Faculdade de Tecnologia de Americana

Curso Superior de Segurança da Informação

GERÊNCIA DE REDES COM SQUID

Jean Eriksen Pinto Arruda Correa de Toledo

tordekk@gmail.com

Americana, SP

2016

Faculdade de Tecnologia de Americana

Curso Superior de Segurança da Informação

GERÊNCIA DE REDES COM SQUID

Jean Eriksen Pinto Arruda Correa de Toledo

tordekk@gmail.com

Trabalho monográfico, desenvolvido em cumprimento à exigência curricular do curso Superior de Tecnologia em Segurança da Informação da Fatec Americana, sob orientação do prof. Me. Clerivaldo Jose Roccia.

Área: Segurança da Informação

Americana, SP

2016

FICHA CATALOGRÁFICA – Biblioteca Fatec Americana - CEETEPS
Dados Internacionais de Catalogação-na-fonte

T582g

Toledo, Jean Eriksen Pinto Arruda Correa de
Gerência de redes com Squid. /. Jean Eriksen Pinto Arruda Correa de Toledo. – Americana: 2016.
54f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.
Orientador: Prof. Me. Clerivaldo José Roccia

1. Rede de computadores I. Roccia, Clerivaldo José II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.519

Jean Eriksen Pinto Arruda Correa de Toledo

Gerência de Redes com Squid

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação, pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 23 de junho de 2016.

Banca Examinadora:

Clerivaldo José Roccia (Presidente)
Mestre
Fatec Americana

José Luis Zem (Membro)
Doutor
Fatec Americana

Alberto Martins Júnior (Membro)
Mestre
Fatec Americana

RESUMO

Este trabalho apresenta o estudo e a aplicação de ferramentas de gerenciamento de rede para otimização de uso de link de internet. Através de um estudo de caso real, realizado no **Centro de Detenção Provisória "AEVP Renato Gonçalves Rodrigues" de Americana**, foi feito um levantamento das funcionalidades da rede sobre o uso do link de Internet, utilizando a ferramenta de análise de desempenho Zabbix. Com base nos resultados da analise através de métricas de monitoramento tais como perda de pacotes, largura de banda e tempo de resposta, foi possível determinar as condições de funcionamento da rede. Na sequência, foi aplicada através da ferramenta de controle de uso de link de Internet, Proxy, regras de acesso que permitiram controlar a utilização da banda disponível de maneira racional. Os resultados desse trabalho proporcionaram uma melhora significativa na rede.

Palavras-chave: gerenciamento de redes, Proxy, Squid, Zabbix

ABSTRACT

This paper presents the study and application of network management tools for Internet link usage optimization. Through a real case study in **Centro de Detenção Provisória "AEVP Renato Gonçalves Rodrigues" de Americana**, *a survey was done of the network features on the use of the Internet link, using Zabbix performance analysis tool. Based on the results of the analysis by tracking metrics such as packet loss, bandwidth and response time, it was possible to determine the network operating conditions. In sequence, was applied via the Internet link usage tracking tool, Proxy, access rules that allowed control the use of the available bandwidth in a rational way. The results of this work have provided a significant improvement in network.*

Keywords: Network management, Proxy, Squid, Zabbix

AGRADECIMENTOS

Primeiramente a Deus, pela saúde, determinação e sabedoria a mim confiada.

À minha esposa Tatiane pela força, paciência e compreensão nos dias em que concentrei toda minha atenção neste trabalho, principalmente próximo à entrega, não podendo demonstrar o quanto ela é especial para mim.

A minha mãe por nos apoiar, nesses longos anos, tomando conta de minha filha para que eu pudesse concluir este curso.

Aos meus colegas de classe, por sempre estarem ao meu lado desenvolvendo trabalhos acadêmicos, compartilhando seus conhecimentos e por participarem da minha fase de graduação.

Ao meu orientador, o prof. Me. Clerivaldo Jose Roccia, por dividir sua experiência e conhecimento. Embora tenha me dedicado, sem sua ajuda, paciência e fé este trabalho não obteria êxito.

A todos os professores da FATEC de Americana pela contribuição na minha formação, dando dicas, ajudando, aconselhando, indicando e conversando.

DEDICATÓRIA

À minha esposa Tatiane, por ser atenciosa, amorosa e sempre me cobrar e me ensinar a nunca desistir de buscar meus objetivos e a nossa filha Yasmin que é a alegria de nossa casa e o nosso maior tesouro.

SUMÁRIO

LISTA DE FIGURAS

1 INTRODUCAO

A utilização da Internet é cada vez mais frequente no dia-a-dia de todos, nos últimos anos a Tecnologia da Informação (TI) teve um aumento exponencial, na qual hoje necessita-se muito de seus recursos, pois ela aumenta a nossa capacidade de entregar o mesmo serviço em um tempo mais curto e com qualidade superior, porém o investimento em infraestrutura ou largura de banda não tem sido compatível com a necessidade.

O cenário analisado neste trabalho é uma Unidade Prisional (UP) que conta com aproximadamente 60 estações de trabalho, ligadas por meio de uma rede cabeada, sustentada por um link dedicado de 4Mbps utilizando tecnologia de par metálico.

Por conta da necessidade de dados mais precisos e ágeis, diversos sistemas online tornaram-se obrigatórios recentemente. Com isso os usuários começaram a utilizar mais recursos de Internet, gerando uma sobrecarga no uso do link disponível. Isso gerou muita reclamação, pois os sites não carregavam ou carregavam parcialmente ou lentamente.

Por conta do aumento da reclamação e da visível dificuldade ao acesso de páginas simples, foram abertos inúmeros chamados à operadora responsável, porém sem sucesso, pois nenhuma anormalidade fora encontrada no serviço de Internet, apontando para o fato de o problema ser interno.

1.1 PROBLEMA

É possível controlar a utilização do link de Internet disponível de maneira racional, oferecendo um serviço de qualidade?

1.2 HIPÓTESE

Utilizando as ferramentas existentes tais como Proxy Squid e Zabbix e, uma definição de políticas de acesso é possível não só monitorar a rede, como também, gerenciar seus recursos.

1.3 OBJETIVO GERAL

O objetivo geral deste trabalho é implantar o Proxy Squid e o Zabbix para monitoramento e gerenciamento da rede.

1.3.1 OBJETIVOS ESPECÍFICOS

Os objetivos específicos deste trabalho são elencados a seguir:

- Implantar o servidor Zabbix
- Implantar o servidor Proxy Squid
- Definir as políticas de acesso
- Definir as métricas de avaliação
- Gerar relatórios de monitoramento da rede
- Gerenciamento do link e recursos da rede

1.4 JUSTIFICATIVA

A implantação do Proxy na rede permitirá fazer um uso racional do link de Internet, bem como o controle dos sites acessados, promovendo segurança e desempenho. Aliado ao Proxy, o uso do Zabbix permitirá analisar o trafego gerado pela rede em tempo real possibilitando um melhor gerenciamento dos recursos disponíveis referentes à infraestrutura.

1.5 MÉTODOLOGIA

Os procedimentos metodológicos adotados são o de pesquisa dedutiva, serão usados procedimentos técnicos e documentos de melhores práticas de mercado, serão utilizados também estudos históricos, caso sejam necessários para elaboração do trabalho final. Os procedimentos de pesquisa utilizados são o de pesquisa aplicada de abordagem qualitativa/quantitativa e testes de conceito em ambiente virtual e posteriormente testes em ambiente físico. Os procedimentos técnicos serão bibliográficos e documentais e posterior análise de conteúdo.

1.6 ESTRUTURA DO TRABALHO BIBLIOGRÁFICO

Este trabalho está organizado em capítulos, sendo o capítulo 1, introdutório. O capítulo 2 aborda o Gerenciamento de Redes de Computadores. O capítulo 3

discorre sobre Proxy. Os capítulos 3 e 4 descrevem o Estudo de Caso e Discussões e Resultados. O capítulo 5 traz as considerações finais.

2 GERENCIAMENTO DE REDES

> O grau de dependência das redes de telecomunicações e da infraestrutura de tecnologia da informação aumentou: à medida que as aplicações e os serviços baseados em redes evoluem e se tornam mais complexos, mais largura de banda é necessária para manter o desempenho destes ambientes em níveis adequados. (POLETO FILHO, 2012).

Para Kurose (2010), o gerenciamento de rede inclui a disponibilização, a integração e a coordenação de elementos de hardware, software e humanos, para monitorar, testar, consultar, configurar, analisar, avaliar e controlar os recursos da rede, e de elementos, para satisfazer às exigências operacionais, de desempenho e de qualidade de serviço em tempo real a um custo razoável.

2.1 TIPOS DE GERENCIAMENTO DE REDES

Kurose (2010) cita em seu livro que a *International Organization for Standardization* (ISO) criou um modelo de gerenciamento mais estruturado, dividindo ele em cinco áreas, sendo:

2.1.1 GERENCIAMENTO DE DESEMPENHO

Kurose (2010) aborda que as metas principais são quantificar, medir, informar, analisar e controlar o desempenho dos componentes de rede, entretanto Poleto Filho (2012) adiciona que se precisa também monitorar as atividades para que se possam obter informações como: nível de utilização, perfil de tráfego, vazão, existência de gargalos, tempo de resposta, latência (atrasos), disponibilidade, perdas de pacotes, entre outros.

Complementa que é responsável por monitorar recursos da rede a fim de estabelecer níveis de desempenho, assim obtendo indicadores de desempenho na qual futuramente podem demonstrar a degradação da rede.

“Estatísticas de desempenho podem ajudar no planejamento, administração e manutenção de grandes redes.” (POLETO FILHO, 2012).

Com o devido monitoramento da rede, pode-se utilizar dos resultados da utilização da rede, para efetuar ações corretivas como, balanceamento de carga,

priorização de aplicações ou tráfego, aumento da velocidade do *link* ou a troca de um equipamento defasado.

2.1.2 GERENCIAMENTO DE FALHAS

Kurose (2010) define em seu livro que a diferença entre o gerenciamento de desempenho e o gerenciamento de falhas é que a falha deve ser tratada imediatamente já o desempenho tem um papel a longo prazo e pode ser planejado.

Poleto Filho (2012), diz em seu artigo que o gerenciamento de falhas deve detectar e reagir às falhas da rede e notificar os fatos ao gerente de rede, mas para que isso seja possível é necessário ter controle do sistema como um todo, sendo que cada componente essencial para o funcionamento seja monitorado individualmente.

Poleto Filho (2012), diz que com o monitoramento dos dispositivos pode-se determinar o componente exato onde a falha aconteceu, isolar a falha, reconfigurar ou modificar a rede para minimizar o impacto e reparar ou trocar o componente com problemas para restaurar o serviço ou a rede.

2.1.3 GERENCIAMENTO DE CONFIGURAÇÃO

Kurose (2010) descreve basicamente permite que o administrador da rede tenha conhecimento dos dispositivos fazem parte da rede e quais suas configurações de Hardware e Software.

Poleto Filho (2012), complementa que também é responsável pelo registro, manutenção, configuração dos serviços e implementação de facilidades para atualizações ou modificações dos recursos de rede, como melhorias de *Hardware* e versões de *Softwares*.

2.1.4 GERENCIAMENTO DE CONTABILIZAÇÃO

“O gerenciamento de contabilização permite que o administrador da rede especifique, registre e controle o acesso de usuários e dispositivos aos recursos da rede”. (KUROSE, 2010).

Para Poleto Filho (2012), o administrador da rede, deve estar habilitado para controlar o uso dos recursos da rede, garantindo que todos utilizem de maneira satisfatória, evitando que um ou mais usuários abuse ou faça uso ineficiente da rede, devendo acompanhar as atividades dos usuários para poder planejar o crescimento da rede.

