III Semana de Tecnologia da Informação – 21 a 25 de novembro de 2016, Paranavaí – PR - ISSN: 2526-1924

Utilizando software livre para implementar uma política de segurança em uma instituição acadêmica

João Paulo De Barros[1], André Ricardo Zavan[1]

[1]Instituto Federal do Paraná (IFPR)
Rua José Felipe Tequinha, 1400 - Paranavaí - PR - Brazil
jpb.ifpr@gmail.com,andre.zavan@ifpr.edu.br

Abstract. This article proposes to define a security policy for the use of computing resources available in the computer labs of an academic institution, using the use of free tools to manage the firewall services, proxy and DHCP (Dynamic Host Control Panel), the to guide the students, teachers, coordinators and service providers on the guidelines relating to information security and use of computational resources of computer labs to protect information assets owned or under their custody, against internal or external threats, deliberate or incidental.

Resumo. *Este artigo propõe a definição de uma política de segurança para uso dos recursos computacionais disponíveis nos laboratórios de informática de uma instituição acadêmica, fazendo uso de ferramentas livres para gerenciar os serviços de firewall, proxy e DHCP (Dynamic Host Control Panel), a fim de orientar os discentes, docentes, coordenadores e prestadores de serviços sobre as diretrizes referentes a segurança da informação e utilização dos recursos computacionais dos laboratórios de informática para proteger ativos da informação de sua propriedade ou sob sua custódia, contra ameaças internas ou externas, deliberadas ou acidentais.*

Palavras-Chave: *Firewall; Segurança da Informação; Proxy; DHCP; Política de segurança*

1. Introdução

Estamos em um ponto crucial no uso da tecnologia para estender e fortalecer a capacidade de comunicação. A maneira como as interações sociais, políticas, pessoais, ocorrem atualmente está mudando rapidamente para acompanhar a evolução da *internet* (BAGURDES, 2015).

A informação é um ativo importante e pode ser representada de diversas formas, independente do meio na qual trafega, ela é fundamental para o funcionamento das organizações e, consequentemente, precisa ser protegida adequadamente. Conforme aponta Morimoto (2011), cada vez mais, as tecnologias de acesso e transmissão de dados são empregadas, o que torna mais complicado manter uma rede segura, já que existem formas inadequadas de se obter informações que poderão ser usadas para prejudicar os processos, tornando-se cada vez mais necessário a proteção das informações que trafegam na rede.

De acordo com a norma ISO 27002 *International Organization for Standardization* a segurança da informação é a proteção contra vários tipos de ameaças com o intuito de garantir a continuidade dos negócios, minimizar os riscos, maximizar o retorno sobre os investimentos e as oportunidades, podendo ser alcançada a partir da implementação de um conjunto de controles adequados, sejam eles de políticas, processos, procedimentos, estrutura organizacionais e funções de *hardware* e *software*.

Ainda subsidiada pela ISO 27002 para definir o nível de segurança em um sistema de computação é necessário de medidas para isso, pensando nelas, será apresentado os pilares fundamentais da segurança da informação.

Na Figura 1 podemos identificar esses pilares, onde na sequencia eles serão abordados.

Figura 1. Pilares da segurança da informação
Fonte: (SILVA, 2015)

A integridade da informação consiste na garantia da exatidão da informação e dos métodos de processamento não sofrendo nenhuma espécie de modificação durante sua transmissão ou armazenamento. Temos também a confidencialidade na qual é a garantia que a informação possa ser acessada somente por pessoas autorizadas a terem acesso, garantindo a privacidade das informações. E por fim a disponibilidade que garante de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário (ISO, 27002).

Partindo desses princípios, podemos constatar que atualmente na instituição de ensino na qual foi escolhida como estudo de caso, não há nenhum tipo de autenticação para os usuários se conectarem à rede e tão pouco regras para utilização dos seus serviços, podendo, acarretar em vulnerabilidades a serem exploradas por indivíduos não autorizados. Devido ao porte da instituição acadêmica, bem como a quantidade de pessoas que fazem uso dos recursos computacionais disponíveis nos laboratórios de informática, percebe-se a necessidade da definição de uma política de segurança para regulamentar a utilização dos recursos de redes disponíveis nos laboratórios de informática.

Buscando sanar os problemas elencados acima, este trabalho tem o objetivo de propor uma política de segurança para regulamentar a utilização da rede e Internet dos

laboratórios de informática da instituição. Para validar essa política, foram implementados os serviços de *proxy, firewall e* DHCP (*Dynamic Host Control Panel*). O serviço de *firewall* será efetuado através da ferramenta *iptables,* onde será acoplado a um servidor *proxy* subsidiado pelo *squid* para validar as regras da política de segurança. Por fim, teremos a etapa de endereçamento dos *hosts* na qual será realizada dinamicamente, através do serviço de DHCP.

2. Referencial Teórico

Esta seção apresenta um breve referencial teórico no desenvolvimento deste trabalho, abordando questões referentes a redes de computadores, sistema *linux*, segurança da informação, *firewall*, *proxies*, política de segurança, Xenserver e Xencenter.

2.1. Redes de computadores

Segundo Maia (2013) uma rede de computadores é um conjunto de dispositivos interconectados com a finalidade de trocar informações e compartilhar recursos. As redes podem ser classificadas conforme a distância física entre os dispositivos que a compõem, geograficamente e podem ser divididas em redes pessoais, redes locais, redes metropolitanas e redes distribuídas. A Figura 2 apresenta alguns componentes que compõe a estrutura física de uma rede de computadores.

Figura 2: Componentes de uma rede de computadores

Fonte: (BAGURDES, 2015)

2.2. Sistemas Linux

Um sistema operacional é um conjunto de rotinas executado pelo processador, de forma semelhante ao *software*. Sua principal função é controlar o funcionamento do *hardware*, gerenciando sua utilização e o compartilhamento dos seus diversos recursos, como processadores, memorias e dispositivos de entrada e saída (TANENBAUM, 2010).

Já Deitel (2005), diz que sistema operacional é um *software* que habilita as aplicações a interagir com o *hardware* de um computador. O *software* que contém os componentes centrais do sistema operacional é denominado núcleo, estes sistemas podem ser encontrados em dispositivos que vão de telefones celulares e automóveis a computadores pessoais e *mainframes*.

Segundo Sobell (2009), o Linux surgiu como um sistema operacional poderoso e inovador que funciona com o Unix. Sua popularidade ultrapassa aquela dos seus predecessores, embora imite o Unix em vários aspectos, o Linux se difere dele de diversas formas, o *kernel* do Linux é implementado independentemente do BSD (*Berkeley Software Distribution*) e do *System* V e seu desenvolvimento continuo ocorre através de esforços combinados de diversas pessoas pelo mundo. A figura 3 apresenta a estrutura do sistema operacional Linux, na sequência os itens da estrutura são abordados.

