UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

***CAMPUS* LUIZ MENEGHEL - CENTRO DE CIÊNCIAS TECNOLÓGICAS**

SISTEMAS DE INFORMAÇÃO

DIONATAN FELIPE MORGANTI DA SILVA

PROPOSTA PARA IMPLANTAÇÃO DE UM MODELO DE AUTENTICAÇÃO DE USUÁRIOS EM UMA REDE INSTITUCIONAL

Bandeirantes

2017

DIONATAN FELIPE MORGANTI DA SILVA

PROPOSTA PARA IMPLANTAÇÃO DE UM MODELO DE AUTENTICAÇÃO DE USUÁRIOS EM UMA REDE INSTITUCIONAL

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito para obtenção do grau de Bacharel em Sistemas de Informação e Licenciado em Computação.

Orientador: Prof. Me. Luiz Fernando Legore do Nascimento

Bandeirantes
2017

DIONATAN FELIPE MORGANTI DA SILVA

PROPOSTA PARA IMPLANTAÇÃO DE UM MODELO DE AUTENTICAÇÃO DE USUÁRIOS EM UMA REDE INSTITUCIONAL

Trabalho de Conclusão de Curso submetido à Universidade Estadual do Norte do Paraná, como requisito para obtenção do grau de Bacharel em Sistemas de Informação e Licenciado em Computação.

COMISSÃO EXAMINADORA

_____
Prof. Me. Luiz Fernando L. do Nascimento
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Ricardo Gonçalves Coelho
UENP – *Campus* Luiz Meneghel

_____
Prof. Me. Wellington A. Della Mura
UENP – *Campus* Luiz Meneghel

Bandeirantes, 26 de Junho de 2017

RESUMO

Com a popularização cada vez mais crescente de dispositivos portáteis que se utilizam da rede internet para inúmeros serviços, depara-se com a necessidade em se efetuar uma eficiente gestão do serviço oferecido, que este caso, o cenário investigado é uma universidade. As preocupações relacionadas a esse cenário são pertinentes a própria gestão, de sua escalabilidade, do nível de segurança aplicados aos seus utilizadores, os quais possuem diferentes perfis de acesso e dos próprios gestores. Assim, esse trabalho surgiu da necessidade em se integrar a autenticação de diferentes equipamentos e usuários com o mínimo possível de configuração na máquina considerada cliente. Desse modo, foram feitos diversos estudos preliminares com o uso de ferramentas *proxy servers* e *firewalls* os quais foram vastamente observados seu emprego em diversas universidades coirmãs durante a realização dos estudos preliminares. Além disso, outros recursos foram igualmente estudados para a construção e segmentação em sub-rede e de equipamentos com softwares embarcados os quais permitissem grande interação com aquilo que se propunha. Como o objetivo é o fato de não ser invasivo aos ativos clientes de rede, que em sua ampla maioria são de propriedade pessoal e não patrimonial a universidade, chegou-se a conclusão que, tais equipamentos poderiam ser plenamente ativados para acesso à rede internet sendo o mais transparente possível ao usuário final. Assim, buscou-se desenvolver um sistema que fosse capaz de efetuar toda a gestão da rede, cabeada e sem fio de forma simples e eficaz. Para isso, o trabalho foi inicialmente pautado em análises e no levantamento junto ao núcleo de tecnologia da universidade. Uma vez desenvolvido esse sistema gestor, o mesmo foi posto a prova em uma das unidades da Universidade Estadual do Norte do Paraná – UENP. Que após implantado, o mesmo foi submetido a avaliação através o método SUS - *System Usability Scale* para avaliação do índice de satisfação por parte do usuários que neste caso, foi reportado resultados muito interessantes. Resultados esses que validam a proposta apresentada e permitem que esse sistema gestor seja homologado e implantado em todas as demais unidades desta universidade, de forma que a autenticação de usuários cadastrados em um banco de dados sincronizado possa atender à todas as demais unidades.

Palavras-chave: Mikrotik®, Autenticação, WiFi, Radius, Gerência de Redes, Firewall

ABSTRACT

With an increasing popularization of portable devices that use the internet for many services, there is a need to efficiently manage the service offered, that in this case, the scenario investigated is a university. The concerns related to this scenario are relevant the management, its scalibility, the level of security applied to its users, which have different access profiles and the managers themselves. This work arises the need to integrate an authentication of different equipment and users with the least possible configuration in the answering machine. Preliminary studies were made with the use of proxy servers tools and firewalls which were widely observed in various universities during that study. In addition, other resources were also studied for subnetting and equipment with embedded software, which allows for a great deal of interaction with what was proposed. As the objective is the fact that it is not invasive to active network clients, which in their vast majority are personal property and non-patrimonial the university, it was concluded that, such audiovisual equipment for access to the internet network being The most transparent Possible to the end user. Thus, we sought to develop a system that smokes capable of performing a whole network management, wired and wireless in a simple and effective. For this, the work was initially installed in analysis and without survey with the technology core of the university. Once this management system was developed, it was tested at one of the units of the State University of Northern Paraná - UENP. Which post was implanted, it was submitted to an evaluation using the SUS - System Usability Scale method to evaluate the satisfaction index by the users. In this case, very interesting results were reported. The results are an ideal solution and are deployed in all other units of the university, in order to authenticate users registered in a synchronized database.

Keywords: Mikrotik®, Authentication, WiFi, Radius, Network Management, Firewall

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

ACL	*Access Control List*
AP	*Access Point*
API	*Application Programming Interface*
BGP	*Border Gateway Protocol*
CHAP	*Challenge-Handshake Authentication Protocol*
CPU	*Central Process Unit*
DHCP	*Dynamic Host Configuration Protocol*
EoIP	*Ethernet over IP*
HP	*Hewlett Packard*
HTTPS	*Hyper Text Transfer Protocol Secure*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IPv4	*Internet Protocol versão 4*
ISP	*Internet Service Provider*
KVM	*Kernel-based Virtual Machine*
L2TP	*Layer 2 Tunnelling Protocol*
LDAP	*Lightweight Directory Access Protocol*
MAC	*Media Access Control*
MVC	*Model View Controller*
NAT	*Network Address Translation*
NTI	Núcleo de Tecnologia da Informação da UENP
OSPF	*Open Shortest Path First*
P2P	*Peer-to-peer*
PAP	*Password Authentication Protocol*
PEAR	*PHP Extension and Application Repository*
PHP	*Personal Home Page*
PPPoE	*Point-to-Point Protocol over Ethernet*
PPPTP	*Point-to-Point Tunneling Protocol*
RADIUS	*Remote Authentication Dial In User Service*
RAM	*Random Access Memory*
RIP	*Routing Information Protocol*
RH	Recursos Humanos
SHA	*Secure Hash Algorithm*

SO	Sistema Operacional
SMTP	*Simple Mail Transfer Protocol*
SSH	*Secure Shell*
SUS	*System Usability Score*
SSID	*Service Set Identifier*
SSL	*Secure Socket Layer*
TLS	*Transport Layer Security*
UENP	Universidade Estadual do Norte do Paraná
VLAN	*Virtual Local Area Network*
VPN	*Virtual Private Network*

SUMÁRIO

1. INTRODUÇÃO

Com a popularização de equipamentos computacionais portáteis, como: *tablets*, smartphones e laptops, criou-se a expectativa de que todo espaço corporativo ou institucional, oferecera algum tipo conexão com a rede Internet. Entretanto, o uso desses dispositivos pode aumentar a vulnerabilidade das informações do local de onde se está fazendo o uso da rede. Assim, torna-se importante e imprescindível que haja pelo menos alguma forma de gerenciamento e controle de acesso sobre as conexões feitas a partir dessa rede. Dessa forma, é possível continuar provendo o serviço a visitantes sem que haja o comprometimento com a segurança dos dados trafegados. Para o pior caso, será possível identificar o usuário supostamente criminoso em função da autenticação feita pelo mesmo.

Para que haja um controle e o monitoramento de acessos, torna-se necessário que os usuários e seus equipamentos sejam de alguma forma identificados. Assim e segundo (STALLINGS e BROWN, 2015) a identificação de um usuário poderá ser feita junto ao sistema responsável o qual prove este serviço, permitindo a este ser autenticado antes da liberação da navegação ao conteúdo web.

Quanto à segurança, uma empresa ou instituição necessita se prevenir de acessos indevidos e impedir que sejam cometidos crimes virtuais, como publicação de conteúdos impróprios, divulgação de pragas e conteúdos relacionados à pedofilia. Para isso, é fundamental identificar os usuários e armazenar os logs, isto é, registros de acesso por um período específico. No caso da legislação brasileira, essa obriga a manter esses registros por um período de um ano, de acordo com o artigo 13 do Marco Civil da Internet.

Para a UENP, que é uma Universidade multi *campi*, sua estrutura física e lógica de redes de computadores ainda não se encontra totalmente consolidada, isto é, dada a natureza pela qual ela foi criada, ainda não existe uma padronização sobre o método de autenticação utilizada para todas suas unidades. Embora já existam diversas formas de se autenticar um usuário, uma instituição de ensino superior torna o processo ainda mais complexo. Isso dado ao fato de que diferentes perfis podem ser nela encontrados. Como por exemplo, visitantes, docentes, técnicos administrativos, estagiários, equipes de projetos e discentes. Perfis esses de grupo que embora pareçam bem definidos, não os são, pois a citar como exemplo, um

docente também exerce cargos administrativos, bem como estagiários que embora sejam discentes também auxiliam na administração.

Assim, esse trabalho busca inicialmente mapear todo o processo de autenticação de usuários existente na rede, levando em consideração as informações colhidas através de questionamentos feitas com os diversos grupos de usuários (perfil) para fins de mapeamento e modelagem de um sistema de autenticação e autorização.

1.1 FORMULAÇÃO DO PROBLEMA

Baseado em informações previas cedidas pelo Núcleo de Tecnologia da Informação da UENP (NTI), foi constatado que a rede institucional para acesso à internet deve:

- Necessitar do mínimo ou nenhum chamado a equipe de suporte técnico para ingresso na rede internet, evitando configurações *in loco* nos navegadores web e dispositivos de rede;

- Oferecer facilidade para acesso à rede para qualquer tipo de equipamento computacional seja ele portátil ou não;

- A grande maioria dos equipamentos conectados à rede institucional é de terceiros, logo a construção de um domínio baseado em LDAP não se aplica em todos os casos;

- Manter registro das atividades de conexão à rede internet em atendimento ao marco civil da internet (Lei N° 12.965/14);

- Impedir que dispositivos mal configurados concedessem o acesso indevido a impressões e arquivos compartilhados;

- Oferecer limite para largura de banda, impedindo o uso indiscriminado de *downloads* via *torrents* os quais possuem grande complexidade para seu total bloqueio.

- Gerenciar os acessos permitindo que haja a concessão de equipamentos conhecidos e bloqueio de dispositivos indesejados ou que ofereçam riscos à saúde da rede.

Assim e diante dos pontos acima apresentados, objetiva-se apresentar uma proposta como forma de gerência a qual seja simples, porém eficaz aos problemas apresentados.

1.2 OBJETIVOS

O objetivo deste trabalho é efetuar um estudo de caso e propor uma modelagem estrutural da rede de computadores, que possa ser utilizada para autenticar usuários de uma rede independentemente da via de acesso, do equipamento e do sistema operacional que o usuário venha a utilizar.

Busca-se, nesse caso, analisar algumas das diversas ferramentas e serviços já existentes, no intuito de atender a uma demanda institucional, onde há diferentes perfis de usuários previamente conhecidos.

A proposta a ser apresentada leva em consideração os conceitos relacionados à segurança da informação, como integridade, confiabilidade e disponibilidade, itens esses inerentes ao gerenciamento de redes de computadores.

Na proposta a ser apresentada ao fim deste trabalho, pretende-se modelar o funcionamento de uma rede internet autenticada e unificada para todas as unidades desta instituição e que seja o mais transparente possível para o usuário. Além disso, todo processo estará documentado o qual permitirá novas propostas e incrementos futuros.

1.2.1 Objetivos Específicos

Os objetivos específicos a serem atingidos são.

a) Efetuar uma análise da atual estrutura utilizada, através de questionamentos técnicos de forma a obter informações sobre a autenticação dos usuários da rede da Universidade Estadual do Norte do Paraná;

b) Modelar a partir de análise prévia, diferentes cenários o qual contemple os diferentes perfis de usuários e grupos;
c) Testar o modelo proposto;
d) Validar o modelo proposto através da aplicação de questionário específico, apresentado no item (a);
e) Apresentar a proposta como modelo de autenticação institucional.

1.3 JUSTIFICATIVA

Considerando que a UENP é uma instituição de ensino superior e que esta se formou a partir da união de 05 (cinco) faculdades, e que cada uma delas possui sua própria estrutura de rede, há, portanto, uma necessidade em se padronizar diversos procedimentos na área de Tecnologia da Informação (TI).

No que se refere ao TI, um dos pontos a ser abordado é a autenticação de usuários na rede. Isto é, há uma necessidade em se manter registrados e autenticados cada um dos diversos elementos que compõem essa estrutura.

Equipamentos e usuários precisam ser conhecidos, para que sejam contabilizados, organizados por diferentes tipos de perfil e atribuído a eles permissões de acesso, evitando problemas com a falta de segurança e com possíveis introduções às quais podem ocorrem de forma anônima.

Além disso, a uma necessidade em se criar um controle padronizado que seja possível gerenciar de forma menos custosa aos administradores e que também sejam transparentes ao usuário, que no caso, utiliza-se tanto de equipamentos da própria instituição como também de natureza proprietária. Nível de complexidade que é aumentada pelo fato de que esses equipamentos possuem diversos sistemas operacionais, como por exemplo: Android, Windows®, Linux, Mac OS, etc.

Diante do exposto e buscando atender a uma demanda institucional, esse trabalho tem por objetivo estudar e propor um modelo que possa ser utilizado para autenticação padronizada de usuários e equipamentos e que seja o mais transparente possível ao usuário, isto é, com o mínimo de interferência possível no quesito, configuração do equipamento proprietário para o uso da rede internet.

1.4 ORGANIZAÇÃO DO TRABALHO

O restante do trabalho está organizado da seguinte forma. O Capítulo 2 mostra os experimentos que foram conduzidos, sendo que na seção 2.1 é descria a análise previa realizada. Em 2.2 são detalhados os perfis de usuários e a definição de materiais e validação do modelo proposto. O Capítulo 3 apresenta a fundamentação teórica. Capítulo 4 detalha todo o processo de desenvolvimento do sistema. No Capítulo 5 apresenta as conclusões da pesquisa.

