliente. Quando o usuário começa a utilizar uma rede às informações dos dispositivos são encaminhadas para algum serviço NAS (No caso de estudo é o RADIUS). E logo após a chegada destas informações o RADIUS irá solicitar as informações de autenticação do como login e senha do usuário, na forma de mensagem ou pelo próprio navegador, como citado pelo CARISANI, Rafael Vicente, e HELIO Crestana Guardia (2016). Após a autenticação ser verdadeira o usuário poderá utilizar o serviço conformar for especificado nos servidores.

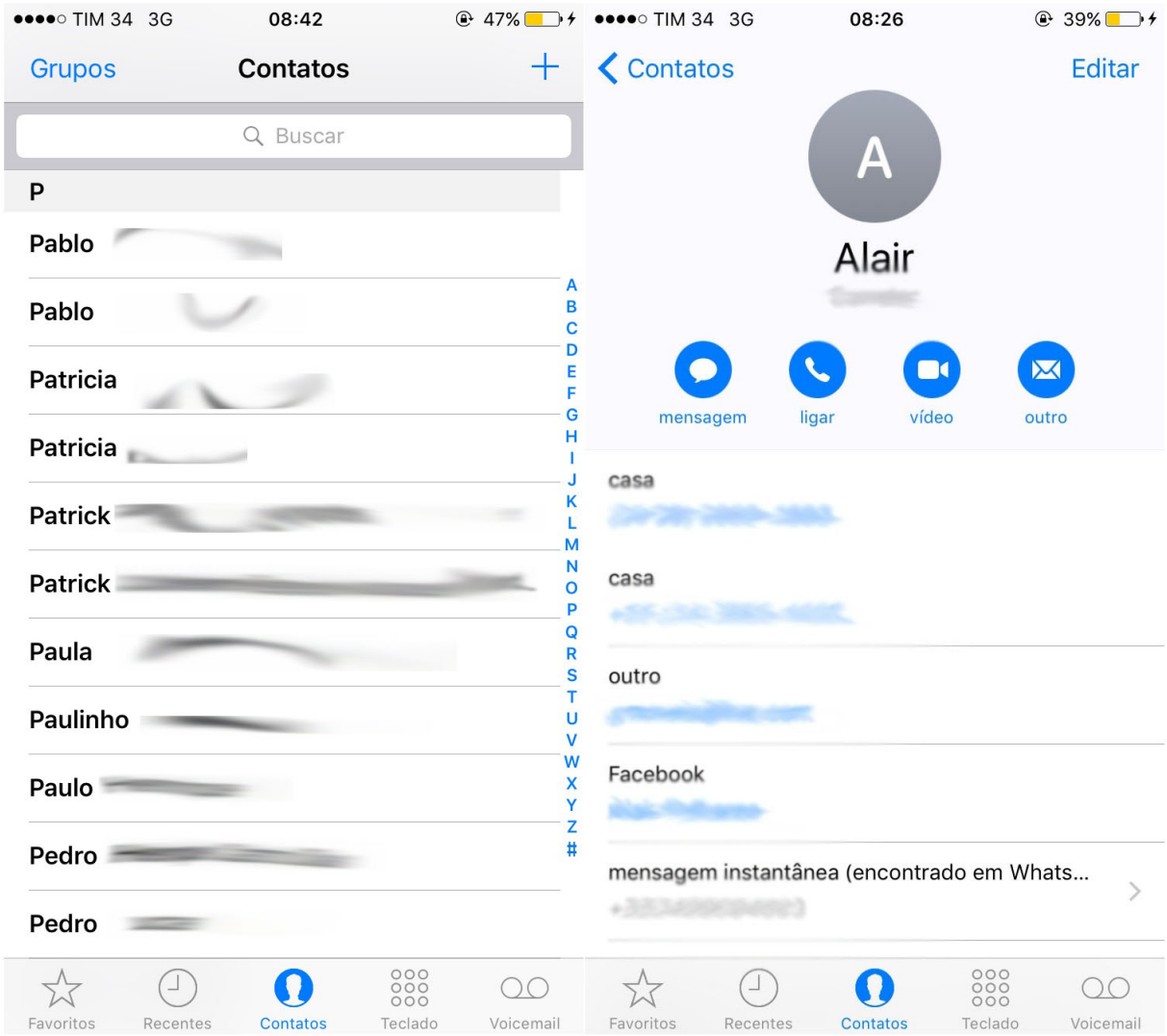
Com a grande flexibilidade do protocolo e com as diversas tecnologia agregado no RADIUS podemos configurar a autenticação local ou mesmo via PROXY no qual irá redirecionar para o Servidor (Proxy PfSense). O RADIUS ele intermedia as mensagens trocadas entre cliente e servidores somente quando ele está a configurar para ser utilizado como PROXY.