2.1.5 GERENCIAMENTO DE SEGURANÇA

Para Kurose (2010), o gerenciamento de segurança tem uma meta, que é controlar o acesso aos recursos da rede de acordo com alguma política definida, também ressalta o uso de *firewalls* para monitorar e controlar pontos externos de acesso.

Para Poleto Filho (2012) deve impedir o uso incorreto dos recursos da rede por parte dos usuários e restringir o acesso indevido de determinados recursos, complementa que para ser eficiente deve-se ter uma política de segurança robusta e efetiva.

2.2 METODOLOGIAS DE GERENCIAMENTO

Um administrador de redes necessita de ferramentas que facilitem o seu gerenciamento e permitam que ele monitore mais facilmente seus dispositivos, para que possa manter a qualidade de seu funcionamento. Nas redes de computadores, as tarefas de gerenciamento são realizadas pelo *Simple Network Management Protocol* (SNMP).

“Qualquer dispositivo de rede que tenha a capacidade de computar, armazenar e disponibilizar informações relevantes à gerência de rede é denominado dispositivo gerenciável”. (MACEDO, 2012).

Kurose (2010), em seu livro descreve que existem três versões do protocolo, sendo que o SNMPv1 [RFC 1157[1], 1990], SNMPV2 [RFC 1442[2], RFC 1444[3], 1993] e o SNMPv3 [RFC 2574[4]].

[1] https://tools.ietf.org/html/rfc1157
[2] https://tools.ietf.org/html/rfc1442
[3] https://tools.ietf.org/html/rfc1444
[4] https://tools.ietf.org/html/rfc2574

Pinheiro (2012), em seu artigo cita que o SNMPv1 e SNMPv2 utilizam uma forma primitiva como serviço de autenticação, chamada de comunidade SNMP (*Community*), na qual cada mensagem SNMP contém a comunidade que será utilizada como parâmetro de identificação.

Por fim Kurose (2010), complementa sobre a melhoria na segurança e administração do SNMP em sua 3ª versão, "SNMPv3 pode ser imaginado como um SNMPv2 com capacidades adicionais de segurança e administração [RFC 3410]."

Segundo o CanalTech (2012), RFC é:

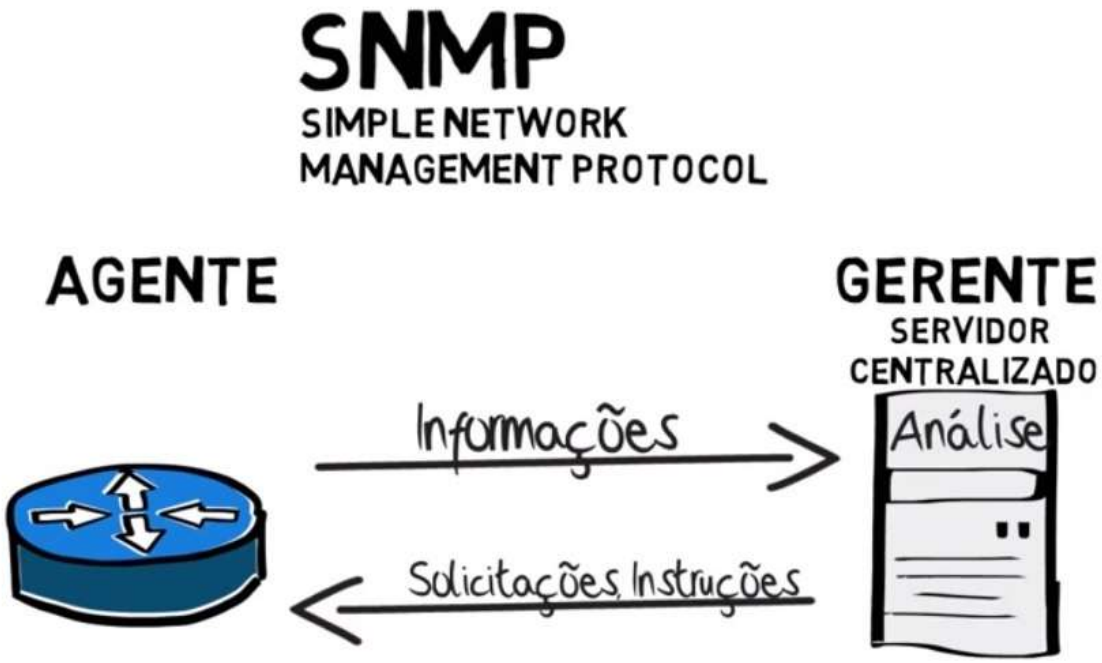
> Acrônimo de *Request for Comments* (ou "pedido para comentários" em português), as RFCs são documentos técnicos desenvolvidos e mantidos pelo IETF (Internet *Enginnering Task Force*), instituição que especifica os padrões que serão implementados e utilizados em toda a Internet. (CANALTECH, 2012).

Cada RFC deve conter o funcionamento detalhado de todos os aspectos do protocolo proposto, caso um padrão torne-se obsoleto e mudanças sejam necessárias é gerado um *Request for Chance*, para que pessoas com o conhecimento sobre o assunto possam oferecer soluções, caso seja aprovado pelo comitê ele se torna uma nova RFC, logicamente com outra numeração, a RFC antiga não é excluída, apenas será marcada como obsoleta, ficando disponível para consulta a quem quiser aprender.

Ainda em seu artigo o CanalTech (2012), comenta sobre a RFC 2826, esta RFC explica o processo de elaboração e aprovação de uma RFC, diz como o interessado pode oferecer ajuda na solução de um problema e se aprovado, será implementado na Internet com o nome do autor original.

O SNMP é o protocolo padrão para gerenciar dispositivos em redes IP (Internet *Protocol)* e sua arquitetura é baseado no conceito de agente e gerente, conforme Figura 1, normalmente o protocolo SNMP utiliza as portas UDP 161 para agente e 162 para o gerente.

Figura 1: Conceito do SNMP



Fonte: adaptado de nic.br

O gerente é o dispositivo que realiza essas coletas, solicitando e analisando as informações dos agentes, normalmente ele é um servidor centralizado, conforme exemplificado na Figura 1, que será capaz de analisar e tratar as informações coletadas e enviar para os agentes ações que devem ser executadas.

Os agentes são os dispositivos que estão sendo gerenciados e de onde são coletadas as informações que se deseja monitorar.

Poleto Filho (2012), explica em seu artigo que o processo gerente coleta informações de duas formas, sendo *polling* e *event-reporting* (ou relatório de evento), por *polling* o gerente solicita ao agente as informações, o agente por sua vez responde com os valores (*request*/*response*). O agente também pode enviar um relatório periodicamente a um gerente, sem que lhe seja solicitado, podendo a sua periodicidade ser configurada pelo gerente.

O SNMP define também uma operação que permite ao agente informar o gerente sobre a ocorrência de um evento específico, que é a função *TRAP*, esta operação é utilizada pelo agente para comunicar ao gerente do acontecimento de

um evento, além dela existem o *SET* para alterar o valor de uma variável e o *GET* para ler um valor, ambas a operações são solicitadas pelo gerente aos agentes.

Contudo o SNMP é apenas uma parte desta ferramenta de gerenciamento, ele atua em conjunto com outras duas estruturas a *Structure of Management Information* (SMI) e a *Management Information Base* (MIB).

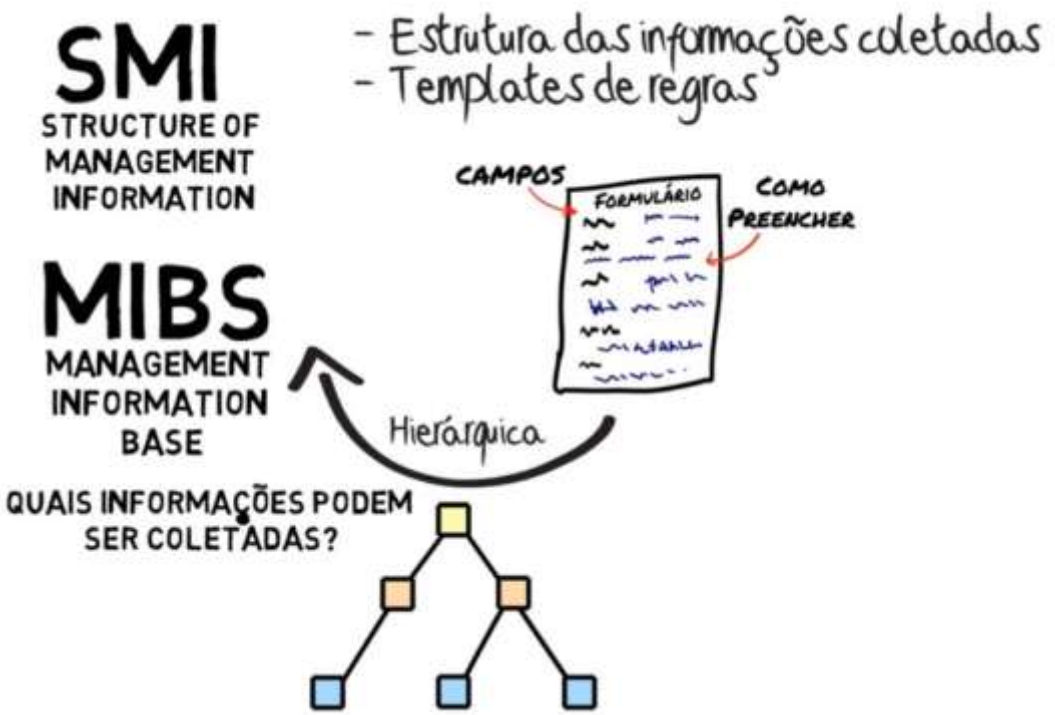
A SMI é uma diretriz do SNMP na qual define a estrutura básica das informações que serão coletadas, uma espécie de modelo, especificando as regras para a criação de nomes, tipos e a forma como as informações serão codificadas para serem enviadas ao gerente, é como uma lista com todos os campos que podem existir e como eles devem ser preenchidos, exatamente como na Figura 2.

Figura 2: SMI: Structure of Management Information

Fonte: adaptado de nic.br

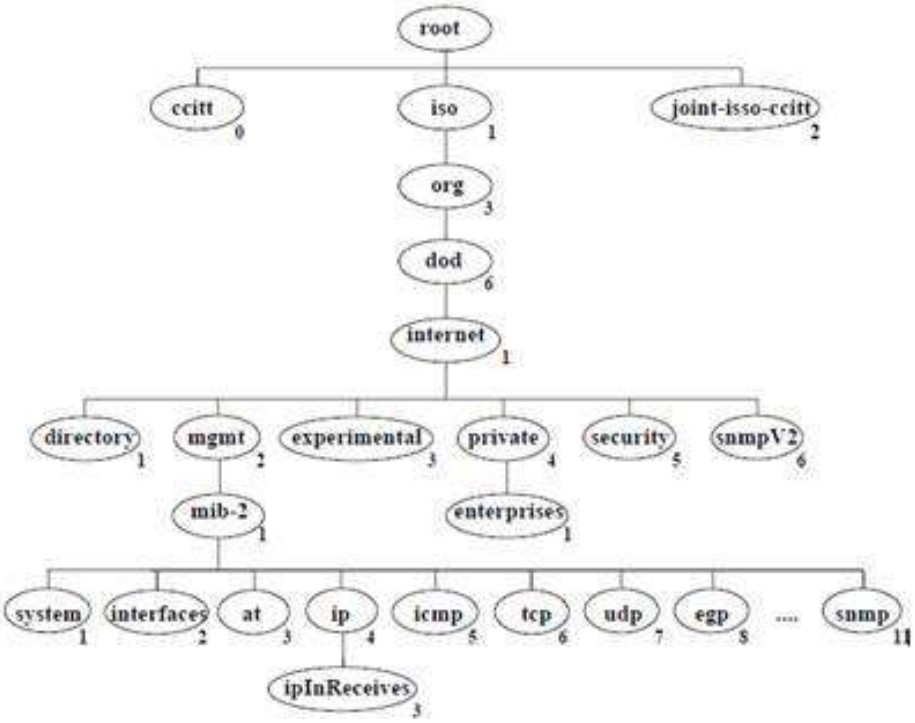
Com base nos modelos definidos na SMI é que são construídas as MIBs, como na Figura 3, elas são as que definem o conjunto de informações que vão ser coletadas pelos agentes, tendo a sua estrutura de forma hierárquica, conforme na Figura 4.

