Proposta de Identificação dos Usuários Wireless em Cumprimento com a Lei do Marco Civil: o caso da Universidade do Estado do Pará – Campus XX

Ramon Pinheiro da Silva[1], Mario Afonso Gomes da Silva[1], Manoel Fernandes Casimiro Damasceno Costa[1], Carlos Benedito Barreiros Gutierrez[1]

[1]Centro de Ciências Naturais e Tecnologia – Universidade do Estado do Pará (UEPA)
CEP 68745-000 – Castanhal – PA – Brazil

{ramonpinheiro04, marioafonsodasilva, casimiro980, cbbgutierrez}@gmail.com

Abstract. *UEPA - Campus XX is included in Brazilians Civil Rights Framework for the Internet as an Autonomous System Administrator, but it lacks a method of storing Internet access and Internet Applications' registries, required by law. This study aims to present a solution to identify users and to store logs of connections using FreeRadius, MySQL and Syslog-NG systems to fit in the law requirements. It was used Laravel PHP framework to develop a user and logs management application. The conclusion was that the goals were accomplished.*

Resumo. *A UEPA - Campus XX enquadra-se no Marco Civil da Internet enquanto Administrador de Sistema Autônomo, mas não possui método para manter registros de conexões à Internet e de acesso a aplicações de Internet, deveres exigidos nessa lei. Este estudo visa apresentar uma solução para identificar usuários e armazenar logs das conexões empregando os sistemas FreeRadius, MySQL e Syslog-NG para atender às obrigações requisitadas. Utilizou-se o framework PHP Laravel para desenvolver uma aplicação de gestão dos usuários e de relatórios dos logs gerados. Constatou-se o cumprimento dos objetivos deste trabalho.*

1. Introdução

Segundo Jindal and Singh (2017), a utilização de redes locais de transmissão de dados sem fio, padrão IEEE 802.11 b/g/n ou Wi-Fi (WLAN), vem tomando proporções cada vez maiores em diferentes ambientes, como no uso doméstico, empresarial, para setores de pesquisa, no uso militar, entre outros, especialmente pelo rápido crescimento na utilização de dispositivos móveis. O maior benefício dessa tecnologia de rede e um fator popularizante é o fato de que os usuários a acessam sem o uso de cabos de rede, havendo autonomia quanto à mobilidade do host, eliminando a necessidade de se planejar a infraestrutura de cabeamento da rede e dos respectivos dispositivos que a acessam, diminuindo a complexidade e o custo da sua implantação [Waliullah, Moniruzzaman and Rahman 2015].

Instituições de Ensino Superior (IES) vêm adotando essa tecnologia para facilitar e melhorar o ambiente para estudos e pesquisas, porém, há o risco de ocorrerem ações ilícitas por meio dessas conexões.

Para Castilho and Fonte (2013), é de grande importância disponibilizar esses recursos, havendo uma extrema necessidade de sigilo das informações transitadas que são

passíveis de uma grande variedade de ameaças, por isso, o zelo pela integridade e a definição de políticas de segurança para esses ativos são primordiais. De acordo com Figueiredo (2016), a demanda por redes Wi-Fi em IES é significativa, sendo de suma importância resguardar os ativos destas, pois as informações transportadas são sensíveis tanto à comunidade acadêmica quanto aos sistemas dessas instituições.

Em relação a esse constante crescimento no uso dessas redes em IES, somado à facilidade e ao anonimato nesse acesso, Moretti and Bellezi (2014) apontam o aumento do risco de crimes serem cometidos nesse meio combinando-se técnicas de invasão com ferramentas já conhecidas e o desenvolvimento de novas ferramentas. Muitos ataques às redes wireless são causados por pessoas sem sentimento de culpa, pois elas agem em ambiente "online" como nunca agiriam "off-line", isto é, na "vida real" [Gonçalves 2014]. Assim, a criminalidade digital se tornou uma ameaça no uso de redes Wi-Fi.

O campus XX da Universidade do Estado do Pará (UEPA), localizado no município de Castanhal, Pará, Brasil, disponibiliza acesso à Internet por meio de uma rede Wi-Fi para o público geral, alunos, funcionários e visitantes. Para utilizá-la, basta autenticar-se por meio da senha correspondente ao respectivo Service Set Identifier (SSID) da rede. Essa senha é disponibilizada em quadros de avisos em espaços de livre acesso do campus, assim sendo, qualquer pessoa pode acessar a rede.

Esse fato gera um cenário de insegurança, pois, segundo Noh, Kim and Cho (2018), descarta-se qualquer proteção advinda da criptografia utilizada na sua senha de acesso à rede Wi-Fi ao divulgá-la indiscriminadamente. Nesse caso, é possível interceptar toda transmissão na rede através de métodos e ferramentas tais como os ataques Man-In-The-Middle, De-Authentication e De-Association, Key-Recovery, Denial-Of-Service, entre outros, apontam Waliullah, Moniruzzaman and Rahman (2015), além de possibilitar o acesso ilegítimo a chaves restritas bem como facilitar a invasão da privacidade dos usuários da rede, pondo em cheque informações sensíveis contidas nas conexões [Noh, Kim and Cho 2018].

Essa fragilidade das redes wireless se dá pela própria natureza de broadcast dessa tecnologia, pois todos os dispositivos próximos na mesma faixa de frequência a enxergam, o que não ocorre em redes cabeadas onde os dispositivos devem estar interligados via cabos de rede. Assim, as camadas da tecnologia Wi-Fi que incrementam o conjunto de vulnerabilidades é a Física e a MAC, pois, em ambas, basta que o host malicioso entre na área da rede para "farejar" as transmissões ou adquirir acesso ilegítimo com a clonagem de endereços MAC [Zou *et al.* 2016].

