Implantação de Um Ambiente de Segurança de Redes de Computadores: Um Estudo de Caso na Prefeitura Municipal de Palmeira das Missões - RS

Denison Molina[1], Sidnei Renato Silveira[2], Fernando Beux dos Santos[3]

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

denisonmolina@gmail.com, sidneirenato.silveira@gmail.com, fernandobeux@gmail.com,

Resumo. *Este artigo apresenta um estudo de caso envolvendo a implantação de um ambiente seguro na rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS, por meio da definição de uma infraestrutura física e lógica, apoiada em conceitos de Gerência de Redes de Computadores e Segurança da Informação. Por meio da criação de VLANs (Virtual Local Area Network) e definição da DMZ (Demilitarized Zone), deseja-se atingir o nível de segurança e gerência de redes desejado pelo departamento de informática, assim como proporcionar uma maior confiabilidade e integridade das informações que trafegam na rede para que os usuários possam executar suas tarefas de forma mais dinâmica em um ambiente seguro e ágil.*

Palavras-Chave*: Vlans; DMZ; Segurança da Informação.*

Abstract. *This paper presents a case study involving the deployment of a secure environment on the computer network at the City Hall in Palmeira das Missões - RS, throughout the definition of a physical and logical infrastructure, supported at concepts of management of computer networks and information security. Through the creation of Vlans (Virtual Local Areas Networks) and definition of DMZ (Demilitarized Zone) is desired to achieve the level of security and network management required by the IT department, as well as provide greater reliability and integrity of information that travel on the network so that the users can perform their tasks more dynamically in a secure and agile environment.*

Keywords*: Vlans, DMZ, Information Security.*

1. Introdução

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

Além disso, cada vez mais tecnologias diferentes de acesso e transmissão de dados estão sendo empregadas, o que torna manter uma rede segura, uma tarefa mais complicada, já que existem diversas formas inadequadas de se obter informações que poderão ser usadas para prejudicar os processos. Neste sentido, torna-se cada vez mais necessário a proteção dos dados que trafegam na rede [MORIMOTO 2011].

A rede de computadores da Prefeitura Municipal de Palmeira as Missões – RS envolve um órgão público, que gerencia muitas informações, tais como informações de contribuintes referentes a débitos e vínculos; contas contábeis com movimentações financeiras públicas; senhas, que devem se manter confidenciais e livres de qualquer problema como (invasão de privacidade, inconsistência de dados); entre outras informações, faz-se necessário proteger os dados que trafegam e são armazenados nos computadores desta rede.

A implantação de um ambiente de segurança na rede de computadores em questão visou trazer melhor qualidade e agilidade a todos os setores e serviços que necessitam da rede para funcionar, da mesma forma que proporciona um ambiente mais seguro e ágil para que todos os usuários da rede possam exercer suas tarefas de forma mais dinâmica. Para a implantação deste ambiente foram aplicados os conceitos de VLANs (*Virtual Local Area Network*) e DMZ (*Demilitarized Zone*), permitindo a definição de uma infraestrutura física e lógica de rede de computadores para atender as necessidades da organização.

Neste contexto, este artigo apresenta, na seção 2, um referencial teórico destacando os conceitos que envolvem as áreas de redes de computadores e segurança da informação. A seção 3 apresenta alguns trabalhos correlacionados ao proposto, visando compor o estado da arte. A solução para a implementação de um ambiente seguro na rede de computadores da Prefeitura de Palmeira das Missões – RS é apresentada na seção 4. Encerrando o artigo, apresentam-se as considerações finais, destacando os resultados obtidos, bem como as referências empregadas.

2. Referencial Teórico

Esta seção apresenta um breve referencial teórico sobre as áreas envolvidas no desenvolvimento deste trabalho, abordando questões referentes a Redes de Computadores, Gerenciamento de Redes e Segurança da Informação.

2.1 Redes de Computadores

A expressão “Redes de Computadores” serve para mencionar um conjunto de computadores interconectados por uma única tecnologia. Dois computadores ou mais estão interconectados podendo trocar informações por uma conexão que pode ser feita por fio de cobre, fibras ópticas, micro-ondas, ondas de infravermelho e satélite de comunicações. Existem redes de muitos tamanhos, modelos e formas. Elas normalmente estão conectadas para criar redes maiores, com a Internet sendo o exemplo mais conhecido de uma rede de redes [TANEMBAUM e WETHERALL 2011].

Redes de computadores são estruturas físicas (equipamentos) e lógicas (programas, protocolos). Quando um computador está conectado a uma rede de computadores, ele pode ter acesso às informações que chegam a ele e, também, às informações presentes nos outros computadores conectados à mesma rede, o que permite um número muito

maior de informações possíveis para acesso por meio daquele computador [TANEMBAUM e WETHERALL 2011].

2.2 Segurança da Informação

Informação é um ativo que, como qualquer outro ativo importante, tem um valor para a organização e, consequentemente, necessita ser adequadamente protegido. A informação é utilizada tanto para administrar internamente a organização como para prever situações. Por esse motivo, ela é um bem poderoso para a organização. Neste contexto, é preciso proteger adequadamente as informações, de acordo com o conceito de Segurança da informação, que é a proteção da informação contra vários tipos de ameaças [ABNT 2005 citado por CARVALHO 2011].

A Segurança da Informação visa garantir a integridade, confidencialidade e disponibilidade das informações processadas pela organização [CAMPOS 2007 citado por CARVALHO 2011].

2.2.1 Política de Segurança

Uma política de segurança é um instrumento importante para proteger uma organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida, neste contexto, como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade). A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação [CERT.br 2015].

Definir uma política de segurança é uma tarefa complicada, já que cada organização deve decidir que aspectos de proteção são mais importantes e, frequentemente, assumir um balanço entre segurança e a facilidade de uso. Por exemplo, uma organização pode considerar [COMER 2007]:

- *Integridade de dados:* a integridade se refere à proteção contra mudança: os dados que chegam em um receptor são exatamente os mesmos que foram enviados?
- *Disponibilidade de dados:* a disponibilidade se refere à proteção contra a interrupção do serviço: os dados permanecem acessíveis para uso legítimo?
- *Confiabilidade dos dados:* confiabilidade se refere à proteção contra acesso não autorizado a dados: os dados estão protegidos contra acesso sem autorização?
- *Privacidade:* a privacidade se refere à habilidade de um remetente se manter anônimo: a identidade do remetente é revelada?

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

A sociedade precisa de mais profissionais de computação treinados em segurança, que possam defender e evitar, com sucesso, ataques contra computadores, bem como usuários treinados em segurança, que possam gerenciar de forma segura sua própria informação e os sistemas que usam. Tradicionalmente, a segurança de informação tem sido definida nos termos do acrônimo C.I.D. (do inglês C.I.A., *confidentiality, integrity, availability*), que significa confidencialidade, integridade e disponibilidade [GOODRICH e TAMASSIA 2013]. A figura 1 apresenta a relação entre os conceitos de confidencialidade, integridade e disponibilidade.

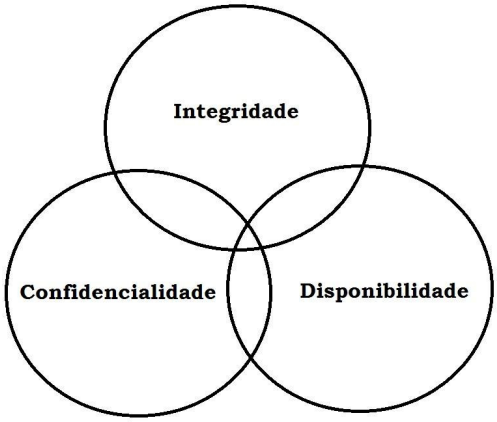


Figura 1: Os conceitos C.I.D: [adaptado de Goodrich e Tamassia 2013]

2.3 Modelo de Gerenciamento de Redes FCAPS

Na área de Redes de Computadores existem certos procedimentos que são exigidos para analisar o desempenho de uma rede e sua integridade. Estes procedimentos envolvem a Gerência de Redes, que é o controle de qualquer objeto passível de ser monitorado dentro em uma estrutura de recursos lógicos e físicos no que diz respeito à eficácia e ao desempenho. Por meio do modelo FCAPS (*Fail Configuration Accounting Performance Security*) de gerência, cada tipo de gerência têm, por finalidade, manter o funcionamento, segurança e eficiência de uma rede de computadores. Para tanto, deve-se definir um conjunto de ferramentas, procedimentos e políticas, independentemente do tamanho ou finalidade da rede de computadores. A Gerência de Redes deve monitorar e manter o bom funcionamento de uma rede em um nível acima do aceitável de utilização, para isso são colhidas certas informações como: configuração, falhas, desempenho, segurança e contabilizações na própria rede que podem ser usadas em conjunto com um mapa desta rede, para indicar quais elementos estão funcionando, quais estão em mau funcionamento, e quais não estão funcionando [KUROSE e ROSS 2005].

O modelo ***FCAPS*** de rede é constituído basicamente por 5 gerências que garantem o bom funcionamento de uma rede [KUROSE e ROSS 2005]:

- *Fail* (Gerência de Falhas);
- *Configuration* (Gerência de Configuração);
- *Accounting* (Gerência de Contabilização);
- *Performance* (Gerência de Desempenho);
- *Security* (Gerência de Segurança).

O FCAPS inclui o fornecimento, integração e coordenação de hardwares, softwares, além do profissional humano para monitorar, testar, configurar, consultar, analisar, avaliar e controlar uma rede. Seus recursos necessitam atender a requisitos de desempenho, qualidade de serviço (QoS), segurança e operação em tempo real dentro de um custo compreensivelmente justo para empresa ou corporação [KUROSE e ROSS 2005].

2.4 Ferramentas para o Gerenciamento de Redes de Computadores

A maioria das ferramentas de gerência de redes de computadores utiliza a combinação de cinco elementos distintos para a medição de desempenho de uma rede [ABREU e PIRES 2004]:

- Disponibilidade: determinar se a rede está realmente funcionando. Se o tráfego não pode percorrer a rede, trata-se de um problema muito maior do que apenas um problema de performance. Obtendo-se sucesso no teste de conectividade, opções mais avançadas podem ser usadas para testes, que se aproximem das necessidades da aplicação, que a rede deve suportar;
- Tempo de resposta: o tempo de resposta é determinado como o tempo que se necessita para que um pacote viaje entre dois *hosts*[1] através da rede (o tempo de resposta de ambos os *hosts* interfere diretamente neste tempo);
- Utilização da rede: o principal fator que influencia na performance de uma rede é a utilização de cada segmento de rede situados no caminho entre dois *hosts*. A utilização da rede é um valor percentual referente à informação transmitida e recebida em determinado período de tempo;
- Vazão (*Throughput*) da rede: o *throughput* de rede consiste em determinar a quantidade de banda[2] disponível para determinada aplicação em um dado momento. É diretamente influenciado por gargalos provocados por segmentos da rede de menor banda ou de maior tráfego;
- Capacidade de transmissão da rede: A capacidade de transmissão de uma rede é outro fator diretamente relacionado ao *throughput* da mesma; para determinar essa variável são utilizadas duas técnicas *packet pair* e *packet trains*. Primeiramente é enviado um par de pacotes para um *host* remoto com um intervalo de tempo de separação conhecido (*packet pair*). Assim que este par de pacotes percorre a rede e chega ao seu destino, o intervalo entre ambos pode variar de acordo com o tráfego na rede (*packet train*). A diferença entre o intervalo de tempo entre os dois pacotes determina a carga na rede; uma rajada de pacotes pode ser enviada até o *host* destino de forma que podemos determinar a taxa ou velocidade a qual a rede é capaz de transportar determinado fluxo de pacotes.

---

[1] *Host* - Ou "hospedeiro" qualquer máquina ou computador conectado a uma rede, podendo oferecer informações, recursos, serviços e aplicações aos usuários [TANEMBAUM e WETHERALL 2011].

[2] Banda (Largura de banda) - É o volume de dados por segundo que pode ser transmitido entre emissor/receptor [TANEMBAUM e WETHERALL 2011].

2.5 Softwares de Teste de Redes

Um Programa de Segurança de redes corporativas de computadores, estruturado de forma adequada, deve prever o combate a ameaças que possam afetar os Sistemas de Informação da organização, tais como ameaças do ambiente: erros humanos, fraudes, indisponibilidade, falhas em sistemas ou nos diversos ambientes computacionais. Para cumprir esses objetivos, um Programa de Segurança da Informação deve seguir quatro princípios: Integridade, Confiabilidade, Disponibilidade e Legalidade (estado legal da informação, ou seja, em conformidade com os preceitos da legislação em vigor) [PINHEIRO 2005].

Com isso é necessário que se avalie, detalhadamente, a amplitude daquilo que se pretende proteger, seguindo as normas da política de segurança que são basicamente as normas e procedimentos definidos dentro de uma organização. Ao delimitar estes processos, deve-se partir para a fase de gerenciamento, passando pela análise de infraestrutura da empresa, auditoria de processos, testes regulares de ataques a vulnerabilidades, revisões e acompanhamento de políticas e tratamento de incidentes [PINHEIRO 2005].

Algumas das aplicações, ferramentas e técnicas que já fazem parte da rotina das organizações para apoiar a gerência de redes e propiciar a segurança da informação envolvem os Antivírus, Balanceamento de Carga, *Firewall*, Autenticações, Detector de Intrusos - IDS (*Intrusion Detection System*), Varredura de Vulnerabilidade, Rede Privada Virtual - VPN (*Virtual Private Network*), Criptografia, Autenticação e Integradores, entre outras [PINHEIRO 2005].

2.6 VLANs (*Virtual Local Area Network*)

Uma VLAN é um agrupamento lógico de estações, serviços e dispositivos de rede que não estão restritos a um segmento físico de uma rede local. A função das VLANs é prover a segmentação lógica na rede, normalmente oferecida por roteadores em uma configuração LAN *(Local Area Network)*, permitindo a implementação de serviços como: filtragem de *broadcast*, sumarização de endereços, segurança e controle de tráfego [SANTOS 2010].

As VLANs São utilizadas para resolver problemas de escalabilidade, segurança e gerência de rede. Toda a configuração das VLANs de uma rede pode ser feita remotamente pelo administrador, tornando desnecessário o acesso ou deslocamento até os armários de fiação. Isto, de forma geral, facilita muito a tarefa do administrador da rede ao custo de um maior planejamento e mais tempo investido na configuração da mesma. Uma rede com VLANs mal configuradas pode também causar diversos problemas administrativos, como inoperabilidade da mesma [SANTOS 2010].

2.7 Zona Desmilitarizada – DMZ

Uma DMZ (*Demilitarized Zone*) ou ainda "Zona Neutra", corresponde ao segmento (ou segmentos de rede) parcialmente protegido, que se localiza entre redes protegidas e redes desprotegidas, e que contém todos os serviços e informações para clientes ou públicos. A DMZ pode também incluir regras de acesso específico e sistemas de defesa

de perímetro para que simule uma rede protegida, induzindo os possíveis invasores para armadilhas virtuais de modo a se tentar localizar a origem do ataque [PINHEIRO 2004].

Existem dois tipos de DMZs: a interna, só acessada pelo usuário da rede interna e a DMZ externa, acessada por qualquer usuário da *Internet*. Este conceito, aliado ao de VLANs também permite a implantação de DMZs privadas, ou seja, a possibilidade de existirem DMZs específicas para cada cliente de *hosting* ou para a hospedagem de servidores [PINHEIRO 2004].

