UNIVERSIDADE FEDERAL DE SANTA MARIA
COLÉGIO TÉCNICO INDUSTRIAL DE SANTA MARIA
CURSO SUPERIOR DE TECNOLOGIA EM REDES DE COMPUTADORES

Daniel Visentini de Barcelos

IMPLEMENTAÇÃO DE UM SISTEMA PARA AUXILIAR NA RASTREABILIDADE DE USUÁRIOS NO ÂMBITO DA UFSM

Santa Maria, RS
2017

Daniel Visentini de Barcelos

IMPLEMENTAÇÃO DE UM SISTEMA PARA AUXILIAR NA RASTREABILIDADE DE USUÁRIOS NO ÂMBITO DA UFSM

Trabalho de Conclusão de Curso (TCC) do Curso Superior de Tecnologia em Redes de Computadores, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Tecnólogo em Redes de Computadores.**

Orientador: Prof. Ms. Tiago Antonio Rizzetti

Santa Maria, RS
2017

Daniel Visentini de Barcelos

IMPLEMENTAÇÃO DE UM SISTEMA PARA AUXILIAR NA RASTREABILIDADE DE USUÁRIOS NO ÂMBITO DA UFSM

Trabalho de Conclusão de Curso (TCC) do Curso Superior de Tecnologia em Redes de Computadores, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Tecnólogo em Redes de Computadores.**

Aprovado em 12 de julho de 2017:

_____

Tiago Antonio Rizzetti, Me. (UFSM)
(Orientador)

_____

Bolívar Menezes Da Silva, Tecg. (UFSM)

_____

Alexandre Silva Rodrigues, Tecg. (UFSM)

Santa Maria, RS
2017

DEDICATÓRIA

Dedico este trabalho à minha mãe Lucia Pedrosina Visentini de Barcelos e à meu pai José Renildo Rossine de Barcelos que nunca deixaram que viesse a faltar algo em nossa casa e foram fundamentais em minha formação moral e ética. Dedico também a minha esposa Raquel Manhago Zimmermann e meu filho Murilo Zimmermann de Barcelos, como forma de agradecimento pelo apoio e companheirismo prestados.

AGRADECIMENTOS

Agradeço a todos que, de alguma forma, contribuíram para conclusão desta jornada e, de maneira especial, agradeço:

- à minha família pelo amor, incentivo e apoio incondicional;

- ao meu orientador Tiago Antonio Rizzetti pela oportunidade e apoio na elaboração deste trabalho;

- aos meus amigos e colegas, pelo incentivo e pelo apoio constante;

Enfim a todos àqueles que fazem parte da minha vida e que contribuem na minha jornada e trajetória.

Determinação, coragem e auto-confiança são fatores para o sucesso. Se estamos possuídos por uma inabalável determinação, conseguiremos superá-los. Independentemente das circunstâncias, devemos ser sempre humilde, recatados e despidos de orgulho.

(Dalai Lama)

RESUMO

IMPLEMENTAÇÃO DE UM SISTEMA PARA AUXILIAR NA RASTREABILIDADE DE USUÁRIOS NO ÂMBITO DA UFSM

AUTOR: Daniel Visentini de Barcelos
ORIENTADOR: Tiago Antonio Rizzetti

Este trabalho apresenta o estudo que a Universidade Federal de Santa Maria está implementando, um *Captive Portal* para Moradia Estudantil na Casa do Estudante localizada Campus do centro da cidade de Santa Maria, com o intuito de prover autenticação de usuários e guarda das conexões de acesso à Internet Acadêmica e Comercial, considerando a Norma Complementar do DSIC (21/IN01/DSIC/GSIPR), que trata das "Diretrizes para o registro de eventos, coleta e preservação de evidências de Incidentes de Segurança em Redes" e o Marco Civil da Internet. A rede da Moradia Estudantil não se integra as demais da Instituição, possui um domínio de broadcast único. Seu contato com a rede da UFSM e Internet Acadêmica/Comercial se dá através de um IP único ao sofrer *NAT*. Após realização de testes, os quais se mostraram bastante satisfatório, foi realizada a implementação do sistema, que está em pleno funcionamento e em processo de expansão.

Palavras-chave: Captive Portal, firewall, pfSense, RADIUS, LDAP.

ABSTRACT

IMPLEMENTATION OF A SYSTEM TO AUXILIATE USER TRACEABILITY IN THE FIELD OF UFSM

AUTHOR: DANIEL VISENTINI DE BARCELOS
ADVISOR: TIAGO ANTONIO RIZZETTI

This work presents the study that the Federal University of Santa Maria is implementing a Captive Portal for Student Housing in the Student House located in Campus of the city center of Santa Maria with the purpose of providing user authentication and guarding of Internet access connections Academic And Commercial, considering the DSIC Supplementary Standard (21 / IN01 / DSIC / GSIPR), which deals with the "Guidelines for the recording of events, collection and preservation of evidence of Security Incidents in Networks" and the Civil Internet Framework. The Student Housing network is not integrated with the rest of the Institution, it has a unique broadcast domain. Your contact with UFSM and Academic / Commercial Internet is through a unique IP when suffering from NAT. After performing tests, which proved to be quite satisfactory, the system was implemented, which is in full operation and in the process of expansion.

Keywords: Captive Portal, firewall, pfSense, RADIUS, LDAP.

LISTA DE FIGURAS

LISTA DE ABREVIATURAS E SIGLAS

LDAP	*Lightweight Directory Access Protocol*
DAP	*Directory Access Protocol*
OSI	*Open Systems Interface*
IETF	*Internet Engineering Task Force*
RFC	*Request For Comments*
SSL	*Secure Sockets Layers*
SASL	*Simple Authentication and Security Layer*
DIT	*Directory Information Tree*
DSE	*Directory Service Entry*
DN	*Distinguished Name*
RDN	*Relative Distinguished Name*
LDIF	LDAP *Data Interchange Format*
RADIUS	*Remote Authentication Dial In User Service*
AAA	*Authentication, Authorization and Accounting*
NAS	*Network Autentication Server*
PPP	*Point-to-Point Protocol*
PAP	*Password Authentication Protocol*
CAHP	*Challenge Handshake Authentication Protocol*
HLB	Hora Legal Brasileira
ON	Observatório Nacional
SIC	Segurança da Informação e Comunicações
IP	*Internet Protocol*
SSH	*Secure Shell*
UTM	*Unified Threat Management*
NTP	*Network Time Protocol*
DNS	*Domain Name System*
MAC	*Media Access Control*
DHCP	*Dynamic Host Configuration Protocol*
CPF	Cadastro de Pessoas Físicas

SUMÁRIO

1. INTRODUÇÃO

Com o amplo acesso da comunidade acadêmica aos recursos de Internet, a Universidade Federal de Santa Maria (UFSM) passou a receber notificações, informando violações das restrições de uso. Sem capacidade de rastrear a origem de acesso a instituição nada pode fazer para tratar o incidente e identificar o autor.

A partir de então, se faz necessário projetar uma solução capaz de registrar, conforme a legalidade, os acessos realizados por usuários na rede da instituição, para que o usuário possa ser identificado mediante as notificações recebidas.

Com o intuito de prover autenticação de usuários e guardar as conexões de acesso à Internet Acadêmica e Comercial, considerando a Norma Complementar do DSIC (21/IN01/DSIC/GSIPR), que trata das "Diretrizes para o registro de eventos, coleta e preservação de evidências de Incidentes de Segurança em Redes" e o Marco Civil da Internet, principalmente em seus Artigos (Art. 5º V, VI, VII, VIII, Art. 11º, Art.13º, e Art. 14º), se faz necessário à implantação de um sistema que auxilie e facilite o trabalho dos funcionários da instituição.

Atualmente a instituição não utiliza nenhum sistema de controle, para este devido fim. E como a Norma Complementar 21 já especifica:

> É interesse do Estado e da sociedade a investigação e a responsabilização por condutas ilícitas que danifiquem ou exponham a segurança das redes e sistemas computacionais ou que possam comprometer a disponibilidade, integridade, confidencialidade e autenticidade da informação na Administração Pública Federal. (Norma Complementar do DSIC (21/IN01/DSIC/GSIPR), 2014, p. 2).

1.1. OBJETIVOS

1.1.1. Objetivo Geral

Implementar um sistema que possibilite o registro das conexões com a Internet e autenticação de usuário.

1.1.2. Objetivos Específicos

- Realizar estudos e pesquisas bibliográficas detalhadas sobre a legislação vigente e tecnologias existentes para implementar o sistema;
- Realizar a instalação do sistema em um ambiente controlado, para realizações de testes preliminares;
- Analisar os resultados obtidos e solucionar possíveis problemas que venham a ocorrer;
- Implantar o sistema na Moradia Estudantil da instituição.
- Discussão dos resultados.

1.2. ESTRUTURA DO TRABALHO

Este trabalho está estruturado da seguinte forma: o capítulo 2 apresenta a fundamentação teórica; capítulo 3 descreve o ambiente para implementação e os testes realizados; capítulo 4 apresenta a implementação do sistema e os resultados, por fim, o capítulo 5 define as considerações finais deste estudo e sugestões para trabalhos futuros.

2. REFERENCIAL TEÓRICO

Para a realização desse trabalho, foram utilizadas algumas tecnologias, como LDAP, pfsense, RADIUS e algumas leis, como a Norma Complementar 21 e a Lei número 12.965. As quais serão descritas nas subseções.

2.1. LDAP

Atualmente, a instituição de ensino faz uso de uma forma de autenticação centralizada, utilizando o protocolo *Lightweight Directory Access Protocol* (LDAP), que permite gerenciar diretórios, quer dizer, acessar a bases de informações sobre os usuários de uma rede através de protocolos TCP/IP.

Segundo CCM (2017), o protocolo LDAP, foi desenvolvido em 1993 pela Universidade do Michigan, tendo por objetivo suplantar o protocolo DAP (*Directory Access Protocol*), o qual serve para conectar-se ao serviço de diretório X.500 do OSI (*Open Systems Interface*). CCM (2017), salienta que a partir de 1995, o LDAP tornou-se um diretório nativo (*standalone* LDAP), não servindo unicamente para acessar diretórios de tipo X.500. O LDAP é assim uma versão melhorada do protocolo DAP, daí o seu nome *Lightweight Directory Acess Protocol*.

Conforme CCM (2017), o protocolo LDAP define o método de acesso aos dados no servidor ao nível do cliente, e não a maneira como as informações são armazenadas. Está atualmente na versão 3 e foi normalizado pelo IETF (*Internet Engineering Task Force*). Assim, existe uma RFC para cada versão de LDAP, constituindo um documento de referência:

RFC 1777 para LDAP v.2 *standard*;

RFC 2251 para LDAP v.3 *standard*.

A RFC (*Request For Comments* - Pedidos de comentários) é um conjunto de documentos que servem de referência para a comunidade da Internet e que tem por objetivo padronizar a especificações de tecnologias empregadas a partir da camada 3 do modelo OSI, auxiliando na padronização das funcionalidades oferecidas pelas implementações em conformidade com a especificação descrita. Desta forma provendo compatibilidade.

Assim, o LDAP fornece aos usuários métodos que lhe permitem:

- conectar-se;
- desligar-se;
- procurar informações;
- comparar informações;
- inserir entradas;
- alterar entradas;
- suprimir entradas.

Por outro lado, o protocolo LDAP (na sua versão 3) propõe mecanismos de codificação (SSL) e de autenticação (SASL) que permitem proteger o acesso às informações armazenadas na base. (CCM, 2017).

A SSL (*Secure Sockets Layers*, que poderia se traduzir por camada de sockets protegida) é um método de segurança das transações efetuadas via Internet. O standard SSL foi criado pela Netscape, em colaboração com a Mastercard, Bank of América, MCI e Silicon Graphics. Utiliza um método de criptografia por chave pública a fim de garantir a segurança da transmissão de dados na Internet. O seu princípio consiste em estabelecer um canal de comunicação protegido (codificado) entre duas máquinas (um cliente e um servidor) após uma etapa de autenticação. (CCM, 2017).

O LDAP apresenta as informações sob a forma de uma arborescência de informações hierárquica chamada DIT (*Directory Information Tree*), na qual as informações, chamadas entradas ou ainda DSE (*Directory Service Entry*), são representadas sob a forma de ramos. (CCM, 2017).

Um ramo situado na raiz de uma ramificação chama-se raiz ou sufixo (em inglês, *root entry*). Cada entrada do diretório LDAP corresponde a um objeto abstrato ou real (por exemplo, uma pessoa, um objeto material, parâmetros). Cada entrada é constituída por um conjunto de pares chave/valor chamados atributos, que permitem caracterizar o objeto que a entrada define. Existem dois tipos de atributos:

- Os atributos normais: estes são os atributos habituais (apelido, nome) caracterizando o objeto;
- Os atributos operacionais: estes são atributos aos quais só o servidor pode acessar a fim de manipular os dados do diretório (datas de modificação).

Uma entrada é indexada por um nome distinto (DN, *distinguished name*) que permite identificar de maneira única um elemento da arborescência. Um DN constrói-se tomando o nome do elemento, chamado *Relative Distinguished Name* (RDN, isto é, o caminho da entrada em relação a um dos seus parentes), e acrescentando-lhe o conjunto do nome das entradas parentescos.