Além do exposto acima sobre as vulnerabilidades próprias da tecnologia Wi-Fi, há outro fator preocupante à UEPA, que é a legislação brasileira vigente sobre crimes cometidos na Internet, sendo inevitável atendê-lo para minimizar ou evitar complicações legais e possíveis punições à instituição.

A principal regulamentação que estabelece os direitos e deveres ao uso da Internet no Brasil é a lei nº 12.965/14, conhecida como o Marco Civil da Internet (MCI). Essa lei exige a manutenção dos registros de conexões à Internet e dos registros de acesso a aplicações de Internet em seus artigos 13 e 22, que devem ser mantidos pelos provedores de acesso a conexão. Esses registros devem permanecer armazenados pelo prazo de um ano, prorrogável por 60 dias. [Brasil 2017]

Ainda segundo o MCI, em seu art. 10, a preservação da intimidade, da vida privada, da honra e da imagem dos envolvidos na provisão de conexão e de aplicações de Internet devem ser atendidas na guarda e disponibilização dos registros. Caso cometa-se um crime com uso da Internet, de acordo com o art. 23 do MCI, garantir o sigilo das informações e preservar a privacidade é dever do juiz encarregado após a disponibilização dos dados decorrente de requisição judicial.

Ao consultar por Número de Sistema Autônomo (ASN) através da Interface de Programação de Aplicações (API) do site IPINFO.IO, consta que a UEPA possui um ASN com o domínio UEPA.BR. Verifica-se em Ipinfo (2018) que essa identificação é atribuída a Provedores de Serviços de Internet (ISP) e organizações que controlam blocos de endereços de Internet Protocol (IP). Com isso, constata-se que a UEPA se enquadra na lei supracitada enquanto um Administrador de Sistema Autônomo que concede acesso à Internet, conforme o inciso IV do art. 5º do MCI.

Essa lei (artigos 24 e 25 – que tratam da atuação estatal na promoção da Internet e aplicações de Internet) prevê a adoção de tecnologias abertas e livres e foca a acessibilidade a todos os interessados, que devem ser atendidos independentemente de capacidade físico-motora, perceptiva, sensorial, entre outras, além da compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações. [Brasil 2017]

O não cumprimento dessas diretrizes pode resultar desde advertências e multas até a suspensão temporária das atividades ou proibição de exercício das atividades. Assim, o cumprimento do exposto acima não é um fator trivial na disponibilização de conexões à Internet no Brasil.

Levando em consideração a prevenção de incidentes quanto ao uso de redes Wi-Fi e o exposto sobre o MCI, há o problema de que a UEPA não realiza a identificação dos usuários nem armazena os registros das conexões à sua rede. Caso ocorra um ato ilícito, não há como garantir informações detalhadas sobre esse ato e o usuário autor a serem disponibilizadas às autoridades competentes para aplicação das medidas cabíveis.

Tendo conhecimento sobre essa falta de segurança e os possíveis empecilhos legais que surgem, é indispensável que haja uma maneira de identificar os usuários e suas ações individualmente, garantindo essas informações pelo prazo determinado de forma segura, íntegra e confiável. Nesse contexto, este estudo tem por objetivo atender aos critérios dos artigos 13 e 22 do MCI, propondo uma solução para o registro e identificação dos usuários, bem como o armazenamento de logs das conexões da rede Wi-Fi da UEPA. Por outro lado, não se pretende solucionar vulnerabilidades da rede Wi-Fi do campus, nem apresentar contramedidas a possíveis ataques e/ou invasões.

2. Materiais e Métodos

Para atingir o objetivo geral deste estudo, foram listados três objetivos específicos: definição da infraestrutura de rede utilizada na instituição, criação de ambiente de rede virtual para aplicação da solução desenvolvida e desenvolvimento de aplicação web de gerenciamento.

Uma análise prévia da infraestrutura de rede Wi-Fi do campus XX foi realizada no setor de Tecnologia da Informação (TI) do campus. A partir da análise das informações obtidas e de pesquisas na literatura, chegou-se na definição da proposta de identificação

dos usuários da rede Wi-Fi que se segue. Utilizou-se ambiente virtualizado para simular a solução desenvolvida configurando-se sistemas de roteamento, controle de usuários de rede e armazenamento de logs de conexões de Internet. Além do desenvolvimento de aplicação web para gerenciamento de usuários e logs da rede.

2.1. Criação do Ambiente de Rede Virtual

Através de entrevista e aplicação de questionário, definiu-se a infraestrutura utilizada na instituição e, com essas informações, desenvolveu-se um novo cenário com recursos disponíveis para propor uma solução viável. A Fig. 1 apresenta um cenário com a utilização do recurso de virtualização de sistemas computacionais por meio do programa Oracle VM VirtualBox, versão 5.1.18.

Figura 1. Ambiente virtualizado e conexão em modo "Bridge".

Na Fig. 1, para validação da proposta, o ambiente foi adaptado para simular a topologia de rede foco deste estudo, por meio da criação de uma conexão "Bridge" e outra denominada "intnet", que representam o link de saída para a Internet (WAN – Wide Area Network) e a rede local (LAN – Local Area Network) de acesso público, respectivamente. Nesse cenário, foram implementados todos os recursos (roteador, servidores e clientes) necessários ao desenvolvimento da solução.

2.2. Instalação do Sistema Roteador Mikrotik RouterOS

A rede do campus conta com um roteador Mikrotik RouterBoard, modelo 951UI-2HND, que atua gerenciando a rede e por onde os links de Internet são conectados para serem distribuídos pelo campus. Os Pontos de Acesso (AP) à rede wireless estão fisicamente interligados na rede cabeada, por meio de cabos Ethernet par trançado CAT-5e.