As DMZs são sub-redes que hospedam os servidores/serviços de um provedor[3] protegidos contra ataques da *Internet* por um *firewall*[4]. Em geral é necessário especificar uma faixa de endereços IP (*Internet Protocol*), ou informar diretamente os endereços das máquinas que devem ser incluídas nessa zona [PINHEIRO 2004]. A figura 2 apresenta um esquema gráfico de uma rede de computadores utilizando *Firewall* e DMZ.

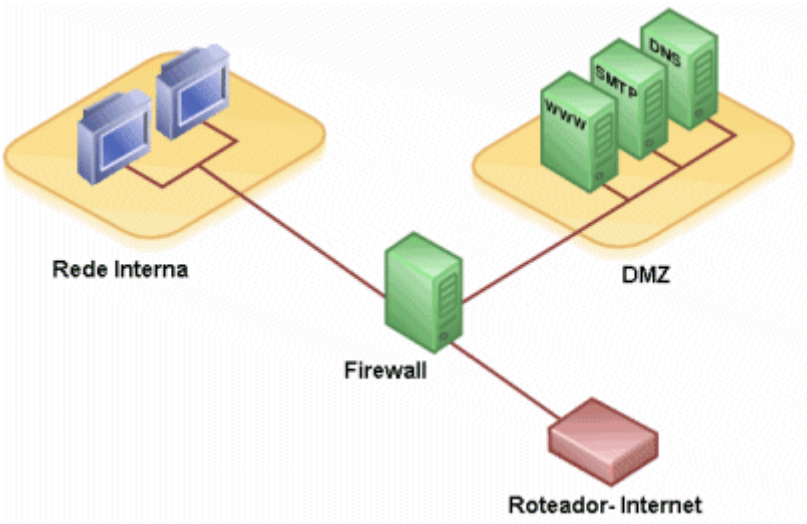


Figura 2: Rede com *Firewall* e DMZ [Pinheiro, 2004].

2.8 *Host* Seguro

Um *host* de segurança ou *host* seguro caracteriza-se geralmente por um ou mais servidores protegidos que residem em uma *DMZ*. Este servidor (ou servidores) tem a função de alocar serviços essenciais, tais como: servidor FTP (*File Transfer Protocol*), *web*, DNS (*Domain Name System*) e SMTP (*Simple Mail Transfer Protocol*). Neste sentido, este servidor precisa ser muito resguardado, pois é vulnerável podendo receber acessos da *internet* e também de usuários internos.

---

[3] Provedor - O provedor é um serviço que tem a função de conectar um computador ou mais à Internet, permitindo a navegação em sites e acesso a serviços como envio e recebimento de e-mail [TANEMBAUM e WETHERALL 2011].

[4] *Firewall* - é uma passagem que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a Internet, pode também estabelecer passagens seguras entre redes internas [TANEMBAUM e WETHERALL 2011].

Sendo assim, tendo-se em vista a importância dos serviços alocados nesses servidores, um *host* de segurança deve ser protegido por recursos de *firewall,* já que estão sujeitos a serem comprometidos em um ataque [CHAPMAN e ZWICKY 1995] [GARFINKEL e SPAFFORD 1996].

3. Estado da Arte

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

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

O trabalho apresentado por Wagner (2012), partiu da necessidade de aumentar a segurança, privacidade e melhorar desempenho da rede de computadores do CITEC (Centro de Inovação Tecnológica) da UTFPR (Universidade Tecnológica Federal do Paraná), tendo como proposta utilizar a segmentação através da criação de VLANs, aumentando a segurança e privacidade das informações contidas em cada sub-rede criada. Além disso, a proposta contou com a utilização de uma DMZ para utilização de equipamentos e serviços comuns a várias sub-redes e até mesmo acesso externos as dependências do departamento.

A segmentação da rede visou trazer maior segurança e privacidade das informações para cada laboratório, por meio da criação de VLANs que fazem todo o trabalho de roteamento e interconexão. Foram aplicadas regras de filtragem utilizando *software* livre e não utilizando *hardware* ou *software* proprietário. Sendo compartilhadas as informações e os recursos somente com quem há de direito, essa segmentação também diminuiu o domínio de *broadcast,*[5] minimizando interferências estranhas ao ambiente.

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 o acesso do *host* específico, ou seja, o *firewall* trabalha com lista branca ("*whitelist"*) ou lista segura, bloqueando todo e qualquer tráfego não autorizado.

Aplicando uma DMZ para acesso comum a todas as sub-redes, permitiu-se a instalação de serviços, servidores, impressoras, etc. que podem ser acessadas de todas as sub-redes e também acessadas externamente, tudo controlado através do *firewall*. Toda a arquitetura utilizada foi implementada por meio de *software* livre, tanto o Sistema Operacional dos equipamentos utilizados, quanto os serviços instalados possibilitando, assim, futuras implementações de novos serviços, podendo ser customizada de forma a atender diversas funcionalidades específicas que possam surgir.

O sistema operacional trata cada VLAN como sendo uma interface de rede, criando uma interface virtual para cada uma. Portanto, deve ser feita a definição do

---

[5] *Broadcast* – É um endereço de IP (e seu endereço é sempre o último possível na rede) que permite que a informação seja enviada para todas as máquinas da rede de computadores e sub-redes [TANEMBAUM e WETHERALL 2011].

endereçamento IP (*Internet Protocol*) para cada interface. Como o sistema reconhece as VLANs como interfaces de rede, dever ser informado ao serviço de DHCP[6] (*Dynamic Host Configuration Protocol*) cada VLAN criada como se fosse uma interface de rede diferente. Sendo assim, faz-se necessário informar ao serviço para quais interfaces ele deve distribuir o endereçamento.

Wagner (2012) concluiu que a segmentação da rede com a utilização de VLANs tornou a rede mais estável, segura e escalonável, diminuindo o custo total da infraestrutura, possibilitando a fácil criação de novos grupos de trabalhos isolados. Além disso, destaca que a DMZ viabiliza o compartilhamento de serviços e equipamentos comuns a vários grupos de trabalhos independentemente a qual sub-rede o usuário pertence. Outra vantagem apresentada foi o uso de um equipamento que utiliza *software* livre, proporcionando liberdade para poder fazer futuras instalações de outras ferramentas para auxiliar a rede de forma rápida e com um custo reduzido.

3.2 Reestruturação de Rede para melhoria do Tráfego e Segurança: a Reestruturação da Rede de Computadores do DC

O trabalho apresentando por Teixeira e Moreira (2014) destaca o uso da rede de computadores do Departamento de Computação (DC) da Universidade Federal de São Carlos (UFSCar) que mudou consideravelmente, desde a implantação da rede estruturada. Os grupos de pesquisa da pós-graduação criaram seus próprios servidores, aumentou a quantidade de salas de docentes e de laboratórios de ensino e a necessidade de aumentar a conectividade e o controle do uso da rede sem fio é latente.

A rede de computadores do DC é uma rede 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: 1) rede de docentes e funcionários, 2) rede da pós graduação, 3) rede de equipamentos destinados aos alunos de graduação e 4) rede sem fio.

Antes da aplicação do trabalho proposto, cada uma das quatro redes tinha seu próprio segmento, mas observou-se que a divisão do fluxo não favorecia questões de confinamento de tráfego e tinha exposições de segurança indesejáveis. Deste modo, várias questões de desempenho e segurança não eram ideais. Não havia mecanismos de controle de banda e o controle de segurança era dificultado nesse ambiente, que misturava redes logicamente destinadas à produção e à pesquisa. De maneira geral, a organização da rede impossibilitava o controle e o monitoramento desejáveis de sua operação, a segurança no acesso aos servidores não era apropriada e o uso indevido da largura de banda da rede ocorria com certa frequência.

Como solução aos problemas apresentados, foi proposta uma reestruturação para a rede de computadores do DC, de modo a facilitar o seu gerenciamento, oferecer qualidade de serviço adequada e melhorar a segurança dos equipamentos conectados, por meio da avaliação e reestruturação física e lógica da rede.

---

[6] DHCP - É um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente [MORIMOTO 2011].

A solução ao problema dos servidores junto com estações de trabalho foi separá-los criando uma DMZ. Além da DMZ para os servidores com visibilidade externa, também foi necessária outra DMZ para servidores com visibilidade interna, para melhorar a segurança de acesso aos dados críticos, necessário para autenticação de usuários, por exemplo. Para melhorar a segurança e o controle de acesso aos servidores com visibilidade externa, um segmento físico e lógico foi separado para a implantação de uma DMZ. Todo servidor com visibilidade externa foi alocado nesse segmento, pois nele, o controle de acesso, tanto a partir da rede externa quanto a partir da rede interna, ficou mais claro, rígido e gerenciável. Essa reorganização também proporcionou o confinamento de tráfego originado externamente.

Alguns servidores críticos podem ser acessados pelos servidores na DMZ, por exemplo, um site autenticando no servidor de LDAP[7] (*Lightweight Directory Access Protocol*) ou acessando um banco de dados. Outros servidores internos podem ser acessados pelos segmentos de rede de estações de trabalho como, por exemplo, a montagem de área pessoal via NFS[8] (*Network File System*) ou a autenticação dos laboratórios de ensino via *Samba* que é um "software servidor", utilizado em sistemas operacionais do tipo *Unix*, que simula um servidor *Windows*, permitindo que sejam realizados o gerenciamento e o compartilhamento de arquivos em uma rede *Microsoft*. Para possibilitar o acesso dos segmentos de rede aos servidores internos, é preciso conectar o *firewall*. Toda a avaliação e reestruturação da rede do DC seguiu o roteiro apresentado no Quadro 1.

Quadro 1: Roteiro da abordagem do problema de reestruturação

Fonte: (Teixeira e Moreira, 2014)

	Passos	**Observar**
1	Levantamento e documentação da estrutura física	Equipamentos utilizados (capacidade livre, tecnologia disponível), segmentação física
3	Levantamento das demandas ao uso da rede	Segmentos e equipamentos envolvidos
4	Estudo do padrão de uso da rede	Utilização de serviços e tráfego entre segmentos e WAN[9] (*Wide Area Network*)
5	Projetar a reestruturação física e lógica	O projeto deve atender as demandas levantadas anteriormente, antevendo a utilização da rede que deverá ocorrer nos próximos anos
6	Planejar os casos de teste	Devem verificar a rede antes e depois da implantação do projeto

[7] LDAP - é um protocolo de aplicação aberto, livre de fornecedor e padrão da indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede de Protocolo da Internet (IP) [CERT.br 2015].

[8] NFS - é um sistema de arquivos distribuídos desenvolvido inicialmente pela *Sun Microsystems Inc.*, a fim de compartilhar arquivos e diretórios entre computadores conectados em rede, formando assim um diretório virtual [CERT.br 2015].

[9] WAN - é uma rede de computadores que abrange uma grande área geográfica, com frequência um país ou continente [TANEMBAUM e WETHERALL 2011].

Teixeira e Moreira (2014) concluíram, ao avaliar os resultados obtidos, que por meio da reestruturação lógica será possível a adição de novos nós no segmento atualmente saturado. Também foi identificado que uma parte considerável do tráfego de dados é feito via UDP[10] (*User Datagram Protocol*), mas que os serviços mais usados são os serviços que usam o protocolo TCP. Além disso, foi proposta uma reestruturação física que possibilitará gerenciar melhor os acessos internos e externos aos serviços de TI oferecidos pelo departamento e pelos grupos de pesquisa. O controle de uso da capacidade de transmissão será possível com a implantação da segmentação que separa estações de trabalho de servidores.

3.3 Implementação e Análise de uma Estrutura de Rede, Contemplando Gerenciamento, Qualidade de Serviços e Segurança

Schultz (2013) apresenta um trabalho que teve, por objetivo, a implementação e análise de uma estrutura de redes de computadores visando à segurança, qualidade de serviços e gerenciamento, juntamente com a implantação de diretivas de qualidade de serviços para priorizar diferentes tipos de tráfegos, como dados e voz.

Na visão de Schultz (2013), gerenciamento, qualidade de serviços e segurança são temas essenciais na implementação de redes de computadores. Neste sentido, é necessário fazer um levantamento dos pontos que possam prejudicar o uso da rede, a partir de uma metodologia que permita a utilização de forma segura e correta. Tendo-se em vista que partes das redes locais são implementadas sem um planejamento adequado, juntamente com o aumento da demanda, maiores taxas de transmissões para o tráfego de redes e o número crescente de ataques, torna-se necessária a configuração e manutenção de ferramentas que possam deixá-las mais seguras, confiáveis e não suscetíveis a falhas.

Nas implementações atuais, muitos administradores de redes não fazem uma verificação e correção das vulnerabilidades, nem o gerenciamento adequado, fazendo com que a rede tenha pontos de falha. Uma rede com pontos de falha pode acarretar em uma baixa qualidade de serviços, a falta de segurança das informações compartilhadas e possibilidade de que dispositivos indesejáveis tenham acesso à rede.

Para a resolução dos problemas apontados, Schultz (2013) fez um estudo teórico sobre um conceito geral de redes de computadores com um aprofundamento em questões de gerenciamento, qualidade de serviços e segurança das mesmas. Posteriormente foi realizado um levantamento e estudo de equipamentos e *softwares* que podem ser utilizados na implantação da rede.

Após esse levantamento, uma topologia de rede foi modelada, contemplando os aspectos de gerenciamento, qualidade de serviços e segurança estudados. Com a topologia definida foram realizadas as implementações física e lógica da rede, a análise do tráfego, a implementação da segurança e do gerenciamento, e com isso pôde-se verificar se a topologia da rede proposta contemplava os requisitos de segurança, QoS e gerenciamento. A rede como um todo foi dividida em sub-redes lógicas, as VLANs, para diminuir os problemas de tempestades de *broadcast*.

---

[10] UDP - é um protocolo simples da camada de transporte. Ele é descrito na RFC 768 e permite que a aplicação escreva um datagrama encapsulado em um pacote IPv4 ou IPv6, e então enviado ao destino [TANEMBAUM e WETHERALL 2011].

Os resultados apresentados por Schultz (2013) permitem verificar a importância de três pilares na infraestrutura de redes: qualidade de serviço (QoS), segurança e gerenciamento, validados por meio da implementação e análise de uma infraestrutura de redes que contemplasse segurança, qualidade de serviços e gerenciamento.

3.4 Segurança da Informação: Uma Proposta para Projeto de Rede Baseada em Software Livre

Dallabona (2013) faz uma abordagem sobre os dias atuais, onde praticamente todas as organizações fazem uso de Tecnologias da Informação e da Comunicação, que são vitais para os negócios. Ao aplicar estas tecnologias surge uma necessidade básica, a segurança, destacando que a seguranca da informação não deve depender única e exclusivamente de equipamentos de seguranca de rede de alto custo, mas também, de políticas de seguranca, treinamento, educação profissional e conscientização em todos os níveis hierárquicos dentro da organização.

Cada organização, dentro do seu ramo de atividade ou rede de computadores possui características únicas que devem ser analisadas individualmente antes da escolha da tecnologia eficaz na proteção de seus dados e informações. Sugere-se então, a utilização de ferramentas baseadas em *software* livre que, respeitando-se as características de cada organização, podem trazer uma camada de seguranca com um baixo custo para a entidade. O *software* livre atende com eficiência as necessidades de seguranca utilizando-se de ferramentas que executam tarefas similares a de equipamentos, por vezes caros, aos quais muitas empresas e instituições não teriam condições financeiras de adquiri-los [DALLABONA 2013].

O local escolhido para o desenvolvimento do projeto foi uma unidade do Governo Federal, com estrutura física dividida em 7 (sete) prédios já ocupados e em funcionamento, contendo diversas seções que estão distribuídas dentro desse espaço. Esta organização, desde o ano de 2010, com a elaboração do Plano de Padronização do Ambiente e Migração para *Software* Livre, vem trabalhando para se alinhar às determinações contidas no plano, tanto no que tange a ferramentas e aplicativos utilizados, bem como à elaboração de políticas e regras de seguranca, tomando-se como princípio básico a adoção de *software* livre em todo o parque de máquinas.