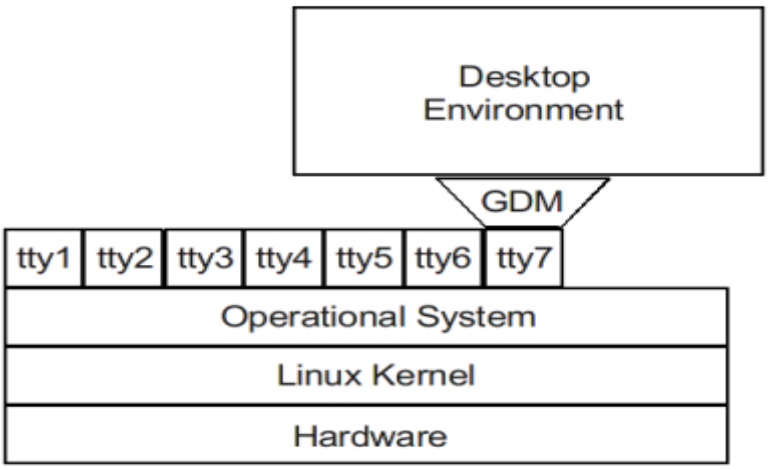

Figura 3. Estrutura do Linux

Fonte: (MAIA, 2013)

Segundo Maia (2013), a arquitetura do sistema operacional Linux pode ser dividida nos seguintes itens:

Hardware - Dispositivos que estão disponíveis para o uso do sistema, tais como *cd-rom*, placa de rede, controladora SCSI (*Small Computer System Interface*) entre outros;

Kernel - O núcleo do sistema operacional é quem faz todas as interações com o *hardware* da máquina, interpretando requisições feitas pelas camadas acima desta;

Sistema Operacional – Essa camada tem como função auxiliar e abrigar todos os aplicativos das camadas superiores.

TtyN – Terminais virtuais onde são executados os comandos e definidas as configurações. As *tty* interpretam os comandos informados por um humano e convertem os mesmos para uma linguagem que a máquina entenda.

DM - A "*layer*" de "*Display Manager*" é responsável por gerenciar os "*logins*" - validação de usuários - na interface gráfica e escolher o tipo de ambiente gráfico que deve ser executado;

Desktop Environment - Mais conhecido como ambiente de trabalho, é responsável por abrigar todos os programas que necessitam de um ambiente gráfico para funcionar.

2.3. Segurança da Informação

A segurança da informação visa garantir a integridade, confidencialidade e disponibilidade das informações processadas pela instituição, podendo ser considerada, atualmente o bem mais valioso de uma organização (CERT.br, 2016).

Existem muitas ameaças que podem compromete-las e trazer prejuízos para as organizações, assim a ISSO 27002, apresenta um conjunto de controles, que quando implementados e seguidos, reduzem os riscos de perda de confidencialidade, integridade e disponibilidade. A política de segurança da informação é um desses controles.

Quando se refere a segurança em redes de computadores, existem dois tipos de preocupações que devem ser abordadas, segurança da infraestrutura de rede e segurança da informação (BAGURDES, 2015). A segurança da infraestrutura de rede inclui a segurança física dos dispositivos que fornecem conectividade a rede e a prevenção de acesso não autorizado ao *software* de gerenciamento presente neles. Já a segurança da informação refere-se a proteção dos dados contidas nos pacotes transmitidos pela rede e das informações armazenadas nos dispositivos conectados à rede. Algumas medidas de segurança devem ser tomadas em uma rede de computadores para que assim elas sejam capazes de inibir os seguintes fatores:

- Impedir divulgação da informação não autorizada;
- Impedir roubo de identidade;
- Impedir modificação não autorizada de informações;
- Impedir a negação de serviço DoS (*Denial of Service*).

2.4. Firewall

Tanenbaum (2010), comparou um serviço de *firewall* como uma adaptação moderna do antigo sistema ativo de defesa medieval: cavar um fosso bem fundo ao redor do seu castelo, onde esse projeto obrigava todos que entrassem ou saíssem do castelo a passar por uma única ponte levadiça onde podiam ser inspecionados pela polícia de entrada e saída.

Já Cheswick (2003) dizia que o serviço de *firewall* é um ponto entre duas ou mais redes, no qual circula todo o trafego, a partir desse único ponto é possível controlar e autenticar as informações que circulam na rede, além de registrar, por meio de *logs*, todo o conteúdo, facilitando sua auditoria.

Os produtos de *firewall* fazem uso de várias técnicas e tipos para determinarem o que é ou não permitido em uma rede, tais técnicas e tipos são apresentados a seguir na Tabela 1:

Tabela 1: Técnicas de firewall

Técnica	Descrição
Filtragem de pacote	Impede ou permite o acesso com base em endereços de IP (*Internet Protocol*) ou MAC (*Media Access Control*).
Filtragem de aplicativo	Impede ou permite o acesso por tipos de aplicativos específicos com base em número de portas.
Filtragem de URL	Impede ou permite o acesso a sites com base em URL (*Uniform Resource Locator*) específicos ou em palavras chave.
Inspeção de status completo do pacote (SPI)	Os pacotes de entrada devem ser repostos legítimas ás solicitações de *hosts* internos. O provedor de internet também pode incluir recurso para reconhecer e filtrar tipos específicos de ataques, como negação de serviço DoS *(Denial of Service*).

O *firewall* pode ser representado por quatro tipos principais conforme demonstrado na Tabela 2.

Tabela 2: Tipos de firewall

Tipo de Firewall	Descrição
Firewall com base em dispositivo	É um *firewall* integrado a um dispositivo de *hardware* dedicado conhecido como um dispositivo de segurança.
Firewalls com base em servidor	Consiste em um aplicativo de *firewall* que é executado em um sistema operacional de rede como UNIX ou Windows.
Firewall integrado	Um *firewall* integrado é implementado ao adicionar a funcionalidade de *firewall* a um dispositivo existente, como um roteador.
Firewall pessoal	Os *firewalls* pessoais residem em computadores *host* e não foram projetados para implementações em uma LAN (Local *Area Network*). Eles podem estar disponíveis por padrão no sistema operacional ou podem vir de um fornecedor externo.

2.4.1. Proxies

O *proxy* pode ser considerado um *firewall* a nível de aplicação, tendo como principal função o armazenamento do conteúdo acessado em sua cache, podendo ser objetos, páginas *web*, imagens, arquivos multimídia, *software* entre outros tipos de conteúdo, agindo sempre como intermediador entre os usuários e os servidores.

Segundo Nakamura e Geus (2007) uma das funções dos *proxies* é a possibilidade de registrar todo o tráfego em uma rede, seja ele de origem ou destino, podendo desse modo ativar um sistema de alarme quando um trafego não apropriado em uma rede estiver em andamento.

O *proxy* pode ser reconhecido por dois tipos, sendo eles transparente e não transparente. No modo não transparente, é necessário configurar em cada *host* conectado à rede através do navegador as configurações especificas do servidor proxy, como o endereço de IP e porta que ele funciona para ter acesso à Internet. Já o *proxy* transparente trabalha escutando todas as conexões na porta 80, mesmo que alguém tente desabilitá-lo manualmente nas configurações do navegador ele continuará sendo utilizado (MORIMOTO, 2008).

