Um Estudo de Caso sobre a Implantação de um Ambiente de Segurança de Redes de Computadores

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) – Campus Frederico Westphalen – RS – Brasil
[3]Departamento de Informática – Prefeitura Municipal de Palmeira das Missões - RS

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 definido 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. A principal contribuição deste estudo de caso foi a implementação de um ambiente de segurança e gerência na rede de computadores da referida Prefeitura.*

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) defined 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. The main contribution of this case study was the implementation of a security and management in the computer network at the City Hasll in Palmeira das Missões – RS.*

Keywords*: Vlans. DMZ. Information Security.*

1. Introdução

A questão da segurança em redes de computadores tem se tornado cada vez mais importante, principalmente devido ao fato de que a Internet tornou-se um ambiente hostil. Neste contexto, 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 necessária 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 (tais como invasão de privacidade e inconsistência de dados); entre outras informações. Sendo assim, 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 relacionados 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; 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; 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, 2018).

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:* refere-se à proteção contra mudança: os dados que chegam em um receptor são exatamente os mesmos que foram enviados?
- *Disponibilidade de dados:* refere-se à proteção contra a interrupção do serviço: os dados permanecem acessíveis para uso legítimo?
- *Confiabilidade dos dados:* refere-se à proteção contra acesso não autorizado a dados: os dados estão protegidos contra acesso sem autorização?
- *Privacidade:* 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 a atenção ou prejudicar alguém (TANEMBAUM; WETHERALL, 2011).

A sociedade precisa de mais profissionais de computação treinados na área de Segurança da Informação, que possam defender e evitar, com sucesso, ataques contra computadores, bem como usuários treinados nessa mesma área, 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; TAMASSIA, 2013).

2.3 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).

2.4 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: 1) a interna, só acessada pelo usuário da rede interna e 2) a DMZ externa, acessada por qualquer usuário da *Internet*. Este conceito, aliado ao conceito 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 protegidos contra ataques da *Internet* por um *firewall*. 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).

3. Trabalhos Relacionados

O trabalho apresentado por Wagner (2012), partiu da necessidade de aumentar a segurança, privacidade e melhorar o desempenho da rede de computadores do CITEC (Centro de Inovação Tecnológica) da UTFPR (Universidade Tecnológica Federal do Paraná), tendo como proposta utilizar a segmentação por meio 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 acessos externos às 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 deve ter acesso, essa segmentação também diminuiu o domínio de *broadcast,* 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 por meio 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 a referida arquitetura 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 endereçamento IP (*Internet Protocol*) para cada interface. Como o sistema reconhece as VLANs como interfaces de rede, dever ser informado ao serviço de DHCP (*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.

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, houve um aumento na 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, além de existirem 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.

A solução para o problema dos servidores estarem juntos com as estações de trabalho foi a de 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, necessária 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, tais como um *site* autenticando no servidor de LDAP (*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 (*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*.

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 pudessem 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 (*Quality of Service*) e gerenciamento. A rede como um todo foi dividida em sub-redes lógicas, as VLANs, para diminuir os problemas de tempestades de *broadcast*.

4. Solução Implementada

Este trabalho teve sua proposta alicerçada na base estrutural do parque computacional da rede de computadores da Prefeitura Municipal de Palmeira das Missões - RS, com o apoio do Departamento de Informática da Prefeitura, visando criar uma reestruturação, visando à melhoria do desempenho da transmissão de dados e fornecendo um ambiente seguro para os seus usuários.

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, definida pelo Departamento de Informática da referida Prefeitura. 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.

A metodologia de pesquisa utilizada para o desenvolvimento deste trabalho foi a Dissertação-Projeto, pois implementou-se uma reestruturação da rede de computadores na Prefeitura já referida. Segundo Ribeiro e Zabadal (2010), nesta metodologia o pesquisador caracteriza um determinado problema e desenvolve, então, um programa, um protótipo ou uma estrutura envolvendo *hardware* e *software*, como prova de conceito para a solução desse problema. Neste sentido, a prova de conceito envolve a definição das VLANs e da DMZ.

4.1 Diagnóstico da Rede de Computadores

No início da implementação deste trabalho, 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 que atendia a prefeitura anteriormente[1] com banco de dados *Firebird* e 3) um *Dell PowerEdge R620 Xen Server* no qual estavam 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;
- *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. Este servidor é destinado, unicamente, para a 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

[1] 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 empresa anterior.

acessos com autenticação e, também, por acessos públicos para diretórios comuns entre departamentos;

- *Windows Server* 2008 R2 – Sistemas de Gestão Pública da empresa Delta.[2] Como os aplicativos da Delta funcionam na plataforma *Windows,* este servidor executa todos os processos de departamentos que têm máquinas com Sistema Operacional *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, 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.