Esse roteador pode ser utilizado tanto em conjunto com dispositivo dedicado fornecido pela própria Mikrotik, quanto em máquinas de terceiros, pois o importante é seu sistema operacional, o Mikrotik RouterOS. Adequando ao contexto de virtualização, foi utilizada a segunda opção e foi configurada uma máquina virtual para receber a versão 5.20 desse sistema.

A Fig. 2 apresenta o WinBox, versão 5.20, que é o software utilitário para configuração do RouterOS. Por meio desse utilitário, foram configuradas as interfaces de rede "Internet" e "Lan" no roteador, as regras para envio dos logs, e habilitados os serviços de autenticação por Radius e Hotspot no roteador, para, então, permitir acesso ao login no serviço de hotspot aos usuários.

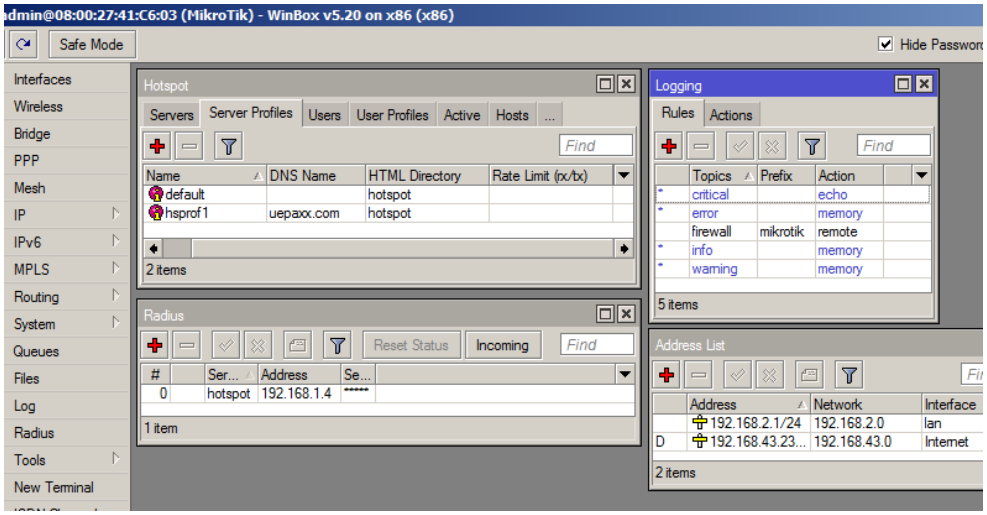

Figura 2. Configurações de interfaces, serviço de Hotspot e Logs.

2.3. Identificação dos Usuários e Logs de Acesso da Rede

Para a identificação dos usuários na rede virtualizada, foi implementado um servidor utilizando a distribuição Linux Ubuntu 14.04, que trabalha em conjunto com o roteador e recebe os parâmetros de Login, para autenticar e registrar a sessão de cada usuário. Esse servidor utiliza o protocolo RADIUS, IETF/RFC 2865, com sistema gratuito e de código aberto chamado FreeRadius, versão 2.1.12.

Para que acontecesse a troca de mensagens entre o roteador e o servidor, foi necessário cadastrar o servidor de Radius no Mikrotik (Fig. 2), definindo o IP da máquina e a porta usada pelo serviço, além de modificar o arquivo “clients.conf” no FreeRadius.

A Fig. 3 apresenta o arquivo “clients.conf” do FreeRadius, onde foram definidas as informações de IP fixo e senha referentes ao cliente, neste caso o roteador, que está apto a enviar solicitações e obter resposta do serviço.

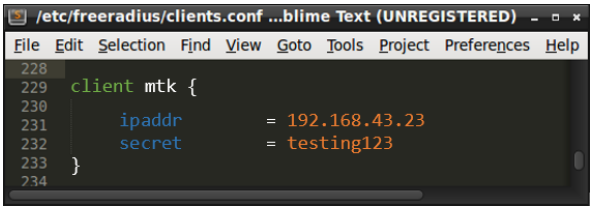

Figura 3. Alterações feitas no arquivo “clientes.conf”.

Esse sistema permite armazenar contas de usuários em uma base de dados local, e, para isso, foi integrado a um banco de dados utilizando-se o MySQL, versão 5.5.60, disponibilizado gratuitamente pela empresa Oracle. Para possibilitar essa integração, foi necessário executar o script do arquivos “admin.sql” e “schema.sql” na base de dados, além de configurar os arquivos "sql.conf" e "radiusd.conf", disponíveis nos diretórios do FreeRadius.

A Fig. 4 apresenta os scripts contidos no arquivo "admin.sql", responsáveis pela criação do banco de dados "radius" e do usuário "usuario_radius", com suas devidas permissões, ambos utilizados pelo FreeRadius.

```
# -*- text -*-
##
## admin.sql -- MySQL commands for creating the RADIUS user.
##
##      WARNING: You should change 'localhost' and 'radpass'
##               to something else.  Also update raddb/sql.conf
##               with the new RADIUS password.
##
##      $Id$
CREATE DATABASE IF NOT EXISTS 'radius';
#
#  Create default administrator for RADIUS
#
CREATE USER 'radius'@'localhost';
SET PASSWORD FOR 'radius'@'localhost' = PASSWORD('radpass');

# The server can read any table in SQL
GRANT SELECT ON radius.* TO 'radius'@'localhost';

# The server can write to the accounting and post-auth logging table.
#
#  i.e.
GRANT ALL on radius.radacct TO 'radius'@'localhost';
GRANT ALL on radius.radpostauth TO 'radius'@'localhost';
```

Figura 4: Scripts do arquivo “admin.sql”.