Na Figura 4 é apresentado o exemplo de um servidor *proxy* funcionando em conjunto com o firewall.

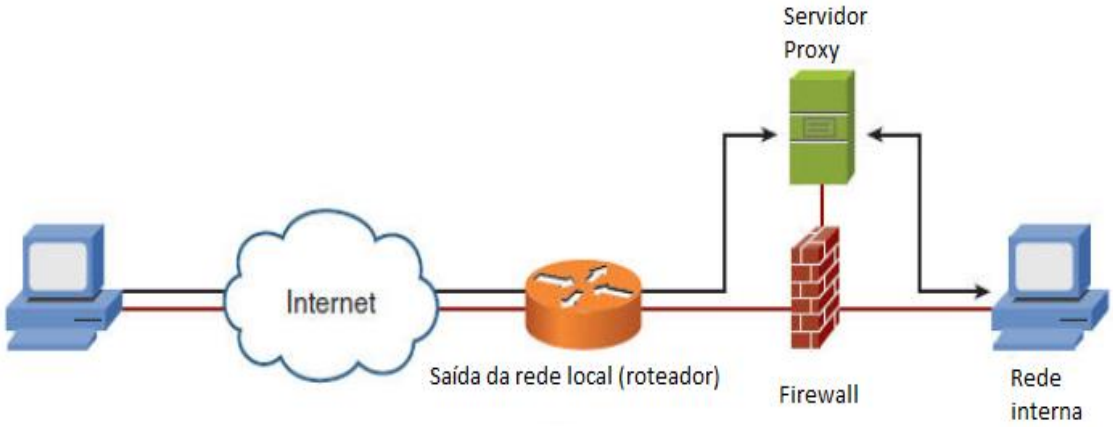

Figura 4: Funcionamento de um proxy
Fonte: (Adaptado de Mason, 2011)

2.5. Política de Segurança

Política de segurança da informação é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações (CERT.br, 2016).

Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Certa ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais: (1) confidencialidade; (2) integridade e (3) disponibilidade. A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui

direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação (CERT.br, 2016).

De acordo com Ferreira (2008) deve-se utilizar uma visão metódica, criteriosa e técnica na elaboração, de forma que possam ser sugeridas alterações na configuração de equipamentos, na escolha de tecnologia, na definição de responsabilidades, e por fim, na elaboração das políticas com o perfil da instituição e dos negócios que ela prática.

Comer (2007) relata que uma política de segurança, é uma tarefa complicada, já que cada instituição deve decidir quais aspectos de proteção são mais importantes, e, frequentemente, assumir um balanço entre a segurança e a facilidade do uso. Uma instituição pode considerar alguns aspectos conforme apresentados na figura 5.

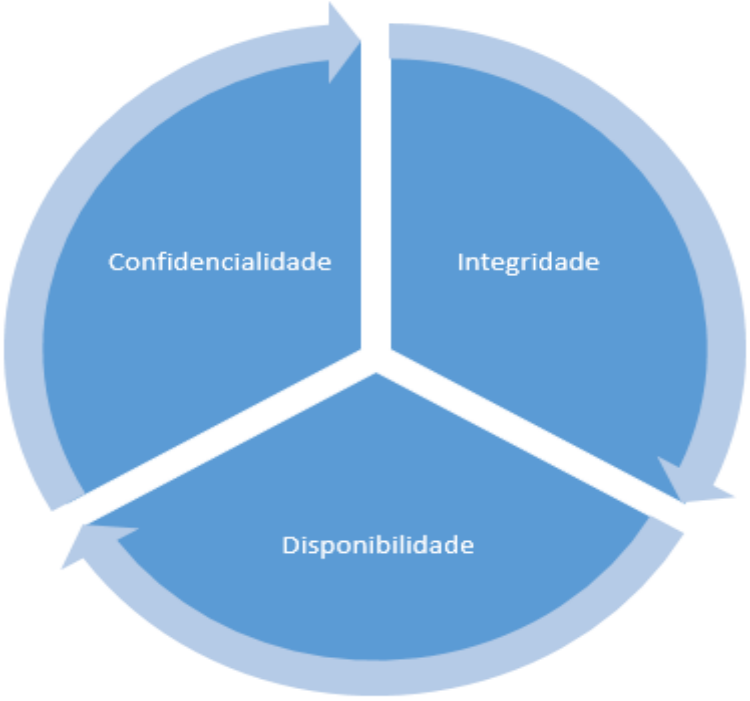

Figura 5: Conceitos de Confidencialidade, Integridade e Disponibilidade

As propriedades da Figura 5, são conhecidas como CID e são definidas por (BAGURDES, 2015), como:

A confidencialidade garante de que a informação é acessível somente por pessoas autorizadas a terem acesso. Já a integridade é a precisão e a preservação da exatidão da informação e dos métodos de processamento. E por fim a disponibilidade que consiste na garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Segundo Spanceski (2004) para a implementação da política de segurança a sugestão é que sejam criados vários documentos referentes a cada política, e estes documentos sejam disponibilizados ao acesso de todos os funcionários, além disso, que sejam divulgados para os alunos e os demais envolvidos. Durante a implementação da política de segurança toda a organização deve ser envolvida e se necessário devem ser feitos treinamentos conscientizando à importância da segurança e do envolvimento de cada um na utilização e divulgação da política.

2.6. Squid

O *squid* é um serviço de *proxy* baseado em Linux licenciado nos termos da GPL (*General Public License*) utilizado como *firewall* a nível de aplicação, por se tratar de um servidor *proxy* que intermedia a rede privada e a Internet, realizando a análise do conteúdo dos pacotes procurando por restrições previamente especificadas nas regras de seu arquivo de configuração.

Segundo Marcelo (2005) o *squid* oferece a possibilidade de restrição de acessos às páginas proibidas, para usuários ou grupos, podendo também limitar horários para os acessos. É possível também, liberar o acesso somente de determinadas categorias de domínios (.gov, .edu, .mil, e outros) e ainda proibir downloads de certos arquivos, seja por nome ou por extensões (.exe, .com, .bat, .mp3, e outros).

Há muitas maneiras de configurar este serviço, onde uma das mais populares é o uso de servidores proxy, que permitem o acesso aos serviços da Internet com segurança e economia de recursos (PINHEIRO, 2010). Entre as vantagens do servidor *proxy Squid*, destacam-se:

- Possibilidade de impor restrições de acesso com base no horário, *login*, endereço IP da máquina, fornecendo flexibilidade ao administrador de rede que precisa deixar o conteúdo livre em determinados horários.
- Operar como um cache de páginas e arquivos armazenando informações já acessadas conforme ilustra a figura 6, onde alguém acessa uma página que já foi carregada, o *proxy* envia os dados que guardou no cache sem precisar acessar a mesma página repetidamente. Isso pode gerar uma economia de banda tornando o acesso mais otimizado sem necessidade de investir em uma conexão mais rápida.