Figura 3: MIB: Management Information Base



Fonte: adaptado de nic.br

Figura 4: Hierarquia MIB

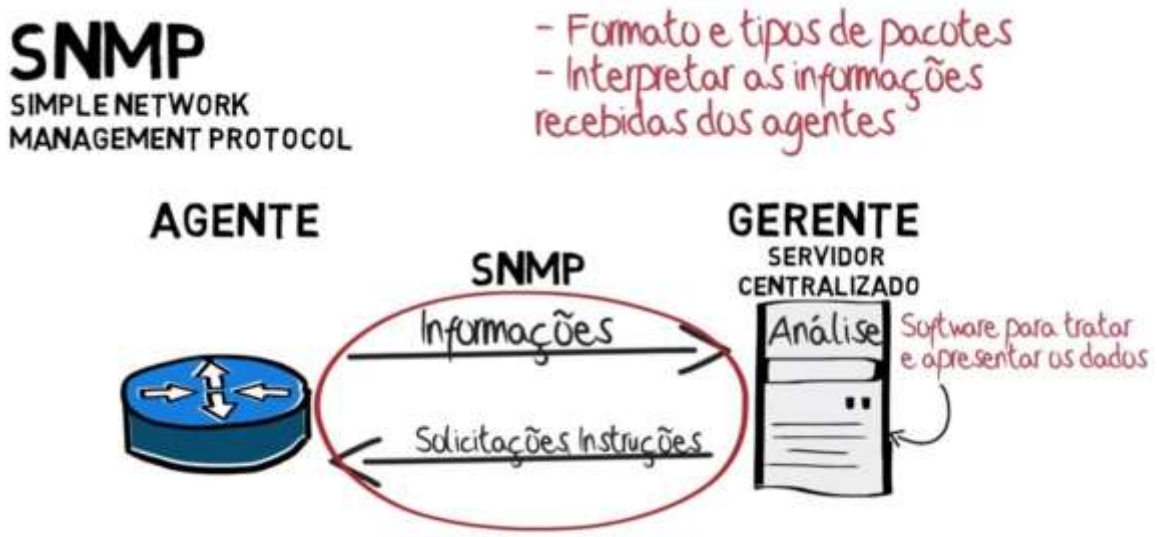


Fonte: www.teleco.com.br

Macedo (2012), explica que o protocolo SNMP não define a MIB, a definição dos objetos da MIB é feita pelo *Abstract Syntax Notation One* (ASN.1), que é uma notação padrão flexível que descreve as estruturas de dados, transmissão, codificação e decodificação, sem a necessidade de se considerar a estrutura nem as restrições do dispositivo de rede no qual será implementada, tornando-o perfeita para o funcionando do SNMP em qualquer linguagem de gerenciamento.

Contudo o SNMP é apenas responsável pela comunicação entre os agentes e o gerente, sendo ele quem define o formato e tipos de pacotes trocados e interpretando as informações recebidas dos agentes, conforme a Figura 5, entretanto para coletar e analisar as informações coletadas, o gerente necessita de um software que trate e apresente os dados de forma mais simples, na qual Macedo (2012) chama-se de *Network Management System* (NMS).

Figura 5: Funcionamento do SNMP



Fonte: adaptado de nic.br

2.3 MÉTRICAS DE GERENCIAMENTO DE REDES

O gerenciamento de redes é realizado por meio da avaliação de métricas de desempenho. Entre as métricas de avaliação podem-se citar: largura de banda, tempo de resposta e perda de pacotes.

A largura de banda estabelece o valor máximo (em bits por segundo) de informação que pode ser trafegado por um canal de comunicação. O tráfego de

informações entre os elementos da rede está limitado pela largura de banda disponível e consome certa quantidade dessa banda. Assim, medir a banda utilizada pelos elementos da rede, e ainda, identificar a distribuição do uso dessa banda, permitirá adotar estratégias de gerenciamento visando o uso equilibrado da banda disponível.

A comunicação entre os elementos da rede é realizada por meio do envio de pacotes de dados entre esses elementos. O parâmetro “perda de pacotes” indica a quantidade de pacotes que se perderam durante a transmissão entre dois pontos da rede. Vários fatores podem causar a perda de pacotes. Por exemplo, em uma região monitorada, quando mais de um elemento da rede simultaneamente tenta transmitir informações, ocorre o que se chama de “colisões”. As colisões causam perda de pacotes e provocam o reenvio dessas informações. Se a quantidade de pacotes perdidos for muito grande, a comunicação pode ficar extremamente comprometida. Avaliar essa métrica permitirá descobrir em quais pontos da rede está ocorrendo um alto número de pacotes perdidos e evitar consumo extra de recursos em função do reenvio desses pacotes de dados.

Tempo de resposta indica o tempo gasto para que as funções de gerenciamento sejam executadas uma única vez. Na abordagem RR, isso significa a quantidade de tempo despendida para enviar as requisições a todos os elementos gerenciados e receber as respectivas respostas. O tempo de resposta está intimamente ligado a perda de pacotes. Quanto maior for o índice de pacotes perdidos, maior será o tempo de resposta.

2.4 FERRAMENTAS DE MONITORAMENTO

Conforme explicado no capitulo 2.2 o NMS é o software que irá solicitar, receber, tratar e exibir os resultados coletados de seus agentes, utilizando o SNMP em sua comunicação. Existem diversas aplicações disponíveis que serão tratadas no presente capítulo.

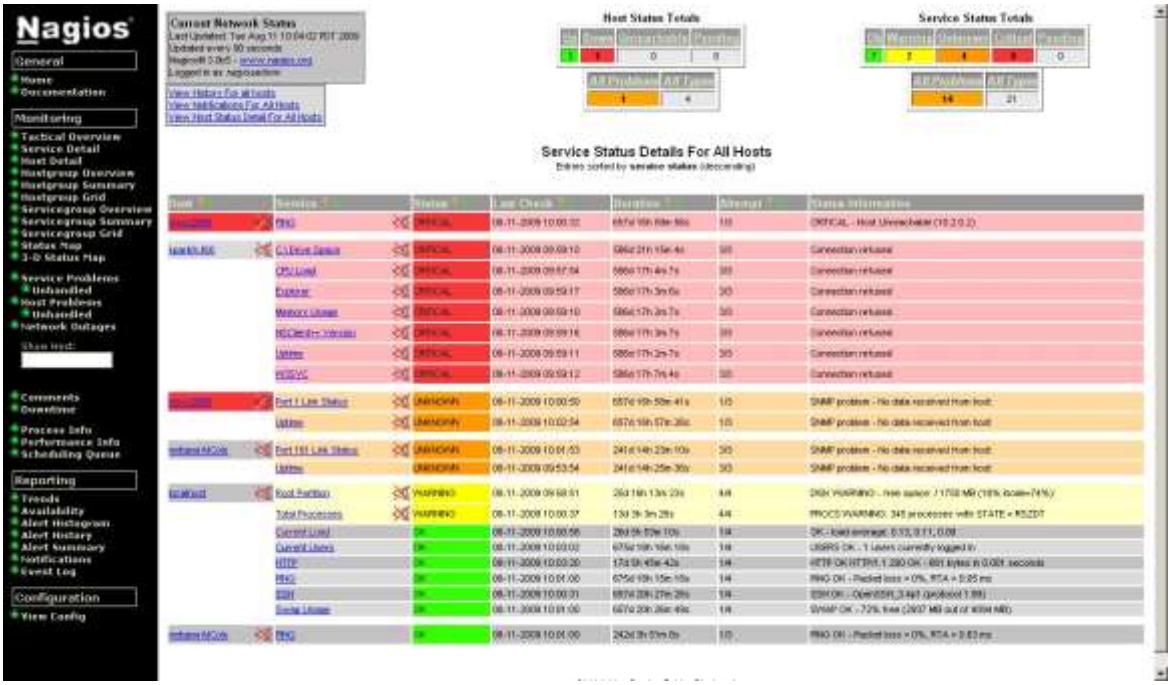
2.4.1 NAGIOS CORE

O Nagios Core é uma aplicação de monitoramento de redes de código aberto e licenciado pelo sistema GPL (*General Public License*) bastante popular.

Ela permite monitorar tanto hosts quanto serviços, alertando-o quando ocorrerem problemas na rede, conforme exemplo da Figura 6, onde é apresentada a tela principal do sistema.

O Nagios Core busca uma forma prática de auxiliar os administradores de redes no processo de monitoração, suas principais características são: o monitoramento de serviços de rede como tráfego de dados de host e serviços que podem ser definidos pelo administrador da rede, além de monitorar serviços como ICMP (Internet *Control Message Protocol*) e SNMP já citados, entre outros, monitora também os recursos de servidores como logs do sistema, carga do processador, uso de memória e uso de disco.

Figura 6: Nagios Core



Fonte: https://serverdensity-wpengine.netdna-ssl.com/wp-content/uploads/2016/02/nagios.jpg

2.4.2 CACTI

Cacti é uma ferramenta que recolhe e exibe informações sobre o estado de equipamentos em uma rede de dados em forma de gráficos, conforme Figura 7, uma série de diferentes gráficos podem ser feitos com os scripts shell ou perl, esta é uma solução web php/mysql usando a engine do RRDtool.

RRDtool é desenvolvido usando a linguagem de programação "C" e ele guarda os dados coletados em arquivos “.rrd", este arquivo tem um tamanho fixo significando que antigos registros são frequentemente removidos. Isto implica que ele obtém figuras precisas, logo para dados muito antigo os gráficos possuem valores aproximado. Por padrão, você pode obter gráficos diários, semanais, mensais e anuais.

Figura 7: CACTI

Fonte: http://www.cacti.net/

2.4.3 ZABBIX

Zabbix vem com uma interface baseada na web contando com uma interface intuitiva, rápida e amigável, contendo informações importantes, como quantidade de hosts monitorados, eventos, gráficos, entre outras opções configuráveis conforme Figura 8, autenticação segura do usuário e um esquema de permissão de usuário flexível, com agentes de alto desempenho coletas nativas de dados a partir de praticamente qualquer sistema operacional popular, métodos de monitoramento sem agente também estão disponíveis.

Figura 8: Tela principal Zabbix

Fonte: Autoria própria

O Zabbix oferece a liberdade de usar uma solução de código aberto sem *vendor lock-in* e código-fonte livremente acessível. Isso inclui não apenas em si Zabbix, mas também componentes necessários (Linux, Apache, MySQL / PostgreSQL, PHP).

A sua instalação e configuração são fáceis, contando com agentes altamente eficientes para plataformas UNIX e Windows (x32, x64) e um sistema de controle centralizado na qual permite armazenar toda a informação em uma base de

dados relacional para um processamento mais fácil e a reutilização de dados. Possui uma capacidade de visualização rica e de fácil entendimento de seus gráficos, conforme Figura 9, procedimentos de limpeza de dados automatizados na qual permite que mantenha uma base de dados controlada e ágil para pesquisa de longo prazo, mas seu grande diferencial é que o Zabbix consegue agregar valores das duas ferramentas citadas anteriormente, Nagios e Cacti.