2. MATERIAIS E MÉTODOS

Nesse capítulo são apresentados os métodos utilizados para que se fossem feitas as análises preliminares para a composição do modelo proposto. Dois questionários foram apresentados ao público alvo. O primeiro questionário e de ordem mais técnica, teve por objetivo obter as informações da rede atual. O segundo questionário seguiu o método SUS (System Usability Score). Esse último, foi apresentado aos utilizadores do modelo proposto o qual foi, portanto implementado e implantado em uma das unidades institucionais. Nesse, o objetivo é o de avaliar o nível de satisfação.

2.1 Análise prévia

Para este trabalho, primeiramente foi necessário efetuar um levantamento da atual situação estrutural da rede internet da UENP no quesito autenticação de usuários. Estas informações serviram de base para mapear e modelar um sistema de autenticação e autorização com base em um C*aptive Portal.*

Para isso, foi elaborado um questionário conforme se observa na Tabela 01, onde houve a participação de alguns membros da comunidade acadêmica para a análise prévia. A partir desse, foi possível estabelecer discussões para a modelagem da proposta.

Tabela 1 - Pontos para mapeamento

	Questões	Sim	Não	Não sei informar
1	Existe a necessidade no uso de uma chave de criptografia para acesso a rede WiFi?			
2	As configurações necessárias para o ingresso na rede internet institucional requerem auxílio de suporte técnico?			
3	Há a disponibilidade do setor técnico para atendimento a qualquer hora, inclusive aos fins de semana?			
4	Foi observado algum termo sobre o uso da rede internet, que dê a ciência das políticas de uso, restrições e permissões?			
5	Quanto ao ingresso do equipamento de natureza não patrimonial da UENP, existe algum tipo de autenticação?			

6	Foi observada a existência de relatórios de acesso que atendam a Lei N° 12.965/14 (Marco Civil da Internet)			
7	É empregado algum tipo controle de largura de banda para rede WiFi e cabeada limitando o uso de *software* utilizados para compartilhamento de arquivos?			
8	Existe avisos do suporte técnico automatizado informando possíveis mudanças e/ou desligamentos programados na rede?			
9	Existem avisos do suporte técnico quanto ao uso de um determinado login estar sendo utilizado em outro equipamento? (Segurança)			
10	Existe algum tipo de bloqueio (firewall) impedindo algum serviço ou de softwares maliciosos?			
11	É observado diferentes tipos de redes e perfis (nome nas redes WiFi) para conexões específicas?			
12	Quanto ao primeiro ingresso na rede internet acadêmica, você considera esse um processo simples?			

Fonte: (AUTOR, 2017)

Participaram dessa coleta de informações, docentes, discentes, visitantes e técnicos administrativos. Os resultados obtidos foram quantificados sem o uso de algum peso para cada questão.

A quantificação dos dados produzidos com as respostas obtidas serviu de base para as análises e a elaboração de um modelo proposto.

2.2 Perfil de usuários existentes

Os perfis de usuários da rede, citados anteriormente (discentes, docentes, estagiários, técnicos administrativos e visitantes) compõem o conjunto de usuários da rede computacional e institucional. Assim, torna-se necessário analisar a segurança e a integridade dos dados que são trafegados nessa rede.

Considerando a discussões realizadas a partir da análise prévia, a proposta se pautou em autenticar os usuários com esses diferentes perfis, mantendo cada qual em uma estrutura lógica segura e isolada quando possível. A Tabela 02 abaixo apresentada, ilustra as principais permissões de acesso observadas para cada um dos perfis conhecidos.

Tabela 2 - Permissões de Acesso

Acessos e Serviços	Visitantes	Alunos	Estagiários /Projetos	Técnicos Administrativos	Professores
Navegação na rede Internet	*Filtrada*	*Livre*	*Livre*	*Livre*	*Livre*
Downloads	*Filtrada*	*Filtrada*	*Filtrada**	*Filtrada**	*Livre*
Portas de comunicação	*Bloqueado*	*Filtrada*	*Filtrada**	*Filtrada**	*Livre*
Laboratórios de Informática	*Bloqueado*	*Livre*	*Livre*	*Bloqueado*	*Livre*
Sistemas Administrativos	*Bloqueado*	*Bloqueado*	*Bloqueado**	*Livre*	*Livre*

Filtrada*: Filtros utilizados permissões diferenciadas de acesso

Fonte: (AUTOR, 2017)

2.2.1 Definição dos Materiais

Para essa proposta de autenticação unificada, utilizou-se de um Portal de Autenticação (Captive Portal), juntamente com o equipamento Mikrotik®, e o protocolo RADIUS. Além de permitir que relatórios de acesso possam ser gerados de forma a atender as normas estabelecidas pelo marco civil da internet (Lei N° 12.965/14).

Para que seja possível o uso dessas ferramentas, foi necessário estudá-las e configurá-las de forma a atender aos diferentes perfis de usuários observadas durante as análises prévias.

2.2.2 Validação do Modelo Proposto

Para avaliar a usabilidade e a satisfação do modelo proposto utilizou-se a aplicação do questionário SUS (System Usability Score). Este questionário, o qual se encontra no Apêndice deste trabalho, foi desenvolvido pela Digital Equipment CO Ltd., para avaliar a usabilidade dos sistemas e produtos desenvolvidos na empresa em questão. Descrito por Brooke (1996) esse questionário é considerado simples e de rápida aplicação que demonstra uma visão geral e subjetiva da avaliação da

usabilidade de um produto e também avalia a satisfação do usuário em relação ao produto. De acordo com os autores, este método consegue alcançar bons resultados com um baixo número de respostas. Ele aponta que a partir de 12 respostas, o método alcança um nível de exatidão de 100%, se comparado aos resultados do total de respostas.

Ainda segundo Brooke (1996), o SUS utiliza a escala Likert para medir as opiniões e atitudes. Este é composto por 10 questões que utiliza uma escala de avaliação com as seguintes pontuações: 1 (discordo plenamente), 2 (discordo), 3 (neutro), 4 (concordo) e 5 (concordo plenamente).

Conforme SIMÕES e MORAIS (2010) essas questões avaliam os seguintes itens:

- Frequência de uso do sistema;
- Complexidade do sistema;
- Facilidade de uso;
- Assistência para usar o sistema;
- Funções integradas do sistema;
- Inconsistência do sistema;
- Rápida aprendizagem;
- Sistema e incômodo e complicado para usar;
- Segurança e confiança para usar o sistema;
- Aprendizagem de outras informações para usar o sistema.

O cálculo utilizado para se obter a média do *System Usability Score* foi a seguinte:

$$\forall\, r_i \in Q_i,\ tal\ que\ 0 < i \geq 10\ Se\ r_i = \begin{cases} par,\ 5 - r_i \\ impar,\ r_i - 1 \end{cases}$$

Isto é, para todas as questões (Q_i) pares, deve-se subtrair a resposta (r_i) obtida do valor 5. Ou seja, se o usuário respondeu 2, deve-se contabilizar 3. Se o usuário respondeu 4, contabiliza-se 1. Para as questões (Q_i) ímpares, o procedimento consiste em subtrair 1 da resposta dada. Exemplo, se o usuário respondeu 3 à questão número 7, então o valor a ser pontuado para essa questão é 3 -1 = 2.

Uma vez que todas as respostas de todas as questões (n) tenham sido pontuadas, ainda é necessário que o resultado do somatório dessas pontuações seja multiplicado por 2,5 pontos.

$$\bar{X} = \frac{(\sum_{i=1}^{10} n) * 2{,}5}{n}$$

De acordo com Cunha (2010), se o valor médio $\bar{X}$ das pontuações obtidas for abaixo de 60 pontos, esses representam sistemas com experiências relativamente pobres e na insatisfação do usuário. Valor médio com pontuações acima de 80 pontos representa experiências muito boas com alto índice de satisfação dos usuários.

Além das 10 questões mencionadas, foi ainda apresentado um campo extra, em aberto, para que os usuários façam qualquer comentário ou sugestão sobre o sistema.

3. FUNDAMENTAÇÃO TEÓRICA

Neste capítulo é apresentada uma revisão de algumas bibliografias sobre ferramentas, conceitos e aplicações sobre o tema proposto. Neste, busca-se familiarizar o leitor para que os conceitos os quais serão na sequencia detalhados sobre seu uso no Capítulo 4. Desenvolvimento

3.1 REDES CABEADAS X REDES SEM FIO

Segundo Amador (2008) “as redes sem fio trazem grandes benefícios para as organizações e usuários, porém trazem também novas vulnerabilidades que podem colocar em risco os negócios da organização”.

A troca de informações realizada por meio de dispositivos que utilizam a rede sem fio, redes que apresentam acesso por meio de ondas de rádio, tais como *smartphone, tablet*, notebook, entre outros, podem acarretar em quebra de sigilo por pessoas não autorizadas de forma mais simplificada que uma rede cabeada, que por sua vez apresenta uma das características de apresentar conexão por meios físicos como fibra óptica, par metálico ou coaxial.

3.2 AUTENTICAÇÃO DE USUÁRIOS

Autenticação em uma rede é o método pelo qual acontecerá a identificação de um usuário junto ao sistema responsável por prover este serviço afim de que aja liberação de acessos para determinados acessos ou consultas. (STALLINGS e BROWN, 2015).

O sistema responsável por promover este credenciamento do usuário junto a rede pode utilizar-se algumas formas baseadas naquilo que o usuário já sabe, que o usuário tem, que o usuário é ou aquilo que o usuário faz.

As informações são encaminhadas ao servidor que fornece este serviço e o mesmo valida as informações passadas pelo usuário consultando em sua base de dados para comprovar a existência de tais informações e validar o processo. (BRANQUINHO, et al 2014).

3.3 AUTENTICAÇÃO BASEADA EM SENHAS

Sendo uma das formas mais utilizadas pelas organizações esta forma de credenciamento consiste em possuir um identificador e uma senha. (BRANQUINHO, et al 2014).

O identificador irá determinar se o usuário possui ou não privilégios para adentrar à rede bem como suas permissões.

Este tipo de autenticação leva em consideração senhas cadastradas anteriormente pelos usuários e são muito difundidos em boa parte dos sistemas existentes que pretendem utilizar uma forma de controlar se o usuário possui ou não privilégios para adentrar à rede bem como suas permissões. (STALLINGS e BROWN, 2015).

A quantidade de organizações que estão dando a devida atenção para este meio de autenticação tem aumentado pelo fato de diversos ataques sendo oriundos de força bruta ou simplesmente por palpites tem acontecido diariamente. (WEIDMAN, 2014).

3.4 AUTENTICAÇÃO BASEADA EM TOKEN

A autenticação por meio de *token* ocorre basicamente por meio daquele que o usuário possui consigo sendo uma chave física como um cartão de identificação apresentando uma chave ou sequência de caracteres que são interpretados por meio eletrônico. (STALLINGS e BROWN, 2015; BRANQUINHO et al, 2014).

Este método inclui outras formas populares de identificar o usuário como os chamados *smart cards* que são cartões semelhantes aos convencionais de instituições bancárias. Esta forma de autenticação apresenta a vantagem de possuir chip com capacidade superior aos convencionais fornecidos por instituições bancárias para armazenar todas as informações pertinentes a cada usuário. (CEGIELSKI, 2012).

Outra forma de efetuar a identificação utilizando os princípios deste modelo é pelo cartão de memória. Esta forma consiste basicamente de uma fita magnética capaz de armazenar apenas uma sequência numérica, semelhante aos cartões bancários. (STALLINGS e BROWN, 2015).

3.5 AUTENTICAÇÃO BASEADA EM BIOMETRIA

Esta forma de autenticação promove a verificação de autenticidade do usuário por meio do reconhecimento de características individuais específicas, tais como voz escrita, traços específicos da digital, entre outras. (SANTOS, 2008).

Graças a avanços no campo da tecnologia a biometria é uma das formas mais seguras e eficazes em termos de reconhecimento e autenticação de usuários. Sua autenticação é passível de ser realizada em meio segundo.

Independendo da forma como a autenticação biométrica é realizada, segundo (CABRAL e CAPRINO, 2015), a leitura biométrica “[...] é a forma mais natural de um ser humano provar quem ele é”.

3.6 SEGURANÇA DA INFORMAÇÃO

De acordo com (DIAS, 2000) “segurança é, por tanto, a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não autorizada, de forma a reduzir a probabilidade e o impacto de incidentes de segurança. Para (MATTOS, 2010), Informação pode ser entendida como uma medida quantificável analisada sobre certos aspectos bem como suas relações.

As informações de uma organização são aceitas como o bem mais valioso, de modo que sua segurança deixe de ser algo trivial para algo fundamental, ainda mais com o avanço contínuo da tecnologia.

Com o advento da tecnologia não houve outro momento da história humana cujas facilidades no acesso a informações privadas fossem realizas com tanta facilidade, já que em décadas passadas certas ferramentas tecnológicas pertenciam apenas à alta esfera do governo, contudo, conforme o tempo foi gradativamente evoluindo este paradigma acabou sofrendo mudanças. (DIAS, 2000).

Os objetivos de um usuário é possuir acesso à suas informações no momento em for mais conveniente, e de modo mais seguro possível sem, no entanto, que terceiros possuam qualquer acesso.

A fim de promover uma melhor política de segurança dentro da organização, é necessário que antes se façam conhecidas as ideias que apresentam impactos de modo a promover um melhor desenvolvimento dos objetivos da segurança. (DIAS, 2000).

Apresentando de modo consistente, Dias (2000), aponta sete objetivos fundamentais a qualquer política de segurança, sendo: confidencialidade, integridade de dados, disponibilidade, consistência, isolamento, auditoria e confidencialidade, onde cada item discrimina, respectivamente, o tipo de prioridade concedido a fim de assegurar ao máximo a segurança.

1. Confidencialidade: garantir que as informações não sejam acessadas por pessoas não autorizadas;
2. Integridade: garantir que os dados acessados não foram modificados de alguma forma sem autorização;
3. Disponibilidade: garantir o acesso aos dados pelo responsável no momento em que houver a necessidade;
4. Consistência: garantir que o sistema e, por conseguinte suas operações estejam em acordo com os requisitos propostos por seu usuário, de modo que um comando/solicitação faça com que seja executado qualquer outro;
5. Isolamento: garantir que o sistema não seja acessado por pessoas não autorizadas;
6. Auditoria: garantir que o sistema não apresenta inconsistências;
7. Confidencialidade: assegurar que independente do que possa vir a acontecer o sistema não disponibilizará as informações que nele pertence.

