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

FERRAMENTA DE CONTROLE DE ACESSO PARA EVITAR A DISPERSÃO DE ALUNOS EM AULAS PRÁTICAS EM LABORATÓRIOS DE INFORMÁTICA

TRABALHO DE CONCLUSÃO DE CURSO

ANTÔNIO CARLOS MISSIO JÚNIOR

Santa Maria, RS, Brasil
2015

FERRAMENTA DE CONTROLE DE ACESSO PARA EVITAR A DISPERSÃO DE ALUNOS EM AULAS PRÁTICAS EM LABORATÓRIOS DE INFORMÁTICA

ANTONIO CARLOS MISSIO JUNIOR

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Tecnologia em Redes de Computadores do Colégio Técnico Industrial de Santa Maria, da Universidade Federal de Santa Maria (UFSM, RS), como requisito parcial para obtenção do grau de **Tecnólogo em Redes de Computadores**.

Orientador: Prof. Me. Miguel Augusto Bauermann Brasil

Santa Maria, RS, Brasil
2015

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

A Comissão Examinadora, abaixo assinada,
aprova o Trabalho de Conclusão de Curso

FERRAMENTA DE CONTROLE DE ACESSO PARA EVITAR A DISPERSÃO DE ALUNOS EM AULAS PRÁTICAS EM LABORATÓRIOS DE INFORMÁTICA

elaborado por
Antônio Carlos Missio Júnior

como requisito parcial para obtenção do grau de
Tecnólogo em Redes de Computadores

COMISSÃO EXAMINADORA

Prof. Me. Miguel Augusto Bauermann Brasil
(Presidente/Orientador)

Viviane Cátia Köhler
(UFSM)

Fábio Teixeira Franciscato
(UFSM)

Santa Maria, 9 de dezembro de 2015

DEDICATÓRIA

Dedico este trabalho a minha família por todo apoio e incentivo durante este tempo, mesmo estando tão longe sempre me estiveram junte de mim. Obrigado por compreenderem a minha falta em diversos momentos.

E a minha companheira das longas noites de estudo Vanessa Zucco, obrigado por estar sempre ao meu lado pelo respeito e amparo nos momentos de dificuldade.

AGRADECIMENTOS

Aos professores do Curso de Redes de Computadores por transmitirem os seus conhecimentos necessários para que consegui-se chegar até aqui.

Aos meus amigos e colegas que apoiaram na realização e conclusão deste trabalho Rafael Copatti e Alberto Fansisco Kummer Neto principalmente, por me ajudar na elaboração dos códigos e realização dos testes.

Aos meus amigos da minha cidade natal Silvio Dance, William Patzer e ao Jean Carlos Gasparotto por me apoiarem deste o início da graduação.

Aos professores da banca que se dispuseram de seu tempo para se fazer a avaliação deste trabalho. Em especial ao meu professor-orientador Miguel Augusto Bauermann Brasil, por aceitar orientar o projeto, aos puxões de orelha, conselhos e acreditar que era possível concluir este trabalho, sou enormemente grato por tudo.

Para obter sucesso,
não é necessário muita coisa.
Somente ter paixão
por aquilo que você faz...
E fazer bem feito!

(Autor desconhecido)

RESUMO

Trabalho de Conclusão de Curso
Colégio Técnico Industrial De Santa Maria
Curso Superior de Tecnologia em Redes de Computadores
Universidade Federal de Santa Maria

FERRAMENTA DE CONTROLE DE ACESSO PARA EVITAR A DISPERSÃO DE ALUNOS EM AULAS PRÁTICAS EM LABORATÓRIOS DE INFORMÁTICA

AUTOR: Antônio Carlos Missio Júnior
ORIENTADOR: Miguel Augusto Bauermann Brasil

Este trabalho visa o desenvolvimento de uma ferramenta que proporcione uma fácil utilização do software de gerenciamento no controle de acesso em nível de rede, sem a necessidade de possuir um grande conhecimento técnico na área administração de redes. A ferramenta foi idealizada a partir da necessidade de inserir uma interface que ajude ao usuário, sem a necessidade de conhecimentos avançados em sistemas GNU/Linux, sobre o *software* Proxy Squid. Tendo em vista que toda a administração dos *softwares* voltados a área desta plataforma dá-se via console, exigindo certa familiaridade na manipulação de comandos em modo texto de seus usuários. Outro fator que impulsionou a criação e desenvolvimento foi a necessidade de realizar um controle mais efetivo sobre a disponibilidade de acesso aos alunos durante o período letivo em aulas práticas em laboratórios de informática, onde o professor passa a ser o administrador da rede. Com a utilização desta ferramenta o professor conseguirá disponibilizar somente o conteúdo de sua aula, evitando que seus alunos se dispersem em sua aula com conteúdos adversos na internet.

Palavras chave: Interface interativa; *Proxy* Squid; Controle de Acesso; Monitoramento.

ASTRACT

Completion Of Course Work
Industrial Technical School Industrial De Santa Maria
Course of Technology in Computer Network
University Federal de Santa Maria

ACCESS CONTROL TOOL TO AVOID WASTING STUDENTS IN PRACTICAL COMPUTER CLASSES IN LABORATORIES

AUTHOR: Antônio Carlos Missio Júnior
SUPERVISOR: Miguel Augusto Bauermann Brasil

This work aims to develop a tool that provides an easy to use management software in the access control at the network level without the need to have a great expertise in the field of network administration. The tool was conceived from the need to insert an interface that helps the user without the need for advanced knowledge in GNU/Linux systems on the Squid Proxy software. Considering that the entire administration of the software-oriented area of the platform takes place via console, requiring some familiarity in handling commands in text mode of its members. Another factor that spurred the creation and development was the need for more effective control over the availability of access to students during the school year in practical classes in computer labs, where the teacher becomes the network administrator. Using this tool the teacher will be able to provide only the content of his lecture, preventing his students disperse in his class with adverse contents on the Internet.

Keywords: Interactive Interface; Squid Proxy; Access Control; Monitoring.

LISTA DE FIGURAS

LISTA DE APÊNDICES

ABREVIATURAS E SIGLAS

AAA	*Authentication, Authorization e Accounting*
CAI	*Computer Assisted Instruction*
DAC	*Discretionary Access Contol*
GCC	*GNU Compiler Collection*
GPL	*General Public License*
HMVC	*Hierarquical Model View Controller*
IP	*Internet Protocol*
LAN	*Local Area Network*
LDAP	*Lightweight Directory Access Protocol*
MAC	*Mantatory Access Control*
MVC	*Model View Controller*
OSI	*Open Systems Interconnection*
PHP	*Personal Home Page*
RBAC	*Role-Based Access Control*
TIC	Tecnologias da Informação e Comunicação
TCP	*Transmission Control Protocol*
URL	*Uniform Resource Locator*

SUMÁRIO

INTRODUÇÃO

O uso das Tecnologias da Informação e Comunicação (TIC) como internet, computador, dispositivos moveis entre outros são um ponto de partida para a construção de uma sociedade da informação, que proporciona grandes oportunidades e desafios para quem a utiliza como forma de auxílio na educação, pois a internet é um mar de conhecimento e informação (CGI.BR, 2013). O impacto da informática no meio educacional provoca mudanças no método de ensino e na educação (OLIVEIRA; FILIZOLA, 2008). O sucesso educacional não provém somente da inserção de novas tecnologias e de novas ferramentas pedagógicas, e sim da presença do professor, o qual está constantemente a procura de novos meios de melhorar a qualidade do ensino (OLIVEIRA; FILIZOLA, 2008). A utilização dos recursos tecnológicos para a educação desencadeia uma nova dinâmica educacional, que propicia mudanças nos paradigmas da forma de educar e transmitir o conhecimento.(MORAN, 2014)

As TIC's são vistas como ferramentas de otimização de conhecimento, mas que ainda precisam ser dominadas para melhores resultados (HACK, NEGRI, 2008). Segundo Moran (2014), se faz de suma importância que alunos e professores discutam e levantem questões relacionadas as pesquisas realizadas em aulas práticas dentro de laboratórios de informática, como: Qual profundidade dessas pesquisas? Quais as fontes e locais confiáveis para obter informações? Entre outros requisitos de elevada importância.

A internet proporciona facilidade na obtenção de informação, a qual motiva o aluno pelo deslumbre de inúmeros *links* e páginas com assuntos que possuem o conteúdo que se está sendo pesquisado. O professor como orientador das pesquisas em uma turma, por mais que se esforce ao seu máximo não possui a capacidade de monitorar a todo o momento o que cada um está a ver em seu computador, informação está que pode ser qualquer de qualquer tipo em sites inapropriados (GOMES, 2002).

Para poder utilizar a internet da maneira mais eficiente possível se deve ter uma certa cautela com relação aos conteúdos disponíveis devido ao acesso livre e

desenfreado, que torna cada vez mais necessário monitorar o acesso. Com isso, surgiram diversas ferramentas que implementam outras diversas funcionalidades como filtros na camada de rede e os *proxys*[1] na camada de aplicação, com base no modelo de referência TCP/IP (*Transmission Control Protocol Internet Protocol*) (TANEBAUM, 2009).

As novas tecnologias desenvolvidas para trabalhar com redes são desenvolvidas para operar em modo console de forma a restringir o manuseio a somente pessoas com elevado conhecimento técnico e computacional. Nesse sentido, o presente trabalho busca avaliar os pontos de reflexão das possibilidades trazidas pela Internet, com foco em uma possível solução para a seguinte pergunta: Como restringir o acesso dos estudantes de modo a guiar o aprendizado em aulas práticas, quando se encontram conectados à internet? E como o professor pode atuar como administrador do acesso de seus educandos?

1.1 Objetivo geral

Desenvolver uma ferramenta com base em *software* livre para que o professor possa realizar a liberação do acesso somente do conteúdo proposto em suas aulas.

1.2 Objetivos específicos

- Construir uma interface de fácil usabilidade de modo a auxiliar o professor na criação de regras de controle de acesso à internet para sua turma;
- Desenvolver *scripts* em PHP capazes de interagir diretamente com o *software Proxy* Squid, de forma a não tornar o professor dependente do

[1] Servidor responsável por intermediar uma requisição entre o cliente e o servidor original de um site.

suporte técnico;

- Em nível de rede, pretende-se otimizar ao máximo a velocidade da LAN e a latência no tempo de resposta no acesso do educando aos sites requeridos.

1.3 Justificativa

Em aulas práticas a utilização das ferramentas de buscas dispostas na internet gera um grande “mar de informação” para o aluno. De forma a dispersar-se da aula em conteúdos diversos e os quais não condizem com sua real finalidade (MORAN, 2014). Com a adoção do método de controle de acesso, espera-se uma melhora na aprendizagem, uma vez que o acesso as URL são controladas. Objetiva-se evitar distrações por parte dos educandos e poder denotar diferentes sites e locais para realizar consultas e pesquisas.

Com a implementação de uma interface que facilite a interação do professor com o *software*, este com pouco conhecimento técnico, possa trabalhar com o sistema responsável pela restrição de acesso de forma independente, de forma a arbitrar os endereços e palavras-chave que deseja realizar pesquisas. Em nível de rede, pretende-se otimizar a velocidade da LAN (*Local Access Network*) e a latência no tempo de resposta no acesso. Uma vez que, somente pessoas pré-cadastradas terão acesso à internet.

1.4 Estrutura do Trabalho

Este trabalho aborda a elaboração de uma ferramenta que possua uma interface que proporcione ao professor que será o administrador da rede em aulas práticas, uma experiência com o *software* de gerenciamento de rede *Proxy* Squid e o analisador de *logs*[2] SARG, voltado para o âmbito escolar. O presente trabalho está

[2] Registro de eventos relevantes num sistema computacional.

estruturado da seguinte maneira.

A primeira parte aborda uma revisão bibliográfica sobre os principais métodos de controle de acesso em rede combinado aos *softwares* escolhido para ser a base deste trabalho. A segunda parte descreve as linguagens de programação, sistema operacional, *frameworks* escolhidos para desenvolvimento, bem como todas as demais ferramentas necessárias para a elaboração do trabalho. A terceira aborda a interface demonstrando funcionalidades e *layout* do sistema WEB. E no último capítulo os resultados e conclusões finais referentes a testes realizados com a ferramenta e o sistema web.

2 REFERENCIAL TEÓRICO

Para um efetivo controle de acesso à internet pode-se utilizar de várias ferramentas, as quais permitem identificar o que e com qual ou qual máquina realizou determinado acesso a um site ou página Web em determinada hora ou período, assim informações de elevada importância poderão ficar armazenadas em arquivos, como *logs* (WOLF; SILVA, 2011). Os mecanismos de controle de acesso se propõem a definir permissões e regras afim, como já citado, prevenir possíveis acessos indevidos e identificar problemas causados pelo mau uso no momento da conexão.

O controle de acesso foi introduzido por Bautler W. Lampson em 1971, quando foi implementado o modelo Matriz de Acesso, o qual se mantém nos dias atuais como modelo de referência simples nas políticas de acesso (LENTO; FRAGA; LUNG, 2006). Com a evolução e necessidade acentuada dos sistemas se adequarem com as novas formas de representar e limitar o acesso a dados e aplicações por meio de enlaces de comunicação, novos modelos e tecnologias são implementados para que toda entidade possa ser identificada e autenticada antes do sistema conceder o acesso a um determinado usuário.

A fim de, concretizar um controle de acesso o qual fica responsável por arbitrar políticas de restrição se faz necessário a utilização de mecanismos de segurança. Estes mecanismos controladores executam códigos internos, cujo comportamento é expresso através de modelos de segurança (STALLINGS, 2008).

2.1 Internet na escola

A internet está integrada no cotidiano da população mundial na sua forma mais ampla, de maneira a se tornar um instrumento indispensável ao crescimento intelectual e econômico, com presença nos mais diferentes locais e possibilitando o acesso a qualquer indivíduo (SOUZA; SILVA, 2013). A utilização do computador na

educação como um novo meio de transmissão de conhecimento torna-se uma ferramenta de suma importância no desenvolvimento educacional.

Muitas escolas ainda não possuem um método estruturado de como utilizar as TICs, permanecem de certo modo perdidas em como utilizar as TICs na educação com seus alunos (MARINHO, 2001). Com a utilização de uma ferramenta que possa ser um auxílio para este problema, poderá abrir caminhos para um aprendizado para ambos os lados.

A internet é um mar de informação que todos podem contribuir para seu crescimento, um lugar onde pode-se publicar e ser autor de qualquer assunto, de forma a elevar qualquer indivíduo aos níveis de mesma potencialidade (CARVALHO, 2007). Levy (2001), cita em seu livro que uma criança que possua acesso à internet e consiga publicar algo se encontrará em pé de igualdade com qualquer outro indivíduo de maior escala hierárquica ou classe social. O uso da internet passa ser um sucedâneo das bibliotecas tradicionais, com o diferencial de apresentar-se mais atrativas e fáceis de realizar pesquisas e encontrar o que realmente se procura.

Na utilização das bibliotecas virtuais o conteúdo é mais dirigido, devido estar ligado a instituições de relevância acadêmica, científica e literária, que se torna um grande aliado na educação, principalmente, um importante canal para que todos tenham acesso à informação (PORTILHO; PINTO, 2012). Um problema enfrentado por parte dos educadores é trazer um maior estímulo aos alunos, a fim de instrui-los em novas formas de pensar e construir sua própria forma de buscar o conhecimento (NASCIMENTO, 2007).

