Gerenciamento de uma rede pública utilizando a ferramenta Hotspot do Sistema Operacional RouterOS

Guilherme Levy[1], Antônio Marcos Zampier[1]

[1]Tecnologia em Análise e Desenvolvimento de Sistemas - Faculdade Guairacá

guilhermelevy@hotmail.com, amzampier@ig.com.br

Abstract. *The article presents information components and methods required for setting up a network to use the RouterOS operating system Mikrotik company, detailing concepts like Firewall and Web Proxy and further demonstrating the configuration and implementation of the Hotspot tool in an academic public, in order to obtain and manage more control band of users, improving effectively blocking traffic and hits that do not have network authentication.*

Resumo. *O artigo apresenta informações de componentes e métodos necessários para configuração de uma rede ao utilizar o sistema Operacional RouterOS da empresa Mikrotik, detalhando conceitos como Firewall e Web Proxy e na sequência demonstrando a configuração e implementação da ferramenta Hotspot em uma rede pública acadêmica, com o objetivo de obter e gerenciar um maior controle de banda dos usuários, melhorando o tráfego de forma eficaz e bloqueando acessos não autorizados à rede.*

1. Introdução

A Internet é utilizada atualmente em muitos segmentos de um ambiente corporativo, sendo que seu uso torna-se quase indispensável para que uma empresa sobreviva em meio a constantes mudanças.

A competitividade entre as empresas possui um nível alto e manter serviços de qualidade é preciso. Possuir um serviço que atenda às necessidades do público é algo imprescindível para o seu status. Nesse projeto foi identificado a necessidade de aumento da qualidade nos quesitos de velocidade e tráfego da Internet em um ambiente público acadêmico, de modo a garantir aos usuários da instituição um serviço amplo e com qualidade.

Assim foi realizada uma proposta de implementação de um servidor *Hotspot* no ambiente público acadêmico, aplicando políticas de segurança como *Firewall* e *Web Proxy*, autenticação por usuário para melhorar o controle de banda e tráfego de usuários, efetuando o bloqueio dos utilizadores que não se autenticarem na rede acadêmica, mostrando quais as vantagens de se utilizar um sistema de *Hotspot* dentro desse mesmo ambiente.

2. Fundamentação teórica

Na sociedade contemporânea a utilização das redes de computadores e a Internet são imprescindíveis para quase todos os ramos que utilizam os sistemas de informação. Kurose e Ross (2003) citam que a Internet pública é basicamente uma rede de computadores em escala mundial, ou seja, ela é responsável por conectar milhões de equipamentos, desde computadores pessoais, servidores, dispositivos móveis e até Web Tv's em todo o planeta. As redes de computadores de acordo com Pinheiro (2003) foram criadas a partir da necessidade de compartilhar recursos da informação e computacionais, como impressoras e arquivos nas empresas e um dos primeiros sistemas utilizados com o auxílio das redes de computadores foi em 1964 para reservas de passagens aéreas.

De acordo com Rainer e Cegielski (2011) a Internet opera através da distância, tempo e línguas diferentes, por meio de um ambiente multi-conectado, permitindo que as pessoas compartilhem e acessem informações de forma mais dinâmica e com vários processos. O'Brien (2006) informa que o uso da internet traz eficiência aos negócios das empresas, fazendo com que ela possa alcançar sucesso em um mundo globalizado, seja no ramo de produtos e serviços, atendimento ao cliente ou outro setor que sempre esteja em mudança devido as novas tecnologias.

Tanembaum (2003) explica que uma rede de computadores associada à Internet tem várias funções para um segmento, como por exemplo ser um meio de comunicação eficaz entre os funcionários de uma empresa, utilizando recursos como o correio eletrônico (*e-mail*), podendo ser um facilitador em negócios eletrônicos com outras empresas, fornecedores e clientes tornando mais eficiente a realização da compra ou venda de suprimentos. Complementando Primak (2009) explica que a partir da aliança entre equipamentos de informática e a Internet, melhorou a agilidade e praticidade ao acessar informações e no gerenciamento nos bens intangíveis de uma empresa, com o principal objetivo de dinamizar processos que antes eram burocráticos e que demandavam um maior tempo e pessoas envolvidas.

Tanembaum (2003) explana sobre pequenas e médias empresas que podem ter mais de uma filial inclusive em outras localidades ou países, e que a Internet possibilita uma comunicação imediata para resolução de problemas, facilitando o acesso a informações disponibilizadas em modo *on-line* como extratos financeiros, averiguação de impostos e estoques entre outros, independente de sua disposição geográfica. Comer (2009) cita que a ligação entre os computadores é usada em cada área do negócio, seja na propaganda, na produção ou transporte de produtos até seu uso final como o faturamento e contabilidade.