Trata-se de utilizar uma série de pares chave/valor que permite localizar uma entrada de maneira única. Eis uma série de chaves geralmente utilizadas, (CCM, 2017):

- uid (userid), trata-se de um identificador único obrigatório;
- cn (common name), trata-se do apelido da pessoa;
- givenname, trata-se do nome;
- Sn (surname), trata-se do apelido da pessoa;
- o (organization), trata-se da empresa da pessoa;
- u (organizational unit), trata-se do serviço da empresa na qual a pessoa trabalha;
- mail, trata-se do endereço de correio electrónico da pessoa (obviamente)

A Figura 1 ilustra um exemplo de entrada quando representada no LDAP *Data Interchange Format* (LDIF):

Figura 1 – Exemplo de LDAP

```
# Cadastrando usuário
dn: cn=Capitao Nascimento,ou=People,dc=cooperati,dc=local
objectClass: inetOrgPerson
sn: Nascimento
homePhone: 1111-1111
mail: cptnascimento@cooperati.local
description: Faca na Caveira
ou: BOPE
```

Fonte: http://cooperati.com.br/2012/02/14/comandos-de-gerenciamento-do-ldap/

Um cliente começa uma sessão de LDAP ligando-se a um servidor LDAP, normalmente pela porta padrão: TCP 389. Este envia requisições para o servidor, o qual devolve respostas. Conforme Sermersheim (2006) as operações básicas são:

- Bind – autentica e específica a versão do protocolo LDAP;
- Search – procura por e/ou recupera entradas dos diretórios;
- Compare – testa se uma entrada tem determinado valor como atributo;
- Add – adiciona uma nova entrada;
- Delete – apaga uma entrada;
- Modify – modifica uma entrada;
- Modify DN – move ou renomeia uma entrada;
- StartTLS – protege a conexão com a *Transport Layer Security* (TLS);
- Abandon – aborta uma requisição prévia;
- Extended Operation – operação genérica para definir outras operações;
- Unbind – fecha a conexão, não o inverso de Bind.

O LDAP tem por finalidade manter uma base de usuários que são utilizados para diversos fins, e muitas vezes o LDAP é o serviço base para operação do servidor de autenticação Radius.

2.2 RADIUS

O RADIUS (*Remote Authentication Dial In User Service*) é um protocolo de autenticação, autorização e contabilização, o primeiro exemplo de um sistema AAA (*Authentication, Authorization and Accounting*), o qual se baseia em pergunta e resposta, utilizando o protocolo de transporte UDP (portas 1812 e 1813) conforme Duque (2016).

Segundo Zúquete (2014), o RADIUS é utilizado, principalmente, para controlar o acesso de pessoas ou equipamentos a redes através de elementos de rede designados por NAS (*Network Autentication Server*). Esse controle é

efetuado centralmente por um servidor RADIUS, o qual colabora com os NAS para realizar a autorização indireta das pessoas ou equipamentos.

A RFC 2138 descreve um protocolo para transportar informações de autenticação, autorização, e configuração, entre um servidor acesso à rede que deseja autenticar suas ligações e um servidor de autenticação compartilhada. (Livingston, Merit, Daydreamer, 1997).

O servidor RADIUS pode suportar uma variedade de métodos para autenticar um usuário. Os métodos que podem ser suportados são: PPP, PAP, CHAP ou UNIX *login*, e outros mecanismos de autenticação.

A autenticação é o procedimento que confirma a validade do usuário que realiza a requisição de um serviço. Este procedimento é baseado na apresentação de uma identidade junto com uma ou mais credenciais, como por exemplo, as senhas e os certificados digitais.

A autorização é a concessão de uso para determinados tipos de serviço, dada a um usuário previamente autenticado, com base na sua identidade, nos serviços que requisita. A autorização pode ser baseada em restrições, que são definidas por um horário de permissão de acesso ou localização física do usuário, por exemplo. Como exemplos de tipos de serviços têm: filtragem de endereço IP, atribuição de endereço, atribuição de rota.

Segundo Duque (2016), o procedimento de contabilização é à coleta da informação relacionada à utilização de recursos de rede pelos usuários. Esta informação pode ser utilizada para gerenciamento, planejamento, registro e etc. A contabilização em tempo real ocorre quando as informações relativas aos usuários são trafegadas no momento do consumo dos recursos.

Nas redes que usam RADIUS há funções distintas, segundo a RFC 2138 que o padroniza, Livingston, Merit, Daydreamer (1997), é composto pelos seguintes equipamentos:

- Cliente: é o host que deseja usufruir de um recurso da rede.
- NAS: é o host que recebe uma solicitação do cliente e autentica esse pedido no servidor RADIUS.
- Servidor RADIUS: é o host que validará o pedido do NAS. A resposta do pedido de autenticação pode ser positiva (*Access-Accept*) acompanhada da tabela de parâmetros de resposta ou negativa (*Access-Reject*) sem nenhum parâmetro. As menssagens trocadas pelo RADIUS são:

- *Access-Request*, enviada para solicitar um serviço;
- *Access-Accept*, aceitação do serviço;
- *Access-Reject*, rejeição do pedido do serviço;
- *Access-Accounting*, contabilização do serviço, que no nosso caso é o tipo mais importante.

O servidor RADIUS é, portanto, uma das técnicas mais empregadas para manter a auditoria de acesso de usuários, o que muitas vezes é exigido por força de leis, conforme se discute na próxima seção.

2.3 Leis

Conforme a Norma Complementar 21, de outubro de 2014, alguns conceitos são importantes:

- Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade.
- Ativos de Informação: os meios de armazenamento, transmissão e processamento da informação; os equipamentos necessários a isso; os sistemas utilizados para tal; os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso.
- Autenticação: processo de identificação das partes envolvidas em um processo.
- Autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade.
- Autorização: processo que visa garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso.

O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a “Hora Legal Brasileira (HLB)”, de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), e no mínimo, os seguintes:

- Autenticação, tanto os bem-sucedidos quanto os malsucedidos;
- Acesso a recursos e dados privilegiados; e
- Acesso a alterações de auditoria.

Os registros dos eventos previstos no item anterior devem incluir as seguintes informações:

- Identificação inequívoca do usuário que acessou o recurso;
- Natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;
- Data, hora e fuso horário, observando o previsto anterior; e
- Endereço IP (*Internet Protocol*), identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

Assim como o artigo 5º da Lei número 12.965, de abril de 2014, que também considera alguns conceitos, como:

- Conexão à Internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;
- Registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à Internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
- Aplicações de Internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet; e
- Registros de acesso a aplicações de Internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de Internet a partir de um determinado endereço IP.

É de responsabilidade da instituição armazenar os logs de acesso durante um período mínimo de 1 ano, de forma sigilosa e sem transferir a responsabilidade para terceiros. No artigo 14 da lei fala “Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de Internet”, por isso nesse trabalho não foi armazenada nenhuma

informação referente ao que o usuário acessou, e sim quando o usuário fez o acesso.

O atendimento as disposições legais, da mesma forma que o eficiente gerenciamento integrado de soluções para provê-las, demanda o uso de ferramentas adequadas para esse fim. Uma ferramenta que vem ganhando cada vez mais visibilidade, e emprego é a utilização da ferramenta PfSense.

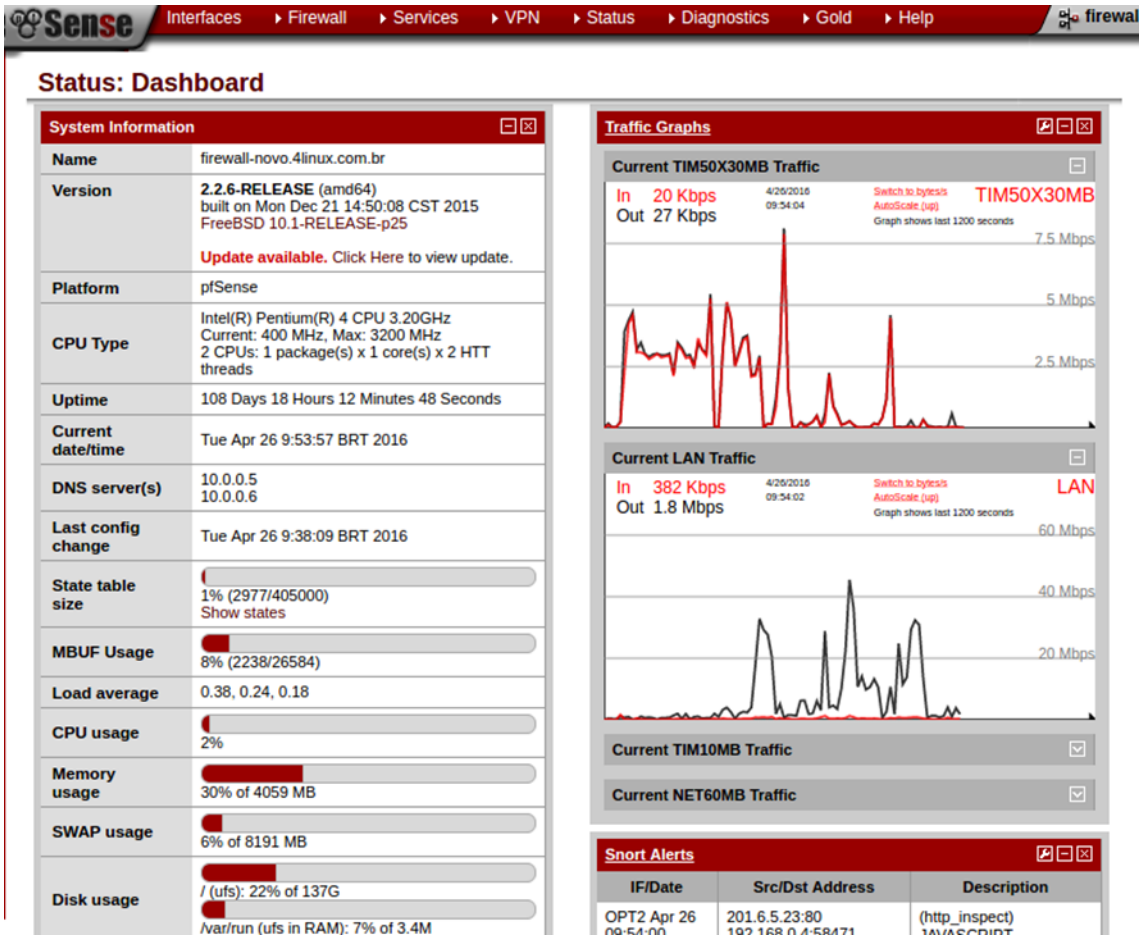
2.4 PfSense

De acordo com Persaud (2012), PfSense é um sistema operacional de código aberto usado para transformar o computador em um firewall, roteador. É uma distribuição FreeBSD feita com base no projeto m0n0wall, uma distribuição de firewall poderoso e leve, se baseia basicamente em m0n0wall e toma decisões de todas as suas funções, e foi adicionado mais uma variedade de serviços de rede mais usadas.

Além de ser gratuito, fácil de manusear, através de uma interface Web, ou através de linha de comando pelo SSH (*Secure Shell*), necessita de pouco recurso de hardware, pouca memória RAM e processador. Além disso, possui atualmente, dezenas de pacotes adicionais que lhe permitem requisitar o posto de UTM (*Unified Threat Management*, "Central Unificada de Gerenciamento de Ameaças" na tradução livre). Na Figura 2 temos o exemplo da tela inicial do pfSense.

Estável, suas atualizações não são frequentes, e são fáceis de fazer. Por ser um software de *firewall* com base no FreeBSD, ele já possui as seguranças mais eficazes contra invasões . Possui vários pacotes que podem ser instalados nele, tais como Snort e Suricata para detecção e prevenção de intrusão, OpenBGPD, MailScanner, HAProxy, Asterisk, Squid com cache e proxy reverso com SquidGuard, antivírus com ClamWin, Varnish3, Postfix, além de outras.

Figura 2 – Tela inicial do pfSense



Fonte: https://www.4linux.com.br/o-que-e-pfsense

Se optou por utilizar o pfSense por ele ter uma grande capacidade de expansão, vários pacotes opcionais que aumentam sua gama de utilização futura, de forma prática e fácil, em comparação por exemplo com o Shibboleth, ou mesmo o CoovaChilli que teríamos que integrar vários sistemas de forma manual para obter o mesmo resultado.

O CoovaChilli, como foi utilizado por Barretos , está homologado para uma versão mais antiga de sistema operacional, Ubuntu Server 12.04 LTS, onde terminou seu ciclo de vida em 28 de abril de 2017, conforme a Canonical, com isso não possui mais atualizações, tornando assim um sistema com possíveis falhas.