3.7 MARCO CIVIL

A necessidade da regulamentação desta ferramenta de comunicação, assim como o seu acesso, tornou-se objetivo em diversos cantos do mundo. No Brasil este processo de normalização, regras e padronizações, só se fez possível através da então sancionada Lei do Marco Civil da Internet. Essa Lei foi promulgada no ano de 2014 pela câmara dos deputados que estabelece diretrizes para o universo on-line. (LEI 12.965, 2015).

A regulamentação da Lei do Marco Civil, se deu em função do aumento na demanda da esfera de criminalidade. Com esta medida, a adequação não somente mensura esta problemática, como também permite a punição de usuários que

possam vir a cometer crimes virtuais os quais ainda não estão ou estiveram previstas no Código Penal brasileiro (TRUZZI, 2008).

A criação desta lei 12.965 se deu por meio de embates ligados a consumidores do serviço internet e de outro as empresas responsáveis por fornecerem tais serviços de modo a proteger os dados de seus utilizadores e dados gerados por meio do serviço.

Em termos de acesso inadequado à internet, é considerado crime, ações desde as já presentes no Código Penal, tais como roubos, como também, o acesso e o arquivo de conteúdos de pedofilia, a disseminação de arquivos maliciosos (vírus), ou mesmo, ofensas pessoais praticadas entre duas ou mais pessoas online (injúria). Todos esses acessos inadequados perante a Lei Marco Civil são crimes e deverão acarretar uma consequência ao autor (TRUZZI, 2008)

O Marco Civil da Internet foi instituído com a finalidade de estabelecer princípios, direitos e deveres ao ambiente virtual e, para que isso ocorra, esta lei define normas e regras gerais sobre a utilização da internet.

Para o melhor entendimento do Marco Civil da Internet são divididos os cincos pontos principais deste:

- Direitos: A Lei do Marco Civil da Internet prioriza a liberdade de expressão do cidadão pela internet, apontando até que a internet é essencial para a vida das pessoas. A vida privada do usuário não pode ser violada e a qualidade da conexão seja garantido conforme contratado e seus dados somente revelados em casos judiciais;

- Neutralidade: Um dos pontos mais questionados da Lei em que determina que as operadoras não podem vender pacotes de dados pelo tipo de uso, a internet deve ser tratada com isonomia;

- Guarda de informações: Existem dois tipos de informações para serem guardadas, os registros de conexão no qual o tempo de armazenamentos é de pelo menos um ano e os registros de acesso a aplicações que tem um prazo menor de seis meses.

- Responsabilidade da guarda de informações: A guarda de logs é de responsabilidade da empresa em que houve o acesso sendo que se

houver algum crime no conteúdo postado o usuário responsável respondera pelo ato judicialmente.

- Obrigações do Governo: O governo deve incentivar o uso da internet, ensinando as pessoas como utilizar e facilitando o acesso da rede.

3.8 PROTOCOLO RADIUS

O padrão IEEE 802.1x (*Port-Based Network Access Control*) é uma extensão do padrão da IEEE 802 e é utilizado para proporcionar o controle de acesso a uma determinada rede corporativa, baseando-se em normas para a autenticação de usuários e dispositivos de forma que possam ser autorizados a receber conectividade à rede interna é baseado no controle de portas, podendo ser aplicado às redes com ou sem fio. O ponto fundamental do protocolo é a capacidade de controlar o acesso à rede, autenticando todos os usuários que acessam seus recursos.

Segundo Blunk e Vollbrecht (2012), para que seja possível implementar uma rede com o padrão IEEE 802.1X é preciso a existência de uma infraestrutura de suporte. Isto é, clientes que tenham suporte ao padrão IEEE 802.1X, *switches*, pontos de acesso sem fio, servidor RADIUS e algum tipo de banco de dados de contas, como LDAP (*Lightweight Directory Access Protocol*) ou uma de suas implementações, como o Active Directory da Microsoft®. O padrão 802.1X tem como objetivo prover controle de acesso nas portas dos dispositivos de conexão, de modo a impedir que conexões clandestinas tenham acesso à rede.

RADIUS fornece autenticação, autorização e atribuição de responsabilidade ou (AAA), além de tratar-se de um protocolo de autenticação muito flexível capaz de atender todas as necessidades propostas pelo sistema. WRIGHTSON (2014).

3.9 CAPTIVE PORTAL

Um Captive Portal é essencialmente a integração de um *firewall* com uma página *web* de autenticação, que embora sejam associados a redes sem fio, ela não está diretamente ligada a elas. (Coleman, Westcott, Harkins e Jackman, 2011).

Quando um cliente abre um navegador independente da página solicitada, ele é redirecionado para uma página web especifica, em geral, esta página contém os termos de uso da rede. (BARKEN, 2004).

3.10 MIKROTIK

Mikrotik é uma empresa letã, voltada para desenvolvimento *wireless,* roteadores ISP e sistemas. Hoje em dia, ela fornece *software* e *hardware* para conectividade da rede internet para todo o mundo. (Amiri e Soltanian, 2015).

Neste trabalho foi utilizado tanto *hardware* quando *software* desta empresa, a qual dois modelos são apresentados na Figura 1 e 2, sendo um modelo mais robusto e outro mais simples.

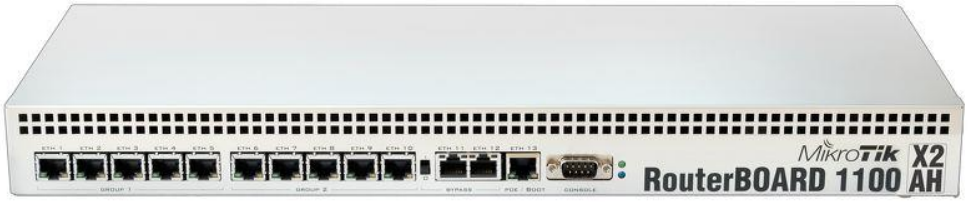

Figura 1 –Mikrotik® Routerboard 1100 AH X2
Fonte: (MIKROTIK, 2017)

Figura 2 - Mikrotik® Routerboard hEX Lite
Fonte: (MIKROTIK, 2017)

Estes equipamentos utilizam de um sistema operacional próprio, o RouterOS, este é um pacote de *software* de roteamento altamente configurável. Este *software* permite usar *hardware* comum para executar aplicativos de roteamento de ponta. A MikroTik cria desenvolve *software*, bem como muitas plataformas de *hardware* diferentes para executá-lo. Essas plataformas de *hardware* oferecem muitas opções, incluindo dispositivos de negócios e dispositivos domésticos de baixo custo, todo o caminho para as principais funções de roteamento de grandes fornecedores e empresas de Internet. (BURGESS, 2011).

Este *software* possui níveis de licença que já estão inclusas quando utilizadas em equipamentos de fabricação da empresa, porém, para outros equipamentos esta deverá ser adquirida de forma separada. Estas licenças impõem algumas limitações com relação as funcionalidades e a quantidade máxima de usuários conectados simultaneamente em determinados serviços, estas vão de 0 a 6, em que a licença de nível 0 é uma versão de teste que permite a utilização de todas as funcionalidades por 24h, as licenças de nível 2 foram descontinuadas e os demais níveis estão descritos na tabela 3. (MIKROTIK, 2015).

Embora haja diversos modelos, a escolha feita para implementação do modelo foi uma routerboard hEX Lite, esta possui uma Central Processing Unit - CPU único núcleo de 850Mhz, 64Mb de memória RAM, 16Mb de armazenamento interno com licença de nível 4 e RouterOS versão 6.28.

Tabela 3 - Níveis de Licença RouterOS

Nível	1	**3**	**4**	**5**	**6**
Suporte Inicial de Configuração	Não	Não	15 dias	30 dias	30 dias
AP sem fio	Não	Não	Sim	Sim	Sim
Cliente Wireless e Bridge P2P	Não	Sim	Sim	Sim	Sim
Protocolos RIP, OSPF e BGP*	Não	Sim (*)	Sim	Sim	Sim
Túneis EoIP	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Túneis / Usuários PPPoE	1	200	200	500	Ilimitado
Túneis / Usuários PPTP	1	200	200	500	Ilimitado
Túneis / Usuários L2TP	1	200	200	500	Ilimitado

Túneis / Usuários Open VPN	1	200	200	Ilimitado	Ilimitado
Interfaces VLAN	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Usuários simultâneos HotSpot	1	1	200	500	Ilimitado
Cliente RADIUS	Não	Sim	Sim	Sim	Sim
Controle de Banda / Queues	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado
Web Proxy	Não	Sim	Sim	Sim	Sim
Sessões no User Manager	1	10	20	50	Ilimitado
Número de KVM Guests	1	Ilimitado	Ilimitado	Ilimitado	Ilimitado

(*) - BGP é incluída na Licença de Nível 3 apenas para Routerboards, para outros dispositivos deverá ser usada a licença de nível 4 para utilizar o BGP.

Fonte: (MIKROTIK, 2015)

4. DESENVOLVIMENTO

Nesse capítulo é apresentada a estrutura da rede modelada, apresentada como proposta para a autenticação dos usuários de todas as unidades da instituição.

4.1 ESTRUTURA DO SISTEMA

O sistema é constituído por um conjunto de serviços e dispositivos integrados que visa prover a autenticação e o controle de usuários em uma rede institucional. A Figura 3 ilustra a estrutura completa do sistema.

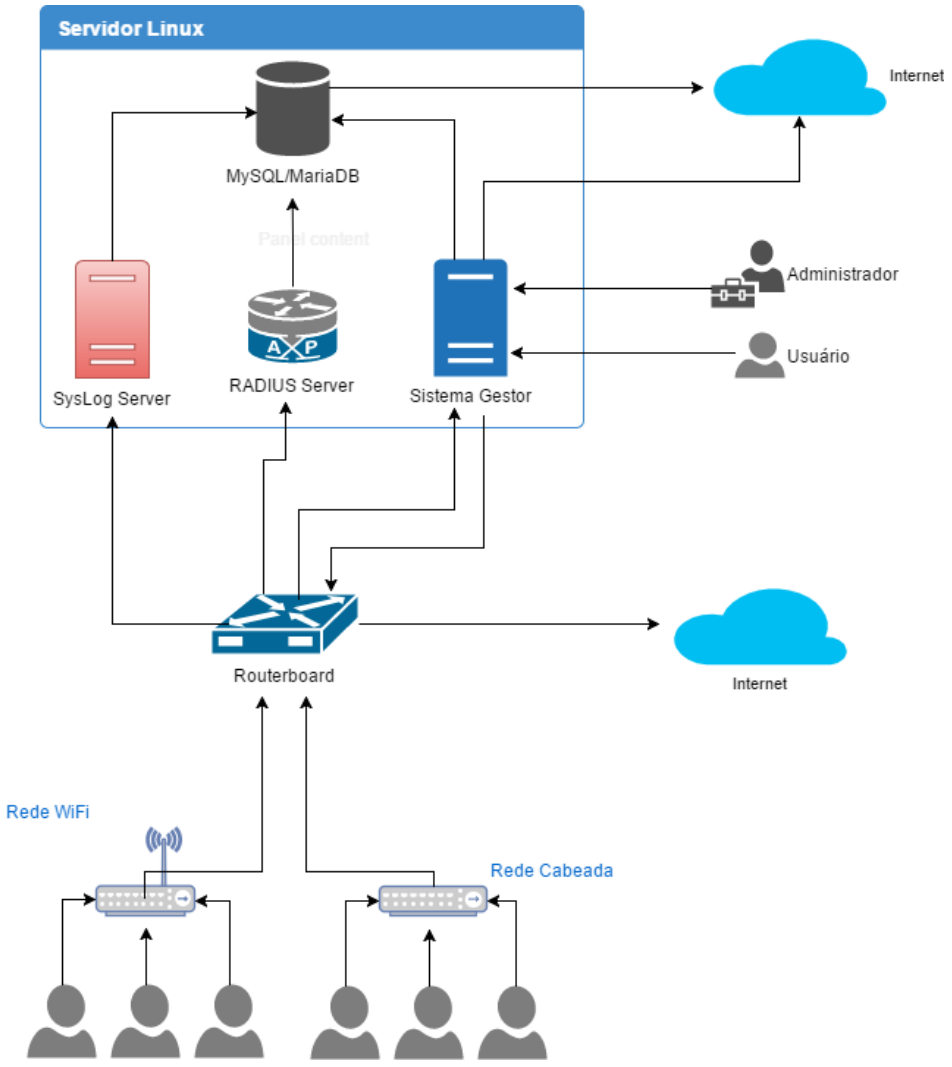

Figura 3 - Estrutura geral do Sistema

Fonte: (AUTOR, 2017)

Todos os serviços foram configurados e testados em ambiente Linux utilizando Ubuntu Server 16.04.2 LTS 64 bits

A estrutura apresentada no esquema da Figura 3 é gerenciada por meio de um sistema gestor web desenvolvido em PHP e utilizando o *framework* Laravel um framework PHP livre e open-source criado por Taylor B. Otwell para o desenvolvimento de sistemas web que utilizam o padrão MVC, (OTWELL, 2017) em sua versão 5.4, Vue.js um framework JavaScript Progressivo para criação de interfaces de usuário (YOU, 2017) versão 1.0.21.

Esse sistema gestor é responsável pelo cadastro e gerenciamento de usuários, grupos, redes, regras de *firewall* e registros de *log*, permitindo agilidade no trabalho do administrador de redes e também que, um agente administrativo sem conhecimentos técnicos possa realizar a gestão de usuários, além do monitoramento de acesso, localização e se necessário bloqueio imediato de um usuário.

A estrutura proposta, além do sistema gestor, também integra mais duas partes, o núcleo, o autenticador.

4.1.1 O Núcleo

O núcleo de autenticação de usuários é constituído por um servidor RADIUS, isto é, de um protocolo de rede que fornece gerenciamento centralizado de Autenticação, Autorização e Contabilização. Os usuários pertencentes a ele se conectam e utilizam o serviço de rede disponível. Neste caso, modelo utilizado foi *freeradius* versão 2.2.8 x86_64.