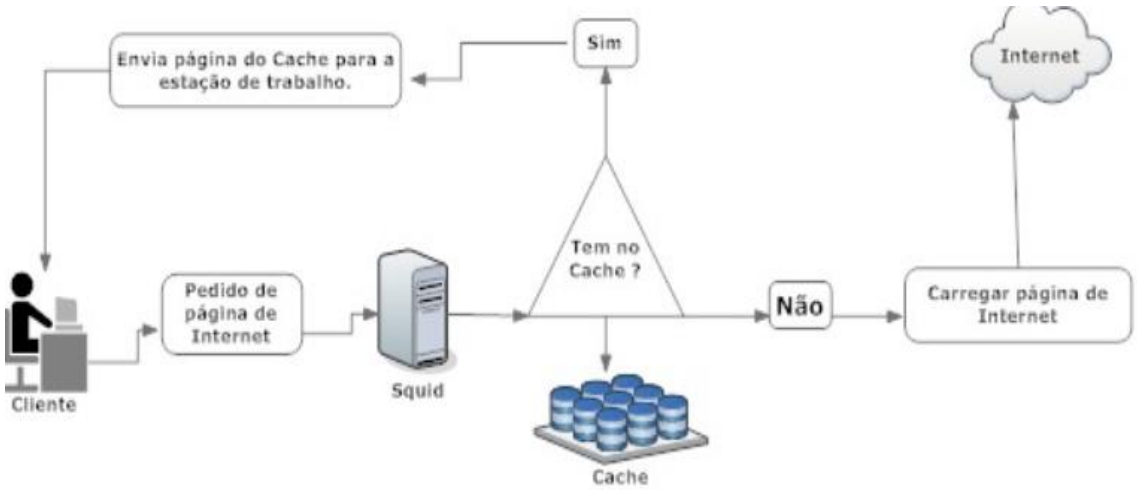

Figura 6 – Proxy cache

Fonte: (SILVA, 2010)

- Dependendo da configuração, o *proxy* pode apenas acelerar o acesso às páginas ou servir como um verdadeiro cache de arquivos, armazenando atualizações do sistema, downloads diversos e pacotes de instalações.

- Utiliza arquivos de logs para registrar os acessos dos usuários, onde o administrador de rede poderá visualizar os acessos posteriormente, usando os relatórios do SARG (*Squid Analysis Report Generator*), assim ele saberá quem acessou o que e em quais horários, isto pode ser subsidio para as listas de bloqueios e auditoria.
- Outra vantagem interessante do *proxy* são as políticas de controle denominadas ACL (*Acces Control List*). Segundo MORIMOTO (2008) através delas é possível criar regras de controle de acesso à internet, das mais diversas formas possíveis, definindo quais usuários ou equipamentos tem permissão a determinados tipos de serviços na rede.

2.7 Iptables

O *Iptables* é serviço baseado em Linux que permite a implementação de filtros e tratamento de pacotes através de simples tabelas que funcionam baseados no endereço/porta de origem/destino do pacote, prioridade, etc. Segundo RIBEIRO (2004) o *iptables* utiliza a infraestrutura do *kernel* através do *netfilter* para saber como filtrar e até alterar dados empacotados com base em diversos critérios, algumas características do *iptables* são destacadas a seguir:

- Rápido, seguro e estável;
- Suporta redirecionamento de portas;
- Suporta SNAT (modificação do endereço de origem das máquinas para um único endereço ou faixa de IPs);
- Suporta DNAT (modificação do endereço de destino das máquinas para um único endereço ou faixa de IPs);
- Suporta interfaces de origem e destino de pacotes;
- Possui mecanismos internos para rejeição automática de pacotes duvidosos ou mal formados.

Segundo Lima (2000) um bom *firewall* não deve permitir que pacotes inválidos entrem na rede protegida. Os pacotes inválidos são aqueles que não satisfazem as regras de filtragem e/ou não pertencem a nenhuma conexão ou sessão existente através do firewall. A figura 7 ilustra a filtragem de conteúdo pelo firewall. Nesse exemplo o firewall nega pacotes de origem à rede LAN com destino ao site www.sexo.com.br.

Figura 7. Filtragem por palavras

Fonte: (SILVA, 2010)

2.8 DHCP - *Dynamnic Host Configuration Protocol*

O serviço de protocolo de configuração dinâmica do *host*, mais conhecido como DHCP permite que os dispositivos em uma rede obtenham endereços IP (Internet *Protocol*), máscara de sub-rede, *gateway*, e outros parâmetros de rede automaticamente, isso é conhecido como endereçamento dinâmico.

O servidor DHCP mantém um *pool* de endereços IP e arrenda um endereço a qualquer cliente habilitado por DHCP quando o cliente é ativado. Os endereços IP são dinâmicos (arrendados), em vez de estáticos (atribuídos permanentemente), os endereços em desuso são automaticamente retornados ao conjunto de realocação.

Figura 8: Funcionamento do DHCP

Fonte: (BAGURDES, 2015)

Como mostrado na figura 8, quando um dispositivo configurado com DHCP inicia ou se conecta à rede, o cliente transmite uma mensagem de descoberta DHCP (DHCPDISCOVER) para identificar qualquer servidor DHCP disponível na rede. Um servidor DHCP responde com uma mensagem de pacote DHCP (DHCPOFFER). A mensagem de oferta contém o endereço IP e a máscara de sub-rede a serem atribuídos, o endereço IP do servidor DNS e o endereço IP de *gateway* padrão. A oferta de locação também inclui a duração da locação. O cliente pode receber diversos pacotes DHCPOFFER se houver mais de um servidor DHCP na rede local; portanto, deve escolher entre eles e transmitir uma mensagem de solicitação de DHCP (DHCPREQUEST) que identifique o servidor explícito e a oferta de arrendamento que o cliente está aceitando. Presumindo que o endereço IP solicitado pelo cliente, ou oferecido pelo servidor, ainda seja válido, o servidor retornará uma mensagem de confirmação DHCP (DHCPACK) que confirma para o cliente que o arrendamento foi finalizado.

2.9 XenServer

Baseado em um *kernel* Linux, o XenServer é um *software open source*, portanto não há custos com licenças associado a sua implementação. Possui suporte às arquiteturas x86, x86_64 e ia64, o XenServer é um sistema *hypervisor* do tipo 1, ou seja, é instalado diretamente sobre o *hardware*, eliminando a necessidade de um sistema operacional hospedeiro, permitindo a criação de máquinas virtuais através de um gerenciador instalado em uma estação remota (XenCenter), executado no Windows. Ele suporta virtualização do tipo paravirtualização sem emulação por *software* e também *Full Virtualization*, que envolve emulação e depende de assistência por *hardware* para que

funcione (Intel VT-X /AMD-V (*Advanced Micro Devices - Virtualization*) e é muito mais rápida.