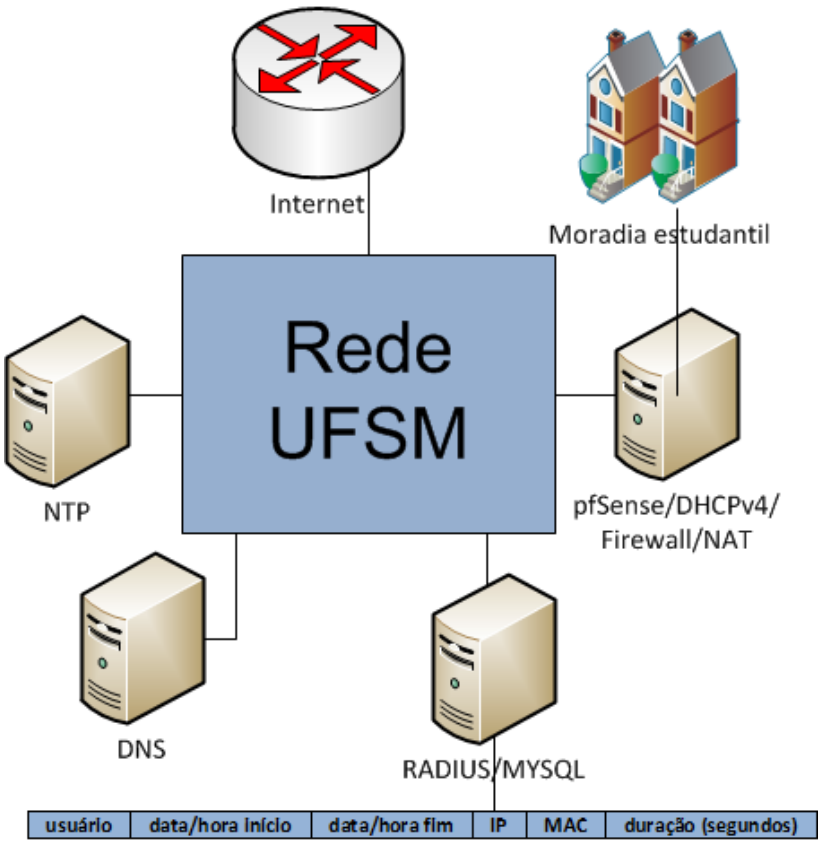
3 Testes de Verificação e Funcionalidades das ferramentas empregadas

Para a futura implementação na moradia estudantil, utilizaremos o cenário mostrado na Figura 3. Onde temos a moradia estudantil ligada ao servidor pfSense, o qual roda um servidor DHCPv4, juntamente com o Captive Portal, um Firewall e ele é o servidor NAT da rede.

O servidor pfSense está conectado na rede da UFSM, a qual possui um servidor de NTP, DNS e RADIUS. Por sua vez, está conectada a Internet.

O servidor NTP é responsável pela sincronização com a Hora Legal Brasileira. DNS, responsável pela tradução dos nomes em endereços IP e vice-versa. RADIUS realiza a autenticação, autorização e contabilização. Como mostrado na Figura 3, onde se coleta usuário, data/hora início, data/hora fim, IP, MAC, duração.

Figura 3 – Cenário utilizado.



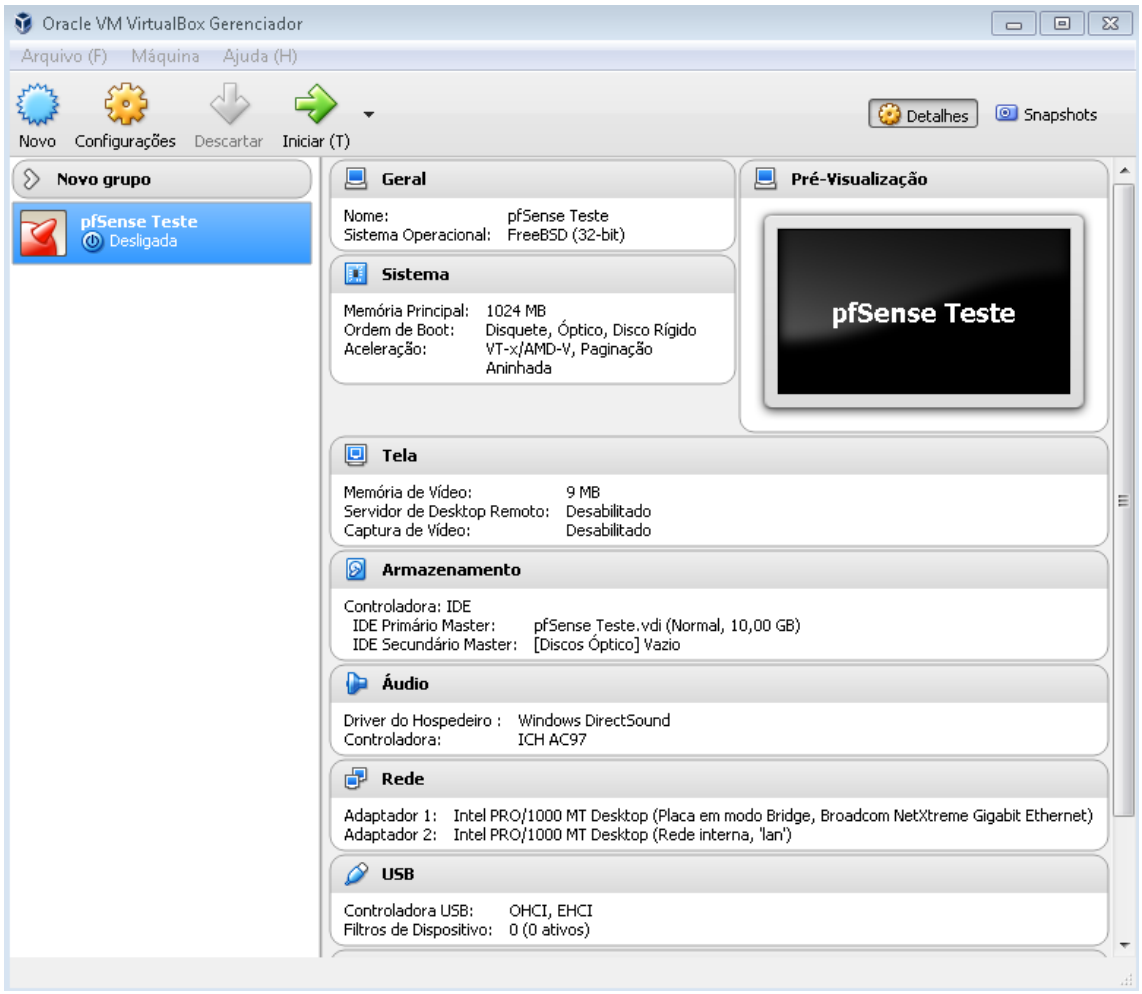
Fonte: Próprio Autor

3.2 Testes

Num primeiro momento foi criado uma máquina virtual, utilizando o VirtualBox, com 1Gb de memória ram, um processador, disco de 10Gb e duas placas de rede, com a finalidade de realizar testes, como se pode observar na Figura 4. Já na Figura 5 se tem a máquina virtual em funcionamento.

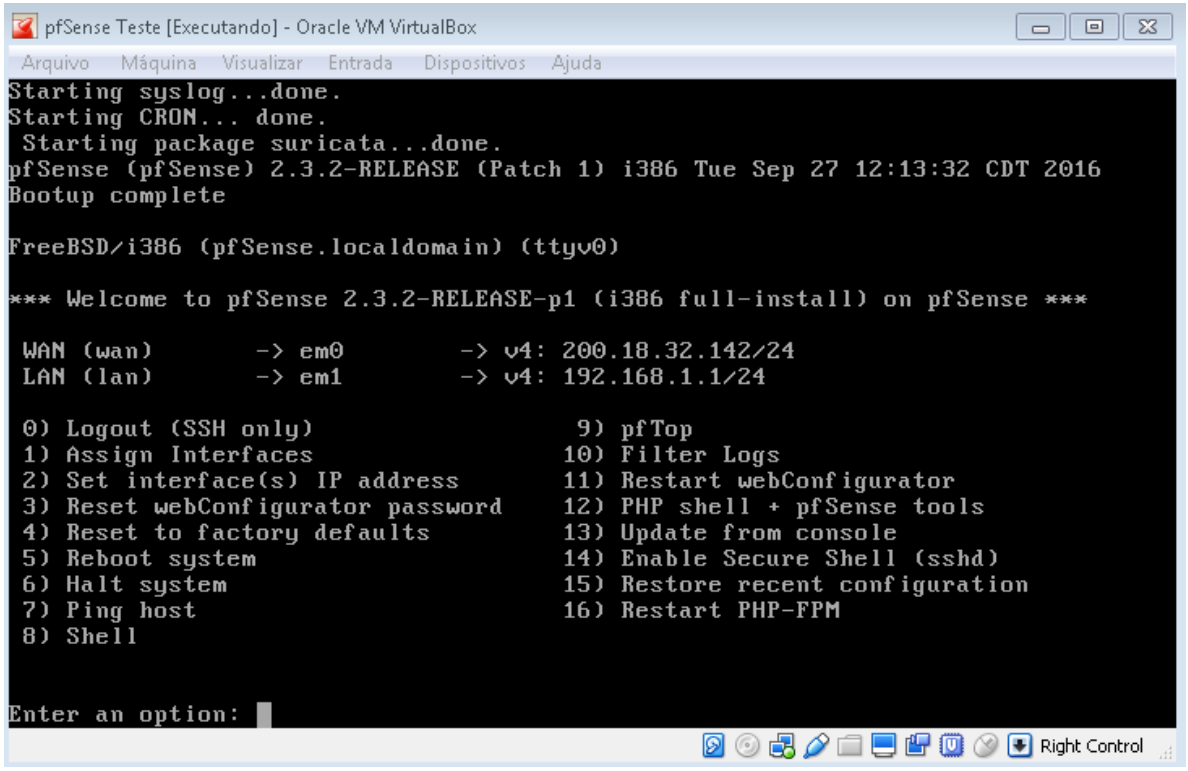
Esse ambiente foi criado para a realização de testes com os seguintes cenários: conexão direta com o servidor, conexão através de um roteador com DHCP e conexão através de um roteador em bridge. Esses cenários representam as possibilidades que se tem para conexão com a Internet no âmbito da instituição.

Figura 4 – Máquina virtual pfSense



Fonte: Próprio Autor

Figura 5 – Máquina virtual em execução



Fonte: Próprio Autor

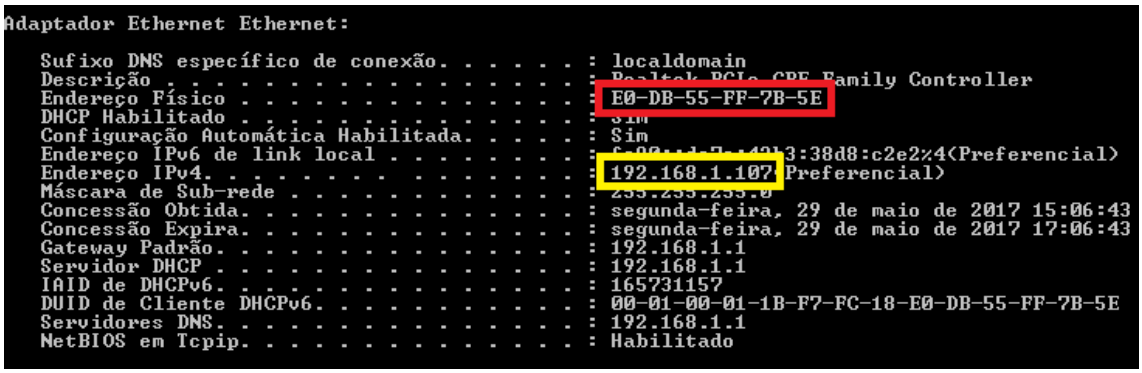
Foi instalado a versão 2.3.2 (i386) do pfSense, configurado os ip's nas placas de rede, uma com acesso externo, e a outra para ser o dhcp da rede. Após as configurações básicas, foi habilitado o Captive Portal, e feito a configuração para acesso ao servidor RADIUS da instituição com a finalidade de autenticação via LDAP.

3.2.1 Conexão direta com o servidor

Os primeiros testes foram realizados utilizando um notebook conectado diretamente ao servidor, autenticando e navegando na Internet.

Na Figura 6 mostra as configurações de rede do notebook, sendo que, destacado em vermelho seu endereço MAC, e em amarelo o endereço IP obtido direto do servidor pfSense.

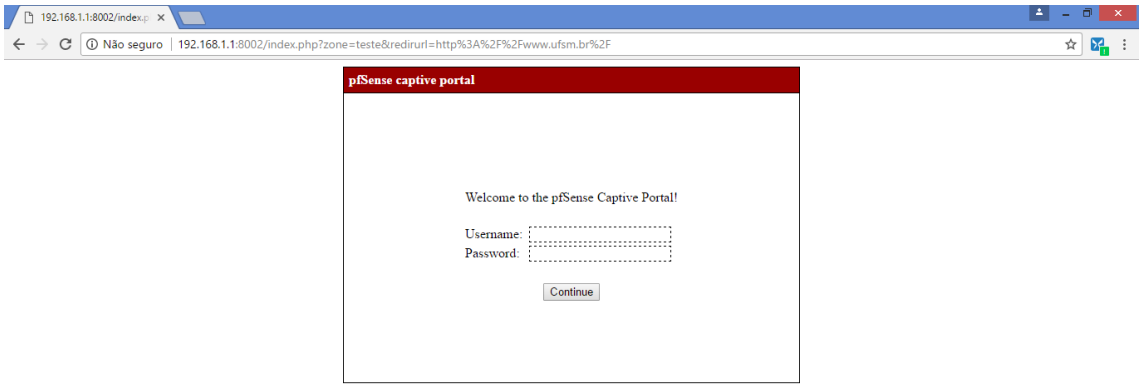
Figura 6 – Configuração de rede notebook.