2.2 Segurança e controle de acesso em rede

Em locais onde possui um grande número de equipamentos conectados à internet, por exemplo, escolas cuja sua maioria os usuários são alunos, adotar regras acesso e monitorar o que cada um está a acessar é uma importante atividade. Adotar medidas de controle neste ambiente escolar se torna indispensável, pois é de suma importância garantir confiabilidade, integridade dos

dados contidos de forma a caracterizar maior segurança da informação (WOLF; SILVA, 2011).

Segundo Stalling (2008), a Norma X.800 do modelo de arquitetura de segurança OSI define que um serviço oferecido por um protocolo da camada inferior, em sistemas abertos, no momento da comunicação e transferência de dados possa garantir segurança ao sistema. Para implementar um controle de acesso necessita-se de ferramentas e protocolos capazes de realizar a autenticação dos equipamentos conectados à rede e de usuários, além de, uma série de verificações quanto a integridade dos sistemas instalados nas máquinas (SILVA, 2011).

As ferramentas disponíveis para realizar o controle de acesso em sua maioria são de código livre, de forma a proporcionar um custo somente no hardware empregado e no treinamento de quem ficará responsável pelo gerenciamento do sistema (LUZ, 2011). Muitos dos mecanismos existentes trabalham sobre a arquitetura *Authentication, Authorization e Accounting* (AAA), referência os procedimentos para autenticação, autorização e contabilização de um ambiente que tenha os requisitos de acesso monitorados para prover uma maior segurança. Segundo Barros e Foltran (2010), padrão AAA está definido em três etapas.

- A autenticação valida a identidade de um usuário em um ambiente e verifica se ele deve ter acesso à rede;
- A autorização garante que somente usuários devidamente registrados terão acesso aos recursos disponíveis;
- Contabilização permite a coleta de informações referentes ao uso dos recursos disponíveis em um ambiente.

2.3 Modelos de controle de acesso

O controle de acesso em sistemas computacionais não é implementado somente no âmbito de proteger o acesso do sujeito a um objeto, mas possui como objetivo impor disciplina por meio de conceitos, metodologias e técnicas a fim de manter a integridade dos dados acessados. Os modelos de controle de acesso

correspondem ao comportamento das regras e algoritmos propostos na política de segurança, apresentados no conjunto de entidades e relacionamentos com a finalidade de representar de forma abstrata o funcionamento das regras sobre o sistema alvo (LENTO; FRAGA; LUNG, 2006).

Os modelos atualmente amplamente aceitos e utilizados para realizar o controle de acesso são descritos em três principais modelos*, Discretionary Access Contol* (DAC), *Mantatory Access Control* (MAC) e *Role-Based Access Control* (RBAC) (ARNAB; HUTCHISON, 2015).

- DAC o qual baseia-se na ideia de que o proprietário da informação deve determinar quem tem o acesso a ela. Este modelo permite a cópia de dados de objeto para objeto, mesmo que o acesso ao dado original seja negado;
- MAC o qual baseia-se na administração de segurança centralizada, a qual as regras ditadas de acesso à informação são incontornáveis. Este modelo possui maior usabilidade em locais que possuem dados com maior grau de sensibilidade para possuir acesso, o sujeito deve possuir um rótulo a fim de informar seu nível confiabilidade para obtê-lo;
- RBAC o qual baseia-se no direito de acesso aos objetos de acordo com a função ou papel do sujeito desempenha. Desta forma, o sujeito pode adquirir acesso a diferentes objetos em diferentes grupos.

2.4 Métodos de controle de acesso

Todo o sistema possui códigos e instruções que regem e seguem uma ordem de execução e ou de prioridade a ser executadas, denominadas de algoritmos. Um algoritmo é uma abstração da realidade, no âmbito computacional o algoritmo é transcrito em passos lógicos para que possam ser interpretados e executados por hardware e *software* ou algum outro sistema autômato capaz de executar tal código (BUFFONI, 2003). Desta forma, algoritmos de controle garantem o pleno funcionamento e restrição no acesso a determinadas informações contidas no

sistema, a permitir ou negar o acesso à leitura, escrita ou modificação dos dados, de acordo com regras estabelecidas(OBELHEIRO, 2008).

O controle de acesso se faz através da mediação da requisição de uma entidade ativa (um usuário ou processo corrente do sistema), a um objeto ou entidade passiva que possui os dados, ou seja, local que se encontra as informações requeridas. Para efetivar a requisição e realizar do acesso do sujeito ao objeto, a conexão passa pelo monitor de referência. Subsistema conceitual, o qual recebe todas as requisições, realiza uma consulta das instruções e regras para verificar se à solicitação de acesso poderá ser feita ou não (MACÊDO, 2012).

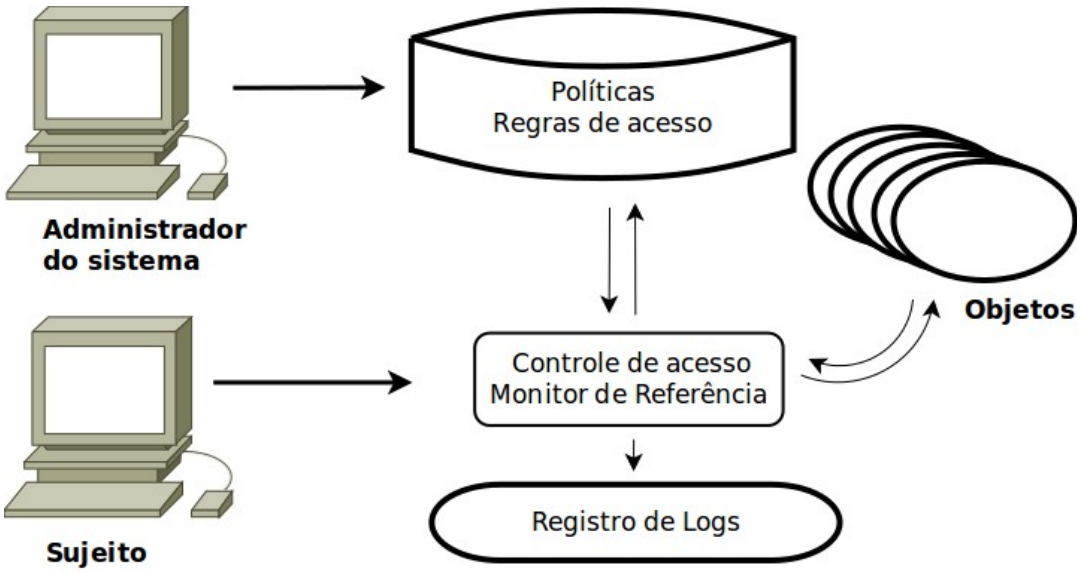


Figura 1 – Esquema de monitoramento de referência
Fonte: Elaborado pelo autor

Como apresentado na Figura 1, o monitor de referência realiza a mediação da conexão entre o sujeito e objeto, a fim de, realizar o acesso às políticas de controle programadas pelo administrador. Conforme as regras impostas, o monitor de referência permite ou nega seu acesso e todos os registros de acesso são mantidos em *logs* para fins de consulta.

O monitor de referências é o algoritmo responsável pela comunicação entre o sujeito e os objetos, que envolve um conjunto de instruções e mecanismos de hardware e *software*, tornando-se o núcleo de segurança (LENTO, FRAGA, LUNG,

2006). Este sistema pode atuar em vários níveis de um sistema que deve possuir algumas propriedades ser inviolável, incontornável estando sempre ativo, possuir poucas linhas de código, porém suficiente para que se possa realizar verificações e passíveis correções (OBELHEIRO, 2008).

2.5 *Proxy*

O *proxy* é um serviço executado em um ambiente servidor, o qual recebe as requisições das máquinas clientes para conexões com a Internet, o qual possui como principal funcionalidade, realizar buscas primeiramente em seu cache local e caso não encontre o documento requisitado, faz a busca no site solicitado pela máquina cliente (SIEWERT, 2007).

Este sistema realiza a comunicação por meio de intermediação entre a página requisitada, servidor se encontra a página ou documento, e a máquina cliente a qual realizou a requisição. O servidor *proxy* atua em nome da máquina cliente de forma transparente, proporciona desta forma o anonimato do requisitante, quebrando a conexão ponto a ponto (SQUID-CACHE, 2013).

Um sistema *proxy* pode atuar sobre diversos protocolos utilizados para comunicação cliente servidor, como páginas web, protocolos *Hyper Text Transfer Protocol* (HTTP), *Hyper Text Transfer Protocol Secure* (HTTPS), transferência de arquivos por protocolo *File Transfer Protocol* (FTP), correios eletrônicos através do protocolo *Simple Mail Transfer Protocol* (SMTP) entre outros. No entanto, a utilização de maior relevância de um servidor *proxy* é para a interceptação de conteúdos de páginas web e transferência de arquivos em rede (LOPES, 2006).

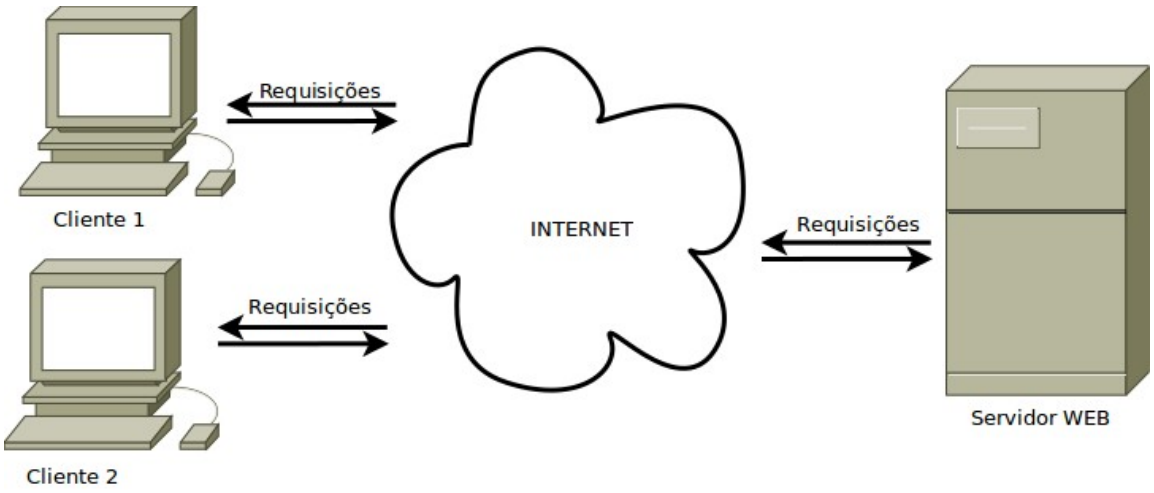


Figura 2 – Requisição Cliente para Servidor WEB sem *proxy*
Fonte: Elaborado pelo autor

O cenário apresentado na Figura 2 demonstra como é realizada a conexão entre a máquina cliente através do protocolo HTTP ou HTTP/S, para o servidor web de forma direta, sem que ocorra alguma nenhum controle ou verificação dos dados trafegados. Desta forma, propicia a quem estiver a utilizar qualquer máquina na rede interna acesso a qualquer tipo de dado ou informação ao meio externo, expondo sua máquina e a rede a ataques externos.

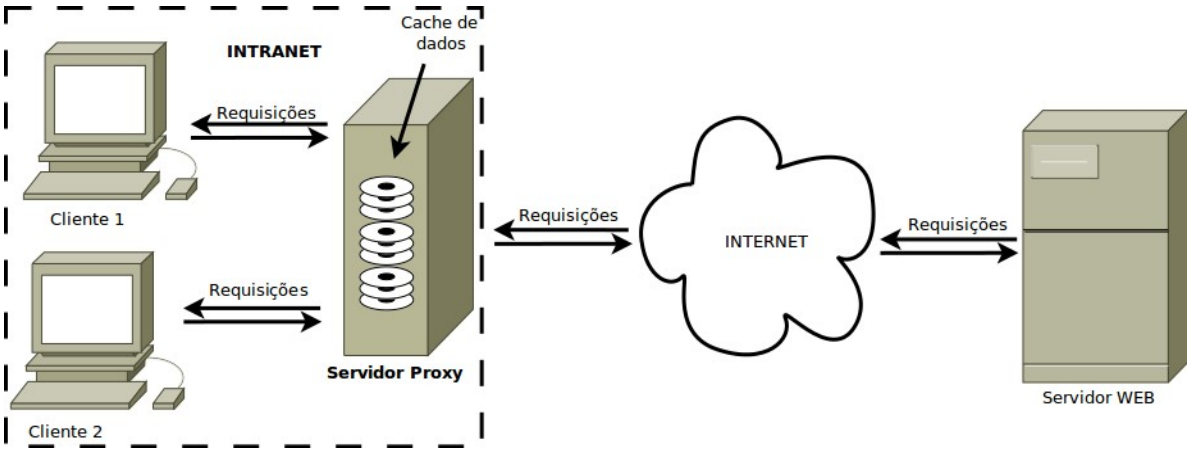


Figura 3 – Requisições controladas pelo Servidor *proxy*
Fonte: Elaborado pelo autor

Todas as requisições de acesso às páginas ou documentos web são realizadas primeiramente ao servidor *proxy*. O servidor *proxy* trabalha como cliente e servidor quase que simultaneamente. Atua como servidor ao receber uma solicitação de um cliente interno da rede e como cliente ao realizar comunicação com o servidor web, caso a página ou arquivo não esteja contido em seus cache de dados (PROXY, 2015).

Com a implementação de um servidor *proxy* é possível impor regras para usuários, grupos de usuários da mesma forma para determinados assuntos e conteúdo que trafegarão na rede. Também, dispor um aumento considerável, não somente no controle de acesso, mas também na segurança e diminuição na latência da rede (SILVA, 2007).

2.5.1 *Proxy* transparente / Não transparente

A utilização de *proxy* transparente livra o usuário de configurar manualmente seus *browsers* para utilizá-lo no acesso à internet, sem a necessidade de explicações de como fazer a configuração. Este método intercepta as solicitações de páginas WEB e as redireciona para o servidor *proxy* da rede, como forma a garantir que todos os usuários da rede realmente vão utilizar *proxy* ou que a conexão passará pelo servidor e suas regras de controle de acesso (MORIMOTO, 2009).

O *proxy* transparente possui uma arquitetura para que o navegador não saiba da existência do *proxy* na rede. O navegador acredita realizar a comunicação direta com o servidor original de sua requisição, enquanto servidor *proxy* é quem realiza a real comunicação, este método é denominado de sequestro de TCP ou TCP *hijacking*[3] (DUARTE, 2011).

Para a utilização de um *proxy* não transparente é necessário utilizar configuração manual, informando ao navegador qual seu endereço IP e porta a qual está atuando. Com a utilização do modelo não transparente, os *hosts* clientes não

[3] Código malicioso que sequestra algo, denominando-se dono.

necessitam estar ligadas diretamente a internet, somente configuradas para realizar as requisições para o servidor *proxy* e este se encarrega de realizar a comunicação final (DUARTE, 2011).

