# Gerenciamento e Controle por Autenticação para Acesso à Estrutura de Rede de Computadores da Prefeitura Municipal de Palmeira das Missões – RS

**Lázaro Hahn Martins[1], Sidnei Renato Silveira[2], Fernando Beux dos Santos[3]**

[1]Curso de Bacharelado em Sistemas de Informação, [2]Departamento de Tecnologia da Informação – Universidade Federal de Santa Maria (UFSM/Campus Frederico Westphalen) – RS – Brasil
[3]Centro de Ciências Humanas e Sociais – Ciência da Computação – Universidade de Cruz Alta (UNICRUZ) Cruz Alta – RS – Brasil

lazarohahn@hotmail.com, sidneirenato.silveira@gmail.com, fernandobeux@gmail.com

**Resumo.** Este artigo apresenta um estudo de caso envolvendo a implantação de um método para controlar e gerenciar a conexão dos usuários ao acesso à estrutura de rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS (PMPM-RS). Desenvolveu-se um meio de controle e gerenciamento por autenticação, para controlar o acesso à estrutura de rede de computadores, usando métodos específicos para coletar dados da rede, visando observar a quantidade de tráfego na rede usado na PMPM-RS e, assim, restringir e registrar acessos conforme Política de Segurança e contexto da segurança de rede definindo critérios para cada perfil de usuário, conforme o seu setor, criando regras administrativas para cada usuário, em relação ao conteúdo que terá acesso.

**Palavras-Chave**: Rede de computadores; VLANs; *Hotspot*.

***Abstract.*** *This paper presents a case study of the implementation of a method to control and manage the connection of users to access the computer network structure of the Palmeira das Missões city - RS (PMPM-RS). Thus, a means of control and management for authentication will be developed to control access to the computer network structure, using specific methods to collect data from the network, aiming at observing the amount of traffic on the network used in the PMPM-RS, and thus restrict and record access as security policy and network security context of defining criteria for each user profile, according to the sector, creating administrative rules for each user, the content that will access.*

***Keywords:*** *Computer network; VLANs; Hot spot.*

## 1. Introdução

Atualmente, a utilização de ferramentas informatizadas é imprescindível em todos os setores de atividades, tais como os órgãos públicos. As organizações estão, cada vez mais, dependentes de ferramentas tecnológicas e do acesso a informações disponíveis em suas redes internas (Intranet) e na Internet. Neste sentido, gerenciar o acesso à rede e

às informações disponíveis passa a ser uma tarefa importante para garantir a segurança e integridade das informações.

A motivação para o desenvolvimento deste trabalho surgiu a partir das atividades exercidas no setor de informática na PMPM-RS (Prefeitura Municipal de Palmeira das Missões-RS) entre 2014 a 2016, onde os autores deste trabalho atuaram. Constatou-se, durante o desenvolvimento destas atividades, fragilidade na questão de segurança dos acessos dos usuários, nas pessoas que possuem acesso à rede (com a falta de identidade dos usuários em seus acessos) e, também, na quantidade de vírus que se espalham nos computadores tanto por descuido, como na questão de falta de comprometimento com o trabalho exercido nos setores. Além disso, havia necessidade em diminuir o tráfego na rede, pois a demanda de acessos a conteúdos que não fazem parte do trabalho desenvolvido pelos servidores públicos era excessiva.

Assim, considerou-se importante controlar o acesso à rede criando perfis para todos os usuários e verificar suas necessidades na navegação, elaborando um sistema para gerenciar o acesso à Internet, permitindo controlar vários recursos, tais como a velocidade que todos os usuários podem ter de *upload*, de *download*, e em que *sites* o usuário pode ou não navegar, dependendo do seu perfil.

Acredita-se que a implantação de um sistema para controlar e registrar o acesso dos usuários possibilitará uma melhor segurança e controle dos acessos e, também, maior qualidade na questão de acesso à rede e na velocidade de tráfego, diminuindo a demanda de suporte no setor de informática, responsável pelo atendimento aos usuários.

Neste contexto, o principal objetivo deste trabalho foi o de definir e implantar um método para controlar e gerenciar o acesso à estrutura de rede de computadores da PMPM-RS visando, por meio da Política de Segurança e critérios administrativos, criar perfis de controles para caracterizar formas de acesso a redes específicas, de acordo com as necessidades de cada usuário.

Para dar conta desta proposta, o artigo está estruturado da seguinte forma: na seção 2 apresenta-se um breve referencial teórico conceituando as principais áreas envolvidas no trabalho. A seção 3 apresenta alguns trabalhos relacionados, visando compor o estado da arte. A seção 4 detalha a solução implementada, definindo tecnologias e ferramentas que foram empregadas para desenvolver o sistema de controle. Encerrando o artigo são apresentadas as considerações finais e as referências empregadas.

## 2. Referencial Teórico

Esta seção apresenta um breve referencial teórico sobre conceitos, aplicação, autenticação e configuração de um sistema de gerenciamento de redes de computadores, que fornecem o embasamento necessário para o entendimento das áreas envolvidas no trabalho apresentado neste artigo.

### 2.1 Redes de Computadores

O termo “Redes de Computadores” serve para descrever um conjunto de computadores conectados por um único meio. Uma rede de computadores consiste, basicamente, em

interligar dois ou mais computadores com o objetivo de compartilhar dados. Esta conexão pode ser feita por meio de cabos, fio de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélite de comunicações. Existem vários tipos de redes, de várias formas, tamanhos e modelos. Geralmente elas estão conectadas a fim de criar redes maiores. A Internet é o exemplo mais conhecido de uma rede de computadores (TANENBAUM; WETHERALL, 2011).

Existem seis componentes básicos de uma rede de computadores, e entender esses componentes pode ser fundamental para ajudar a proteger a rede apropriada para seu uso tanto doméstico quando empresarial (HUGHES, 2013):

- **Interfaces de rede:** Todo dispositivo em uma rede deve ter alguma forma de interface, que às vezes é chamada de NIC ("*Network Interface Card*", placa de interface de rede) e pode estar integrada à placa-mãe de um computador ou separada dela. A NIC é o componente que toma a informação do computador e a envia pelo cabo de rede ou pelo ar, no caso de uma rede sem fio;

- ***Hubs:***Quando vários computadores são conectados em uma rede, eles se comunicam com um dispositivo central, chamado "*hub*". Esse componente é responsável por mover o sinal de rede de um cabo para outro. No caso de um "*hub*" básico, o sinal de um computador é enviado para todos os outros; cada NIC decide se a informação recebida é para ela, e a descarta em caso negativo;

- ***Switches:***Os *switches* são *hubs* inteligentes, pois podem criar tabelas que permitem saber qual computador está conectado a cada uma das portas. Com essa inteligência, um *switch* não transmite toda a informação para todos os outros computadores conectados a ele e, sim, apenas ao computador destino. A tecnologia de *switching* ajuda a reduzir o congestionamento de uma rede e deve ser utilizada em redes de 10 ou mais computadores;

- **Roteadores:**Os roteadores são *switches* inteligentes, pois são cientes da existência de outras redes (os *hubs* e *switches* são cientes apenas da rede à qual servem). Os roteadores são utilizados para conectar uma rede local (LAN – *Local Area Network*) com outra, muitas vezes através de grandes distâncias, usando portadoras de dados comerciais. Os roteadores podem atualizar a informação de encaminhamento automaticamente e detectar quando um caminho para uma rede não funciona e, nesse caso, acabam buscando outro caminho disponível;

- **Meios cabeados:**Logicamente, nenhum destes dispositivos funcionará se eles não estiverem conectados uns aos outros, e isso pode ser feito por vários meios. O mais comum é utilizar cabeamento *Ethernet*, que é uma das várias categorias de cabeamento de par trançado não blindado UTP (*Unshielded Twisted Pair*, Par Trançado sem Blindagem). Quanto mais alta for a categoria do cabo (Cat5, Cat6, Cat7), maior será a largura de banda suportada pelo mesmo. Além disso, existe a fibra óptica, que é mais cara e usa luz laser ou *led* ao invés de pulsos elétricos. As redes *wireless* (sem fio)

se tornaram populares nas casas, pois são fáceis e baratas de montar. O meio de transmissão em uma rede sem fio é o ar, através do qual as NICs transmitem sinais de rádio que levam a informação;

- **Software:**O *software* é a inteligência que permite que todos os componentes funcionem juntos. Os *softwares* de rede mais populares de hoje usam o que se conhece como suíte de protocolos, ou pilha, TCP/IP (*Transmission Control Protocol/Internet Protocol,* Protocolo de Controle de Transmissão). A suíte é composta por camadas de *software*, tendo cada uma delas funções definidas. Embora o modelo OSI (*Open System Interconnection*) de 7 camadas (física, enlace, rede, transporte, sessão, apresentação e aplicação) seja o ponto de início das pilhas de rede, o modelo Internet possui 4 camadas (enlace, Internet, transporte e aplicação) que combinam as do modelo OSI de uma forma particular. No entanto, ambas as pilhas trabalham com as mesmas regras, fazendo com que os sistemas de computadores heterogêneos possam comunicar-se uns com os outros, sem importar as diferenças no *hardware* ou no sistema operacional.

## 2.2 Segurança da Informação

A segurança da informação pode ser usada como se fosse uma arma estratégica em qualquer tipo de empresa e, também, é um processo de vital importância dentro de uma organização. A segurança da informação tem, como finalidade, administrar e proteger internamente a organização prevendo situações de risco. "A segurança da informação de uma empresa garante, em muitos casos, a continuidade de negócio, incrementa a estabilidade e permite que as pessoas e os bens estejam seguros de ameaças e perigos" (BLUEPHOENIX, 2008).

A informação está em toda parte, podendo ser armazenada em qualquer tipo de meio, tais como imagens, vídeos, papéis impressos, eletronicamente, ficheiros, banco de dados e até mesmo em conversas entre os funcionários. Porém, na grande maioria das vezes, a informação só tem a devida importância quando ela é perdida, destruída ou até mesmo roubada. "O custo de se proteger contra uma ameaça deve ser menor que o custo da recuperação se a ameaça o atingir" (DAVIS, 1997 citado por BLUEPHOENIX, 2008). O custo citado por Davis tem como significado apurar o valor das perdas tanto em dinheiro quanto na questão da reputação da organização, na confiança e nos outros valores que a organização mantém como princípio de sua missão como empresa.

Para que se possa implantar um projeto de segurança de informação dentro de uma determinada empresa é necessário, primeiramente, estabelecer conceitos, diretrizes, mecanismo de segurança, políticas e procedimentos, ferramentas de proteção e autenticação, além da sua relação custo-benefício. É extremamente fundamental estabelecer o nível de segurança. Este nível de segurança deve garantir que, cada funcionário só poderá acessar o conteúdo que lhe é permitido; por exemplo, um tesoureiro deve ter acesso apenas ao conteúdo de informação que faz parte do seu trabalho e não poderá acessar um dado que for de outro departamento que não tenha nenhuma relação com as funções as quais ele desempenha Este exemplo citado demonstra que a informação deve estar segura e disponível apenas para quem está autorizado. "Em termos organizacionais, a informação tem um papel vital no que diz

respeito à gestão, à organização e subsistência das entidades. O valor que a informação representa não é mensurável e a sua perda pode resultar em paragens, produtividade, desorganização e instabilidade" (BLUEPHOENIX, 2008).

Para que se garantam informações seguras é necessário se levar em conta alguns conceitos, tais como: riscos associados à falta de segurança; benefícios e custos de implementação dos mecanismos de segurança.Existem diversos riscos que podem ser associados à falta de segurança de informações. Sendo assim, todos os arquivos e dados podem ser perdidos, excluídos ou até mesmo roubados. Por exemplo, o ataque de pessoas com más intenções, tais como *hackers.* Eles podem explorar falhas em um banco de dados e conseguir se infiltrar dentro do sistema da organização. Após se infiltrarem dentro do sistema, eles podem ter acesso a todos os dados relacionados à empresa, bem como os dados de seus clientes. Desta forma, é necessário adotar uma politica de segurança de informação, levando em conta não só esses fatores, mas também fatores naturais, tais como incêndios e inundações. (SÊMOLA, 2003).

Os benefícios esperados com a implantação de técnicas de segurança da informação são o de evitar vazamentos, fraudes, espionagem comercial, uso indevido, sabotagens e diversos outros problemas que possam prejudicar uma determinada empresa. A questão da segurança visa, também, aumentar a produtividade dos funcionários, por meio de um ambiente mais organizado, além de viabilizar aplicações críticas das empresas. Os custos de implementação dos mecanismos variam de acordo com o que a organização pretende implementar.

### *2.2.1 Ameaças, perigos e vulnerabilidades à segurança*

Existem diversas formas de ameaças à questão da segurança nas empresas e organizações, tanto por causas naturais como por falhas humanas, como por exemplo, falhas de energia, sabotagem, vandalismo, roubo e incêndio, entre outras. Com o passar do tempo e aumento da necessidade de se usar a Internet dentro das organizações, outras preocupações começaram a ocorrer. O uso da Internet trouxe novas vulnerabilidades na rede interna. Como se não bastassem as preocupações existentes com espionagem comercial, fraudes, erros e acidentes, agora as empresas também precisam se preocupar com os *hackers*, invasões, vírus e outras ameaças que penetram através desta nova porta de acesso. Os principais pontos de vulnerabilidade e risco vêm das redes de computadores, bancos de dados, sistemas de informações, sistemas de energia e comunicação. Sendo assim, é necessário aplicar alguns elementos básicos para que se possa ter uma maior segurança na Internet ou Intranet, sendo eles: 1) segurança na estação (cliente); 2) segurança no meio de transporte; 3) segurança no servidor e 4) segurança na rede interna (SÊMOLA, 2003).

### *2.2.2 Política de Segurança*

Uma política de segurança é um instrumento importante para proteger uma organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida, neste contexto, como a quebra de uma ou mais de suas três propriedades fundamentais, que são: confidencialidade, integridade e disponibilidade. A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui

direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação (CERT.br, 2015).