Magdalena e Costa (2003) cita que a inserção de novas tecnologias de informação e comunicação no ambiente escolar aumentam os processos de produção de redes, pessoais e coletivas, dando oportunidade à criação de rotas alternativas e criativas entre os pontos conectados. Essa rede de usuários conectados proporciona a superação das barreiras disciplinares e das hierarquias de conteúdo.

A Internet tem oferecido um grande suporte ao ensino e educação, pois conforme Costa (2007) a quantidade de informações disponibilizadas em milhares de sites são imensas e podem ter várias finalidades como acesso a sites de empresas com produtos e serviços, conteúdo jornalístico com assuntos diversificados como política,

economia, trabalhos acadêmicos, empregos, esportes. Kampff (20096) cita também ambientes virtuais de aprendizagem, assim como o Portal *Moodle* e o Portal AVA, que com o apoio da Internet proporciona grande flexibilidade de horários para acessar, inserir, ler ou retirar materiais tornando esse sistema um grande aliado da educação independente da localização geográfica, transpondo barreiras de tempo e espaço, e Kalinke (2003) ainda destaca um maior desenvolvimento individual pois as possibilidades de interação que a Internet proporciona são muitas, e permite ao aluno definir qual o melhor método para a sua aprendizagem em um mesmo assunto, podendo utilizar vídeos, imagens, textos ou outros subsídios chegando a um resultado comum.

Além da Internet que se expandiu com o desenvolvimento das redes de computadores, houve também os Sistemas de Informação que se expandiram, como dito por Olifer e Olifer (2008)os sistemas de informação só foram disponibilizados por que houve uma união entre as redes de computadores e as telecomunicações, e segundo Audy, Andrade e Cidral (2005) foram utilizados como mecanismos para deixar esses sistemas mais robustos, por que as tecnologias empregadas trouxeram mais agilidade e melhor competência ao manipular uma informação, dando a ela uma melhor confiabilidade ao disponibilizá-la pela Internet ou outro meio de comunicação.

Boghi e Shitsuka (2007) descrevem alguns tipos de Sistemas de Informação utilizados em diversas empresas como o Sistema de Controle de Processos, Sistema de Automação de Escritórios com a ideia principal de automatizar tarefas administrativas rotineiras com o objetivo de agilizar a produtividade no escritório e outros Sistemas de Apoio à Decisão, Orientado para Executivos ou Desempenho, Inteligência Artificial e Sistemas de Comunicação e Apoio ao Ensino. Ainda Boghi e Shitsuka (2007) descrevem os Sistemas de Apoio ao Ensino como sendo um auxílio ao treinamento de funcionários e alunos como o objetivo fortalecer o conhecimento usando sistemas *e-learning* como uma solução relativamente barata de ensino e que possa ser acessado em qualquer local que possua conexão com a Internet. Complementando Comer (2009) elucida que instituições de ensino têm, em todos os níveis de conhecimento, do ensino básico até a graduação, fornecido aos estudantes e professores acesso imediato a informações em bibliotecas *on-line* para os estudantes facilitando o aprendizado.

Com o aumento da utilização da Internet em ambientes acadêmicos necessita-se de um modo de facilitar a disponibilização da conectividade, para um controle mais amplo da rede que será disponibilizada podemos utilizar o *RouterOS* como servidor de rede, segundo a documentação oficial do site wiki.mikrotik.com (2015) o *RouterOS* é um sistema operacional *stand-alone* baseado no *Kernel Linux* v.3.3.5, instalado em um microcomputador ou rodando em uma *Routerboard* ele transforma-se em um poderoso servidor de rede com várias ferramentas, tais como servidor DHCP, cliente DHCP, Hotspot, limitador de banda, Firewall, *Web Proxy*, VPN, entre outros. Segundo Primak (2015) um servidor de rede é um equipamento cuja função primária é servir e controlar a rede a partir de regras, que são as informações de configuração que lhe são atribuídas.

Tsuji e Watanabe (2000) explicam que o DHCP é um serviço que fornece automaticamente endereços de IP de uma faixa de endereços previamente configurada pelo administrador da rede. Quando o DHCP é utilizado em uma rede de computadores ele determina um endereço de IP dinamicamente a um microcomputador ou dispositivo móvel baseado nas regras prévias implementadas no servidor de rede.

Em um ambiente acadêmico em que são vários acessos simultâneos por parte dos utilizadores, é necessário um administrador de redes estar atento a todas as situações que podem causar riscos ou acessos indesejados aos arquivos dos utilizadores. Torres (2010) cita algumas situações que as empresas estão expostas como o acesso físico ou lógico de pessoas não autorizadas a lugares restritos, a obtenção de senhas de usuários e até mesmo os locais onde equipamentos físicos estão alojados. Portanto é necessário utilizar sistemas de segurança eficazes como servidores de *Firewall*, *Web Proxy* e sistemas de autenticação de usuários para tentar evitar esses problemas. Nakamura e De Geus (2007) explica que as falhas na segurança de um sistema trazem prejuízos ao seu desempenho, os problemas podem surgir devido a dois fatores: erro na criação das regras ou erro na implementação dessas regras.