2.5.2 Cache *Proxy*

Conforme Watanabe (2000), cache é o local ou diretório onde os arquivos requisitados pelo servidor *proxy* são armazenados em um diretório dentro do sistema e posteriormente repassado a seus clientes da rede. O local é armazenado estes arquivos, deve ser constantemente monitorado, uma vez que, o disco ou diretório não esteja disponível o servidor poderá vir a falhar.

Os servidores de cache para comunicação entre servidores *proxy* realizam comunicação via *Internet Cache Protocol* (ICP). ICP é um protocolo de troca de mensagens de formato leve, possui como objetivo prover um método mais rápida e eficiente para obter objetos já cacheados em outros servidores (RFC2187, 1997).

Com a utilização do ICP, a transferência de dados e a comunicação se torna mais rápida por utilizar mensagens de tamanho a cerca de 66 bytes, para reduzir assim ao máximo a solicitação no servidor original do objeto requerido. Durante a requisição, os “vizinhos” enviam um HIT caso a comunicação foi bem-sucedida ou MISS, caso a comunicação seja perdida.

Desta forma, consegue-se uma percepção do estado da rede na volta, caso ocorra MISS, a rede encontra-se congestionada ou o *host* encontra-se inativo. Outra percepção pode ser obtida pela ordem de chegada de HIT, que ajuda a informar quais *hosts* estão em distâncias lógicas menores ou com menos carga de acesso (RFC2186, 1997).

Para controle de cache, os servidores *proxy* utilizam algoritmos de substituição, que realizam o monitoramento dos objetos contidos em memória do disco, conforme seu cabeçalho contendo as informações de período, tamanho e histórico de acesso (WATANABE, 2000). Estes algoritmos são utilizados a fim de monitorar o uso, para que novos objetos possam ser armazenados através dos

campos contidos nos cabeçalhos.

- *Last Recently Used* (LRU), algoritmo que verifica o período mais longo dos objetos utilizados, e estes são eliminados para conceder espaço a novos objetos de entrada (TANEBAUM, 2009).
- *Heapsort,* algoritmo em árvore, os nós de maior chave são sempre “pai” dos quais possuem chaves menores. Nós de menores chaves são excluídos.
- *Heap Greedy Dual Size Frequency* (GDSF), otimiza o "hit rate[4]" pois mantém objetos pequenos e populares no cache, os objetos de menor tamanho são excluídos.
- *Heap Last Frequency Used with Dynamic Aging* (LFUDA), otimiza o “byte hit rate[5]”, sua chave é calculada de acordo com a frequência de utilização e o tempo de permanência em cache.

Ainda os cache podem ser classificados em três categorias:

a) *Browser* cache: Cache próprio do navegador ou visualizador HTML do usuário.
b) *Proxy* cache: Sistema que compartilha os arquivos por vários usuários, atua como intermediário entre clientes e a Internet;
c) *Transparent Proxy* cache: Atua interceptando todo o tráfego do usuário com a Internet, sem a necessidade de configurações nos *browsers* dos usuários.

2.5.3 Filtros do *proxy*

Uma característica do sistema *proxy*, além da possibilidade do armazenamento de cópias das páginas Web em cache, é a possibilidade da criação de filtros. Os filtros são regras pré-determinadas pelo administrador, denominadas de *Access Control Lists* (ACL) (ROMMEL, 2007).

Os filtros trabalham para verificar quem ou com qual dispositivo requisitou um

[4] É a razão entre a quantidade de objetos servidos pelo *cache*, pelo total de objetos requisitados.
[5] É a razão da quantidade de *bytes* servidos pelo *cache*, pelo total de *bytes* requisitados.

determinado endereço Web. Segundo Rommel (2007), existem diversos tipos de filtros que podem operar junto ao sistema *proxy*, e modo a aumentar sua eficiência no controle de sites.

Estes filtros são denominados de filtros de conteúdo, que percorrem toda a página antes de ser entregue a seu destinatário, sendo eles:

- *Appliances* dedicados a filtragem, inclui dispositivos específicos e projetados para o monitoramento e controle de acesso à internet.
- Servidor pré-configurado para filtragem, os equipamentos possuem um propósito geral e já saem configurados de fábrica para desempenhar tal finalidade.
- Aplicação de filtragem baseada em servidor, programas que trabalham em conjunto com o sistema operacional como forma de plug-*ins* para aplicação do servidor *proxy*.
- *Addons* para serviço de filtragem no *firewall*, serviços adicionados ao sistema de *firewall*.
- Aplicação de filtragem baseada no cliente, plug-ins que podem ser instalados nos *browsers* dos clientes.

2.5.4 Vantagens e desvantagens da utilização de *proxy*

Com a utilização de mecanismos de controle e intermediação do acesso com o uso de sistema de *proxy*, consegue-se obter algumas vantagens e algumas desvantagens em relação às limitações a protocolos suportados.

- Redução do tráfego da rede e latência na requisição das páginas. Uma vez que um usuário realizar um acesso a uma página, esta estará disponível no servidor interno, e disponível aos demais. Desta forma, não será utilizada a banda para carregar o mesmo endereço web ou conteúdo diretamente da internet por outro usuário;
- Redução da carga dos servidores. É realizado um menor número de requisições a servidores web, diminuindo a possibilidade de

congestionamentos no momento do acesso;

- Possibilidade de acesso. Caso uma página encontra-se *off-line*, se está estiver em cache, consegue-se obter acesso à última informação disposta na página;
- Segurança no controle de acesso. Através de regras impostas, consegue-se monitorar e controlar o que poderá ser acessado e o que não dever ser acessado. Para maior efetivação no controle é necessário a utilização de implementação junto ao *firewall*;
- Poucos serviços suportados. Nem todos os serviços ou protocolos possuem suporte a servidores *proxy* atuais;
- Atualizações de sistemas internos da rede. Um número elevado de diferentes sistemas, poderá ocasionar sobrecarga ao servidor de cache, devido a uma grande requisição de atualizações dos equipamentos;

2.6 *Firewall*

O *firewall* é um sistema de controle de trafego ancorado em hardware ou *software*. Pode ser considerado como ponto de conexão entre duas redes não confiáveis, permitindo que toda a comunicação entre elas seja monitorada. Atua como a primeira camada de segurança, barreira que intercepta toda a conexão de entrada e saída de uma rede interna para externa ou da rede externa para a rede interna. (HARTHI, MASUD, 2013).

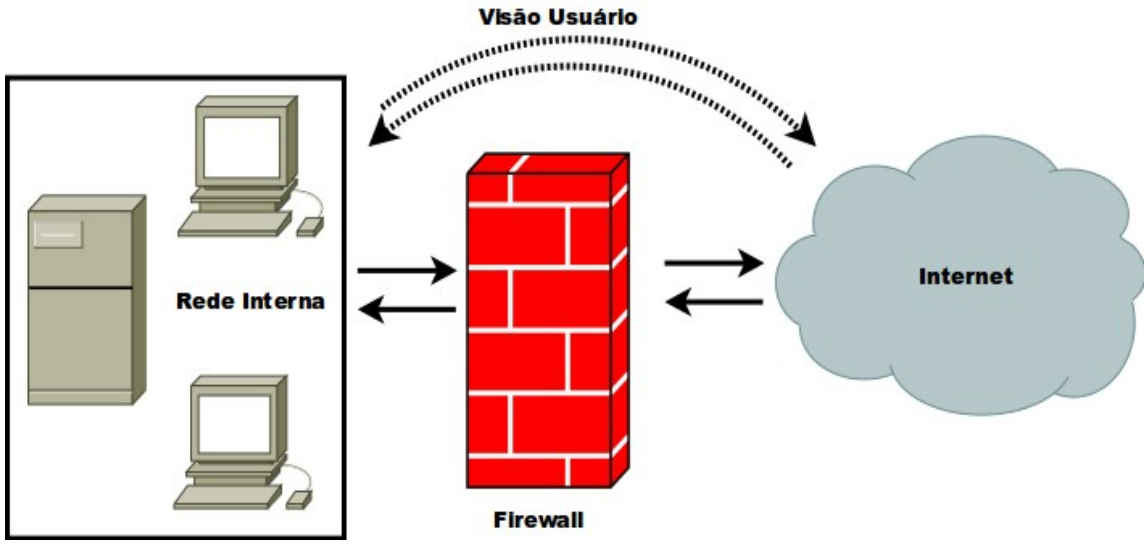


Figura 4 – Representação básica de um *firewall*
Fonte: Elaborado pelo autor

A Figura 4 demonstra um sistema básico de *firewall*. O sistema *firewall* consiste de maneira geral de dois componentes os filtros e um sistema de *gateway*[6], o qual fica responsável pela conexão entre as redes. As regras de filtragem são configuradas para permitir ou negar o tráfego de acordo com as características do pacote, como endereço de IP de origem e destino, tipo de serviço ou protocolo, tamanho, entre outros atributos. O *firewall* analisa as informações de cada pacote e realiza um comparativo com todas as regras impostas em sua lista, podendo realizar alguma tarefa relacionada, como a geração de *logs* (ALECRIM, 2013).

2.7 Arquitetura dos *firewalls*

O *firewall* consiste em um conjunto de regras, que realiza filtragem de pacotes que trafegam na rede. Para cada finalidade a ser empregado um *firewall*, deve-se adotar uma arquitetura específica. As arquiteturas recebem denominações

[6] Máquina ou conjunto de máquinas que oferece serviços através de *proxy*.

diferentes, por possuírem peculiaridades específicas para cada uma.

Os *firewalls* estão agrupados basicamente em três tipos de arquiteturas:

- *Dual-Homed Host*: *Host* que fica entre a rede interna e a rede externa, não possuindo outro caminho para acessar a rede externa a não ser por este. Possui no mínimo duas interfaces de rede, sendo o possível gargalo do acesso caso venha ficar sobre carregado e pondo em risco o a rede interna caso venha ser invadido, pode ser observada na Figura 4;

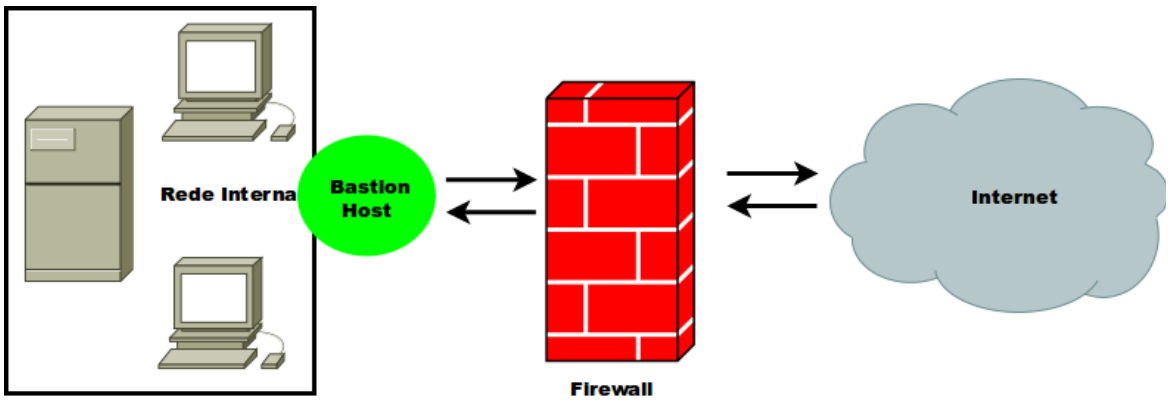


Figura 5 – Arquitetura *Screened Host*
Fonte: Elaborado pelo autor

- *Screened Host*: Arquitetura atuam dois *hosts*, um atua como *firewall* propriamente e outro como roteador da rede interna, não permitindo comunicação direta da rede interna com o *host firewall*, pode ser observada na Figura 5;

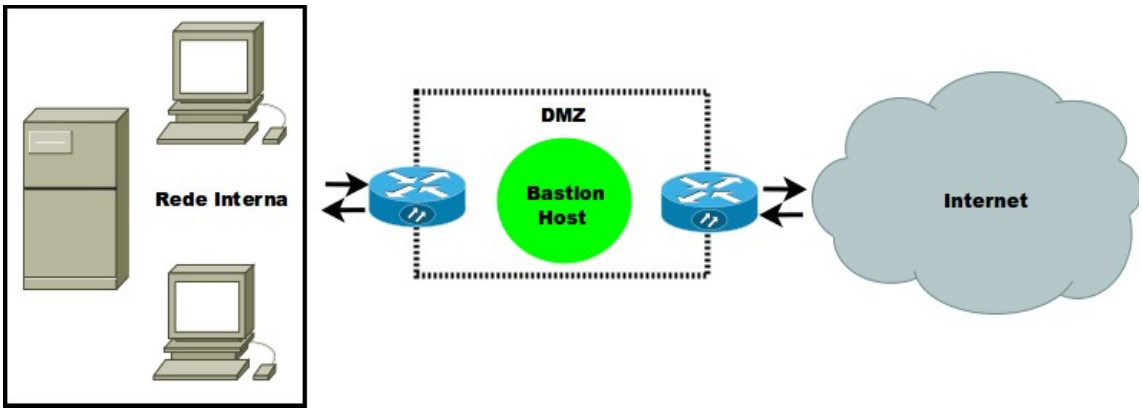


Figura 6 – Arquitetura *Scrrened Subnet*
Fonte: Elaborado pelo autor

- *Screened Subnet:* Atua como a arquitetura *Scrrened Host*, porém o host responsável por intervir a comunicação direta com o *host firewall* fica dentro de uma DMZ[7]. Entre a rede interna e a DMZ existe um roteador que trabalha com filtros de pacotes e entre a DMZ e a internet existe outro roteador com as mesmas configurações, pode ser observada na Figura 6.

[7] Subrede física ou lógica que contém serviços de conexões externas.

3 MATERIAIS E MÉTODOS

3.1 Sistema Operacional

Para emprego deste trabalho foi utilizado como sistema base, uma distribuição do sistema operacional GNU/Linux. Por ser um sistema de código aberto e que possui compatibilidade com diversas ferramentas e protocolos necessários para desenvolvimento do trabalho e no gerenciamento da rede utilizada como ambiente de teste.

O sistema GNU/Linux empregado em um *host* servidor centralizado, de forma a gerenciar e fornecer serviços a rede interna, como apresentado na Figura 3. Toda a comunicação dos clientes da rede interna obrigatoriamente passa por este sistema.

O sistema Linux originalmente foi elaborado para atuar como sistema operacional em servidores, compartilhado com muitos usuários e com diferentes serviços rodando simultaneamente. Os servidores podem ser divididos em dois grandes grupos, servidores de rede local e servidores de Internet (MORIMOTO, 2009).

a) Servidor local trabalha em uma rede compartilhando conexões e serviços (DHCP, impressão, arquivos, LDAP, entre outros) para uma rede LAN;
b) Servidores de Internet, mais conhecidos como servidores WEB, trabalham com hospedagem de sites e aplicações para serem utilizadas em qualquer parte da grande rede mundial de internet.

3.2 *Framework* CodeIgniter

CodeIgniter é um *framework* de desenvolvimento de aplicações em

linguagem PHP, o qual possui como objetivo, facilitar a utilização da linguagem no desenvolvimento de projetos. Sua estrutura possui conjunto de bibliotecas voltadas a tarefas mais comuns, para desenvolver projetos mais rápidos que construir do zero.