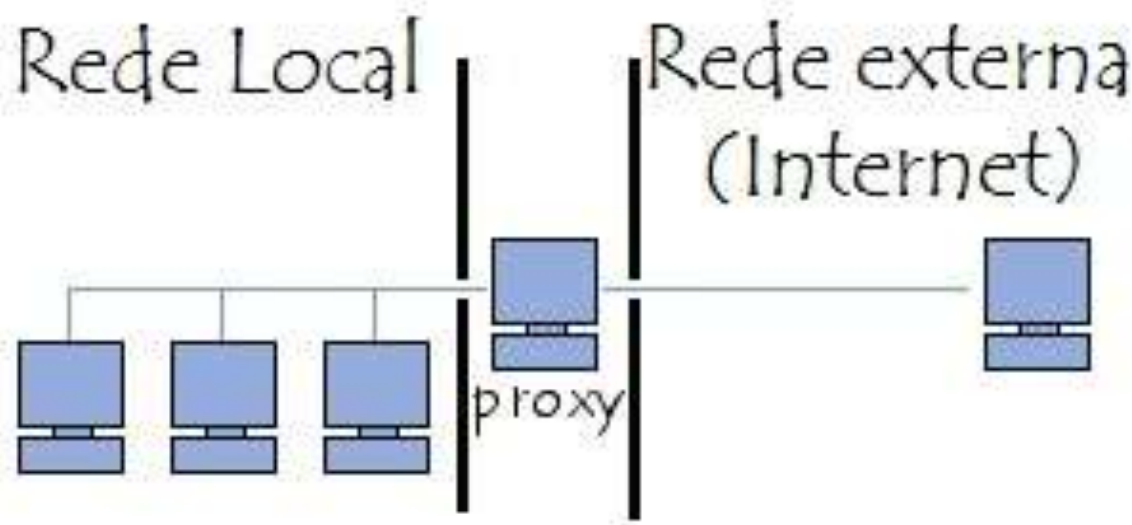
Figura 9: Gráficos Zabbix

Fonte: Autoria própria

3 PROXY

BARWINSKI (2009) explica que ao final da década de 80, o cientista Tim Berners-Lee inventou uma nova forma de ver a Internet, criando a World Wide Web, WWW como conhecemos hoje, com a criação desta nova ferramenta surgiu a necessidade de interligar a rede local (LAN ou rede interna) com a Interweb (rede externa), conforme na Figura 10, com isso surgiu o Proxy, sem este serviço a própria existência da Internet seria complicada, sendo economicamente inviável interligar todas as redes de comutadores do mundo, quem dirá computadores domésticos, sem o Proxy usuários comuns dificilmente conseguiriam utilizar a Internet.

Figura 10: Funcionamento do Proxy



Fonte: adaptado de CCM[5]

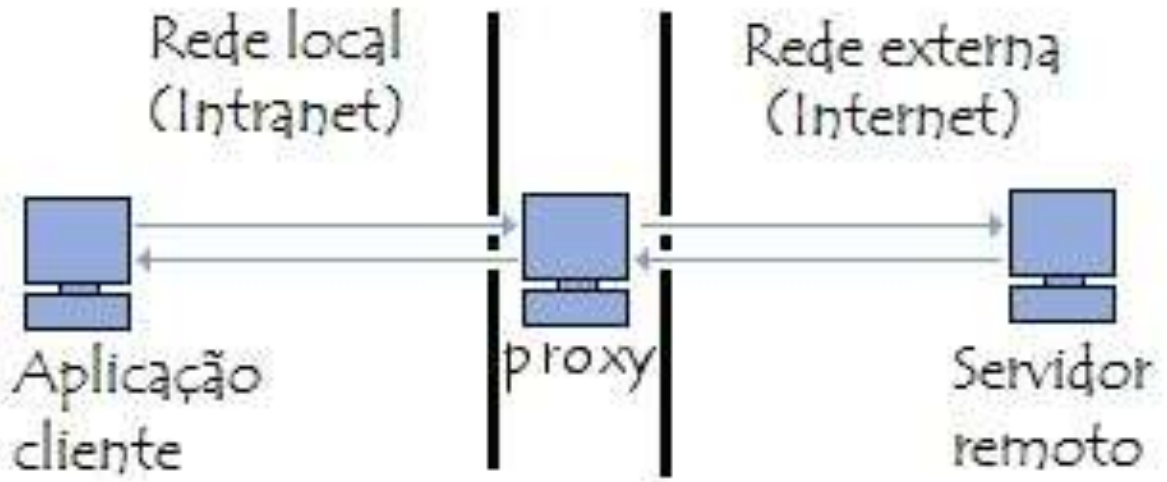
3.1 O PRINCÍPIO DE FUNCIONAMENTO DO PROXY

Observa-se na Figura 10 que todo o tráfego de rede passa pelo Proxy, sendo ele o intermediário entre a rede interna (LAN) e a rede externa (Interweb). Portanto toda solicitação de acesso a uma página é feita ao Proxy e ele é quem

[5] http://br.ccm.net/contents/301-servidores-proxy-servidores-mandatarios-e-reverse-proxy

solicita ao servidor remoto as informações, ao receber o solicitado ele entrega ao cliente, conforme é mostrado na Figura 11.

Figura 11: Funcionamento de requisição do Proxy.



Fonte: adaptado de CCM[6]

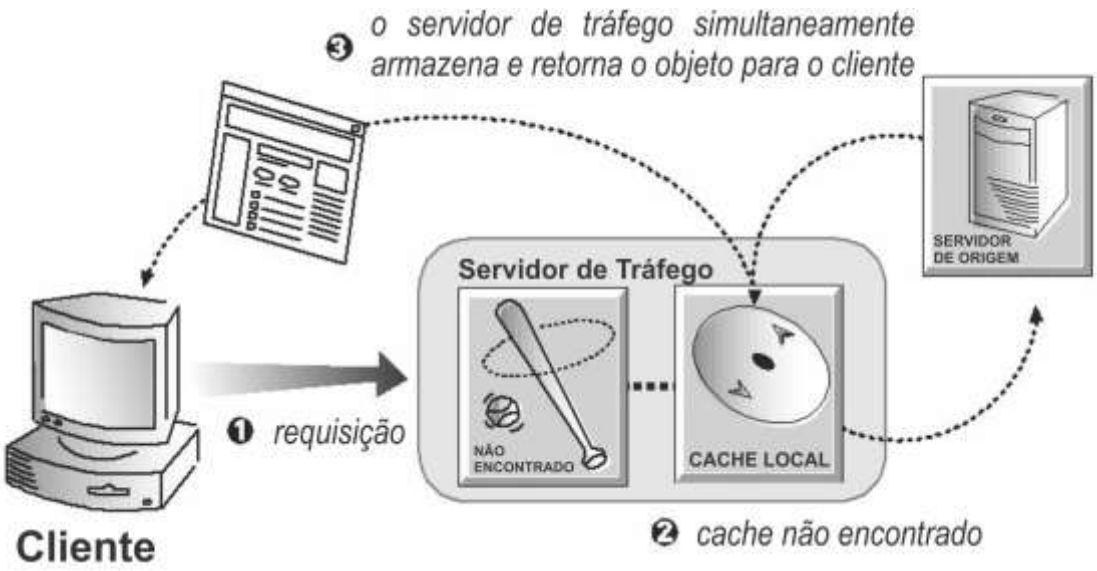
3.2 ARMAZENAMENTO EM CACHE

Segundo TANENBAUM (2003), no início de uso da Internet sua popularidade quase a arruinou, pois, o aumento repentino de sua carga foi desproporcional ao suporte da rede, fazendo com que servidores, roteadores e linhas de frequência sobrecarregassem. Em função disso, pesquisadores desenvolveram várias formas para melhorar o desempenho.

O Proxy de armazenamento local web (ou caching web Proxy), é um recurso do servidor Proxy que armazena as páginas para o caso delas serem solicitadas novamente, conforme na Figura 12, segundo Tanenbaum (2003) “Essa técnica é especialmente efetiva com páginas muito visitadas, como www.yahoo.com e www.cnn.com“.

[6] http://br.ccm.net/contents/301-servidores-proxy-servidores-mandatarios-e-reverse-proxy

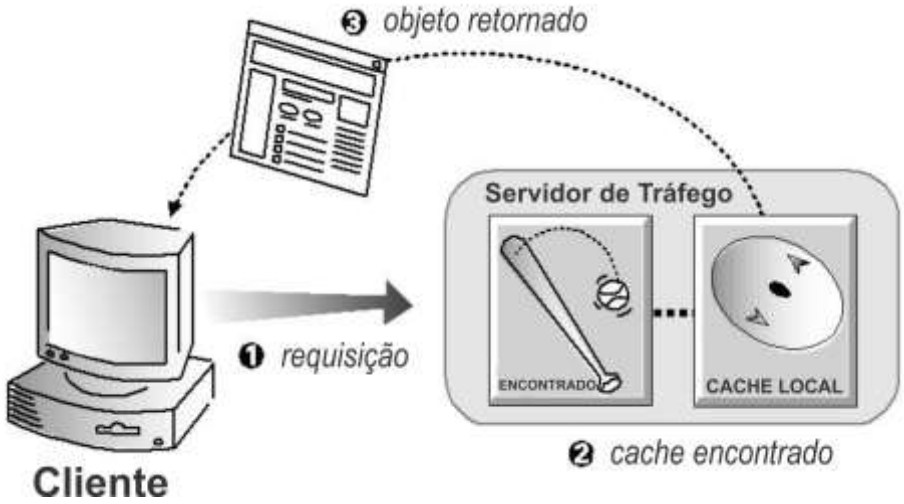
Figura 12: Página encontrada no cache



Fonte: adaptado de TRAFFICSERVER

Tanenbaum (2003) explica que o processo de cache, pode melhorar o tempo de resposta das páginas mais visitadas e o aumento da largura de banda já caso haja outro pedido da mesma página o Squid apresenta este cache localmente para o usuário, com isto economizando link de conexão e tempo de acesso, tornado o link mais eficiente e a resposta mais, conforme demonstrado na Figura 13, também há uma redução do trafego efetuado pelo link, já que algumas páginas serão entregues a partir do cache local.

Figura 13: Página não encontrada no cache



Fonte: adaptado de TRAFFICSERVER

3.3 PROGRAMAS

A Cia do Software (2012) explica que Software é um conjunto de instruções lógicas que permitem ao computador realizar várias tarefas para o seu dia a dia.

Com isso necessitamos de um ou mais softwares para que o objetivo deste trabalho possa ser alcançado, neste capítulo serão apresentados alguns dos softwares mais populares de Proxy.