Definir uma política de segurança é uma tarefa complicada, já que cada organização deve decidir que aspectos de proteção são mais importantes e, frequentemente, assumir um balanço entre segurança e a facilidade de uso. Tradicionalmente, a segurança de informação tem sido definida nos termos do acrônimo C.I.D. (do inglês C.I.A., *Confidentiality*, *Integrity*,*Availability*), que significa confidencialidade, integridade e disponibilidade (GOODRICH; TAMASSIA, 2013). Sendo assim, uma organização, visando garantir a segurança da informação, deve considerar (COMER, 2007):

- **Autenticidade:** Garantirá que a mensagem ou arquivo é autêntico;
- **Disponibilidade:** indica se o serviço usado está ou não disponível para acesso;
- **Confidencialidade:** garante que as informações estão circulando de uma maneira sigilosa;
- **Integridade:** refere-se justamente à integridade da mensagem, se está realmente tudo inteiro, que nada foi corrompido.

A segurança é um assunto abrangente e inclui inúmeros tipos de problemas. Em sua forma mais simples preocupa-se em impedir que pessoas mal intencionadas leiam, ou pior ainda, modifiquem mensagens secretamente enviadas a outros destinatários. A segurança trata de situações em que mensagens legítimas são capturadas e reproduzidas. A maior parte dos problemas de segurança é causada por pessoas que tentam obter algum benefício, chamar atenção ou prejudicar alguém (TANENBAUM; WETHERALL, 2011).

A sociedade precisa de mais profissionais de computação treinados em segurança, que possam defender e evitar, com sucesso, ataques contra computadores, bem como usuários treinados em segurança, que possam gerenciar de forma segura sua própria informação e os sistemas que usam.

## 2.3 Protocolo TCP/IP

O TCP/IP é o principal protocolo de envio e recebimento de dados. TCP significa *Transmission Control Protocol* (Protocolo de Controle de Transmissão) e o IP, *Internet Protocol* (Protocolo de Internet). O protocolo é um tipo de linguagem utilizado para a comunicação, para que dois ou mais computadores consigam se comunicar entre si. Por mais que duas máquinas estejam conectadas à mesma rede, se não “falarem” a mesma língua, não há como estabelecer uma comunicação. Sendo assim, TCP/IP é uma espécie de idioma que permite às aplicações conversarem entre si (TANENBAUM, 2003).

O protocolo TCP/IP consiste em um conjunto de quatro protocolos, sendo dividido em quatro camadas: aplicação, transporte, rede e interface. Cada camada é responsável pela execução de tarefas distintas. Essa divisão de camadas é o método

utilizado para garantir a integridade dos dados que trafegam pela rede (TANENBAUM, 2003)[1].

## 2.4 VLANs (*Virtual Local Area Network*)

Uma LAN (*Local Area Network*) inclui todos os dispositivos em um mesmo domínio *broadcast*, que funciona da seguinte forma: quando um dispositivo envia algum *frame* de *broadcast*, todos os outros dispositivos da LAN recebem uma cópia deste *frame* (BEGNAMI; MOREIRA, 2013).

A VLAN nada mais é que a segmentação de uma LAN, feita de forma lógica. As VLANs funcionam de maneira semelhante a uma LAN mas a grande diferença é que cada VLAN possui seu próprio domínio de *broadcast*, diminuindo o tráfego de maneira significativa. Quando não se utiliza VLAN, o *switch* considera que todas as interfaces estão na mesma LAN. Com a utilização de VLAN, podem-se criar vários domínios de *broadcast* e colocar cada dispositivo em domínios distintos. É importante entender também que, quando a rede é plana, ou seja, quando não se utiliza VLAN, um grande problema de segurança ocorre, pois os dispositivos da rede "enxergam" todos os outros dispositivos (BEGNAMI; MOREIRA, 2013).

Como se pode ver na Figura 1, existem duas VLANs, com dois dispositivos em cada uma, em apenas um *switch*.

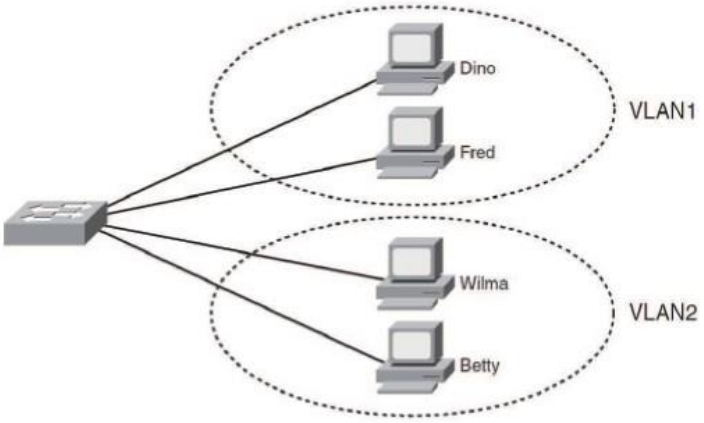


**Figura 1: VLANs (WENDELL et al., 2008)**

Existem 3 tipos de níveis para VLANs: o nível 1 (VLAN por porta ou *port-based*), o nível 2 (VLAN por MAC ou *MAC-based*) e o nível 3 (VLAN por protocolo ou *protocol-based*) (BEGNAMI; MOREIRA, 2013):

- Nível 1: define uma VLAN para cada porta do *switch*;

[1] **Modelo OSI:** O modelo de referência OSI descreve um conjunto de padrões que garantem uma maior compatibilidade e interoperabilidade entre várias tecnologias de rede (VIEGAS, 2009).

- Nível 2: define uma VLAN para cada endereço MAC dos dispositivos. Este tipo de VLAN é muito mais flexível que a do nível 1, pois a VLAN é configurada independente da localização física do dispositivo;

- Nível 3: Define uma VLAN por protocolo, agrupando todos os dispositivos que utilizam o mesmo protocolo em uma mesma VLAN.

## 2.5 Alguns métodos para gerenciamento do acesso a rede

Esta seção apresenta alguns tipos de métodos que podem ser usados para administrar a estrutura de uma rede de computadores, tal como a rede da PMPM-RS, gerenciando e controlando acessos dos usuários, visando principalmente diminuir o tráfego na rede e, também, diminuir a quantidade de vírus que se espalham nos computadores, devido à falta de controle e à falta de comprometimento dos usuários. Sendo assim, é importante controlar o acesso à rede criando perfis para todos os usuários e verificar suas necessidades na navegação, elaborando um sistema para gerenciar o acesso à Internet, permitindo controlar vários recursos, tais como a velocidade que todos os usuários poderão ter de *upload*e de *download*, além de definir em que *sites* o usuário poderá ou não navegar, dependendo do seu perfil.

### *2.5.1 Autenticações de conexão em rede*

Em um ambiente de rede onde o meio de acesso é compartilhado e aberto, tanto na rede cabeada como na rede não cabeada, nas quais existem elementos de rede que não podem ser verificados, a confiança nos *hosts* fica limitada. Para contornar esses aspectos, que comprometem os pilares da segurança (confiabilidade, integridade e disponibilidade dos ativos da rede), existem protocolos disponíveis para implementação de um meio de autenticação (SÊMOLA, 2003).

Sendo assim, sabe-se que o protocolo 802.1x fornece autenticação entre os usuários da rede na qual os mesmos estão conectados, podendo este ser conectado em um *switch* ou conectado a outro ponto de acesso, que seria um AP (*Access Point*) para acesso à rede não cabeada. Dessa forma, diminuem-se os riscos às ameaças, tornando os clientes da rede confiáveis (ENGST; FLEISHMAN, 2005).

O protocolo 802.1X é um padrão do *Institute of Electrical and Electronic Engineers* – IEEE para controle de acesso à rede com base em portas e faz parte do grupo IEEE 802.1, grupo de protocolos de redes. Segundo Brown (2007), 802.1x é um protocolo que estende o *Extensible Authentication Protocol* - EAP sobre a *Local Area Network* - LAN por um método chamado *ExtensibleAuthentication Protocolo Over LANs* – EAPoL. Todos esses protocolos são fundamentais para o funcionamento da autenticação 802.1x.

Como mostrado na Figura 2, o protocolo 802.1x abraça uma estrutura cliente-servidor com três entidades: um sistema suplicante, um sistema autenticador e um sistema servidor de autenticação.

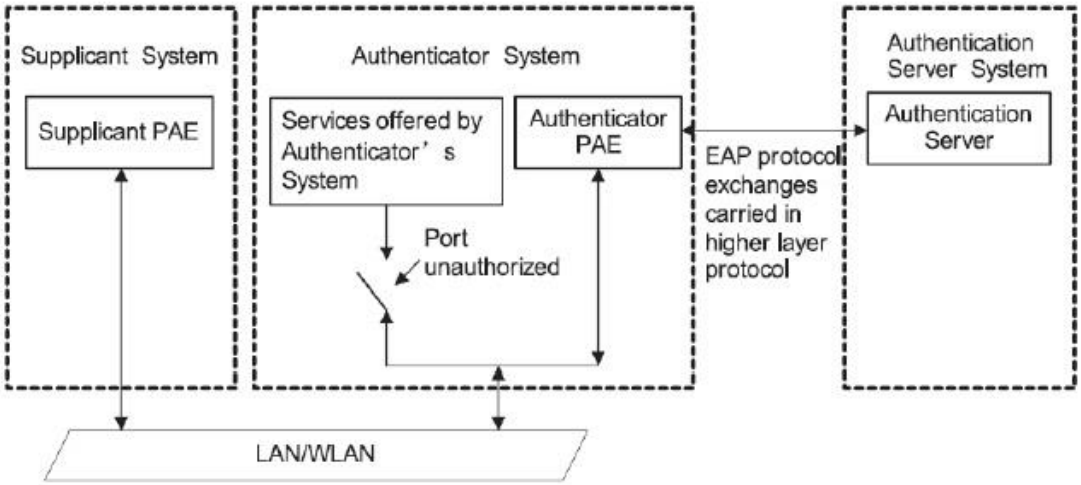


**Figura 2: Exemplo de como funciona o protocolo 802.1x (3Com, 2006)**

O sistema suplicante é uma entidade localizada em uma ponta de ligação da LAN e é autenticado pelo sistema autenticador na outra ponta da ligação da LAN. Uma autenticação 802.1x é iniciada pelo programa cliente do sistema suplicante. O programa cliente deve suportar o protocolo EAPoL (*Extensible Authentication Protocol over LAN*). O sistema autenticador é a entidade localizada no outro lado da ligação da LAN. Ele autentica o sistema suplicante conectado. O sistema autenticador é geralmente um dispositivo de rede que suporta o protocolo 802.1x. Ele fornece uma porta física para o sistema suplicante acessar a LAN (SILVA, 2012).

O sistema servidor de autenticação é uma entidade que fornece o serviço de autenticação para o sistema autenticador. Geralmente é implementado com o uso de um servidor RADIUS (*Remote Authentication Dial-In User Service*). O sistema servidor de autenticação oferece serviço que realiza a Autenticação, Autorização e *Accouting* – AAA para os usuários. Ele também armazena informações do usuário, como o nome de usuário, senha, a VLAN a qual pertence ao usuário, prioridade e *Access Control List* – ACL.

Segundo Brown (2007), essas entidades fazem três diferentes comunicações para realizarem a autenticação, duas são trocas físicas e uma troca lógica. Há uma comunicação física entre o suplicante e o autenticador e, também, entre o autenticador e o servidor. Assim, o autenticador funciona como um tradutor entre o suplicante e o servidor de autenticação. A comunicação entre o suplicante e o servidor de autenticação é inteiramente lógica, já que não há nenhuma ligação física entre eles.

Quando o sistema autenticador e o sistema suplicante se comunicam, utilizam o protocolo EAPoL na camada dois do modelo OSI. Qualquer coisa que o sistema suplicante tentar fazer fora do protocolo é ignorado pelo sistema autenticador. É possível configurar o processo de autenticação para permitir um tráfego específico oriundo da rede até o suplicante (TANENBAUM, 2003).

Assim que um dispositivo é conectado à porta, o sistema autenticador solicita a credencial de identificação. Nesse momento é utilizado um *frame* EAPoL, chamado de *Request Identity*. Se existir um sistema suplicante na outra ponta do enlace, ele responderá com o pacote "*Response*". O sistema autenticador aceitará o pacote de "*Response*" e encaminhará ao sistema servidor de autenticação, utilizando o protocolo

RADIUS. O sistema autenticador empacota esses dados do sistema servidor de autenticação e encaminha um *Request Identity* ao suplicante, utilizando um pacote do protocolo EAPOL. Este tipo de comunicação continuará até que o processo de autenticação seja completo (TANENBAUM, 2003).

### *2.5.2 Servidores proxy*

A principal importância de se aplicar um servidor *Proxy* é sua funcionalidade como *firewall* e filtro de conteúdo, permitindo controlar o que pode ou não ser acessado na rede. Um servidor *Proxy* pode bloquear páginas tanto por IP, como por palavras que acompanham um texto, sendo importante, também, no processo de aceleração da navegação na *web*, aproveitando a página de um usuário para compor a página de outro, melhorando o desempenho.

Um servidor é todo conjunto de *hardware* e *software* que tem, como principal objetivo, o de disponibilizar recursos de serviços e dados para uma rede de computadores ou servidores. O servidor tem a função de gerenciar toda e qualquer informação de uma empresa, melhorando o compartilhamento de informação e recursos, além de acrescer segurança, justamente por que filtram alguns tipos de conteúdo na *web* e *softwares* mal-intencionados (MARCELO, 2005).

O servidor *Proxy* tem, como principal objetivo, o de funcionar como um servidor que armazena dados temporários, que são chamados de "*cache*", armazenando todas as páginas recém-visitadas na Internet. Isso ajuda a aumentar o desempenho do carregamento das páginas quando forem acessadas novamente (MARCELO, 2005).