Na Fig. 4, são exibidos os parâmetros de configuração padrão do arquivo "admin.sql" e foram definidas outras credencias de acesso durante a execução do script neste estudo por questões de segurança.

Após criado o banco, foi necessário modificar o arquivo "sql.conf". A Fig. 5 apresenta esse arquivo e nele são cadastradas as informações referentes ao nome do banco, campo "radius_db", endereço do servidor, campo "server", porta de serviço do MySQL, campo "port" e nome de usuário e senha, campos "login" e "password", respectivamente.

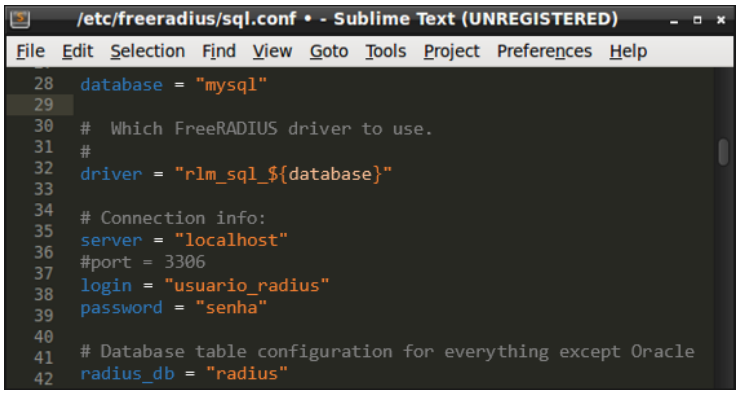

Figura 5: Configurações do arquivo “sql.conf”.

Ainda no arquivo "sql.conf", foi necessário descomentar a linha "#readclients = yes", removendo o caractere "#", para possibilitar o retorno de informações do banco aos clientes, neste caso o roteador Mikrotik.

Com o intuito de habilitar o módulo SQL no FreeRadius, foi necessário descomentar também a linha "#$INCLUDE sql.conf" do arquivo "radiusd.conf" e todas as linhas que constam "#sql" no arquivo “default”, em “sites-available” do diretório “freradius”.

Dentro do MySQL, foram executados os scripts do arquivo "schema.sql", necessários à geração das tabelas de registro de usuários e logs, utilizadas pelo FreeRadius. A Fig. 6 apresenta as tabelas que são criadas a partir dessa execução.

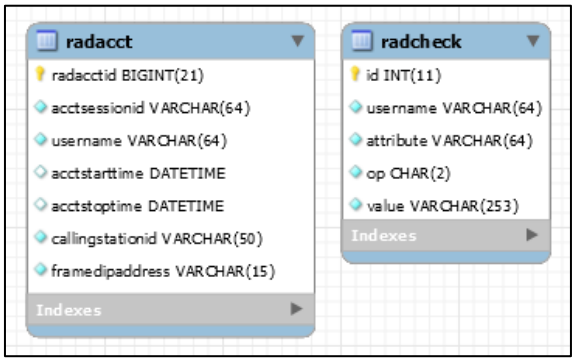

Figura 6: Tabelas usadas pelo FreeRadius.

Baseando-se na Fig. 6, no banco de dados MySQL por meio de scripts, os usuários são registrados na tabela “radcheck” e são associados aos atributos “username” e “value”, que representam o nome de usuário (login) e senha de cada utilizador da rede, respectivamente.

A tabela “radacct” registra o histórico de sessões de cada usuário. O campo “acctsessionid” armazena o identificador da sessão, o campo “username” grava o nome do usuário que iniciou a sessão, “acctstarttime” e “acctstoptime” guardam data e hora de início e fim da sessão, respectivamente; o campo “callingstationid” armazena o endereço MAC do dispositivo conectado e “framedipaddress” guarda o endereço IP atribuído ao dispositivo do usuário que se conectou à rede.

Para atender às solicitações de identificação do MCI foi criada uma tabela para registro das informações pessoais de cada usuário. A Fig. 7 apresenta essa tabela, nomeada “lan_user”.

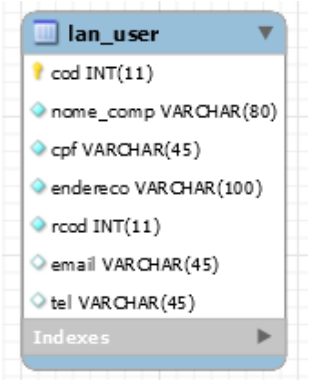

Figura 7: Estrutura da tabela “lan_user” no banco de dados.

Na Fig. 7, a tabela “lan_user” se relaciona com a tabela "radcheck" através da chave estrangeira "rcod" e permite armazenar dados como nome completo, CPF, data, telefones e e-mail para contato.

Para o cadastro dos usuários da rede, foi construída uma aplicação utilizando as tecnologias PHP, versão 5.6.36, HTML5 e Javascript. Quanto ao acesso dos usuários, o Mikrotik já dispõe de uma tela de login padrão que foi modificada para se adaptar às necessidades deste estudo. Ambas são apresentadas no tópico 3. deste artigo.

Como o campus XX utiliza o mecanismo de Network Address Translation (NAT) para compartilhar o endereço IP e garantir a conexão à Internet aos usuários, foi necessário identificar os usuários individualmente. De acordo com Tebaldi and Guardia

(2016), essa identificação se dá por meio dos endereços IP locais e portas TCP ou UDP de origem, além dos endereços IP requisitados e portas de destino de todas as conexões.