Como objetivo, Dallabona (2013) visou implementar o projeto lógico da rede de dados de uma organização, apresentando uma proposta para uso de ferramentas baseadas em *software* livre nos serviços a serem disponibilizados aos usuários, estabelecendo regras visando à segurança da informação, sem a necessidade de adquirir equipamentos e *softwares* proprietários de alto custo. Para tanto, foram seguidos os passos destacados abaixo:

- Levantar, junto aos usuários da rede, a relação dos serviços, *sites* e outras informações necessárias sobre a rotina de trabalho, para definir o enlace de Internet e o planejamento das regras de acesso à Internet e servidores;
- Buscar, junto às empresas fornecedoras de enlaces de acesso à Internet existentes na cidade sede da organização em questão, a opção mais adequada às necessidades do grupo;

- Realizar reuniões com a gerência da organização, para definição das restrições de acesso às informações, as quais foram detalhadas em uma cartilha de segurança da informação elaborada;
- Documentar o detalhamento do projeto lógico, os quais foram armazenados no departamento responsável pela segurança da organização.

Dallabona (2013) apresenta algumas opções de segurança do software *pfSense. O pfSense* é um *software* livre adaptado para assumir o papel de um *firewall* e/ou roteador de redes, incluindo possibilidades de configurações para o uso de VLANs e DMZ. Dallabona (2013) destaca que, normalmente as pessoas são o elo mais frágil quando o assunto é segurança da informação, ou seja, as soluções técnicas não contemplam totalmente sua segurança. Desta forma torna-se necessário que os conceitos pertinentes à segurança sejam compreendidos e seguidos por todos dentro da organização, sem distinção de níveis hierárquicos.

3.5 Estudo Comparativo

A partir dos trabalhos correlacionados estudados, elaborou-se um quadro destacando as principais características dos mesmos, comparando-os à solução apresentada neste artigo. Estas características são apresentadas no Quadro 2.

Quadro 2 Comparações entre ferramentas utilizadas e resultados obtidos

Trabalhos	Softwares e Ferramentas Utilizados	Resultados alcançados em relação aos objetivos
Trabalho 1 [WAGNER 2012]	IpTables com Netfilter	- Rede mais estável e segura e escalonável - Possibilitando a fácil criação de novos grupos de trabalhos - DMZ viabiliza o compartilhamento de serviços e equipamentos comuns a vários grupos de trabalhos - Melhor performance tanto na gerência como na segurança
Trabalho 2 [TEIXEIRA e MOREIRA 2014]	IpTraf, JPerf, IPerf, Nmap	- Manter o fluxo de dados onde é realmente necessário através da reestruturação lógica - Adição de novos nós no segmento atualmente saturado assim melhorando a escalabilidade - Através da DMZ foi possível melhorar a segurança e a performance da rede
Trabalho 3		- Melhor gerenciamento, segurança e qualidade de serviço - Se a rede somente tiver o suporte à segurança poderá ter problemas com QoS

[SCHULTZ 2013]	Iperf, Wireshark, GNS3, Nmap, Cacti.	- Caso haja uma sobrecarga nos equipamentos de redes e se o administrador de redes não tiver o auxílio de um *software* de gerenciamento, ele só irá descobrir a falha quando o *hardware* parar de funcionar
Trabalho 4 [DALLABONA 2013]	NTop, Pfsync, Ipchains, Iptables, pfSense, Snort, Truecrypt	- Com a ferramenta pfSense foi possível gerenciar toda sua rede - Identificação dos pontos de riscos a que a informação está exposta identificando quais os pontos que necessitam de maior empenho em proteção - Identificar quais os riscos que as informações estão expostas deve-se iniciar um processo de segurança física e lógica, com o intuito de alcançar um nível aceitável de segurança
Solução Implementada neste trabalho	Zabbix, Packet Tracer, Sarg	- Maior gerência e segurança da rede com as Vlans e DMZ - Com Zabbix possível ter respostas muito mais rápidas e tomar decisões mais acertadas - Com um controle maior da rede é possível fazer uma maior previsão em quesitos como gerência e escalabilidade

O Quadro 3 apresenta um comparativo envolvendo os problemas encontrados nas redes de computadores estudadas e que foram destacados nos trabalhos.

Quadro 3 Comparações entre os problemas dos trabalhos

Trabalhos	Problemas dos Trabalhos Comparados
Trabalho 1 [WAGNER 2012]	Segmentação da Rede, Segurança e Privacidade das Informações, *Broadcast*, Escalabilidade e Instabilidade da Rede.
Trabalho 2 [TEIXEIRA e MOREIRA 2014]	Segurança, Gerenciamento, Qualidade de Serviço (QoS), Escalabilidade.
Trabalho 3 [SCHULTZ 2013]	Segurança, Gerenciamento, Qualidade de Serviço (QoS), *Broadcast*.
Trabalho 4 [DALLABONA 2013]	Segurança da Rede, Segurança da Informação, Gerenciamento.

Solução Proposta	Segurança da Rede, Segurança da Informação, Gerenciamento, Escalabilidade, *Broadcast.*

Analisando-se os trabalhos estudados, verifica-se que existem problemas reais em comum (como mostram as informações do quadro 3), que necessitaram de melhorias em suas redes de computadores. Os problemas destacados envolviam dificuldades de gerenciamento, desempenho e segurança, principalmente.

No quadro 2 pode-se visualizar os diferentes tipos de softwares e ferramentas que foram utilizados para solucionar os mais diversos problemas e os resultados e conclusões obtidos através de seus respectivos trabalhos sendo possível atingir suas metas.

Um ponto forte em comum, que pôde ser constatado, envolveu o uso de VLANs, DMZ e *software* livre. Em todos os trabalhos estudados verificou-se que foi possível resolver os problemas, ou pela menos boa parte deles, com a utilização destes recursos.

Outro fato interessante foi que as soluções propostas puderam ser aplicadas de forma prática em ambientes reais (organizações), permitindo que seus resultados pudessem ser comprovados. Assim pode-se constatar que apesar de serem organizações diferentes os problemas com redes de computadores geralmente se têm boa parte deles em comum principalmente quando se trata de segurança e gerenciamento de redes de computadores.

4. Solução Implementada

Este trabalho teve sua proposta alicerçada na base estrutural do parque computacional e Departamento de Informática para aprimoramento da segurança da rede de computadores e desempenho da transmissão de dados da Prefeitura Municipal de Palmeira das Missões - RS, promovendo, assim, um ambiente seguro.

Buscou-se a definição de um modelo de estrutura física e lógica da rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS, por meio da identificação de ambientes convergentes à utilização das tecnologias necessárias para garantir o máximo de segurança para todos os processos que tramitam na mesma, promovendo, assim, um ambiente seguro com a definição da DMZ e de VLANs, atendendo à Política de Segurança vigente. Pretendeu-se aplicar conceitos de Segurança da Informação e de Projetos de Infraestrutura para auxiliar neste processo.

Para ocorrer este processo de implantação de um ambiente seguro nesta rede de computadores, fez-se necessário o estudo de ferramentas, *softwares*, conceitos de Segurança da Informação, Sistemas Operacionais e Gerenciamento de Redes de Computadores para, então, poder aplicar a política de segurança à rede, de modo que atendesse às necessidades dos usuários de forma satisfatória. Pretendeu-se detectar os pontos mais "frágeis" da rede para elaborar uma solução condizente, a partir de um diagnóstico da situação existente antes da implementação deste trabalho. Com base nestas informações foram escolhidas as ferramentas e *softwares* a serem utilizados e as medidas a serem adotadas.

4.1 Diagnóstico da Rede de Computadores

No início da implementação deste trabalho (primeiro semestre de 2015), a Prefeitura Municipal de Palmeira das Missões – RS possuía, em sua estrutura de rede, três servidores físicos, sendo eles: 1) *HP – ProLiant ML150 xeon*, que estava desativado e onde foi configurada a DMZ, 2) um *HP – ProLiant ML150G6* com *Windows Server 2008 R2*, que é usado para o sistema de gestão pública da empresa Digifred[11] com banco de dados *Firebird* e 3) um *Dell PowerEdge R620 Xen Server* no qual estão virtualizados 5 servidores, sendo eles:

- *Ubuntu Server*: *Proxy* Transparente - Transparente pelo endereço lógico (endereço IP). Servidor de *Cache* de *Internet* transparente ao usuário, onde não há necessidade de configuração alguma na estação de trabalho; porém, o controle é feito por IP fixos nas máquinas; fornecendo permissão diferenciada para cada máquina de forma isolada conforme necessidade. Também existe a configuração de limite de banda utilizada;
- *Ubuntu Server*: *Proxy* Autenticado - Sistema de controle de acesso por autenticação de usuário, onde cada usuário tem um login e senha que podem ser configurados com permissões diferentes para acessos restritos ou liberados. Também existe a configuração de limite de banda utilizada;
- *CentOS Server* – Banco de dados *Sybase* da empresa Delta. Unicamente para execução de processos do banco de dados com chamadas remotas e acessos administrativos para configuração;
- *Ubuntu Server* Samba - Compartilhamento de repositório de dados, para armazenamento de informações de departamentos específicos controlados por acessos com autenticação e também por acessos públicos para diretórios comuns entre departamentos;
- *Windows Server* 2008 R2 – Sistemas de Gestão Pública da empresa Delta.[12] Como os aplicativos da Delta funcionam na plataforma *Windows,* este servidor executa todos os processos de departamentos que têm máquinas com *Linux* ou departamentos externos à *LAN* (*local Area Network*) da Prefeitura pela *internet* com conexão remota via *Windows,* mantendo, assim, o processamento do sistema neste servidor e com conexão direta com o banco de dados.

Nota-se a predominância do uso do sistema operacional *Ubuntu* que é um *software* livre desenvolvido pela comunidade, adequado para utilização em diferentes equipamentos, tais como *laptops*, *desktops* e servidores. O Ubuntu é desenvolvido visando segurança e, a cada 6 meses, é lançada uma nova versão. O *download* do

---

[11] A prefeitura usava os sistemas da empresa Digifred. Atualmente estão sendo implantados os novos sistemas da empresa *Delta*. Durante o período de transição entre os sistemas, será necessário realizar consultas ao banco de dados dos sistemas da Digifred.

[12] A *Delta Easy Solutions* atualmente é a empresa que supre a demanda de todos os sistemas para gestão pública usados na Prefeitura.

Ubuntu pode ser feito por meio do link: http://ubuntu-br.org/ubuntu [UBUNTU-BR.ORG, 2015].

A estrutura física da rede possuía mais cinco pontos de acesso externo, sendo um na Secretaria de Saúde, um no Hemocentro e mais três em postos de saúde. Todos esses pontos externos estão ligados ao nó principal via *bridge*[13]. Os serviços de rede executados nos servidores envolviam um *firewall* e um *proxy*[14], configurados no servidor de Internet *Ubuntu Server - Samba*. O objetivo da utilização dessas ferramentas era o de garantir a segurança e integridade das informações e dos equipamentos da Prefeitura. O *firewall* foi configurado com a definição de bloqueio total e liberação das regras utilizadas pela prefeitura como serviços.

O *proxy* estava configurado por IP, ou seja, apenas determinadas máquinas possuíam acesso restrito a *links* externos. Esta decisão foi tomada pelo Departamento de Informática verificando-se quais setores eram mais vulneráveis e necessitariam dessa proteção. Já o *firewall* estava configurado para atender a toda rede e evitar a propagação de vírus, por exemplo, por meio de *e-mails* infectados, além de evitar que existissem acessos externos às informações que trafegam pela rede.

4.2 Levantamentos de Demandas da Rede de Computadores

Esta seção relata o levantamento de demandas para a implantação de recursos de Segurança da Informação na rede de computadores em questão. Buscou-se identificar situações que tenham uma demanda da rede e que possam aumentar seu tráfego e fluxo, podendo causar lentidão e conflito. Foram levantados dados dos serviços que atuam na rede, enfatizando os sistemas da empresa *Delta Easy Solutions*, que atendem toda a demanda de *software* para gestão pública que a prefeitura necessita, e também um levantamento dos demais serviços que necessitam da rede, como *softwares* e sites do Governo Federal e Estadual, além de outras demandas de acesso.

No início do ano de 2015 a empresa *Delta* começou a implantação dos seus sistemas para atender toda a demanda de gestão pública na Prefeitura, fazendo a migração dos sistemas da empresa Digifred. Todos os sistemas implantados pela *Delta* fazem conexão com o banco de dados que está hospedado no servidor da Prefeitura, por meio da conexão com sua rede de computadores gerando, assim, um maior fluxo de dados. Os sistemas implantados são: Tributos, Folha Salarial, Contabilidade, Tesouraria, Frota, Patrimônio e Compras, que atendem à demanda de todos os setores.

Com base no levantamento das informações, realizado de forma empírica, por meio de reuniões com os membros do Departamento de Informática, sobre os diversos sistemas utilizados na Prefeitura, bem como o uso da rede pelos mesmos, foi possível constatar que o sistema tributos é um dos que tem uma demanda grande da rede, devido ao seu uso constante em diversos setores e número elevado de usuários. Além de todos

---

[13] *Bridge* - é o termo utilizado em informática para designar um dispositivo que liga duas ou mais redes, como, por exemplo, ligação de uma rede de um edifício com outro [TANEMBAUM e WETHERALL 2011].

[14] *Proxy* – é um sistema ou aplicação que age como um intermediário para requisições de clientes solicitando recursos de outros servidores, avalia a solicitação como um meio de simplificar e controlar sua complexidade [TANEMBAUM e WETHERALL 2011].

os usuários usando as funcionalidades "internas" do sistema, o mesmo possui uma aplicação externa chamada Cidadão *web*, disponibilizada no *site* da prefeitura municipal. Esta aplicação não possui limite de usuários (cidadãos contribuintes), que podem usar serviços tais como emitir boletos, guias e certidões gerando, assim, um maior fluxo na rede. Esta aplicação faz conexões com a nuvem[15] disponibilizada pela *Delta* onde são armazenados modelos de guias, alvarás, etc. Quando o contribuinte gera uma guia ou certidão, por exemplo, a mesma é gravada (por meio de um *download*) no banco de dados hospedado no servidor da prefeitura aumentando, dessa maneira, a demanda de conexão.

Outro ponto importe de se destacar é a aplicação chamada *Fly Transparência Online* (Portal da Transparência) que, por força de lei, deve disponibilizar uma série de informações aos cidadãos, tais como: empenhos, liquidações, ordens de pagamentos, salários dos servidores e que também está disponibilizada no site da Prefeitura. Este é outro exemplo de aplicação que pode ser acessada a qualquer hora e sem limites de usuários. Diariamente estas informações são atualizadas automaticamente, por meio de sistemas internos executados na prefeitura, também gerando fluxo de dados na rede. Além disso, ainda existem as conexões externas com órgãos da área de saúde. Esta conexão ocorre via *bridge*, sendo mais um fator a ser considerado na demanda da rede.

Outros fatores relevantes a serem considerados envolvem: 1) o setor de departamento pessoal que, geralmente do dia 15 à 30 de cada mês, faz a geração da folha de pagamento por meio do Sistema *Folha*; 2) o sistema da tesouraria que se integra com o sistema tributos, por meio do qual são feitos lançamentos com muita frequência, sendo necessário atualizar informações como pendências, pagamentos e 3) integrações entre os diversos sistemas dos setores da prefeitura, tais como a integração da tesouraria com o sistema de tributos, por exemplo.