Fonte: Próprio Autor

A Figura 7 mostra o portal de autenticação, quando o usuário tentou realizar uma navegação web.

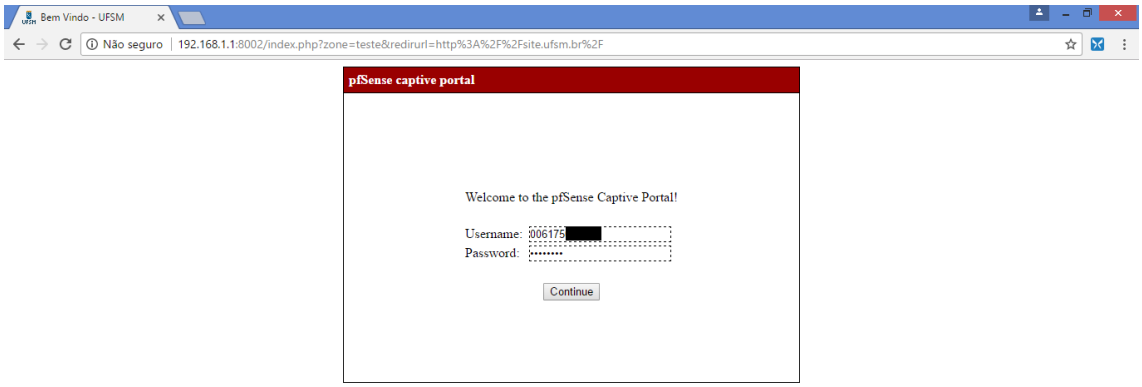
Figura 7 – Portal de autenticação.



Fonte: Próprio Autor

Na Figura 8, o usuário inseriu sua credencias, para realizar a autenticação e posterior navegação. Para garantir a confidencialidade dos usuários, os CPF foram encobertos com uma tarja preta, deixando amostra somente os seis primeiros dígitos.

Figura 8 – Credenciais do usuário.



Fonte: Próprio Autor

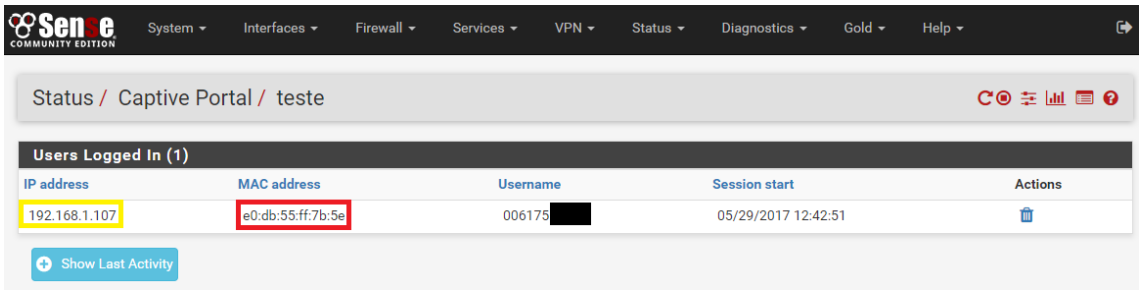
Após a realização da autenticação, é liberada a navegação para o usuário, como mostra a Figura 9.

Figura 9 – Navegação web.

Fonte: Próprio Autor

Na Figura 10 podemos observar o status do *Captive Portal* no servidor pfSense, onde mostra destacado em amarelo o endereço IP do cliente e em vermelho o endereço MAC do cliente.

Figura 10 – Status Captive Portal cliente conectado direto.



Fonte: Próprio Autor

Já na Figura 11 temos o log do servidor RADIUS, mostrando destacado em vermelho o endereço MAC do cliente e em amarelo o endereço IP do cliente, para realizar a consulta foi utilizado o seguinte sql "*SELECT `username`, `callingstationid`, `framedipaddress`, `acctstarttime`, `acctstoptime`, `acctterminatecause` FROM `radacct` WHERE `nasipaddress` LIKE '200.*.*.*' ORDER BY `acctstarttime` DESC*".

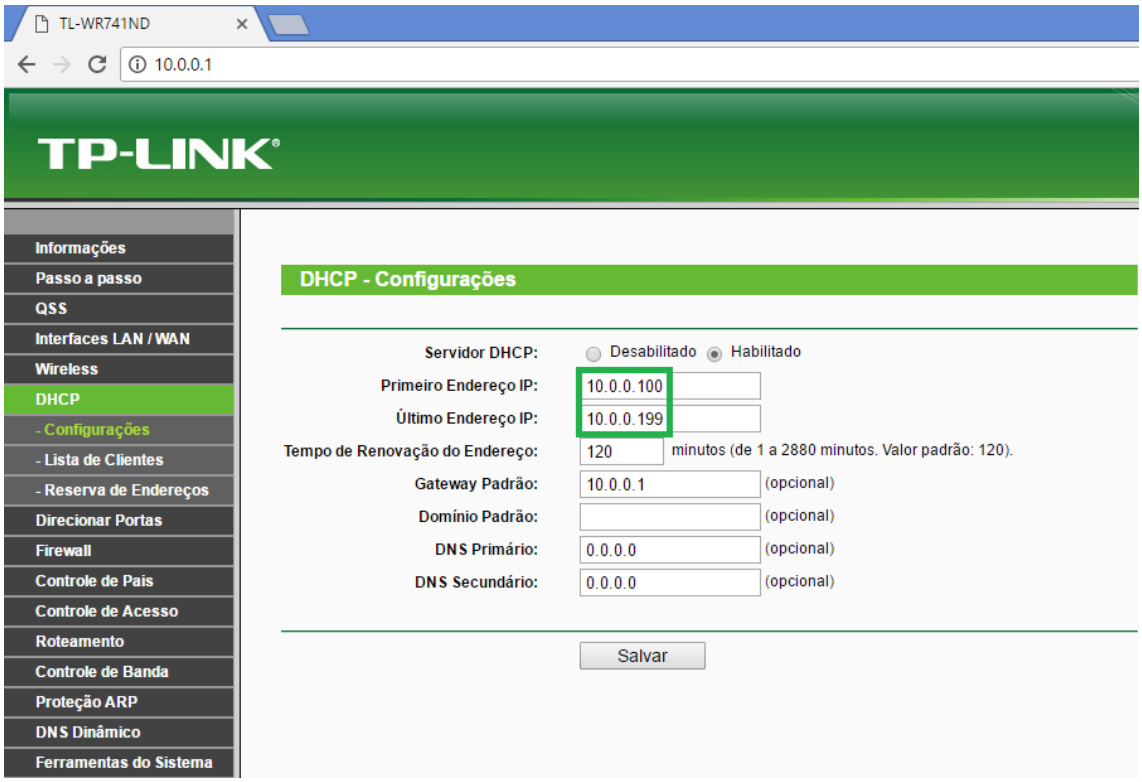
Figura 11 – Log servidor RADIUS, cliente conectado direto.

Fonte: Próprio Autor

3.2.2 Conexão através de um roteador com DHCP

Posteriormente, foi configurado um roteador wireless, com seu servidor DHCP ativo, como mostra a Figura 12, e foram realizados testes.

Figura 12 – Configuração DHCP do roteador.



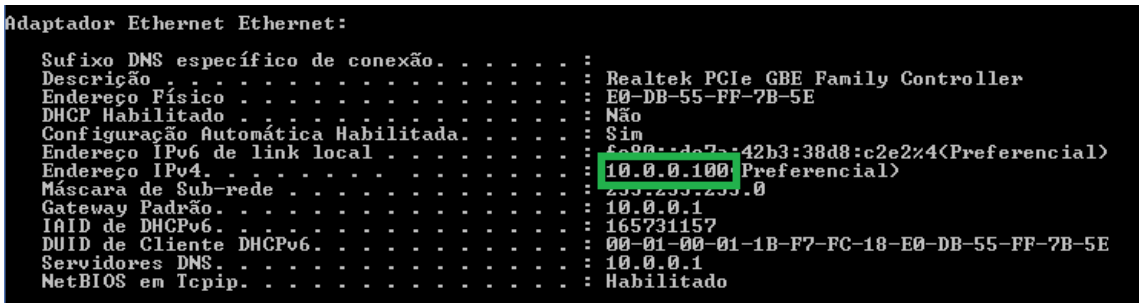
Fonte: Próprio Autor

A Figura 13 mostra as configurações de rede do notebook, sendo que, destacado em verde o endereço IP obtido pelo roteador.

A Figura 14 mostra as configurações de rede do celular, destacado em verde o endereço IP obtido pelo roteador.

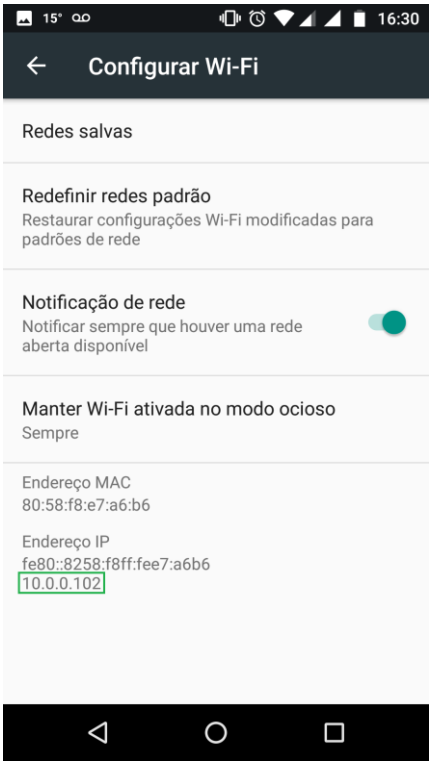
Com a Figura 15 podemos observar a configuração de rede do roteador, obtendo endereço IP do servidor pfSense, destacado em amarelo.

Figura 13 – Configuração de rede do notebook, através do roteador.



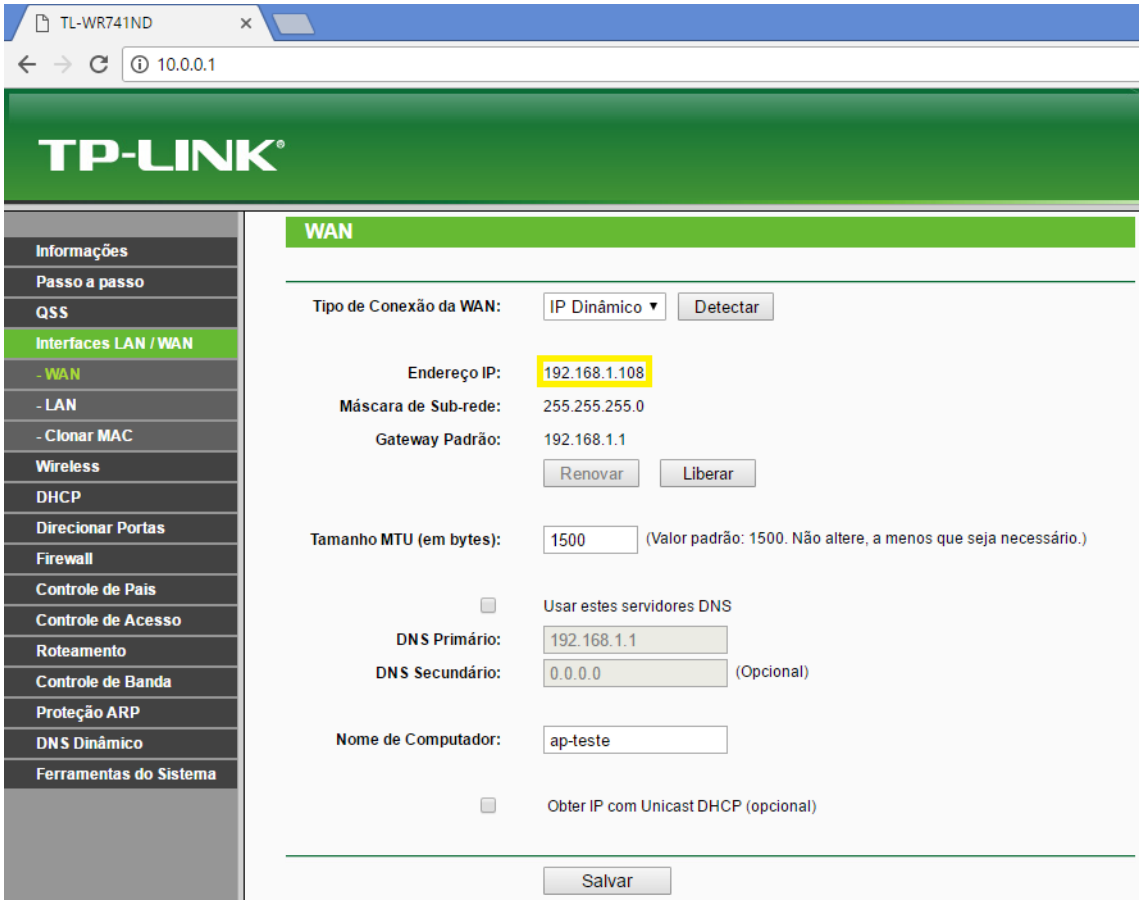
Fonte: Próprio Autor

Figura 14 – Configuração de rede do celular, através do roteador.