O *framework* permite ao desenvolvedor manter o foco no projeto de forma a minimizar linhas de códigos necessários para realizar determinada tarefa. O CodeIgniter foi desenvolvido sobre o paradigma de programação orientada a objetos sob padrão de arquitetura *Model Viewer Controller* (MVC), com suporte a metodologia *Hierarquical Model View Controller* (HMVC) (GABARDO, 2012).

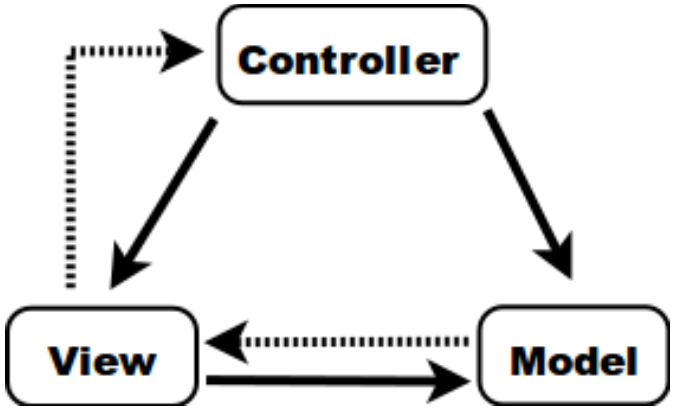


Figura 7 – Modelo MVC
Fonte: Elaborado pelo autor

O paradigma MVC é um padrão da arquitetura de *software* desenvolvido na engenharia de *software*, a qual separa a representação da informação da interação do usuário, de forma a tornar o sistema modular. A representação do modelo MVC pode ser observado na figura 7 demonstra um diagrama simples exemplificando como fica a estrutura do projeto (W3SCHOOLS, 2015). A linha contínua indica associação direta e as tracejadas indicam associação indireta.

- Modelo é a camada que representa os dados, o acesso à leitura e escrita. Toda a validação dos dados está dentro desta camada;
- Visualização é a camada a qual o usuário realiza a interação com o projeto. Realiza somente a manipulação dos dados para exibição. A

persistência e manipulação dentro do projeto é realizada pela camada de controle;

- Controlador é a camada que possui as ações referentes ao projeto. Realiza a interação entre a camada do modelo e a camada de visualização, de forma a determinar qual modelo utilizar, quais pedidos fazer a camada modelo e qual a combinação de visualizações aplicar.

O HMVC é tido como uma evolução do modelo MVC. A estrutura de funcionamento do modelo HMVC é como se houvesse um nível hierárquico, englobando cada tríade MVC dentro de um nível.

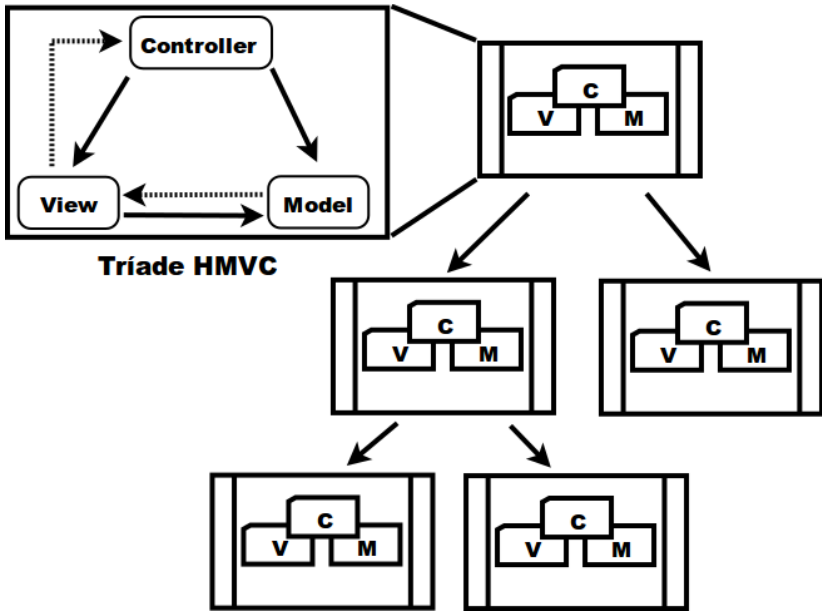


Figura 8 – Modelo HMVC
Fonte: Elaborado pelo autor

A principal vantagem da abordagem HMVC é a reutilização e praticidade dos códigos utilizadas. Caso necessário a utilização de algum módulo em outro projeto, somente é realizado uma cópia para o novo projeto, desenvolvendo novos projetos mais rápidos em curto prazo de tempo (ZEMEL, 2010).

3.3 *Personal Home Page* – PHP

Entre as diversas e diferentes tipos de linguagem de programação voltada para desenvolvimento de sistemas web, a linguagem de PHP. O PHP é uma linguagem que possui destaque na geração de projetos dinâmicos, facilidade de programar e segurança, em servidores (PHP, 2015).

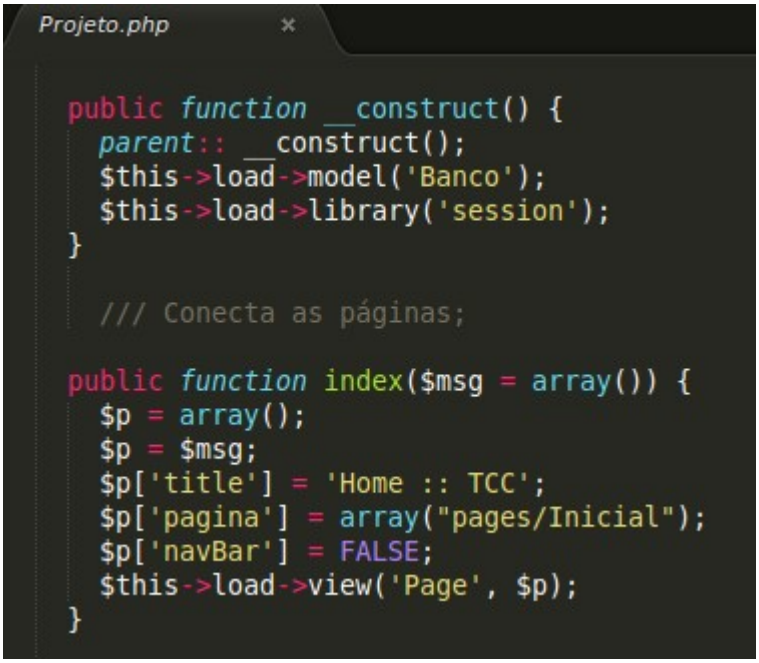


Figura 9 – Exemplo de código PHP
Fonte: Sistema de controle de acesso

Para interação com o *software* responsável por realizar e aplicar as regras de controle de acesso, foram elaborados códigos em linguagem PHP, dentro da estrutura do CodeIgniter.

3.4 *Hyper Text Markup Language* – HTML

O HTML é uma linguagem de marcação de textos utilizada na exibição de e formatação de páginas web, seu conteúdo é mostrado e interpretado pelo navegador (W3C). O HTML foi empregado para apresentação das páginas, bem como para todo o layout do sistema.

Venetianer (1997) cita em seu trabalho que o HTML é uma linguagem de programação simples, utilizada para criar documentos de hipertexto, suportada por várias plataformas computacionais. Foi incorporado a interface do sistema um designe responsivo, para assim, melhor a experiência do usuário com qualquer dispositivo independente da resolução de sua tela.

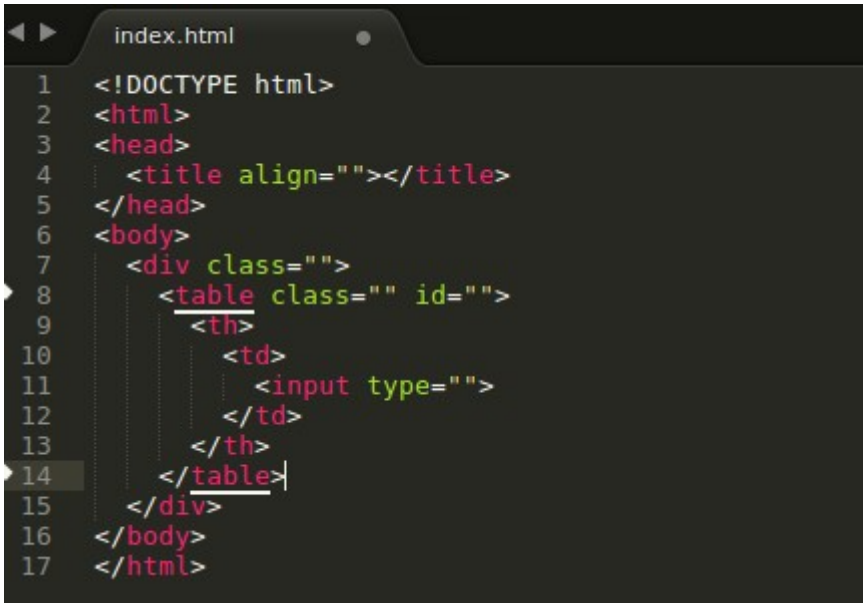


Figura 10 – Exemplo de código HTML

Exemplo de código HTML

3.5 Javascript

O *Javascript* é uma linguagem de programação utilizada para criar efeitos em páginas HTML, foi a primeira linguagem de *scripts* para web, utilizada principalmente para propiciar interatividade com os usuários. Códigos *Javascript*, como todo os códigos de um sistema web, ficam armazenados no servidor, mas diferentemente do PHP o *Javascript* é executado no lado cliente, no browser requisitante (SILVA, 2010).

Devido à necessidade de possuir uma interface responsiva, dinâmica e interativa com o usuário, o *Javascript* é uma importante linguagem empregada na construção da ferramenta.

vereficarCampos.js

```
28    return true;
29  }
30
31  $(document).ready(function () {
32    var nome = $('#nome');
33    nome.attr('data-toggle', 'tooltip');
34    nome.attr('data-placement', 'top');
35    nome.prop('title', 'Informe seu nome!');
36  });
37
38  function check_email() {
39    var ver = /^[a-zA-Z0-9_.+-]+@[a-zA-Z0-9-]+\.[a-zA-Z0-
40    var email = $('#email');
41    var parent = email.parent();
42    if (ver.test(email.attr('value')) === false) {
43      parent.removeClass('has-success');
44      parent.addClass('has-error');
45      email.tooltip('show');
46      $('#salvar').prop('disabled', true);
47      return false;
48    }
```

Figura 11 – Exemplo de código Javascript
Fonte: Sistema de controle de acesso

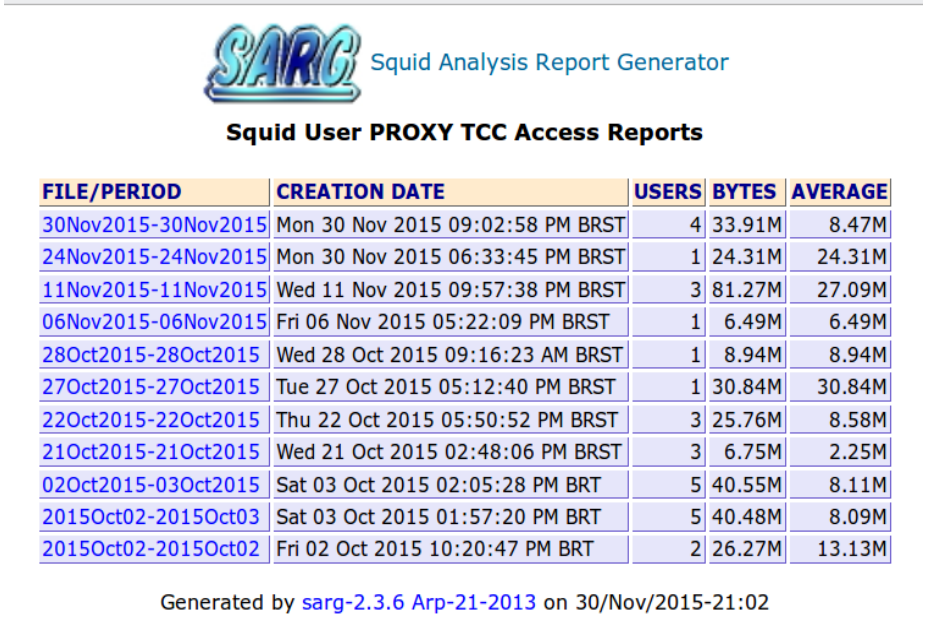
3.6 Apache *Server*

Servidor Apache ou Servidor de HTTP *(Hyper-Text Transfer Protocol*) é o servidor mais utilizados no mundo para trabalhar com serviços voltados a web, por possuir compatibilidade de instalação e poder ser utilizado em diferentes sistemas operacionais. Servidor HTTP é responsável por aceitar pedidos HTTP de clientes exemplo *browsers*, retornando uma resposta HTTP com objetos requeridos (ALECRIM, 2006).

Além do Apache existem outros tipos de Servidores HTTP como *XAMP, TinyWeb, Apache Tomcat, AnalogX SimpleServer, LiteSpeed Web Server*, entre outros. O Servidor apache foi adotado por ser *software* livre e compatibilidade com execução de outras linguagens de programação dentro de sua estrutura como PHP e Shell Script, e também por possuir uma ampla documentação estruturada.

3.7 Squid *Analysis Report Generator* – SARG

O SARG, como o próprio nome já diz, é uma ferramenta de análise e interpretação de logs do *Proxy* Squid. Ele cria um conjunto de páginas dívidas por dia, acompanhado de uma lista de todas as páginas acessadas, organizadas por usuários. Mostra também, de acordo com regras impostas no Squid, se o acesso a uma determinada URL ou domínio foi negado ou permitido (MORIMOTO, 2009).



Squid Analysis Report Generator

Squid User PROXY TCC Access Reports

FILE/PERIOD	CREATION DATE	USERS	BYTES	AVERAGE
30Nov2015-30Nov2015	Mon 30 Nov 2015 09:02:58 PM BRST	4	33.91M	8.47M
24Nov2015-24Nov2015	Mon 30 Nov 2015 06:33:45 PM BRST	1	24.31M	24.31M
11Nov2015-11Nov2015	Wed 11 Nov 2015 09:57:38 PM BRST	3	81.27M	27.09M
06Nov2015-06Nov2015	Fri 06 Nov 2015 05:22:09 PM BRST	1	6.49M	6.49M
28Oct2015-28Oct2015	Wed 28 Oct 2015 09:16:23 AM BRST	1	8.94M	8.94M
27Oct2015-27Oct2015	Tue 27 Oct 2015 05:12:40 PM BRST	1	30.84M	30.84M
22Oct2015-22Oct2015	Thu 22 Oct 2015 05:50:52 PM BRST	3	25.76M	8.58M
21Oct2015-21Oct2015	Wed 21 Oct 2015 02:48:06 PM BRST	3	6.75M	2.25M
02Oct2015-03Oct2015	Sat 03 Oct 2015 02:05:28 PM BRT	5	40.55M	8.11M
2015Oct02-2015Oct03	Sat 03 Oct 2015 01:57:20 PM BRT	5	40.48M	8.09M
2015Oct02-2015Oct02	Fri 02 Oct 2015 10:20:47 PM BRT	2	26.27M	13.13M

Generated by sarg-2.3.6 Arp-21-2013 on 30/Nov/2015-21:02

Figura 12 – Sistema de análise de *logs*
Fonte: Sistema de controle de acesso

Como apresentado na Figura 12 os dados de *logs* ficam agrupados por períodos, número de usuários bem como taxa de uso de dados. Desta forma consegue-se um monitoramento completo de todos as URLs e domínios acessados ao realizar o acesso aos arquivos. Com a utilização do SARG no trabalho e a partir da análise periódica dos registros de *logs,* pode-se elaborar, modificar e estipular novas regras de acesso e restrição de acordo com a necessidade da utilização de determinados sites.