Em algum momento, dada a necessidade de levantar relatórios, esses registros podem ser cruzados com os dados das tabelas de sessão do FreeRadius, por meio dos endereços de IP, data e hora para identificação de um usuário que realizou determinado acesso.

O sistema roteador da MikroTik e o servidor FreeRadius não realizam o armazenamento dos registros de acesso à Internet, sendo assim, é indispensável o uso de outra solução para esse fim.

O sistema básico que foi utilizado para o registro de logs de acesso foi o Syslog-NG, em sua versão 3.5.3, pois é compatível com o sistema RouterOS e de código aberto. Por questões de praticidade foi instalado no servidor do FreeRadius, visto que é uma aplicação direcionada a distribuições Linux.

Para que os acessos fossem gravados, foi necessário configurar o firewall do MikroTik para que ele permitisse o redirecionamento dos pacotes para o servidor de Log (Fig. 2), além de efetuar modificações no Syslog-NG.

A Fig. 8 apresenta o arquivo "syslog-ng.conf", onde foram definidas as informações de IP do cliente, o roteador MikroTik, responsável por enviar os logs das conexões TCP e o fluxo UDP ao servidor. Também foi definido o diretório de armazenamento desses registros, definido por meio dos parâmetros ano, para a pasta, e mês e dia atuais, para o arquivo de log gerado.

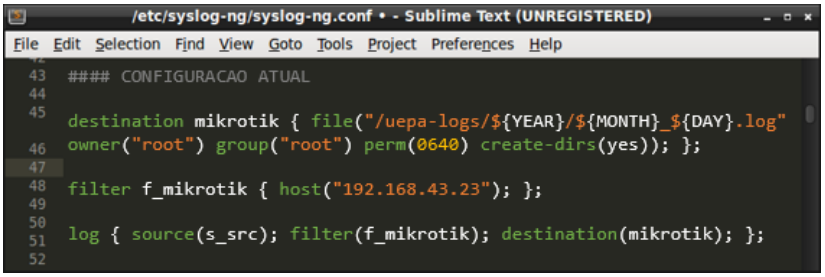

Figura 8: Configurações feitas no arquivo "syslog-ng.conf".

2.4. Aplicação de Gestão de Usuários e Relatórios

Como diferencial deste estudo, foi desenvolvida uma aplicação para ambiente web, construída utilizando o framework PHP Laravel, versão 5.4.36, que emprega a arquitetura MVC (Model View Controller) e incentiva o uso de boas práticas de Programação Orientada a Objetos (POO), em conjunto com as linguagens Javascript, HTML5 e CSS3.

Essa aplicação é responsável por gerenciar os registros recolhidos pelos sistemas FreeRadius e Syslog-NG, e a partir dessas informações emitir relatórios sobre as sessões e logs de acesso dos usuários da rede, tendo seu acesso restrito aos funcionários da instituição.

3. Resultados e Discussão

A Fig. 9 apresenta o resultado da análise junto ao corpo de TI do campus, onde foi possível compreender o design da topologia física e equipamentos da rede local da instituição.

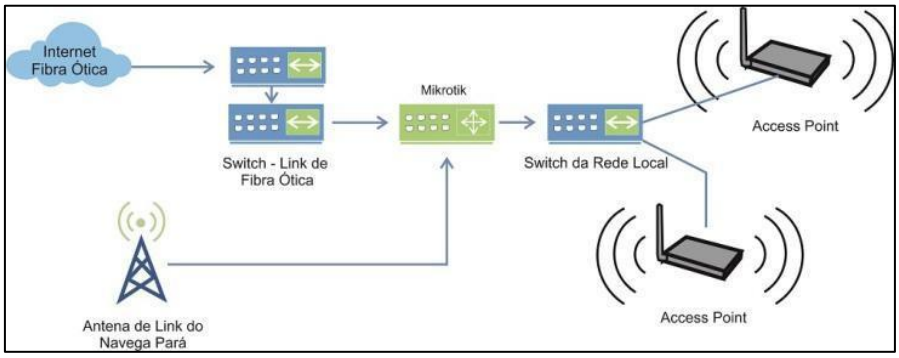

Figura 9: Topologia de Rede do Campus XX da UEPA.

Como observa-se na Fig. 9, o campus conta com um link de fibra ótica sem limitação de banda e que faz parte da rede metropolitana de castanhal. Esse link é a porta de entrada e saída de todo o tráfego da rede local, e tem sua velocidade de transmissão reduzida ao padrão ethernet de 100 Mbps ao chegar ao switch da instituição. E como link reserva, em substituição ao de fibra ótica, é utilizado um canal de rádio de 4 Mbps do programa Navega Pará, fornecido pela Empresa de Tecnologia da Informação do Estado do Pará (PRODEPA). Ambos os links são redirecionados ao Mikrotik, que distribui o sinal de Internet para todos os usuários da rede Wi-Fi da instituição em conjunto com os switches e AP locais.

Para atender as necessidades deste estudo, na estrutura de rede apresentada (Fig. 9), foi adicionada uma máquina servidora responsável pelo armazenamento dos logs e da aplicação de gestão desses arquivos. A Fig. 10 destaca a mudança ocorrida, onde é estabelecida a comunicação do servidor de logs com o roteador Mikrotik por cabo de rede ethernet.