O PfSense é um sistema operacional livre baseado em FreeBSD, como foi citado pelos (SEVERINO, Paulo Jacinto Rosa; ARAÚJO, Fabrício Geraldo 2016), no qual pode ser customizado conforme a necessidade e seus pacotes adicionais

podem considerar ele um UTM (Unified Threat Management, "Central Unificada de Gerenciamento de Ameaças") este é uns dos motivos que vem crescendo sua em muitas redes.

O Active Directory e um serviço que podemos explicar de uma forma mais simples como uma agenda de um smartphones no qual demonstra qual o sentido da AD.

Figura 2 Agenda de um smartphones



Na agenda de contatos podemos organizar todos os contatos com algumas informações como aniversários, número de telefones, endereços, e-mails e muito mais. Como foi citado por Marinho Rover (2012), uma das principais funções de um serviço AD e organizar e ter um local central para que deixe a busca de informações mais rápida e fácil para que seja utilizada durante o dia a dia.

Quando precisamos criar um novo usuário iremos utilizar o serviço AD para guardar as informações principais do usuário como nome, telefone, nome de usuário, senhas e muito mais podemos até mesmo definir um grupo especifico para este usuário para que facilite na gerencia de até onde ele pode utilizar a rede.

2. INFRAESTRUTURA DA REDE

O ambiente escolhido para este projeto foi um hotel localizado em Uberaba próximo parque de exposição no qual foi escolhido por ser um local rotativo e com um grande fluxo de pessoas que possuem dispositivos com a tecnologia para conectar a uma rede WLAN. Onde temos uma grande variedade de usuários, que são compostos em geral por clientes, funcionários e administradores do estabelecimento.

O ambiente possui:

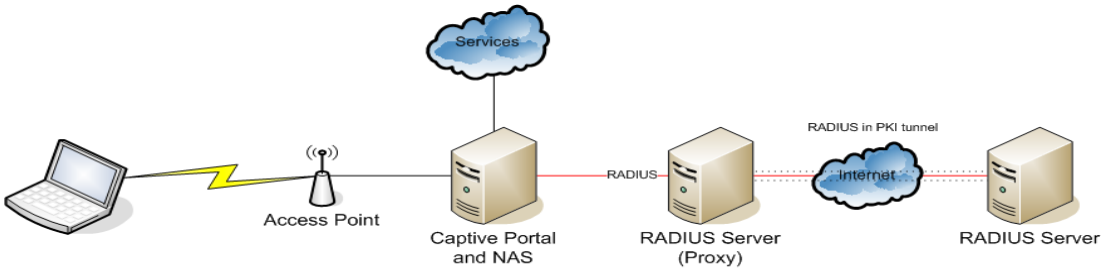
- 1 Servidor com o Windows Server 2012;
- 1 Servidor para o PfSense;
- 2 Access Point;
- Alguns dispositivos com tecnologia Wi-Fi de rede como smartphones, tablets e notebooks.

A Figura 3 está representando um processo para autenticar dos logins que irá ser realizada nos seguintes locais da rede. O processo iniciara primeiro no servidor do PfSense e posterior AD (Active Directory) por fim o RADIUS (Remote Authentication Dial In User Service).

Quando algum usuário tentar se conectar na rede wireless com algum dispositivo e ele realiza a verificação incialmente se ela está disponível. Quando a rede estiver disponível irá iniciar o processo de autenticação para ter acesso a WLAN após isso o Active Directory envia uma solicitação para o PfSense e o navegador do dispositivo será aberto e irá solicitar os dados do usuário para que tenha o acesso permitido ou negado dependendo do que o usuário digitar. O

PfSense enviará ao RADIUS os dados do login. No RADIUS será feita a verificação no *database* do AD para saber se os dados informados são válidos. Em caso de a validação ser positiva o RADIUS avisa para o PfSense que são dados positivos e irá liberar o acesso daquele dispositivo e controlar o tráfego de dados conforme a regra configurada no servidor Proxy.