Comer (2009) conceitua *Firewall* com uma barreira entre a rede de computadores de uma empresa e a Internet, reforçando as políticas internas de segurança da corporação. Primak (2015) descreve *Firewall* como um dispositivo que tem a finalidade de estabelecer uma política de segurança eficiente em uma rede de computadores. Neto (2004) explana que o *Firewall* tem como uma de suas funções, avaliar os cabeçalhos, desviar o pacote do destino e destruir ou liberá-lo para tráfego até o destino inicial, baseando-se nas regras previamente implementadas. Carvalho (2005) descreve como *Firewalls* híbridos, o uso dos recursos de filtro de pacotes em conjunto com *proxies* para proporcionar um melhor desempenho, esse tipo de *Firewall* fornece uma verificação mais completa aos serviços que necessitam de um nível de verificação maior, tal como FTP.

O *Firewall* configurado no *RouterOS* foi utilizado como método de proteção do sistema por estar sujeito aos riscos da rede externa, entretanto após o *Firewall* efetuar o tratamento dos pacotes é necessário algum método que auxilie na filtragem dos dados que possam causar danos ao funcionamento do sistema, nesse caso o *Web Proxy*. Carmona (2006) explica que o *Web Proxy* serve como um filtro de conteúdo, em que o administrador da rede define o que pode ser acessado ou não pelos usuários na Internet, e o que não for autorizado será bloqueado e em seguida será apresentada uma tela com uma mensagem alertando o usuário da restrição daquele conteúdo. Ainda segundo Carmona (2006) o *Web Proxy* possui uma funcionalidade de *CacheOnDisk*, que serve para aumentar a velocidade da conexão com a internet evitando a utilização desnecessária do link, ele delimita uma área no disco rígido e armazena o conteúdo das páginas mais acessadas, impedindo assim a busca das informações repetidamente na Internet.

Forouzan (2008) complementa que o filtro de pacotes de um *Web Proxy* analisa as informações disponíveis nos cabeçalhos de transporte (IP e TCP/UDP) e nos pacotes de camadas de uma rede para determinar se há restrição nos dados requeridos pelo usuário. O modo de configuração utilizado no *RouterOS* será o transparente, como define Peterson e Davie (2004) ele analisa os pacotes que passam através dele sem que fique visível ao transmissor ou receptor em caso da liberação do conteúdo, mas no caso de bloqueio o *Web Proxy* alertará o usuário. O modo de *Web Proxy* transparente utilizado não solicita configuração específica no equipamento do usuário nem mesmo uma autenticação prévia.

Conforme Sousa (2010) o controle de acesso tem como função permitir o acesso do usuário a sistemas e aplicações somente se as credenciais dos usuários forem válidas,

a autenticação do usuário também tem como função controlar as permissões do usuário, segmentando por perfis o que ele pode e não pode acessar. Tanembaum (2009) informa que todo sistema computacional que tem a intenção de ser seguro deve determinar que o usuário faça a autenticação ao conectar-se. Forouzan (2008) explica que a autenticação do usuário irá verificar a sua identidade ou do processo que deseja se comunicar com o sistema protegido, para tal controle de acesso será utilizado a ferramenta *Hotspot* do *RouterOS*. No ambiente acadêmico utilizado nesse projeto, a autenticação se dá por usuário e senha ou usuário e endereço MAC, segundo Stalllings (2008) o controle de acesso tem como função limitar a utilização dos sistemas e aplicações baseados nos enlaces de comunicação da rede. Para isso cada dispositivo precisa ser identificado para obter acesso à rede, de modo que a liberação de acesso e conteúdo possa ser adaptada de modo diferente a cada usuário autenticado.

Nakamura e De Geus (2007) explana que para o usuário utilizar a internet de um serviço de *Hotspot* ele precisa iniciar seu equipamento sem fio com um adaptador *wireless* para acessar a rede, esse acesso ainda depende de como os equipamentos e servidores estão configurados.

Conforme especifica a documentação oficial do site wiki.mikrotik.com (2015) o *Hostspot* do *RouterOS* disponibiliza aos usuários acesso à rede utilizando uma conexão cabeada ou *wireless*. O usuário será direcionado até a uma tela de *login* onde será requerida uma credencial para a sua autenticação. Ainda conforme a documentação oficial do site wiki.mikrotik.com (2015) esse sistema é indicado para instituições de ensino, hotéis, aeroportos, cafés e outros locais que necessitem disponibilizar o acesso à internet de modo público. Esse modo de conectividade não requer do usuário nenhuma instalação de *software* adicional e nenhuma configuração de rede específica.