Na comunicação com a Internet existe uma comunicação entre um servidor e um usuário, como mostra a Figura 3.

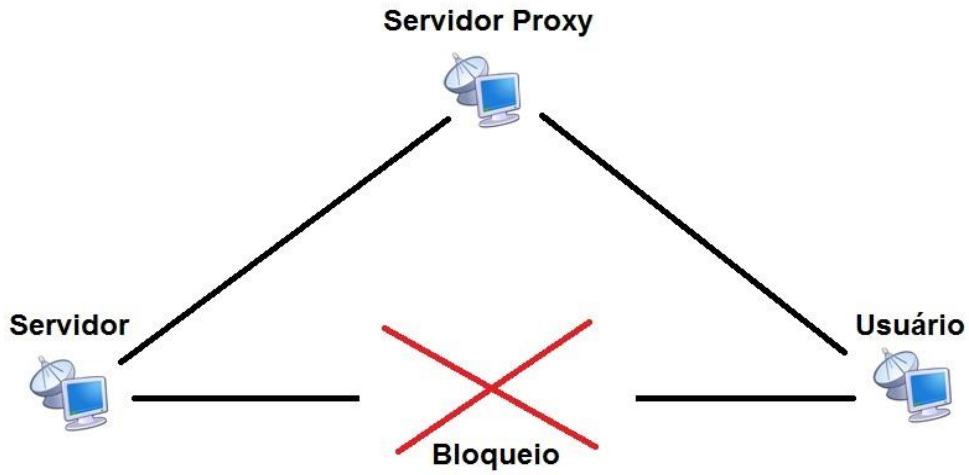


**Figura 3: Servidor *Proxy* (Fonte: dos autores, 2017)**

De acordo com a Figura 3, existe um servidor e, desse servidor, os dados são enviados diretamente para o usuário que está do outro lado do computador. Essa

comunicação é direta porém, existe um servidor, chamado servidor *Proxy*, que faz a comunicação entre um servidor e um usuário. Por exemplo, supondo que o usuário esteja em um local onde a comunicação com um determinado *site* seja bloqueada. Quem faz o bloqueio é a parte da ligação entre o servidor e o usuário. Como a comunicação está bloqueada, utiliza-se um servidor *Proxy*, que fará a ligação do servidor para o servidor *Proxy* e, em seguida, para o usuário. Neste caso, todos os dados que passariam direto do servidor para o usuário, passariam primeiro pelo servidor *Proxy*.

### *2.5.3 Autenticação por portal (hotspot)*

O termo chamado *hotspot* é uma autenticação por portal, baseada na autenticação via interface HTTP/HTTPS (*HyperText Transfer Protocol/HyperText Transfer Protocol Secure*), na configuração de regras de *firewall* dinâmicas e outros recursos centralizados, colocados em um instrumento de controle – este no caso deve possuir acesso à rede externa – que é conectado em uma rede local por um meio guiado. Nesse tipo de autenticação, todo tráfego vindo dos pontos de acesso será interceptado e, somente após a autenticação do cliente, liberado (CARRION, 2005).

Desta maneira, o usuário terá seu acesso completamente bloqueado, até que se forneçam as credenciais válidas, verificadas em um banco de dados, para autenticação. Depois de verificadas as credenciais corretas, dinamicamente o *firewall* irá liberar o acesso para o cliente até que outra regra modifique essa ação, como por exemplo, o tempo de inatividade ou o desligamento do computador (FLECK; POTTER, 2002).

Um dos principais fatos que encoraja a adoção do mecanismo de *hotspot* é a grande facilidade de acesso, pois não requer nenhum *software* ou configuração por parte do usuário. A autenticação por portal pode ocorrer de muitas maneiras, entre elas: *closed* portal, o qual pode ser utilizado para restringir o acesso a um determinado grupo de usuários com credenciais de usuário e senha, ou então exigir o pagamento para utilização por tempo determinado; *open* portal, que simplesmente requer a aceitação de um termo de uso para liberação do acesso (FLECK; POTTER, 2002).

Como se pode ver na Figura 4, existe um bloqueio que impede o acesso à Internet, sendo necessário informar o usuário e a senha correta para que assim seja liberado o acesso.

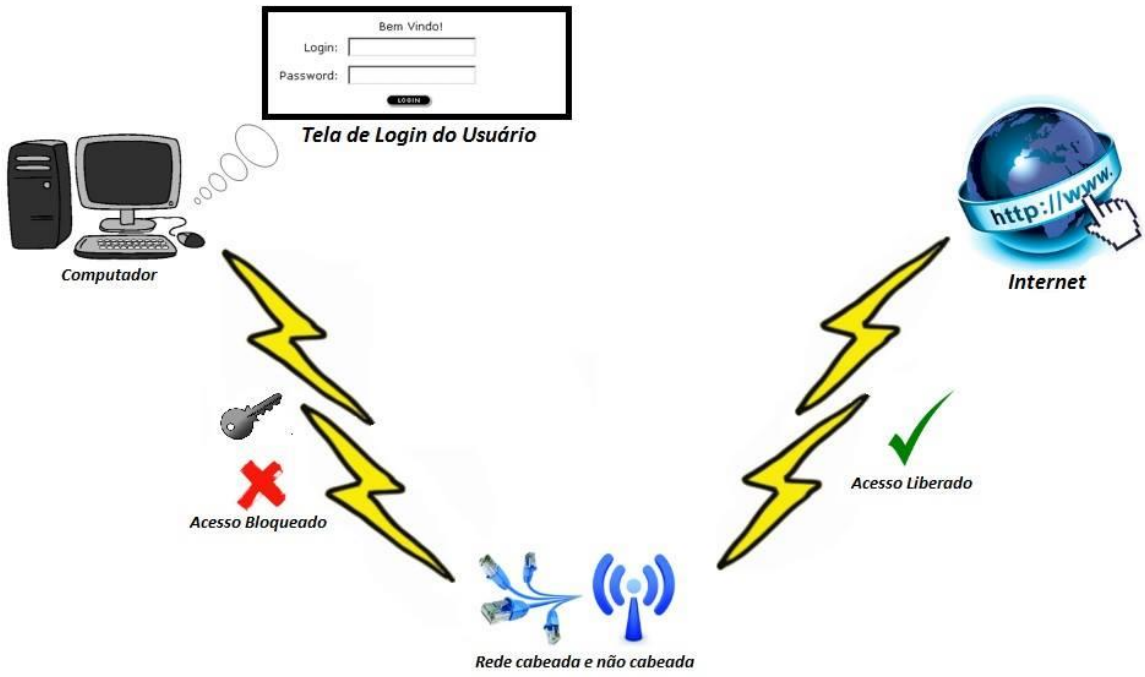


**Figura 4: Autenticação por portal (*hotspot*) (Fonte: dos autores, 2017)**

## 2.6 Seguranças de Conexão de Rede

O tema que envolve a segurança em redes de computadores e segurança da informação, tem se tornado cada vez mais importante à medida que a Internet tornou-se um ambiente hostil e as ferramentas para capturar tráfego, quebrar sistemas de encriptação, capturar senhas e explorar vulnerabilidades diversas tornam-se cada vez mais sofisticadas (MORIMOTO, 2011).

Sendo assim, é necessário tomar medidas para que haja uma maior proteção e segurança tanto para casos de perdas de documentos, vinculados a vírus e *malwares*, quanto a ataques de *hackers* a informações pessoais. Essas medidas irão garantir Autenticidade, Disponibilidade, Confidencialidade e Integridade (CAMPOS, 2007 citado por CARVALHO, 2011).

## 2.7 Formas de filtro

Esta seção apresenta algumas formas de filtros usando *firewall*. Sendo assim, estudaremos sua definição e seus tipos de filtros, sendo eles: filtros de pacotes, filtros de estado, *firewall* de aplicação e IDS (*Intrusion Detection System*), visando identificar o método mais adequado para ser aplicado neste trabalho.

*Firewall* define-se como equipamento ou dispositivo de rede que tem, como principal objetivo, o de manter a segurança, aplicando políticas de segurança a um determinado ponto de controle de uma rede de computadores ou mesmo um dispositivo constituído pela combinação de *software* e *hardware*, utilizado para dividir e controlar o acesso entre redes de computadores. Os *firewalls*permitem controlar e regular o tráfego de dados na própria rede, ou em rede distintas, impedindo a transmissão ou recepção de acessos não permitidos de uma rede para outra (CERT.br, 2003).

O *firewall* pode ser tanto lógico, ou seja, um *software* que possui a funcionalidade de controle e filtro de tráfego a um computador, quanto físico, que são equipamentos de uso dedicado para filtragem de redes, instalados em pontos críticos de controle de trafego ou, até mesmo, a combinação de ambos, que ajuda a tornar a rede cada vez mais segura quanto mais complexa (CERT.br, 2003).

### *2.7.1 Tipos de firewalls*

Existem quatro tipos básicos de *firewall*, sendo eles (NED, 1999):

- **Filtro de Pacotes:** este filtro analisa individualmente os pacotes, na medida em que são transmitidos, verificando informações das camadas dois e três do modelo OSI;

- **Filtro de Estados:** tem, como função, analisar e identificar o protocolo dos pacotes transitados para saber as respostas. Resumindo, o *firewall* guarda o estado de todas as últimas transações efetuadas e analisa, inspecionando o tráfego para evitar pacotes não legítimos;

- ***Firewall* de Aplicação:** esse *firewall* trata dos pacotes vindos da última camada do modelo OSI (camada de aplicação), sendo instalado junto com a aplicação a ser protegida; ele analisa particularidades do protocolo utilizado e toma decisões que podem evitar ataques maliciosos à rede;

- **IDS:** é sistema de detecção de intrusão, que tem como objetivo principal detectar se existe alguém tentando invadir o sistema ou se é apenas um usuário legítimo que está fazendo mau uso do mesmo. Esta ferramenta é executada, normalmente, em *Backgroud* e só envia alguma notificação quando detecta alguma atividade que seja suspeita ou ilegal.

### *2.7.2 Melhor utilização do firewall*

A localização de um sistema de*firewall,* dentro de uma rede, depende particularmente das políticas de segurança. Para cada caso, entretanto, existe um conjunto de regras que devem ser aplicadas, são elas (NED, 1999):

- Todo fluxo de rede, ou seja, todo tráfego, deve passar pelo *firewall*, caso contrário, existindo rotas alternativas, pode-se comprometer a segurança da rede;

- Deve existir um filtro de pacotes no perímetro da rede, localizado entre o roteador e as estações de trabalho ou mesmo na borda da rede interna com a externa aumentando, assim, a proteção contra acessos indevidos e bloqueio global de tráfego indesejado;

- Os servidores com conteúdo *web*devem ser instalados o mais isolados possível dos outros computadores da rede, para que estes não fiquem vulneráveis à rede externa (Internet). Este conceito é conhecido como DMZ (*Desmilitarized Zone*, ou Zona Desmilitarizada);

- Utilizar *firewalls* no contexto da rede interna, assim isolando redes separadas, e distintas, para que não exista colisão ou mesmo intercepção do tráfego entre elas.

### *2.7.3 Critérios de filtragem*

Basicamente existem duas maneiras ou dois critérios de filtragem que podem ser empregados em um *firewall*, sendo: 1) *default deny*, *o*u seja, todo tráfego que não for explicitamente permitido é bloqueado; 2) *default allow*, todo tráfego que não for explicitamente proibido é liberado (STATO FILHO, 2009).

Porém, a configuração dos *firewalls* deve seguir a configuração das políticas de segurança da rede a ser aplicada. Normalmente utiliza-se com maior frequência o *default deny*,que exige uma interação bem mais ativa do administrador, que é obrigado a intervir de maneira explícita para liberar o tráfego desejado, evitando assim erros e falhas de segurança(NED, 1999).

### *2.7.4 Implantação de firewall*

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br, 2006), a implantação de um *firewall* como em qualquer outro fator em uma rede, também pode ser empregada e modelada dependentemente da sua estrutura de rede. Isto inclui fatores tanto lógicos como físicos, dependendo de quanto a rede vai ser protegida dos custos, das funcionalidades pretendidas, entre muitos outros fatores. Na Figura 5 pode-se ver um exemplo de uma aplicação de um *firewall*.

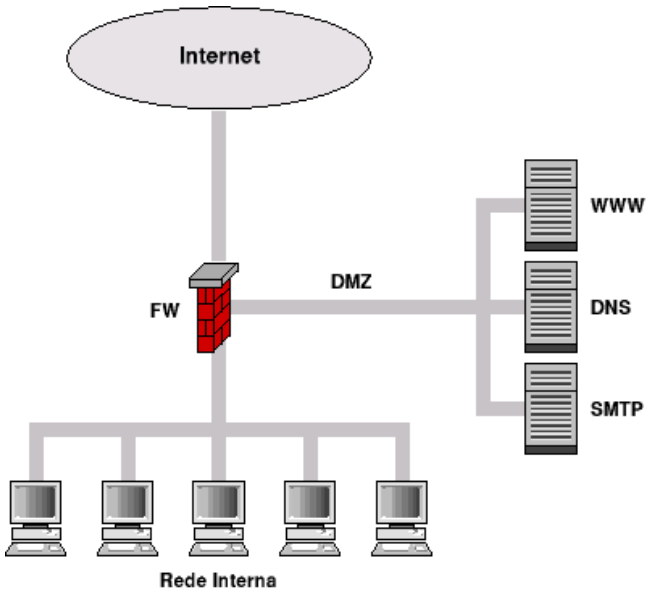


**Figura 5: Exemplo de um *firewall*(CERT.br, 2009)**

Utilizando o modelo da Figura 5 como exemplo, tem-se uma arquitetura funcional que pode, eventualmente, ser adotada em alguma situação real devido à

simplicidade do modelo, porém não deixando de lado a possível existência de algumas adaptações. A Figura 5 mostra um exemplo simples de uso de *firewall*. Nesse exemplo, o computador do *firewall* contém três interfaces de rede: uma para a rede externa, uma para a rede interna e outra para a DMZ (*Desmilitarized Zone*). Por padrão, este *firewall* bloqueia tudo, liberando apenas o que for explicitamente declarado em suas regras (*default deny*). O tipo de *firewall* recomendado a ser utilizado é o *Stateful firewall*, que dinamicamente gera regras que permitem a entrada de respostas oriundas das conexões iniciadas na rede interna. No entanto, não é necessário incluir regras específicas e separadas para a entrada dessas respostas individualmente.