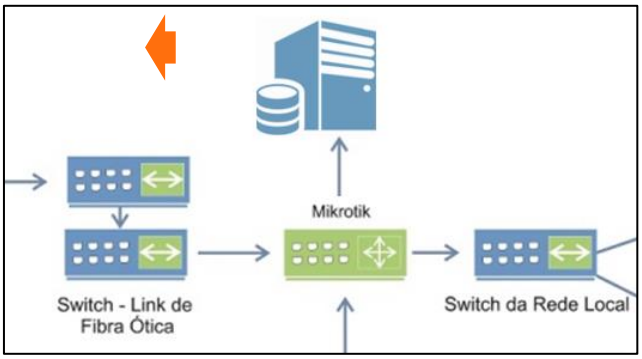

Figura 10: Topologia da rede após a integração do servidor de logs.

A Fig. 11 apresenta a tela de login que é disponibilizada pelo roteador Mikrotik para a qual o usuário é redirecionado ao conectar-se aos AP do campus. Essa página foi modificada para se adaptar à instituição e possui os campos “usuario” e “senha”, que representam as colunas da tabela “radcheck”, necessários à autenticação na rede.

Figura 11: Tela de acesso à rede pública do campus.

Por questões de segurança, para evitar o uso não autorizado dos recursos da rede, o usuário não cadastrado deverá solicitar à coordenação da instituição que o encaminhará ao setor de TI para o cadastro no banco de usuários para ter acesso à rede [Castilho and Fonte 2013].

O usuário devidamente cadastrado, ao realizar login, tem seu acesso liberado e receberá uma mensagem de boas-vindas, conforme figura 12a. Ao mesmo tempo, é aberta uma janela pop-up que possibilita ao usuário desconectar-se da rede e mostra informações relativas ao tempo e tráfego da sessão, ilustrado na figura 12b.

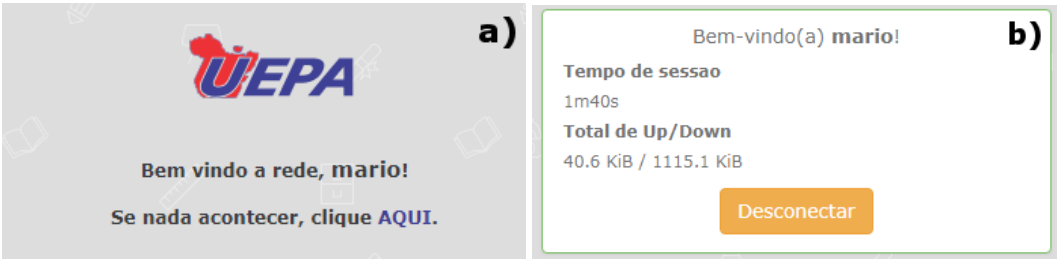

Figura 12: Telas após login.

A Fig. 13 apresenta a tela de acesso à aplicação de gestão de relatórios e usuários da rede, que é restrita aos funcionários da administração. Nessa tela há os campos “usuario” e “senha”, que são os parâmetros para acessar o sistema.

Figura 13: Tela de acesso ao sistema de gestão de usuários e relatórios.

O funcionário já cadastrado, ao realizar login, é redirecionado para a tela de gestão de usuários, conforme ilustra a figura 14. As opções apresentadas são "Cadastro de usuário" e "Usuários cadastrados".

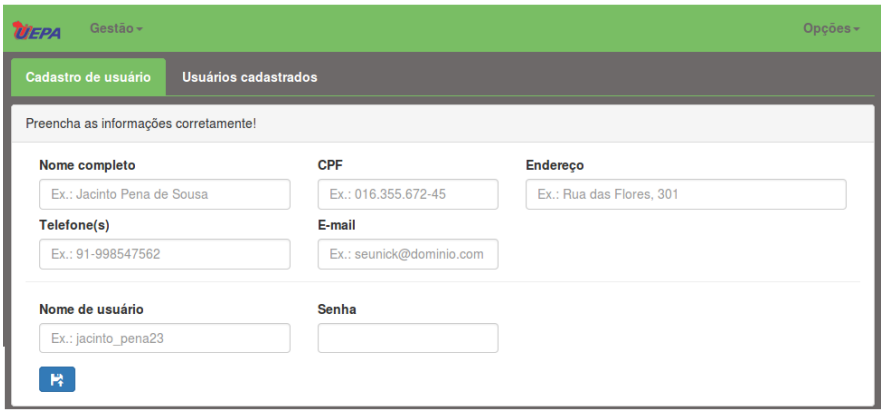

Figura 14: Tela de gestão de usuários.

Na primeira opção, "Cadastro de usuário", são exigidas informações pessoais do solicitante para criar uma conta de acesso à rede. O ato de cadastrar o usuário faz com que as informações como Nome, CPF e informações para contato sejam armazenadas na tabela “lan_user”, apresentada no tópico 2.3. deste artigo. O nome e o CPF são informações que têm validade jurídica e servem para atender ao requisito de identificação do usuário do MCI.

Já na segunda opção, “Usuários cadastrados”, é possível realizar pesquisas de usuários castrados na base de dados, com o intuito de atualizar os dados ou desativar uma conta específica.

Caso o usuário entre no menu "Gestão" e selecione a opção "Relatórios", ele será redirecionado à tela de “Relatório de sessões”, conforme a figura 15. Nessa área, por meio dos parâmetros "Data" e "Horário", é possível saber quais usuários estavam ativos na rede em um momento específico, além de dados como início e término de cada sessão, endereço MAC do usuário e IP atribuído ao seu dispositivo durante a conexão. Caso não sejam informados os parâmetros, a página retorna com todas as sessões abertas no momento da pesquisa.