2.9.1 Citrix XenCenter

O Citrix XenCenter oferece funções de monitoramento, gerenciamento e administração geral de VMs (*Virtual Machine*) em uma única interface que permite à equipe de TI gerenciar facilmente centenas de máquinas virtuais a partir de um console de gerenciamento centralizado e altamente disponível, que pode ser instalado em qualquer desktop Windows.

3. Trabalhos Correlatos

Nesta seção serão apresentados alguns trabalhos correlacionados ao apresentado neste artigo.

3.1. Segmentação e Roteamento de Vlan's em Servidores Linux Utilizando o Protocolo 802.1Q

O trabalho apresentado por Wagner (2014) surgiu da necessidade de aumentar a segurança, privacidade e melhorar o desempenho da rede de computadores do CITEC (Centro de Inovação Tecnológica) da UTFPR (Universidade Tecnológica Federal do Paraná), tendo como proposta a utilização de segmentação através da criação de VLANs (*Virtual Local Area Network*) para aumentar a segurança e privacidade das informações pertencentes a cada sub-rede criada.

A segmentação das redes visou trazer maior segurança para cada laboratório, através da criação de VLANs, facilitando todo o trabalho de roteamento e interconexão, onde toda a arquitetura utilizada foi implementada por meio de *software* livre possibilitando futuras implementações de novos serviços, podendo ser customizada de forma que possa atender diversas funcionalidades específicas que podem surgir.

Baseando-se nas regras de firewall já existentes foi gerada uma tabela de regras para acesso à rede com endereçamentos públicos utilizados com a DMZ. A regra padrão para acesso à DMZ foi a de bloqueio geral, liberando somente acesso do host em específico, ou seja, o firewall trabalha com uma lista branca, bloqueando qualquer tráfego não autorizado.

Wagner (2014) conclui que a segmentação da rede junto a utilização de VLANs tornou a rede mais estável, segura e escalável, diminuindo o custo da infraestrutura, possibilitando a fácil criação de novos grupos de trabalhos isolados. Outra vantagem percebida foi o uso de um equipamento de utiliza *software* livre, proporcionando liberdade para fazer futuras instalações que possam auxiliar a rede de forma rápida e com custo reduzido.

O trabalho desenvolvido por Wagner (2014) contribuiu para o desenvolvimento do presente trabalho ajudando na criação das configurações realizadas no servidor referente ao *proxy* e as VLANs.

3.2. Reestruturação da Rede para melhoria do Tráfego e segurança: a Reestruturação da Rede de computadores do DC

O trabalho apresentado por Teixeira *et al.* (2014) evidencia o uso da rede de computadores do DC (Departamento de Computação) da UFSCar (Universidade Federal de São Carlos). As redes de computadores do DC são redes TCP/IP *(Transmission Control Protocol/Internet Protocol*) baseada em *Ethernet* e composta de quatro segmentos fisicamente distintos, cada um com sua própria sub-rede de endereços IP:

- Rede de docentes e funcionários;
- Rede da pós graduação;
- Rede de equipamentos destinados aos alunos de graduação;
- Redes sem fio.

Antes da aplicação do trabalho, cada uma das redes tinha seu próprio segmento, mas foi possível observar que a divisão do fluxo não favorecia questão de confinamento de tráfego e tinha exposições de segurança indesejáveis. Não havia mecanismo de controle de banda e todo o controle de segurança era dificultado, a organização da rede impossibilitava o controle e monitoramento desejáveis de suas operações, sendo que o uso indevido da largura de banda ocorria com frequência.

Como solução para os problemas identificados foi realizado uma reestruturação para a rede de computadores do DC, para facilitar o seu gerenciamento, oferecer qualidade de serviço e melhorar a segurança dos equipamentos conectados, por meio da avalição da reestruturação física e lógica da rede.

Teixeira et al. (2014) concluíram que ao avaliar os resultados obtidos, através da reestruturação lógica será possível adicionar novos nós no segmento configurado. Foi identificado que os serviços mais usados utilizam protocolo TCP, mas que uma parte considerável do tráfego da rede é feito por UDP (*User Datagram Protocol*).

O trabalho apresentado por Teixeira (2014) contribui para a reestruturação da rede nos laboratórios da instituição na qual este trabalho está sendo aplicado como estudo de caso para facilitar o gerenciamento, desempenho e serviço de qualidade, melhorando a segurança dos equipamentos conectados a ela.

3.3. Política de segurança da informação - Desenvolvimento de um modelo voltado para instituição de ensino

O trabalho apresentado por Spanceski (2004) aborda um estudo sobre política de segurança da informação, sendo uma das principais medidas de segurança adotadas pelas organizações com o objetivo de garantir a segurança da informação. Dentre as medidas de segurança implantadas pelas organizações, para garantir a segurança da informação está a política de segurança que tem por objetivo definir normas, procedimentos, ferramentas e responsabilidades que deem ser seguidas pelos usuários das organizações, de modo a garantir a segurança da informação.

Conforme o autor afirma que após a implementação da política de segurança foi possível identificar algumas contribuições importantes, como:

- Identificação do cenário atual da segurança da informação e das medidas de segurança utilizadas pelas empresas;

- Estudo da utilização da importância da polícia de segurança como medida de segurança utilizada pelas empresas;
- Desenvolver um estudo sobre os modelos de políticas de segurança utilizadas em instituições de ensino;
- Desenvolvimento de um modelo de política de segurança.

O autor destaca que para a implementação da política a sugestão de que sejam criados vários documentos referentes a cada política e os mesmos sejam disponibilizados ao acesso de todos os funcionários, além disso que sejam divulgados para os alunos e os demais envolvidos. Se necessário devem ser feitos treinamentos conscientizando a importância da segurança da informação e do desenvolvimento de cada um na utilização e divulgação da política de segurança.

O trabalho desenvolvido por Spanceski (2004), contribui para a elaboração e definição da política de segurança destinada aos laboratórios de informática da instituição.

4. Definição da Política de Segurança

A utilização da infraestrutura tecnológica é fundamental para o desenvolvimento das atividades acadêmicas realizadas pelos alunos nos laboratórios de informática da instituição acadêmica sendo disponibilizada exclusivamente como ferramenta de trabalho e apoio acadêmico. Com isso, alguns procedimentos devem ser adotados para delinear o que é permitido ou não, bem como garantir o adequado desempenho dessas atividades. Assim, toda a rede interna, *hardware* e *software* dos laboratórios de informática estão sujeitos a monitoração e, portanto, o administrador da rede da instituição poderá manter histórico de acessos realizados aos seus sistemas.

A política de segurança definida por este trabalho é dividida em três grupos específicos, sendo o primeiro grupo referente ao uso de equipamentos pessoais nos laboratórios de informática, o segundo grupo é referente ao uso da rede e seus recursos dos laboratórios de informática, e por fim o terceiro que se diz respeito a adição de recursos para utilização nos laboratórios.