Complementando a documentação oficial do site wiki.mikrotik.com (2015) o *Hostspot* do *RouterOS* pode utilizar diferentes métodos de autenticação dos clientes, utilizando uma base de dados local no *RouterOS*, ou um servidor *Radius* remoto. Ainda conforme a documentação oficial do site wiki.mikrotik.com (2015) o *Hotspot* do *RouterOS* permite a criação de perfis de usuário com diferentes permissões, restrições de conteúdo, limites de banda, limite de utilização por tempo, restrições de horário, restrições de quantidade de fluxo de dados, etc.

A documentação oficial do site wiki.mikrotik.com (2015) complementa que pode ser criadas regras de *Bypassed*, ou seja, tirando a obrigatoriedade de preenchimento de credencias de usuários previamente configurados, o *RouterOS* disponibiliza também a função *Walled Garden*, que libera o acesso a sites previamente especificados pelo administrador mesmo sem a autenticação no *Hotspot*. No *Hotspot* do *RouterOS* pode ainda serem criadas contas de acesso *Trial*, que permite ao usuário ter uma conexão por um período de testes à rede por um tempo previamente determinado pelo administrador da rede.

Em nosso projeto, a implementação de um *Hotspot* está atrelada à distribuição do sinal de rede utilizando pontos de acesso *wireless* (AP), conforme define Nakamura e De Geus (2007) AP (*Access Point*) são dispositivos que fornecem conectividade a microcomputadores e dispositivos móveis não necessitando o uso de cabeamento.

3. Materiais e Métodos

O presente projeto parte da premissa que hoje o mundo se tornou uma grande rede de pessoas e instituições que precisam estar conectadas constantemente, sob o risco de prejuízos, sejam eles financeiros, culturais, políticos, etc. O crescimento do mercado tecnológico e as facilidades de pagamento trazidas pelas empresas de venda também fizeram com que a quantidade de usuários que necessitam estar conectados constantemente aumentassem. Atrelado a esse aumento veio a necessidade de serem criados métodos com a finalidade de facilitar essa conexão do usuário à internet, independentemente da finalidade, seja ela, lazer, trabalho ou estudo.

Sabendo dessa necessidade de conexão constante, e ainda levando em consideração que essa conexão deve ter um nível de qualidade aceitável e um nível alto de segurança para que os usuários não sejam prejudicados esse projeto irá implementar uma solução de conexão internet que imponha regras e permissões de conectividade aos usuários em um ambiente acadêmico.

Anteriormente esse ambiente possuía um *link* de internet que era distribuído por roteadores wireless com uma senha única e sem nenhum critério de permissão e regras de bloqueio de usuários não autorizados, ou seja, se um acadêmico fornecesse a senha para um usuário não autorizado, esse então poderia utilizar da conexão de internet do ambiente acadêmico.

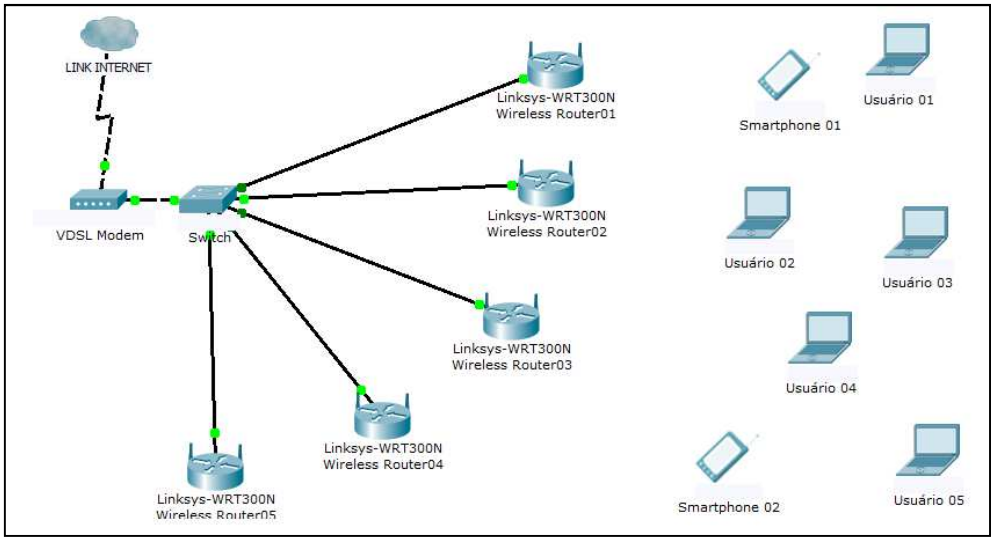

Figura 1: Representação da infraestrutura física de rede do ambiente acadêmico anterior à implantação do Hotspot. Fonte: Elaborada pelo autor

A infraestrutura anterior à implantação do novo projeto era composta por:

- 01 Modem Roteador VDSL
- 01 Switch 16 portas 10/100
- 05 Roteadores *Wireless* 52Mbps
- Computadores e *Smartphones* dos Acadêmicos

O link de internet da instituição era autenticado por um modem VDSL e enviado ao switch que fazia a distribuição do *link* aos roteadores wireless, o modem VDSL também era responsável pela distribuição dos endereços de IP através de um DHCP server configurado nele, os roteadores wireless por sua vez recebiam os endereços de IP em seu DHCP *Client* e novamente faziam a distribuição dos endereços de IP com a ajuda do DHCP *server* configurado em cada um deles individualmente, o lease time estava configurado para 24 horas, que regularmente fazia com que o DHCP *server* do roteador *wireless* travasse devido ao uso de todos os endereços de IP do *range* disponíveis.

Cada roteador tinha um SSID o que fazia com que se o acadêmico tivesse que mudar de local de estudo, ele tivesse que se desconectar do roteador onde estava e conectar no roteador mais próximo, ainda sobre os roteadores, a senha era única, o que facilitava a conexão de usuários não autorizados.

Após verificarmos os erros existentes na infraestrutura utilizada, foi buscado então uma proposta de implementação de uma infraestrutura e um sistema que unificasse os usuários em um servidor, com a seguinte proposta:

- Padronização do SSID;
- Praticidade em alterações futuras na estrutura da rede;
- Centralização de um DHCP *Server*;
- Controle de permissões e regras de acesso dos usuários à internet;
- Controle de banda dos usuários;
- Bloqueio de conteúdo através de um *Web Proxy*;

Após a proposta elaborada ser aprovada pela direção da instituição o primeiro passo foi escolher um sistema operacional robusto e confiável, capaz de suprir essas necessidades e que possuísse essas funcionalidades buscadas, esse sistema operacional também deveria possuir uma ferramenta que crie um servidor Hotspot, aplicativo essencial para o desenvolvimento do projeto.

O escolhido foi o Sistema Operacional *RouterOS* da empresa *Mikrotik*, esse sistema pode ser instalado tanto em um microcomputador baseado na arquitetura X86 como pode ser adquirido juntamente com seu *hardware* compatível que também é fabricado e fornecido pela empresa *Mikrotik*. A opção escolhida para esse caso foi a da utilização da *Routerboard*, pois a mesma já é manufaturada com as especificações necessárias para o funcionamento do *RouterOS*.

Após a escolha do sistema operacional para a base da nossa implantação precisamos efetuar a configuração da *Routerboard* para a implantação.

Inicialmente escolhemos quais interfaces da *Routerboard* serão responsáveis pelo recebimento do *uplink* da internet e a que vai ser responsável pela liberação do fluxo de dados já tratados pelo *RouterOS* para o *Switch* e consequentemente para os AP’s que fornecerão internet aos usuários cadastrados renomearemos elas de ether1 e ether5 como UpLink e OutSwitch respectivamente.

Após a padronização das interfaces nós criamos as *Adress List*, isto é, os endereços de IP que serão reconhecidos pela *Routerboard* e que poderão navegar dados

dentro dela, após a criação da *Adress List* criamos um IP POOL, que é uma faixa de endereços de IP que será disponibilizada pelo DHCP *Server* aos usuários do *Hotspot*.

Depois de criado o IP POOL podemos criar o DHCP *Server* e fazer a sua configuração, assim com a configuração da aba *Networks*, que especificará o *Gateway* para a rede criada. Na configuração do DHCP especificaremos que todo o equipamento conectado à porta OutSwitch receberá um endereço de IP e esse endereço ficará disponível para ele durante 2 horas, como configurado na opção *Leases*. Ainda na configuração do DHCP *Server* escolheremos qual será a faixa de endereços de IP que será fornecido pelo DHCP *Server*, essa opção pode ser escolhida no campo *Address Pool*.

Logo após a configuração do DHCP *Server* criaremos um DHCP *Client*, o DHCP *Client* será responsável pela recepção do *uplink* de internet, recebendo dinamicamente as configurações de um servidor DHCP externo. Desse modo, mesmo que haja uma mudança no endereço de IP do uplink de internet, seja pela troca do modem, plano ou operadora, *RouterOS* dinamicamente adotará as novas configurações do novo *uplink.*

Nesse momento a *Routerboard* podemos conectar o cabo do *uplink* à *Routerboard*, a conexão do *uplink* na *Routerboard* e o reconhecimento do *uplink* pelo DHCP *Client* faz com que a *Routerboard* esteja conectada na internet.