As interfaces deste *firewall* estão assim constituídas:

*Interface Externa:*

- **Saída:** libera saída de todas as informações, com exceção dos pacotes com endereços de origem pertencentes a redes privadas e pacotes com endereços de origem pertencentes a blocos de rede interna;
- **Entrada:** Libera a entrada apenas aos pacotes que obedecem às seguintes combinações de protocolo, endereço e porta de destino: Porta 25, protocolo TCP, endereço do servidor SMTP (*Simple Mail Transfer Protocol*); porta 53, protocolo TCP e porta 53, protocolo UDP (*User Datagram Protocol*), endereço do servidor DNS (*Domain Name System*);

*Interface Interna:*

- **Saída:** Libera a saída de todas as informações;
- **Entrada**: Não libera a entrada de nenhuma informação;

*Interface DMZ:*

- **Saída:** Libera a saída das portas 25 no protocolo TCP (Servidor SMTP), 53 protocolo UDP e TCP (Servidor DNS) e 80 protocolo TCP (Servidor *web*);
- **Entrada**: Além das mesmas regras de entrada da interface externa, também é permitido o tráfego para todos os servidores da porta de destino 22/TCP (SSH - *Secure Shell*) e endereço de origem na rede interna.

Com essas políticas aplicadas, a segurança de rede se torna bem menos frágil a ataques, e são estas regras particulares de cada serviço e/ou recurso disponibilizado que tornam a rede inacessível aos acessos externos e internos indevidos (CERT.br, 2006).

## 3. Estado da Arte

Nesta seção serão apresentados alguns trabalhos correlacionados ao apresentado neste artigo, bem como a comparação entre os mesmos e o trabalho desenvolvido.

### 3.1 Gestão da Segurança da Informação no Contexto da Vulnerabilidade Técnica e Humana inserida nas Organizações

O trabalho apresentado por Peixoto (2004) tem, como principal objetivo,o de demonstrar que, mesmo com pouco investimento, conseguem-se resultados satisfatórios no quesito de segurança da informação, principalmente por estar voltado ao ambiente humano. Além disso, o trabalho realizado fornece auxílio concreto para elaboração de um *software* que sirva como ferramenta para efetivação dos cálculos, análises e posterior classificação dos riscos, das situações mais criticas e, por fim, das justificativas de investimento em segurança da informação.

Cada vez mais as empresas de TI (Tecnologia da Informação) têm investido na questão da segurança de suas informações. Este alto investimento está relacionado a preocupações em se proteger cada vez mais dos ataques, tanto de *hackers* como de *crackers* e de vírus. Com o crescimento da inclusão digital em toda parte do mundo, o acesso à informação está cada vez mais fácil. O reflexo deste novo panorama traduz-se em episódios cada vez mais frequentes de saques eletrônicos indevidos, clonagem de cartões de crédito, acessos a bases de dados confidenciais, entre outras inúmeras ameaças relacionadas à questão de segurança.

O tema "Segurança da Informação" tem sido motivo de grande debate atualmente. As organizações estão buscando soluções práticas e efetivas, que possam trazer otimização de suas atividades mas, ao mesmo tempo, segurança em operar seus mecanismos de trabalho. A forma como as organizações deverão gerir este desafio, divide-se em duas frentes: a segurança da informação em âmbito físico e técnico. Entretanto, quase sempre a preocupação é somente com a tecnologia e toda a estrutura a ser empregada, esquecendo-se do elo mais fraco de todas as empresas de qualquer setor: o fator humano. Neste contexto surge um novo conceito, a insegurança tecnológica e humana, chamada de engenharia social.

Por meio desse quadro critico em que se encontram quase todas as organizações, quando se tratam de suas informações, sejam elas confidenciais ou não, torna-se extremamente fundamental, não somente ao profissional da área de TI, mas também, aos demais responsáveis por qualquer tipo de informação que comprometa a empresa, serem orientados, instruídos e comprometidos ao melhor tratamento e cuidado com as informações.

Peixoto (2004) concluiu que o principal fator que agrava a falta de segurança dentro das organizações é a falta de instrução e conscientização por parte dos funcionários. Sendo assim, o principal o propósito do trabalho realizado foi o de dar subsídios concretos aos profissionais de TI, para que possam prezar pela segurança das informações, empregando ferramentas para análises de risco e conhecimentos atualizados sobre as técnicas de engenharia social. Outro resultado apontado pelo autor é de que o valor de investimentonecessário é consideravelmente baixo com relação às medidas para implantar uma política efetiva de segurança da informação. Isso ocorre devido às definições de risco serem situações propícias (a maioria delas) a fatores ligados ao elo mais fraco quando se trata de segurança das informações, que é o fator humano.

### 3.2 Implantação de um Ambiente de Segurança de Redes de Computadores: Um Estudo de Caso na Prefeitura Municipal de Palmeira das Missões – RS

Molina, Silveira e Santos (2015) apresentam um estudo de caso desenvolvido na PMPM–RS onde, por meio da definição de uma infraestrutura física e lógica, implantaram um ambiente seguro em sua rede de computadores, visando garantir uma maior confiabilidade e gerenciamento da mesma. Por meio da criação de VLANs e definição da DMZ, foi possível atingir um nível de segurança mais elevado, como o Departamento de Informática da PMPM-RS desejava.

Para tanto, os autores realizaram um estudo de toda a infraestrutura física e lógica existente na PMPM-RS e também de ferramentas, *softwares*, sistemas operacionais e conceitos de segurança da informação. A partir deste estudo foi possível detectar os pontos mais "frágeis" da rede e dar prioridades para colocar em prática demandas da política de segurança que não haviam sido sanadas até então. Desta forma foi possível realizar um diagnóstico da situação em que se encontrava a rede de computadores naquele momento.

Com as demandas levantadas verificou-se que existiam muitas prioridades e serviços diferentes que necessitavam da rede. Em um primeiro momento, realizou-se um estudo com os relatórios e recursos disponibilizados pelo software *Zabbix*, para que pudessem ser realizados comparativos posteriormente. As VLANs foram simuladas no *software Packet Tracer*, que é um *software* gratuito para simulação de redes de computadores desenvolvido pela Cisco, com foco educacional. Ainda durante a implantação os autores utilizaram o SARG (*Squid Analysis Report Generator*), que tem a função de gerar relatórios de acesso à Internet, tornando-se uma ferramenta auxiliar muito importante em conjunto com o *Zabbix* e as VLANs. Com o apoio destas ferramentas, no momento em que se detectar um fluxo elevado na rede, é possível verificar os *hosts* e saber se essa demanda é de Internet e se o conteúdo acessado está de acordo com as normas da política de segurança.

A partir de reuniões realizadas junto ao Departamento de Informática da PMPM-RS, foi definido que as VLANs seriam estruturadas por departamentos já existentes e assim aplicadas, e os recursos do *Zabbix* utilizados para fazer tal monitoramento e comparações. O trabalho destaca vários pontos como: estruturação das VLANs, configuração do *gateway* (TAG), regras de *firewall* para as VLANs e serviço de Internet com regras de *proxy*. Também destaca a configuração da DMZ utilizando 3 servidores físicos disponíveis na prefeitura, sendo aplicadas as regras já existentes no *firewall* para determinar o acesso aos principais serviços da DMZ.

Entre os resultados destacam-se vários aspectos que antes não eram possíveis de serem monitorados, tais como: horários de maior fluxo de rede e setores que necessitavam de uma atenção "extra", devido ao volume de informações transitadas. A partir de uma nova definição de infraestrutura física e lógica, além do apoio do *softwareZabbix*, foi possível realizar este monitoramento. Os autores destacam a necessidade de compreender muito bem o funcionamento da organização, para que seja possível obter informações sobre a rotina de trabalho e como os diferentes setores gerenciam as informações.

### 3.3 implantação do *firewall PfSense*

O trabalho de Neves, Machado e Centenaro (2014), apresenta pesquisas e aplicações necessárias para a implementação de um *firewall* utilizando o *software* livre *PfSense* em empresas que possuem um menor recurso financeiro para investir na área de segurança, mas que, mesmo assim, necessitam de uma segurança adequada, para que seus dados sejam mantidos internamente e/ou trafeguem de forma segura para o ambiente externo. Esta aplicação se faz necessária devido à grande evolução das comunicações do mercado corporativo, que trouxe junto consigo, pessoas mal intencionadas que se utilizam de mecanismos para furtos de informações e, até mesmo, de serviços e produtos.

Com base nas informações colhidas por meio de pesquisas em algumas empresas, foi proposta uma solução de *firewall* aconselhada para pequenas empresas que não possuam muita verba parainvestimento na área de segurança da informação. Apesar de ser uma soluçãobaseada em *software* livre, a ferramenta possui muitos recursos e apresenta grandegrau de segurança a um custo mais acessível. A implantação do *firewallPfSense* visa implantar serviços como: filtragem de origem e destino IP, protocolo IP, portas de origem e destino para tráfegos de protocolos UDP e TCP; habilidade de limitar, por meio de uma política de regras, conexões simultâneas; opção de realizar ou não os relatórios baseados somente em regras selecionadas; habilidade de criação de grupos de endereços, redes e portas visando à facilidade de gerenciamento e a clareza das regras criadas; capacidade de gerenciamento de tabela de estados e interface *web*fácil de gerenciar.

Seguindo nesse contexto, a implantação deste projeto foi guiada por manuais, normas e guias que tratam o tema. Este projeto foi desenvolvido em quatro etapas: na primeira etapa foi realizada uma contextualização sobre o tema segurança, sendo apresentadas as motivações que levaram ao desenvolvimento do *firewall*, destacando-se a importância, seus principais conceitos e os principais equipamentos utilizados no mercado. Na segunda parte do projeto, foi apresentada a tecnologia *PfSense*, suas funções, configurações e maneiras de implantação. Na terceira etapa foi realizada uma simulação que demonstrou, na prática, o funcionamento do *firewall* e os principais atributos necessários para a implantação desta tecnologia. A quarta e última etapa visou vincular o conhecimento obtido nas simulações ao conhecimento teórico, para demonstrar os reais benefícios desta tecnologia.

O *PfSense* é um *software* livre customizado da distribuição de FreeBSD, sendo adaptado para o uso como *firewall* e roteador, que é inteiramente gerenciado via interface *web*. Além de ser um poderoso *firewall*, e uma plataforma de roteamento, possuindo uma variada lista de recursos que podem ser adicionados por meio de *downloads* de pacotes permitindo, assim, a adição de funcionalidades de acordo com a necessidade do usuário.

Os autores concluíram que o projeto do *firewallPfSense* foi muito útil, principalmente para a aplicação de uma série de conhecimentos na montagem de um projeto de utilidade profissional. Os resultados demonstram que o *PfSense* pode ser mais que uma solução de *firewall* para uma pequena empresa mas, sim, uma solução de gerência de redes com diversas funções, tais como o servidor DHCP (*Dynamic Host Configuration Protocol*) e *proxy* integrado, além de possuir uma fácil interface de gerenciamento e manutenção por meio de telas de *status e debugging*. Como o valor de

investimento da tecnologia *PfSense* é baixo, demonstra-se como uma solução para pequenas e, em alguns casos, para médias empresas. Sendo assim, os autores destacam que o projeto do *firewall PfSense* é viável e a melhor opção *Open Source*, atendendo a demanda por segurança, bem como os objetivos propostos no trabalho.

### 3.4 Estudo Comparativo

A partir dos trabalhos correlacionados estudados, elaborou-se um quadro destacando as principais características dos mesmos, comparando-os à solução apresentada neste artigo. Estas características são apresentadas no Quadro 1.

**Quadro 1 – Estudo Comparativo**

| **Trabalhos** | ***Software* e ferramentas utilizadas** | **Resultados alcançados em relação aos objetivos** |
|---|---|---|
| Trabalho 1 (PEIXOTO 2004) | | - colaborar como instrumento de compreensão didático-metodológico; no contexto das inúmeras vulnerabilidades técnicas e humanas inseridas nas Organizações, agregando-se a futura elaboração de uma ferramenta para melhor gerir a segurança das informações. |
| Trabalho 2 (MOLINA, SILVEIRA e SANTOS 2015) | *Zabbix*, *Packet Tracer*, SARG | - Maior gerência e segurança da rede com as VLANs e DMZ<br>- Com o *Zabbix* foi possível ter respostas muito mais rápidas e tomar decisões mais acertadas<br>- Com um controle maior da rede é possível fazer uma maior previsão em quesitos como gerência e escalabilidade. |
| Trabalho 3 (NEVES, MACHADO e CENTENARO 2014) | *Firewall PfSense* | - Filtragem de origem e destino IP, protocolo IP, portas de origem e destino para tráfegos de protocolos UDP e TCP;<br>- Habilidade de limitar através de uma política de regras, conexões simultâneas;<br>- Opção de realizar ou não os relatórios baseados somente em regras selecionadas;<br>- Habilidade de criação de grupos de endereços, redes e portas visando à facilidade de gerenciamento e a clareza das regras criadas;<br>- Capacidade de gerenciamento de tabela de estados;<br>- Interface *web* de extrema facilidade de gerenciamento; |
| Solução Implementada | Autenticação por portal *(hotspot)* | - controle e gerência do acesso à estrutura de rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS |

O Quadro 2 detalha os tipos de problemas que foram abordados nos trabalhos estudados e na solução aqui apresentada.