Figura 3 Método de autenticação do login



Fonte: https://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service Acessado em 12 de maio 2017

2.1. CONFIGURAÇÃO DO PFSENSE

O PfSense foi instalado em um dispositivo igual ao do servidor com o sistema da Microsoft:

- Processador Intel Core i5-3337U 1.8GHz 64bits.
- 8 GBs de memória RAM.
- 1 TBs de disco rígido.

Por tratar-se de um sistema operacional customizado do FreeBSD e por este motivo ele utiliza poucos recursos quando comparados com solicitado pelo Sistema da Microsoft, com isso ele pode ser instalo em computadores mais simples que seus concorrentes e com isso ele vem sendo utilizados em pequenas redes, porem ele tem potencial para grandes redes como de grandes empresas. Assim o hardware atende todos os requisitos para o PfSense. A instalação do PfSense conteve as seguintes configurações:

- Interface para a LAN;

- Serviço Proxy;
- Servidor de DHCP;
- Captive-Portal.

Lembrando que quando decidimos o protocolo para a autenticação temos por obrigação utilizar ele RADIUS e no PfSense, pois caso contrário irá apresentar falha na autenticação dos logins.

Na Figura 4 temos o ambiente de usuário e senha que é do Captive-Portal do PfSense para que o usuário realize a autenticação na rede Wi-Fi. Uma vez a autenticação for verdadeiras, o usuário poderá utilizar a wireless seguindo as suas permissões de acesso.

Figura 4 Tela de inserção de dados para acessar a Rede sem Fio

2.2. WINDOWS SERVER 2012

Neste artigo foi utilizado o seguinte hardware para o servido com o sistema da Microsoft Windows Server 2012 no qual este servido já era utilizado no estabelecimento.

- Processador Intel Core i5-3337U 1.8GHz 64bits.
- 8 GBs de memória RAM.
- 1 TBs de disco rígido.

A informação encontrada no site oficial da Microsoft tem como recomendações mínimas os seguintes requisitos.

- 1,4 GHz (processador de 64 bits) ou mais rápido para núcleo único.
- Memória RAM 2 GB.
- Disco rígido de 160 GB com uma partição de sistema de 60 GB.

O Windows Server 2012 foi escolhido por quer o estabelecimento adquiriu o mesmo quando foi realizou a compra do dispositivo.

3. RESULTADOS OBTIDOS

Para validar processo proposto, inserimos alguns usuários no sistema de AD. Foram adicionados os logins com o *username* como “usuario1, usuario2, usuario3…” e como senha padrão para todos os usuários teste será numerais de 1 até o 8.

Os testes que foram realizados são:

- Tempo de resposta para o usuário digitar seus dados.
- O tempo de verificação dos dados do login.
- Verificação das validações de segurança.

3.1. CONFIGURAÇÃO DOS DISPOSITIVOS DOS CLIENTES

Foram realizados os testes em dois tipos de clientes. O primeiro dispositivo era uma que tinha como sistema principal o Windows 8 (64 bits) e a segundo tinha distribuição Fedora 25 (64 bits).

Os dispositivos dos clientes Windows como Fedora possuem o mesmo hardware.

- Processador Intel Core i5-3337U 1.8Ghz 64bits.
- 250 GBs de Disco Rígido (HD)
- 6 GBs de memória RAM DDR3.

Ambas as estações dos clientes foram recém-formatada para que não tenha qualquer tipo de alteração no tempo de resposta e foram instalados os seguintes navegadores Google Chrome e Firefox, com o motivo de serem os navegadores mais utilizados ultimamente no brasil.