Além das demandas citadas, foram constatadas demandas de acesso a *sites* específicos de uso em cada departamento, além de aplicações dos governos Estadual e Federal, os quais possuem diversas aplicações *online* com envio constante de informações via *web* gerando demandas para a rede. A figura 3 demonstra a situação física da rede de computadores da Prefeitura Municipal no 1º semestre de 2015.

[15] Nuvem - O conceito de computação em nuvem refere-se à utilização da memória e das capacidades de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, o armazenamento de dados é feito em serviços que poderão ser acessados de qualquer lugar do mundo [CERT.br 2015].

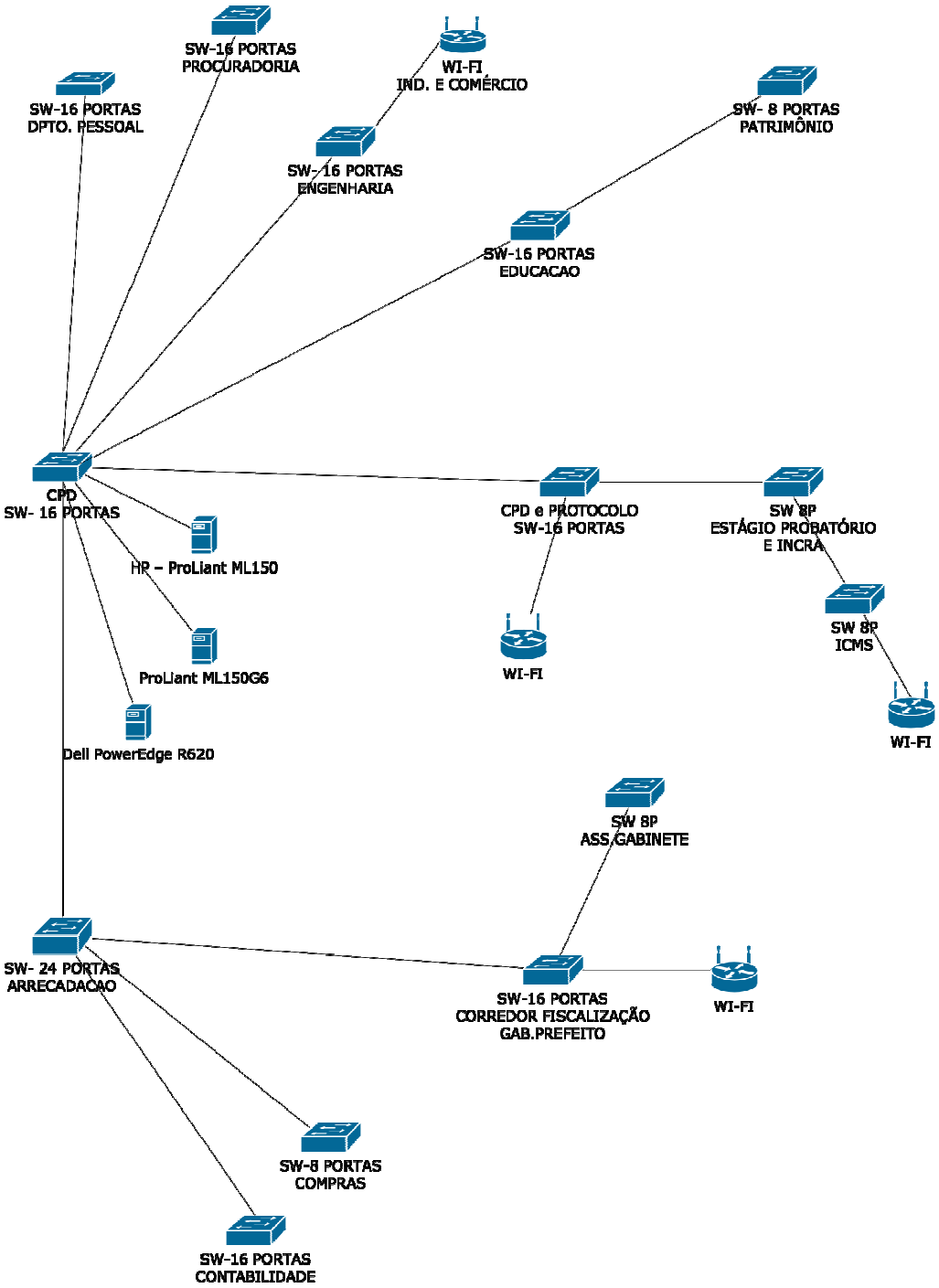


Figura 3: Situação da Rede de Computadores da Prefeitura Municipal de Palmeira das Missões no 1º Semestre de 2015 Fonte: Dos Autores, 2015

A Figura 3 demonstra a situação da rede de computadores da Prefeitura Municipal no primeiro semestre de 2015 antes da implantação do ambiente de segurança da rede de computadores.

4.3 Tecnologias e Ferramentas Empregadas

Após o levantamento dos requisitos físicos da rede de computadores da Prefeitura foi constatado que não seria necessária a aquisição de *hardware,* pois o *hardware* já existente suporta as mudanças e demandas que irão ocorrer na rede.

Em um primeiro momento realizou-se um estudo com os relatórios e recursos disponibilizados pelo *software Zabbix* que é um *software* livre, para efeitos comparativos posteriormente. O *Zabbix* trata-se de uma ferramenta de monitoramento de redes, servidores e serviços, pensada para monitorar a disponibilidade, experiência de usuário e qualidade de serviços. A arquitetura *Zabbix* e a flexibilidade dos módulos permitem que a ferramenta seja utilizada para o monitoramento convencional (*on/off*), acompanhamento de desempenho de aplicações, análise de experiência de usuário e análise de causa raiz em ambientes complexos, por meio do servidor *Zabbix* e as regras de correlacionamento. A ferramenta possui interface *web* para administração e exibição de dados. Os alertas do sistema de monitoramento podem ser configurados para utilizar vários métodos de comunicação, como *SMS*, *e-mail* e abertura de chamados em sistemas de *helpdesk*. O sistema permite ainda que ações automáticas como, por exemplo, restart de serviços sejam executados a partir de eventos. Os principais módulos são [ZABBIX, 2015]:

- ***Zabbix server*** - coleta dados para o monitoramento sem agentes e de agentes que fazem parte do contexto do Zabbix, visando acompanhar ativamente recursos e aplicações locais como discos rígidos, memória, processador. Quando alguma anormalidade é detectada, alertas são emitidos visualmente e por meio de uso de sistemas de comunicação como *e-mail* e *SMS (Short Message Service).* O servidor *Zabbix* mantém um histórico dos dados coletados em banco de dados (*Oracle*, *MySQL* e *PostgreSQL*), a partir dos quais são gerados gráficos, painéis de acompanhamento e *slide-shows* que mostram informações de forma alternada;
- ***Zabbix proxy*** - coleta as informações de uma parte do parque monitorado e repassa para o *Zabbix server*. É um item essencial para uma arquitetura de monitoramento distribuído. O *Zabbix proxy* permite: 1) a coleta assíncrona em redes distintas, onde não é possível a manutenção de regras de roteamento e *firewall* para cada *host* monitorado; 2) trabalhar como ponto de resiliência nos casos de instabilidade nos *links* entre redes distintas(*WAN*); e 3) diminuir a carga do *Zabbix server;*
- ***Zabbix agent -*** permite coletar métricas comuns - específicas de um sistema operacional, como processador e memória. Além disso, o agente *Zabbix* permite a coleta de métricas personalizadas com uso de *scripts* ou programas externos permitindo a coleta de métricas complexas e até tomada de ações diretamente no próprio agente *Zabbix*.

As VLANs foram simuladas no *software Packet Tracer* que é um *software* gratuito para simulação de redes de computadores desenvolvido pela Cisco, com foco educacional. Este *software* oferece visualização, simulação, criação, avaliação e recursos de colaboração que facilitam o ensino e aprendizagem de diversos conceitos complexos de tecnologias de redes e telecomunicações [CISCO, 2015].

Após a simulação, as VLANs foram configuradas no *switch Dell PowerConnect* 2848 da Prefeitura de Palmeira das Missões, por meio de associação estática que consiste em designar uma determinada porta do *switch* e atribuí-la a determinada VLAN. Esse método é mais utilizado por permitir um gerenciamento mais prático, não sendo necessário o cadastramento de dispositivos a ingressar na rede. Isso de certa forma é mais seguro também, pois era possível clonar ou alterar o endereçamento físico dos adaptadores de rede, possibilitando o ingresso a outra sub-rede sem a devida autorização.

Para a configuração da DMZ utilizou-se dos 3 servidores físicos disponíveis na prefeitura, sendo aplicadas as regras já existentes no *firewall* para determinar o acesso aos principais serviços da DMZ.

Os testes e validação desta proposta foram realizados com o apoio do *software Zabbix,* por meio de comparativos que permitiram analisar as informações da rede antes e depois das mudanças aplicadas, bem como se comportou a nova estrutura de rede, e também mediante a confirmação do Departamento de Informática da Prefeitura de Palmeira das Missões perante os resultados alcançados.

Também foi utilizado o *software* SARG (*Squid Analysis Report Generator*) que tem a função de gerar relatórios de acesso à *internet.* Todo esse acesso é mantido pelo *Squid*[16] e fica armazenado em um arquivo chamado *access.log.* Entretanto, esse arquivo grava as informações mas não permite uma fácil leitura e interpretação do mesmo. O SARG, a partir das informações contidas no *access.log*, cria várias páginas em formato HTML (*HyperText Markup Language*) para melhorar a apresentação dos dados. Por meio do SARG é possível visualizar: acessos a *sites*, por usuários; tempo de permanência; consumo em *bytes*; quantidade de conexões; *sites* mais acessados; *sites* negados e falha de autenticação. Com isso é possível aprimorar a política de segurança de dados da organização [GIL, 2015].

4.4 Implementação da Solução Proposta

A implementação da solução proposta teve início a partir da instalação do *software Zabbix*, para que fosse possível começar a análise da rede e, assim, poder direcionar de forma mais clara a implantação de um ambiente melhor gerenciado e com uma maior segurança.

4.4.1 Validação do fluxo de rede com Zabbix

O primeiro passo foi o de disponibilizar um servidor para alocar o serviço do *Zabbix*. Utilizou-se, então, o *hardware* do servidor *Dell PowerEdge R620* e a plataforma de

[16] *Squid* - é um servidor *Proxy* e *cache* que permite tanto compartilhar o acesso à *web* com outros computadores da rede, quanto melhorar a velocidade de acesso por meio do *cache* [SQUID,2015].

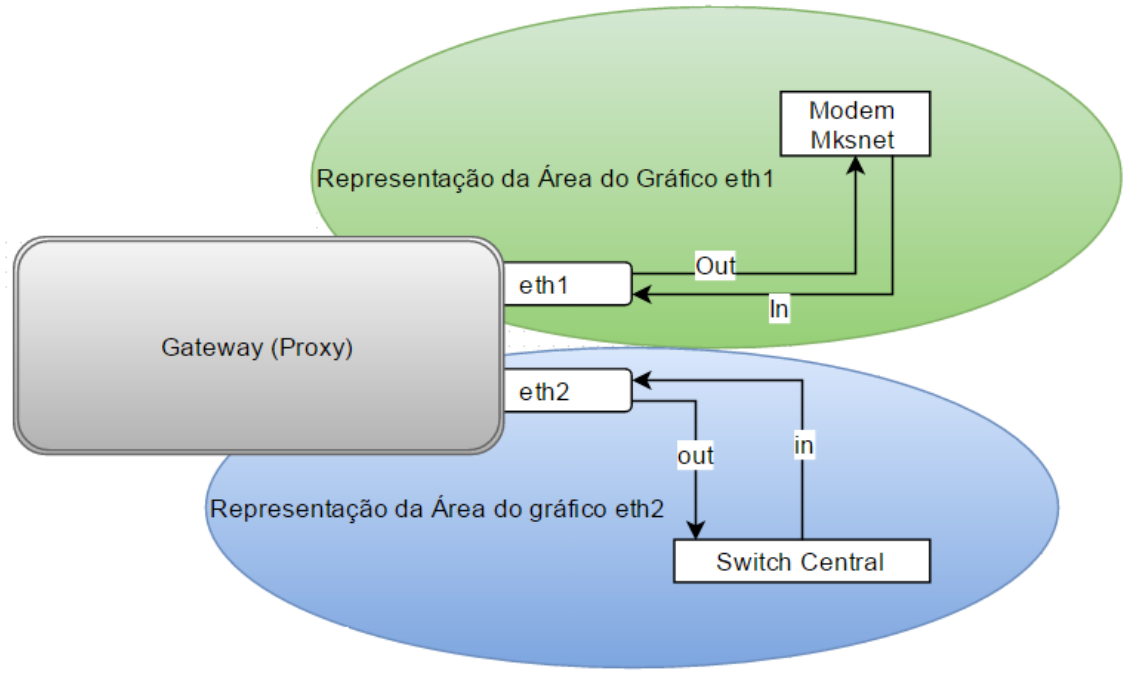
virtualização de servidores *XenServer*, onde criou-se uma máquina virtual com as seguintes configurações: 2 núcleos de processadores, 2*GB* de memória *RAM,* e 80*GB* de *HD (Hard Disk*) na qual foi instalado o sistema operacional *Ubuntu Server*. A partir disto, instalou-se e configurou-se o *Zabbix* e suas dependências como *MySQL e PHP* [ADONIS, 2015].

Com o serviço do *Zabbix* configurado de forma personalizada, dentro das expectativas de gerenciamento atual, onde a proposta se encaixa em monitorar o tráfego dos nodos centralizadores, o próximo passo envolveu a instalação e configuração dos agentes *Zabbix*[17] nos computadores da rede da Prefeitura, de forma a representar uma máquina com maior fluxo dentro dos departamentos. Além do *Gateway* que realiza o roteamento interno das *LANs* (*Local Area Network*) e também *NAT* (*Network Address Translation*), faz parte também da estrutura de serviços, gerenciada pelo *Zabbix,* o *Windows Server* 2008 R2 que hospeda os Sistemas de Gestão Pública da empresa Delta (bem como seus Bancos de Dados), o *Gateway* que também faz *Proxy*, TS (*Terminal Server*) – Saúde, Samba, *Firewall*, SGA (Sistema de Gerenciamento de Atendimento) *software* livre que está em fase inicial de implantação para atender as necessidades da Prefeitura como: fluxo de atendimento, controle de filas e geração de senhas, bem como o próprio *Zabbix*.

A partir de reuniões realizadas junto ao Departamento de Informática da Prefeitura, foram escolhidos os recursos do *Zabbix* que seriam utilizados, a partir da criação das VLANs realizada por meio do *switch* gerenciável *Dell PowerConnect 2848.* A rede foi dividida em "sub-redes", permitindo, assim, com o apoio dos recursos do *Zabbix,* gerenciar e monitorar estas VLANs de forma individual, proporcionando um gerenciamento mais adequado da rede.

A Figura 4 apresenta uma ilustração das conexões utilizadas para acesso aos serviços básicos do Servidor *Gateway* geral da rede, onde as interfaces eth1 e eth2 definem o fluxo de dados em *in* (entrada) e *out* (saída), conforme a conexão estabelecida entre o Provedor de Acesso à Internet e a rede interna.

[17] Agentes *Zabbix* - São componentes de software distribuído.