4.1 Grupo 1 – Equipamentos pessoais

Os equipamentos particulares devem seguir as seguintes normas de utilização**:**

a. O usuário é inteiramente responsável pela segurança dos dados nos equipamentos que sejam conectados à rede por ele;

b. O usuário será responsabilizado por quaisquer incidentes de segurança gerados ativa ou passivamente pelo equipamento por ele ligado à rede. O equipamento será desconectado da rede e o usuário sofrerá as sanções administrativas e legais que a instituição julgar cabível;

c. O usuário deverá observar a política de segurança da informação da instituição utilizando a rede somente para o desempenho das funções acadêmicas ou administrativas;

d. O usuário é responsável pelo licenciamento de software utilizado em seu equipamento, sendo vedada a instalação cujas licenças pertençam a instituição, salvo autorização especifica do administrador da rede;

e. A manutenção do equipamento e do *software* contido no mesmo é de total responsabilidade do usuário, não cabendo ao administrador de rede nenhum serviço referente ao suporte dos mesmos;

f. A criação e manutenção de copias de segurança (*backup*) dos arquivos contidos no equipamento são de inteira responsabilidade do usuário;

g. A instituição se reserva o direito de cancelar o acesso fornecido a qualquer momento sem prévio aviso.

4.2 Grupo 2 – Acesso aos serviços de rede dos laboratórios de informática

Os acessos originados em maquinas conectados à rede interna da instituição, com destino à Internet podem ser realizados através dos equipamentos pertencentes a instituição e também de equipamentos de uso pessoal dos alunos conectados à rede através dos pontos de acessos disponibilizado pela instituição ou por uma rede cabeada, caso esteja disponível.

A navegação a sites não relacionados diretamente à atividade acadêmica dos usuários não é proibida, porém seu uso deve ser feito de maneira equilibrada e responsável, para assegurar ao usuário e a instituição máxima segurança e desempenho no trabalho, de modo que abusos serão punidos com bloqueio de acesso a tais sites sem aviso prévio.

O bloqueio de conteúdo da internet fica a critério do administrador de rede e seguirá de acordo com a seguinte política para acessos a Internet:

a. Fica terminantemente proibida a navegação aos sites pertencentes as categorias: pornográfico e de caráter sexual; compartilhamento de arquivos (ex: *peer to peer,Bit Torrent, uTorrent*, MEGA, etc.); apologia ao terrorismo; apologia ás drogas; *crackers*; sites de relacionamento; jogos, salvo com conteúdo relacionado diretamente às atividades administrativas ou acadêmicas; violência e agressividade (racismo, preconceito, etc.); áudio e vídeo, salvo com conteúdo relacionado diretamente a atividades administrativas ou acadêmicas; conteúdo improprio, ofensivo, ilegal, discriminatório e similares, salvo quando pertinentes a conteúdos acadêmicos.

b. Não é permitida a troca de arquivos de vídeo ou música, bem como de quaisquer informações que estejam incluídas nas categorias acima;

c. É proibida a transferência de qualquer tipo de programa, jogo e similares, a partir da Internet, para a rede interna da instituição, com a exceção do administrador de rede com autorização especifica para tal;

d. É proibido acessar todo e qualquer site que apresente vulnerabilidade de segurança ou que possa comprometer, de alguma forma, a segurança e a integridade da rede.

4.3 Grupo 3 - Adição de recursos

É vedada aos usuários da rede a adição de quaisquer recursos, sejam eles microcomputadores, impressoras, roteadores, ou outros equipamentos. A adição de novos equipamentos por parte do usuário deve ser solicitada por comunicação interna e deverá ser aprovada pelo administrador de rede. Todos os equipamentos ligados à rede devem obedecer padrões de instalação, de designação de endereços e domínio, portanto, uma vez aprovada a solicitação, será realizada a adição do equipamento pelo administrador de rede.

5. Metodologia

Para o desenvolvimento deste trabalho, as seguintes etapas foram estabelecidas:

a) Levantamento bibliográfico

Na etapa inicial foi realizado o levantamento bibliográfico das informações pertinentes ao tema do trabalho. Também foi descrito a situação do ambiente atual para que possa estabelecer o parâmetro de avaliação entre solução proposta e a situação atual, a fim de analisar se as soluções serão validades.

b) Preparação do ambiente

Para a simulação do ambiente de implantação, inicialmente foi realizado a instalação do *XenServer* em um servidor disponibilizado pela instituição, este servidor possui as seguintes configurações:

- ✓ Processador *Intel Xeon* E5620 2.4Ghz,12MB Cache, HT, 1066 MHz
- ✓ 8GB de memória DDR3 1333MHZ
- ✓ Fonte de alimentação 580W real
- ✓ Disco rígido de 1TB, 7200rpm, 3.5,
- ✓ DVD 16X DVD-ROM, SATA, INTERNO.

Inicialmente foi realizado instalação do *XenServer* no servidor para virtualização do sistema utilizado para a implementação dos serviços de *firewall*, *proxy* e DHCP. O sistema virtualizado através da plataforma do *Xen* foi o Debian, uma distribuição Linux voltada para utilização em servidores.

c) Definição da política de segurança

Durante seu desenvolvimento houve a necessidade do envolvimento do técnico dos laboratórios de informática, técnico de tecnologia da informação, coordenador do curso de Análise e Desenvolvimento de Sistema para análise, argumentação, elaboração, compreensão e definição da política de segurança, após a definição da política foi realizado alguns testes em ambiente onde serão abordados na próxima etapa.

d) Testes

Após a implementação dos serviços propostos foram realizados experimentos em ambiente de teste, como a autenticação de usuários para acesso à Internet, registros de

acesso, bloqueio de alguns conteúdos proibidos conforme expressos na política de segurança.

7. Resultados

Após a implementação da solução proposta foi possível observar melhorias na rede, como a possibilidade do gerenciamento de acesso através dos *logs* registrado conforme demonstra a Figura 9 os acessos registrados pelo *log* do squid sendo exibidos pelo SARG (*Squid Analysis Report Generator)*.

Squid Analysis Report Generator

RelatÃ³rio do Squid

Period: 2016 Nov 16
Sort: bytes, reverse
Top users

Top sites
Sites & Users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		172.30.0.144	269	28.95M	99.79%	0.00%	100.00%	03:40:00	13,200,804	99.11%
2		172.30.0.145	5	24.20K	0.08%	0.00%	100.00%	00:00:07	7,653	0.06%
3		172.30.0.157	17	20.19K	0.07%	0.00%	100.00%	00:01:20	80,849	0.61%
4		172.30.0.137	3	8.22K	0.03%	0.00%	100.00%	00:00:00	931	0.01%
5		172.30.0.116	14	2.88K	0.01%	0.00%	100.00%	00:00:23	23,060	0.17%
6		172.30.0.124	4	2.17K	0.01%	0.00%	100.00%	00:00:03	3,762	0.03%
7		172.30.0.146	6	1.87K	0.01%	0.00%	100.00%	00:00:02	2,219	0.02%
8		172.30.0.122	1	312	0.00%	0.00%	100.00%	00:00:00	55	0.00%
		TOTAL	**319**	**29.01M**		**0.00%**	**100.00%**	**03:41:59**	**13,319,333**	
		AVERAGE	**39**	**3.62M**				**00:27:44**	**1,664,916**	

Generated by sarg-2.3.2 Nov-23-2011 on Nov/16/2016 19:35

Figura 9 – Relatório de log de acesso à Internet

Porém para que estes resultados fossem alcançados inicialmente foram realizadas configurações em diferentes serviços para ter o melhor desempenho e segurança durante a implementação. Inicialmente foi desenhado através do *Cisco Packet Tracer* uma estrutura resumida somente da rede dos laboratórios de internet até a infraestrutura da instituição, onde chega o link de internet, a Figura 10 apresenta tal situação.