Uma vez que um usuário solicita o ingresso na rede, é gerado uma requisição para o RADIUS, que valida as informações enviadas como *login*, senha, endereço MAC, entre outras que serão utilizadas para autorizar ou não o usuário. Caso o mesmo seja autorizado, o servidor retorna parâmetros referente ao seu perfil que serão utilizadas pelo autenticador para definir suas permissões de acesso.

As informações são armazenadas em um banco de dados relacional MySQL (utilizada versão 5.7.18) o qual foi escolhido pelo fato do servidor RADIUS possuir *driver* nativo para comunicação.

4.1.2 Banco de Dados

Conforme apresentado anteriormente, o banco de dados utilizado foi o MySQL, nele foram utilizadas as tabelas nativas do FreeRadius além de outras auxiliares para uma melhor organização das informações, conforme a Figura 4.

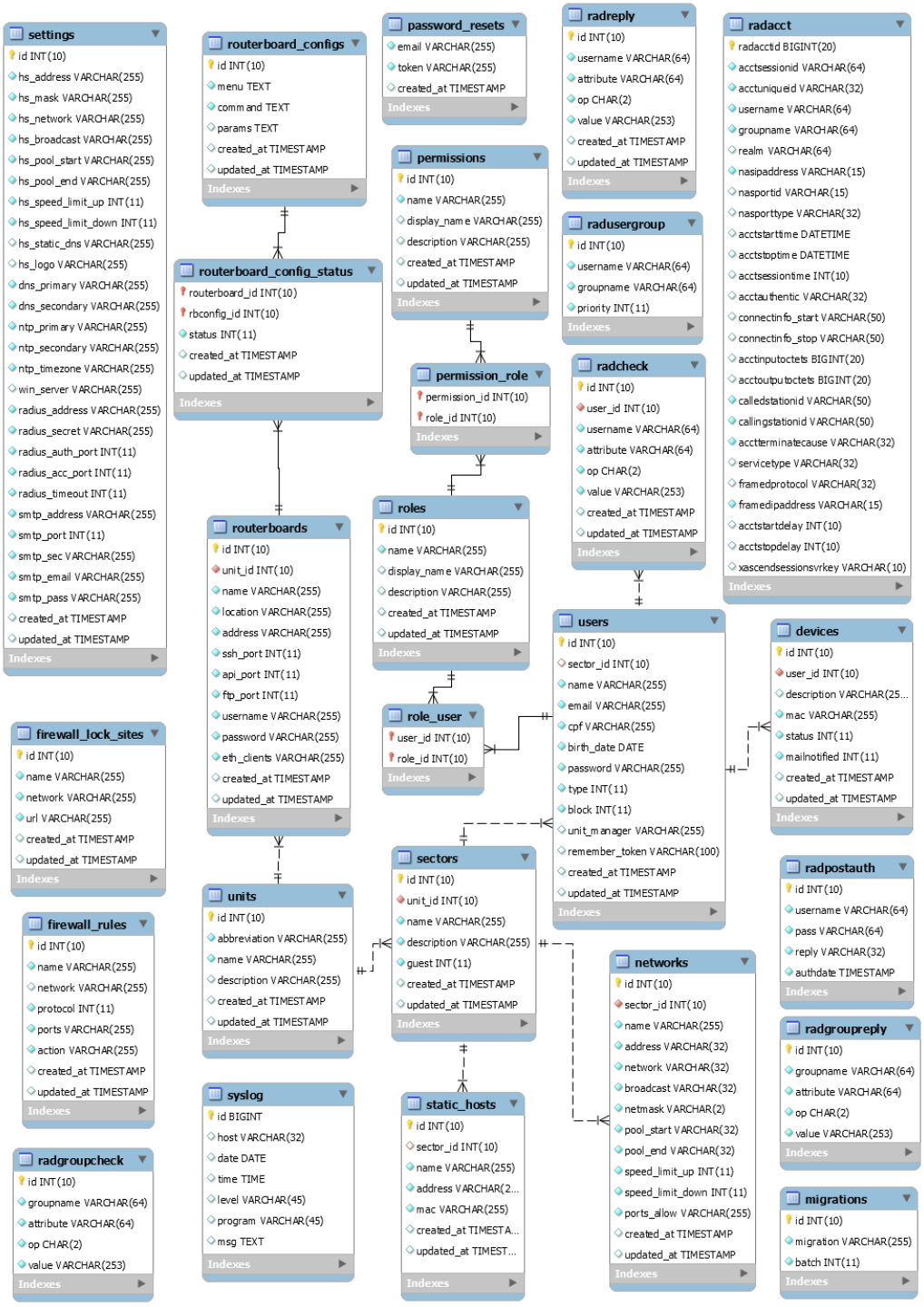

Figura 4 - Banco de Dados

Fonte: (AUTOR, 2017)

4.1.3 Autenticador

É constituído por roteadores Mikrotik, também denominado de Routerboard que realiza a autenticação do usuário por meio do serviço de *HotSpot*, desta forma, estes equipamentos serão responsáveis por todo o gerenciamento, autenticação e gestão da rede como controle de banda, firewall, etc. Quando um usuário tenta utilizar qualquer recurso da rede, o mesmo é redirecionado para o *captive portal,* onde as credenciais de acesso são solicitadas.

A *routerboard* utiliza do servidor RADIUS para verificar as credenciais do usuário e utiliza para isso, os parâmetros retornados para definir inúmeras permissões de acesso geradas em tempo de execução. Esses parâmetros fazem parte de um dicionário de comunicação do *RouterOS* que especifica vários comandos a serem utilizados pelo RADIUS que são interpretados pela *routerboard* após a autenticação.

Este modelo permite que várias *routerboards* autentiquem em um servidor RADIUS e também que cada *routerboard*, utilize de mais de um servidor, permitindo assim não só várias *routerboards* autenticarem em um único servidor, mas também que uma *routerboard,* autentique em mais de um servidor, possibilitando consultas em bases diferentes ou até mesmo uma base secundária caso a principal venha a falhar.

4.1.4 Integração

O sistema utiliza a mesma base do servidor RADIUS e de suas tabelas tanto nativas como adicionais para efetuar a gestão de suas configurações. Dessa forma o sistema gestor registra tanto suas tabelas como as tabelas do RADIUS com os parâmetros necessários para autenticação dos usuários, controlando assim a atividade do servidor pelo banco de dados.

Para a configuração do autenticador, o sistema gestor envia as configurações para as *routerboards*, que permitem o acesso via interface gráfica, interface web, linha de comando SSH e API. Para este sistema foi utilizado a comunicação via API por meio da biblioteca PEAR2/RouterOS, permitindo assim que o sistema execute configurações em qualquer routerboard.

Ao registrar uma configuração, o sistema gestor cria comandos compatíveis com as *routerboards* e salva essas informações no banco de dados. Em seguida, monta uma relação de todos os comandos gerados no banco juntamente com as *routerboards* cadastradas, gerando um *status* dessa relação *routerboard*/configuração, de modo a garantir que todas as configurações sejam aplicadas em todas as *routerboards.*

As configurações realizadas somente serão aplicadas na *routerboard* caso seja selecionada a opção aplicar, ou seja, inúmeras alterações podem ser realizadas e aplicadas de uma só vez em uma ou mais *routerboards*, conforme a Figura 5.

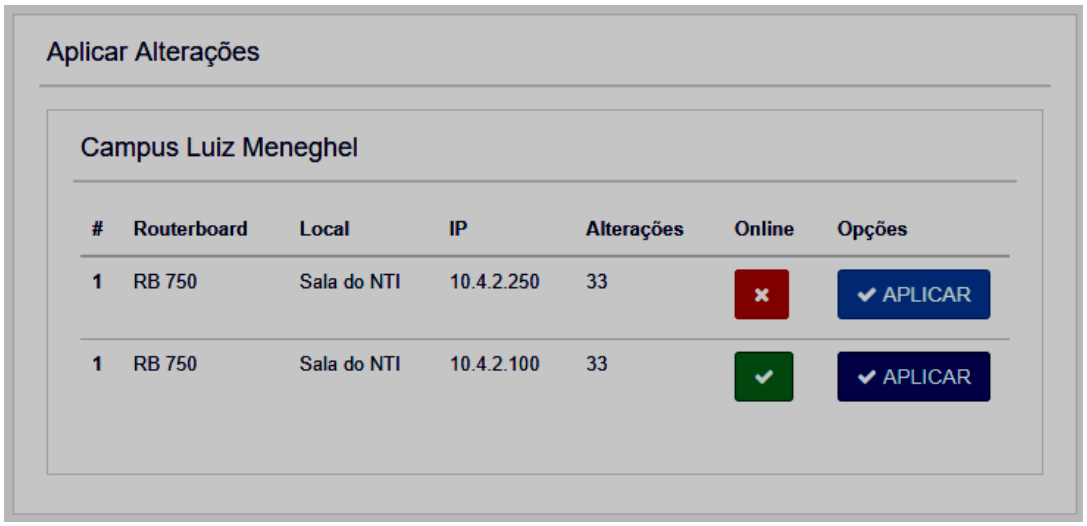

Figura 5 – Aplicar alterações
Fonte: (AUTOR, 2017)

Ao aplicar serão exibidas todas as configurações e o status da mesma com relação aquela *routerboard* conforme a Figura 6.

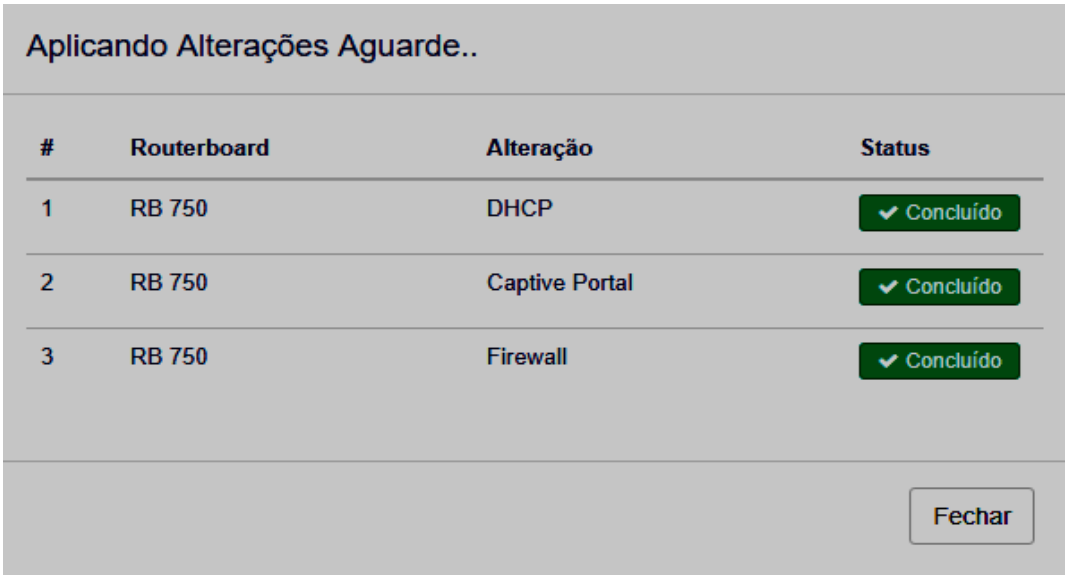

Figura 6 - Status Aplicar configurações

Fonte: (AUTOR, 2017)

Dessa forma o sistema gestor registra parâmetros relacionados ao perfil do usuário na base do RADIUS, e registra as mesmas configurações em cada uma das *routerboards,* de modo que quando o usuário ingressa na rede, suas permissões de acesso são configuradas adequadamente, caso não haja a possibilidade de gerá-las o usuário não será autorizado.

Partindo desse princípio, a Figura 7 ilustra o processo que o sistema gestor realiza para registro de uma nova configuração, tanto no RADIUS, quanto em uma *routerboard,* de modo que seja possível a comunicação entre os dois.

Figura 7 - Schema de comunicação para configuração

Fonte: (AUTOR, 2017)

Considerando o pressuposto de que o processo apresentado na Figura 6 tenha sido realizado com sucesso. O processo de autenticação do usuário é então iniciado. A Figura 8 ilustra como acontece a comunicação entre uma *routerboard* e o RADIUS.

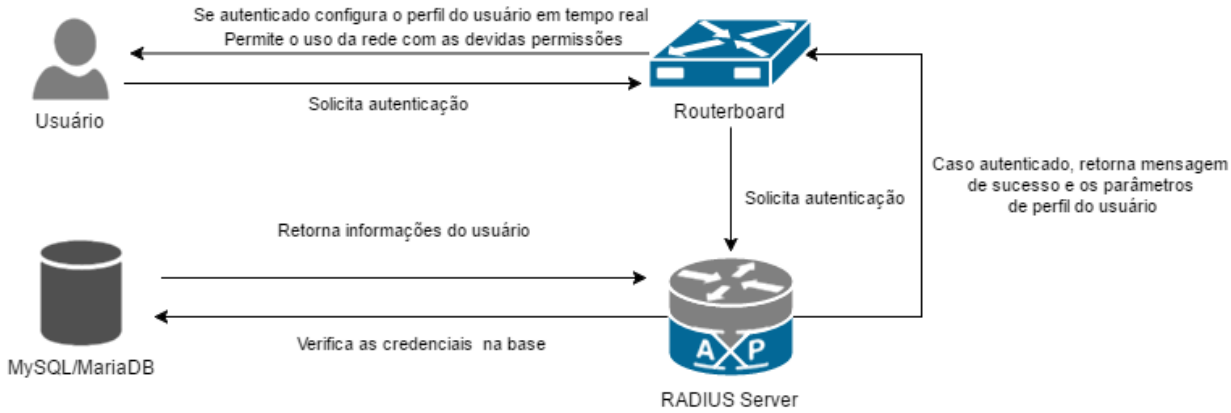

Figura 8 - Esquema de comunicação para autenticação do usuário na rede.
Fonte: (AUTOR, 2017)

O processo de autenticação do usuário com a *routerboard* é realizado via protocolo HTTPS, uma vez que o processo é realizado via *browser*, faz-se necessário o uso de um certificado de segurança SSL/TLS válido assinado por uma autoridade certificadora, que ficará armazenado em cada *routerboard*.

A autorização do servidor RADIUS é realizada por meio de PAP, visto que devido às diferenças entre os protocolos suportados pelas *routerboards* PAP e CHAP, com relação ao armazenamento das senhas do banco de dados, o PAP permite que a senha seja gravada em formado de HASH. A Tabela 4 ilustra os protocolos suportados pelo FreeRadius e a compatibilidade de armazenamento das senhas para cara protocolo utilizado para autenticação.