[18]

Figura 4: Representação da área em que foi realizada a medida dos gráficos eth1 e eth2
Fonte: Dos Autores, 2015

Na Figura 4 pode-se observar a primeira área que foi analisada (detalhada no gráfico da Figura 5), onde foi considerado o fluxo da interface eth1, que tem como conexão o provedor de acesso à *Internet* com *link* dedicado de 20 Mbps (*link* real de *down* e *up*). A Figura 5 representa a análise de um fluxo de rede para a interface *eth1* com bases nas entradas e saídas ocorridas no dia 24 de setembro de 2015.

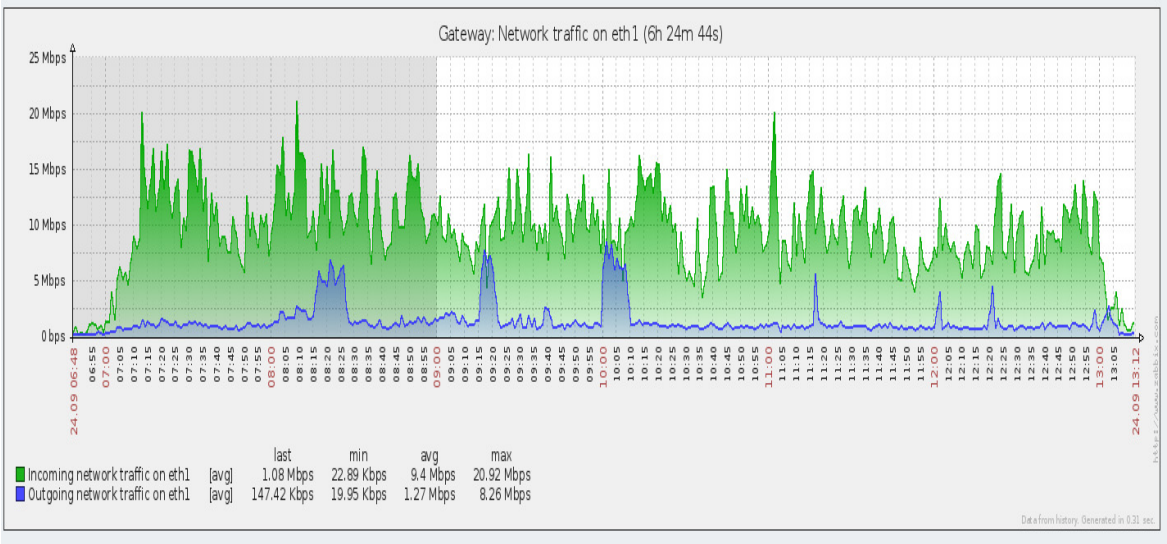


Figura 5: Porta eth1 – Fluxo de Tráfego de Internet da Rede de Computadores

Fonte: Dos Autores, 2015

[18] Mksnet – Atual Provedor de Acesso à Internet da Prefeitura Municipal de Palmeira das Missões -RS.

Como é possível visualizar no gráfico apresentado na Figura 5, monitorou-se o fluxo de tráfego na Internet pela porta *eth1* (cor verde, representando a entrada do fluxo e, na cor azul a saída). O gráfico está representando um período de aproximadamente 6 horas, devido ao expediente de turno único que se realiza na Prefeitura, cujo horário é das 7h às 13h, na data de 24 de setembro de 2015. Pode-se observar no gráfico que, por volta de 6h55min da manhã o fluxo está praticamente inativo e, a partir das 7h já se começa a visualizar saltos na rede e grandes picos. Isso se deve, principalmente, ao acesso aos recursos que necessitam de Internet, tais como diversos *sites* que os setores da Prefeitura necessitam acessar, envolvendo Receita Federal, Receita Estadual observando-se que neste momento a rede encontrava-se com o tráfego de navegação interna sem qualquer filtro ou bloqueio de *sites.* O fluxo constante deste período em relação à entrada (*in*) manteve-se em uma média (*avg*) de 9,4*Mbps*, máxima de 20,92*Mbps*, mínima de 22,89*Kbps* e *last* (se refere ao último dado coletado) com valor de 1,08*Mbps*. Já em relação à saída (*out*), o fluxo manteve-se em uma média de 1,27*Mbps*, máxima de 8,26*Mbps*, mínima de 19,95*Kbps* e *last* de 147,42*Kbps*.

Já o gráfico apresentado na Figura 6 mostra o tráfego do *gateway* correspondente à conexão com a rede interna no dia 24 de setembro de 2015, em um período de aproximadamente 6 horas.

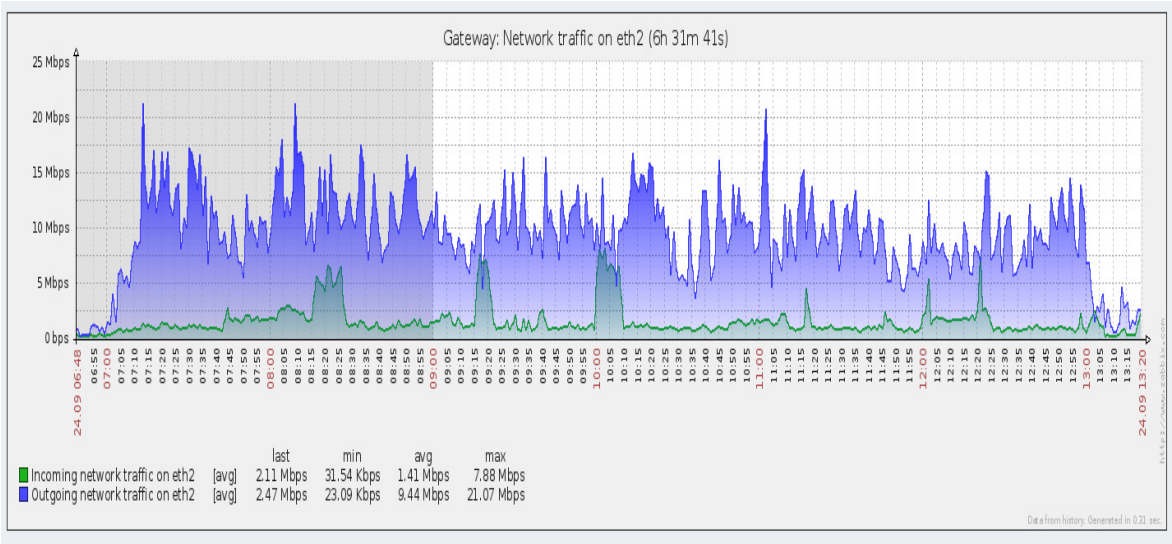


Figura 6: Porta eth2 - Fluxo de Rede interno para a navegação na Internet

Fonte: Dos Autores, 2015

O gráfico apresentado na Figura 6 também corresponde a um período referente ao expediente de turno único, na mesma data do gráfico anterior. Entretanto, este gráfico representa a interface *eth2*, que corresponde ao fluxo de entrada e saída da rede interna com a Internet (a cor verde representa a entrada de fluxo e, a cor azul, a saída). Em azul tem-se a demanda do que está sendo enviado pela rede para a conexão externa, caracterizado como *upload*. Assim, pode-se notar que às 7h, quando os computadores estão sendo ligados no início do expediente, o gráfico já demonstra saltos e, logo em seguida que os usuários começam a usar os recursos da rede, o gráfico apresenta picos.

Esses picos podem ser interpretados com um pequeno exemplo das diversas rotinas que ocorrem na rede, tais como o acesso a pastas compartilhadas na rede. O fluxo constante deste período referente à entrada (*in*) manteve-se em uma média de 1,41*Mbps*, máxima de 7,88*Mbps*, mínima de 31,54*Kbps* e *last* de 2,11*Mbps*. Analisando os dados de saída, (*out)* a média é de 9,44*Mbps*, máxima de 21,07*Mbps*, mínima de 23,09*Kbps* e *last* de 2,47*Mbps*.

4.4.2 Projetando as VLANs

O próximo passo para a implementação da solução proposta envolveu o planejamento das VLANs. Para que fosse possível visualizar um ambiente com uma ideia mais prática para a implementação, utilizou-se o *software Packet Tracer*. A Figura 7 apresenta uma simulação com três departamentos existentes na Prefeitura Municipal, que são o Protocolo, CPD e a Secretaria de Educação.

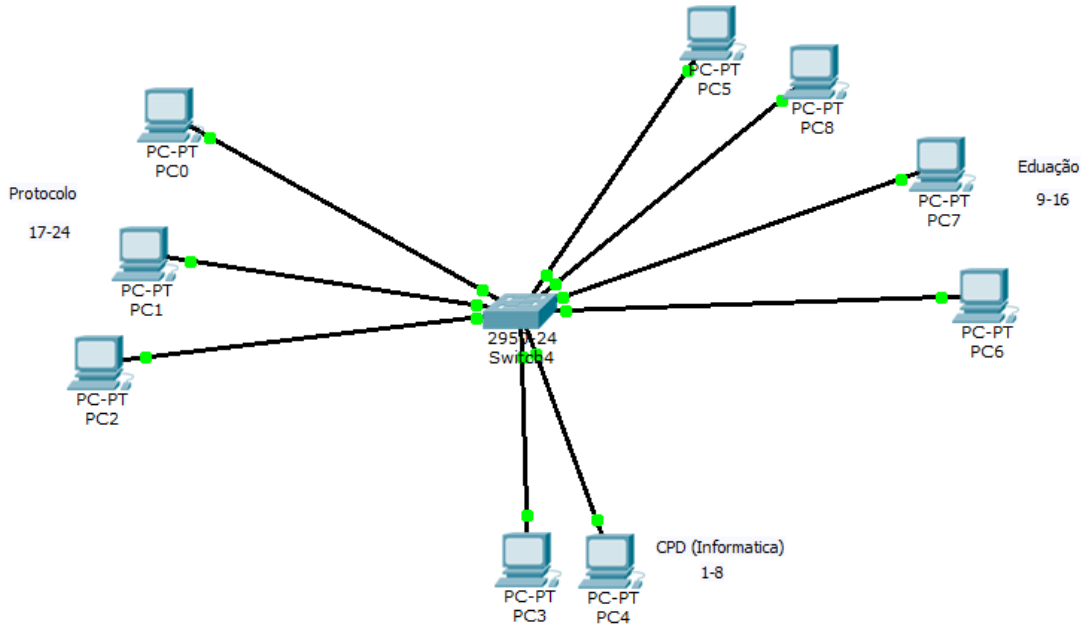


Figura 7: Representação da Simulação de VLANs

Fonte: Dos Autores, 2015

Conforme mostra a figura 7, foram simuladas 3 VLANs em menor escala (com um número menor computadores). Nessa simulação foi usado um *switch* de 24 portas e associadas as VLANs, sendo elas: VLAN CPD com associação da porta 1-8, VLAN Educação na porta 9-16 e VLAN Protocolo na porta 17-24. Um computador de cada um destes departamentos foi associado a uma porta do *switch*, deixando-se o resto das portas vagas dentro de sua própria VLAN. Foram feitos testes com envio de pacotes internamente às suas próprias VLANs e constatou-se que todos os testes funcionaram corretamente. Além destes testes, realizou-se o envio de pacotes de uma VLAN para outra, ocasionando a falha no envio do pacote. Assim, verificou-se que a simulação das VLANs funcionou de acordo com o esperado.

4.4.3 Estruturando as Vlans

Como a ideia na Prefeitura Municipal era a de configurar as VLANs por departamentos, setores ou secretarias que realizam suas atividades no prédio da Prefeitura, planejou-se uma tabela com as respectivas VLANs para auxiliar no projeto de implementação da proposta, já que existe um número considerável de aproximadamente 20 departamentos atuando no prédio da Prefeitura Municipal.

Considerando que alguns setores possuem apenas um ou dois computadores, definiu-se, então, a maneira mais adequada de se planejar as VLANs como, por exemplo, a VLAN 11 (Cadastro e Arrecadação) já que o setor de cadastro possui apenas um computador. Também pensou-se nas VLANs de *Wi-fi*, o Departamento de Informática definiu que quatro VLANs seriam suficientes para atender as demandas de rede sem fio na Prefeitura Municipal.

A partir da definição das VLANs o gerenciamento pode ser feito de forma a caracterizar as mesmas isoladamente, possibilitando, assim, um monitoramento e gerenciamento direcionado ao tráfego real de cada VLAN específica. O Quadro 4 apresenta as configurações e os dados usados nas VLANs.

Vlan	Nome	Porta SW	Truncamento	IP Rede
1	**Default**	1, 32-48		
2	DMZ	2 - 6	1	10.10.2.0/24
3	CPD (Informática)	7	1	10.10.3.0/24
4	RH	8	1	10.10.4.0/24
5	Engenharia	9	1	10.10.5.0/24
6	SMIC	10	1	10.10.6.0/24
7	Procuradoria	11	1	10.10.7.0/24
8	Gab. Prefeito	12	1	10.10.8.0/24
9	Protocolo	13	1	10.10.9.0/24
10	ICMS	14	1	10.10.10.0/24
11	Cad. e Arrecadação	15	1	10.10.11.0/24
12	Licitação	16	1	10.10.12.0/24
13	Compras	17	1	10.10.13.0/24
14	Contabilidade	18	1	10.10.14.0/24
15	Patrimônio	19	1	10.10.15.0/24
16	Cons. Tutelar	20	1	10.10.16.0/24
17	Est. Prob/Incra	21	1	10.10.17.0/24
18	Tesouraria	22	1	10.10.18.0/24
19	Fiscalização	23	1	10.10.19.0/24
20	P2P	24,25,26,27	1	10.10.20.0/24
21	Wi-fi 1	28	1	10.10.21.0/24
22	Wi-fi 2	29	1	10.10.22.0/24
23	Wi-fi 3	30	1	10.10.23.0/24
24	Wi-fi 4	31	1	10.10.24.0/24
25	Educação	32	1	10.10.25.0/24

Quadro 4: Quadro com o planejamento das VLANs Fonte: Dos Autores, 2015

No Quadro 4 é possível visualizar a configuração identificando as *flags* e os endereços lógicos das VLANs que foram utilizados tanto na identificação dos *hosts* nos departamentos e dados para a configuração das mesmas no *switch Dell PowerConnect 2848.*

O quadro possui, na sua primeira coluna, o número correspondente de cada VLAN; na segunda coluna o nome, que serve para uma organização de gerência; a terceira coluna corresponde à porta do *switch* para cada VLAN. Destaca-se que as VLANs *DMZ* e *P2P* possuem mais de uma porta e a *vlan1* (*default*) é uma VLAN pré-determinada com configurações do *switch.* Esta VLAN foi alocada na porta 1 do *switch,* restando da porta 32 a 48 para novas configurações. A quarta coluna especifica o truncamento de cada VLAN. Todas as VLANs estão truncadas com a porta 1, que faz conexão com a interface de rede eth2 do servidor *Dell PowerEdge R620.* Por fim, na quinta coluna está o *range* de *IP* referente ao prefixo e sufixo, indicando que apenas os sufixos, no caso os *hosts*, poderão variar sua numeração. Por exemplo, a *vlan2* poderia variar seus *hosts* de 10.10.2.0 a 10.10.2.255, e assim determinando por meio do /24 a definição de sua máscara de rede em 255.255.255.0.

4.4.4 Configuração do *Gateway* (TAG)

Após a definição de endereçamento lógico e *flags* no planejamento das VLANs, o próximo passo foi a configuração do *switch,* que envolvia em configurar as portas correspondentes a cada VLAN e a função de truncamento que consiste no processo de interligar mais de uma VLAN por meio de um *link* único chamado de *trunking* (tronco)*,* por onde passam informações destinadas e originadas por mais de uma VLAN. O *link* de tronco não pertence a nenhuma das VLANs individualmente. A configuração foi realizada por meio da implementação de um *script* no Linux. A Figura 8 apresenta o script para configurar as TAGs da VLANs.