A próxima etapa foi a configuração do *Firewall*, para fazermos a *Routerboard* navegar precisamos configurá-lo para que a nossa rede tivesse permissão do *Firewall* para trafegar dados, com essa regra criada efetuamos a configuração do NAT da *Routerboard*, a regra de mascaramento do NAT da *Routerboard* se faz necessária para que ao sair da rede interna o usuário que navega mascare seu endereço de IP da rede local com o IP válido disponibilizado pela interface UpLink, na opção NAT também criamos a regra de redirecionamento da porta 80 (http) para a porta do nosso *Web Proxy*, que será configurado a seguir, usaremos a porta 3128 para o *Web Proxy*.

Nas configurações de *Web Proxy*, ao habilitarmos seu funcionamento precisamos também informar qual porta ele utilizará para receber os pacotes a serem tratados, também foi informado um e-mail de contato para os usuários que necessitarem. Foram criadas duas regras de bloqueio no *Web Proxy*, uma para a palavra ***4shared*** e para a palavra ***sourceforge***, assim os usuários do *Hotspot* não poderiam acessar esses sites. Foram criadas regras também para o bloqueio de conteúdo pornográfico.

Na seqüencia criamos o servidor *Hotspot* que usou essas configurações anteriores como base para seu funcionamento, esse servidor utilizou a interface OutSwitch e efetua o controle das permissões e regras de acesso à internet.

Após criarmos o servidor nós prosseguimos com a criação dos perfis de usuário, que seria utilizado depois para diferenciar usuários com uma banda maior e permissões específicas, de usuários com uma banda reduzida e bloqueios específicos. Nesse caso, foram criados usuários com autenticação utilizando senha para os administrador e diretores, e usuários que fariam a autenticação via vinculação com o endereço MAC de seu computador ou dispositivo, nesse caso o acadêmico não poderia passar suas credenciais para outro utilizador da rede não autorizado, porque o *Hostpot* faz a verificação com base em suas credenciais vinculada ao endereço MAC do microcomputador ou dispositivo.

Para usuários que ainda não são cadastrados e autorizados a utilizar a internet da instituição de ensino superior configuramos regras de *Walled Garden*, que libera o tráfego de sites específicos, escolhidos pelo administrador mesmo sem o usuário ter autenticado no sistema.

Após a configuração do *Hotspot* e cadastro dos usuários a página de acesso que aparece quando o utilizador tenta a autenticação foi padronizada para ajudá-lo, e dar uma identificação visual padronizada da instituição acadêmica.

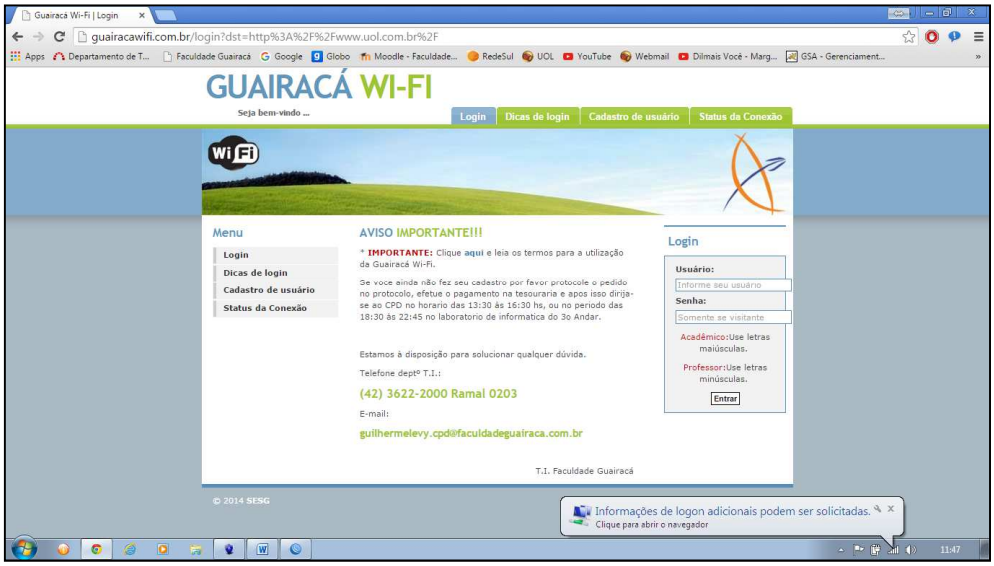

Figura 2: Tela de autenticação do *Hotspot*. Fonte: Elaborada pelo autor

Assim que as configurações acabaram, a *Routerboard* foi conectada à rede da instituição para seu funcionamento, ela foi posicionada entre o modem VDSL e o *switch* de distribuição do tráfego dos dados, no *switch* foram conectados os AP's configurados internamente como modo AP, isto é, recebem os pacotes por cabo e repassam por *wireless* sem fazer alterações, ficando sob responsabilidade do *RouterOS* o controle de DHCP *Server*, *Firewall*, *Web Proxy*, etc.