Tabela 4 - Compatibilidade de Protocolos e Senhas FreeRadius

	Clear-text	NT hash (ntlm_auth)	MD5 hash	Salted MD5 hash	SHA1 hash	Salted SHA1 hash	Unix Crypt
PAP	✓	✓	✓	✓	✓	✓	✓
CHAP	✓	x	x	x	x	x	x
Digest	✓	x	x	x	x	x	x
MS-CHAP	✓	✓	x	x	x	x	x
PEAP	✓	✓	x	x	x	x	x
EAP-MSCHAPv2	✓	✓	x	x	x	x	x
Cisco LEAP	✓	✓	x	x	x	x	x
EAP-GTC	✓	✓	✓	✓	✓	✓	✓
EAP-MD5	✓	x	x	x	x	x	x
EAP-SIM	✓	x	x	x	x	x	x
EAP-TLS	x	x	x	x	x	x	x

Fonte: (DEKOK, 2014)

Estabelecendo um paralelo entre os protocolos CHAP e PAP, observa-se que o primeiro apresenta um maior nível de segurança no tráfego das informações, porém, não dá suporte para o armazenamento criptografado das senhas dos usuários na base de dados, contudo, o segundo protocolo tem como recurso principal o fato de poder armazenar estas senhas utilizando-se do formato HASH, mas o tráfego das informações fluem livremente pela rede podendo facilitar o processo de captura por parte de pessoas não autorizadas.

Com base nas informações descritas, o PAP foi o protocolo escolhido pelo fato de que na estrutura de rede proposta para o sistema a comunicação da *routerboard* e o núcleo deva ser feita por uma rede privada, a qual será inacessível aos usuários do sistema, assim a possibilidade de armazenar as senhas cifradas foi considerada a melhor opção de modo a ampliar a segurança dos usuários, que atualmente estão sendo armazenadas em SHA1, contudo, esse é um padrão de comunicação que pode ser alterado no sistema de modo que o administrador da rede possa definir qual método se encaixa melhor em sua estrutura, como mostra a Figura 9.

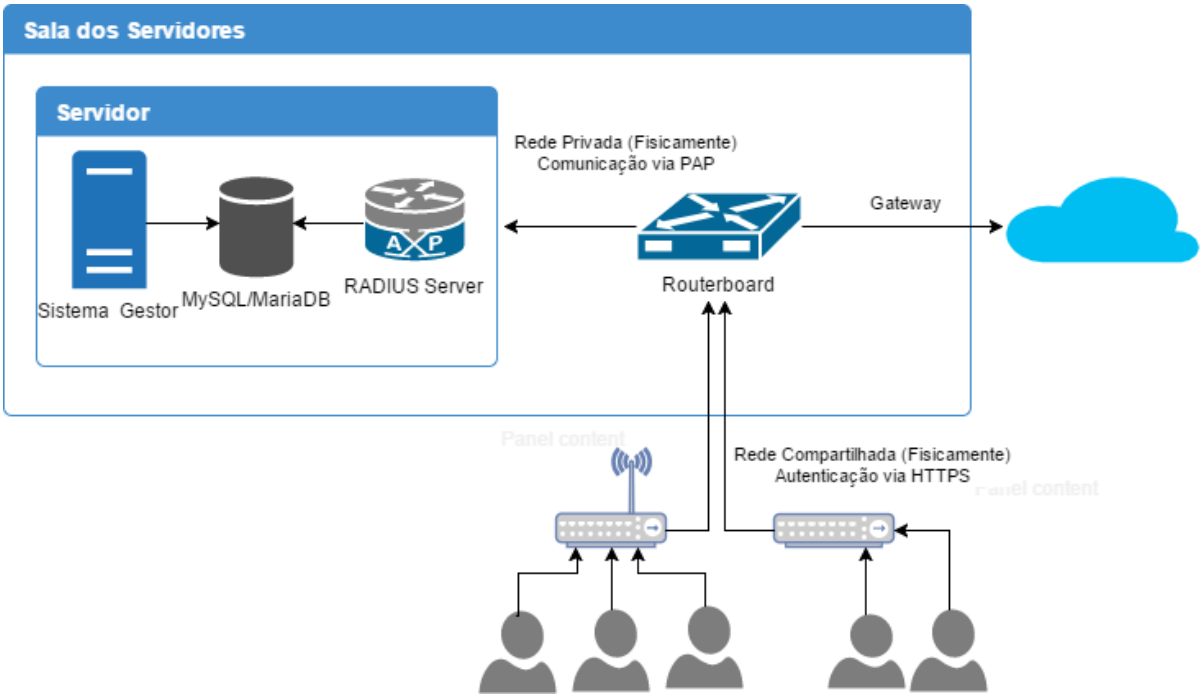

Figura 9 - Estrutura dos equipamentos da rede

Fonte: (AUTOR, 2017)

4.1.5 Comunicação

Conforme ilustrado na Figura 10, existem vários fluxos de comunicação entre as partes do sistema, sendo:

1. Utilizada para a replicação[1] do banco de dados entre as unidades;
2. Conexão usada para envio das informações recebidas pelo *syslog-ng server* afim de armazená-las no banco de dados;
3. Utilizado para consultas de autenticação do servidor RADIUS e para o registro de todas as sessões dos usuários, controladas pelo servidor;
4. Manipulação e gestão das informações do banco de dados;
5. Possibilita que o sistema seja acessado remotamente pela internet de modo que o administrador possa acompanhar o andamento da rede de qualquer lugar;

[1]Replicação, segundo Coulouris et. al. (2013), "é uma técnica para manter automaticamente a disponibilidade dos dados, a despeito das falhas no servidor."

6. Interface de administração da rede;

7. Interface do usuário para visualização de seu perfil, alteração de senha e bloqueio/desbloqueio de dispositivos;

8. Canal de envio do log do aparelho para o syslog-ng;

9. Canal de autenticação e autorização dos usuários via PAP;

10. Canal de comunicação via API utilizado para a configuração da *routerboard,* realizada pelo sistema gestor através de comandos pré-definidos;

11. Coleta de dados em tempo real das *routerboards* para exibição no sistema gestor, como status do aparelho e usuários online, também realizada via API;

12. *Gateway*[2] de saída para os usuários autenticados na rede. Também permite a disponibilidade da *routerboard* externamente através de um IP público, possibilitando ao gestor de outra unidade realizar novas configurações sejam aplicadas nas demais *routerboards* de todas as unidades em tempo real;

13. Processo de autenticação dos usuários na rede via HTTPS, e tráfego de informações quando autorizado.

[2] Gateway, segundo Carmona (2007), "é um dispositivo intermediário usado, geralmente, para interligar redes, separar domínios de colisão ou atuar como conversor de protocolos, permitindo, assim a comunicação entre redes incompatíveis. Um grande exemplo de gateway é o roteador!

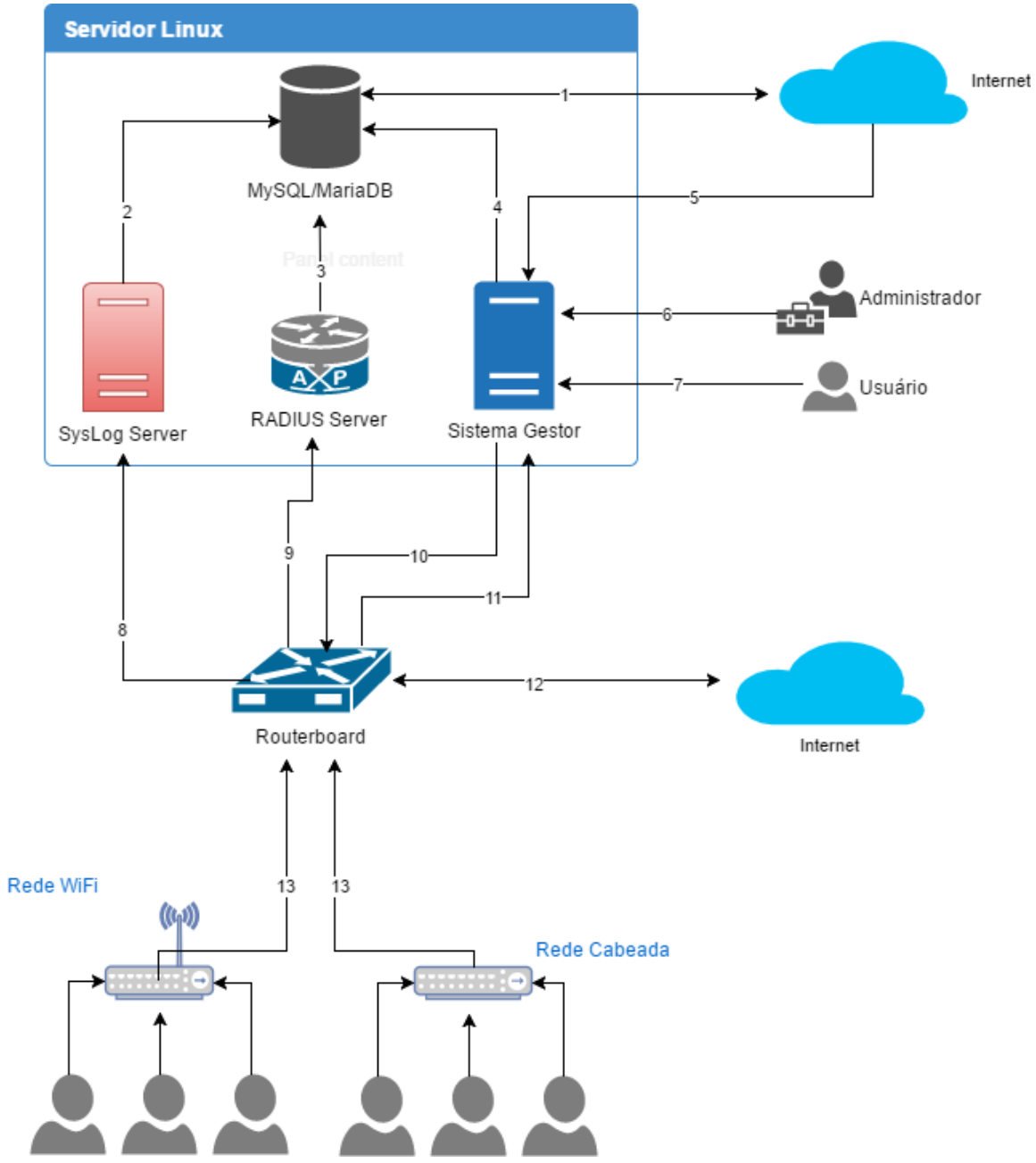

Figura 10 – Estrutura de comunicação.

Fonte: (AUTOR, 2017)

4.1.6 Usuários

Considerando a estrutura multi *campi* da instituição, o sistema gestor possibilita uma hierarquia para a organização dos usuários de modo que seja possível gerenciá-los de acordo com seu setor e/ou vínculo com a instituição.

O nível mais alto do sistema é chamado de unidade, isto é, cada endereço predial presente em suas respectivas cidades. O nível abaixo da unidade é chamado de Setor, ou seja, um grupo em que será possível agrupar uma quantidade de usuários vinculados a um determinado curso, centro ou setor, como por exemplo: RH, NTI, Direção, etc.

Paralelo ao Setor têm-se uma categoria padrão denominada Visitantes, esta por sua vez, agrupará todos os usuários que não possuem qualquer vínculo com a instituição. Aos usuários deste grupo, será liberado acesso à Internet com permissões restritas.

No último nível hierárquico, estão os usuários, que necessariamente estarão vinculados a um Grupo/Setor conforme ilustra a Figura 11.

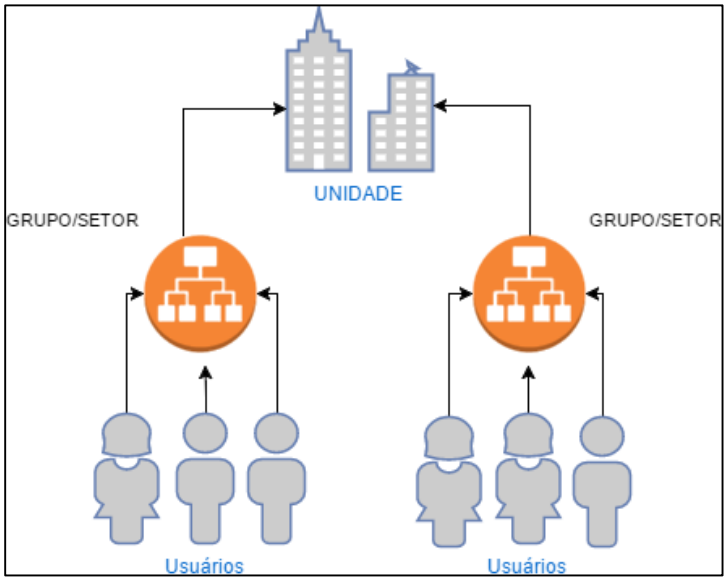

Figura 11 - Organização de Usuários

Fonte: (AUTOR, 2017)

Cada setor possuirá uma rede IPv4 e a ela são atribuídas devidas permissões de acesso. Assim todos os usuários vinculados ao setor compartilham dessas permissões e podem comunicarem-se somente entre si, ou seja, não é permitida a comunicação entre diferentes sub redes.

4.1.6.1 Login

O processo de login dos usuários é realizado através de um C*aptive Portal*. Este que é único para qualquer sistema operacional, bastando apenas o uso de um navegador para que o processo seja realizado. A página de login também, possui as opções de esqueci minha senha e realizar novo cadastro, conforme pode ser visto na Figura 12.

Figura 12 - Tela de Login
Fonte: (AUTOR, 2017)

4.1.6.2 Cadastro

O cadastro de usuários poderá ser feito pelo próprio usuário, que deverá informar seus dados pessoais bem como sua unidade/setor que está vinculado. O cadastro foi elaborado para que seja simples e rápido de modo que não torne um processo extenso e cansativo, Figura 13.

Ao se cadastrar o usuário precisa concordar com os temos de uso da rede, este que é formulado pela instituição que proverá o serviço de acesso à internet. O usuário também receberá via e-mail o link de seu painel de usuário. Neste constam

as informações sobre o uso da rede e também sobre notificações que o sistema enviará informando sua atividade da rede.