Na Figura 8 são apresentados trechos importantes do *script* desenvolvido para a criação das VLANs, usando como exemplo as VLANs *Vlan* 2, *Vlan* 3 e *Vlan* 4 com os nomes *DMZ,* CPD e RH sendo criadas na interface de rede eth2. Para isso foi necessário fazer as *tags* das VLANs*,* que consiste na definição dos "rótulos ou etiquetas" nos pacotes, para que o *switch* possa definir fisicamente a conexão das portas com a rede específica nas portas plugadas e com o truncamento de portas compartilhadas como o caso da porta 1 (*gateway*). Por meio do *script* mostrado na Figura 8, iniciando no comando *vconfig*, que cria novas interfaces de redes virtuais a partir de uma interface de rede real, no caso a eth2, atribuindo números de *VLANs* diferentes para cada rede criada.

O *script* está basicamente dividido em duas partes iniciando (*start*) e desmontando (*stop*). A rede então fica configurada com a segmentação definida pelo comando *set_flag*, e o comando *ifconfig* sendo usado para configurar e manter as interfaces de rede e para mostrar as interfaces de rede.

Esse *script* teve que ser aplicado no servidor *Dell PowerEdge R620* pois o *switch Dell PowerConnect 2848* só possui acesso à camada *Layer* 2 (camada de enlace do modelo OSI). Um *switch Layer 2* apenas possui a capacidade de trabalhar com *MAC addresses* (endereço físico). Isso permite que ele se comunique apenas baseado em endereços MAC. Ele propaga todo *broadcast* e não tem capacidade de interligar redes ou sub-redes. Já um *switch Layer 3* (camada de rede do modelo OSI) além de código *MAC*, tem a capacidade de roteamento e também trabalha com endereçamento lógico, portanto, possui a capacidade de identificar redes e sub-redes (endereço *IP* e máscara), além de interconectar redes ou sub-redes, sendo muito usado para criação de VLANs.

```
####################     VLANS     ################################
#
# by : Denison Molina  /  Fernando Beux
# Data: 23 / 10 / 2015
# Edit:
#
VCONFIG=/sbin/vconfig

case "$1" in start)

echo "Criando Vlans"
echo " "
echo "Vlan DMZ"
echo " "
    $VCONFIG add eth2 2
    $VCONFIG set_flag eth2.2 1
    ifconfig eth2.2 10.10.2.1 netmask 255.255.255.0 up

    echo "Vlan CPD"
echo" "
    $VCONFIG add eth2 3
    $VCONFIG set_flag eth2.3 1
    ifconfig eth2.3 10.10.3.1 netmask 255.255.255.0 up

echo "Vlan RH"
echo" "
    $VCONFIG add eth2 4
    $VCONFIG set_flag eth2.4 1
    ifconfig eth2.4 10.10.4.1 netmask 255.255.255.0 up

    ifconfig eth2.2 10.10.2.1 netmask 255.255.255.0 up
    ifconfig eth2.3 10.10.3.1 netmask 255.255.255.0 up
    ifconfig eth2.4 10.10.4.1 netmask 255.255.255.0 up
     ;;

     stop)

echo "Removendo vlans ..."
    $VCONFIG rem eth2.2
    $VCONFIG rem eth2.3
    $VCONFIG rem eth2.4

    ifconfig eth2.2 10.10.2.1 netmask 255.255.255.0 down
    ifconfig eth2.3 10.10.3.1 netmask 255.255.255.0 down
    ifconfig eth2.4 10.10.4.1 netmask 255.255.255.0 down

    echo "vlans.sh [stop|start]"
    exit 1
  ;;

esac
exit 0
```

Figura 8: *Script* da Criação das VLANs no Servidor Fonte: Dos Autores, 2015

4.4.5 Regras de *Firewall* para as VLANs

As regras de *firewall* são relacionadas ao tráfego de rede para determinar quais operações de transmissão de dados podem ser executadas controlando, assim, a entrada (*in*) e a saída (*out*). O *firewall* também deve estabelecer o que pode ou não pode passar entre uma rede e outra, além de fazer o papel de roteamento entre as VLANs.

No *script* desenvolvido há regras padrão com a finalidade de prover acesso à *internet* e utilizando o servidor *Proxy*. Desta forma o script redireciona o tráfego de navegação da porta 80 para a porta 3128 do *Squid*. Esta definição é feita para cada VLAN criada com a intenção de controlar de forma personalizada as regras e filtros de navegação. A Figura 9 apresenta trechos importantes do *script* das Regras de *Firewall* que foi usado para a configuração das VLANs.

```
#!/bin/bash
#
# Shell Script - Firewall
# ========================
# Autor:-  Fernando Beux dos Santos
# Email:-  ti@palmeiradasmissoes-rs.com.br
#

# IP da Rede
NETWORK=192.168.1.0/24
VLAN2=10.10.3.0/24
VLAN7=10.10.7.0/24
VLAN21=10.10.21.0/24
VLAN4=10.10.4.0/24

# Interface da Rede Local - LAN
ILAN=eth2

# Interface da Rede Externa - Internet
INET=eth1

IPT=/sbin/iptables

=====================================
PROXYY () {



    ############################################################
    #Mascara as conexoes da rede interna e armazena os logs
    ############################################################
    #/usr/sbin/iptables -t nat
#   echo Mascarando Rede Interna

    $IPT -t nat -A POSTROUTING -s $NETWORK -o $INET -j MASQUERADE
        $IPT -t nat -A POSTROUTING -o $INET -s $VLAN -j MASQUERADE
        $IPT -t nat -A POSTROUTING -s $VLAN2 -o $INET -j MASQUERADE
        $IPT -t nat -A POSTROUTING -s $VLAN7 -o $INET -j MASQUERADE
        $IPT -t nat -A POSTROUTING -s $VLAN21 -o $INET -j MASQUERADE
        $IPT -t nat -A POSTROUTING -s $VLAN4 -o $INET -j MASQUERADE

=============================================================
    ################################################
    # Redireciona conexÃµes porta 80 para Proxy-3128
    ################################################
    echo Redirecionando Proxy

    $IPT -t nat -A PREROUTING -p tcp -s 192.168.1.0/24 --dport 80 -j REDIRECT --to 3128
        $IPT -t nat -A PREROUTING -p tcp -s $VLAN2 --dport 80 -j REDIRECT --to 3128
        $IPT -t nat -A PREROUTING -p tcp -s $VLAN7 --dport 80 -j REDIRECT --to 3128
        $IPT -t nat -A PREROUTING -p tcp -s $VLAN21 --dport 80 -j REDIRECT --to 3128
        $IPT -t nat -A PREROUTING -p tcp -s $VLAN4 --dport 80 -j REDIRECT --to 3128
```

Figura 9: *Script* Regras de Firewall Fonte: Dos Autores, 2015

A função Proxy no *script* define que haverá um mascaramento de IP pela função *NAT* e que todas as VLANs setadas abaixo serão redirecionadas da porta 80 para 3128, assim, participando do *cache* e dos filtros definidos nas regras de *Squid*. Na Figura 9 foram usadas como exemplos as VLANs 3, 7, 21 e 4 porque até o momento essas já tinham sido configuradas.

4.4.6 Serviço de Internet com Regras de *Proxy*

Para navegação nos *hosts* das VLANs existem configurações específicas para cada uma delas criando, assim, uma organização lógica de sub-redes. Isto permite que as VLANs sejam gerenciadas de forma a isolar regras de cada setor ou departamento, conforme estabelece a política de segurança. A Figura 10 mostra o *script* do *Proxy* utilizado na configuração das VLANs.

```
#!/bin/bash
#squid.conf
http_port 3128 transparent
...
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl to_localhost dst 127.0.0.0/8
acl lan src 192.168.1.0/24
acl vlan2 src 10.10.3.0/24
acl vlan7 src 10.10.7.0/24
acl vlan21 src 10.10.21.0/24
acl vlan4 src 10.10.4.0/24
...
Regras gerais de bloqueios (personalizado conforme política de segurança)
...
# Liberando todos os outros acessos para a lan
http_access allow lan
http_access allow vlan2
http_access allow vlan7
http_access allow vlan21
http_access allow vlan4
```

Figura 10: *Script* do *Proxy* Fonte: Dos Autores, 2015

Na Figura 10 são apresentados trechos importantes do *script* do *Proxy* referente às VLANs. No primeiro momento pode-se observar as VLANs que tinham sido criadas até então, sendo atribuídas variáveis às mesmas; no meio do *script* são criadas as regras gerais de bloqueio. Essas regras podem ser o bloqueio de uma determinada rede social ou *site*. Essas regras serão personalizadas e remodeladas conforme a política de segurança que a Administração Municipal pretender implantar.

Com as VLANs estando configuradas no *switch* e o *script* para fazer o *tag* das VLANs, permissões de *firewall e Proxy* configurados, o próximo passo envolveu a configuração dos *hosts* das VLANs. Para isso, foi preciso deslocar-se a cada departamento da Prefeitura, para realizar as configurações de IP nos *hosts,* seguindo o critério de *range* de IP de cada VLAN. Após realizar essa configuração, a próxima tarefa envolveu a reconfiguração dos *hosts* no servidor *Zabbix*, referentes às VLANs configuradas. Essa configuração envolveu a redefinição dos IPs dos *Agentes zabbix* no servidor, para voltar a realizar o monitoramento individual dos *hosts.*

5. Resultados e Comparações

Esta seção tem como objetivo fazer uma análise e validação da solução implementada, destacar os principais pontos referentes às mudanças que ocorreram na rede de computadores da Prefeitura Municipal e descrever os resultados alcançados.

Todas as figuras dispostas nesta seção demonstram um período de aproximadamente 6 horas, tendo-se em vista que os gráficos foram gerados durante o exercício das atividades nos setores e a Prefeitura está realizando seus trabalhos em turno único correspondente, das 7h às13h.

As VLANs foram configuradas na interface de rede eth2 que corresponde ao fluxo de rede interno da Prefeitura. Elas estão representadas nos gráficos a seguir como uma parte de toda a rede eth2, sendo possível, assim, gerenciar e monitorar a rede por partes com às VLANs. Também realizou-se uma avaliação técnica correspondente à execução de atividades nos *hosts* que geram fluxo de rede em cada setor ou departamento onde foi aplicada a VLAN. Para que o trabalho não ficasse muito extenso, escolheu-se 3 VLANs para serem utilizadas nas comparações, sendo as VLANs do Departamento de Informática, Cad. Arrecadação e Wi-fi 1.

A Figura 11 representa a VLAN 3, que corresponde à VLAN do Departamento de Informática, que é representada no gráfico pela interface de rede eth2.3. O número 3 corresponde ao número da VLAN implementada, como mostrado no exemplo do *script* da Figura 8.

A VLAN do CPD (Dpto. Informática) foi a primeira VLAN a ser implementada devido a alguns fatores como: proximidade aos equipamentos em que foram implementadas, não afetar o trabalho dos outros setores durante a implantação e um suporte mais rápido já que era possível realizar as configurações necessárias com maior agilidade.

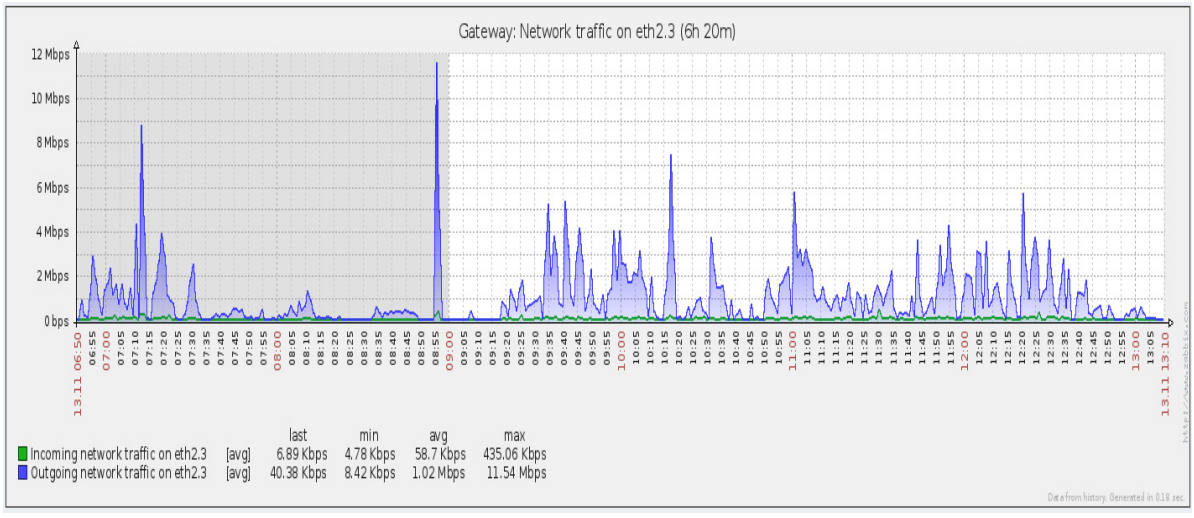


Figura 11: VLAN 3 CPD (Informática) Fonte: Dos Autores, 2015

O gráfico da Figura 11 demonstra o fluxo de rede durante as atividades do Departamento de Informática no dia 13 de novembro de 2015. Pode-se notar que, a partir das 7h, o gráfico já começa a demonstrar fluxo (geralmente é quando começam os suportes por acesso remoto, causando uma demanda na rede, representada pela cor

azul). Como o CPD praticamente não utiliza os *softwares* da empresa Delta, apenas prestando suporte aos mesmos, esse fluxo de rede não se origina disso e sim de uma demanda de Internet, e acessos na rede via *Samba*.

A Figura 12 representa a VLAN 11, que corresponde à VLAN Cadastro e Arrecadação, representada no gráfico pela interface de rede eth2.11. O número 11 corresponde ao número da VLAN implementada.

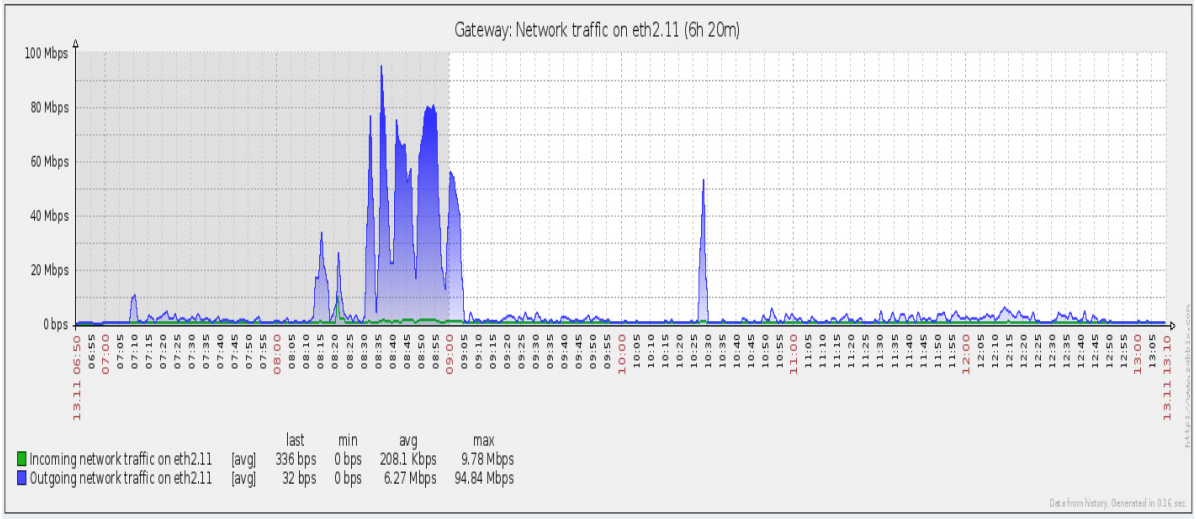


Figura 12: VLAN 11 Cad. Arrecadação Fonte: Dos Autores, 2015

A VLAN 11 também teve seu gráfico gerado no dia 13 de novembro de 2015. O gráfico demonstra alguns pontos importantes neste dia: o Sistema Tributos, que é utilizado pelo setor, teve uma atualização de aproximadamente 600*Mb* e começou sua atualização por volta das 8:30h. O gráfico demonstra picos na rede de até 94,84*Mbps* o que é considerado alto, já que a rede tem transmissão de até 100*Mbps*. As atualizações são disponibilizadas por meio de uma partição no *Samba* podendo, assim, ser acessada pelos *hosts* diretamente de seus setores. Constatou-se que isso gera uma grande demanda na rede, lembrando que o Sistema Tributos e os demais realizam muitas operações que geram uma demanda interna na rede de computadores.