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.* Os serviços de rede executados nos servidores envolviam um *firewall* e um *proxy*, 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 necessitavam 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 trafegavam 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, tais 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 que atendia anteriormente a Prefeitura. 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,

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

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 os usuários usando as funcionalidades "internas" do sistema, o mesmo possui uma aplicação externa chamada Cidadão *web*, disponibilizada no *site* da Prefeitura. 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[3] disponibilizada pela empresa *Delta,* onde são armazenados modelos de guias, alvarás, entre outros. 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 a 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 Departamento de 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.

[3] 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, 2018).

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. O *Zabbix* trata-se de uma ferramenta de monitoramento de redes, servidores e serviços, desenvolvida 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. O sistema permite ainda que ações automáticas como, por exemplo, *restart* de serviços sejam executados a partir de eventos. A ferramenta *Zabbix* é bastante completa, pois já possui diversas funcionalidades sem a necessidade de instalação de *plug-ins*, o que facilita e diminui o tempo de configuração da ferramenta. Além disso, é uma ferramenta gratuita, com constantes atualizações e de aperfeiçoamento para cada pessoa ou empresa, dependendo do grau de suas complexidades e necessidades diárias. Os principais módulos são (ZABBIX, 2018):

- ***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;
- ***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.

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 os processos de ensino e de aprendizagem de diversos conceitos complexos de tecnologias de redes e telecomunicações (CISCO, 2018).

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 em outra sub-rede, sem a devida autorização.

Para a configuração da DMZ foram utilizados os 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*[4] 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 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 o SGBD (Sistema Gerenciador de Bancos de Dados) *MySQL* e o ambiente para programação em PHP (ADONIS, 2018).

Com o serviço do *Zabbix* configurado de forma personalizada, dentro das expectativas de gerenciamento definidas pelo Departamento de Informática da Prefeitura, onde a proposta se encaixa em monitorar o tráfego dos nodos centralizadores, o próximo passo envolveu a instalação e configuração dos agentes *Zabbix*[5] nos

[4] *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,2018].

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

computadores da rede, 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 1 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.

Na Figura 1 pode-se observar a primeira área que foi analisada (detalhada no gráfico da Figura 2), 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 2 representa a análise de um fluxo de rede para a interface *eth1* com bases nas entradas e saídas ocorridas no dia 24 de setembro.

Como é possível visualizar no gráfico apresentado na Figura 2, 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. 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*.

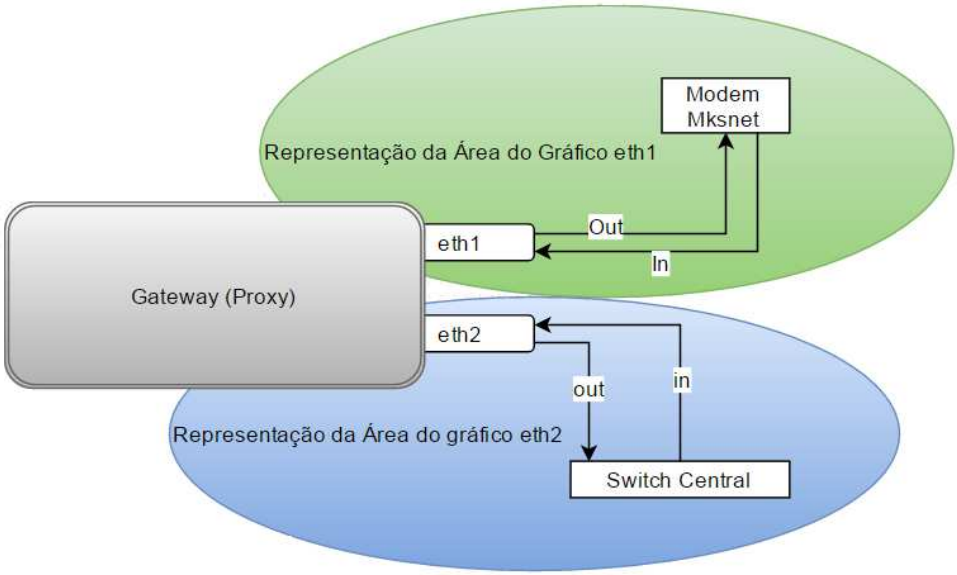

Figura 1. Representação da área em que foi realizada a medida dos gráficos eth1 e eth2
Fonte: os autores (2018)