3.8 Sistema de Gerenciamento de Banco de Dados – SGBD

SGBD é um conjunto de *softwares* responsáveis por gerenciar uma base de dados, com objetivo principal gerir a manipulação, organização e acesso aos dados. O sistema também é utilizado para compartilhar informações de forma segura,

garantir a integridade e a consistência dos dados, permitir acesso rápido e eficiente, oferecer uma forma de afastar do usuário comum a necessidade de compreender as estruturas físicas dos dados.

3.9 *Dynamic Host Configuration Protocol* – DHCP

Servidor DHCP (*Dynamic Host Configuration Protocol* ou Protocolo de Configuração Dinâmica de Endereços de Rede) é um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente. Este protocolo permite uma maior facilidade e agilidade na distribuição de endereços IP em redes com um grande número de hosts conectados.

O protocolo DHCP utiliza um modelo cliente-servidor, sendo que o servidor DHCP faz gestão centralizada dos endereços IP que são usados na rede. O protocolo DHCP possui três configurações específicas, pode-se adotar a que for estipulada nas regras de acesso (ISC DHCP, 2015).

- Automático, a máquina cliente realiza uma requisição IP e o servidor retorna com um endereço válido;
- Dinâmico, o procedimento é parecido com o automático, porém a alocação do IP com o cliente é limitada por um período de tempo pré-configurado;
- Manual, administrador aloca um endereço IP ao *mac address* do cliente.

O serviço DHCP foi utilizado para que os *hosts* da rede interna pudessem se comunicar sem a que o *proxy* intervisse dentro da rede interna.

3.10 Squid Cache

Squid é um sistema de *proxy* que possui armazenamento da cópia de sites em cache, com suporte a vários protocolos como HTTP, HTTPS, FTP. O *Squid* é utilizado para controlar o acesso a determinados sites e reduzir o uso de banda, a

fim de melhorar o tempo de resposta no acesso, devido ao armazenamento em cache e reutilização das páginas acessadas mais frequentemente acessadas na internet (SQUID-CACHE, 2013).

3.10.1 *Access Control List* – ACL

ACL são listas de controle, as quais constituem a grande flexibilidade e eficiência do *Squid*. Através das ACL's, consegue-se criar regras para controlar o acesso a diversos conteúdos da internet das mais diferentes formas. Quase todo o processo de controle de acesso do *Squid* é feito através de ACLs, são realizadas verificações comparativos com as regras definidas nas listas. A fim de intervir o acesso dos usuários através de listas totalmente customizadas (WATNABE, 2000).

Para criação das listas deve-se tomar alguns cuidados, pois é através destas que é realizado todo o controle de conteúdo, pois se bem configuradas pode propiciar uma ótima barreira de acesso. Se mal configuradas terá o efeito reverso do proposto.

3.10.2 Modo de Configuração

Todas as configurações do servidor *Squid* se encontram no arquivo `squid.conf`. O arquivo original do *Squid*, assim que instalado, consta mais de 1500 linhas de configurações nativas válidas comentadas. Para realizar um controle por autenticação, o Squid trabalha com dois principais modos de configuração:

a) *Proxy*

Transparente, trabalha combinado ao sistema de *firewall*, todo o tráfego é direcionado para o servidor *Squid*, forçando o usuário a utilizar o servidor *proxy Squid.* No entanto, como abordado em outro tópico anteriormente, existem várias desvantagens neste método.

b) *Proxy* Autenticado, consiste em realizar autenticação por meio de credenciais informadas ao iniciar a comunicação do *browser* com o *Squid* na solicitação de conteúdo online. A cada solicitação *Squid* armazena as credenciais do usuário por um determinado tempo, para que possam ser usadas posteriormente em futuras conexões.

4 DESCRIÇÃO DO SISTEMA

4.1 Modo de acesso

Como discutido no capítulo anterior o método de controle escolhido para atuar no controle de acesso foi o *proxy* não transparente, deve-se informar ao navegador as informações pertinentes à existência de um servidor proxy na rede. Assim o navegador possa comunicar-se com a rede externa. A figura a seguir demonstra a configuração necessária no para utilizar a rede no browser.

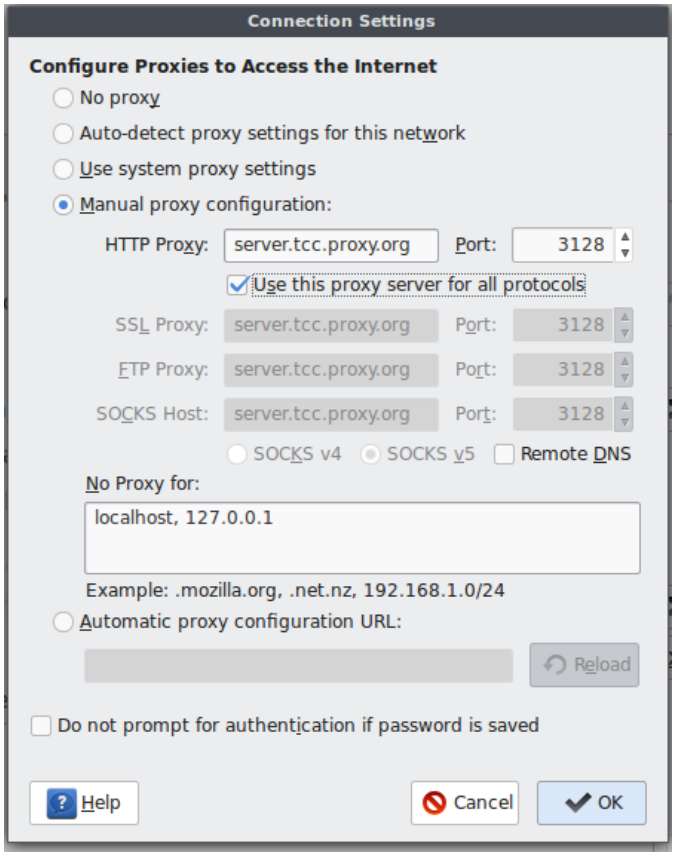


Figura 13 – Configuração *proxy* no browser
Fonte: Elaborado pelo autor

4.2 Hierarquia de acesso

A interface web permitirá realizar as configurações e manipulação de arquivos e visualização destes por parte de todos os usuários, enquanto os códigos realizaram as funcionalidades desenvolvidas. O sistema foi elaborado para ser acessado por diferentes tipos de usuários como professor, aluno, visitante e administrador. Para realizar o acesso ao sistema, cada tipo de usuário possui algumas limitações e restrições.

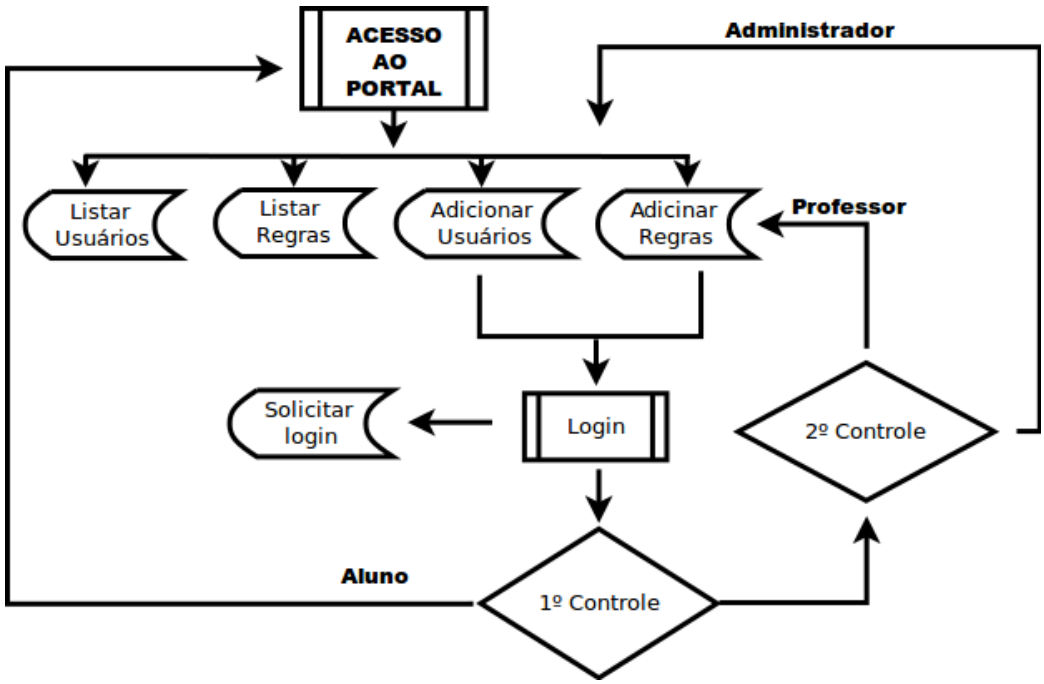
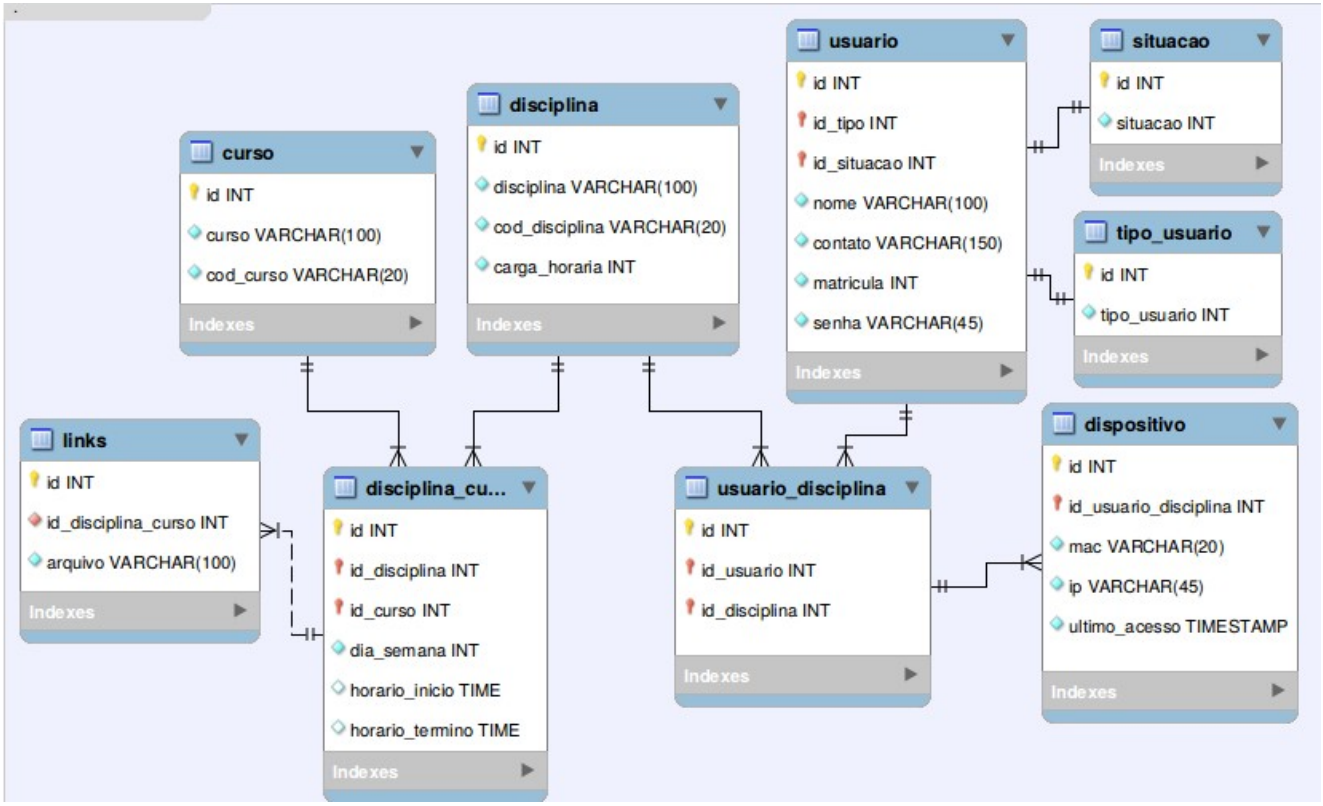


Figura 14 – Hierarquia de acesso
Fonte: Elaborado pelo autor

Para um melhor entendimento da Figura 14, será apresentado casos de uso por parte de cada um dos tipos de usuários através de diagramas de *Unifield Modeling Languade* (UML).

4.3 Sistema de banco de dados

Para que fosse possível realizar um controle mais efetivo e centralizado dos dados, foi utilizado um sistema de banco de dados, a fim de simular um sistema completo de um ambiente escolar. Este sistema consiste na leitura dos dados para que se possa verificar as ligações entre as diferentes tabelas e informações referentes a cada tipo de usuário e suas atribuições.



Fonte: Elaborado pelo autor

O sistema de banco de dados consiste em nove tabelas interligadas por índices:

- Tabela curso: Possui as informações referentes a nomes de diferentes

Cursos apresentados no momento do cadastro, seguido de um código de referência;

- Tabela disciplina: Possui as informações referentes ao nome de diferentes disciplinas apresentadas seguido de seu Curso referente, possui um código de referência e um campo Carga Horaria a fim de informar o número máximo de horas da mesma;
- Tabela disciplina_curso: Possui índices que realizam a ligação entre o Curso e suas respectivas Disciplinas, pois um curso poderá possuir mais de uma disciplina e a mesma disciplina ser ofertada em diferentes cursos;
- Tabela links: Possui ligação com a tabela disciplina_curso, no momento da criação das ACLs o sistema realiza uma verificação de quais links estão indexadas para cada disciplina e quais alunos estão matriculados nestas disciplinas;
- Tabela usuario: Informações referentes a todos os usuários cadastrados no sistema;
- Tabela usuario_disciplina: Possui índice entre a tabela usuario e tabela disciplina que informa quais usuários estão vinculados a quais disciplinas;
- Tabela tipo_usuario: Possui os diferentes tipos de níveis que os usuários poderão ser submetidos no momento do cadastro (aluno, professor, convidado);
- Tabela situacao: Possui as situações que o usuário se encontra para que possa realizar o acesso (aprovado, reprovado, aguardando aprovação);
- Tabela dispositivo: Possui as informações referentes aos dispositivos que realizam a conexão com a rede, possuindo o valor do *mac address, IP* e o índice do usuário.

4.4 Caso de uso do acesso usuário ao Squid

Para melhor visualização das funcionalidades da interface web com o servidor proxy, será apresentado alguns casos de uso para cada tipo de usuários e

permissões atribuídas a um.