**Quadro 2 - Comparações entre os Problemas Abordados**

| Trabalhos | Problemas dos Trabalhos Comparados |
|---|---|
| Trabalho 1 (PEIXOTO 2004) | Segurança da Informação e vulnerabilidade nas organizações |
| Trabalho 2 (MOLINA, SILVEIRA e SANTOS 2015) | Segurança da Rede, Segurança da Informação, Gerenciamento, Escalabilidade, *Broadcast* |
| Trabalho 3 (NEVES, MACHADO e CENTENARO 2014) | Demonstrar as configurações da tecnologia *PfSense* e apresentar um projeto de segurança utilizando a mesma |
| Solução Implementada | Segurança e Gerenciamento de Redes de Computadores |

Analisando-se os trabalhos estudados, verifica-se que existem problemas em comum, que necessitaram de melhorias na questão da segurança da informação. Os problemas destacados envolvem dificuldades de gerenciamento, desempenho e segurança, principalmente.

No quadro 1, pode-se visualizar os diferentes tipos de *software* e ferramentas que foram utilizados para solucionar os mais diversos problemas e os resultados obtidos em cada um dos trabalhos. Um fato interessante é que todos os trabalhos visam à questão de segurança da informação, tanto estudando conceitos e vulnerabilidades, quanto a aplicação de métodos em ambientes reais (organizações), permitindo que seus resultados pudessem ser comprovados. Sendo assim, pode-se constatar que, apesar de serem organizações diferentes, os problemas ligados às redes de computadores são comuns, principalmente quando se trata de segurança e gerenciamento de redes de computadores.

## 4. Solução Implementada

A solução implementada neste trabalho envolveu a definição e implementação de um método de autenticação para controle e gerenciamento da conexão dos usuários da rede de computadores da PMPM-RS (rede de computadores que foi utilizada para compor o estudo de caso) para, assim, restringir e registrar os acessos conforme a Política de Segurança e contexto da segurança de rede baseada em perfil de usuários. A solução

permitiu controlar o acesso dos usuários e diminuir o tráfego na rede, por meio de técnicas de autenticação usando o protocolo 802.1x, utilizando-se perfis de acesso e estabilidade definida por VLANs.

O método de pesquisa empregado neste trabalho foi o estudo de caso. Segundo Yin (2001), os estudos de caso são uma metodologia de pesquisa adequada quando se colocam questões do tipo "como" e "por que", que fazem parte do objetivo geral deste trabalho – como implantar um método de acesso a rede de computadores, por exemplo. Yin (2001) ainda coloca que os estudos de caso podem ser usados para diversos tipos de pesquisas entre eles política, pesquisa em administração pública, sociologia, estudos em organizações e gerenciais, pesquisas em planejamentos regionais, dissertações e teses em ciências sociais, áreas profissionais como administração empresarial, entre outras.

Desenvolveu-se um meio de controle e gerenciamento por autenticação, para controlar o acesso à estrutura de rede de computadores, usando métodos específicos para coletar dados da rede, visando observar a quantidade de tráfego na rede usado na PMPM-RS. Para isso, foram definidos critérios para cada perfil de usuário, conforme o seu setor, criando regras administrativas para cada usuário, em relação a o conteúdo que terá acesso.

O desenvolvimento do estudo de caso foi dividido nas seguintes etapas:

1. levantamento do material bibliográfico envolvendo as áreas abrangidas no estudo de caso, para que fosse possível elaborar o referencial teórico e o estado da arte;

2. estudo dos métodos para gerenciamento de acesso a redes de computadores, visando identificar o método mais adequado para autenticação no contexto da rede de computadores da PMPM-RS;

3. definição dos critérios de avaliação dos perfis de usuários, para se estabelecer as regras administrativas relacionadas a cada perfil;

4. aplicação do método de gerenciamento definido na rede de computadores da PMPM-RS;

5. realização de testes para validar os limites de acesso de cada usuário em relação ao conteúdo que pode ou não ser acessado;

6. coleta de dados para verificar se os acessos estão ocorrendo de forma adequada, possibilitando a redução do tráfego na rede;

7. análise e discussão dos resultados do estudo de caso.

### 4.1 Método para Gerenciamento

O método escolhido para o controle e gerenciamento de acesso dos usuários foi o de autenticação por portal, denonimada "*hostpot*", que consiste em uma página "*web Landing".* Esta autenticação pode ser apresentada por um *"layer 3"* ou "*layer 2".* O *layer 2* apenas possui a capacidade de trabalhar com *MAC addresses*. Isso permite que ele se comunique apenas baseado em endereços *MAC;* ele também propaga todo

*broadcast* e não tem capacidade de interligar redes ou sub-redes. O *layer 3*, além de código *MAC*, tem a capacidade de roteamento e também trabalha com endereçamento lógico. Dessa forma, tem a capacidade de identificar redes e sub-redes (endereço IP e máscara), possibilitando a interconexão de redes ou sub-redes, sendo utilizado para a criação de VLANs. Eles sãomostrados para os usuários antes que os mesmos possam ter um acesso mais amplo às *URLs* (*Uniform Resource Locator*) ou serviços de Internet baseados no protocolo HTTP. Os *layers* são usados, muitas vezes, para apresentar uma página de *login* às interceptações do portal e pacotes observados até o momento em que o usuário está autorizado a iniciar as sessões do navegador (CHEN, 2010).

Depois de ser redirecionado para uma página *web* que pode exibir autenticação, pagamento, políticas de uso aceitável ou outras credenciais válidas, o *host* do usuário concorda com as informações fornecidas. Logo após, é concedido ao usuário o acesso à Internet de forma condicional, isto é, restrito em alguns *sites*. Esses serviços de *hostpot* são usados cada vez mais para obter uma melhor segurança, tanto nas redes cabeadas quanto nas não cabeadas, para acesso empresarial e residencial, por exemplo, em edifícios de apartamentos, quartos de hotel, centros de negócios, etc. (CHEN, 2010).

A página de *login* para acesso à Internet apresentada ao usuário é armazenada localmente no *gateway*[2] ou no servidor de hospedagem na *web*. Isso requer acesso a uma lista aprovada de acesso, ou "*white-list*", uma característica essencial de uma empresa segura. Dependendo do conjunto de recursos do *gateway*, os servidores *web* podem ser *white-list*, isto é, que possuem*iframes* ou *links* dentro da página de *login*. Além de *white-list*, as URLs de servidores *web* e alguns *gateways* podem listar portas TCP. O endereço MAC[3](*Media Acess Control*) de clientes conectados também pode ser configurado para esse processo de *login*.

Existe mais de uma forma para se implementar uma autenticação por portal. O tráfego do cliente também podem ser redirecionado usando redirecionamento ICMP (*Internet Control Message Protocol*) no nível de camada 3 do modelo OSI (HINDLE, 2013).

Quando o usuário solicita o acesso um determinado *site*, a DNS[4] (*Domain Name System*) é consultada pelo navegador. O *firewall* irá certificar-se que somente o servidor DNS fornecido pelo DHCP pode ser utilizado pelo usuário. Este servidor DNS retornará o endereço IP da página com o *hotspot*, como resultado de todas as pesquisas de DNS.

Um serviço de *hotspot* é conhecido por ter um conjunto de regras de *firewall* completo. Em algumas aplicações o conjunto de regras será feito por meio de solicitações via DNS de clientes para a Internet ou o servidor DNS fornecido, atendendo às solicitações de DNS do cliente (HINDLE, 2013).

Alguns serviços de *hotspot* podem ser configurados para permitir que os agentes do usuário sejam adequadamente equipados para detectar o *hotspot* e, autenticar de

---

[2]***Gateway:***é a porta de entrada e de saída da rede (MORIMOTO, 2011)

[3]MAC (*Media Acess Control*): Um endereço MAC é um identificador de 48 bits atribuído a uma interface de rede pelo seu fabricante (GOODRICH; TAMASSIA, 2013)

[4]DNS (*Domain Name System*, ou sistema de nomes de domínios): São os responsáveis por localizar e traduzir para números IP os endereços dos *sites* digitados nos navegadores (MORIMOTO, 2011)

forma automática. Esses agentes de usuários são aplicações de *software* que funcionam como um cliente em um protocolo de rede. Os agentes de usuário e aplicativos complementares, assim como o *Captive Portal Assistente* da *Apple*, podem, por vezes, ignorar de forma transparente a exibição de conteúdo *hotspot* contra a vontade do operador de serviço, desde que eles tenham acesso à correção das credenciais, ou podem tentar autenticar com credenciais incorretas ou obsoletas, resultando em consequências não intencionais, tais como bloqueio de conta acidental. Um *hotspot* que usa endereços MAC para controlar dispositivos conectados às vezes pode ser contornado através da ligação via *hard-fio* de um roteador que permite a configuração do endereço MAC do roteador. Muitos *firmwares* de roteadores chamam isso de clonagem MAC. Uma vez que um computador ou *tablet* foi autenticado ao *hotspot* usando um nome de usuário válido e senha válida, o endereço MAC desse computador ou *tablet* pode ser inserido no roteador que, muitas vezes, continua a ser conectado através do *hotspot*, pois mostra ter o mesmo endereço MAC como o computador ou *tablet* que foi conectado anteriormente (HINDLE, 2013).

Entretanto, existem algumas limitações como, por exemplo, algumas dessas implementações simplesmente exigem que os usuários passem por uma página de *login* SSL (*Secure Socket Layer*) criptografado. Após a verificação de usuário e senha, o seu endereço IP e MAC são autorizados a passar através do *gateway,* como se fosse um simples tubo funcionando como um filtro de pacote. Uma vez que os endereços IP e MAC de outros computadores conectados são encontrados para serem autenticados, qualquer máquina pode falsificar o endereço MAC e IP do serviço autenticado, e poder dispor de uma rota através do *gateway*. Por esta razão, uma solução possível é criar mecanismos de autenticação estendidos para limitar o risco de usurpação (HINDLE, 2013).

*O hotspot* requer o uso de um navegador *web.* Este é geralmente o primeiro passo para que os usuários comecem a navegar na Internet, mas, se o usuário usar um programa específico para leitura de *e-mails* antes de abrir o navegador, vai perceber que a conexão não está funcionando. O acesso só será liberado quando o navegador for aberto e a conexão for validada. Um problema semelhante pode ocorrer se o cliente usa AJAX[5] *(Asynchronous JavaScript and XML*) ou se tentar navegar na rede com as páginas já carregadas em seu navegador, causando um comportamento indefinido quando essa página tenta solicitações HTTP para o seu servidor de origem (SONDAG; FEHER, 2007).

Plataformas que têm *Wi-Fi* e uma pilha TCP/IP, mas não têm um navegador *web* que suporta HTTPS, não podem usar um sistema de *hotspot*. Essas plataformas incluem o DS da Nintendo executando jogos que usam *Nintendo Wi-Fi Connection*. Uma autenticação sem navegador é possível usando WISPr (*Wireless Internet Service Provider roaming*), um protocolo baseado em XML (*eXtensible Markup Language*) de autenticação para esse fim, a autenticação baseada em MAC ou autenticações baseadas em outros protocolos (SONDAG; FEHER, 2007).

---

[5]AJAX *(Asynchronous JavaScript and XML*): O AJAX funciona carregando e renderizando uma página, utilizando recursos de *scripts* executados no lado cliente, buscando e carregando dados em *background* sem a necessidade de *reload* da página (ROSA, 2009).

### 4.3 Definição dos Perfis de Acesso

A Internet é um recurso de enorme potencial para a ampliação de serviços aos usuários. Tal como outras tecnologias da informação, a Internet é uma caixa preta a ser aberta para que seus recursos sejam explorados. O país tem a infraestrutura básica para tal e, sob parâmetros arquivísticos, torna-se premente explorar todas as possibilidades disponíveis para um acesso mais seguro e confiável (CONARQ, 2000).

O acesso à imensa quantidade de informações veiculadas pela Internet, aliada à crescente disponibilidade de acervos arquivísticos e bibliográficos em rede, faz com que os usuários tenham um amplo acesso a informações desnecessárias na *web*, sendo importante um controle de acesso para que *websites* desnecessários não sejam abertos, evitando assim supostos vírus e assuntos indesejados (CONARQ, 2000).

O *website* deve ser visto como um instrumento de prestação de serviços – dinâmico e atualizável – e não simplesmente como a reprodução de um folder institucional. Trata-se, na verdade, de um espaço virtual de comunicação com os diferentes tipos de usuários. Dado o potencial e as características da Internet, este espaço, além de redefinir as formas de relacionamento com os usuários tradicionais, poderá atrair outros que, por várias razões, dificilmente ou raramente procurariam o arquivo como realidade física (CONARQ, 2000).

Sendo assim, a acesso a *sites* seguros e de qualidade, com conteúdos relevantes e que realmente atendam aos interesses ligados às funções exercidas pelos usuários, é um problema a ser considerado, diante da amplitude e diversidade de *sites* existentes na Internet. Dessa forma, pretende-se com este trabalho, avaliar metodologias para avaliação de *sites*, por meio da análise dos critérios de avaliação dos usuários, com base na identificação das atividades exercidas conforme o setor correspondente de cada um. Assim, serão verificadas suas necessidades de acordo com as funções exercidas, para que os mesmos tenham acesso a informações externas e sistemas existentes para efetivação do seu trabalho. Dessa forma, cada perfil terá acesso ao conteúdo que corresponde as suas necessidades diárias, determinando as permissões de cada usuário após sua autenticação na rede. Pode-se, assim, definir os principais critérios de avaliação dos *sites* em que os usuários poderão ter acessos: conteúdo, objetivos do *site*; abrangência, propósito e funcionalidade.

Para a realização deste trabalho criou-se, para cada setor e/ou departamento da PMPM, um perfil de acesso à Internet. Os perfis poderão ser alterados pelos administradores do sistema. Em alguns casos específicos, o usuário poderá requisitar acesso diferenciado. Para isso terá que detalhar, por escrito, suas necessidades reais de acessos. Isso significa uma possibilidade de usuários, do mesmo setor, possuírem perfis diferentes. Alguns exemplos de setores da PMPM são: Arrecadação, Incra, Protocolo, Planejamento, Tesouraria, Assessoria de Imprensa, etc.