3.3.1 RouterOS

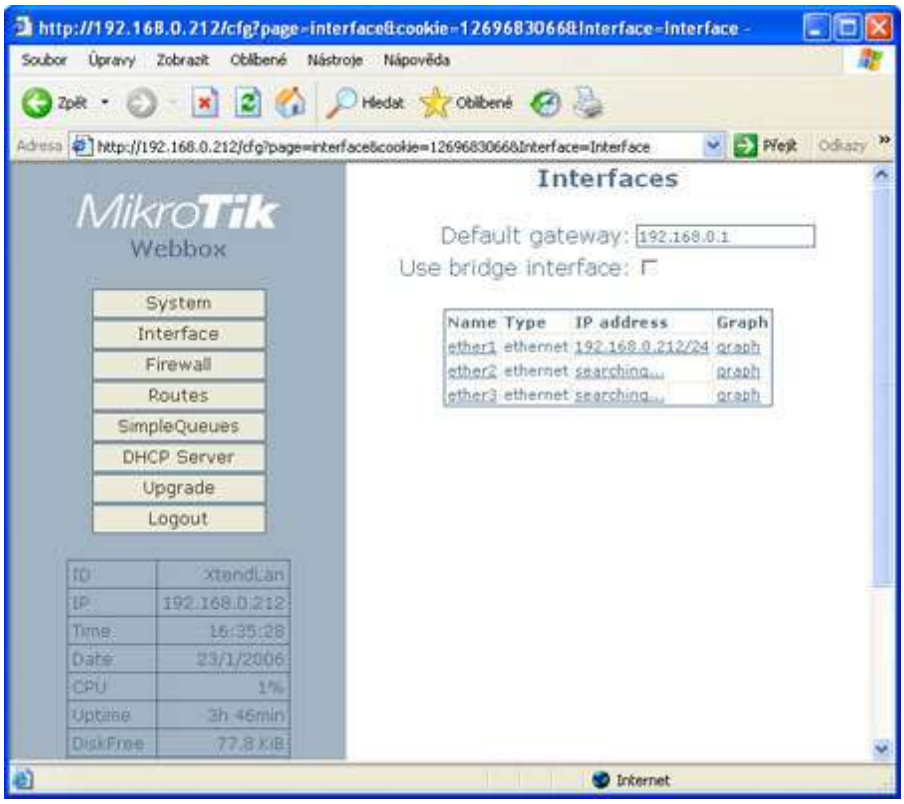
A MikroTik é uma empresa da Letônia, fundada em 1995 para desenvolver roteadores e Sistemas Wireless para Provedores. A MikroTik em 2002 começou a fabricar seu próprio hardware, sob a marca RouterBOARD.

RouterOS é o sistema operacional (S.O) das RouterBOARDs. Ele também pode ser instalado em PCs comuns, até mesmo nos mais antigos, transformando-o em um poderoso roteador, com todas as funções necessárias para Roteamento, Firewall, Gerência de Banda, Wireless, Proxy, Servidor de VPN, entre outros.

O RouterOS conta com uma interface web amigável como também uma ferramenta de acesso remoto compatível com S.O Windows e linux, assim facilitando a sua administração, conforme Figura 14 e Figura 15.

Contudo o MikroTik RouterOS é um software pago, sendo possível a utilização gratuita para testes por 24 horas, no site da empresa possui um simulador do Software, como também documentação, exemplos, FAQ, link para download do Sistema Operacional.

Figura 14: MikroTik webBox (software de gerenciamento via web browser)



Fonte: Autoria própria

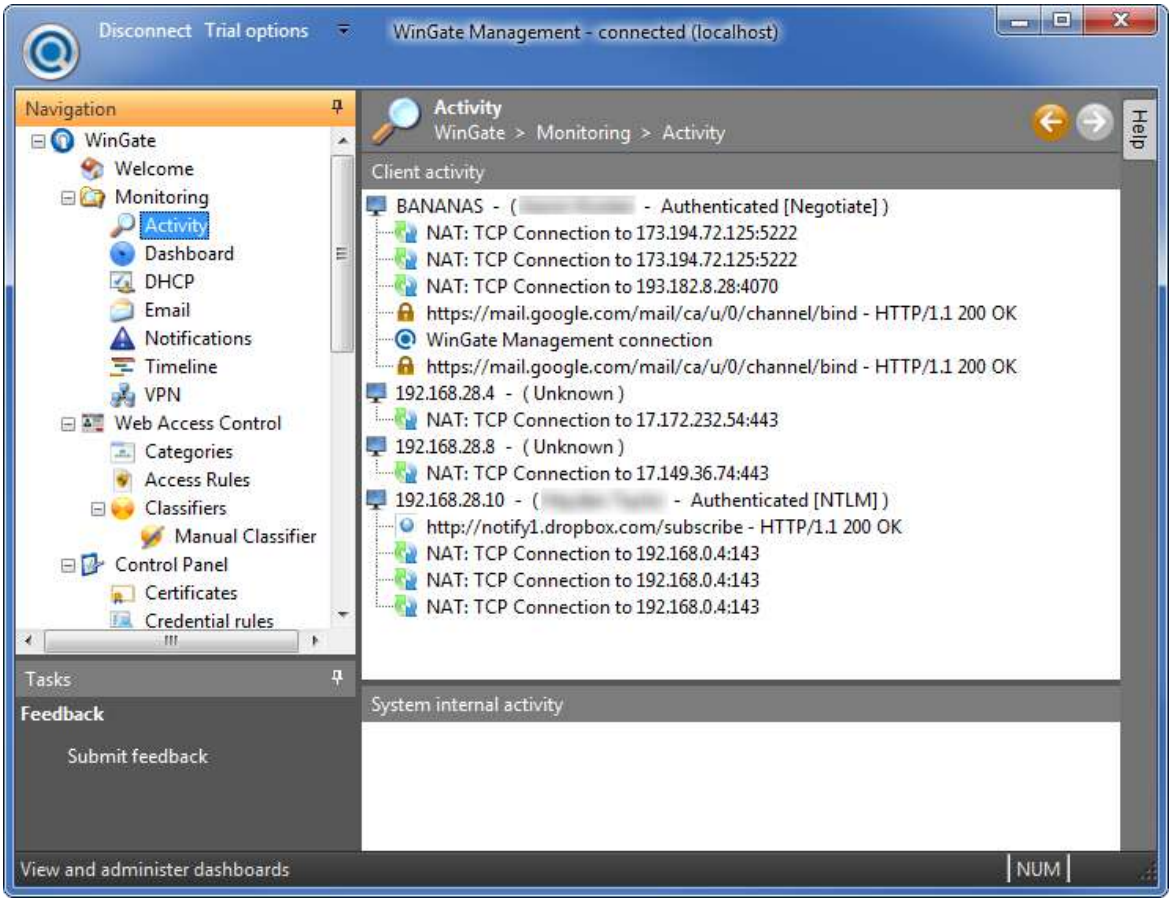
Figura 15: MikroTik WinBox (Ferramenta de gerenciamento remoto)

Fonte: Autoria própria

3.3.2 Wingate Proxy

O Wingate é um software desenvolvido para rodar no S.O Windows e atualmente está na versão 8.5.3, está é uma ferramenta completa de gerenciamento de redes contando com vários módulos, como VPN, anti-virus de rede, análise de logs, entre outros, por se tratar de uma ferramenta Windows, tem como ponto forte a sua interface gráfica de fácil interpretação (Figura 16).

Figura 16: Tela principal do WinGate Management



Fonte: Autoria própria

Contudo o WinGate é um software licenciado e pago, porém a empresa disponibiliza em seu site uma versão *free* com limitações, trata-se do WinGate 7.2 limitado a 3 conexões simultâneas com severas restrições segundo o site do desenvolvedor.

3.3.3 Squid

Squid é um software especializado em fazer a operação de Proxy web HTTP, HTTPS, FTP e outros, gratuita e com excelente suporte para operação em servidores Linux. Ele reduz a utilização da conexão e melhora os tempos de resposta fazendo cache de requisições frequentes de páginas web numa rede de computadores.

O Squid é um software na qual não possui um ambiente gráfico sendo originalmente todo em arquivos de texto, entretanto a sua aplicação é devidamente simples, ele trabalha com uma série de parâmetros que podem ser informados no squid.conf e suas regras são criadas através de *Access Control List* ou Lista de Controle de Acesso (ACL) e o seu funcionamento se resume a, o que quer bloquear, o que quer liberar.

O Squid ao receber uma requisição percorre o seu arquivo txt de configuração “squid.conf” de cima para baixo até encontrar uma regra que se encaixe, a execução é feita por meio de uma função interna chamada “http_access”, esta função do Squid bloqueia (*deny*) ou libera (*allow*) de acordo com o que está configurada em sua ACL e então finaliza aquele processo, logo as regras precisam ser cuidadosamente analisadas, pois a ordem da ACL implica em seu resultado.

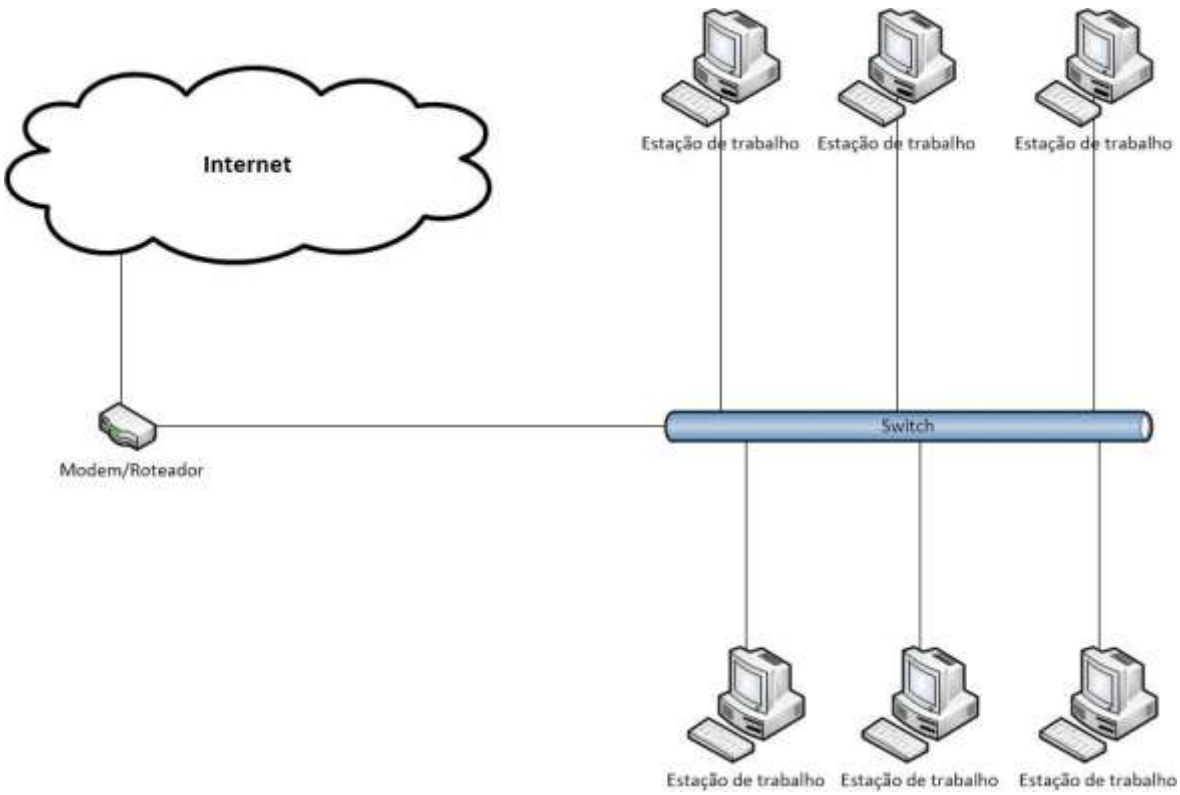
4 ESTUDO DE CASO

Para ilustrar e compreender a importância do gerenciamento, foi desenvolvido um estudo de caso em um ambiente real de trabalho para identificar as possíveis causas da lentidão da internet e tentar solucionar ou reduzir seu efeitos.

4.1 DESCRIÇÃO DO CENÁRIO

O cenário deste estudo de caso é simples e comum, sendo uma rede de computadores, interligadas por um switch a uma única conexão com a internet, conforme na Figura 17.