O gráfico demonstra na entrada (*in*) de fluxo, representada pela cor verde, uma mínima de 0*bps*, média de 208,1*kbps*, máxima de 9,78M*bps* e *last* de 336*bps*. Já referente à saída (*out*), representada pela cor azul, tem-se uma mínima de 0*bps*, média de 6,27*Mbps*, máxima de 94,84*Mbps* e *last* de 32*bps*.

A Figura 13 representa a VLAN 21, que corresponde à VLAN Wi-fi 1, representada no gráfico pela interface de rede eth2.21. O número 21 corresponde ao número da VLAN implementada.

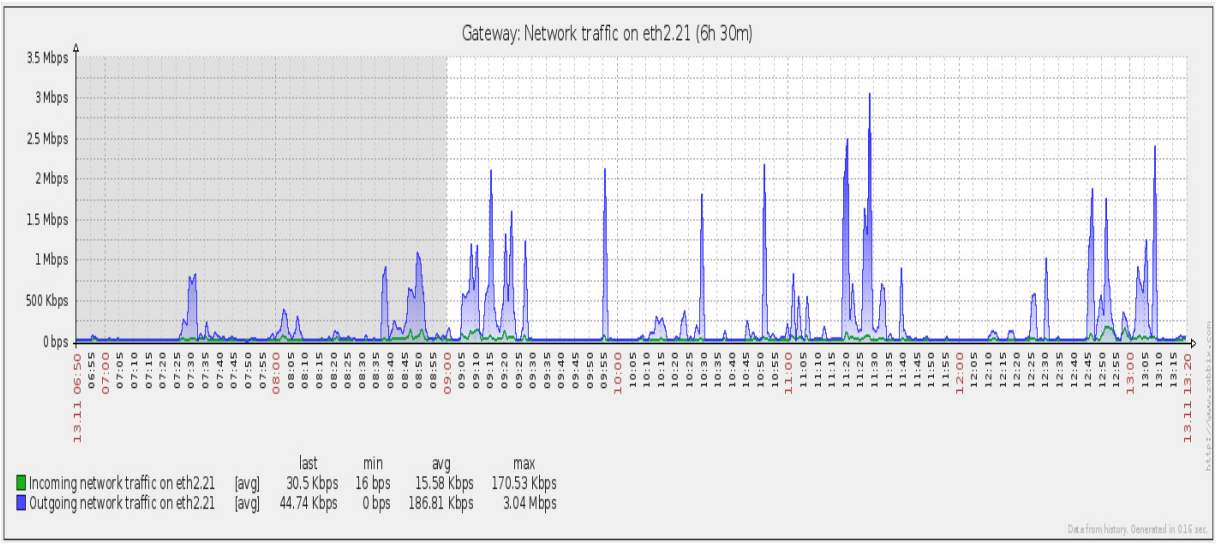


Figura 13: VLAN 21 Wi-fi 1 Fonte: Dos Autores, 2015

A VLAN 21 foi a primeira VLAN destinada a rede sem fio a ser configurada. O ponto de *wi-fi* está instalado eu um dos pontos estratégicos da prefeitura, por ser próximo a setores como Administração e Gabinete do Prefeito, onde ocorrem muitas reuniões e pequenas palestras, que necessitam de um fácil acesso à *Internet.*

O gráfico demonstra na entrada (*in*) de fluxo, representada pela cor verde, uma mínima de 16*bps*, média de 15,58*kbps*, máxima de 170,53*kbps* e *last* de 30,5*kbps*. Já referente à saída (*out*), representada pela cor azul, tem-se uma mínima de 0*bps*, média de 186,61K*bps*, máxima de 3,04*Mbps* e *last* de 3,04*Mbps*.

A Figura 14 demonstra a interface de rede eth2 e representa todo o fluxo de rede interno da Prefeitura Municipal no dia 13 de novembro de 2015.

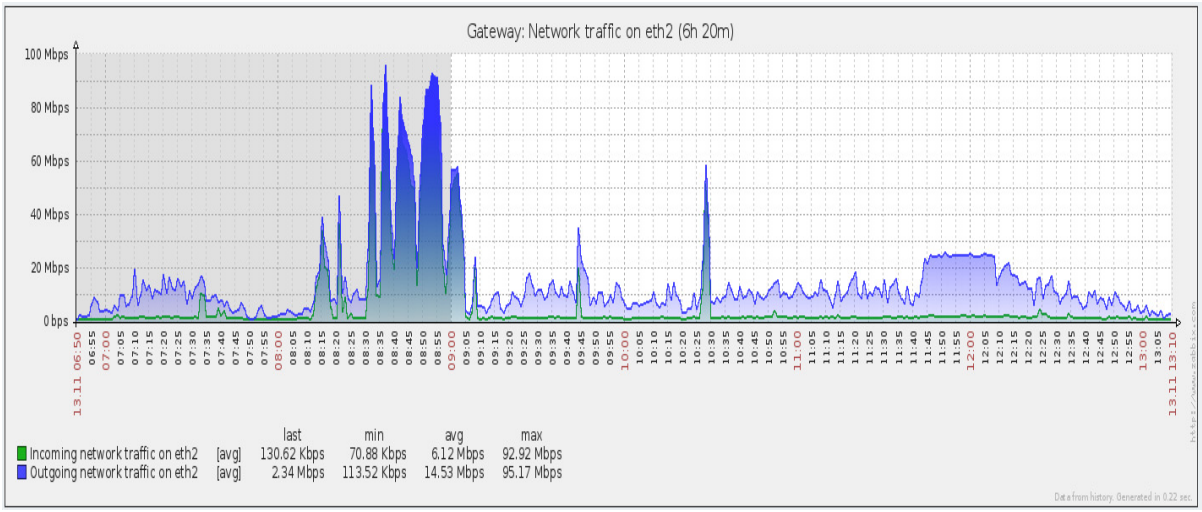


Figura 14: Porta eth2 - Fluxo de Rede interno após configuração das VLANs

Fonte: Dos Autores, 2015

Comparando o fluxo de rede interna da interface de rede eth2, nota-se que das 7h até aproximadamente 8h30min, verifica-se que se mantém um fluxo médio de até 20*Mbps.* Porém, a partir desse horário que horário o gráfico já demonstra alguns saltos, atingindo

seu pico máximo de 95,17*Mbps* em uma rede que pode chegar até 100*Mbps.* Desta forma, verifica-se que isso não representa um fluxo normal de rede interno ou fluxo de *internet,* pois o *link* do provedor de *internet* é de 20*Mbps*.

Apurando-se as possíveis causas, constatou-se que o fluxo interno de rede está muito elevado. Determinar os possíveis *hosts* que estariam causando esse fluxo foi possível por meio da configuração das VLANs. Ao observar os gráficos individuais de cada VLAN, verificou-se que a VLAN 11 *Cad. e Arrecadação* estava causando este fluxo elevado. Desta forma é possível identificar questões como essa, para aprimorar gerenciamento da rede.

O gráfico da Figura 14 demonstra na entrada (*in*) de fluxo, representada pela cor verde, uma mínima de 70,*88Kbps*, média de 6,*12Mkbps*, máxima de 92,92*Mbps* e *last* de 130,62*kbps*. Já referente à saída (*out*), representada pela cor azul, tem-se uma mínima de 113,*52Kbps*, média de 14,53Mbps, máxima de 95,17*Mbps* e *last* de 2,34*Mbps*.

A Figura 15 demonstra a interface de rede eth1 e representa todo o fluxo de rede interno da Prefeitura Municipal no dia 13 de novembro de 2015.

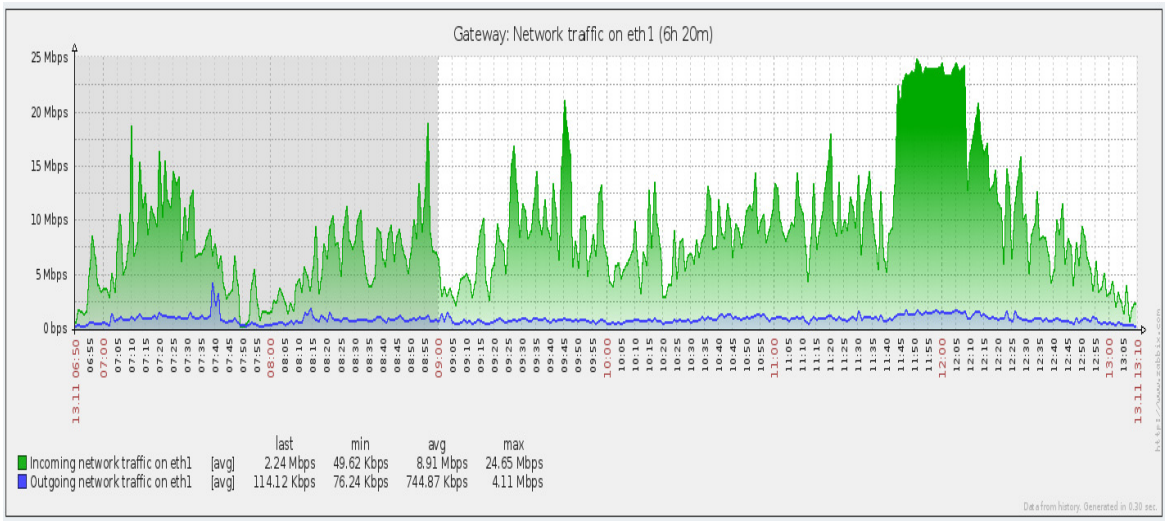


Figura 15: Porta eth1 – Fluxo de Tráfego de Internet após configuração das Vlans

Fonte: Dos Autores, 2015

O gráfico da Figura 15 demonstra na entrada (*in*) de fluxo, representada pela cor verde, uma mínima de 49,62*Kbps*, média de 8,91*Mbps*, máxima de 24,65*Mbps* e *last* de 2,24*Mbps*. Já referente à saída (*out*), representada pela cor azul, tem-se uma mínima de 76,24*Kbps*, média de 744,87Kbps, máxima de 4,11*Mbps* e *last* de 114,12*Kbps*.

Como é possível verificar na Figura 16, o *software* SARG gerou um relatório diário de todo o acesso à *web* que aconteceu no dia 13 de novembro de 2015. Nessa lista são mostrados os *hosts* que tiveram uma maior demanda de acesso sendo, assim, possível visualizar todo o conteúdo acessado por cada *host*.

O SARG tornou-se uma ferramenta auxiliar muito importante em conjunto com o *Zabbix* e as VLANs pois, no momento em que se detectar um fluxo elevado na rede (por meio do gráfico da interface eth 2 gerado pelo *zabbix*), pode-se filtrar a VLAN que

esteja gerando um fluxo excedente e, por meio do SARG, verificar os *hosts* e saber se essa demanda é de *internet* e se o conteúdo acessado está nas normas da política de segurança. Cabe lembrar que a atual política de segurança está disposta pelas normas do Departamento de Informática, estando em uma fase de aprimoramento, em conjunto com as novas normas que Administração Municipal pretende implementar.

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		192.168.1.212	10.74K	260.96M	45.95%	4.37%	95.63%	24:56:37	89,797,920	24.30%
2		192.168.1.31	1.37K	77.24M	13.60%	1.60%	98.40%	04:08:34	14,914,767	4.04%
3		10.0.4.24	460	46.34M	8.16%	6.81%	93.19%	09:23:25	33,805,081	9.15%
4		192.168.1.207	327	36.51M	6.43%	1.03%	98.97%	02:29:02	8,942,673	2.42%
5		10.0.4.30	3.37K	32.32M	5.69%	14.28%	85.72%	13:38:02	49,082,127	13.28%
6		10.10.11.12	794	26.37M	4.64%	32.44%	67.56%	07:50:44	28,244,682	7.64%
7		10.10.7.14	1.00K	24.84M	4.38%	7.80%	92.20%	13:48:06	49,686,450	13.45%
8		10.0.4.12	1.44K	19.09M	3.36%	6.98%	93.02%	05:10:09	18,609,432	5.04%
9		192.168.1.131	1.82K	15.16M	2.67%	18.32%	81.68%	00:56:04	3,364,425	0.91%
10		10.0.3.24	680	9.77M	1.72%	1.00%	99.00%	10:13:31	36,811,768	9.96%
11		10.0.0.14	303	8.52M	1.50%	4.81%	95.19%	06:19:53	22,793,238	6.17%
12		192.168.1.222	517	7.41M	1.31%	13.06%	86.94%	00:31:31	1,891,856	0.51%
13		192.168.1.187	252	2.39M	0.42%	25.91%	74.09%	02:53:56	10,436,470	2.82%
14		10.0.1.18	809	402.35K	0.07%	92.59%	7.41%	00:02:34	154,176	0.04%
15		192.168.1.46	54	299.74K	0.05%	59.47%	40.53%	00:08:07	487,632	0.13%
16		115.230.124.174	16	64.28K	0.01%	100.00%	0.00%	00:00:00	24	0.00%
17		192.168.1.8	24	60.24K	0.01%	50.50%	49.50%	00:03:37	217,586	0.06%
18		192.168.1.129	10	43.08K	0.01%	41.92%	58.08%	00:03:25	205,426	0.06%
19		192.168.1.74	20	30.06K	0.01%	26.53%	73.47%	00:01:36	96,614	0.03%
20		115.231.222.14	4	16.06K	0.00%	100.00%	0.00%	00:00:00	5	0.00%
21		104.148.44.191	4	15.00K	0.00%	100.00%	0.00%	00:00:00	4	0.00%
22		185.25.151.159	1	4.04K	0.00%	100.00%	0.00%	00:00:00	0	0.00%
23		185.49.14.190	1	4.04K	0.00%	100.00%	0.00%	00:00:00	0	0.00%
24		61.160.213.110	1	3.91K	0.00%	100.00%	0.00%	00:00:00	1	0.00%
25		111.248.103.32	1	3.62K	0.00%	100.00%	0.00%	00:00:00	0	0.00%
26		36.231.254.21	1	3.62K	0.00%	100.00%	0.00%	00:00:00	0	0.00%
		TOTAL	24.05K	567.94M		6.73%	93.27%	102:39:02	369,542,357	
		AVERAGE	925	21.84M				03:56:53	14,213,167	

Figura 16: SARG - Relatório geral de acesso à Internet Fonte: Dos Autores, 2015

Após as mudanças implementadas na rede de computadores da Prefeitura Municipal, elaborou-se um novo mapa da topologia de rede para que se pudesse entender de melhor forma como a rede iria se comportar daquele momento em diante, além de visualizar de maneira mais ampla de como ficou sua reestruturação, possibilitando identificar os pontos positivos e os que ainda precisam ser melhorados, visando planejar cada vez mais questões como gerenciamento, desempenho e segurança. A Figura 17 demonstra de maneira geral e ampla as mudanças estabelecidas pela implantação das melhorias na rede de computadores.