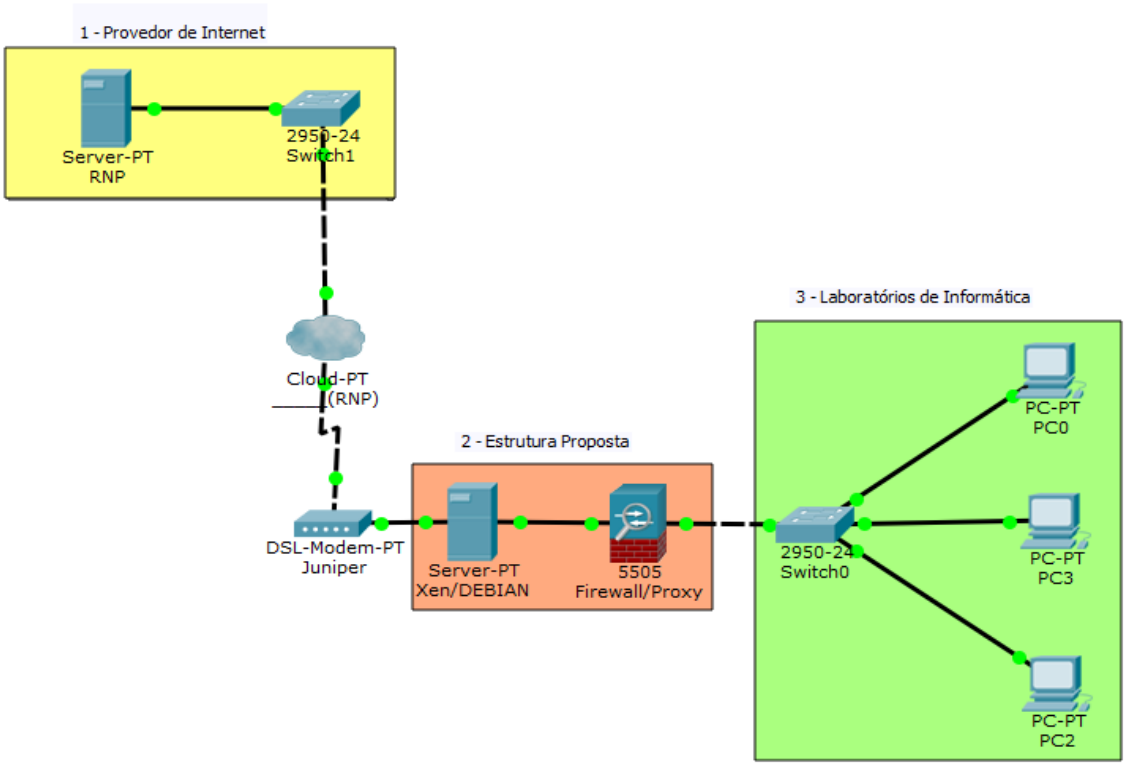

Figura 10 – Estrutura resumida da rede dos laboratórios de informática

Fonte: [Dos Autores, 2016]

O primeiro quadro diz respeito ao link de Internet que chega a infraestrutura de rede da instituição, o segundo quadro está relacionado ao servidor e aos serviços de *firewall*, *proxy* e DHCP nele hospedado para gerenciamento da rede dos laboratórios e por fim o terceiro quadro estão os laboratórios de informática, onde foi aplicada a política de segurança.

Conforme mencionado anteriormente, foi necessário realizar configurações de alguns serviços para que a solução proposta funcionasse corretamente, uma das configurações nas quais são de suma importância para funcionamento da solução foram as alterações nas interfaces de rede do servidor, no que se diz respeito às interfaces eth0 e eth1, tais configurações são apresentadas na Figura 11, onde inicialmente é realizado a configuração do IP da interface eth0, neste caso a interface que receberá a conexão da internet, o endereço de IP fixado na mesma é um endereço de IP fornecido pelo provedor de internet da instituição de ensino, caso este endereço seja diferente do endereço fornecido não é possível realizar a navegação pela rede, já na interface eth1 as configurações não são muito diferente, configura-se essa interface para que ela libere o acesso à internet para a rede local dos laboratórios de informática.

```
#As linhas abaixo ira configurar manualmente um ip na porta eth0
auto eth0
iface eth0 inet static
address 200.17.101.74
netmask 255.255.255.240
broadcast 200.17.101.255
network 200.17.101.64
gateway 200.17.101.65

#As linhas abaixo configuram a interface de rede eth1 manualmente
auto eth1
iface eth1 inet static
address 172.30.0.100
netmask 255.255.0.0
network 172.30.0.0
broadcast 172.30.255.255
```

Figura 11 – Configuração das interfaces de rede do servidor

Para navegação dos hosts a Internet existem configurações especificas, isso permite ao *proxy* facilidade no gerenciamento da rede. A Figura 12 apresenta uma parte do *script* do *proxy* implementado utilizado nos experimentos em ambiente de teste.

```
1  #Porta na qual o SQUID ira ouvir
2  http_port 3128
3
4  #Nome visível do servidor
5  visible_hostname ifprlabs
6
7  #Configurações minimas recomendadas
8  acl all src 0.0.0.0/0.0.0.0
9  acl manager proto cache_object
10 acl localhost src 127.0.0.1/255.255.255.255
11 acl SSL_ports port 443 563
12 acl Safe_ports port 80 # http
13 acl Safe_ports port 21 # ftp
14 acl Safe_ports port 443 563 # https, snews
15 acl Safe_ports port 70 # gopher
16 acl Safe_ports port 210 # wais
17 acl Safe_ports port 280 # http-mgmt
18 acl Safe_ports port 488 # gss-http
19 acl Safe_ports port 591 # filemaker
20 acl Safe_ports port 777 # multiling http
21 acl Safe_ports port 901 # swat
22 acl Safe_ports port 1025-65535 # portas altas
23
24 #Autenticação dos usuários para ter acesso a Internet
25 auth_param basic realm Autenticação de usuários
26 auth_param basic program /usr/lib/squid3/ncsa_auth /etc/squid3/squid_passwd
27 acl autenticados proxy_auth REQUIRED
28 http_access allow autenticados
```

Figura 12 – Script do proxy

Podemos dar ênfase aos trechos importantes do script do *proxy*. No primeiro momento pode observar que a porta padrão de operação do *squid* é a 3128 que se diz respeito a (linha 2), logo abaixo o nome visível para os *hosts* na (linha 5) e em seguida

as configurações das portas consideradas seguras, posteriormente a partir da linha 24 até a linha 28 são configurados a autenticação dos usuários.