Figura 17: Estrutura de redes inicial



Fonte: Autoria própria

4.2 JUSTIFICATIVAS DA ESCOLHA DOS SOFTWARES

Tendo em vista que a operadora de Internet excluiu a possibilidade de o problema ser irregularidades de infra ou o link, ferramentas de diagnóstico de rede seriam necessárias para encontrar a falha.

Devido à urgência em saber o motivo do problema e sua solução, as ferramentas teriam que ser gratuitas, pois se trava de um órgão público e a compra demoraria ou até poderia ser negada.

Logo diversas aplicações gratuitas foram pesquisadas e testadas, três delas se destacaram na característica de gerenciamento de redes e apresentação de relatórios, conforme visto no item 2.4.

O Zabbix foi à escolha, já que conforme abordado no item 2.4, ele agrega os valores do Cacti e o Nagios Core, está aplicação é um open source e utiliza licença GPL. É um software que vem sendo muito utilizado recentemente, por sua excelente gestão, ser multi-plataforma, com relatórios muito bem elaborados e de fácil manuseio, podendo rodar em um micro comum.

A princípio a implantação do Zabbix seria apenas para efetuar, registrar e armazenar pings ininterruptamente em um intervalo pré-determinado, para que com isso pudesse obter duas métricas, a perda de pacotes e o tempo de resposta, conforme visto na Figura 19.

A implantação do Zabbix foi de suma importância, para um diagnóstico preciso, pois com ele foi possível medir a utilização de banda do link e constatar que a sua utilização estavam sempre no máximo contratado e por consequência disso a lentidão da Internet e suas interrupções, logo a necessidade de uma ferramenta de controle de acesso seria necessária.

Entretanto a empresa não tinha nenhuma política ou controle de acesso aos recursos de Internet, uma reunião com a administração foi solicitada e os gráficos iniciais gerados pelo Zabbix foram utilizados para demonstrar que o consumo do link contratado estava sendo totalmente utilizada, conforme demonstrado na Figura 18, portando uma política de acesso e uma ferramenta de gerenciamento deveria ser implantada, para tentar controlar o uso deliberado da banda.

A administração reconheceu os gráficos e concordou que a política e a ferramenta deveriam ser implantadas, as regras de acesso foram básicas.

- Todo endereço de rede social, radio online, streaming devem ser bloqueados para todos os usuários.

- Todos os sites do governo, não devem ter bloqueio, inclusive o diário oficial.

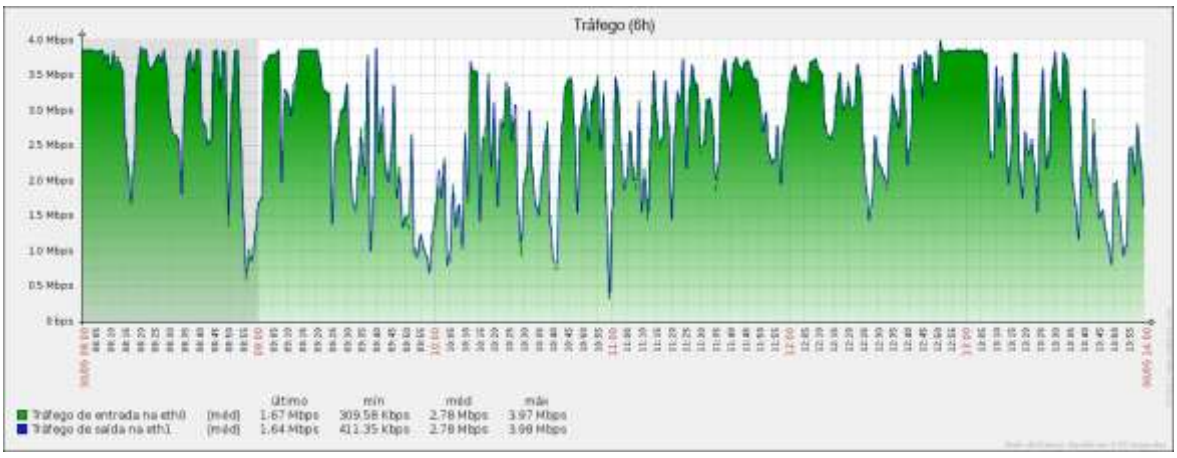
Então uma pesquisa a procura de uma ferramenta de controle de acesso, respeitando a mesma característica utilizada para o Zabbix e o software escolhido foi o Proxy Squid, embora esta ferramenta não tenha um ambiente gráfico, conforme abordado no item 3.3.3, é compatível com a versão do Linux do servidor Zabbix, assim facilitando a sua instalação, é utilizado por grandes empresas do mercado de trabalho, devido a sua estabilidade e compatibilidade.

4.3 TESTES

Antes de iniciar a implantação, as ferramentas de gerenciamento, controle de acesso e as políticas foram testadas em um ambiente virtual, utilizando o VirtualBox[7].

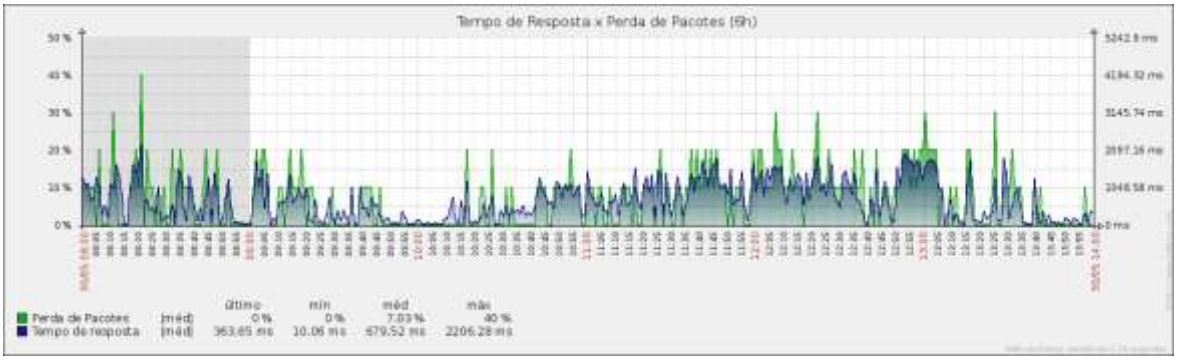
Para obter as métricas precisa-se medir o consumo de banda, a perda de pacotes e o tempo de resposta, então para facilitar o trabalho, foi feita uma pesquisa no próprio fórum do Zabbix, por um modelo com este requisito e foi encontrado o modelo “Conectividade[8]”, utilizando este modelo foi possível obter o tráfego da rede, conforme Figura 18, tempo de resposta e perda de pacotes do link, conforme Figura 19.

Figura 18: Tráfego sem controle de acesso



Fonte: Autoria própria

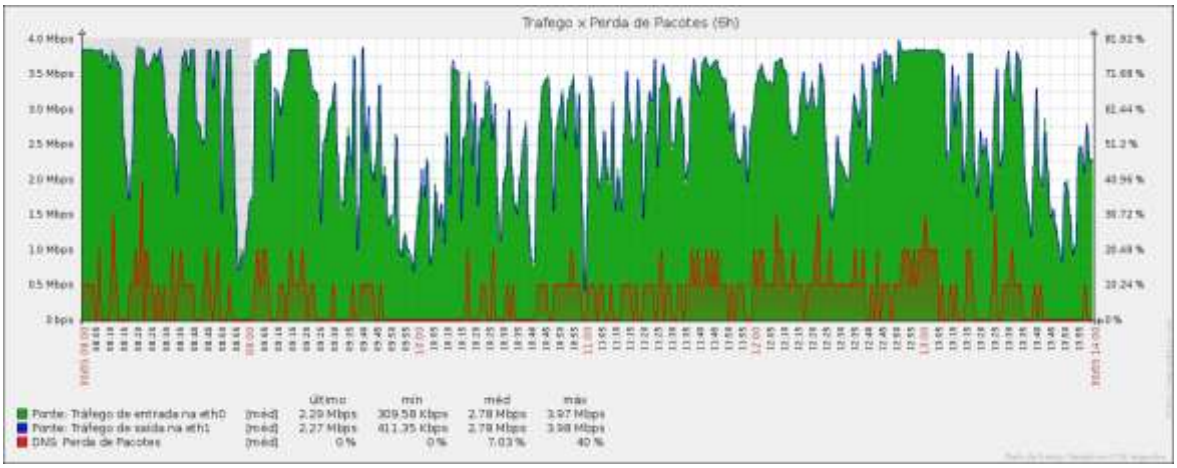
Figura 19: Tempo de resposta x Perda de pacotes sem controle de acesso



Fonte: Autoria própria

Na Figura 20, tem-se uma melhor visão da relação entre o consumo do link e a perda de pacotes, já na Figura 21 se vê a ligação entre o consumo e o tempo de resposta, pois conforme abordado no item 2.3, a largura de banda é o limite de comunicação, logo se o consumo está próximo de seu limite ou o atinge, o número de pacotes perdidos e o tempo de resposta vão se elevar, afetando assim a qualidade da Internet e ocasionando lentidão.

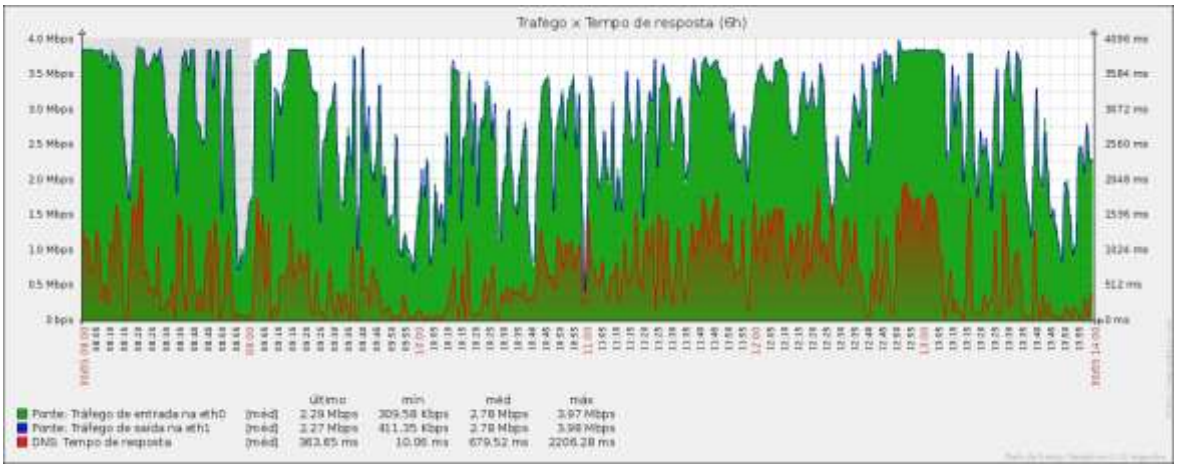
Figura 20: Trafego x Perda de pacotes sem controle de acesso



Fonte: Autoria própria

[7] https://www.virtualbox.org/
[8] https://www.zabbix.com/forum/attachment.php?attachmentid=6105&d=1376403438

Figura 21: Trafego x Tempo de resposta sem controle de acesso

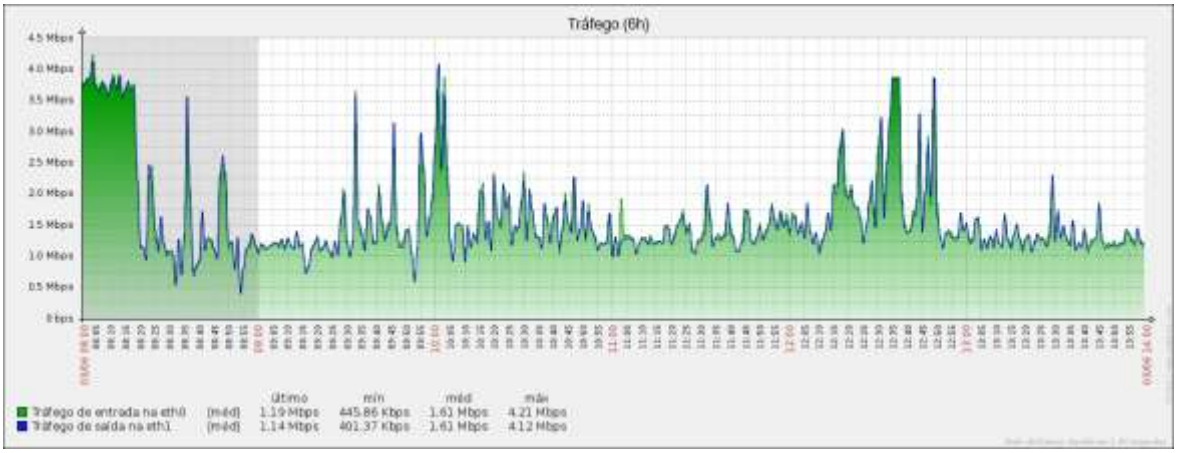


Fonte: Autoria própria

5 DISCUSSÕES E RESULTADOS

Após a implantação do Squid e a configuração em todos os usuários da rede, uma nova medição foi feita para avaliar se houve melhora na perda de pacotes, tempo de resposta e tráfego do link. Para ter uma base confiável e sólida o mesmo horário do primeiro gráfico foi analisado, conforme demonstrado na Figura 22 e Figura 23.