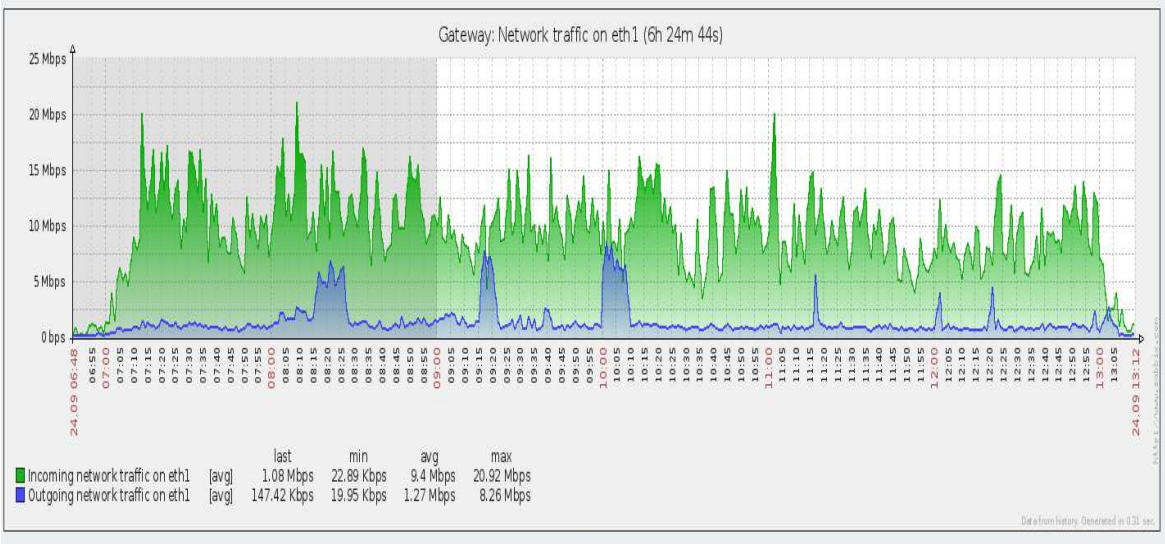

Figura 2. Porta eth1 – Fluxo de Tráfego de Internet da Rede de Computadores

Fonte: os autores (2018)

Já o gráfico apresentado na Figura 3 mostra o tráfego do *gateway* correspondente à conexão com a rede interna no dia 24 de setembro, em um período de aproximadamente 6 horas.

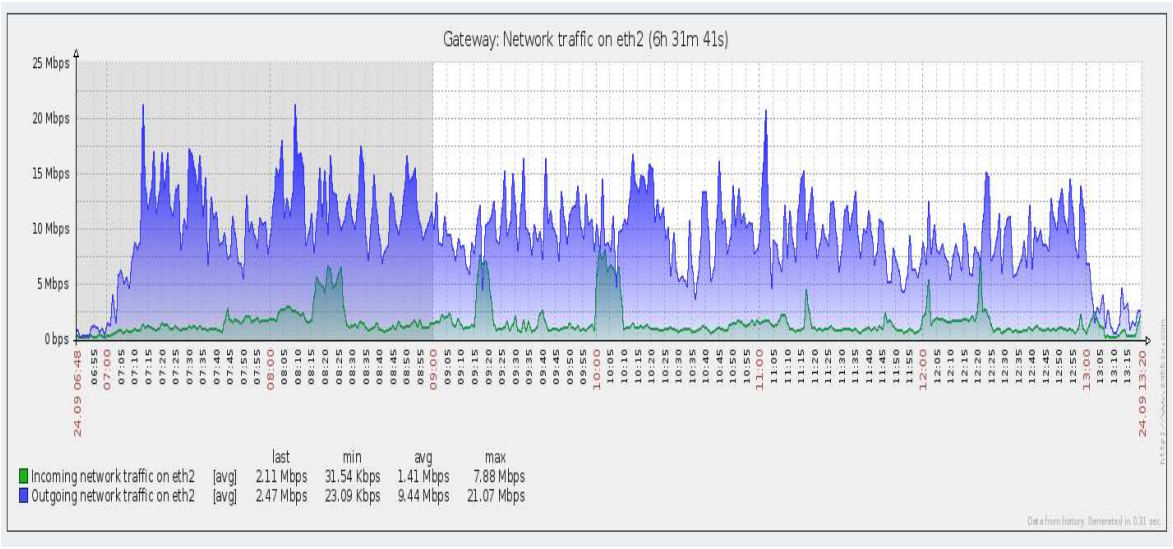

Figura 3. Porta eth2 - Fluxo de Rede interno para a navegação na Internet

Fonte: os autores (2018)

O gráfico apresentado na Figura 3 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 desenvolvida 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 4 apresenta uma simulação com três departamentos existentes na Prefeitura Municipal, que são o Protocolo, CPD (Centro de Processamento de Dados – Departamento de Informática) e a Secretaria de Educação.