A infraestrutura da rede da instituição ficou desse modo apresentado na figura a seguir após as alterações:

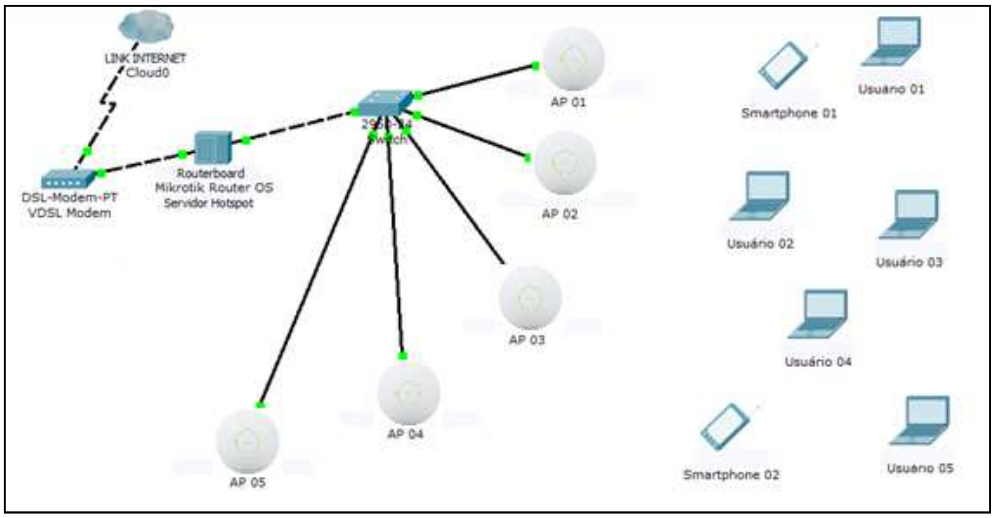

Figura 3: Representação da infraestrutura física de rede do ambiente acadêmico após a implantação do Hotspot. Fonte: Elaborada pelo autor

Devido às configurações feitas, todos os usuários que se conectam à rede *wireless* disponibilizada na instituição recebem um endereço de IP da rede local e é direcionado ao portal de autenticação para digitar suas credenciais e se corretamente digitadas, o usuário é liberado para o acesso à internet estando sujeito às regras impostas pelo *RouterOS*.

4. Resultados

A implementação do sistema operacional *RouterOS* trouxe grandes vantagens aos usuários e ao administrador da rede wireless disponibilizada aos acadêmicos da instituição de ensino superior, o administrador pôde resolver questões de segurança mais rapidamente pela facilidade da sua interface gráfica, e os usuários puderam utilizar a internet disponibilizada pela instituição de ensino com mais segurança, e com os limites de banda especificados no servidor *Hotspot* houve uma melhor administração e utilização da banda disponível, foi possível também um controle minucioso de quais usuários poderiam ou não acessar a internet.

A instalação da *Routerboard* também propiciou ao administrador uma agilidade na implementação do *Hotspot*, por se tratar de um *hardware* que já vem com o sistema operacional instalado, não dando brechas de incompatibilidade entre o *software* e o *hardware*.

O *Web Proxy* disponibilizado pelo *RouterOS* também traz uma maior segurança aos administradores, pois bloqueia o tráfego dos dados que possuam um conteúdo que seja de caráter ofensivo ou que possa burlar as diretrizes de utilização da instituição de ensino superior.

A regra de *Walled Garden* funcionou como uma propaganda para a instituição de ensino, pois foi liberado o tráfego do seu site para a navegação, mesmo a usuários que não estivessem autenticados, ou seja, visitantes ou turistas que passarem por frente da instituição e se conectarem à rede wireless podem conhecer a sua infraestrutura e cursos contidos no seu *site*.

Em suma, o projeto aumentou meu conhecimento profissional durante seu período de implementação, os resultados obtidos atenderam a proposta inicial enviada à diretoria da instituição de ensino, trazendo vantagem competitiva para a empresa.

5. Considerações Finais

Com a necessidade de crescimento profissional constante e na oportunidade de satisfazer as metas estabelecidas em um estudo, a implantação do sistema operacional *RouterOS* proporcionou a mim o aumento da minha concepção e entendimento sobre como, quando, de que modo fazer, colocando-me a frente de questões técnicas aparentemente sem solução, mas que em uma segunda vista mais detalhada fizeram com que eu criasse modos e desvios lógicos, para chegar ao final do projeto obtendo êxito.

Uma outra oportunidade que conquistei com a realização desse projeto foi a criação de um manual de configuração e implementação do *RouterOS*, que tem como principal finalidade o auxílio aos administradores de rede que possuírem dúvidas.