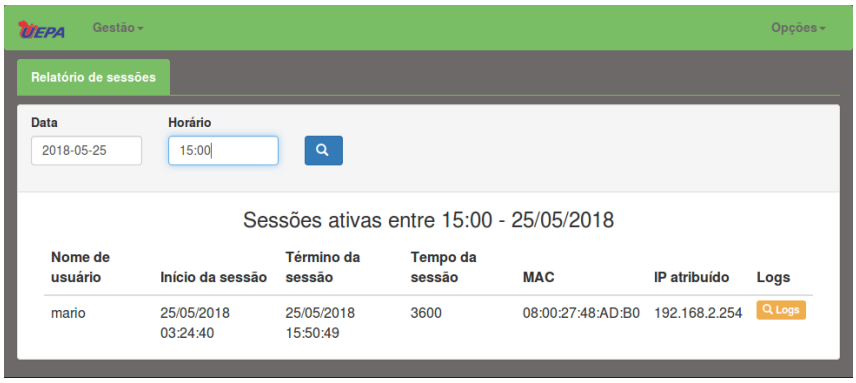

Figura 15: Tela de relatórios de sessões.

Para cada uma das sessões listadas na Fig. 15, há um ícone ao lado denominado "Logs". Ao clicar nesse ícone, uma janela é aberta e são apresentados todos os logs de acesso da sessão selecionada, apresentados na figura 16. Para isso, são cruzadas as informações de IP, data e hora dos logs com os registros de sessão (figura 15).

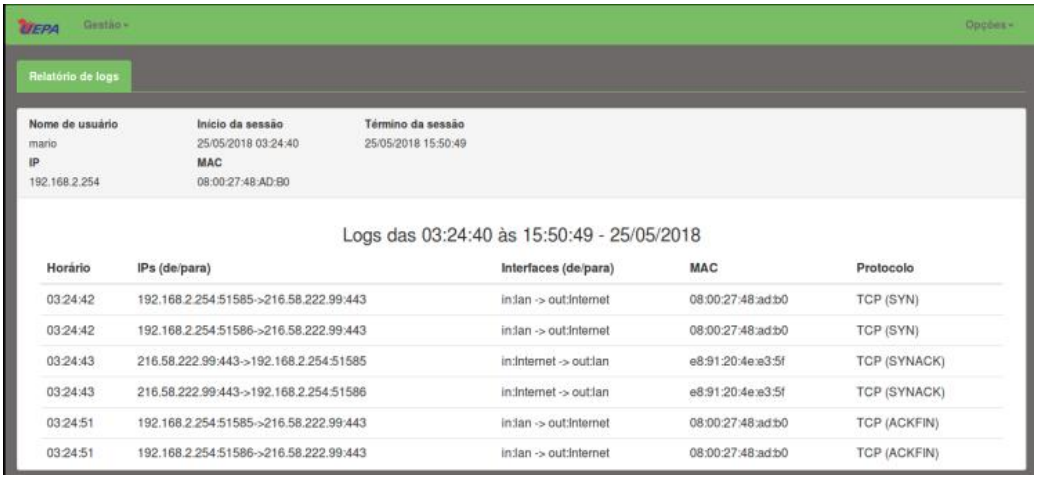

Figura 16: Tela de relatórios de Logs.

Esses logs não guardam as URLs que são acessadas pelo usuário nem qualquer outro tipo de informação que possa ferir a sua privacidade, além disso, atende ao requisito de identificação solicitado pela lei: somente é guardado o IP de origem e destino das requisições.

Verificou-se em ambiente de testes que o acesso a uma página web aumenta 4kB o tamanho do arquivo de log em média. Usando como base de cálculo 50 usuários ativos na rede, cada usuário acessando 50 páginas por dia, dentro do prazo mínimo previsto em lei, de um ano para manter os registros armazenados, o consumo em armazenamento seria de 3,6 GB, aproximadamente, desprezando o consumo acrescentado aos logs de outras tarefas e aplicações. Sendo assim, propõe-se o desenvolvimento de um método para compressão dos arquivos de log, visando otimizar o consumo de espaço em disco, além de incrementar o recurso de "Relatório de sessões" (Fig. 14) com outras possibilidades de busca, como, por exemplo, filtragem de sessões por usuário específico.

3.1. Discussão

Correlacionando este a outros estudos similares, em Carisani and Guardia (2016), objetivou-se a utilização das tecnologias de protocolo 802.1X, serviço Radius e servidor de diretórios Lightweight Directory Access Protocol (LDAP), IETF/RFC 1487, para autenticação e registro dos usuários em uma rede corporativa sem fio. Na proposta dos autores, a autenticação inicia-se a nível de porta de comunicação com os AP e utiliza como base usuários pré-cadastrados em um repositório local. Diferentemente, este estudo propõe um sistema que permite o acesso à rede por meio de portal web, exigindo como pré-requisitos estar conectado a um AP e cadastrado em base de dados SQL criada pelo FreeRadius. A solução deste estudo, além de registrar os logs das conexões da rede da instituição, armazena todos os logs de acesso à Internet feitos pelos usuários, o que não é abordado no estudo supracitado.

Kuptsov, Khurri and Gurtov (2009) apresentam um esquema de autenticação distribuída para hosts baseado em Host Indentity Protocol (HIP), IETF/RFC 4423, implementado em uma WLAN pública na cidade de Oulu, na Finlândia. Em cada AP da rede, foi configurado um firewall compatível que se comunica com um servidor de proxy HIP central. Essa abordagem possibilitou apenas o tráfego de clientes pré-estabelecidos em uma lista de controle de acesso Host Indentity Tag (HIT) compartilhada e sincronizada entre os firewalls, além de prover autenticação, garantindo por meio do IP Security

Protocol (IPSec) um canal de comunicação seguro com os usuários. A autenticação na rede se dá de forma automática e transparente ao usuário, sem interação manual, e não são apresentados mecanismos para registro do histórico de logs de conexão e acesso dos clientes, o que distingue deste estudo, pois não possibilita a verificação de cada acesso à rede.