Figura 13 - Tela de Cadastro

Fonte: (AUTOR, 2017)

O cadastro também pode ser realizado por um Administrador de modo que quando isto ocorrer, ao vincular o usuário a um setor o mesmo será inserido na rede e suas permissões automaticamente atribuídas, caso o usuário tenha se auto cadastrado seu acesso à internet será liberado imediatamente, porém, com as mesmas restrições aplicadas aos visitantes, até que o administrador valide se realmente o referido usuário possui vínculo com a instituição/setor informado. A partir desse ponto o usuário receberá os privilégios do setor a qual foi inserido. O administrador também poderá bloquear o acesso, caso constate que as informações

fornecidas no cadastro não sejam verídicas, ou simplesmente ignorar a solicitação que deixará o usuário continuar utilizando a rede como visitante.

4.1.6.3 Dispositivos

O usuário poderá utilizar suas credencias de acesso em quantos dispositivos forem convenientes, uma vez que o sistema captura o MAC de cada um deles e gera uma lista, e para cada dispositivo é gerado um histórico de login, o qual fica registrado seu local, data e horário referentes ao início e término da sessão e a quantidade de banda consumida.

Esta lista de dispositivos fica disponível no painel do usuário, possibilitando que ele tenha conhecimento de todos os dispositivos que utiliza a rede permitindo que o próprio usuário bloqueie ou desbloqueie a qualquer momento seus dispositivos. A listagem também indica a atividade desses ativos. Assim é possível saber se o mesmo está online ou não, podendo desconectá-lo instantaneamente caso haja suspeita de uso irregular. A listagem dos dispositivos do painel de usuário é ilustrada na Figura 14.

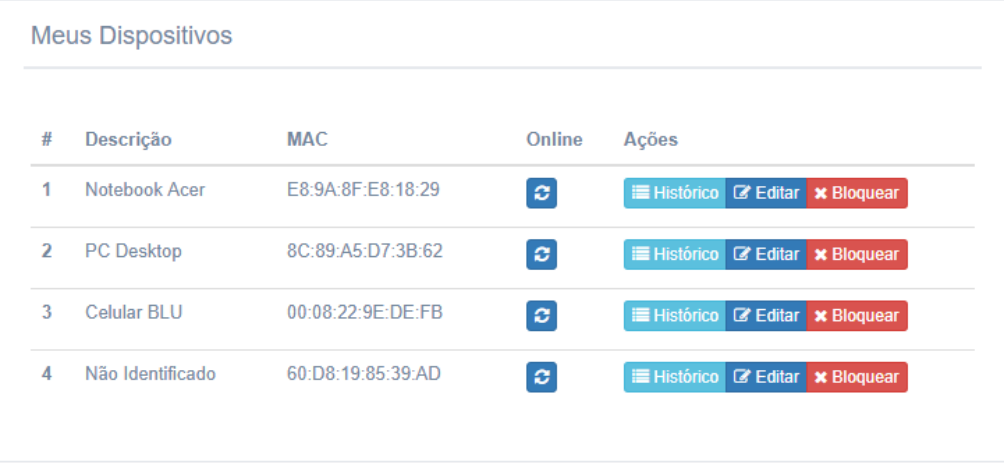

Figura 14 - Listagem de dispositivos
Fonte: (AUTOR, 2017)

Afim de que cada usuário seja responsável por suas credenciais e para aumentar o nível de segurança, toda vez que este realizar o *login* em um dispositivo nunca utilizado anteriormente, o sistema envia uma notificação via e-mail ao usuário informando que um novo dispositivo entrou na rede com suas credenciais.

Uma vez está ação seja do próprio usuário, a mensagem poderá ser ignorada, porém, caso contrário através do e-mail enviado é possível bloquear o dispositivo e também alterar a senha, conforme a Figura 15.

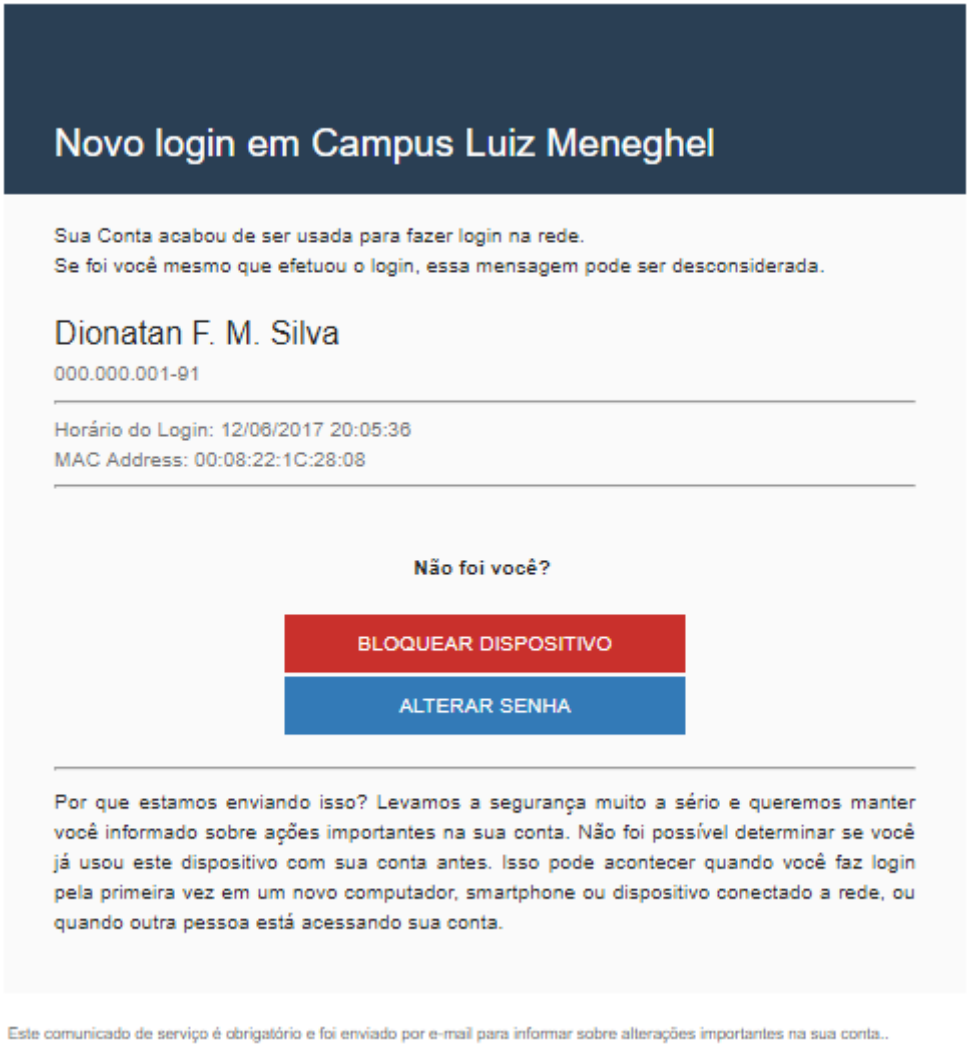

Figura 15 – E-mail Atividade na rede

Fonte: (AUTOR, 2017)

Ao bloquear um dispositivo o mesmo é desconectado instantaneamente da rede, uma vez que o sistema localiza a *routerboard* a qual ele está conectado e o desconecta, além de registrar o endereço MAC como não autorizado para utilizar aquela credencial, ou seja, um outro usuário poderá acessar no mesmo dispositivo uma vez que somente a combinação de credencial e MAC são bloqueadas, desta

forma as mesmas credenciais não ficam bloqueadas para o acesso em outros dispositivos.

Caso o usuário bloqueie um dispositivo indevidamente ou se arrependa da ação, o mesmo pode acessar seu painel do usuário e o desbloqueá-lo e ainda poderá bloquear qualquer outro dispositivo sempre que julgar necessário. Estas ações também podem ser realizadas por um administrador da rede.

Nenhum dispositivo ou registro de *login* pode ser apagado, seja pelo usuário ou administrador da rede.

Esta função é realizada através do módulo que executa funções do servidor RADIUS que após a autenticação do usuário executa um *script*[3] enviando parâmetros do dispositivo que acabara de se conectar. O script envia os dados para o sistema utilizando cURL[4] que realiza toda a checagem e envia a notificação caso pertinente.

Vale ressaltar que o processo de autenticação do servidor aguarda a execução do script para que conclua o processo, assim o usuário informa suas credenciais, o servidor as valida e caso sejam aceitas é executado o script e apenas após sua conclusão é retornando a mensagem para a *routerboard.* Neste caso como o script faz parte de uma função que envia um e-mail para o usuário se for um novo dispositivo, o tempo de resposta do servidor de e-mail, pode impactar diretamente na performance da autenticação e até impedi-la caso o tempo do servidor seja maior que o timeout da *routerboard* (limite máximo 10 segundos). Desta forma para evitar tais situações o sistema gestor apenas registra o e-mail no banco de dados e já finaliza o processo para que o usuário seja autenticado e envia esses e-mails através de um processo rodando em segundo plano no servidor.

4.2 AUTENTICAÇÃO

Nesta sessão é descrito tanto o processo de autenticação de um usuário ao acessar a rede quanto o processo que o sistema realiza para provê-la.

---

[3] Script segundo Costa (2009) “é um arquivo contendo um conjunto de comandos, que serão executados (interpretados) por um interpretador”.

[4] cURL segundo George (2014) “é um utilitário de linha de comando para transferência de dados que entende vários protocolos. Ou seja, podemos acessar uma URL via cURL e obter sua resposta.

4.2.1 Captive Portal (HotSpot)

A fim de reduzir a demanda de trabalho do administrador da rede e não permitir que um usuário mal intencionado tenha acesso a outras redes e permissões acesso apenas alterando manualmente o endereço IP de seu dispositivo, todas as regras são controladas pelo *Captive Portal*, isso significa que não é necessário cadastrar o MAC de um dispositivo ou colocar um IP fixo na máquina para que o mesmo faça parte de uma rede diferente, basta o usuário realizar a autenticação que todas as permissões ligadas ao seu usuário serão concedidas em tempo de login, independentemente do endereço IP de seu dispositivo.

Para que o usuário chegue ao *hotspot* o sistema dispõe de uma faixa de controle, ou seja, uma faixa de IP para todos os dispositivos que ingressam na rede, que servirá apenas para levar os usuários até a página de autenticação. O tamanho da rede é definido pelo administrador dependendo da quantidade de usuários. Uma vez configurada essa faixa de controle será habilitado um servidor DHCP[5]que entregará um endereço para cada host que ingressar na rede, com a máscara de 32 bits, por exemplo, uma rede de controle 10.200.255.254/16 cada host receberá um endereço de 10.200.0.1 a 10.200.255.253 com mascará de 32 bits considerando que o servidor DHCP seja 10.200.255.254. Isso faz com que um host não seja capaz de se comunicar com o outro, inclusive com o servidor, evitando a descoberta de rede entre eles e também o excesso de *broadcast*[6].

O simples fato da máquina possuir um endereço IP e um Gateway de saída já faz com que ele seja interceptado pelo *hotspot.*

Cada dispositivo autenticado na rede possui um tempo de vida*(timeout)* de quinze minutos, desta forma se o usuário estiver desconectado durante esse período, o sistema permitirá que o host reconecte na rede sem a necessidade de uma nova autenticação. Considerando uma unidade com vários blocos, um usuário pode mover-se entre eles sem a necessidade de efetuar login novamente.

---

[5]DHCP, segundo Ross (2008), "é uma forma de alocação dinâmica de endereços IP".

[6]Broadcast, segundo Comer (2015), refere-se a entrega de uma cópia de um pacote para vários destinos simultaneamente".

Este princípio só é válido dentro de uma única *routerboard,* ou seja, se a unidade inteira for atendida por uma routerboard em que a rede seja distribuída com *switches*[7], o usuário poderá alterar de SSID[8] ou até mesmo trocar o ponto de acesso de rede sem desconexão desde que isto ocorra dentro do intervalo permitido. O login é vinculado ao endereço MAC, assim se o usuário alterar a interface de rede terá que logar novamente.

4.2.2 Autorização

O processo de autorização do usuário acontece no momento que ele autentica na rede e suas credencias são aceitas pelo servidor RADIUS, a partir daí, são executados parâmetros ligados ao seu perfil, permitindo e/ou negando serviços ao usuário que subdivide-se em três tipos:

- **Usuário visitante:** esta categoria não possuí parâmetros de autorização, e uma vez autenticado, será liberado apenas acesso à internet com limite reduzido de banda, portas e demais regras de firewall definidas para esta rede pelo administrador.
- **Usuário bloqueado:** esta categoria possui parâmetros de bloqueio para o usuário, independentemente do dispositivo usado, seu login será permitido, porém, com navegação bloqueada, e ao tentar abrir qualquer site será redirecionada para uma página informando que seu cadastro se encontra bloqueado, cabendo procurar o setor responsável para regularização.
- **Usuário vinculado à instituição:** um usuário vinculado a um setor possui parâmetros que indicam a qual rede ele irá pertencer. Esta rede está associada a um setor previamente cadastrado pelo administrador, que é associado a uma rede IPv4, por exemplo, a rede 172.18.10.0/24 em que todas as permissões desse grupo são definidas para todos os endereços dentro do range.

  Quando um usuário é autenticado, o servidor retorna a identificação do POOL[9] relacionado ao usuário, isso faz com que o próximo endereço

[7] Switch, de acordo com Pedro (2009), "é um dispositivo que em a função de compartilhar a sua rede".

[8] SSID é o nome da sua rede (GRALLHA, 2005).

[9] POOL é usado para definir um range de endereços IP que são usados por um servidor DHCP. (MIKROTIK, 2010).

disponível dentro desse POOL seja associado ao endereço da faixa de controle na máquina do usuário, de modo que ele não seja conhecido dentro da rede pelo IP que realmente está em sua máquina (10.200.0.1/32), mas sim o IP associado ao seu POOL (172.18.10.1/24) representando seu setor, conforme a figura 16.