4.4.1 Caso de uso usuário Aluno ou Visitante

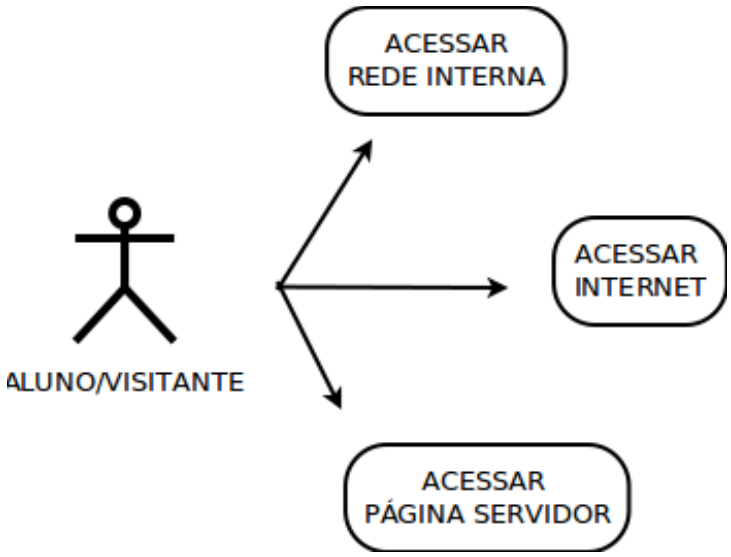


Figura 16– Diagrama de caso de uso do acesso do Aluno/Visitante
Fonte: Elaborado pelo autor

Para melhor entendimento da Figura 16, pode-se visualizar nos Apêndice A – Acesso na rede interna aluno/visitante até o Apêndice C – Acesso ao servidor web por aluno/visitante.

4.4.2 Caso de uso usuário aluno ou Professor

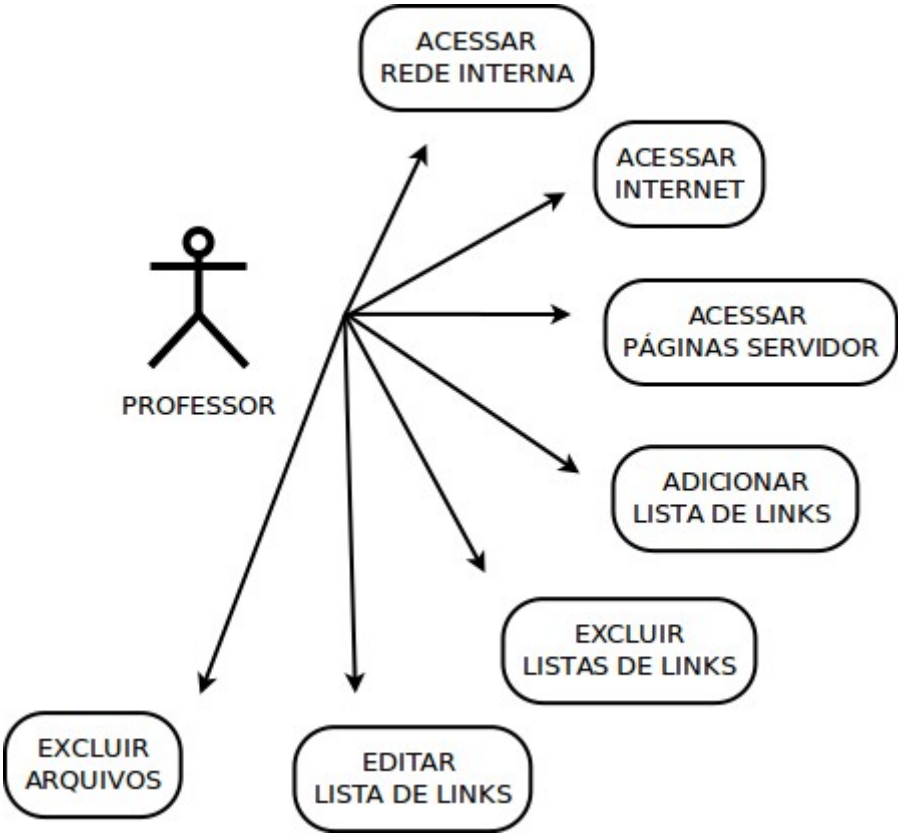


Figura 17 – Diagrama de caso de uso do acesso do Professor
Fonte: Elaborado pelo autor

Para melhor entendimento da Figura 17, pode-se visualizar os Apêndice D – Acesso ao servidor web por professor até o Apêndice J – Exclusão de arquivos para turma, que detalha cada item.

4.4.3 Caso de uso usuário Administrador

O administrador possui total acesso a qualquer dado ou tabela, somente se faz necessário a realização de login e senha no momento de acesso no servidor web.

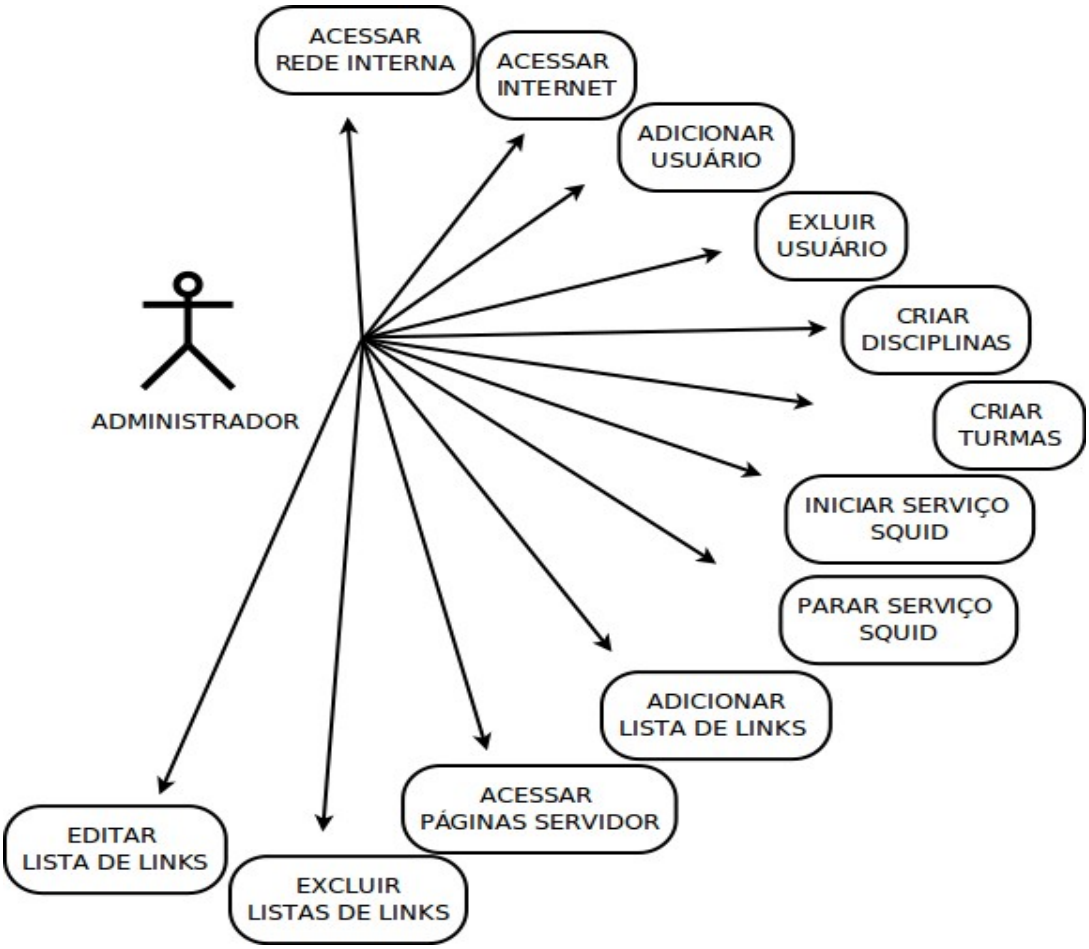


Figura 18 – Caso de uso pelo administrador
Fonte: Elaborado pelo autor

Para melhor entendimento da Figura 18, pode-se visualizar o Apêndice K – Acesso rede interna administrador até o Apêndice U – Cadastro de uma nova disciplina, que detalha cada item.

4.4.4 Caso de uso do sistema

O sistema é o responsável por abranger os demais *softwares*, comandos e gerenciamento da aplicação.

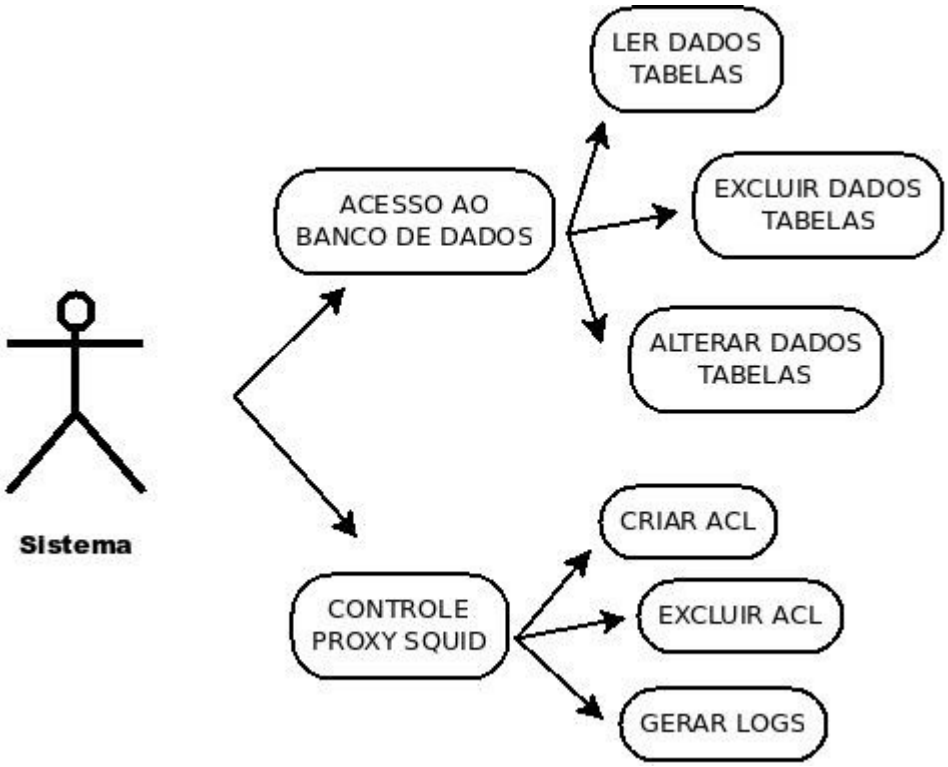


Figura 19 – Caso de uso sistema de gerenciamento
Fonte: Elaborado pelo autor

Para melhor entendimento da Figura 17, pode-se visualizar o Apêndice V – Acesso ao sistema de banco de dados até o Apêndice CC – Geração de Logs de acesso, que detalha cada item.

4.5 Descrição da interface web

Com a utilização da interface web do servidor o usuário poderá ter uma experiência de gerenciamento da rede sem a necessidade de possuir um

conhecimento técnico elevado sobre o *software* Squid. Toda a interface é apresentada em HTML junto com JavaScript que torna a interface dinâmica e intuitiva.

4.5.1 Página principal

Primeira página que o usuário se encontra ao acessar o servidor web, todas as funcionalidades e locais para navegação às páginas se encontram neste *layout.*

Figura 20 – Página principal servidor web
Fonte: Sistema de controle de acesso

A Figura 20 mostra a página principal apresentada ao usuário ao realizar ao acesso. Toda a interface do sistema é responsiva, ou seja, se ajusta a qualquer tamanho de tela. Com interface responsiva o professor ou usuário não possuirá a necessidade de realizar o acesso ao sistema web somente em um computador,

assim poderá acessar através de um *smartphone* ou *tablet.*

4.5.2 Página de login

Como já apresentado nos diagramas de casos, para poder acessar determinadas páginas se faz necessário informar as credenciais. Assim, o através de controles de acesso o sistema verifica o que cada usuário poderá acessar e visualizar dentro do sistema web.

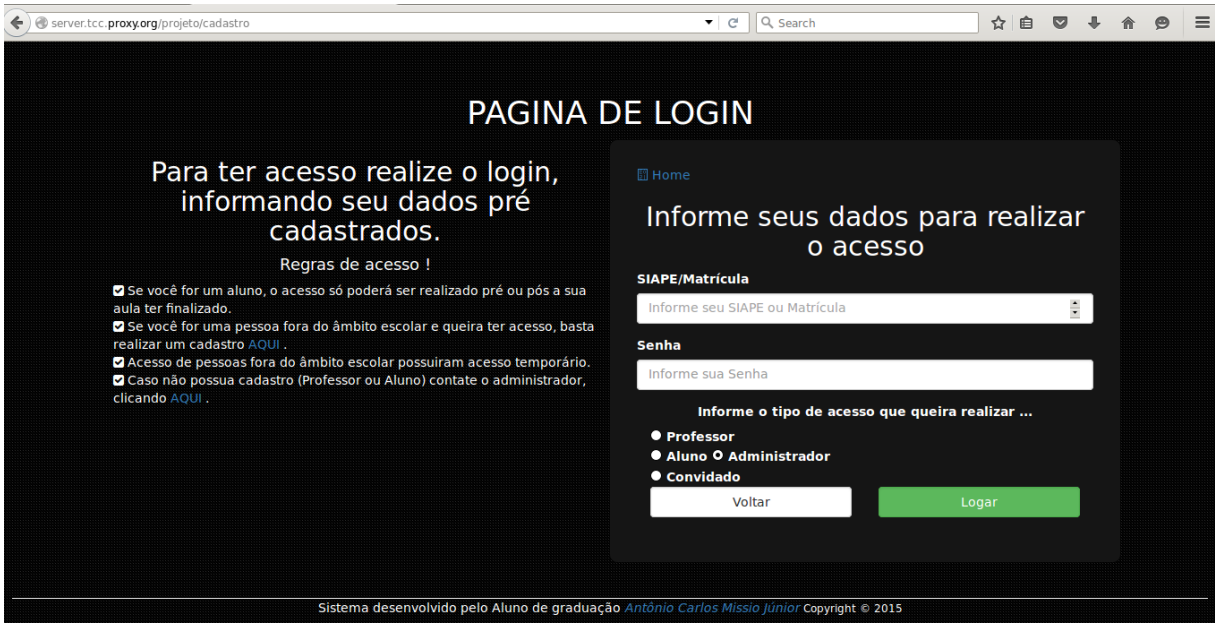


Figura 21 – Página de login
Fonte: Sistema de controle de acesso

Como apresentado na Figura 21, existe uma pequena lista de informações ao lado esquerdo. Caso o usuário não possua cadastro e deseja realizar, pode entrar em contato com o administrador através do link informado junto a esta página.

4.5.3 Lista de usuários

O sistema possui uma página contendo alguns dados de todos os usuários, para consulta de alguns dados.

Figura 22 – Página de consulta de usuários
Fonte: Sistema de gerenciamento de acesso

Como apresentado na Figura 22, caso o usuário não lembre de sua matrícula ou situação, poderá realizar um acesso a está página. Na coluna “Tipo de Usuário”, trás uma informação que informa a qual nível se encontra, no campo “Situação” se este está aprovado reprovado ou ainda aguardando aprovação do administrador para poder ter acesso.