8. Considerações Finais

Durante a realização deste trabalho foi possível identificar como se encontrava a rede de computadores dos laboratórios de informática da instituição, bem como a demanda de serviços que necessitam da mesma. Além disso foi possível observar situações relacionadas à segurança e gerenciamento das informações que circulam pela rede.

A partir das informações registradas no log, pôde-se observar um ambiente mais claro para a configuração e definição das regras de *proxy* e *firewall* e com isso atingir expectativas de gerenciamento e segurança da rede de computadores.

Considerando a complexibilidade da implantação em um ambiente de segurança de redes, houveram pontos mais complicados, pois alguns projetos tais como o desenvolvimento de projetos da instituição que são desenvolvidos dentro dos laboratórios não podiam ficar sem acesso à rede.

A principal contribuição deste estudo de caso foi a implementação de um ambiente segurança, gerenciamento na rede de computadores nos laboratórios de informática e a definição da política de segurança, pois mesmo que de forma indireta pretende-se que melhorar de alguma forma os serviços oferecidos pela rede

Através da política de segurança observou-se a reponsabilidade por parte dos usuários em relação a segurança de seus equipamentos, uso dos recursos de rede, *software* particular, manutenção foram identificadas conforme o esperado da política, a navegação a sites não relacionados a atividade acadêmica não foram proibidos, porém o uso destes foi identificado como equilibrado e responsável, segurando ao usuário e a instituição segurança e desempenho no trabalho, a adição de recursos de roteadores, pontos de acessos e outros equipamentos foram diminuídos, pois a política orienta quais procedimentos são necessários para utilização destes equipamentos.

Como trabalhos futuros ainda existem pontos a serem melhorados na rede de computadores dos laboratórios de informática, tais como:

- Implementação dos serviços de IPS (*Intrusion Prevention System*) para impedir possíveis incidentes e IDS (*Intrusion Detection System*) para detectar manipulações de sistemas de computadores indesejadas, normalmente através da internet.
- Desenvolvimento de uma interface web para facilitar o gerenciamento dos recursos oferecidos pelo *proxy*.

Referências

ABNT (2005). NBR ISO/IEC 27002 - Tecnologia da informação. Técnicas de segurança. Código de prática para a gestão da segurança da informação. ABNT.

ABREU, F. R.; PIRES, H. D. (2004) Gerência de Redes. Trabalho apresentado na Disciplina de Redes de Computadores I, Departamento de Engenharia de Telecomunicações, Universidade Federal Fluminense. Disponível em: <http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf>. Acessado em 20 de agosto de 2016.

BAGURDES, R. (2015). Cisco CCNA: Introduction to networking. In Computer Science, Technology and Applications Computer Networks. Nova Science Publishers.

CERT.br (2016). Centro de estudos, respostas e tratamento de incidentes de segurança no Brasil. Disponível em: http://www4.planalto.gov.br/cgti/assuntos/publicacoes/2511466.pdf. Acessado em: 20 de Agosto de 2016.

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviel D. Firewalls and Internet security: repelling the wily hacker. Addison-Wesley Longman Publishing Co., Inc., 2003.

COMER, D. E. 2007 Redes de computadores e internet: abrange transmissão de dados, ligações inter-redes, web e aplicações. 4. ed. Porto Alegre: Bookman

DEITEL, H.M., Deitel, P.J., CHOFFNES, D. R, Sistemas Operacionais, 3 Ed. Prentice Hall, 2005

FRANCIS, B. Machado; MAIA, Luiz Paulo. Arquitetura de Sistemas Operacionais. 2013.

FERRIRA, F. N. F.; ARAUJO, M. T. (2008). Política de Segurança da Informação: Guia Prático Para Elaboração e Implementação. CIENCIA MODERNA.

GABBAY, Max Simon. Fatores influenciadores da implementação de ações de gestão de segurança da informação: um estudo com executivos e gerentes de tecnologia da informação das empresas do Rio Grande do Norte. 2006.

LIMA, Marcelo Barbosa. Provisão de Serviços Inseguros Usando Filtros de Pacotes com Estados. São Paulo: UNICAMP–Campinas, 2000.

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

NAKAMURA, E. T.; GEUS, P. L. (2007). Segurança de Redes em Ambientes Cooperativos. Novatec.

PINHEIRO, A. C. S. Uso e configuração do Squid como servidor proxy. [s.n.], 2010. Disponível em: http://www.squid-cache.org.br/index.php?option=com_content&task=view&id=82&Itemid=27. Acessado em: 20 de Agosto de 2016.

MARCELO, Antonio. Squid-Configurando o Proxy para Linux (5a edição). Brasport, 2006.

RIBEIRO, U. Certificação Linux. Rio de Janeiro: Axcel Books, 2004.

SPANCESKI, F. R. (2004). Política de segurança da informação: desenvolvimento de um modelo voltado para instituições de ensino. Instituto Superior de Tupy – Joinville, SC. Brasil – Trabalho de Conclusão de Curso em Sistemas de Informação.

TANENBAUM, A. S; WETHERALL, D. J. Redes de Computadores. 5. Ed. São Paulo: Pearson Prentice Hall, 2011.

TANENBAUM, Andrew S.; GONÇALVES, Ronaldo AL. CONSULARO, Luís A.(Trad.). Sistemas Operacionais Modernos. 3ª Ed. São Paulo: Prentice Hall, 2010.

TEIXEIRA, G. S. O.; SEGATTO, G.; MOREIRA, J. (2014). Reestruturação de rede para melhoria do trafego e segurança: a reestruturação da rede de computadores do DC. Revista Tecnologias, Infraestrutura e Software. UFSCAR, 3(1).

SILVA, Alexsandro Queiroz da. Implantação de servidor proxy utilizando o Squid em modo não autenticado, junto com o DansGuardian para controle de conteúdo na instituição de ensino. 2015.

SOBELL, Mark G. Um guia prático Linux de comandos, editores e programação de Shell. Rio de Janeiro: Alta Books, 2009.

NAKAMURA, Emilio Tissato; GEUS, Paulo Licio. Segurança de Redes: em ambientes cooperativos. São Paulo: Novatec, 2007.

WAGNER, D. E. (2014). Segmentação e roteamento de vlan's em servidores Linux utilizando o protocolo 802.1Q. Universidade Tecnológica Federal do Paraná, departamento acadêmico de eletrônica, Curso de Especialização em Software Livre aplicado à Telemática, Curitiba/PR. Disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/1840/1/CT_CESOL_I_2012_03.pdf. Acessado em: 20 de Agosto de 2016.