Visualizando-se a Figura 17, na cor roxa pode-se observar que está sendo representado o *switch Dell PowerConnect 2848* e as VLANs simbolizadas nele com

suas referentes portas, cujas informações estão descritas no Quadro 4. Na cor cinza a representação dos 3 servidores físicos, na cor vermelha os *firewalls*, na cor azul os *links* de Internet (um sendo o provedor de Internet principal – *Mksnet* - e o outro *link* da empresa Oi telefônica, sendo um *link* complementar de Internet) e, nas cores amarelas, os serviços operando no servidor *Dell PowerEdge R620.*

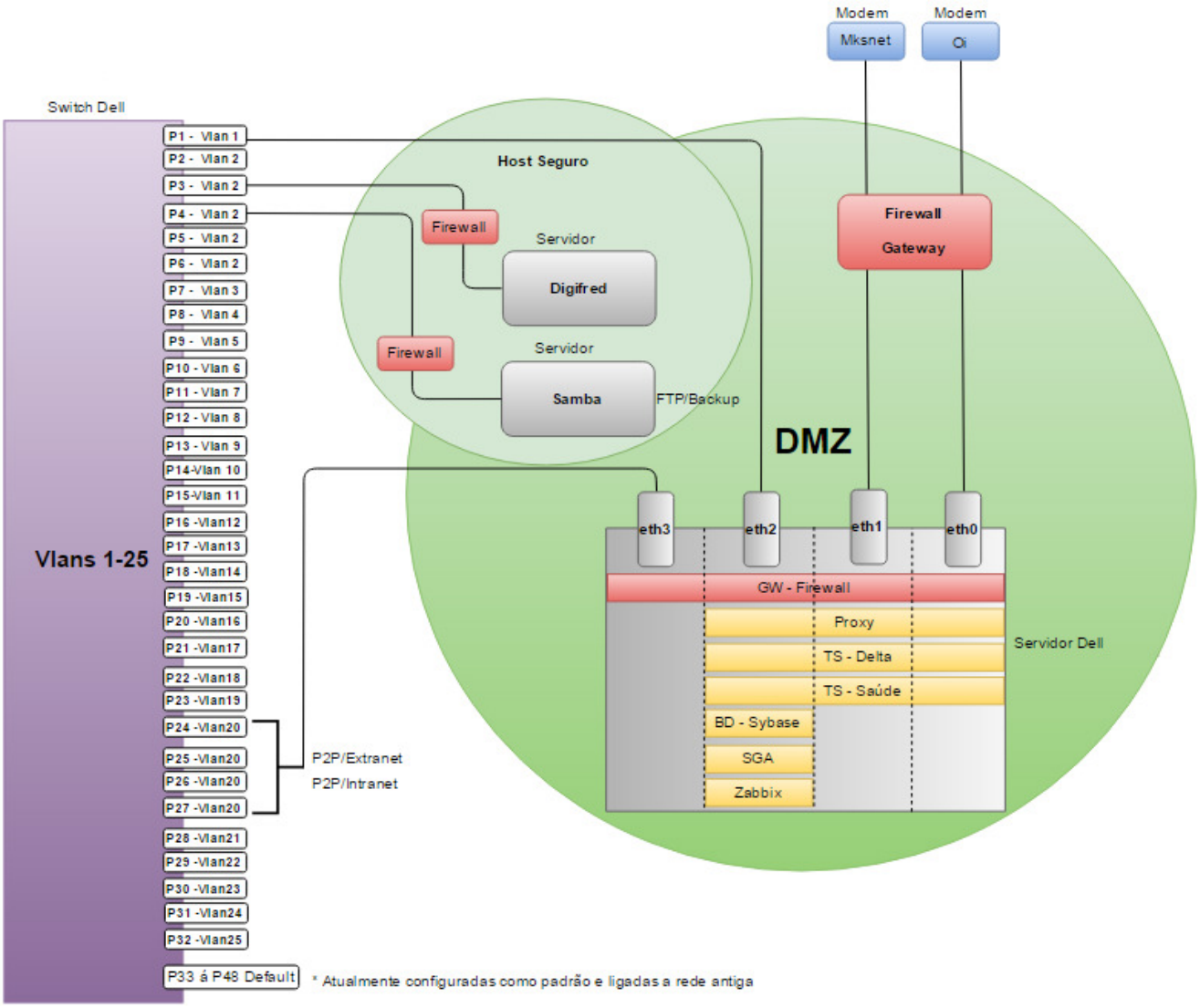


Figura 17: Rede da Prefeitura após as mudanças realizadas Fonte: Dos Autores, 2015

Analisando a Figura 17, verifica-se que os 3 servidores ficaram abrangidos pela DMZ, sendo um *HP – ProLiant ML150 HP (Digifred)* e um *HP ProLiant ML150G6* (Samba) com os serviços de FTP e *Backup* eles estão alocados em um *host* seguro Ambos estão ligados nas suas portas da VLAN 2. O terceiro servidor *Dell PowerEdge R620* possui os principais serviços da Prefeitura Municipal e suas 4 interfaces de rede. As interfaces de rede eth0 e eth1 estão ligadas aos seus dois provedores de Internet (*Mksnet* e Oi) e, entre essa ligação, está um *firewall* que tem o papel de bloquear e liberar o tráfego conforme as suas configurações. O servidor *Dell PowerEdge R620* possui a interface de rede eth2 (rede interna) que está ligada na porta 1 do *switch Dell PowerConnect 2848,* que corresponde à VLAN 1 (padrão) e que está truncada a todas as

demais portas do *switch* e assim em suas respectivas VLANs. Assim, a VLAN que desejar acessar os serviços do servidor *Dell* irá fazer sua conexão por meio do truncamento da porta 1 do *switch* VLAN 1. Outro ponto a ser observado é que, para as VLANs configuradas no *switch* acessarem os serviços alocados no servidor *Dell,* precisarão passar por outro *firewall* configurado para proteger esses serviços. As regras desse *firewall* têm o papel de liberar ou não estes acessos.

Ainda observando o servidor *Dell PowerEdge R620* e os seus serviços (*Proxy*, TS-Delta, TS-Saúde, BD – *Sybase*, SGA, *Zabbix*), pode-se notar que a imagem mostra o compartilhamento de acessos deles entre as interfaces de rede como, por exemplo, BD – *Sybase*, que está disponível para acesso apenas pela interface de rede eth2, e o TS – Delta, disponível pelas interfaces de rede eth0, eth1 e eth2.

Tendo-se em vista a próxima licitação, que irá ocorrer no início do ano de 2016, o próximo provedor de *Internet* deverá fornecer conexões de unidades de saúde (postos de saúde, secretarias) ligados à rede da prefeitura via *bridge*. Estabeleceu-se a VLAN P2P, configuradas nas portas 24, 25, 26 e 27 do *switch* para fazer essa conexão externa que terá o papel de Intranet e Extranet deixando, assim, a interface de rede eth3 do servidor *Dell PowerEdge R620* para realizar a disponibilização dos serviços que se fizerem necessários para a VLAN P2P.

6. Considerações Finais

Durante a realização deste trabalho, foi possível fazer um diagnóstico de como se encontrava a rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS, bem como a demanda de serviços que necessitam da mesma. Além disso, foi possível identificar situações relacionadas à segurança e gerenciamento das informações que circulam pela rede.

Nota-se que é necessário compreender muito bem o funcionamento da organização, para que seja possível obter informações sobre a rotina de trabalho e como os diferentes setores gerenciam as informações. Isso acaba se tornando uma tarefa complexa, pois existem muitas demandas e prioridades para poder ocorrer um fluxo desejável de trabalho entre os departamentos e funcionários da Prefeitura.

A partir das informações coletadas, pôde-se visualizar um ambiente muito mais "claro" para a configuração e definição das VLANs e DMZ e, com isso, atingir as expectativas de gerenciamento e segurança da rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS. O Anexo 1 apresenta a autorização do setor responsável pela rede de computadores, para que o estudo de caso possa ser realizado na Prefeitura de Palmeira das Missões – RS.

Apesar de não ter sido possível configurar todas as VLANs até o término deste trabalho, pôde-se constatar que foi implantado o ambiente de gerência e segurança e a finalização dessas configurações depende apenas de fatores como tempo, pessoal, além de uma pequena disponibilização financeira por parte da administração pública para a aquisição de materiais, tais como cabos de rede, *switches* e *hubs*, tendo-se em vista que as VLANs foram configuradas por associação estática e demandam a aquisição de equipamentos. Por outro lado, isto representa maior segurança.

Considerando a complexidade da implantação de um ambiente de segurança de redes, deve-se levar em consideração fatores tais como estar ocorrendo, em paralelo a este trabalho, uma implantação de sistemas de gestão pública da empresa Delta que envolvia todo pessoal do Departamento de Informática já que seus softwares são distribuídos e dependiam de suporte do setor de Informática para sua implantação. Além disso, existem as demandas cotidianas que o Departamento de Informática tem, tais como as atividades de suporte e o trabalho em conjunto com os demais setores para uma agilidade maior nos serviços.

Houve pontos um pouco mais complicados para que fosse possível configurar as VLANs, pois alguns setores, tais como os de Arrecadação e Departamento Pessoal (RH), não podiam ficar com os seus serviços que necessitam da rede parados.

A principal contribuição deste estudo de caso foi a implementação de um ambiente de segurança e gerência na rede de computadores da Prefeitura de Palmeira das Missões, principalmente com as características de um órgão público, pois mesmo que de forma indireta pretende-se que melhore de alguma forma os serviços que a Prefeitura Municipal presta aos cidadãos, levando-se em consideração os serviços que dependem da área de informática.

Como trabalhos futuros ainda existem pontos a serem melhorados na rede de computadores da Prefeitura, tais como:

- Uma reconfiguração das VLANs, para que os *hosts* sejam associados e monitorados por endereço MAC (*Media Access Control*), sendo possível, assim, fazer uma configuração DHCP (*Dynamic Host Configuration Protocol*) na rede;
- Configuração de triggers conforme o fluxo para a aferição de rede;
- Definição de uma nova Topologia da Rede de Computadores, para que os órgãos externos da Administração Municipal sejam ligados à rede principal (*backbone*) da Prefeitura.

6. Referências

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>. Acesso em 16 de abril de 2015.

ADONIS, R. (2015) Vídeo aula - Zabbix - Instalação no Linux Ubuntu. Disponível em: < https://www.youtube.com/watch?v=UZMbwsbaLds >. Acesso em:17 de Agosto de 2015.

CARVALHO, I. R. F. (2011) **Segurança da Informação:** Um Instrumento para Avaliação do Plano de Continuidade do Negócio Aplicado em Uma Organização Pública**.** Disponível em: <http://www.bsi.ufla.br/wp-content/uploads/2013/07/ItaloRFCarvalho.pdf>. Acesso em 19 de abril de 2015.

CERT.br. (2015) **Centro de Estudos, Respostas e Tratamentos de Incidentes de Segurança do Brasil.** Disponível em: <http://www.cert.br/docs/seg-adm-redes/seg-adm-redes.html#subsec2.1.> Acesso em 20 de março de 2015.

CISCO. (2015) **Packet Tracer**. Disponível em: < http://tools.cisco.com/search/results/en/us/get#q=packet+tracer&pr=enushomesppublished&basepr=enushomesppublished&prevq=&sort=cdcdevfour&start=0&hits=10&qid=1&websessionid=nsPL0pxh6wvBPV6VG6AyMp&navexp=&navlist=&navsel=&navop=&to=0&fr=7&un=true&aus=false&ec=0&pf=& > Acesso em 12 de Junho de 2015.

CHAPMAN, B.; ZWICKY, E. D. (1995) **Building Internet Firewalls**. O'Reilly Media.

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

DALLABONA, N. S. (2013) **Segurança da Informação: Uma Proposta para Projeto de Rede Baseada em Software Livre.** Universidade Tecnológica Federal do Paraná, Especialização Semipresencial em Configuração e Gerenciamento de Servidores e Equipamentos de Redes. Curitiba/PR. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2416/1/CT_GESER_IV_2014_07.pdf>. Acesso em: 20 de Maio de 2015.

GARFINKEL, S.; SPAFFORD, G. (1996) **Practical UNIX and Internet Security.** 2nd Edition. O'Reilly Media.

GIL, A. P. (2015) **OpenLDAP Ultimate**. Edição Digital: Buqui.

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

KUROSE, J. F.; ROSS, K. (2006) **Redes de computadores e a internet: uma abordagem top-down**. 3. ed. São Paulo: Addison Wesley.

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

PINHEIRO, J. M. S. (2004) **Projeto de Redes – Redes de Perímetro.** Disponível em: <http://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php>. Acesso em 18 de Abril de 2015.

PINHEIRO, J. M. S. (2005) **Projeto de Redes – Programas de Segurança para Redes Corporativas.** Disponível em**: <**http://www.projetoderedes.com.br/artigos/artigo_programas_de_seguranca_para_redes_corporativas.php**>**. Acesso em 16 de Abril de 2015.

SANTOS, R. E. (2010) **VLAN: Estudo, Teste e Análise desta Tecnologia**. Disponível em: <http://wiki.sj.ifsc.edu.br/wiki/images/3/37/ProjetoFinal_RicardoEleuterio.pdf>. Acesso em 16 de abril de 2015.

SCHULTZ, K. C. (2013) **Implementação e Análise de uma Estrutura de Rede, Contemplando o Gerenciamento, Qualidade de Serviços e Segurança.** Universidade Tecnológica Federal do Paraná, Departamento Acadêmico de Informática, Curso de Bacharelado em Sistemas de Informação, Curitiba/PR. Disponível em: <http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/2031/1/CT_COBSI_2013_1_04.pdf>. Acesso em 20 de Maio de 2015.

SQUID. (2015). **Squid: Optimização de entrega Web.** Disponível em: < http://www.squid-cache.org/ >. Acesso em: 20 de Novembro de 2015.

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

TEIXEIRA, G. S. O; MOREIRA, J. (2014) **Reestruturação de Rede para melhoria do Tráfego e Segurança: a Reestruturação da Rede de Computadores do DC.** Revista Tis – Tecnologias, Infraestrutura e Software, 2014. Ufscar – Universidade Federal de São Carlos. Disponível em: <http://revistatis.dc.ufscar.br/index.php/revista/article/view/71/65>. Acesso em: 20 de Maio de 2015.

UBUNTU-BR.ORG. (2015) **Ubuntu.** Disponível em: <http://ubuntu-br.org/ubuntu>. Acesso em 12 de junho de 2015.

WAGNER, D. E. (2012) **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 >. Acesso em: 20 de Maio de 2015.

ZABBIX. (2015). **The Enterprise-class Monitoring Solution for Everyone.** Disponível em: <http://www.zabbix.com/download.php>. Acesso em: 12 de Junho de 2015.

ANEXO 1

AUTORIZAÇÃO

Autorizo o acadêmico Denison Molina, do Curso de Bacharelado em Sistemas de Informação da UFSM/Frederico Westphalen, a realizar o trabalho "**Implantação de Um Ambiente de Segurança de Redes de Computadores: Um Estudo de Caso na Prefeitura Municipal de Palmeira das Missões – RS**" com base nas informações e infraestrutura disponibilizadas pelo Departamento de Informática da Prefeitura de Palmeira das Missões – RS.

Palmeira das Missões, 23 de novembro de 2015.

Chefe do Departamento de Informática

Analista de Sistemas

Fernando Beux dos Santos
Analista de Sistema
Portaria n.º 442/2012

Fernando Beux dos Santos