3.2. LOCAL DOS TESTES

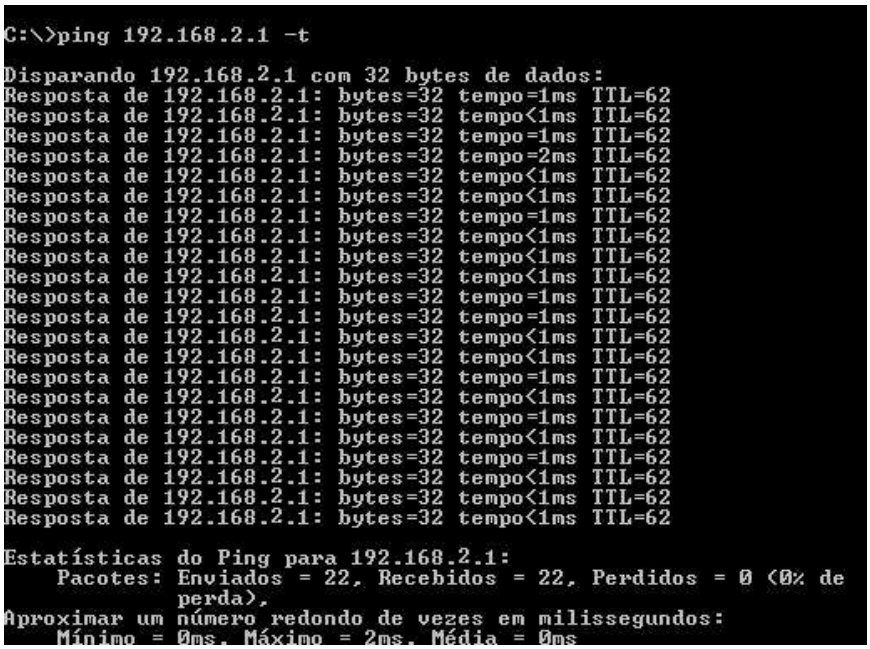
Em uma sala com os servidores e com os softwares do estabelecimento no primeiro andar e o segundo local de teste foi realizado também no segundo pavimento. Forma instalado dois *Acess Points* (APs) no estabelecimento, com um no primeiro piso onde a recepção e alguns outros quartos e outro no segundo piso onde fica os demais quartos dos hospedes o PfSense.

RADIUS e AD ficaram na sala que localizam os servidores no primeiro andar. Foi realizado um teste inicial da rede para ter como um parâmetro e o tempo que foi gasto na deslocação de um dado entre os *Acess Points* e o PfSense conseguiram os seguintes dados.

Os dados encontrados foram registrados nas Figuras 5 e 4.

Figura 5 Tempo de resposta do primeiro APs com PfSense

Figura 6 Tempo de resposta do segundo APs com PfSense



Nas figuras acima foram mostradas o tempo médio de resposta dos APs e na *interface* PfSense tiveram tempo menores de 1ms, podemos desconsiderar este tempo para este cenário.

3.3. TEMPO DE RESPOSTA DA PAGINA DE AUTENTICAÇÃO

De acordo com o Aiftimiei *et al* (2012), quando iniciar um navegador, o usuário em sua maioria aguarda que sua tela inicial seja carregada no menor tempo possível, mesmo que este não seja a página final para o usuário. A maioria dos navegadores está configurado como pagina principal sites de busca ou até mesmo em alguns casos como alguma página de autenticação. Se o tempo de resposta da página for maior de 250ms para carregar a página inicial, poderá causar desconforto para o usuário.

Foram utilizadas duas aplicações gratuitas que tem como finalidade a analisar do tempo de resposta da página de autenticação.

São elas:

- *Page Speed Monitor: Plug*in para o Firefox.
- *DevTools:* Chrome T*ools*.

O teste que foi realizado mostrou o tempo de resposta da tela de autenticação de login. Utilizamos uma amostra de 50 acesso na tela de autenticação em cada

navegador em cada dispositivo de cliente. Os resultados encontrados estão mostrados na Gráfico 1.