Figura 22: Tráfego depois de implantado controle de acesso



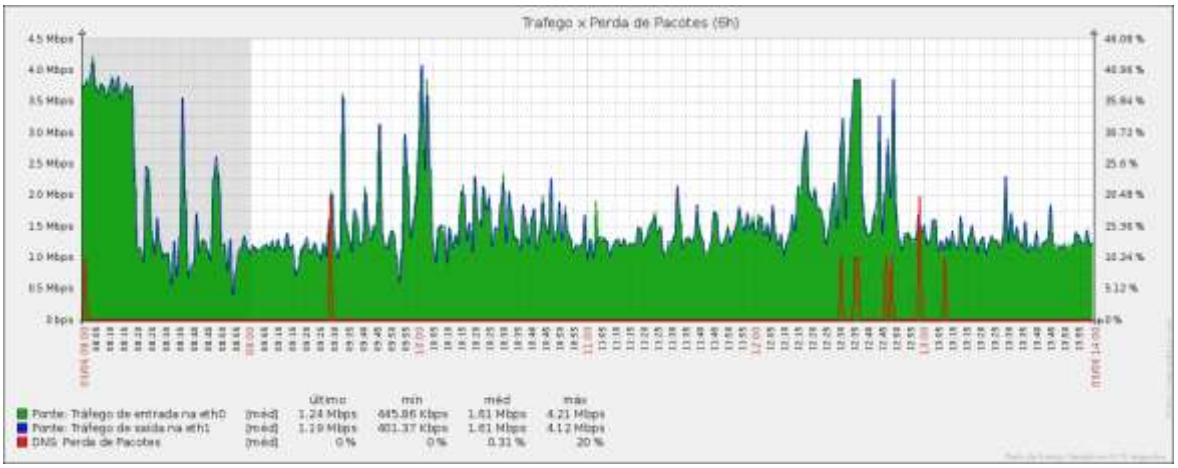
Fonte: Autoria própria

Figura 23: Tempo de resposta x Perda de pacotes com controle de acesso

Fonte: Autoria própria

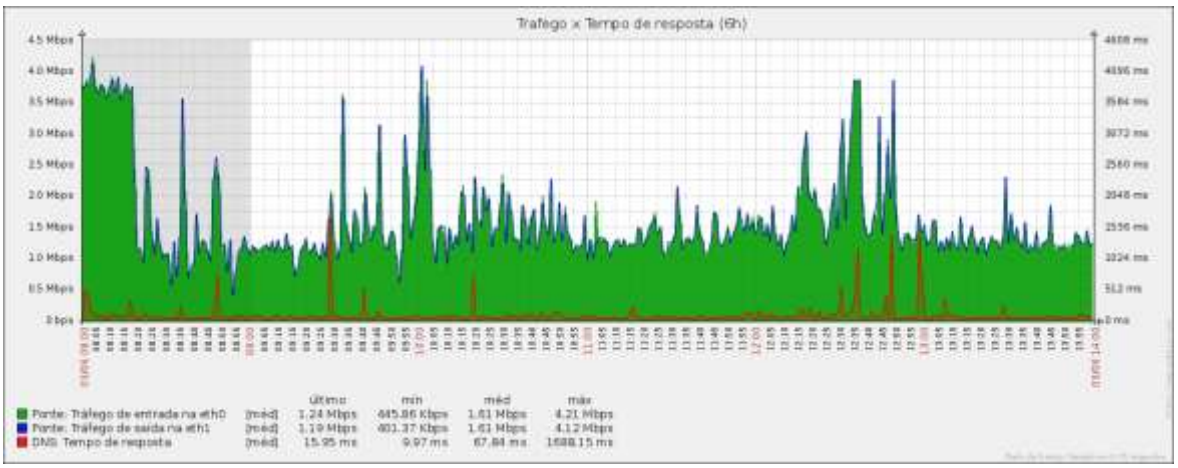
Para uma melhor visualização um combinando entre tráfego e perda de pacotes na qual é demonstrado na Figura 24 e outro entre tráfego e tempo de resposta visto na Figura 25, em ambos apesar de alguns picos, mantem-se estável e em níveis aceitáveis, os picos estão relacionados o nível de utilização de largura de banda, conforme abordado no item 2.3.

Figura 24: Trafego x Perda de pacotes com controle de acesso



Fonte: Autoria própria

Figura 25: Trafego x Tempo de resposta com controle de acesso



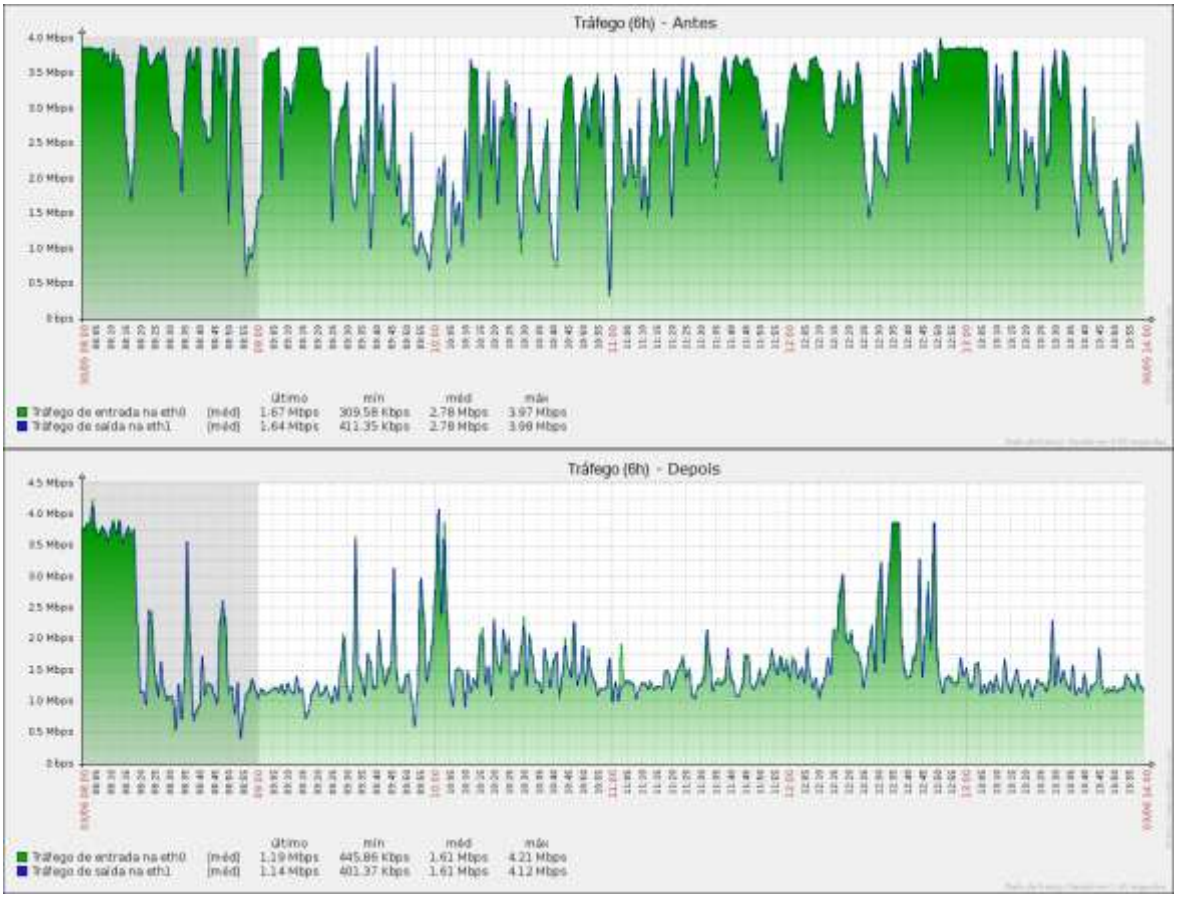
Fonte: Autoria própria

6 CONSIDERAÇÕES FINAIS

Através da Figura 26 tem-se uma comparação entre o primeiro gráfico do Zabbix antes da implantação do Squid e outro após todo o controle, a redução de tráfego é visível, já na Figura 27 tem-se o tempo de resposta e perda de pacotes e novamente a redução está visível, com alguns picos, entretanto em níveis aceitáveis.

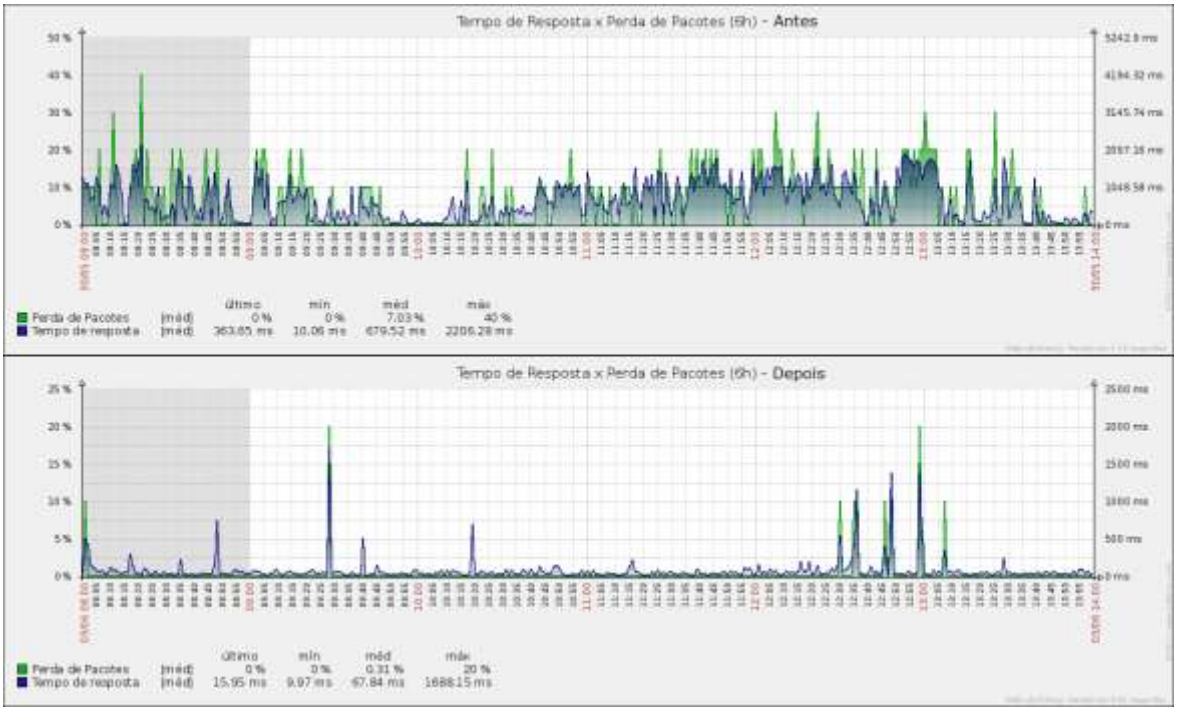
Então na Figura 28 é demonstrado o efeito do Squid neste caso de uso, nele é demonstrado que o tráfego total analisado gerou 68,42GB de dados, entretanto 21,01% de todo site acessado foi entregue pelo cache, conforme abordado no item 3.2, o cache economiza a largura de banda e agiliza a entrega do site, melhorando o desempenho como um todo.