No estudo de Farias and Sales (2016), apresenta-se um mecanismo para rastreabilidade dos acessos na rede do Campus XX da UEPA. Nessa proposta, é utilizado um banco de dados SQL contendo as credenciais de cada cliente apto a acessar a rede para a autenticação dos usuários. Além disso, são registradas todas as sessões iniciadas, porém não se armazenam registros das conexões à Internet de cada usuário como é requisitado no MCI e abordado no presente estudo.

Este estudo desenvolveu uma aplicação exclusiva para gestão dos usuários e de relatórios dos logs das conexões à rede, o que o diferencia dos estudos correlatos apresentados.

4. Conclusão

O sistema proposto garantiu o cumprimento dos artigos 13 e 22 do MCI, desta forma, atingindo o objetivo proposto pelo estudo. Quanto ao art. 13, o sistema garante a manutenção de logs dos registros das conexões da rede Wi-Fi da UEPA para o prazo mínimo de um ano, além de não transferir a responsabilidade pela manutenção desses registros a terceiros, a solução é mantida pelo setor de TI da própria instituição. No que concerne ainda ao artigo 13, os registros de conexão podem permanecer armazenados por prazo superior a um ano, possibilitando atendimento de requisição judicial. O sistema proposto pelo estudo também atende ao art. 22 quanto ao fornecimento dos registros de acesso a aplicações de internet das respectivas conexões, os quais podem ser garantidos por soluções em nível de software. Além disso, esse sistema possui um diferencial relevante que é o módulo de gestão dos usuários e logs da rede acessível a funcionários autorizados pela instituição, facilitando a verificação e disponibilização desses registros em relatórios. Almeja-se que com a implementação do sistema de autenticação e registro de logs de conexões e acessos, os usuários da rede Wi-Fi da instituição passem a ter conscientização sobre os riscos decorrentes do uso inadequado da rede, o que leva a uma mudança positiva de comportamento quanto ao uso dos recursos da rede do campus, possibilitando a geração de benefício mútuo, pois com a adoção dessa nova política de segurança, a UEPA passa a não ser alvo constante e totalmente conivente com ações maliciosas e os usuários passam a ser mais responsáveis em seus acessos.

Referências

Brasil. Lei n° 12.965/2014 de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Access Date: 11 ago. 2017.

Carisani, Rafael Vicente; Guardia, Helio Crestana. Identificação dos Usuários em Rede Corporativa. Revista TIS, v. 4, n. 2, 2016.

Castilho, Sérgio Duque; FONTE, Miguel Feitoza da. Política de segurança da informação aplicada em uma instituição de ensino mediante análise de Risco. RETEC-Revista de Tecnologias, v. 5, n. 2, 2013.

Farias, Ana Paula Pereira; Sales, Luiz Augusto Viana. Implementação de Métodos de Rastreabilidade e Controle de Acesso à Rede Interna da UEPA - Campus XX de Castanhal. 2016. Trabalho de conclusão de curso - Universidade do Estado do Pará (UEPA), Castanhal, 2016.

Figueiredo, Davis Anderson. Análise de vulnerabilidades e ameaças presentes em redes Wi-Fi (IEEE 802.11) de instituições de ensino superior de Minas Gerais. 2016. 126. Dissertação (Mestrado Profissional em Sistemas de Informação e Gestão do Conhecimento) – Universidade FUMEC Faculdade De Ciências Empresariais.

Gonçalves, Wilson José (organizador). Termos Técnicos Fundamentais – teoria e prática. Campo Grande - MS: UFMS, 2014.

Ipinfo.Io. Network Universidade do Estado do Pará. Disponível em: <https://ipinfo.io/AS262533>. Access Date: 16/06/2018. 2018.

Jindal, Poonam; Singh, Brahmjit. Quantitative analysis of the security performance in wireless LANs. Journal of King Saud University-Computer and Information Sciences, v. 29, n. 3, p. 246-268, 2017.

Kuptsov, Dmitriy; Khurri, Andrey; Gurtov, Andrei. Distributed user authentication in Wireless LANs. In: World of Wireless, Mobile and Multimedia Networks & Workshops, 2009. WoWMoM 2009. IEEE International Symposium on a. IEEE, 2009. p. 1-9.

Moretti, Cleber; Bellezi, Marcos Augusto. Segurança em Redes Sem Fio 802.11. Revista TIS, v. 3, n. 1, 2014.

Noh, Jaewon; Kim, Jeehyeong; Cho, Sunghyun. Secure Authentication and Four-Way Handshake Scheme for Protected Individual Communication in Public Wi-Fi Networks. IEEE Access, v. 6, p. 16539-16548, 2018.

Tebaldi, Lucas; Guardia, Helio Crestana. Serviço de autenticação, identificação e registro de usuários para redes sem fio públicas usando infraestrutura em nuvem. Revista TIS, v. 4, n. 2, 2016.

Waliullah, Md; Moniruzzaman, A. B. M.; Rahman, Md Sadekur. An Experimental Study Analysis of Security Attacks at IEEE 802. 11 Wireless Local Area Network. International Journal of Future Generation Communication and Networking, v. 8, n. 1, p. 9-18, 2015.

Zou, Yulong; Zhu, Jia; Wang, Xianbin; Hanzo, Lajos. A survey on wireless security: Technical challenges, recent advances, and future trends. Proceedings of the IEEE, v. 104, n. 9, p. 1727-1765, 2016.