Fonte: Próprio Autor

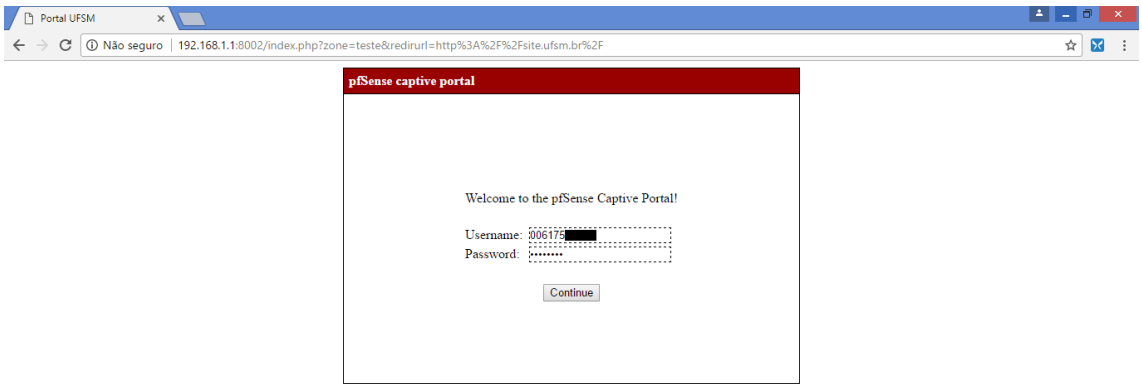
Figura 15 – Configuração de rede do roteador, através do pfSense.



Fonte: Próprio Autor

Na Figura 16, o usuário inseriu sua credencias, para realizar a autenticação e posterior navegação.

Figura 16 – Credenciais do usuário, através do roteador.



Fonte: Próprio Autor

Após a realização da autenticação, é liberada a navegação para o usuário, como mostra a Figura 17.

Figura 17 – Navegação web, através do roteador.

Fonte: Próprio Autor

Já a navegação através do celular não foi necessário a autenticação, como mostra a Figura 18, pois o servidor pfSense, detectou que já havia ocorrido a autenticação, como podemos observar na Figura 19.

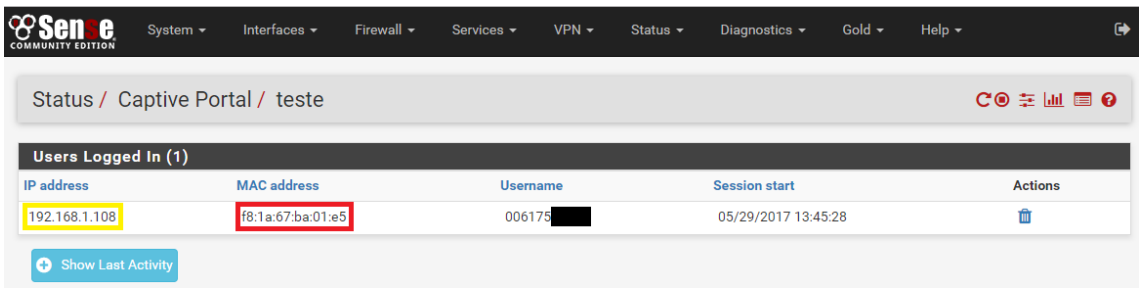
Já na Figura 20 temos o log do servidor RADIUS, mostrando destacado em vermelho o endereço MAC do roteador e em amarelo o endereço IP do roteador.

Com essa configuração no roteador, como pode-se observar nas Figuras 19 e 20, não se consegue rastear os usuário corretamente, pois somente o primeiro usuário é autenticado.

Figura 18 – Navegação web pelo celular, através do roteador.

Fonte: Próprio Autor

Figura 19 – Status Captive Portal cliente conectado pelo roteador.



Fonte: Próprio Autor

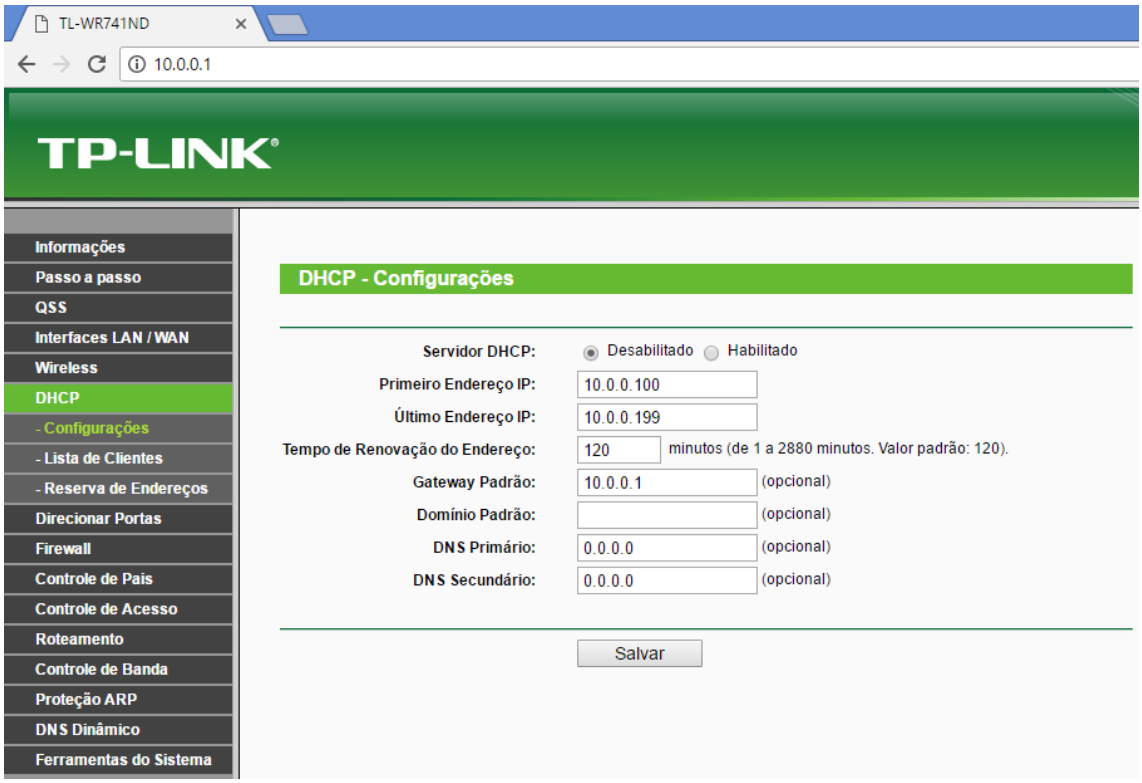
Figura 20 – Log servidor RADIUS, roteador.

Fonte: Próprio Autor

3.2.3 Conexão através de um roteador em bridge

Num terceiro momento esse roteador foi reconfigurado, desabilitando sua distribuição de IP, como mostra a Figura 21, deixando no modo de bridge, Figura 22, e novamente realizados testes.

Figura 21 – Configuração DHCP, roteador em bridge.

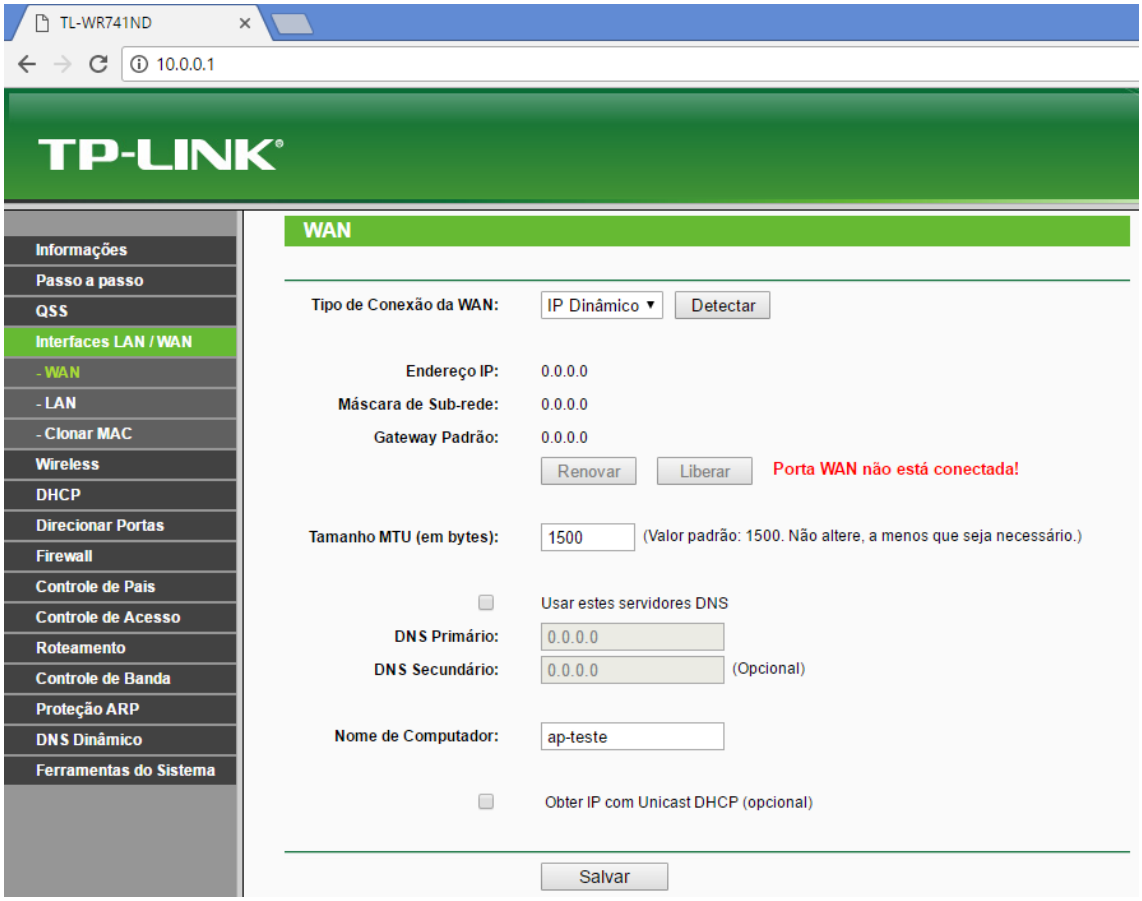


Fonte: Próprio Autor

A Figura 23 mostra as configurações de rede do notebook, sendo que, destacado em amarelo o endereço IP obtido pelo pfSense e em vermelho o endereço MAC.

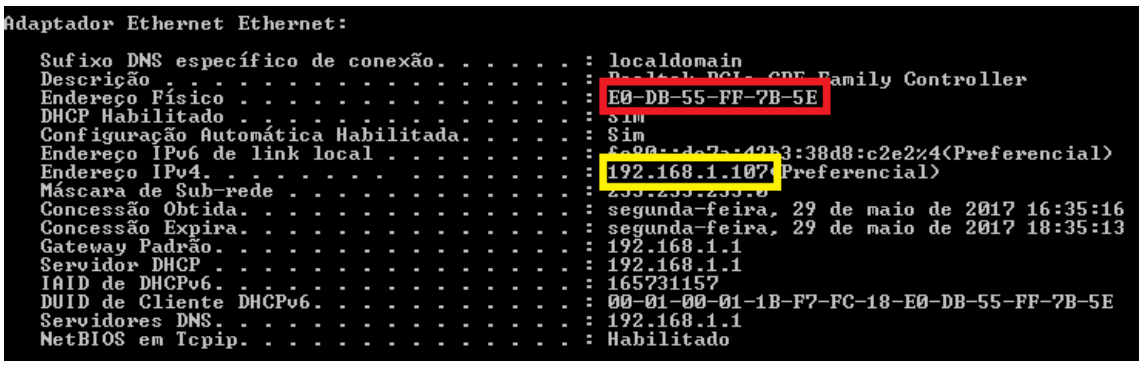
A Figura 24 mostra as configurações de rede do celular, sendo que, destacado em verde o endereço IP obtido pelo pfSense e em azul o endereço MAC.

Figura 22 – Configuração WAN, roteador em bridge.