Como mostra na Gráfico 1 os tempos de resposta dos navegadores nas estações dos clientes. Podemos observar uma melhor resposta no navegador Firefox no sistema Windows com o tempo entre 39ms e 84ms. O tempo médio no navegador

Firefox

- 55ms no Windows;
- 53ms no sistema Fedora (Linux);

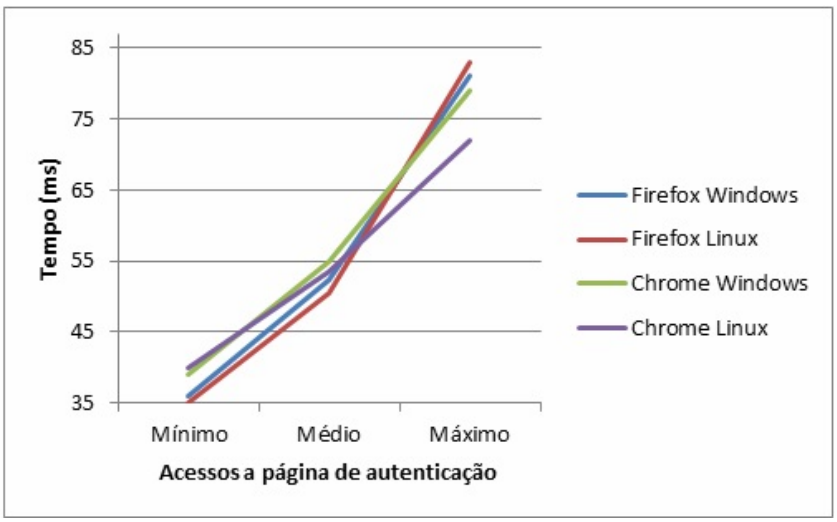
Google Chrome

- 58,02ms no Windows;
- 56,4ms no Fedora (Linux):

Nestes dados podemos observar que os clientes que utilizam o navegador Firefox, o tempo gasto para abrir a página de autenticação do login foi menor que os usuários que utilizam o navegador da Google Chrome. E comparando os clientes que utilizam sistema operacional Linux foi melhor que os possui sistema operacional do Windows.

Comparando os dados que encontramos com os dados de Aiftimiei *et al* (2012), de 120ms com um ressaltado em tem como média final de 55,7ms e tivemos uma média menor e por este motivo pode considerar satisfatório.

Gráfico 1 Tempo de resposta de autenticação de login



3.4. VALIDAÇÃO E AUTENTICAÇÃO DE DADOS DO LOGIN

O teste realizado agora será um dos mais importante que será realizado, pois, se tiver alguma falha na autenticação qualquer pessoa poderá passar por qualquer usuário com isso ele poderá ter acesso às informações a dados da rede.

Nesta etapa foram escolhido os seguintes requisitos para teste:

- Todos dados de login incorretas.
- Todos dados de login corretas.
- Metade dos usuários de forma aleatórios com senha “123123”.

Nesta parte do teste obtivemos um resultado de 100% do esperado. O objetivo deste teste foi saber se os usuários vão ter acesso ou não conforme os dados informando na página de autenticação e até onde cada usuário poderá acessar conforme a configuração do Servidor. O resultado encontrado nesta etapa foi adquirido através dos históricos de *logs* do servidor *Windows Server no* qual tem a aplicação AD.

3.5. TEMPO DE RESPOSTA DE AUTENTICAÇÃO DOS LOGINS

Nesta etapa iremos utilizar como requisito os mesmos parâmetros utilizados no item 3.4 neste item iremos utilizar os dispositivos que deixamos como dos clientes no item 3.3. Iremos utilizar series de cinquenta por usuários como amostra dos cadastrados no servidor como estão descritos no item 3. Encontramos os seguintes resultados:

3.5.1- VALIDAÇÃO COM DADOS DE LOGIN INCORRETOS

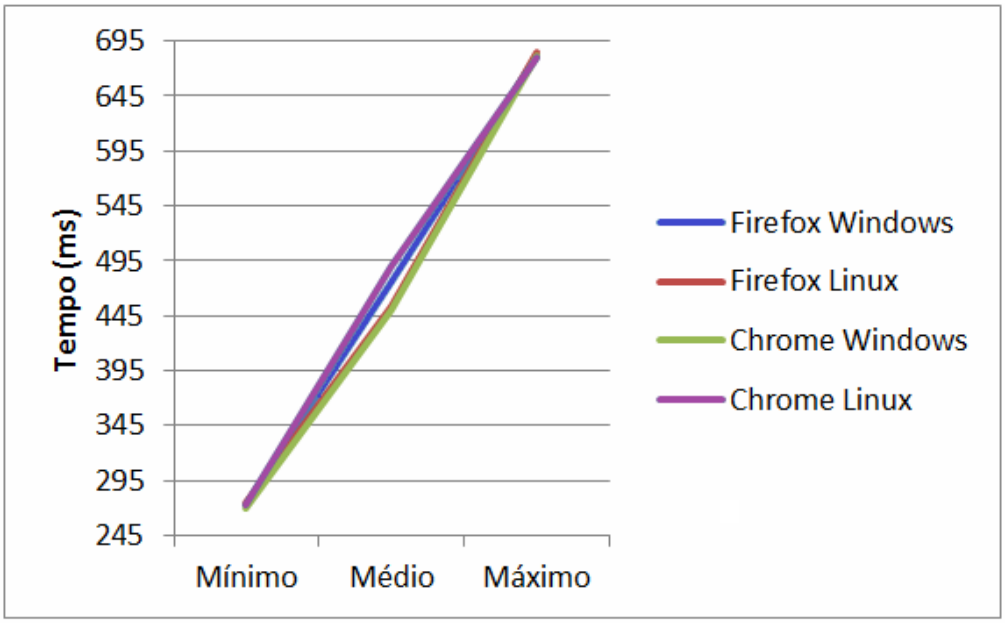
No gráfico 2 demonstra à variação do tempo durantes as cinquentas tentativas do acesso com senhas e/ou username incorretas.

O gráfico 2 demonstra que toda tentativa de resposta da autenticação os tempos ficaram entre 255ms até 665ms. Tivemos como tempo médico nos navegadores foi:

- Firefox
  - 470,5ms no Windows
  - 447,81ms no Fedora:

- Chrome
  - 443,4ms no Windows:
  - 483,54ms no Fedora:

Gráfico 2 Tempo de resposta com dados incorretos do login



3.5.2- VALIDAÇÃO COM TODAS AS SENHAS CORRETAS

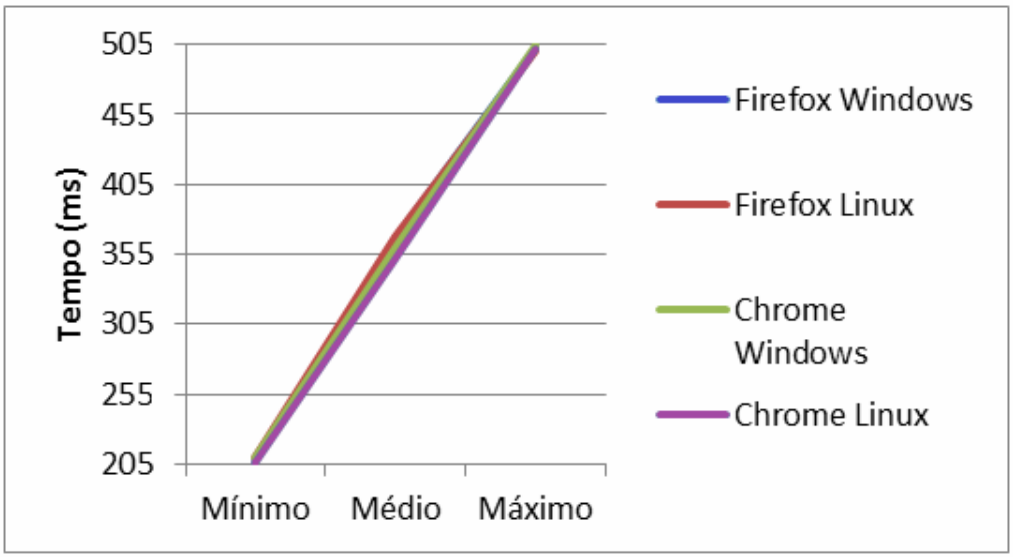
No Gráfico 3 mostra o tempo de autenticação com os dados corretos de todas tentativas. Os dados que foram encontrados no Gráfico 3 mostra que os resultados médios ficaram entre o intervalo de 205ms e 505ms. Essas informações foram orbitadas através da *Page Speed Monitor e DevTools:* Chrome T*ools* foram:

- Windows:

- 361 ms no Firefox.
- 353,4 ms no Chrome.

- Fedora
  - 365,1 ms no Firefox.
  - 346,3 ms no Chrome.