A melhoria constante do conhecimento continua, e os próximos passos são referentes à otimização e criação de novos processos e regras para a segurança da rede utilizada no trabalho, incluindo regras de *Firewall*, *Web Proxy*e modos diferentes de autenticação dos usuários. Serão levantadas também questões de segurança quanto a diferença de perfis de usuário na hora da conexão, que propicie ao administrador a possibilidade de efetuar o bloqueio ou liberação de uma gama de equipamentos em determinada época, como por exemplo em períodos de provas efetuar o bloqueio dos dispositivos móveis que possam facilitar fraudes ou acessos indevidos nesse momento, e após a implementação dessas novas funcionalidades a intenção é propiciar o aumento na qualidade dos serviços prestados pela instituição.

Referências bibliográficas

AUDY, Jorge L.N, ANDRADE, Gilberto K. e CIDRAL, Alexandre. Fundamentos de Sistemas de Informação. Porto Alegre RS: Bookman 2005.

BOGHI, Cláudio e SHITSUKA, Ricardo.Sistemas de Informação: Um Enfoque Dinâmico. 3º Ed. São Paulo SP: Érica 2007.

CARMONA, Tadeu. Treinamento prático em redes de computadores. São Paulo SP: Digerati Books 2006.

CARVALHO, Luciano G. Segurança de redes. Rio de Janeiro RJ: Ciência Moderna 2005

COMER, Douglas E. Redes de computadores e Internet. Porto Alegre RS: Bookman 2009.

COSTA, Gilberto C. G. Negócios Eletrônicos: uma abordagem estratégica e gerencial. Curitiba PR: Ibpex 2007.

FOROUZAN, Behrouz A. Comunicação de dados e redes de Computadores. São Paulo SP: Bookman Companhia 4º Ed. 2008.

KALINKE, Marco A. Internet na Educação. Curitiba PR: Chain 2003:

KAMPFF, Adriana J. C. Tecnologia da Informática e Comunicação na Educação. Curitiba PR: IESDE Brasil S.A 2006.

KUROSE, James F. e ROSS, Keith W. Redes de computadores e a Internet: umanova abordagem.1º Ed. São Paulo SP: Addison Wesley 2003.

MAGDALENA, Beatriz C. e COSTA, Iris E. T. Internet em sala de aula. Porto Alegre RS: Artmed 2003.

MORAES, Alexandre F. de. Segurançaem Redes Fundamentos. São Paulo SP: Érica 2010.

NAKAMURA, Emilio T. e DE GEUS, Paulo L. Segurança de redesemambientescooperativos. São Paulo SP: Novatec 2007

NETO, Urubatan. Dominando Linux Firewall Iptables. Rio de Janeiro RJ: Ciência Moderna 2004.

O'BRIEN, James A. Sistemas de informação e as decisões gerenciais na era da Internet.2º Ed. São Paulo SP: Saraiva 2006.

OLIFER, Natália e OLIFER, Victor. Redes de computadores: princípios, tecnologias e protocolos para o projeto de redes. Rio de Janeiro RJ: LTC 2008.

PETERSON, Larry L. e DAVIE, Bruce S. Redes de Computadores: uma abordagem de sistemas. Rio de Janeiro RJ: Elsevier 2004.

PINHEIRO, José M. dos S. Guia completo de cabeamento de redes. 10º Ed. Rio de Janeiro RJ: Elsevier, 2003.

PRIMAK, Fábio V. Infortabilidade – A Contabilidade na era da informática. Rio de Janeiro RJ: Ciência Moderna 2009.

PRIMAK, Fábio V. Tecnologias da Informação Aplicadas ao Direito. Rio de Janeiro RJ: Ciência Moderna 2015.

RAINER, R. Kelly Jr. e CEGIELSKI, Casey G. Introdução a Sistemas de Informação - Apoiando e transformando negóciosna era da mobilidade. 3ª Ed. Rio de Janeiro RJ: Elsevier 2011.

SOUSA, Lindeberg B. Redes de computadores guia total. São Paulo SP: Érica 2010

STALLINGS, Willian. Criptografia e segurança de redes. São Paulo SP: 4ª Ed. Pearson Prentice Hall 2008.

TANEMBAUM, Andrew S. Redes de Computadores. 4ª Ed. Rio de Janeiro RJ: Elsevier 2003.

TANEMBAUM, Andrew S. Sistemas Operacionais Modernos.3ª Ed. São Paulo SP: Pearson Prentice Hall, 2009.

TORRES, Gabriel. Redes de Computadores. Vila Isabel RJ: Novaterra 2010.

TSUJI, Hidenori e WATANABE, Takashi. Configurando um Servidor Linux. São Paulo SP: Makron Books, 2000.

MIKROTIK site Oficial. Disponível em:

http://www.mikrotik.com/pdf/what_is_routeros.pdf/>Acesso em20/09/2015 às 15h 27min.

MIKROTIK Documentation. Disponível em:

http://wiki.mikrotik.com/wiki/Main_Page />Acesso em27/09/2015 às17h 21min.