4.5.4 Inserção de links e domínios

Para realizar disponibilizar os links e palavras para serem trabalhadas em aula, o sistema possui uma área específica para tal operação. Área de acesso restrito a somente por professores e administradores do sistema.

Figura 23 – Página de inserção de domínios e expressões
Fonte: Sistema de controle de acesso

Como apresentado na Figura 23, a página possui três colunas e uma área de seleção do curso e disciplina referente ao curso que o professor está apto a ministrar aula. A seguir escolhe qual tipo de material e para próximo é reiniciar o serviço ou verificar os *logs* de acesso.

4.5.5 Listar arquivos

Para que os alunos possam visualizar o que está disponibilizado a eles e também para quem possua acesso administrativo possa realizar alterações nos arquivos, o sistema possui uma área para tal função.

Figura 24 – Lista de arquivos
Fonte: Sistema de controle de acesso

Após criar os arquivos e salvar, estes já estão dispostos para serem visualizados por todos que possuírem credenciais válidas. Como apresentado na Figura 24, o painel possui três botões, os quais ficam dispostos para quem possua acesso administrativo possa realizar alterações e a exclusão do arquivo.

4.5.6 Painel de *log*

Com a utilização do analisador de *logs* SARG, consegue-se obter uma análise mais detalhada e abrangente de todos os sites acessados, bem como sites que foram bloqueados no momento do acesso.

Squid Analysis Report Generator

Squid User PROXY TCC Access Reports

Period: 30 Nov 2015

Authentication Failures

USERID	IP/NAME	DATE/TIME	ACCESSED SITE
02930293'	172.22.0.10	11/30/2015-19:57:11	self-repair.mozilla.org:443
		11/30/2015-19:57:11	ssl.google-analytics.com:443
1234	172.22.0.10	11/30/2015-19:38:19	http://ajax.googleapis.com
		11/30/2015-19:38:19	http://fonts.googleapis.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
		11/30/2015-19:38:19	http://shop.canonical.com
			4 more authentication failures not shown here...
172.22.0.10	172.22.0.10	11/30/2015-18:58:58	aus4.mozilla.org:443
		11/30/2015-19:00:24	aus4.mozilla.org:443
		11/30/2015-19:38:53	aus4.mozilla.org:443
		11/30/2015-19:02:24	blocklist.addons.mozilla.org:443
		11/30/2015-18:59:28	facebook.com:443
		11/30/2015-18:55:30	fhr.data.mozilla.com:443
		11/30/2015-19:10:42	fhr.data.mozilla.com:443
		11/30/2015-19:18:08	http://172.17.21.209
		11/30/2015-19:38:12	http://ajax.googleapis.com
		11/30/2015-19:57:12	http://ajax.googleapis.com
			95 more authentication failures not shown here...
172.22.0.15	172.22.0.15	11/30/2015-19:48:42	aus4.mozilla.org:443
		11/30/2015-19:50:42	blocklist.addons.mozilla.org:443
		11/30/2015-19:56:29	blocklist.addons.mozilla.org:443
		11/30/2015-19:56:31	blocklist.addons.mozilla.org:443
		11/30/2015-19:56:31	blocklist.addons.mozilla.org:443
		11/30/2015-19:56:32	blocklist.addons.mozilla.org:443
		11/30/2015-19:56:32	blocklist.addons.mozilla.org:443

Figura 25 – Lista de sites com tag de bloqueio
Fonte: Sistema de controle de acesso

Como apresentado na Figura 25, a página de logs contém os dados referentes aos usuários, seu IP, o período do acesso, os sites acessados e qual o protocolo utilizado.

5 Conclusão

Este trabalho teve como objetivo desenvolver uma ferramenta com base em *software* livre para que o professor possa realizar a liberação do acesso à internet somente do conteúdo proposto em suas aulas de forma a evitar a dispersão dos alunos e diminuir latência da rede. Com a utilização desta ferramenta o usuário terá uma experiência de gerenciamento da rede sem a necessidade de possuir um conhecimento técnico elevado sobre o *software* Squid.

Durante a elaboração da ferramenta e desenvolvimento da interface foram encontradas algumas dificuldades. O objetivo inicial era utilizar um sistema de proxy transparente, mas ao decorrer do desenvolvimento do sistema verificou-se a impossibilidade de tal utilização. Com a utilização deste método, o sistema de controle não conseguia realizar o bloqueio a alguns sites por utilizarem protocolos não compatíveis. Para isto foi realizado uma pesquisa de outro método de realizar o controle por dispositivo, por um identificador único como o endereço *mac address* do dispositivo, sendo necessário recompilar o código fonte do *software* Squid passando parâmetros para habilitar mais esta funcionalidade.

Outro problema encontrado foi com tamanho das partições do sistema (*hard disk*) e algoritmos a serem utilizados para o uso e controle dos dados armazenados em cache, deve-se realizar um estudo em relação ao número de usuários que utilizaram a rede, para que se tenha uma noção do volume dados que serão armazenados. No entanto, a maior dificuldade foi de disponibilizar o acesso a um restrito número de links disponibilizados para um número variado de usuários.

Pois muitos sites utilizam mais de um *link* externo para que sua página seja carregada como por exemplo, a página de e-mails da Microsoft que realiza uma série de redirecionamentos até carregar por completa sua página. Com isso, foi realizado uma verificação mais detalhada dos dados trafegados a fim de verificar quais domínios seriam necessários liberar para que a página de e-mail pudesse ser acessada.

Ao término deste trabalho conclui-se que a utilização de uma interface mais dinâmica e interativa, utilizando diferentes elementos e linguagens de programação

interoperáveis é uma ótima forma de passar uma experiência divertida e diferenciada. Desta forma, usuários que não possuem um conhecimento técnico elevado terão a oportunidade de conhecer algumas ferramentas amplamente utilizadas no gerenciamento de redes e a oportunidade conhecê-las e se interessar em realizar um estudo mais detalhado.

No entanto, como mencionado anteriormente o administrador terá de verificar constantemente os *logs* e monitoramento da rede a fim de atribuir novas regras para que o professor ao realizar a inserção dos dados para que os alunos possam realizar o acesso. Este problema foi relatado na prática, na elaboração do trabalho, pois é realizado um bloqueio de todo o tipo de acesso e sendo liberado somente algumas específicas.

6 TRABALHOS FUTUROS

Como proposta para a realização de trabalhos futuros poderá ser implementado em um ambiente real para que se consiga resultados mais satisfatórios diferentes de um ambiente controlado. Realizar testes de usabilidade da ferramenta com pessoas que gostariam de aplicar em sala de aula, de modo a torná-la mais intuitiva e proporcionar uma boa experiência ao usuário.

Como proposta para um possível trabalho a implementação de um sistema transparente e que o professor necessite somente realizar a inserção dos dados e o sistema realizar todo o controle de forma automática. Desta forma o professor teria mais comodidade e rapidez para iniciar uma aula.

7 APÊNDICE

Apêndice A – Acesso na rede interna aluno/visitante

Descrição	Acessar computadores rede interna
Ator	Aluno ou visitante
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Iniciar acesso;
Fluxo Alternativo	a) O host acessado encontra-se desligado;
Pós-condição	O aluno/visitante terá acesso ao host se estiver ligado.

Apêndice B – Acesso à rede externa por aluno/visitante

Descrição	Acessar rede externa
Ator	Aluno ou visitante
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Configurar navegador; c) Iniciar acesso;
Fluxo Alternativo	a) Navegação a local desejado inválido; b) Não informado servidor proxy na rede; – Voltar ao passo b do fluxo principal; c) Local bloqueado para acesso;
Pós-condição	O aluno/visitante terá acesso ao local desejado caso tenha credencial válida.

Apêndice C – Acesso ao servidor web por aluno/visitante

Descrição	Acessar servidor
Ator	Aluno ou visitante
Pré-condição	Iniciar ambiente com as credenciais;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d)Navegar entre as páginas;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador;
Pós-condição	O aluno/visitante terá acesso ao local desejado caso tenha credencial válida.

Apêndice D – Acesso ao servidor web por professor

Descrição	Acessar computadores rede interna
Ator	Professor
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Iniciar acesso;
Fluxo Alternativo	a) O host acessado encontra-se desligado;
Pós-condição	O professor terá acesso ao host se estiver ligado.

Apêndice E – Acesso à rede externa por professor

Descrição	Acessar rede externa
Ator	Professor
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Configurar navegador; c) Iniciar acesso;
Fluxo Alternativo	a) Navegação a local desejado inválido; b) Não informado servidor proxy na rede; – Voltar ao passo b do fluxo principal; c) Local bloqueado para acesso;
Pós-condição	O professor terá acesso ao local desejado caso tenha credencial válida.

Apêndice F – Acesso ao servidor web por professor

Descrição	Acessar servidor
Ator	Professor
Pré-condição	Iniciar ambiente com as credenciais;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválidos; c) Iniciar acesso; d)Navegar entre as páginas;
Fluxo Alternativo	a) Usuários ou senha inválidos; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador;
Pós-condição	O professor terá acesso ao local desejado caso tenha credencial válida.

Apêndice G – Adicionar links/expressões para turma

Descrição	Acessar página requerida de adição de links/expressões
Ator	Professor
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Inserir links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválida; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar curso; f) Selecionar disciplina; g) Selecionar Link ou Expressões; h) Adicionar link ou expressões; i) Salvar; j) Reiniciar Serviço Squid;

Fluxo Alternativo	a) Usuários ou senha inválida; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador; b) Selecionar curso; – Caso não selecionar curso, não carregará disciplinas; c) Selecionar disciplina referente ao curso; – Caso não selecionar disciplina, não gerará o arquivo nem as configurações; d) Adicionar link ou expressões; – Campos em branco são inválidos; e) Salvar; f) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados na página do servidor web

Apêndice H – Alterar links/expressões para turma

Descrição	Acessar página requerida de alteração de links/expressões
Ator	Professor
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Alterar links/expressões; Salvar; Reiniciar serviço Squid;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválidos; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar arquivo; f) Alterar links;

	g) Salvar; h) Reiniciar Serviço Squid;
Fluxo Alternativo	a) Usuários ou senha inválidos; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador; b) Selecionar arquivo que deseja alterar; c) realizar alterações; d) Salvar; e) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados e alterados na página do servidor web

Apêndice I – Excluir links/expressões para turma

Descrição	Acessar página requerida de alteração de links/expressões
Ator	Professor
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Excluir links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválidos; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar arquivo; f) Excluir links; g) Salvar; h) Reiniciar Serviço Squid;

Fluxo Alternativo	a) Usuários ou senha inválidos; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador; b) Selecionar arquivo que deseja alterar; c) realizar exclusões; d) Salvar; e) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão os links já disponibilizados na página do servidor web

Apêndice J – Exclusão de arquivos para turma

Descrição	Acessar página requerida de alteração de links/expressões
Ator	Professor
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Excluir arquivo com links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválidos; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar arquivo; f) Excluir; g) Reiniciar Serviço Squid;
Fluxo Alternativo	a) Usuários ou senha inválidos; – Verificar dados e retornar passo “b” fluxo principal; – Solicitar login para o Administrador; b) Selecionar arquivo que deseja alterar; c) realizar exclusão;

	d) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados e alterados na página do servidor web

Apêndice K – Acesso rede interna administrador

Descrição	Acessar computadores rede interna
Ator	Administrador
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Iniciar acesso;
Fluxo Alternativo	a) O host acessado encontra-se desligado;
Pós-condição	O administrador terá acesso ao *host* se estiver ligado.

Apêndice L – Acesso à internet administrador

Descrição	Acessar Internet
Ator	Administrador
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir o navegador; b) Iniciar acesso;
Fluxo Alternativo	a) Acesso a internet livre; b) Sem conexão com provedor;
Pós-condição	O administrador terá acesso à internet sem restrições.

Apêndice M – Acesso ao servidor web administrador

Descrição	Acessar servidor
Ator	Administrador
Pré-condição	

	Iniciar ambiente com as credenciais;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d)Navegar entre as páginas;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console;
Pós-condição	O Administrador terá acesso ao local desejado caso tenha credencial válida.

Apêndice N – Adição de links/expressões administrador

Descrição	Acessar página requerida de adição de links/expressões
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Inserir links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar curso; f) Selecionar disciplina; g) Selecionar Link ou Expressões;

	h) Adicionar link ou expressões; i) Salvar; j) Reiniciar Serviço Squid;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Cadastra-se via console; b) Selecionar curso; – Caso não selecionar curso, não carregará disciplinas; c) Selecionar disciplina referente ao curso; – Caso não selecionar disciplina, não gerará o arquivo nem as configurações; d) Adicionar link ou expressões; – Campos em branco são inválidos; e) Salvar; f) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados na página do servidor web

Apêndice O – Alteração de links/expressões administrador

Descrição	Acessar página requerida de alteração de links/expressões
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Alterar links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso;

	d) Navegar entre as páginas; e) Selecionar arquivo; f) Alterar links; g) Salvar; h) Reiniciar Serviço Squid;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Cadastrar-se via console; b) Selecionar arquivo que deseja alterar; c) Realizar alterações; d) Salvar; e) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados e alterados na página do servidor web

Apêndice P – Exclusão de links/expressões administrador

Descrição	Acessar página requerida de exclusão de links/expressões
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Excluir links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar arquivo;

	f) Excluir links; g) Salvar; h) Reiniciar Serviço Squid;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Cadastrar-se via console; b) Selecionar arquivo que deseja alterar; c) Realizar exclusões; d) Salvar; e) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados na página do servidor web

Apêndice Q – Exclusão de arquivos de links/expressões

Descrição	Acessar página de exclusão de arquivos de links/expressões
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página; Excluir arquivo com links/expressões; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Selecionar arquivo; f) Excluir; g) Reiniciar Serviço Squid;

Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console; b) Selecionar arquivo que deseja excluir; c) Realizar exclusão; d) Reiniciar serviço Squid;
Pós-condição	Alunos da turma corrente cadastrada terão links já disponibilizados e alterados na página do servidor web

Apêndice R – Cadastro de um novo usuário

Descrição	Realizar o cadastro de um novo usuário
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página de cadastro; Cadastrar com dados dos usuários; Salvar; Reiniciar serviço Squid
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) inserir os dados do usuário; f) Salvar;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console; b) Inserir dados do novo usuário; c) Cadastrar; d) Informar ao usuário para realizar o primeiro acesso; d) Reiniciar serviço Squid;

Pós-condição	Usuário cadastrado terá acesso à rede;

Apêndice S – Exclusão de um usuário

Descrição	Realizar a exclusão de um usuário
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página da lista de usuários; Selecionar usuário; Excluir;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Excluir usuário;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console; b) Selecionar dados do usuário; c) Excluir;
Pós-condição	Usuário não terá mais acesso à rede;

Apêndice T – Cadastro de um novo curso;

Descrição	Realizar o cadastro de um novo curso;
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página de cadastro; Cadastrar com dados do curso; Salvar;
Fluxo principal	a) Abrir o navegador;

	b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Inserir os dados da novo curso ; f) Salvar;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console; b) Inserir dados do novo curso c) Cadastrar;
Pós-condição	Curso cadastrado;