Conforme mostra a Figura 4, foram simuladas 3 VLANs em menor escala (com um número menor computadores). Nessa simulação utilizou-se um *switch* de 24 portas e foram 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 as 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.

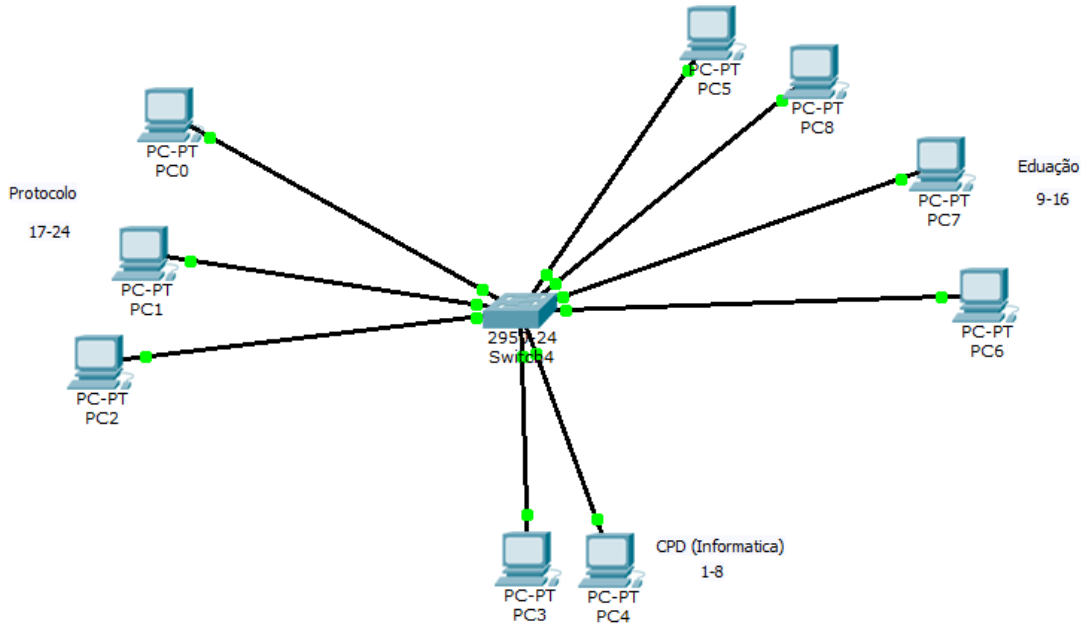

Figura 4. Representação da Simulação de VLANs

Fonte: os autores (2018)

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 nova estrutura da rede, já que existe um número considerável de departamentos atuando no prédio da Prefeitura Municipal (aproximadamente 20 departamentos).

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 às 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 1 apresenta as configurações e os dados usados nas VLANs.

Quadro 1. Quadro com o planejamento das 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

Fonte: os autores (2018)

5. Resultados e Comparações

As VLANs foram configuradas na interface de rede *eth2*, que corresponde ao fluxo de rede interno da Prefeitura, sendo possível, assim, gerenciar e monitorar a rede por partes com as 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.

O SARG tornou-se uma ferramenta auxiliar muito importante em conjunto com o *Zabbix* e as VLANs pois, no momento em que se detecta 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 estabelecida pelo Departamento de Informática. 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 a Administração Municipal pretende implementar.

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 5 demonstra, de maneira geral, as mudanças estabelecidas pela implantação das melhorias na rede de computadores da Prefeitura.