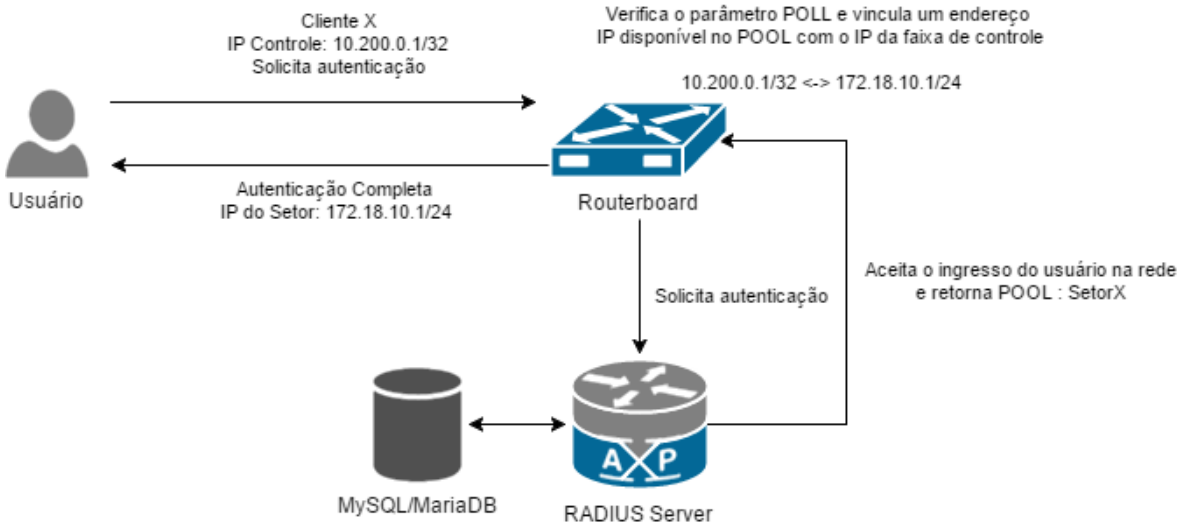

Figura 16 - Atribuição de IP do Setor

Fonte: (AUTOR, 2017)

Dessa forma o IP de controle é utilizado apenas para a comunicação do Host com a *routerboard,* que a partir desse ponto realiza a tradução para o endereço específico setor/grupo do usuário. Dentro desse POOL é permitida a comunicação entre hosts do mesmo setor. Conforme mostra a Figura 17.

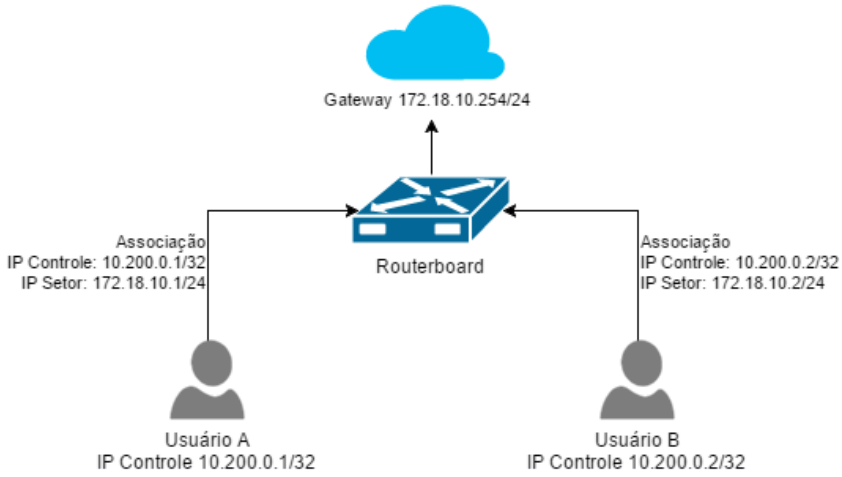

Figura 17 - Comunicação dentro de um Setor

Fonte: (AUTOR, 2017)

No exemplo acima Figura 16, o usuário A e B pertencem ao mesmo grupo e ambos podem comunicar-se, porém, utilizando o IP do setor, que apesar de virtual, é exibido na tela de status de login. Caso o usuário A tente se comunicar com o B utilizando a rede 10.200.0.0 a comunicação não será permitida pela máscara de 32 bits, já na rede 172.18.10.0 há permissão devido a sua máscara de 24 bits.

O gateway de saída também é diferente para cada rede, neste caso o gateway do setor é 172.18.10.254 e para usuários visitantes é utilizado o IP da faixa de controle 10.200.255.254 como gateway.

O IP do setor é registrado e funciona somente dentro da *routerboard,* uma vez que um usuário utilizar um endereço IP fixo da faixa de um setor, não surtirá efeito, visto que ele será utilizado apenas para comunicação com o captive portal que funciona como se estivesse na faixa de controle, assim o seu IP de comunicação será atribuído pelo nível de permissão de seu login. Caso seja um visitante, será gerada uma tradução de endereço para o IP da máquina para o IP que realmente deveria pertencer aquele host que é a faixa de controle e visitantes (10.200.0.0).

Considerando que a tradução de endereços é realizada na *routerboard,* qualquer comunicação entre hosts obrigatoriamente passa por ela, das quais em um ambiente que utiliza compartilhamento de arquivos pesados em vários setores, o tráfego não ficará apenas entre a *switch* e os *hosts* dentro do local, mas será direcionado a *routerboard* responsável pela

tradução. Neste cenário esta questão deverá ser analisada pelo administrador da rede antes da implantação do sistema para uma melhor distribuição dos equipamentos para que não haja gargalo na rede.

4.2.3 Hosts Estáticos

Para este trabalho considera-se um host estático como sendo ele um dispositivo conectado à rede o qual não é capaz de se autenticar utilizando o *Captive Portal*, como impressoras, *access points*, câmeras IP, entre outros. Para isso criou-se uma sessão que permite o cadastro e a inclusão desses dispositivos na rede de forma automática por meio de seu endereço MAC, caso contrário, o mesmo receberia um endereço da faixa de controle que o deixaria inacessível dentro da rede visto que seria necessário que estes dispositivos fizessem autenticação na rede utilizando uma credencial.

Através desse cadastro o sistema indica para a *routerboard* qual endereço o IP que sempre deverá ser entregue para o dispositivo, por meio do DHCP, além disso, é autorizada a comunicação com o dispositivo via MAC combinado com o IP de modo que o endereço não seja utilizado por hosts indevidos, porém, não garante que o endereço seja utilizado por um host malicioso que tenha clonado o MAC da impressora utilizando o mesmo IP em um momento que a mesma esteja desligada.

4.3 DISTRIBUIÇÃO

O sistema foi desenvolvido para ser implantado em um servidor local em cada unidade, que por sua vez, é responsável pela autenticação e gestão dos equipamentos dessa unidade, contudo, pode receber e autenticar usuários de outras unidades, uma vez que a base de dados será replicada em todas as demais unidades, assim, caso haja deslocamento de pessoas de uma unidade para outra, o usuário cadastrado em uma unidade poderá conectar-se à outra com as mesmas credenciais.

Desse modo a replicação dos dados não é realizada de forma sistêmica, mas sim, pela replicação do banco de dados em cada unidade que utiliza uma instância do sistema.

O objetivo a ser alcançado neste caso é evitar a centralização única de uma base de autenticação, a fim de reduzir ao máximo a suscetibilidade a falhas, erros e diversos tipos de ameaças.

O sistema permite a cada gestor de unidade gerir apenas a sua unidade e um gestor geral toda a universidade.

Dentro do escopo de todas as unidades não haverá a possibilidade de utilizar duas vezes uma mesma rede IPv4, uma vez que ela será única para um setor e permitirá que um usuário utilize dos mesmos privilégios de sua unidade principal em todas as outras. A Figura 18 ilustra o modo que a replicação deve ser realizada.

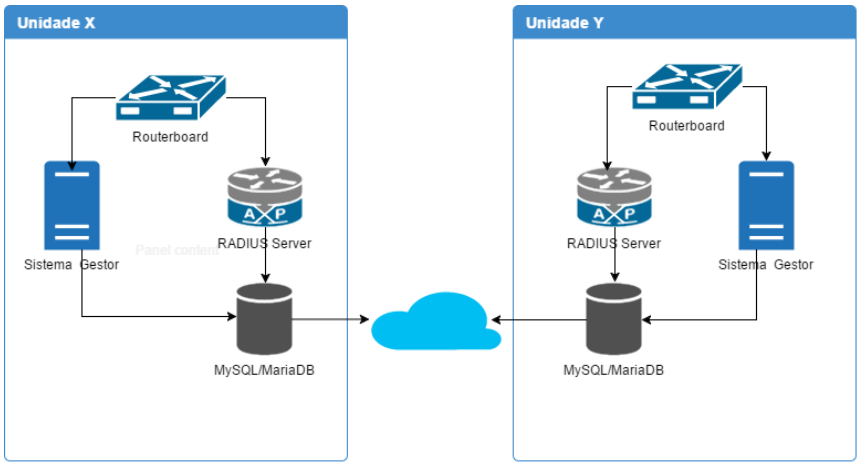

Figura 18 - Replicação dos dados

Fonte: (AUTOR, 2017)

4.4 CONTROLE DE ACESSO

O sistema permite que sejam elegidos administradores para geri-lo, esse processo consiste na autorização de um usuário já existente na rede como administrador, apresentando como obrigatoriedade que o usuário já possua cadastro junto ao sistema. Assim o administrador utiliza as mesmas credenciais para acesso à rede, gerenciamento de seu painel pessoal e administração da rede.

O controle de permissões é realizado de duas formas, sendo o primeiro voltado para o controle de unidades, uma vez que um administrador da universidade tem acesso a todas as unidades, enquanto que os administradores locais possuem acesso apenas a unidade a qual exista vínculo, assim o administrador local tem acesso a todas as funcionalidades do sistema, porém, apenas relacionadas com a

sua unidade. Um administrador local também não possui autorização de alterar qualquer permissão relacionada à administração do sistema gestor, cabendo somente ao administrador da universidade.

A segunda forma de permissão é realizada por meio de um controle de permissões, esse controle é vinculado com cada ação do sistema, ou seja, independentemente de um administrador ser geral ou local, haveria a possibilidade de estar vinculado a um grupo, possibilitando, por exemplo, que usuários administradores apenas visualizem informações do sistema sem permissão de editar, adicionar ou remover, como, por exemplo, acessar o cadastro de usuário e não a parte de gestão das redes, firewall, etc. Todas essas configurações são previamente definidas pelo administrador geral no próprio sistema por meio do navegador.

4.5 FIREWALL

O sistema conta com gerenciamento de regras de firewall, em que duas funcionalidades estão disponíveis dentro do sistema gestor.

- **Controle de acesso a portas**: Permite a permissão/bloqueio de uma ou mais portas separadas por vírgula ou um range de portas separado por hífen em todas as redes ou para redes específicas. O sistema gera configurações referentes ao firewall e envia as regras para cada *routerboard* que habilita as regras nas redes informadas.

- **Controle de acesso a sites:** Permite o bloqueio de acesso a sites através do domínio ou palavra-chave, da mesma forma que o controle de portas, são geradas regras que são enviadas para cada routerboard que por sua vez cria um filtro na camada de aplicação, que coleta os primeiros 10 pacotes de uma conexão ou os primeiros 2KB e procura o padrão nos dados coletados. Através desse padrão são criadas regras de firewall que bloqueiam todas as conexões que se encaixem no padrão da palavra chave inserida na regra. O bloqueio também pode ser realizado para todas as redes, ou para uma rede especifica.

4.6 Log

- **Log do Sistema**

  O log do sistema abrange todas as ações que acontecem dentro dele originadas de ações de usuários, seja ele um administrador ou um usuário comum que utiliza da rede.

  O administrador terá todas as suas ações registradas, referentes à administração da rede, criação, edição e remoção de itens. Quanto aos registros do usuário, são armazenados no log, data de cadastro, notificações enviadas, bloqueios e/ou desbloqueios de dispositivos.

- **Log das Routerboards**

  Este por sua vez monitora tudo que acontece nas routerboards, ou seja, todos os eventos que estão acontecendo. Cada dispositivo já possui um log e além do mais, possibilita enviar esse registro para um servidor remoto assim que qualquer ocorra um determinado evento.

  O dispositivo tem seu log apagado assim que sua alimentação é cortada. Algumas opções permitem que ele seja gravado no disco interno, entretanto o equipamento não permite um grande armazenamento de informações, além de que em um ambiente com várias routerboards, cada log ficaria em seu dispositivo de forma isolada. Desta forma o log das routerboards podem ser centralizados em um único servidor de log.

  Para a gestão do log no servidor foi utilizado o syslog-ng server versão 3.5, serviço que permite sua coleta e armazenamento, tanto do sistema operacional quanto de sistemas externos. Neste caso foram habilitadas regras para receber dados de servidores externos, no caso as routerboards, registrando-os no banco de dados, assim todos os logs são preservados. Estes logs são armazenados da forma que são gerados, em texto puro em que o syslog-ng indica a atividade e o dispositivo que encaminhou a ação.

- **Log de firewall**

  Este trabalho não contempla registros de conexões, ou seja, por quais servidores o usuário se conectou, porém, com sua estrutura de log, isso é permitido uma vez que o firewall do RouterOS possibilita que todo o tráfego

que passa por suas regras sejam registradas no log. Assim pode-se verificar inúmeros quesitos como o registro de cada conexão do usuário que passa pelo NAT, capturando seu endereço e porta de origem, de destino, protocolo e endereço MAC, ou verificar se existem tentativas de acesso a sites e/ou portas bloqueadas, entre outras inúmeras coisas que sejam controladas pelo firewall, desde que em acordo com a lei do marco civil de modo a não comprometer a privacidade do usuário.

Os logs de conexão podem ser enviados para o *syslog-ng server* utilizando categorias específicas e armazenadas de forma organizada de acordo com seu tipo e não apenas no formato em que é gerado.

5. RESULTADOS OBTIDOS

O modelo proposto foi em caráter de teste implantado no NTI do campus Luiz Meneghel de Bandeirantes - PR, abrangendo 4 computadores desktop, 3 notebooks, 4 smartphones, além de duas impressoras de rede HP (Hewlett Pakcard). Os dispositivos contaram com sistemas operacionais diferentes sendo Microsoft Windows®, Linux, Android e iOS.

Foram realizados testes de desempenho durante 30 dias. Durante esse período foi possível testar a autenticação, cadastros, permissões de acesso, alteração de endereços IP e clonagem de MAC, além dos ativos considerados fixos, como as impressoras em suas devidas sub-redes. Controle de banda, acesso à sites e portas, bloqueio de dispositivos, notificações via e-mail também foram testadas e validadas com sucesso.