### 4.4 Criação do servidor *web*

A aplicação do método de gerenciamento teve início a partir de agosto de 2016, com a criação de um servidor *web*. Esse servidor *web* é o responsável por armazenar e trocar informações com os computadores da rede. Por exemplo, considerando um número mínimo de dois participantes envolvidos em uma troca de informações: um usuário, que solicita informações, e um servidor, que atende a esses pedidos, para que cada lado

funcione perfeitamente é necessário um programa especializado para gerenciar a troca de dados.

No caso do usuário, é usado um *browser*, como o *Google Chrome* ou o *Mozilla Firefox*. No lado do servidor, porém, existem várias opções de *softwares* disponíveis, mas todos têm uma tarefa semelhante: gerenciaratransferência de dados entre clientes e servidores via HTTP, o protocolo de comunicações da *web* (FIELDING; GETTYS, 1999).

Uma comunicação simples entre o usuário e o servidor *web* funciona da seguinte forma: o *browser* do cliente decompõe a URL em várias partes, tais como o nome de domínio, nome da página e protocolo. Por exemplo, para a URL http://www.xxx.com.br/xxx.php, o protocolo é o HTTP, o nome de domínio é www.xxx.com.br e o nome da página é xxx.php.Um servidor de nome de domínio (DNS) traduz o nome de domínio, informado pelo usuário, para seu endereço de IP, que é uma combinação numérica que representa o endereço real do *site* na Internet. Por exemplo, o domínio xxx.com.br é traduzido para 200.132.250.42. O *browser*, a partir disso, determina qual protocolo deve ser usado. Alguns exemplos de protocolos incluem FTP (*File Transfer Protocol*) e HTTP.

### 4.5 Desenvolvimento das regras

A parte da aplicação desenvolvida neste trabalho, em que são criadas as regras iniciais de controle, foi escrita em linguagem *script* no SO, testando-se em um Sistema Operacional *Ubuntu Linux*. Como suporte para armazenar os dados, foi utilizado o SGDB (Sistema Gerenciador de Bancos de Dados) *MySQL*, além da criação da página de *login*utilizando-se a linguagem de programação PHP. Com a integração do PHP com o *shell*, pela função “shell_exec” (nativa do PHP), foi possível um gerenciamento dinâmico nas regras de *firewall*.

Atendendo às finalidades deste projeto, foi criado um arquivo que faz as alterações iniciais de regras do sistema, sendo executado na inicialização do SO, a fim de que, ao iniciar o sistema, sejam executadas as rotinas a seguir descritas:

- Exclusão de todas as regras e *firewall* pré-existentes;
- Ativação do roteamento no SO;
- Redirecionamento do tráfego de todos os endereços IPs da rede para o sistema de autenticação;
- Criação das politicas de controle de tráfego;
- Verificação dos usuários que possivelmente estavam conectados e a reconexão deles (função usada para o caso de uma queda no sistema ou reinicialização do servidor).

## 4.6Aplicação do Método de Gerenciamento

Nesta seção serão detalhados os procedimentos necessários para iniciar a implementação do *hotspot*, método escolhido para este trabalho, utilizando um servidor RADIUS e a aplicação *CoovaChilli*. Esta aplicação é responsável por distribuir números IPs (serviço DHCP) e a página de autenticação aos utilizadores que se conectem via *Wireless* (sem fios) ao servidor. A partir da conexão, a aplicaçãoutilizando o*freeRADIUS* encarrega-se do registro e verificação da autenticação.

O *freeRADIUS* é uma implementação de RADIUS modular, de alta performance e rica em opções e funcionalidades. Esta inclui servidor, cliente, bibliotecas de desenvolvimento e muitas outras utilidades. Pode ser instalada em sistemas *Linux* e *Machintosh*. Devido a estas características e, tendo em conta o fato de ser uma aplicação *open source* (código aberto), esta será a implementação de RADIUS utilizada para o desenvolvimento deste trabalho(HASSELL, 2002).

### *4.6.1 Servidor de RADIUS*

O RADIUS (*Remote Authentication DialInUser Service*) é um protocolo utilizado para realizar autenticação segura a partir de um servidor de rede central, para usuários remotos que querem ter acesso a um sistema ou serviço de rede (HASSELL, 2002).

O RADIUS disponibiliza acesso à rede por meio de um protocolo *Authorization, Authentication, and Accouting* (AAA) e pode autenticar usuários e sistemas. O AAA tem três fases (SANCHES, 2005):

- Autenticação: as credenciais do usuário são comparadas com as existentes no banco de dados;

- Autorização: o acesso ao recurso é aceito ou recusado;

- Contabilidade: as informações são coletadas para realizar análise, auditorias, etc.

Normalmente em redes *wireless*, o RADIUS está presente nos *Access Points* que possuem segurança com autenticação nos padrões 802.1X ou 802.11i, pois ambos realizam o processo de autenticação por meio de um servidor RADIUS. Nos dois padrões, a autenticação entre o suplicante (estação de trabalho) o autenticador (neste caso, o *Access Point*) e o servidor de autenticação é realizada por meio do *Extensible Authentication Protocol* (EAP), podendo toda a comunicação ser realizada com a implementação de protocolos de segurança tais como EAP-MD5 e EAPTTLS (*EAP Tunneled Transport Layer Security*), entre outros (BAUER, 2005).

### *4.6.2 Instalação do freeRADIUS e a Base de Dados*

O primeiro passo para utilização do *freeRadius* envolve a criação da base de dados. A base de dados armazenará todos os dados dos utilizadores que serão definidos para autenticação no *freeRADIUS*. A estrutura das tabelas já são definidas por *default*, basta apenas realizar a criação da base de dados no *MySQL*, inserir as tabelas e definir os privilégios de acesso, como mostra o exemplo de da Figura 6. Para executar os comandos o usuário deve estar logado como *root*.

```
#myql –u root –p
enter password:
mysql> CREATE DATABASE radius;
mysql> quit;

# mysql –u root –p radius < /etc/freeradius/sql/mysql/schema.sql
# mysql –u root –p radius < /etc/freeradius/sql/mysql/nas.sql

#myql –u root –p
Enter password: mysqladminsecret
mysql> GRANT ALL PRIVILEGES ON Radius.* TO 'radius'@'localhost' IDENTIFIED BY 'mysqlsecret';
mysql> FLUSH PRIVILEGES;
mysql> quit;
```

**Figura 6 –Criação da Base de Dados (Fonte: dos autores; 2017)**

*4.6.3 Configuração do freeRADIUS*

A configuração do *free*Radius baseia-se na edição de alguns *scripts files.* Para realizar a configuração pode-se consultar ajuda na página oficial da ferramenta, no *link*<http://freeradius.org/doc/>ou pelo comando *man freeradius*. Usando um editor via terminal, tais como Nano ou Vi, deve-se editar o arquivo /etc/freeradius/sql.conf, por meio da linha de comando *# nano –w /etc/freeradius/SQL.conf.* Deve-se, então, editar as linhas referentes às informações do servidor, *login* e senha de acesso, como mostra o exemplo da Figura 7.

```
Server= "localhost"
Login= "root"
Password= "mysqlsecret"
```

**Figura 7 – Configuração do *freeRadius* (Fonte: dos autores; 2017)**

O próximo passo é editar o arquivo */etc/freeradius/clients.conf*, definindo a palavra-chave em "*secret*" para o *FreeRADIUS*, a palavra "*secret*" funciona como um comando padrão no *FreeRADIUS*, como podemos ver na Figura 8.

```
Client localhost {
Ipaddr = 127.0.0.1
Secret= radiussecret
}
```

**Figura 8 – Configuração dos Clientes do *freeRadius* (Fonte: dos autores: 2017)**

A seguir, deve-se editar o arquivo */etc/freeradius/user*se desfazer o comentário, isto é, apagar os símbolos # no arquivo para que o programa não ignore as linhas que estavam comentadas, a partir do comando *#nano -w /etc/freeradius/users.* Neste caso é

necessário apagar os símbolos para que os comandos desejados sejam executados sem problemas, desconsiderando as linhas “John Doe” que são padrão no *Ubuntu*. No arquivo *user*stambém é necessário apagar o símbolo # nas linhas, como é apresentadona Figura 9.

```
# "John Doe" Auth-Type := Local, User-Password == "hello"
# Reply-Message = "Hello, %u"
```

**Figura 9 – Configuração do arquivo *users* (Fonte: dos autores: 2017)**

Após a alteração, o sistema deve ser reiniciado, por meio do comando #reboot. Após reiniciar o sistema, deve-se fazer a alteração da autorização do “file” para “sql ”, isto é, ligar as contas e autorizações dos utilizadores no *freeRADIUS* à base dados (*radius*) criada no *MySQL*.Para isso, deve-se editar, novamente, o arquivo /etc/freeradius/sql.conf e excluir o comentário (#) na linha onde está escrito *#readclients = yes.*

O próximo passo envolve a edição do arquivo */etc/freeradius/sites-enabled/default*. Primeiramente, deve-se adicionar o cardinal (#), ou seja, comentar a linha de código onde se encontra a palavra “files”. Posteriormente, deve-se remover todos os comentários (#) onde se encontram as palavras “sql” nas respectivas seções, como mostra a Figura 10.

```
# VersãoInicial
Authorize {
        Files
#       SQL
}
Accounting {
#         SQL}
Session {
#         sql}
```

```
# Versão modificada
Authorize {
#        Files
       SQL
}
Accounting {
         SQL}
Session {
sql}
```

**Figura 10 – Configuração do arquivo inicial e sua versão modificada (Fonte: dos autores: 2017)**

Para finalizar a configuração é preciso editar o arquivo */etc/freeradius/radiusd.conf* e excluir o comentário (#) na linha que apresenta o comando *#INCLUDE SQL.conf.*

*4.6.4 Adicionar e testar o usuário*

Para verificar o funcionamento do *freeRADIUS*, deve-se testar o funcionamento de registro de usuários no *MySQL*para autenticação no *freeRADIUS*, registrar um usuário e verificar a conexão, como mostram os comandos da Figura 11.

```
#mysql –u root –p
Enter password:
Mysql>use radius;
Mysql> INSERT radcheck (UserName. Attribute, Value) VALUES (‘usuarioteste’, ‘Password’, ‘passteste’);
Mysql>exit;
Bye
```

**Figura 11 – Inserção de Usuários (Fonte: dos autores; 2017)**

Deve-se, então, reiniciar o *freeRADIUS* e testar a conexão, por meio dos comandos apresentados na Figura 12.

```
#/etc/init.d/freeradius restart
#radtest usuarioteste passteste 127.0.0.1 1812 radiussecret
```

**Figura 12 – Teste da Conexão (Fonte: dos autores, 2017)**

Caso o resultado do teste seja positivo, deve-se visualizar as informações apresentadas na Figura 13.

```
Sending Access-Request of id 94 to 127.0.0.1 port 1812
User-Name = “usuarioteste”
User-Password = “passteste”
NAS-IP-Address = 127.0.1.1
NAS-Port = 1812
Rad recv: Access-Accecpt packet from host 127.0.0.1 port 1812, id=94, length=20
```

**Figura 13 – Resultado da Conexão (Fonte: dos autores, 2017)**

Após serem realizados todos os passos apresentados nesta seção, o *freeRADIUS* e o *MySQL* já estão configurados.

*4.6.5 Instalação do CoovaChilli*

Após a instalação do *freeRadius* é necessário instalar o*CoovaChilli* e suas dependências. Esta aplicação é composta por um conjunto de regras de *IPTables* que faz o controle de acesso dos usuários por meio de uma página *web* de autenticação, além de realizar a distribuição de IPs (serviço DHCP). Mais informações sobre o *CoovaChilli* podem ser acessadas no *site*<http://coova.org/CoovaChilli>.

A configuração desta aplicação é baseada em um arquivo de configuração padrão, encontrado na pasta "*chilli"*, chamado "*defaults"*. Este arquivo deve ser copiado na mesma pasta com o nome de "config" e editado da linha 12 a 85 conforme as configurações da rede, do *RADIUS* e do *CoovaChilli*(COOVA.ORG, 2017).

Logo após deve-se criar dois diretórios (ou pastas) na pasta "www" localizada dentro da pasta *chilli*, chamados "images" e "uam". No segundo diretório são descarregados os arquivos responsáveis pela página *web* e configurados de acordo com as informações atribuídas à rede, como o IP, o *host* e porta. Antes de testar a configuração da aplicação ativa-se o ligamento automático durante o *boot* do SO no arquivo *chilli* encontrado na pasta "*default*" e em seguida, executa-se o debug do *chilli* para verificar possíveis erros.

Esta aplicação *web* possui uma página de *login*, aqual possui suas configurações específicas. Sendo assim deve ser descompactada do arquivo *hotspotlogin.cgi.gz* e nestearquivo configurar a palavra secreta do *chilli* colocada no arquivo *config*. A criação de um *VirtualHost* é indispensável para aceitar as conexões ao servidor, permitindo que ele funcione por meio de um arquivo de configuração no servidor *Apache*(APACHE, 2017).

Para o funcionamento adequado das autenticações é necessária a instalação e configuração dos arquivos da aplicação *Haserl*, responsável por criar *scripts* utilizando *shell* ou *Lua script*.

A instalação do portal de autenticação encerra-se com os comandos para ativação do serviço e reinicialização do servidor *webApache*. Após isso, complementa-se a customização final com a cópia do conteúdo que será mostrado aos usuários para a pasta do servidor, a cópia da imagem padrão do *Coova* e a inserção das devidas permissões aos arquivos utilizados pela aplicação.