Visualizando-se a Figura 5, 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 1. 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 – serviço contratado pela Prefeitura da empresa *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.*

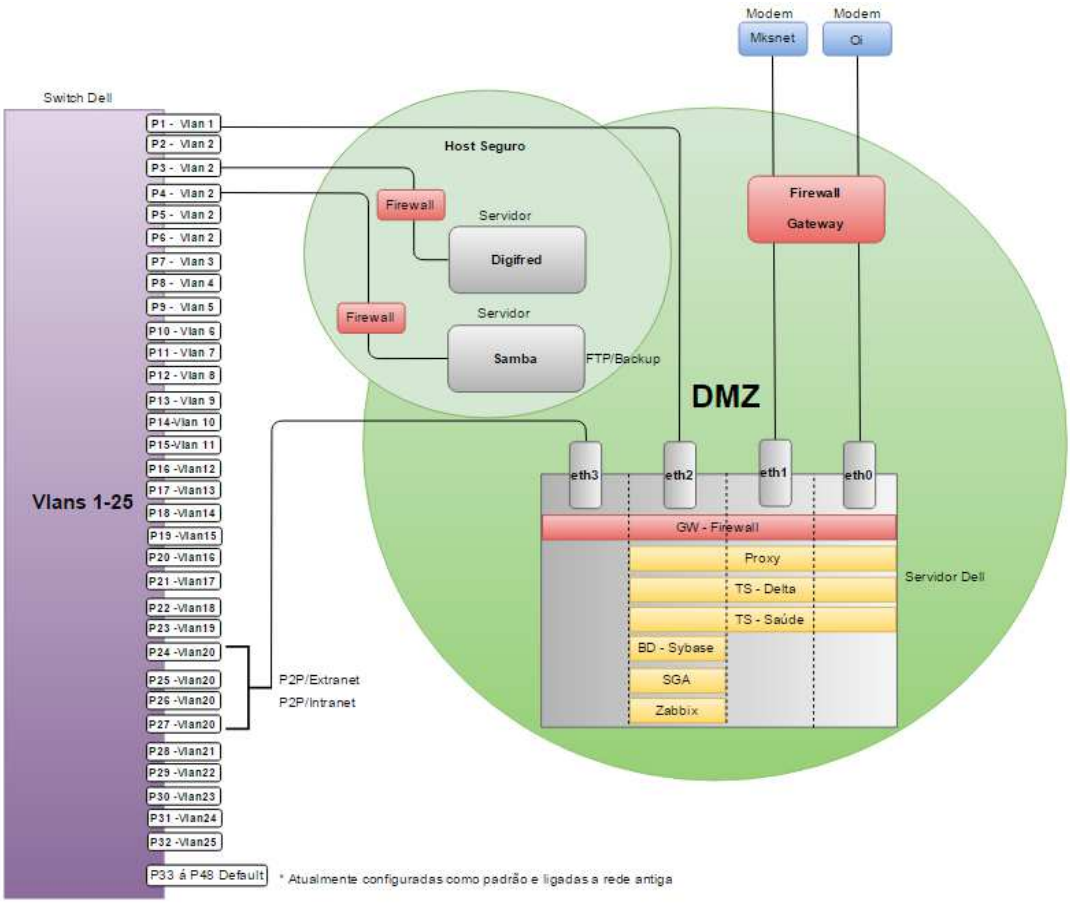

Figura 5. Rede da Prefeitura após as mudanças realizadas

Fonte: os autores (2018)

Analisando a Figura 5, verifica-se que os 3 servidores ficaram abrangidos pela DMZ, sendo um *HP – ProLiant ML150 HP* e um *HP ProLiant ML150G6* (Samba) com os serviços de FTP (*File Transfer Protocol*) e *Backup*. Eles estão alocados em um *host* seguro e 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 Figura 5 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 uma próxima licitação, que ainda irá ocorrer, o próximo provedor de *Internet* deverá fornecer conexões às unidades de saúde (postos de saúde, secretarias), ligadas à rede da Prefeitura via *bridge*. Estabeleceu-se a VLAN P2P, configurada 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 realizar um diagnóstico de como se encontrava a rede de computadores da Prefeitura Municipal de Palmeira das Missões – RS, bem como a demanda de serviços desta rede. 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.

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 Departamento 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.

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.

Referências

ADONIS, R. (2018) Vídeo aula - **Zabbix** - Instalação no Linux Ubuntu. Disponível em: < https://www.youtube.com/watch?v=UZMbwsbaLds >. Acesso em:17 de Agosto de 2018.

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 2018.

CERT.br. (2018) **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 2018.

CISCO. (2018) **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 2018.

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

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

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

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 2018.

RIBEIRO, V. G.; ZABADAL, J. (2010). **Pesquisa em Computação.** Porto Alegre: UniRitter.

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 2018.

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 2018.

SQUID. (2018). **Squid: Optimização de entrega Web.** Disponível em: <http://www.squid-cache.org/ >. Acesso em: 20 de Novembro de 2018.

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 2018.

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 2018.

ZABBIX. (2018). **The Enterprise-class Monitoring Solution for Everyone.** Disponível em: <http://www.zabbix.com/download.php>. Acesso em: 12 de Junho de 2018.