Após a construção e validação do protótipo, esse foi implantado em uma escala maior, agora, na unidade *campus* de Cornélio Procópio. Após três semanas de utilização, foi possível contabilizar 394 usuários cadastrados, todos estes sem a necessidade se suporte técnico para ingresso a rede. Destes usuários 21 eram visitantes, 315 cadastrados foram homologados pelo administrador da rede em 7 diferentes perfis, 58 usuários aguardavam homologação. Dentro deste cenário foram registrados 812 dispositivos que foram utilizados para acessar a rede, média de 2 por usuário, estes somaram 7971 solicitações de acesso ao serviço de autenticação dos quais 6243 foram aceitos e 1729 rejeitadas.

O que se seguiu foi a apresentação do questionário SUS, com o objetivo encontrar um índice de satisfação por parte do usuário e de validar a proposta apresentada.

Os resultados obtidos revelaram segundo Cunha (2010), um significativa satisfação dos usuários, uma vez que o valor obtido com a resposta de 42 usuários foi de 75, 6 conforme pode ser vista no Anexo B.

Observando as respostas da questão deixada em aberto, (questão nº 11), foi possível observar dois itens que impediram que o resultado da avaliação fosse ainda melhor. Os 05 usuários que atribuíram um valor baixo de 60 pontos fizeram menção a esses dois intens.

O primeiro item pontuado de forma negativa refere-se ao estado de inatividade permitido, Keep Alive Timeout, (Sessão 4.2.1) o qual foi configurado com valor extremamente pequeno. Neste caso os usuários precisavam se acessar novamente após 5 minutos de inatividade na rede, que ocorre quando determinado dispositivo se desconecta da rede. Seja por falta de cobertura da rede WiFi ou por inatividade do usuário no dispositivo. Geralmente essas desconexões também estão associadas as configurações de economia de energia.

O segundo item refere-se a área de cobertura da rede *WiFi*. Como houve a substituição de equipamentos de curto alcance por equipamentos mais eficientes, esses precisaram ser realocados. Novos pontos passaram a ser avaliados e instalados sob a crescente demanda. Buscando neste caso instalar mais equipamentos *WiFi* impedindo a sobreposição de sinais de rádio frequência e eliminando pontos considerados áreas de sombra.

6. CONSIDERAÇÕES FINAIS

A avaliação ao geral da proposta de autenticação de usuários na rede institucional se mostrou muito positiva, tanto em relação à pontuação ao obtida no SUS, quanto em relação às opiniões e sugestões apresentadas pelos usuários que avaliaram o ambiente.

Entende-se também que foi possível atender à quase todos os pontos apresentados na formulação do problema. Embora alguns desses pontos ainda necessitem ser melhorados, novas implementações devem ser constantemente feitas e que essas possam tornar esse sistema de autenticação ainda mais robusto e eficaz.

Almeja-se para tanto que esse sistema de autenticação possa ser homologado pelo Núcleo de TI institucional e tornar-se disponível de forma redundante e síncrona em todas as unidades desta instituição.

6.1 Trabalhos Futuros

Como sugestão de implementação em trabalhos futuros, torna-se interessante avaliar *(Keep Alive Timeout), isto é,* o aumento do tempo em que o usuário necessita permanecer conectado. Para esse caso, a sugestão é o uso de *cookies*.

Outro item sugerido, é a integração com outras bases de dados, como é o caso da base LDAP. Neste caso sugere-se a supressão da autenticação via *Captive Portal* e integra esse a uma base de domínio para equipamentos de natureza patrimonial da instituição (laboratórios e máquinas administrativas).

Somado a trabalhos paralelos que estão sendo realizados, é sugerido um estudo sobre os *logs* de registros expedidos pela *routerboard* de forma a atender os critérios pontuados pela Lei do Marco Civil da Internet.

REFERÊNCIAS

AMADOR, Wilson Junior de Brito. Analise de desempenho do padrão IEEE 802.1x em redes cabeadas utilizando infra-estrutura de chave publica. Disponível em <http://repositorio.uniceub.br/bitstream/123456789/3273/2/20115379.pdf> Acesso em 26/09/2016.

AMIRI, Iraj Sadegh; SOLTANIAN, Mohammad Reza Khalifeh. Theoretical and Experimental: Methods for Defending Against DDoS Attacks. Waltham: Elsevier, 2016.

BARKEN, Lee. Wireless Hacking: Projects For Wi – Fi Enthusiasts. Rockland: Syngress, 2004.

BLUNK, L.; VOLLBRECHT, J. RFC 2284 - PPP Extensible Authentication Protocol (EAP), disponível em <http://www.ietf.org/rfc/rfc2284.txt> Acesso em 22/10/2016.

BRANQUINHO, Marcelo Ayres; SEIDL, Jan ; MORAES, Leonardo Cardoso de; BRANQUINHO, Thiago Braga; JUNIOR, Jarcy de Azevedo. Segurança de Automação e Industrial e SCADA. Rio de Janeiro: Elsiever, 2014.

BRASIL, PARANÁ. Lei, 12.965, 23 de abril de 2014. Ementa. Câmara dos Deputados.

BROOKE, J. Sus-a quick and dirty usability scale. Usability evaluation in industry, 189(194):47, 1996.

BURGESS, Deniss. Learn Routeros. 2ª ed. Raleigh: lulu.com, 2011.

CABRAL, Carlos; CAPRINO, Willian. Trilhas em Segurança da Informação: Caminhos e Ideais para a Proteção de Dados. Rio de Janeiro: Brasport, 2015.

CARMONA, Tadeu. Guia técnico de redes de computadores. São Paulo: Digerati Books, 2007.

CEGIELSKI, Casey. Introdução a Sistemas de Informação: Apoiando e Transformando Negócios na era da Mobilidade. 3. ed. Rio de Janeiro: Elsiever, 2012.

COLEMAN, David D.; WESTCOTT, David A.; HARKINS, Bryan E.; JACKMAN, Shawn M. CWSP – Certified Wireless Security Professional Official Study Guide: Exam PWO - 204. Danvers: Wiley, 2010.

COMER, Douglas. Interligação de redes com tcp/ip – vol. 1: princípios, protocolos e arquitetura. 6ª ed. Rio de Janeiro: Elsevier, 2015.

COSTA, Daniel Gouveia. Administração de redes com scripts: bash script, python e vbscript. Rio de Janeiro: Brasport, 2007.

COULOURIS, George; DOLLIMORE, Jean; KINDBERG, Tim; BLAIR, Gordon. Sistemas distribuídos. 5ª ed. Porto Alegre: Bookman, 2013.

CUNHA, M. L. C. Redes sociais dirigidas ao contexto das coisas. Master's thesis, PUC - RJ, 2010.

DEKOK, Alan. Freeradius howtos: getting things done quickly. Disponível em: < http://deployingradius.com/documents/protocols/compatibility.html>. Acesso em: 22/02/2017.

DIAS, Claudia. Segurança e auditoria da tecnologia da informação. Rio de Janeiro: Axcel Books, 2000

GEORGE, Mauro. RSpec: crie especificações executáveis em ruby. São Paulo: Casa do Código, 2014.

HASSEL, Jonathan. RADIUS. California: O'Reilly Media, 2002.

MATTOS, Alessandro Nicoli de. Informação é Prata Compreensão é Ouro: Um Guia para Todos Sobre Como Produzir e Consumir Informação na Era da Compreensão.[S.l.: s.n.], 2009.

MIKROTIK, Documentation. Manual. Disponível em: <https://wiki.mikrotik.com/wiki/Main_Page>. Acesso em: 17/11/2016.

OTWELL, Taylor B. Laravel: The PHP Framework For Web Artisans. Disponível em: <https://laravel.com/>. Acesso em: 11/07/2017.

RODRIGUES. Edson Junior Lobo. Curso de Engenharia de Software: Métodos e Processos para Garantir a Qualidade no Desenvolvimento de Softwares. São Paulo: Digerati Books, 2008.

ROSS, Julio. Redes de computadores. Rio de Janeiro: Livrotec, 2008.

SANTOS, Alfredo. Quem Mexeu no meu Sistema? Segurança em Sistemas de Informação. Rio de Janeiro: Brasport, 2008.

SIMÕES. A. P.; MORAES. A. Aplicação do questionário sus para a avaliação da satisfação e usabilidade de um software de ead. Anais do 10º Congresso Internacional de Ergonomia e Usabilidade de Interfaces Humano-Computador. 10, (Mai, 2010).

STALLINGS, William; BROWN, Lawrie. Segurança de Computadores: Princípios e Prática. 2. ed. Rio de Janeiro: Elsiever, 2014.

TRUZZI, Gisele. "Crimes virtuais", 2008. Disponível em: <http://www.truzzi.com.br/pdf/artigo-crimes-virtuais-gisele-truzzi-2008.pdf>. Acesso em: 14 jul. 2016>

WEIDMAN, Georgia. Testes de Invasão: Uma Introdução Prática ao Hacking. São Paulo: Novatec, 2014.

WIGHTSON Tyler,; SILVA, Aldir Jose Coelho Correa. Segurança de redes sem fio. Porto Alegre: Bookman, 2014.

YOU, Evan. Vue: The Progressive JavaScript Framework. Disponível em: <https://vuejs.org/>. Acesso em: 11/07/2017.

ANEXO A

Pesquisa sobre o Sistema Institucional de Controle de Acesso à Internet da Universidade Estadual do Norte do Paraná - UENP

01 - Gostaria de usar este serviço frequentemente. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

02 - Achei que o serviço era desnecessariamente complexo. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

03 - Achei o serviço simples de usar. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

04 - Penso que iria precisar de apoio técnico para usar o serviço. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

05 - Achei as várias funcionalidades do serviço bem integradas. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

06 - Penso que havia demasiadas inconsistências no serviço. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

07 - Imagino que a maioria das pessoas aprenda rapidamente a usar o serviço. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

08 - Achei que o serviço não era trivial de usar. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

09 - Senti-me muito confiante a usar o serviço. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

10 - Preciso de aprender muito antes de poder usar este serviço. *

	1	2	3	4	5	
Discordo Muito	○	○	○	○	○	Concordo Muito

11 - Escreva aqui suas opiniões e sugestões sobre o Sistema.

ANEXO B

Resultados Obtidos (SUS)

Questão01		Questão02		Questão03		Questão04		Questão05		Questão06		Questão07		Questão08		Questão09		Questão10	
Nota	nota -1	Nota	5 - nota	Nota	nota -1	Nota	5 - nota	Nota	nota -1	Nota	5 - nota	Nota	nota -1	Nota	5 - nota	Nota	nota -1	Nota	5 - nota
5	4	2	3	3	2	1	4	3	2	2	3	4	3	2	3	4	3	2	3
3	2	2	3	4	3	1	4	2	1	3	2	4	3	2	3	3	2	1	4
5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4
5	4	3	2	5	4	2	3	5	4	4	1	5	4	3	2	5	4	3	2
5	4	3	2	3	2	3	2	3	2	1	4	3	2	3	2	3	2	1	4
5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4
5	4	3	2	1	0	4	1	2	1	3	2	3	2	3	2	1	0	4	1
5	4	1	4	5	4	1	4	2	1	2	3	5	4	1	4	5	4	1	4
5	4	3	2	3	2	1	4	3	2	1	4	5	4	1	4	5	4	1	4
5	4	2	3	4	3	1	4	4	3	2	3	5	4	3	2	4	3	1	4
4	3	3	2	4	3	2	3	4	3	3	2	4	3	3	2	4	3	1	4
4	3	1	4	5	4	1	4	5	4	1	4	5	4	3	2	5	4	1	4
5	4	4	1	5	4	1	4	5	4	4	1	5	4	1	4	5	4	1	4
5	4	5	0	1	0	5	0	1	0	5	0	3	2	1	4	1	0	5	0
5	4	4	1	2	1	1	4	4	3	2	3	5	4	2	3	5	4	2	3
4	3	3	2	5	4	1	4	3	2	3	2	4	3	3	2	2	1	1	4
5	4	1	4	5	4	1	4	3	2	3	2	4	3	4	1	4	3	1	4
5	4	3	2	4	3	1	4	5	4	5	0	4	3	4	1	5	4	1	4
5	4	5	0	2	1	3	2	2	1	4	1	1	0	5	0	2	1	2	3
2	1	5	0	2	1	1	4	2	1	5	0	3	2	3	2	3	2	2	3
5	4	3	2	3	2	1	4	3	2	3	2	5	4	1	4	3	2	1	4
5	4	1	4	3	2	2	3	3	2	3	2	4	3	3	2	4	3	3	2
5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4
5	4	1	4	1	0	1	4	4	3	1	4	5	4	1	4	4	3	1	4
5	4	1	4	5	4	1	4	4	3	3	2	3	2	3	2	2	1	1	4
5	4	3	2	5	4	2	3	3	2	3	2	4	3	3	2	3	2	2	3
5	4	1	4	5	4	3	2	3	2	4	1	4	3	1	4	4	3	3	2
5	4	1	4	4	3	1	4	3	2	2	3	4	3	4	1	4	3	2	3
5	4	1	4	5	4	3	2	5	4	5	0	5	4	1	4	5	4	1	4
5	4	1	4	5	4	1	4	4	3	3	2	5	4	1	4	3	2	4	1
5	4	1	4	5	4	1	4	5	4	2	3	5	4	1	4	5	4	1	4
5	4	1	4	5	4	1	4	4	3	2	3	5	4	1	4	3	2	1	4
5	4	4	1	3	2	3	2	4	3	3	2	5	4	3	2	5	4	1	4
5	4	1	4	5	4	1	4	3	2	2	3	4	3	1	4	5	4	1	4
5	4	3	2	5	4	1	4	3	2	3	2	5	4	3	2	4	3	2	3
5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4	5	4	1	4
5	4	2	3	4	3	1	4	3	2	3	2	5	4	3	2	5	4	1	4
5	4	3	2	4	3	2	3	3	2	2	3	4	3	2	3	4	3	1	4
5	4	4	1	5	4	1	4	4	3	2	3	5	4	4	1	5	4	1	4
5	4	1	4	5	4	1	4	2	1	1	4	5	4	1	4	5	4	1	4
5	4	5	0	1	0	1	4	1	0	1	4	1	0	1	4	3	2	2	3
5	4	4	1	4	3	1	4	4	3	1	4	4	3	1	4	5	4	5	0
	160		**111**		**123**		**146**		**104**		**104**		**137**		**120**		**125**		**140**
Total Soma		**vezes 2,5**				**Valor Médio**													
	1270			**3175**			**75,60**												