### *4.6.6 Instalação e configuração do Haserl*

O *Haserl* é um pequeno programa que usa *shell* ou Lua*script* para criar *scripts* .CGI (*Common Gateway Interface*) em páginas *web*. Ele é destinado a ambientes onde os arquivosPHP podem ser muito grandes. É um complemento necessário para o funcionamento da autenticação do *CoovaChilli*, visto que é necessário suporte para visualização da página onde o usuário fará a autenticação. Mais informações sobre o *Haserl* podem ser encontradas no site <http://haserl.sourceforge.net/>.

Para instalar e configurar o *Haserl* é necessário fazer o *download* do arquivo com o comando: *cd /tmp && wget http://downloads.sourceforge.net/project/haserl/haserl-devel/0.9.27/haserl-0.9.27.tar.gz.* Logo após deve-se extrair o arquivo e instalar o programa no *root*. Após deve-se configurar o *Haserl* no *CoovaChilli*, editando o arquivo */etc/chilli/www*, e o arquivo */etc/chilli/up.sh*, adicionando as linhas de código no final do arquivo, como mostra a Figura 14.

```
# may not have been populated the first time; run again
[ -e "/var/run/chilli.iptables" ] &&sh /var/run/chilli.iptables 2>/dev/null
# force-add the final rule necessary to fix routing tables
iptables -I POSTROUTING -t nat -o $HS_WANIF -j MASQUERADE
```

**Figura 14 – Arquivo modificado utilizando o *Haserl* (Fonte: dos autores, 2017)**

Para concluir, deve-se atualizar os *scripts* para que tomem as funções definidas, com o seguinte comando: *#sudo update-rc.d chilli defaults.*

Após reiniciar o servidor deve-se verificar no *bootlog* se os serviços *chilli + freeradius + apache*estão iniciando com êxito. Em caso afirmativo, o servidor deve ser ligado à rede*wireless* ou pela interface eth1, para que seja possível verificar se o*CoovaChilli* está distribuindo IP´s e fornecendo a página de autenticação corretamente. Caso tudo esteja funcionando adequadamente o *hotspot* está configurado com sucesso.

## 5. Testes e Resultados

Para testar a configuração do ambiente implementado, visando verificar se está funcionando corretamente, é preciso executar o *debug*, por meio do comando #chilli –f –d no root.

Caso no *debug*seja indicado algum erro na configuração, deve-se usar o comando *netstat – pnl* para verificar o ID (identificador de processo). Este *debug* tem, como finalidade,a de encontrar e reduzir os erros e os *bugs* do sistema procurando corrigi-los (RACKSPACE, 2016).

Utilizando os recursos do *software Zabbix* foi possível monitorar e visualizar os relatórios de consumo de rede na PMPM-RS. O *Zabbix* é um *software* livre com a finalidade de monitorar redes e melhorar a qualidade de serviços tanto para o usuário como para os administradores de rede. A sua arquitetura e a flexibilidade dos módulos permite que a ferramenta seja utilizada para o monitoramento convencional, acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes mais complexos, por meio do servidor *Zabbix* e as regras de correlacionamento (ZABBIX,2015).

Com a ajuda do *Zabbix* pode-se ter uma ideia de consumo de Internet na PMPM-RS nos últimos 6 meses, como mostram os gráficos das Figuras 15, 16 e 17.

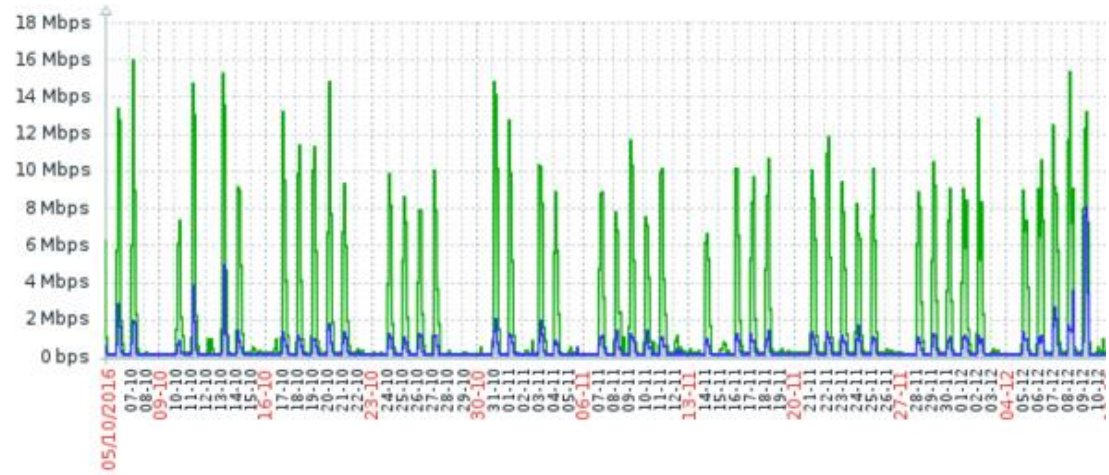


**Figura 15 – Gráfico com o consumo de rede entre 05/10/2016 e 10/12/2016**

**(Fonte: dos autores, 2017)**

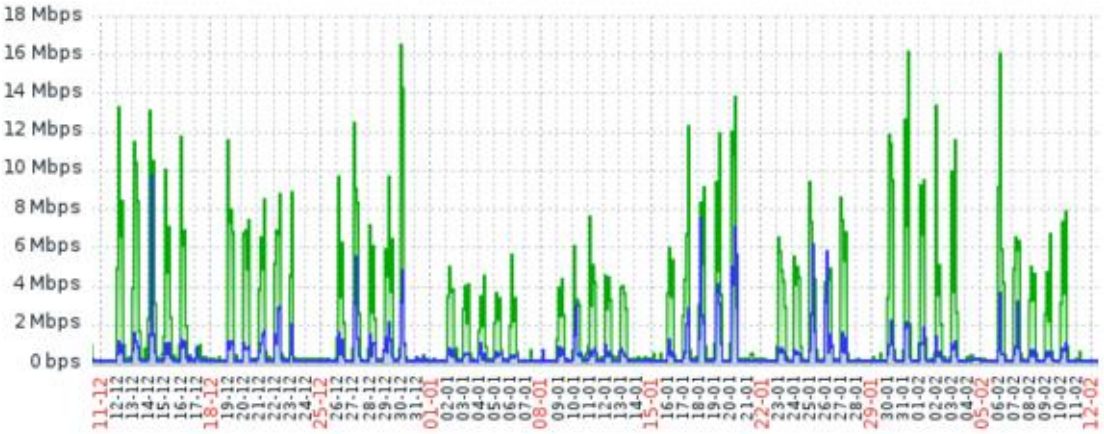


**Figura 16 – Gráfico com o consumo de rede entre 11/12/2016 e 12/02/2017**

**(Fonte: dos autores, 2017)**


**Figura 17 – Gráfico com o consumo de rede entre 13/12/2016 e 02/04/2017**

**(Fonte: dos autores, 2017)**

Como se pode observar, analisando os gráficos das Figuras 15, 16 e 17, o consumo de Internet durante os últimos 6 meses variou constantemente durante os meses, atingindo picos mais elevados de consumo de Internet.

Para que se possa ter uma ideia dos resultados que poderão ser atingidos com a implantação do sistema de gerenciamento e controle de acesso à Internet aqui proposto, definiu-se um setor hipotético com 4 computadores sendo eles denominados A,B,C, e D, sendo eles monitorados com o *Radius* e o *Zabbix*. Este método simulado foi proposto diante a falta de tempo de seus idealizadores de realizar a implantação completa em todos os setores, pois precisaria uma dedicação e cuidado extra, envolvendo todos os funcionários e departamentos dentro da PMPM-RS.

Os gráficos apresentados nas Figuras 18, 19, 20 e 21foram construídos após as permissões dos usuários hipotéticos terem sido configuradas adicionando restrições e bloqueios em *sites* mais comuns e mais acessados sem ter necessidades tais como, redes sociais (*Facebook*), *YouTube*, sites nocivos e com conteúdo considerado impróprio; sendo esses *sites* totalmente liberados o acesso em determinados momentos, para que se pudesse simular como o fluxo de rede aumentaria caso estes *sites* fossem liberados.

Tendo como base este setor hipotético, utilizando o sistema de controle de usuário nos computadores, a simulação mostra que o consumo de Internet na rede diminuiria de 30% a 50%. Por exemplo, na simulação do computador A (Figura 18), pode-se veriricar que, em cerca de 1 hora o consumo de Internet dobrou quando o seu usuário estava sem utilizar o sistema de controle, podendo acessar quaisquer *sites* na Internet, podendo navegar em *sites* desnecessários e fazer *downloads* de conteúdos na rede. Em outro caso o usuário iniciou o *download* de um arquivo e o controle de velocidade do tráfego foi feito em tempo real, aumentando ou diminuindo a velocidade conforme a qual foi configurada, sem a necessidade de pausar o *download* ou efetuar uma nova autenticação.

Com o controle de usuários também é possível monitorar e identificar usuários que, mesmo bloqueados, tentam acessar determinados *sites* indevidos com frequência, podendo assim geram advertências para este usuário.

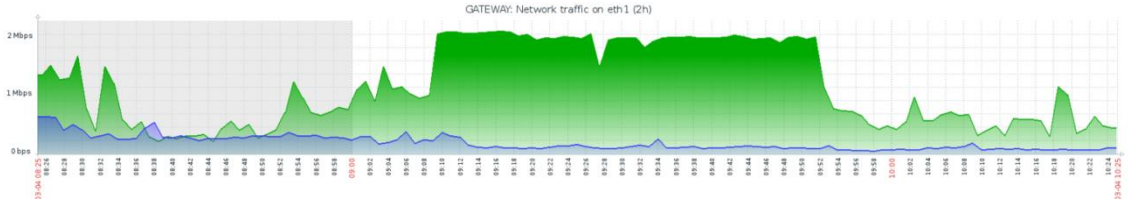


**Figura 18 – Gráfico com o fluxo de rede no computador A (Fonte: dos autores, 2017)**

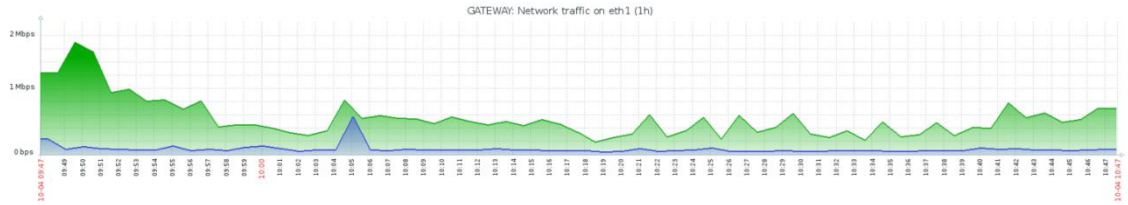


**Figura 19 – Gráfico com o fluxo de rede no computador B (Fonte: dos autores, 2017)**

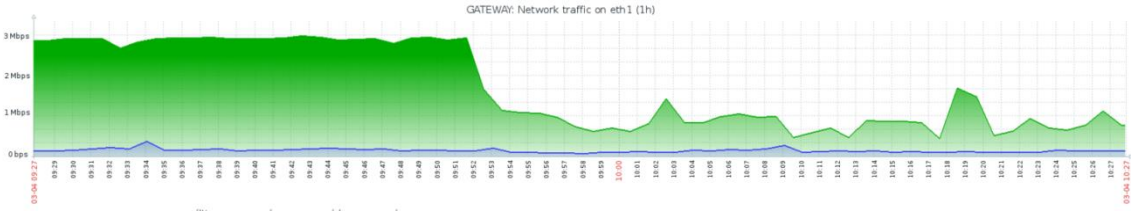


**Figura 20 – Gráfico com o fluxo de rede no computador C (Fonte: dos autores, 2017)**

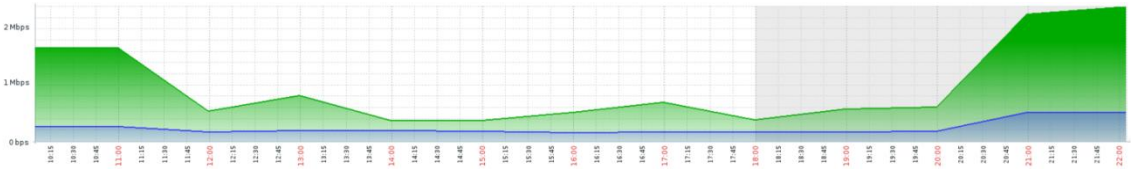


**Figura 21 – Gráfico com o fluxo de rede no computador D (Fonte: dos autores, 2017)**

Após todas as configurações e testes realizados, foi possível disponibilizar o *hotspot* totalmente gerenciado pelo RADIUS e trabalhando em conjunto com o *CoovaChilli*. Com estes *softwares*, além do usuário ter muito mais segurança no seu acesso ele irá se relacionar com uma interface de autenticação amigável, fornecendo agilidade para o seu acesso. O usuário, ao se conectar ao ponto de acesso previamente conectado na interface eth1, receberá as configurações de IP automaticamente e a indicação do uso da página de autenticação para a liberação do acesso. O usuário ainda não estará permitido a navegar na Internet, sendo solicitado a inserir seu nome de usuário e senha no portal do *CoovaChilli*na página, como mostra a Figura 22.