Gráfico 3 Tempo de resposta com dados corretos dos usuários



Comparando o gráfico 2 com o gráfico 3 percebesse que o tempo de resposta de autenticação dados incorretos é maior que os tempos que possui dados correto.

3.5.3- USUÁRIOS ALEATÓRIOS COM SENHA “123123”

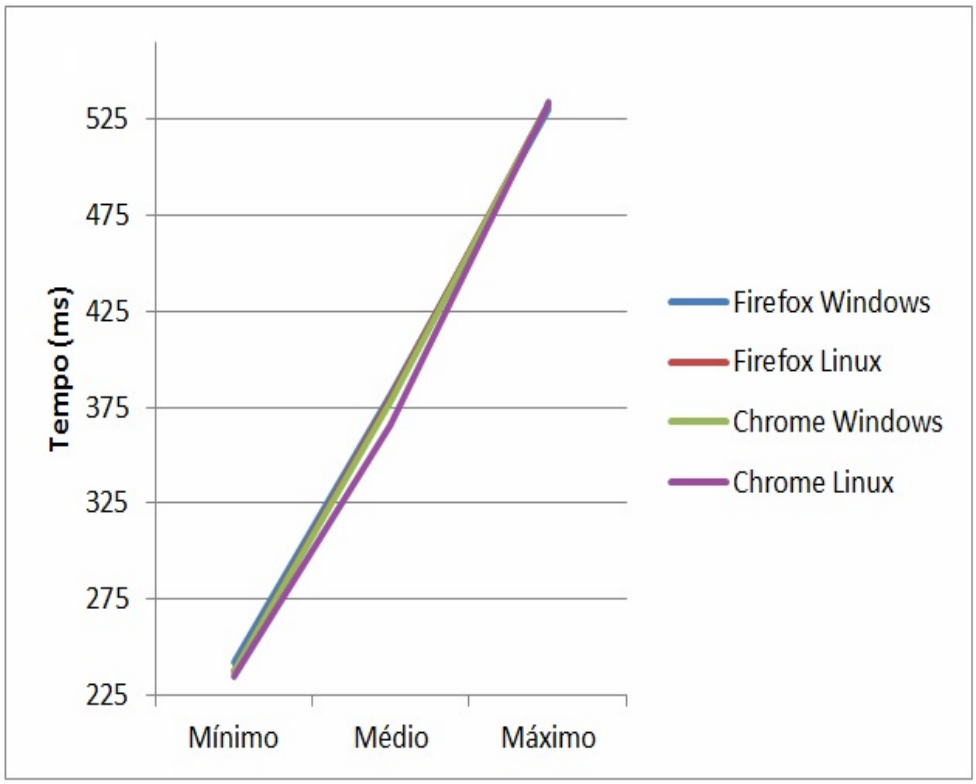
No gráfico 4 teremos o tempo de resposta de cinquentas tentativos acesso ao sistema no qual vinte e cinco fora com senha incorreta e foi escolhido por padrão de “123123”.

Nos resultados encontrados foram mostrados que em todas tentativa de autenticação de login os tempos ficaram entre os intervalos de 225ms e 535ms. As médias de tempo obtidas por navegadores foram:

- Firefox
  - 375,44ms no Windows.
  - 373,8ms no Linux.

- Chrome
    - 373,53ms no Windows.
    - 361,7ms no Linux.

Gráfico 4 Tempo de resposta com senha "123123



Comparando com os gráficos anteriores, nota que o tempo médio se encontra entre os valores anteriores. Podendo sugerir que alguns usuários tentam acessar com diferente da cadastrada gera uma demora dos servidores para responder o tempo de autentificarão dos logins.

4. CONCLUSÃO

No ambiente em que foi estudado mostrou que com as ferramentas utilizadas podemos realizar um controle de acesso e gerenciar uma rede com uma eficaz sem precisar-te grandes gastou ou com dificuldade e os testes que foram realizados tiveram resultados como esperados. Todo hardware que foram utilizados são os mais comuns utilizados ultimamente.

Com os dados coletados nos testes que foram realizados neste artigo obtivemos que o tempo de autenticação são aceitáveis e podem até ser considerado rápidos, mesmo que em algum teste chegando próximo dos 500ms, no qual este tempo para os usuários podemos considerar desprezíveis.