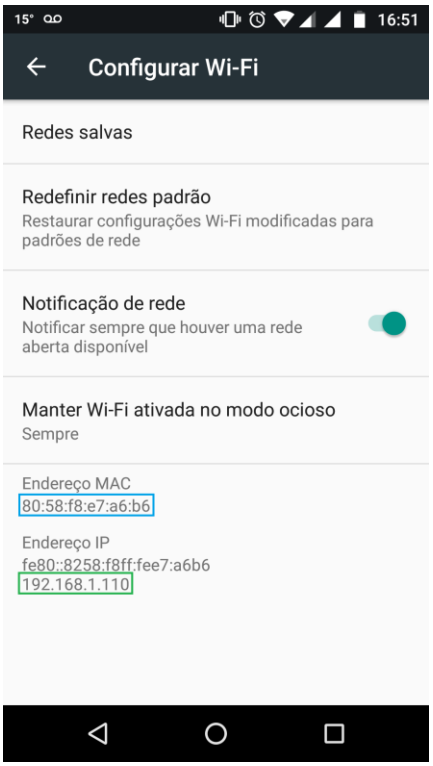
Fonte: Próprio Autor

Figura 23 – Configuração de rede do notebook, roteador em bridge.



Fonte: Próprio Autor

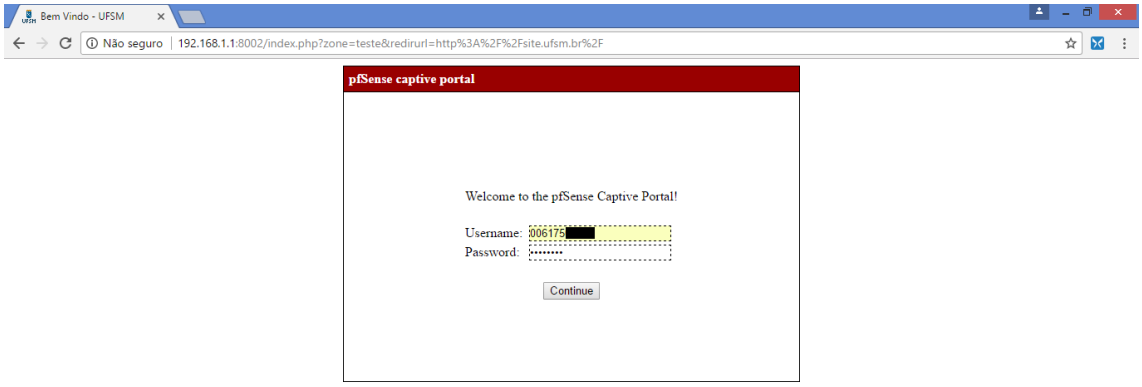
Figura 24 – Configuração de rede do celular, roteador em bridge.



Fonte: Próprio Autor

Na Figura 25, o usuário inseriu sua credencias, para realizar a autenticação e posterior navegação, pelo notebook.

Figura 25 – Credenciais do usuário, pelo notebook, roteador em bridge.



Fonte: Próprio Autor

Após a realização da autenticação, é liberada a navegação para o usuário, como mostra a Figura 26.

Figura 26 – Navegação web, pelo notebook, roteador em bridge.

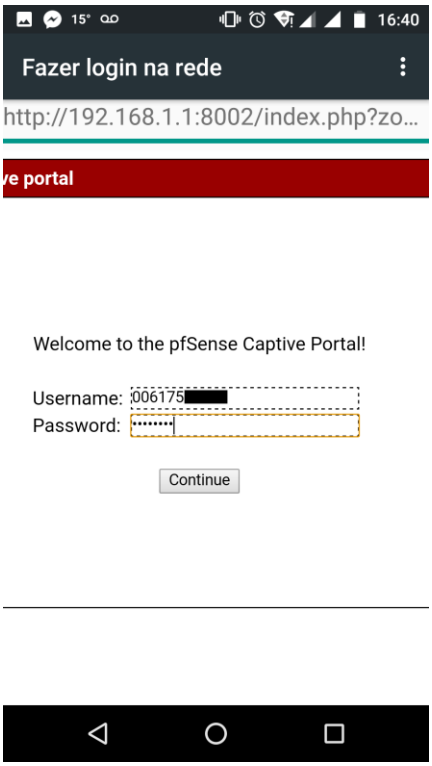
Fonte: Próprio Autor

Na Figura 27, o usuário inseriu sua credencias, para realizar a autenticação e posterior navegação, pelo celular.

Na Figura 28 se pode observar o status do *Captive Portal* no servidor pfSense, onde mostra destacado em amarelo o endereço IP do notebook, em vermelho o endereço MAC do notebook, em verde o endereço IP do celular e em azul o endereço MAC do celular.

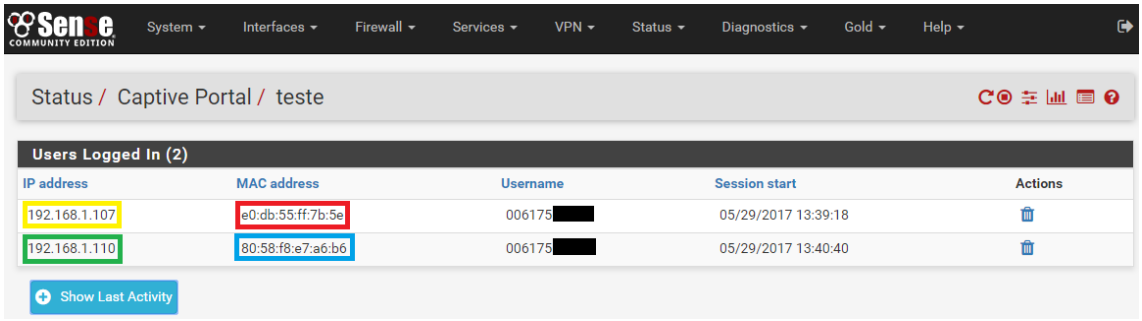
Já na Figura 29 se tem o log do servidor RADIUS, mostrando destacado em amarelo o endereço IP do notebook, em vermelho o endereço MAC do notebook, em verde o endereço IP do celular e em azul o endereço MAC do celular.

Figura 27 – Credenciais do usuário, pelo celular, roteador em bridge.



Fonte: Próprio Autor

Figura 28 – Status Captive Portal, roteador em bridge.



Fonte: Próprio Autor

Figura 29 – Log servidor RADIUS, roteador em bridge.

username	callingstationid	framedipaddress	acctstarttime ▾ 1	acctstoptime	acctterminatecause
006175	80:58:f8:e7:a6:b6	192.168.1.110	2017-05-29 16:40:40	*NULL*	
006175	e0:db:55:ff:7b:5e	192.168.1.107	2017-05-29 16:39:17	*NULL*	

Fonte: Próprio Autor

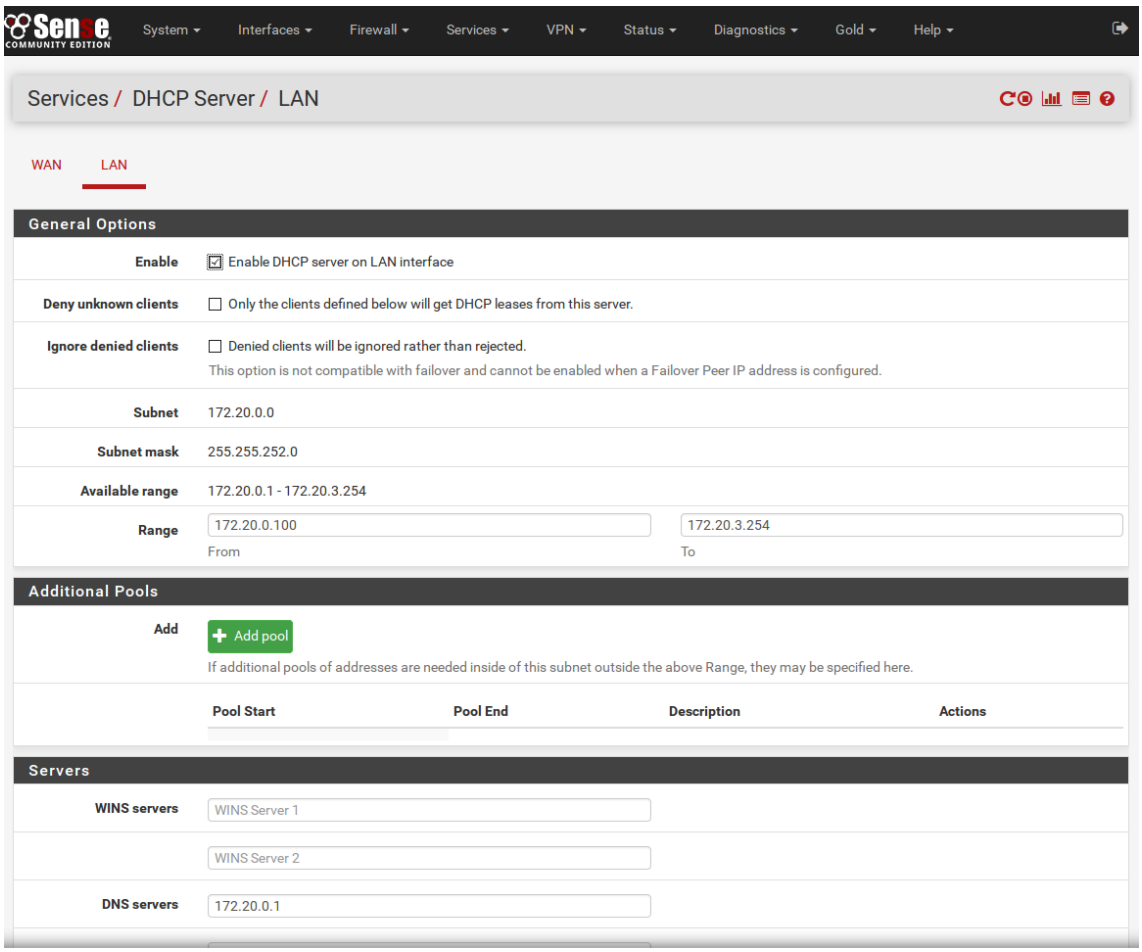
Após os testes realizados, conseguiu-se observar que o cenário mais adequado para implementação é o com os roteadores com DHCP desabilitado e em modo bridge. Pois, com esse cenário, se consegue melhor rastreabilidade dos usuários logados no sistema, atendendo assim as leis vigentes.

4 IMPLEMENTAÇÃO E RESULTADOS

Esse capítulo apresenta como foi realizada a implementação do sistema na moradia estudantil, mostrando algumas configurações realizadas e os resultados obtidos com isso.

Para a implementação na moradia estudantil, se utilizou um computador com dois processadores de 2.66GHz e 2Gb de memória ram, no qual foram realizadas algumas configurações no servidor pfSense, como por exemplo, foi habilitado o servidor DHCP para a rede LAN, como mostra a Figura 30. Onde foi configurada a rede 172.20.0.0/22 e como DNS da rede o próprio servidor.

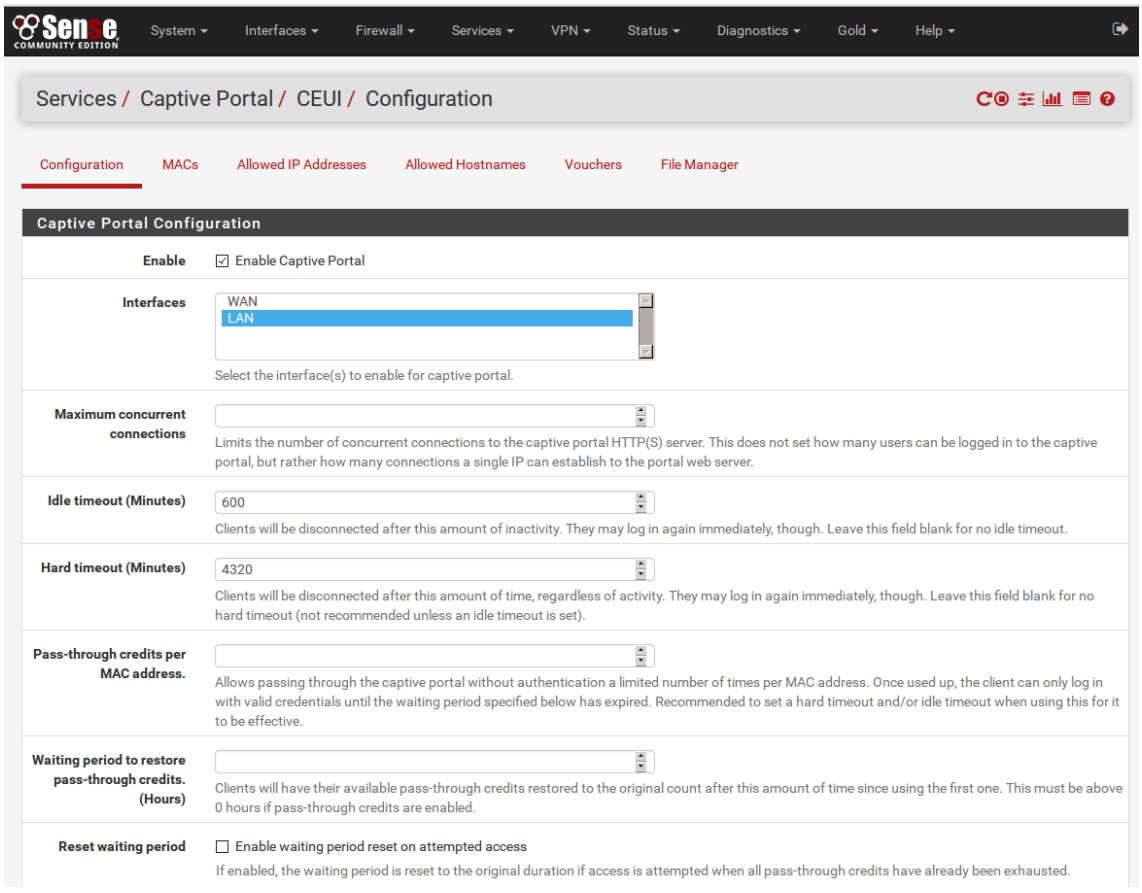
Figura 30 – Configuração DHCP do pfSense.