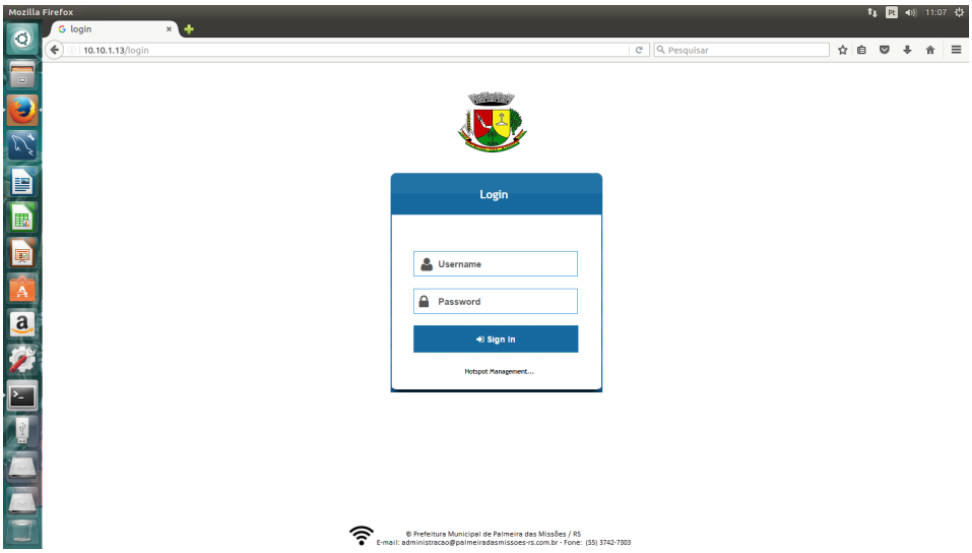


**Figura 22 – Tela de *login* de usuário para acesso àInternet na PMPM-RS (Fonte: dos autores, 2017)**

## 6. Considerações Finais

Este trabalho teve, como objetivo principal, o de identificar e aplicar o método mais adequado para autenticação no contexto da rede de computadores da PMPM-RS. Para tanto, realizou-se um estudo de caso envolvendo todos os setores da PMPM-RS, definindo critérios de avaliação dos perfis de usuários que tem acesso à Internet, identificando situações-problema ocasionadas pela falta de controle de acesso à rede de computadores, tais como o perigo de ter acesso a *sites* nocivos com risco de receber SPAM, que contenham vírus e *malwares*, redes sociais que venham a atrapalhar o rendimento tanto dos funcionários como a quantidade de banda de internet que será consumida ocasionando, assim, uma possível lentidão da rede, e *sites* que contenham conteúdos considerados impróprios para um setor de trabalho.

No processo de desenvolvimento deste trabalho foram encontradas dificuldades quanto à falta de textos e exemplos sobre o assunto proposto. Os autores também tiveram dificuldades devido à falta de tempo para estarem presentes na PMPM-RS, local onde a implementação da autenticação por portal foi proposta. Mas isso foi superado aos poucos, graças à dedicação e ajuda principalmente dos funcionários do Departamento de Informática da Prefeitura, sendo realizadas as atividades, não da maneira que se tinha previsto no começo do projeto, mas apresentando bons resultados quanto às necessidades existentes na PMPM-RS.

A implantação de um sistema para controlar e registrar o acesso dos usuários possibilita uma melhor segurança e controle dos acessos e, também, maior qualidade na questão de acesso à rede e na velocidade de tráfego, diminuindo principalmente a demanda de suporte no setor de informática da PMPM-RS, responsável pelo atendimento aos usuários.

Durante a realização desse trabalho notou-se que é necessário entender melhor como a organização funciona para compreender todas as necessidades dos funcionários

em relação às informações que podem ou não ser acessadas via rede. Isso acaba tendo uma grande resistência dos funcionários, principalmente dos mais antigos que não compreendem muito bem como funcionará o controle de acesso à Internet.

Após a definição do método mais adequado de controle de acesso, realizou-se a simulação da aplicação do sistema de gerenciamento em um setor hipotético tendo em vista o controle de usuário com e sem o bloqueio de acesso a internet. A realização de testes ocorreu conforme a política de segurança da PMPM-RS, considerando o perfil e as necessidades de um determinado funcionário, visando ter melhor segurança e melhor qualidade no acesso à Internet.

Este trabalho possibilitou a implementação de uma ferramenta muito eficiente no propósito a que se destina: controlar o acesso à Internet, efetuado por usuários utilizando rede sem fio ou rede cabeada, além de proporcionar um maior conhecimento sobre *firewalls*.

O aplicativo de autenticação *FreeRadius* apresenta-se como uma opção adequada para implementação de controle de acesso à Internet, atingindo os objetivos específicos propostos, liberando o acesso só aos usuários autenticados, garantindo assim a segurança de banda de redes cabeadas e não cabeadas, ou simplesmente o controle dos usuários que devem utilizar deste recurso dentro da instituição.

Os resultados alcançados até o presente momento servem de base para uma ferramenta que possui abertura para agregar novas funcionalidades assim fornecendo uma solução adequada, não apenas para um mecanismo de segurança que possa autenticar um usuário, mas também é uma solução que pode informar quais os serviços disponíveis, qual o tamanho de consumo de banda por usuário, informando assim registros para possíveis auditorias.

A aplicação utilizada até o presente momento é válida, pois fornece subsídios para implementações de versões futuras. Para isso verifica-se a necessidade de um estudo aprofundado das tecnologias e ferramentas utilizadas, bem como a do próprio projeto, para dar continuidade ao desenvolvimento de aplicações futuras.

## Referências


3Com. (2006). **3Com *Switch 5500 Family Configuration Guide***. Disponível em: <http://h20628.www2.hp.com/km-ext/kmcsdirect/emr_na-c02581968-1.pdf>. Acesso em 31 de outubro de 2016.

APACHE. (2017) **Apache.** Disponível em: <http://https.apache.net>. Acesso em: 16 de Março de 2017.

BAUER, M. (2005)**Paranoid Penguin Securing WLANs with WPA and FreeRADIUS, Part I**, Março, 2005.Disponível em: http://www.linuxjournal.com/article/8017

BEGNAMI, V. L.; MOREIRA, J. (2013) **Segmentação de Rede Local Utilizando VLAN, com foco em segurança e Desempenho**. Disponível em:

<http://revistatis.dc.ufscar.br/index.php/revista/article/view/46/47T.I.S.> Acesso em 10 de abril de 2016.

BLUEPHOENIX. (2008) "**Boas práticas de segurança**". Disponível em: <www.bluephoenix.pt.> Acesso em 18 de maio de 2016.

BROWN, E. (2007) **Lyle.802.1x Port-Base Authentication**. United States of America: Taylor & Francis Group.

CARRION, D. (2005). **Avaliação de protocolos de autenticação em redes sem fio.** Rio de Janeiro: Universidade Federal do Rio de Janeiro. Disponível em: <http://www.ravel.ufrj.br/arquivosPublicacoes/tese_demetrio.pdf>. Acesso em 14 de abril de 2016. Tese.

CARVALHO, I. R. F. (2011) **Segurança da Informação:** Um Instrumento para Avaliação do Plano de Continuidade do Negócio Aplicado em Uma Organização Pública**.** Disponível em: <http://www.bsi.ufla.br/wpcontent/ uploads/2013/07/ItaloRFCarvalho.pdf>. Acesso em 19 de maio de 2016.

CERT.br. (2003) **Práticas de Segurança para Administradores de Redes Internet**. Disponível em: <http://www.cert.br/docs/ seg-adm-redes/seg-adm-redes.html>. Acesso em 28 de maio de 2016.

CERT.br. (2006) **Cartilha de Segurança para Internet.** <http://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf> Acesso em 09 de junho de 2016.

CERT.br. (2009) **Segurança da Internet no Brasil e Atuação do CERT.br.** Disponível em: <http://www.cert.br/docs/palestras/certbr-prodesp2010.pdf> Acesso em 09 de junho de 2016.

CERT.br. (2015) **Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança do Brasil.** Disponível em: <http://www.cert.br/docs/seg-adm-redes/segadm-redes.html#subsec2.1>. Acessoem 25 de maio de 2016.

CHEN, W. L. (2010) **A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal**. Graduate Institute of Communication Engineering.Disponívelem<http://journals.sfu.ca/apan/index.php/apan/article/view/ 80>.Acesso em 15 de junho de 2016.

COOVA.ORG (2017)***CoovaChilli.*** Disponível em: <http://coova.org/CoovaChilli>. Acesso em: 16 de Março de 2017.

COMER, D. E. (2007) **Redes de Computadores e Internet**. Porto Alegre: Bookman.

CONARQ - CONSELHO NACIONAL DE ARQUIVOS, (2000). **Diretrizes gerais para a construção de websites de instituições arquivisticas**. Rio de Janeiro:

Disponível em: <http://www.arquivonacional.gov.br/pub/virtual/diretrizes.htm>. Acesso em 16 de junho de 2016.

ENGST, A; FLEISHMAN, G. (2005) **Kit do Iniciante em Redes Sem Fio**: O guia prático sobre redes Wi-Fi para Windows e Macintosh. 2. ed. São Paulo: Pearson Makron Books..

FLECK, B.; POTTER, B. (2002).**802.11 Security.** Ed. O'Reilly.

FIELDING.; GETTYS.; (1999) **Hypertext Transfer Protocol -- HTTP/1.1** Disponível em: <https://www.rfc-editor.org/info/rfc2616> Acesso em 08 de novembro de 2016.

GOODRICH, M. T.; TAMASSIA, R. (2013) **Introdução à Segurança de Computadores.** Porto Alegre: Bookman.

HASSELL, Jonathan et al. RADIUS. Editora O'Reilly, outubro. 2002.

HUGHES, A. (2013) **Seis componentes básicos de uma rede de computador.** Disponível em: <http://www.ehow.com.br/seis-componentes-basicos-rede-computadores-info51378/>. Acessoem 11 de abril de 2016.

HINDLE, A. (2013) **SWARMED:** Captive Portals, Mobile Devices, and Audience Participation in Multi-User Music Performance.Department of Computing Science University of Alberta Edmonton. Alberta, Canada. Disponível em <http://nime.org/proceedings/2013/nime2013_62.pdf>. Acesso em 15 de junho de 2016.

MARCELO, A. (2005)**Squid**: configurando o proxy para Linux. 4. ed. Rio de Janeiro: Brasport.

MORIMOTO, C. E. (2011) **Redes:** Guia Prático. Porto Alegre: Sul Editores.

MOLINA, D.; SILVEIRA S. R.; SANTOS, F. B. (2015) **Implantação de Um Ambiente de Segurança de Redes de Computadores:** um estudo de caso na Prefeitura Municipal de Palmeira das Missões – RS.Universidade Federal de Santa Maria (UFSM/CESNORS) – Frederico Westphalen – RS – Brasil. Trabalho de Graduação em Sistemas de Informação. Disponível em: <http://w3.ufsm.br/frederico/images/ImplantacaodeumAmbientedeSegurancadeRedesdeComputadoresUmEstudodeCasonaPrefeituradePalmeiradasMissoes.pdf>Acesso em 12 de Junho de 2016.

NED, F. (1999). **Ferramentas de IDS.** Disponível em: <http://www.rnp.br/newsgen/9909/ids.html>. Acesso em 12 de Junho de 2016.

NEVES F. C.; MACHADO L. A.; CENTENARO R. F.; (2014) **Implantação de *Firewall PfSense.*** Universidade Tecnológica Federal do Paraná Departamento Acadêmico de Eletrônica - Curso Superior de Tecnologia em sistemas de

Telecomunicações. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/3968/1/CT_COTEL_2014_2_02.pdf>. Acesso em 12 de Junho de 2016**.**

PEIXOTO, M. C. P. (2004) **Gestão da segurança da informação no contexto da vulnerabilidade técnica e humana inserida nas Organizações.** UNITRI – Centro Universitário do Triângulo Pró- Reitoria de Ensino de Graduação Curso de Ciência da Computação. Disponível em: <https: //e3baea88-a-62cb3a1a-s-sites.googlegroups.com/site/pedronunots/Home/academico-3/auditoria-de-seguranca-e-sistemas-de-informacao/artigos-relacionados/contexto_da_vulnerabil.pdf>. Acesso em 12 de Junho de 2016.

RACKSPACE (2017) ***Check listening ports with netstat***. Disponível em: <https://support.rackspace.com/how-to/checking-listening-ports-with-netstat/>. Acesso em 02 de maio de 2017.

ROSA, E. (2009) **O que é o AJAX e como ele funciona.** Disponível em: <http://codigofonte.uol.com.br/artigos/o-que-e-o-ajax-e-como-ele-funciona> Acesso em 17 de junho de 2016.

SANCHES, C. A. et al. (2005) **Projetando Redes WLAN:** Conceitos e Práticas. São Paulo: Érica.

SÊMOLA, M. (2003) **Gestão da Segurança da Informação.** Rio de Janeiro: Campus.

SILVA, R. M. (2012) **Estudo de caso:** Autenticação IEEE 802.1x aplicada á Rede Ethernet da Câmara Legislativa do Distrito Federal. Disponível em: <http://repositorio.uniceub.br/bitstream/235/8135/1/5091083.pdf> Acesso em 8 de Maio de 2016.

SONDAG, T.; FEHER, J. (2007) **OpenSource Wifi Hotspot Implementation**.Information Technology and Libraries. Disponível em: <http://crawl.prod.proquest.com.s3.amazonaws.com/fpcache/14bb83ed7ff3950ef024f7c4996012c0.pdf > Acesso 15 de Junho de 2016.

STATO FILHO, A. (2009) **Linux**: Controle de Redes. Florianópolis: Visual Books.

TANENBAUM, A. S.; WETHERALL, D. (2011) **Redes de Computadores**. São Paulo: Pearson Prentice Hall.

TANENBAUM, A. S. (2003) **Redes de Computadores.** 4. ed. Amsterdam, Campus.

VIEGAS, M. P. (2009) **Modelo OSI.**Redes Cisco Para Profissionais, FCA.

WENDELL O. (2008) CCIE Nº. 1624. CCENT/CCNA ICND1. **Guia Oficial de Cerificação do Exame**. Segunda Edição. Rio de Janeiro.

YIN, R. K. (2001) **Estudo de Caso:** planejamento e métodos. 2. ed. Local: Bookman.

ZABBIX.(2015). **The Enterprise-class Monitoring Solution for Everyone**.Disponível em: <http://www.zabbix.com/download.php>. Acesso em: 04 de Abril de 2017.