5. REFERENCIA

FRANCO, Bruno Santolin Dornelles. **Gerenciamento de uma rede sem fio com pfSense**. 2015. Trabalho de Conclusão de Curso. Universidade Tecnológica Federal do Paraná.

MARVÃO Susana: **25% das redes Wi-Fi públicas não são seguras, diz Kaspersky**: Disponível em: http://www.bitmag.com.br/2016/11/25-das-redes-wi-fi-publicas-nao-sao-seguras-diz-kaspersky/> Acesso em Abril 2017.

DALLABONA, Nilson Sérgio. Segurança da informação: uma proposta para projeto de rede baseada em software livre. 2013.

PEREIRA, Júlio Cesar; SILVA, Rafael Mariano Rodrigues. **A Importância De Firewall's Para Ambientes Corporativos.** Paranavaí. 2015. Disponível em: <web. unipar.br/~seinpar/2015/_include/artigos/Rafael_Mariano_Rodrigues_Silva.pdf>. Acesso em: Jan 2017.

SILVA, Veridiano António Fernandes de Carvalho. **Soluções wireless/VoIP para redes comunitárias**. 2010. Dissertação de Mestrado. Universidade de Aveiro.

SOUZA, Leonardo. **Servidor DHCP no PfSense. 2015**. Disponível em: < http://mundofreebsd.com.br/servidor-dhcp-no-pfsense/>. Acesso em: Jan 2017.

SILVA, Cesar Augusto; PERUFFO, Leandro. **Artigo em segurança de rede - pfsense**. Campinas. 2015. Disponível em: < http://www.trabalhosfeitos.com/ensaios/Artigo-Em-Seguran%C3%A7a-De-Rede/305286.html>. Acesso em: Out 2016.

MARINHO Rover. **O que é o Active Directory.** São Paulo. 2017. Disponível em < http://www.linhadecodigo.com.br/artigo/2422/o-que-e-o-active-directory.aspx> Acesso em: Maio 2017

CABIANCA, Luís Antonio. BULHMAN, Haroldo José **Redes LAN / MAN Wireless I: Padrões 802.11 a, b, e g.** Campinas. 2015. Disponível em: < http://www.teleco.com.br/DVD/PDF/tutorialrwlanman1.pdf>. Acesso em: Maio 2017.

DOS SANTOS PINHEIRO, José Maurício. Ameaças e Ataques aos Sistemas de Informação: Prevenir e Antecipar. **Cadernos UniFOA**, v. 3, n. 5, p. 11-21, 2017.

Microsoft**. Protocolo RADIUS**. Disponível em: https://technet.microsoft.com/pt-br/library/dd197481(v=ws.10).aspx > Acesso em: Maio 2017.

CARISANI, Rafael Vicente, and HELIO Crestana Guardia. "**Identificação dos Usuários em Rede Corporativa.**" *Revista TIS* 4.2 (2016). Acesso em Maio 2017.

Marocco, Carlos Alberto Duarte. "**Proposta de topologia de rede de dados com segurança e foco na produtividade, utilizando ferramentas de software livre (2016)**." Disponível em: < http://repositorio.uniceub.br/bitstream/235/8157/1/51307936.pdf> Acessado em Maio 2017.

SEVERINO, Paulo Jacinto Rosa; ARAÚJO, Fabrício Geraldo. **CRIAÇÃO DE UMA INFRAESTRUTURA DE REDE ABORDANDO VLANS, UTILIZANDO PFSENSE NO ROTEAMENTO**. In: **XIII-Congresso Mineiro de Empreendedorismo 2016**. > acessado em maio 2017.

BATTISTI. Júlio. **WINDOWS 2000:** AD – Active Directory**.** Campinas. 2015. Disponível em: < http://www.juliobattisti.com.br/fabiano/artigos/activedirectory.asp >. Acesso em maio 2017.

Sallum, William Geraldo, and Marcelo Caramuru Pimentel Fraga. "**Sistemas Operacionais II**." (2016).

ROVER, Marinho. **O que é Active Directory, topologia física e lógica?** Parte1**.** Campinas. 2015. Disponível em: < https://technet.microsoft.com/pt-br/library/jj206711.aspx>. Acesso em maio 2017.