Apêndice U – Cadastro de uma nova disciplina

Descrição	Realizar o cadastro de uma nova disciplina;
Ator	Administrador
Pré-condição	Iniciar ambiente com as credenciais; Navegar até a página de cadastro; Cadastrar com dados da disciplina; Salvar;
Fluxo principal	a) Abrir o navegador; b) Informar credenciais; – Login ou senha inválido; c) Iniciar acesso; d) Navegar entre as páginas; e) Inserir os dados da nova disciplina; f) Salvar;
Fluxo Alternativo	a) Usuários ou senha inválido; – Verificar dados e retornar passo “b” fluxo principal; – Realizar cadastro via console; b) Inserir dados da nova disciplina;

	c) Vincular a disciplina a um curso; c) Cadastrar;
Pós-condição	Disciplina cadastra;

Apêndice V – Acesso ao sistema de banco de dados

Descrição	Acessar sistema de banco de dados
Ator	Sistema de Gerenciamento;
Pré-condição	Iniciar acesso;
Fluxo principal	a) Abrir conexão; b) Iniciar acesso; c) Realizar pesquisas; d) Extrair dados;
Fluxo Alternativo	a) O sistema de gerenciamento realiza consulta, inserções e modificações no banco;
Pós-condição	É apresentado retorno do resultado da conexão;

Apêndice W – Acesso ao Proxy Squid

Descrição	Controle Proxy Squid
Ator	Sistema de Gerenciamento;
Pré-condição	Executar scripts (comandos);
Fluxo principal	a) Executa scripts; b) Aguarda retorno da execução (sucedida, não sucedida);
Fluxo Alternativo	a) Usuário (administrador/professor) através da interface solicita a excução de determinada funcionalidade; b) Interação entre PHP e Squid;
Pós-condição	Execução do comando;

Apêndice X – Acesso aos dados da tabela

Descrição	Ler dados tabela

Ator	Sistema de controle
Pré-condição	Abrir conexão; b) Iniciar acesso; c) Realizar pesquisas; d) Extrair dados;
Fluxo principal	a) Realiza consultas referentes aos requeridos pelo usuário; b) Carregar dados (páginas da interface web, controle login); c) Exibi resultados;
Fluxo Alternativo	Sistema verifica se os dados requeridos existem. Caso exista, é exibido ao usuário;
Pós-condição	É apresentado retorno do resultado da conexão; Encerrada conexão;

Apêndice Y – Deletar dados do sistema de banco de dados

Descrição	Excluir dados tabela
Ator	Sistema de controle
Pré-condição	Abrir conexão; b) Iniciar acesso; c) Realiza pesquisa; d) Seleciona os dados; e) Exclui os dados selecionados;
Fluxo principal	a) Realiza consultas referentes aos requeridos pelo usuário; b) Executa comando de exclusão; c) Realiza exclusão;
Fluxo Alternativo	Sistema verifica se os dados requeridos existem. Caso exista, é realizada a exclusão;
Pós-condição	É apresentado retorno do resultado do comando; Encerrada conexão;

Apêndice Z – Alterar dados tabelas sistema de banco de dados

Descrição	Alterar dados tabela
Ator	Sistema de controle
Pré-condição	a) Abrir conexão; b) Iniciar acesso; c) Realiza pesquisa; d) Seleciona os dados; e) Realiza alterações aos dados selecionados;
Fluxo principal	a) Realiza consultas referentes aos requeridos pelo usuário; b) Executa comando de alteração; c) Realiza as alterações;
Fluxo Alternativo	Sistema verifica se os dados requeridos existem. Caso exista, é realizada a alteração nos dados;
Pós-condição	É apresentado retorno do resultado do comando; Encerrada conexão;

Apêndice AA – Inserção de novas ACLs

Descrição	Criar ACLs
Ator	Proxy Squid
Pré-condição	a) Abrir conexão como banco de dados; b) Iniciar acesso; c) Realizar pesquisas; d) Extrair dados; e) Abrir arquivos de texto; f) Extrair dados arquivos; g) Montar ACL;
Fluxo principal	a) Consulta tabela usuario_disciplina; b) Consulta tabela de equipamentos; c) Carrega dados referentes aos usuários que estarão em aula d) Carrega os dados para um arquivo-texto; e) Realiza consulta em arquivos contendo as regras; f) Cria ACL referente arquivo contendo os dados dos usuários, seguido das listas de controle; g) Reinicia serviço; h) Realiza o controle de acesso para determinados dispositivos;
Fluxo Alternativo	Sistema verifica se os dados requeridos existem. Caso exista, montado ACLs referentes a cada turma corrente em aula com os dados dos alunos
Pós-condição	É realizado o controle de acesso;

Apêndice BB – Exclusão de ACLs

Descrição	Excluir ACLs
Ator	Sistema de controle
Pré-condição	a) Verifica hora do sistema (fora do período letivo);

	b) Deleta arquivo; c) Deleta ACLs;
Fluxo principal	a) Realiza consultas referentes as datas de criação de cada ACLs; b) Executa comando de exclusão; c) Reinicia o serviço;
Fluxo Alternativo	Sistema verifica se os dados requeridos existem. Caso exista, é realizada uma verificação da hora no sistema, se for fora do período letivo pode-se excluir ACLs antigas;
Pós-condição	É reiniciado o serviço;

Apêndice CC – Geração de Logs de acesso

Descrição	Gerarar Logos
Ator	Sistema de controle
Pré-condição	a) Analisa as URLs acessadas; b) Compara com os contidos nas listas; c) Salva em um arquivo texto (permito ou negado);
Fluxo principal	a) Realiza consultas referentes as URLs em cada ACLs; b) Salva os registros de acesso em LOGs (arquivos de texto);
Fluxo Alternativo	Sistema apenas relata os dados trafegados e salva-os em arquivos para futuras consultas com *softwares* analisadores;
Pós-condição	Log gerado para consulta

8 REFERÊNCIAS

ALECRIM, E. **O que é Linux e qual a sua história?**, 2011. Disponível em <http://www.infowester.com/historia_linux.php> Acessado 22 de novembro de 2015.

ALMEIDA, M. E. B. de. Informática e Formação de Professores, PROINFO. Coleção **Informática para a mudança na Educação**, Brasília: Ministério da Educação/SEED, 2000;

ANTONIO, J. C. **O uso pedagógico da sala de Informática da escola**, Professor Digital, SBO, 08 de Maio de 2010. Disponível em: <https://professordigital.wordpress.com/2010/05/08/o-uso-pedagogico-da-sala-de-informatica-da-escola/>. Acesso em: 20 de abril de 2015.

ARNAB, A.; e HUTCHISON, A. **Persistent Access Control:** A Formal Model for DRM, 2007, Disponível em <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.129.5957&rep=rep1&type=pdf >. Acessado em 27 de outubro de 20015;

BARBOSA, A. F. Pesquisa sobre o uso das tecnologias de informação e comunicação nas escolas brasileiras: **TIC Educação**, 2013 [livro eletrônico] – 1. ed. – São Paulo: Comitê Gestor da Internet no Brasil, 2014. Disponível em: <http://cgi.br/media/docs/publicacoes/2/tic-educacao-2013.pdf> Acessado em 05 outubro de 2015.

BARROS, L. G.; FOLTRAN, D. C. **Autenticação IEEE 802.1X em Redes de computadores Utilizando TLS e EAP,** 2010. Disponível em: <http://www.4eetcg.uepg.br/oral/62_1.pdf>. Acessado em: 07 setembro 2015.

BUFFONI, S. **Apostila de Algoritmo Estruturado.** Fiaa-Faculdades Integradas Anglo-Americano Curso De Sistemas De Informação, 2003.

CARVALHO, A. A. A. **Rentabilizar a Internet no Ensino Básico e Secundário**: dos Recursos e Ferramentas Online aos LMS, 2007. Disponível em <https://repositorium.sdum.uminho.pt/bitstream/1822/7142/1/sisifo03PT02.pdf>. Acessado 27 de outubro de 2015.

DUARTE, D. **Por que proxy não transparente é melhor que o transparente**, 2011 Disponível em: <http://www.purainfo.com.br/hardwareredes/por-que-proxy-no-transparente-melhor-que-o-transparente/>. Acessado 27 de novembro de 2015.

FILHO, V. S.; SILVA, M. S. da. **Biometria através de Impressão Digital**, 2011. Disponível em <http://web.unifoa.edu.br/cadernos/edicao/15/19.pdf>. Acessado 27 de outubro de 2015.

GABARDO, Ademir Cristiano. **PHP e MVC com CodeIgniter**. São Paulo. Editora Novatec, 2012.

GOMES, N. G. **Os Computadores Chegam À Escola**: E, agora professor? Trabalho apresentado no IV Seminário de Pesquisa Em Educação Da Região Sul, Florianópolis, 2002.

HACK, J. R.; NEGRI, F. **Capacitação docente para o uso da mídia como ferramenta didática:** Um espaço de reflexão e ação. 2008. Disponível em <http://www.abed.org.br/congresso2008/tc/429200862022pm.pdf>. Acessado 27 de outubro de 2015.

HARTHI, Z. A.; MASUD, M. M.; MUSTAFA, U.; TRABELSI, Z.; WOOD, T.; Firewall Performance Optimization Using Data Mining Techniques. **Wireless Communications and Mobile Computing Conference (IWCMC),** p: 934**,** 2013 IEEE

LEITE, S. A. da.; PALMA, L. V. **Teoria E Prática De Professores Considerados**

Construtivistas*, 1995. Disponível em <http://rbep.inep.gov.br/index.php/RBEP/article/viewFile/317/318>. Acessado 18 de agosto de 2015.

LENTO, L. O. B.; FRAGA, J. da S.; LUNG L. C. **A Nova Geração de Modelos de Controle de Acesso em Sistemas Computacionais**, Cap. 4, 2006 <http://gcseg.das.ufsc.br/wssec/pubs/lento06_sbseg.pdf>. Acessado 05 de Setembro de 2015;

LÉVY, P. **Filosofia do World O Mercado, o Ciberespaço, a Consciência**, 2001.

MARINHO, S. P. P. **WebQuest** – Um uso inteligente da Internet na escola. Artigo publicado em Caderno do Professor, n7, p.55-64, 2001.

MACÊDO, D. **Mecanismos de Controle de Acesso**, 2012, Disponível em: <http://www.diegomacedo.com.br/mecanismos-de-controle-de-acesso/>. Acessado 02 de setembro de 2015.;

MENDES, D. R. **Redes de Computadores** – Teoria e Prática, 2007 Disponível em: <https://novatec.com.br/livros/redescom/capitulo9788575221273.pdf> Acessado 07 de setembro de 2015.

MORAN, J. M. A educação que desejamos; Novos Desafios e como chegar lá; Cap. 4 **As possibilidades das redes de aprendizagem**, 2014.

MORIMOTO, C. E. **Servidores Linux, guia prático**. Porto Alegre: Sul Editores, 2009. 735 p.

NASCIMENTO, J. K. F. do. **Informática aplicada à educação**. Brasília: Universidade de Brasília, 2007.

OBELHEIRO, R. R. **Controle de Acesso,** 2008, Disponível em:

<http://www2.joinville.udesc.br/~dcc2rro/seg-bcc/2009.1/resumo-controle-acesso.pdf>. Acessado 13 de Setembro de 2015;

PHP, 2015. Disponível em <http://php.net> Acessado 27 de novembro de 2015.

PORTILHO. G.; PINTO. J. **O que são bibliotecas virtuais?** Disponível em: <http://revistaescola.abril.com.br/fundamental-2/sao-bibliotecas-virtuais-681243.shtml>. Acessado 02 de Setembro de 2015.

PERICLES, L. **Ferramentas de controle de acesso à rede,** 2011. Disponível em: <http://dascoisasqueaprendi.com.br/tiseguranca/ferramentas-para-controlar-o-acesso-a-rede/>. Acessado 04 de setembro de 2015;

PROXY, 2015. Disponível em <http://proxy.org/> Acessado 26 de novembro de 2015.

RFC 2186, **Internet Cache Protocol (ICP), version 2**. 1997. Disponível em <https://tools.ietf.org/html/rfc2186> . Acessado 18 de novembro de 2015.

RFC 2187, **Application of Internet Cache Protocol (ICP), version 2**. 1997. Disponível em <https://tools.ietf.org/html/rfc2187>. Acessado 18 de novembro de 2015.

ROMMEL, R. P. G. B. S. **Proposta de Controle Eficaz do Acesso à Interne**t, Monografia apresentada ao Curso de Pós-graduação em Segurança de Redes de Computadores da Faculdade Salesiana de Vitória, 2007.

SILVA, M. G. G. da.; LIMA, E. B. L. de. **Educação e Professor Diante do Uso das Novas Tecnologias**, 2010. Disponível em: <http://editorarealize.com.br/revistas/fiped/trabalhos/98b297950041a42470269d56260243a1.pdf>. Acessado 13 de Setembro de 2015;

SILVA, L. A. F.; DUARTE, O. C. M. B. **RADIUS em Redes sem fio**. Disponível em:

<http://www.gta.ufrj.br/seminarios/CPE825/tutoriais/lafs/RADIUS_em_Redes_sem_Fio.pdf>. Acesso em 05 setembro 2015.

SILVA, M. S.: **JavaScript:** Guia do Programador. São Paulo: Novatec Editora, 2010.

SQUID-CACHE. 2013. Disponível em <http://www.squid-cache.org> Acessado em 05 de outubro de 2015

TANEBAUM, A. S. **Sistemas Operacionais**, 3Ed; 2009.

VALENTE, J. A. **Diferentes usos do Computador na Educação**, 2000. Disponível em: <http://www.educacaopublica.rj.gov.br/biblioteca/tecnologia/0022.html>. Acessado em 20 de abril de 2015.

VALENTE, J. A. **Informática na educação:** instrucionismo x construcionismo, 1997. Disponível em<http://www.educacaopublica.rj.gov.br/biblioteca/tecnologia/0003.html>. Acessado em 12 de maio de 2015.

VENETIANER, T. **HTML: desmistificando a linguagem da Internet**. São Paulo: Makron Books, 1996. 289p.

WATANABE, C. S. **Introdução ao Cache da Web**, Boletim bimestral sobre tecnologia de redes produzido e publicado pela RNP – Rede Nacional de Ensino e Pesquisa, vol. 4, 2000 <https://memoria.rnp.br/newsgen/0003/cache.html>. Acessado 25 de Outubro de 2015.

WOLF, L. A.; SILVA, V. C. O. da. **Controle de acesso em segmentos de rede para usuários autorizados em um ambiente corporativo**, Universidade Luterana do Brasil (ULBRA), Curso Superior de Tecnologia Em Redes De Computadores – Campus Canoas, Junho de 2011.

W3C, **HTML, The Web's Core Language**, 2015. Disponível em: <http://www.w3.org/html/> Acessado 28 de novembro de 2015.

W3SCHOOLS.COM, **The MVC Programming Model**, 2015. Disponível em: <http://www.w3schools.com/aspnet/mvc_intro.asp> Acessado 15 de novembro de 2015.

ZEMEL, T. **HMVC no CodeIgniter com Modular Extensions**, 2010. Disponível em: <http://codeigniterbrasil.com/tutoriais/hmvc-no-codeigniter-com-modular-extensions/> Acessado 15 de novembro de 2015.