Fonte: Próprio Autor

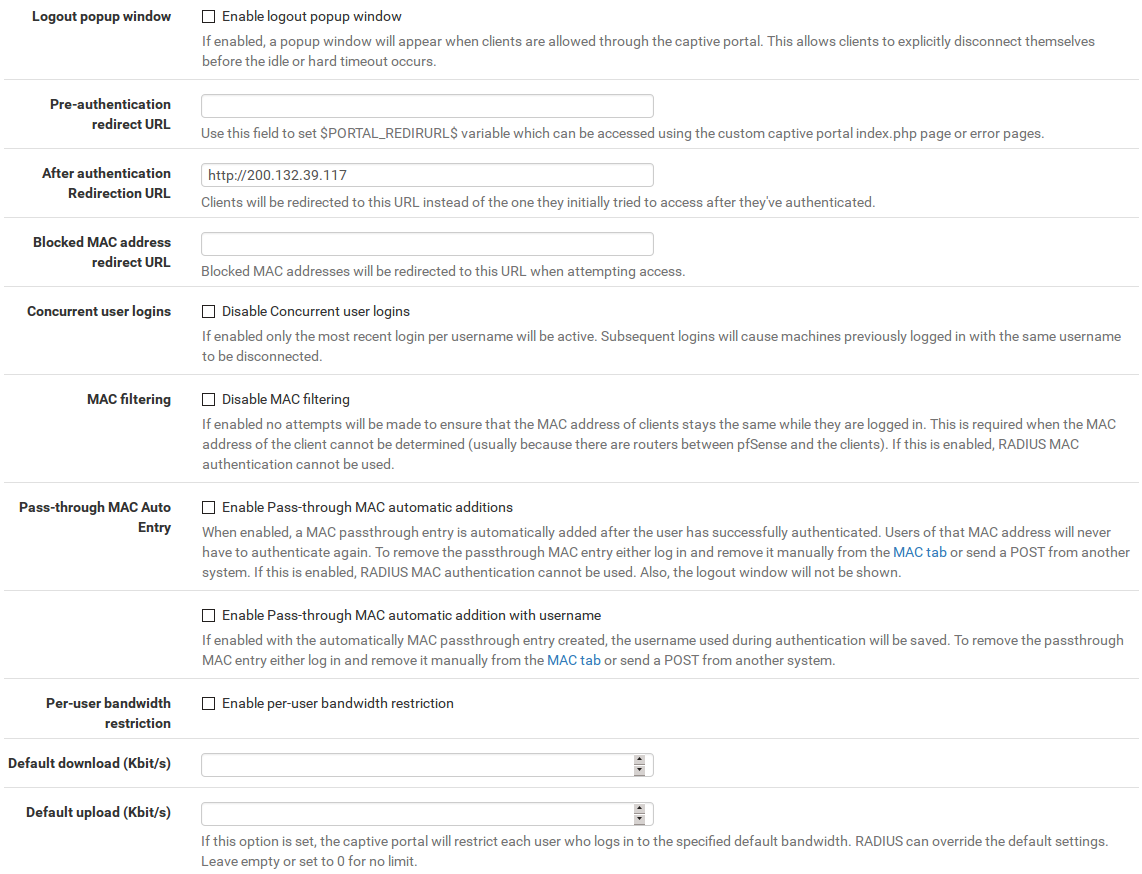
O *Captive Portal* foi configurado na interface LAN, para o campo de tempo limite inativo (*idle timeout*), onde o usuário é desconectado por inatividade após certo período, o tempo foi de 600 minutos ou 10 horas. Já no campo de tempo limite (hard timeout), onde o usuário é desconectado após certa quantidade de tempo independente da atividade, o tempo foi de 4320 minutos ou 72 horas. Como mostra a Figura 31. No campo URL de redirecionamento após autenticação (*after autentication redirection* URL), os clientes serão redirecionados para a URL configurada, após autenticação realizada, http://200.132.39.117, que é a URL da página principal da UFSM, Figura 32.

Figura 31 – Configuração 1 *Captive Portal* do pfSense.



Fonte: Próprio Autor

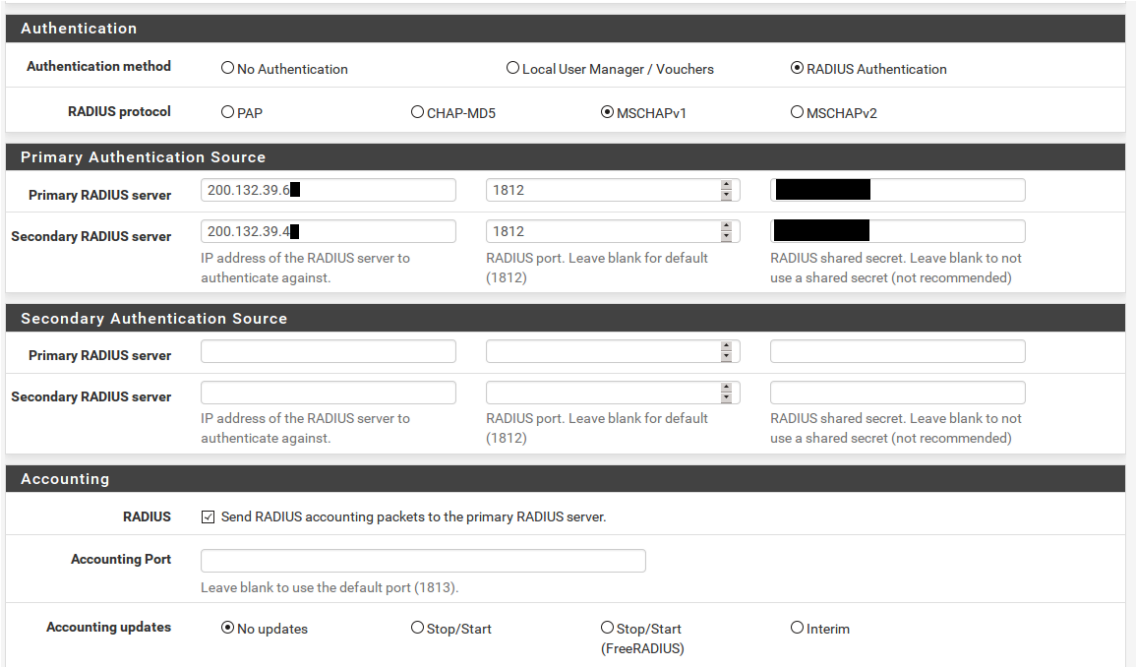
Figura 32 – Configuração 2 *Captive Portal* do pfSense.



Fonte: Próprio Autor

No campo autenticação, foi selecionado o método que utiliza o RADIUS, com protocolo MSCHAPv1. Para o servidor RADIUS primário, foi informado o endereço IP do servidor utilizado, a porta de funcionamento, e a senha compartilhada, o mesmo ocorreu para o servidor RADIUS secundário. Para a opção de contabilização, foi selecionado para o servidor pfSense enviar os pacotes contábeis para o servidor RADIUS configurado previamente, como mostra a Figura 33. Esse servidor já vem sendo utilizado pela instituição, por isso não foi preciso alterar suas configurações.

Figura 33 – Configuração 3 *Captive Portal* do pfSense.



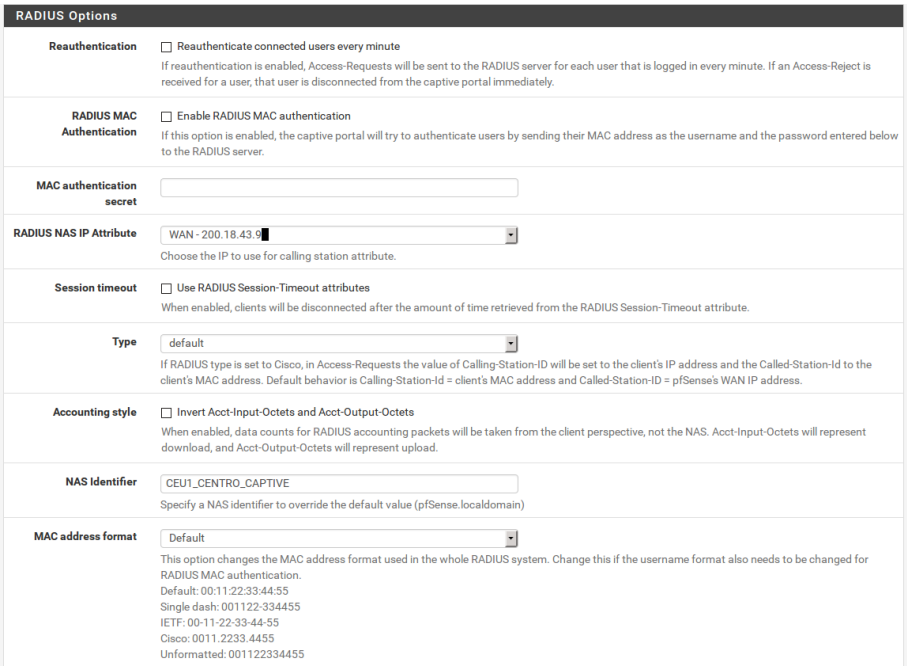
Fonte: Próprio Autor

Nas opções do RADIUS, foi selecionado o endereço IP da interface WAN para o atributo IP do NAS e para o identificador de NAS, foi utilizado “CEU1_CENTRO_CAPTIVE”, como mostra a Figura 34. As demais opções foram mantidas no padrão da instalação.

Para se ter uma coordenação dos serviços foi configurado o serviço de NTP do pfSense para sincronizar com os servidores a.ntp.be, b.ntp.br e ntp.pop-rs.rnp.br, os quais já estão configurados nos demais servidores da instituição. Pode se observar essa configuração no pfSense na Figura 35.

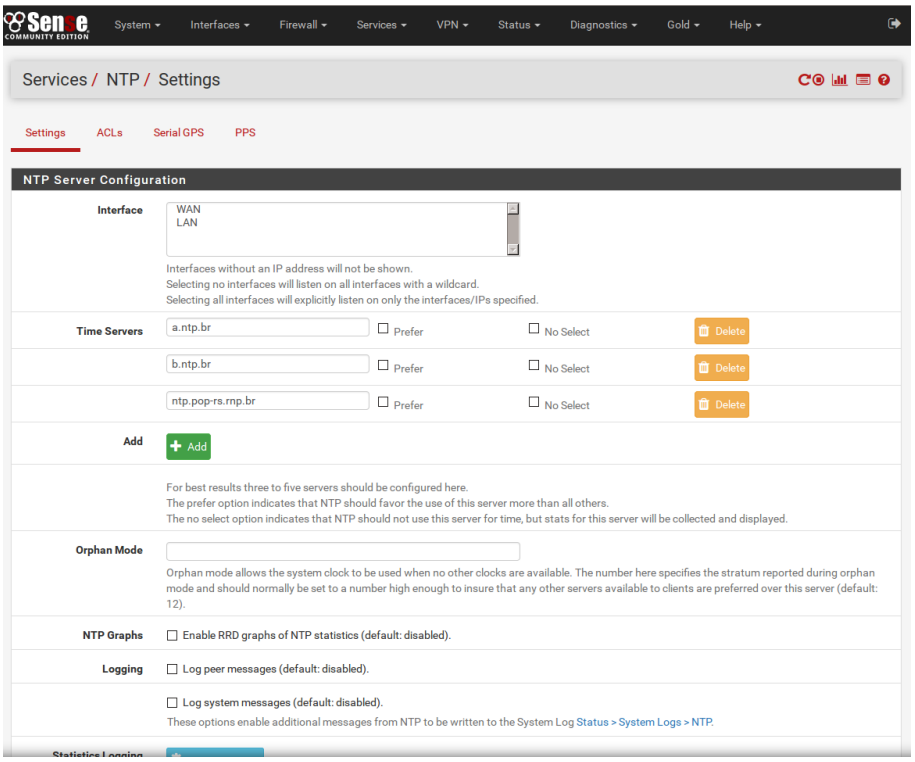
Para não causar um impacto muito grande aos usuários, optou-se por utilizar a mesma tela de autenticação já utilizada pela *wireless* institucional. Trazendo uma interface já conhecida pelos usuários, como se pode observar na Figura36.

Figura 34 – Configuração 4 *Captive Portal* do pfSense.



Fonte: Próprio Autor

Figura 35 – Configuração NTP do pfSense.



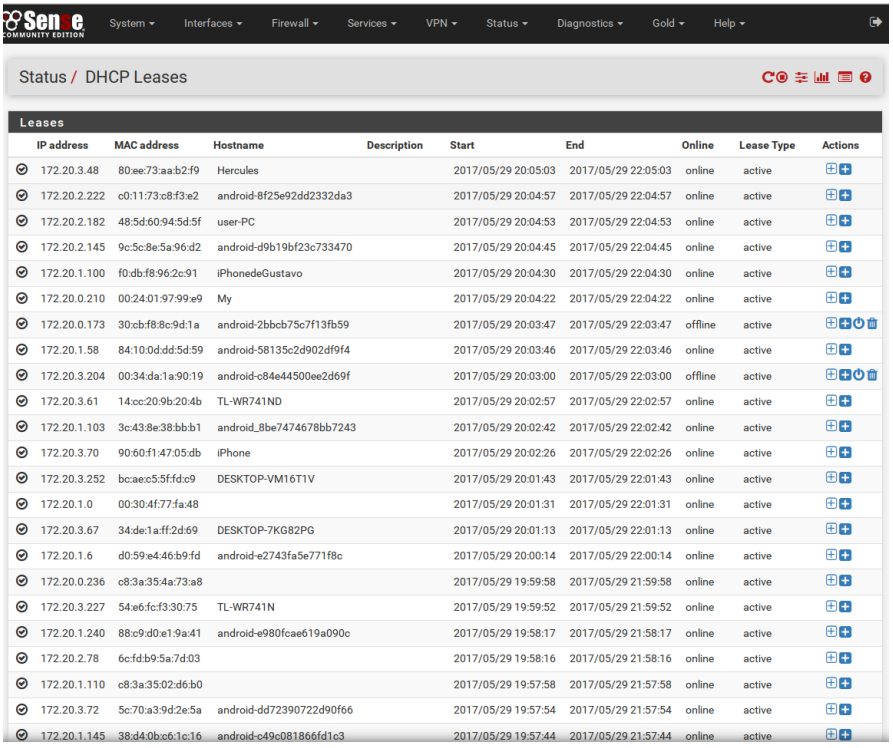
Fonte: Próprio Autor

Figura 36 – Tela de autenticação do pfSense.

Fonte: Próprio Autor

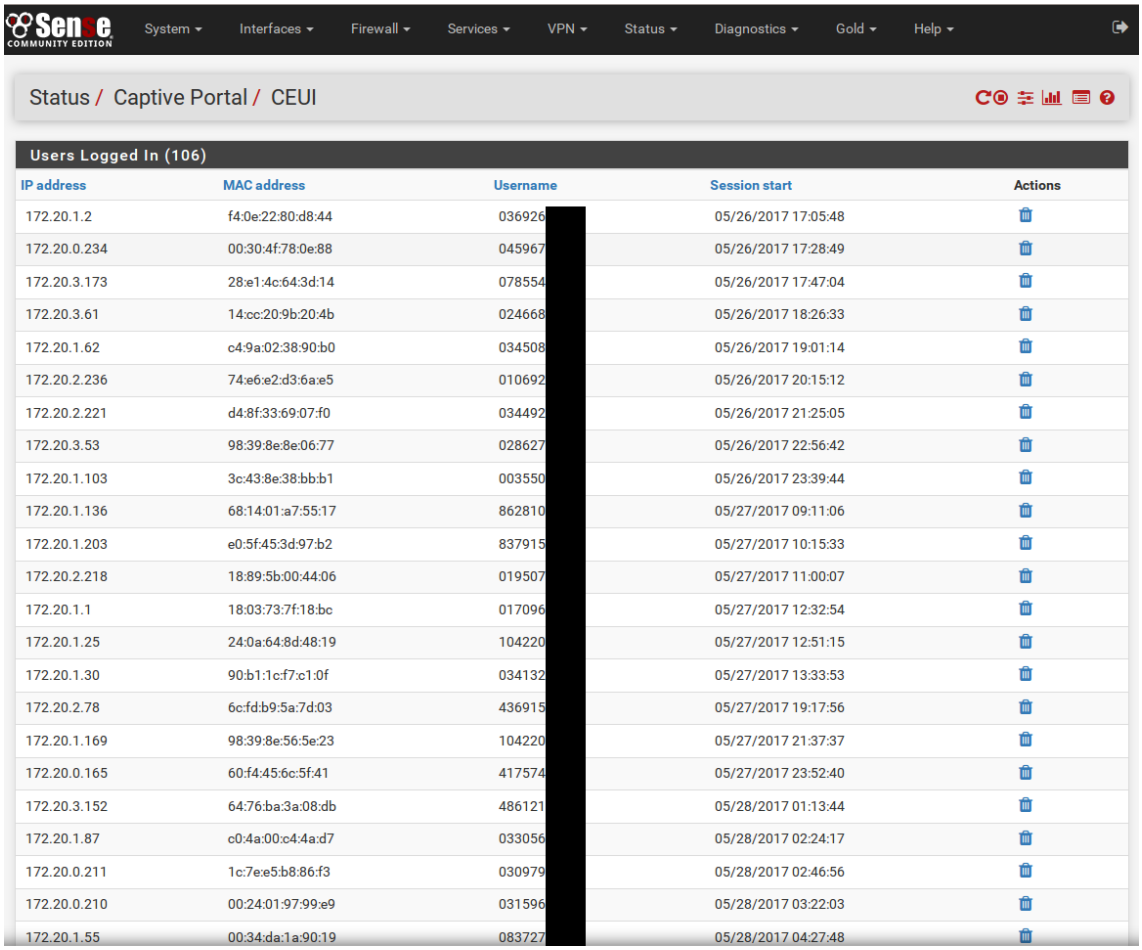
Como resultados da implementação tem-se algumas figuras, mostrando os clientes DHCP conectados, se pode observar na Figura 37, os clientes do *Captive Portal*, Figura 38 e a consulta realizada no servidor RAIDUS Figura 39.

Figura 37 – DHCP *Leases* do pfSense.



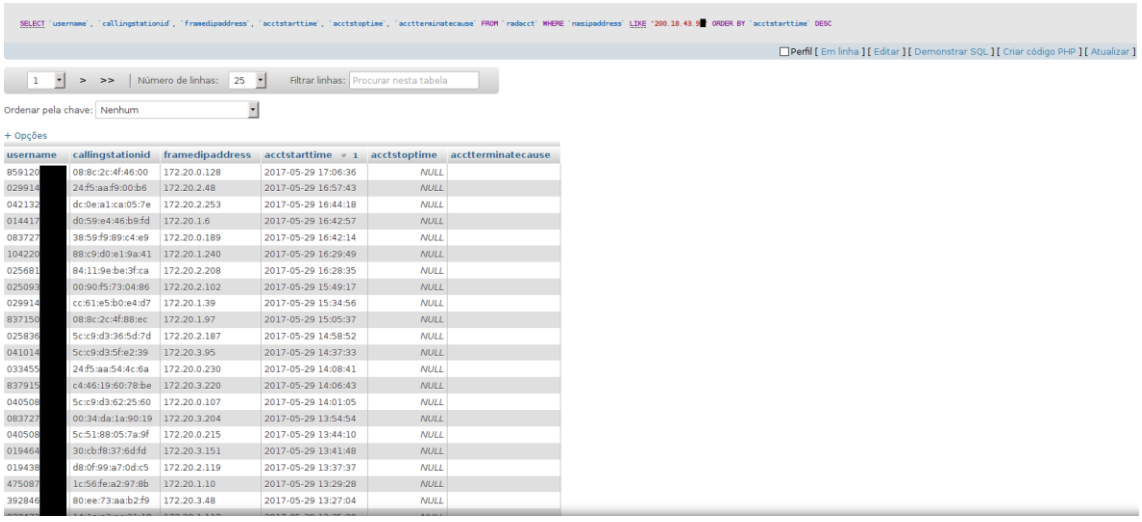
Fonte: Próprio Autor

Figura 38 –*StatusCaptive Portal* do pfSense.



Fonte: Próprio Autor

Figura 39 – Consulta no servidor RADIUS.



Fonte: Próprio Autor

5 CONCLUSÃO

Durante a realização dos testes se notou que o cenário que melhor atendia as exigências da lei, cenário com o roteador em modo *bridge*, seria o mais trabalhoso. Tendo que reconfiguar todos os roteadores dos usuários da moradia estudantil, os quais foram um total de 20 roteadores de várias marcas e modelos, para assim atender de forma satisfatória o presente trabalho. Mesmo requerendo mais tempo para a realização, foi implementado.

De forma resumida, se concluiu que os resultados obtidos com os testes foram satisfatórios, atendendo ao fim ao qual foi proposto, de proporcionar rastreabilidade dos usuários logados no sistema. Atualmente esse sistema se encontra funcionando plenamente e em fase de expansão para demais segmentos de redes.

5.2 TRABALHOS FUTUROS

Como sugestões para trabalhos futuros destacam-se a instalação de um certificado homologado no servidor pfSense, para poder habilitar o protocolo https para realizar a autenticação, melhorando assim ainda mais a segurança do sistema. Outra proposta é a adesão ao Ipv6. E um estudo sobre a possibilidade da utilização de um controle de banda por usuário, se necessário for.

REFERÊNCIAS BIBLIOGRÁFICAS

CCM; **O protocolo LDAP**, abril de 2017. Disponível em: <http://br.ccm.net/contents/271-o-protocolo-ldap>. Acesso em 2017.

CCM; **Criptografia - Secure Sockets Layers (SSL),** junho de 2017. Disponível em: < http://br.ccm.net/contents/143-criptografia-secure-sockets-layers-ssl>. Acesso em 2017.

SERMERSHEIM, J.; **RFC 4511: *Lightweitght Access Protocol (LDAP): The Protocol***, junho de 2006. Disponível em: <https://tools.ietf.org/html/rfc4511#section-4.2>. Acesso em 2017.

LIVINGSTON, C. R; MERIT, A. R.; DAYDREAMER, W. S.; LIVINGSTON, S. W.; **RFC 2138: *Remote Authentication Dial In User Service (RADIUS)***, abril de 1997. Disponível em: <https://tools.ietf.org/html/rfc2138>. Acesso em 2017.

CCM; **RFC – Pedido de Comentários**, abril de 2017. Disponível em: <http://br.ccm.net/contents/279-rfc-pedido-de-comentarios>. Acesso em 2017.

DUQUE, L. H.; **Banda Larga: Autenticação Radius**. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialblcdr/pagina_2.asp>. Acesso em 2017.

Departamento de Segurança da Informação e Comunicações, “DIRETRIZES PARA O REGISTRO DE EVENTOS, COLETA E PRESERVAÇÃO DE EVIDÊNCIAS DE INCIDENTES DE SEGURANÇA EM REDES”. Disponível em: http://dsic.planalto.gov.br/documentos/nc_21_preservacao_de_evidencias.pdf. Acesso em 2017.

Presidência da República, “LEI Nº 12.965, DE 23 DE ABRIL DE 2014”. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 2017.

ESCOLA LINUX; **10 motivos para considerar o pfSense como o gateway da sua rede**, julho de 2015. Disponível em:

<https://www.escolalinux.com.br/blog/10-motivos-para-considerar-o-pfsense-como-o-gateway-da-sua-rede>. Acesso em 2017.

4LINUX; **O que é pfSense**. Disponível em: <https://www.4linux.com.br/o-que-e-pfsense>. Acesso em 2017.

PETERSOHN, N.; **Community Help Wiki WifiDocs/CoovaChili**. Disponível em: <https://help.ubuntu.com/community/WifiDocs/CoovaChili> . Acesso em 2017.

PFSENSE; **Open Source Security**. Disponível em: <https://www.pfsense.org/>. Acesso em 2017.

WILLIAMSON, M.; **Pfsense 2 Cookbook.** Editora Packt Publishing, 2011. Traduzido PERSAUD, C. 2012.

BARRETOS, CTI–IFSP Câmpus. Gerenciamento do HotSpot no IFSP-Câmpus Barretos através de Servidor RADIUS e tecnologias Open Source. Disponível em: <http://brt.ifsp.edu.br/v2/images/fotos_artigos/III%20FMEPT/Gerenciamento%20do%20HotSpot%20no%20IFSP%20-%20C%C3%A2mpus%20Barretos%20atrav%C3%A9s%20de%20Servidor%20RADIUS%20e%20tecnologias%20Open%20Source%20-%20Copia.pdf>. Acesso em 2017.

CANONICAL Ltd. **Ubuntu 12.04.5 LTS**. Disponível em: <http://releases.ubuntu.com/12.04/>. Acesso em 2017.

ZUQUETE A.; **Segurança em Redes Informáticas**. 4ª ed., FCA Editora de informática, 2013, Lisboa.

KUROSE, J. F.; ROSS, K. W.; **Redes de Computadores e a Internet: Uma abordagem top-down**. Trad. 3 ed., Addison Wesley, São Paulo, 2006.

TANENBAUM, A. S.: **Redes de Computadores**. 4ª Ed., Editora Campus (Elsevier), 2003.