Figura 26: Comparação do tráfego



Fonte: Autoria própria

Figura 27: Comparação do tempo de resposta e perda de pacotes



Fonte: Autoria própria

Figura 28: Relatório de uso do Squid

NUM		USUÁRIO	CONEXÃO	BYTES	%BYTES	IN-CACHE-OUT		TEMPO GASTO	MILISEG	%TEMPO
1		10.14.239.96	416.81K	6.85G	10.02%	12.33%	87.67%	1751:02:34	6,303,754,781	10.16%
2		10.14.239.33	337.22K	4.36G	6.37%	50.88%	49.12%	168:12:52	605,572,279	0.98%
3		10.14.239.76	260.18K	3.87G	5.66%	27.78%	72.22%	808:22:56	2,910,176,849	4.69%
4		10.14.239.32	269.20K	3.39G	4.96%	54.07%	45.93%	143:21:51	516,111,323	0.83%
5		10.14.239.55	173.32K	3.35G	4.90%	13.51%	86.49%	961:20:39	3,460,839,713	5.58%
6		10.14.239.67	78.41K	2.78G	4.06%	5.95%	94.05%	732:16:12	2,636,172,717	4.25%
7		10.14.239.47	217.50K	2.75G	4.03%	12.27%	87.73%	717:12:11	2,581,931,430	4.16%
8		10.14.239.30	161.60K	2.75G	4.03%	11.43%	88.57%	680:39:04	2,450,344,187	3.95%
9		10.14.239.62	131.84K	2.74G	4.01%	36.99%	63.01%	475:22:52	1,711,372,578	2.76%
10		10.14.239.123	42.38K	2.46G	3.60%	5.18%	94.82%	287:20:25	1,034,425,169	1.67%
11		10.14.239.31	237.33K	2.19G	3.21%	30.80%	69.20%	313:57:21	1,130,241,971	1.82%
12		10.14.239.86	195.16K	1.91G	2.81%	30.99%	69.01%	353:34:16	1,272,856,990	2.05%
13		10.14.239.46	128.18K	1.88G	2.76%	18.82%	81.18%	629:57:01	2,267,821,404	3.66%
14		10.14.239.57	224.39K	1.82G	2.66%	28.69%	71.31%	163:40:34	589,234,630	0.95%
15		10.14.239.124	81.52K	1.72G	2.52%	33.98%	66.02%	540:18:38	1,945,118,223	3.14%
16		10.14.239.91	40.40K	1.04G	1.52%	21.07%	78.93%	523:33:36	1,884,816,810	3.04%
17		10.14.239.120	89.36K	1.02G	1.50%	17.92%	82.08%	434:27:38	1,564,058,976	2.52%
		TOTAL	**4.30M**	**68.42G**		**21.01%**	**78.99%**	**17227:22:21**	**62,018,541,243**	
		MÉDIA	**86.06K**	**1.36G**				**344:32:50**	**1,240,370,824**	

Fonte: Autoria própria

Através da Figura 29 têm-se os valores analisados e nota-se uma enorme melhora, já que o consumo médio teve uma redução de 57,91%, a perda de pacotes 2267,74% e o tempo de resposta em 1001,65%, esta melhora é visível ao tentar utilizar a internet, mesmo páginas novas tem a sua exibição muito rápida e não a negação de acesso e nem falha ao acesso a qualquer site.

Logo este estudo de caso conclui que com uma política de acesso e uma ferramenta de controle de acesso é possível controlar a utilização do link de internet de maneira racional, oferecendo um serviço de qualidade sem afetar o andamento do trabalho, além do mais este estudo não gerou custos a empresa de aquisição de software ou licenças de uso, pois todos os softwares são gratuitos, livres e com seu código fonte inclusos.

Figura 29: Comparativo de resultados

	Antes			
	Mínimo	Média	Máximo	
Entrada	309,58 Kbps	2,78 Mbps	3,97 Mbps	
Saida	411,35 Kbps	2,78 Mbps	3,98 Mbps	
Perda de pacotes	0	7,03%	40%	
Tempo de resposta	10,06ms	679,52ms	2206,28ms	
	Depois			Redução
	Mínimo	Média	Máximo	
Entrada	445,86 Kbps	1,61 Mbps	4,21 Mbps	57,91%
Saida	401,37 Kbps	1,61 Mbps	4,12 Mbps	57,91%
Perda de pacotes	0	0,31%	20%	2267,74%
Tempo de resposta	9,97ms	67,84ms	1688,15ms	1001,65%

Fonte: Autoria própria

7 FUTURO

O caso de uso atingiu seu objetivo com perfeição, entretanto foram abordados apenas dois softwares e de uma forma simplista, mas após o término do estudo aplicações complementares foram vistas e são interessantes para incrementar este projeto.

Neste caso de uso a forma de filtro utilizada foi por endereço ip de cada máquina, não necessitando de autenticação, entretanto o Squid tem suporte para diversas formas de autenticação, inclusive com o *Active Directory* (AD) da Microsoft, com tal recurso, podem-se determinar níveis de acesso e um maior controle por usuário e não apenas pelo endereço ip, tornando o sistema mais flexível a mudanças e aumentando a segurança, tendo em vista que a liberação do acesso será por usuário.

O Squid é um analisador de URL, logo todo o seu controle baseia-se no endereço do site, entretanto existe uma ferramenta completar a ele na qual analisa o conteúdo das páginas acessadas seu nome é DansGuardian que também é um Open Source e gratuito, este software pode melhorar a qualidade das regras de filtro da empresa.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago. - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

ANCORADOR. **Proxy**: conheça toda sua história. Disponível em: <**Erro! A referência de hiperlink não é válida.**>. Acessado em: 30 set. 2015.

BATTISTI, Julio. 2012. **Listas de Controle de Acesso – ACL's.** Disponível em: http://juliobattisti.com.br/tutoriais/luisepedroso/acl001.asp. Acessado em 20 abr. 2016.

CANALTECH. 2012. Disponível em: <http://canaltech.com.br/o-que-e/internet/O-que-e-um-RFC/>. Acessado em: 02 mai. 2016.

CIADOSOFTWARE. 2014. Disponível em: <http://www.ciadosoftware.com.br/sejalegal.asp>. Acessado em: 20 jan. 2016.

CCM; **Servidores proxy (servidores mandatários) e reverse-proxy.** Disponível em: <http://br.ccm.net/contents/301-servidores-proxy-servidores-mandatarios-e-reverse-proxy>. Acessado em 05 out. 2015.

COSTA, Eduardo Augusto. **Controle de acesso através do Squid.** 2015. Disponível em: <http://repositorio.ufla.br/jspui/bitstream/1/9630/1/ARTIGO_Controle_de_acesso_atraves_do_Squid.pdf>. Acessado em: 13 de out. 2015.

DUTRA, Djair. 2006. **A verdade sobre as ACLs do Squid**. Disponível em: < https://www.vivaolinux.com.br/artigo/A-verdade-sobre-as-ACLs-do-Squid>. Acessado em 20 abr. 2016.

FILHO, Olavo Poleto. 2012: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes1>. Acessado em: 05 jan. 2016.

FILHO, Olavo Poleto. 2012: Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes2>. Acessado em: 05 jan. 2016.

FTECH. 2011. **Proxy**: Qual sua finalidade? Disponível em: <http://www.ftech.net.br/?p=618>. Acessado em: 30 set. 2015

TRAFFICSERVER. **HTTP proxy caching**: Disponível em: <http://trafficserver.readthedocs.io/en/latest/admin-guide/configuration/cache-basics.en.html#understanding-http-web-proxy-caching>. Acessado em: 15 de out. 2015.

IETF. 1990. Disponível em: <www.ietf.org>. Acessado em: 10 mai. 2016.

KUROSE, James F. **Redes de computadores e a Internet**: uma abordagem top-down. Ed. 5. São Paulo: Addison Wesley, 2010.

MACEDO, Diego. 2012. Disponível em: <http://www.diegomacedo.com.br/gerenciamento-de-redes-protocolo-snmp/>. Acessado em: 23 mai. 2016.

MIKRODICAS. **O que é Mikrotik e RouterOS? .** Disponível em: <http://www.mikrodicas.com.br/2012/09/o-que-e-mikrotik-e-routeros.html>. Acessado em: 13 de out. 2015.

NIC. 2016. Disponível em: <http://www.nic.br/>. Acessado em: 12/04/2016.

PAULINO, Daniel. 2009. **Squid o que é?**. Disponível em: <https://www.oficinadanet.com.br/artigo/1998/squid_o_que_e>. Acessado em: 14 de out. 2015.

PINHEIRO, Ricardo. 2012. Disponível em: https://www.mundotibrasil.com.br/o-protocolo-snmp/?doing_wp_cron=1464131564.5238308906555175781250>. Acessado em: 28 abr. 2016

RUSSO, Rafael. 2014. Disponível em: <http://escreveassim.com.br/2014/03/19/gerencia-de-redes-com-fcaps/>. Acessado em: 03 mai. 2016.

SIGNIFICADOS. **Significado de Software.** 2012. Disponível em <http://www.significados.com.br/software/>. Acessado em: 20 jan. 2016.

SOARES, Alexandre Seixas. et. All. 2010. Disponível em: <http://www.gta.ufrj.br/grad/10_1/snmp/snmp.htm>. Acessado em: 01 mai. 2016.

TANENBAUM, Andrew S. **Redes de Computadores**. 2003.

BARWINSKI, Luísa. **A World Wide Web completa 20 anos, conheça como ela surgiu.** Disponível em: <http://www.tecmundo.com.br/historia/1778-a-world-wide-web-completa-20-anos-conheca-como-ela-surgiu.htm>. Acessado em: 30 set. 2015.

APÊNDICE A – Instalação e configuração do Zabbix

Para instalação foi utilizado o Ubuntu Server 12.04 LTS em sua instalação padrão, foi escolhido o Zabbix 2.2 sendo facilmente instalado em poucas etapas exatamente como apresentado no item 2.4.3 utilizando o tutorial de Hernandes Martins[9], também disponível em pdf[10] conforme será apresentado abaixo.

Instale o pacote de configuração do repositório utilizando o comando “wget http://repo.zabbix.com/zabbix/2.2/ubuntu/pool/main/z/zabbixrelease/zabbix-release_2.2-1+precise_all.deb” conforme ilustrado na Figura A 1, este pacote contém arquivos de configuração do Zabbix 2.2 para Ubuntu 12.04 LTS.

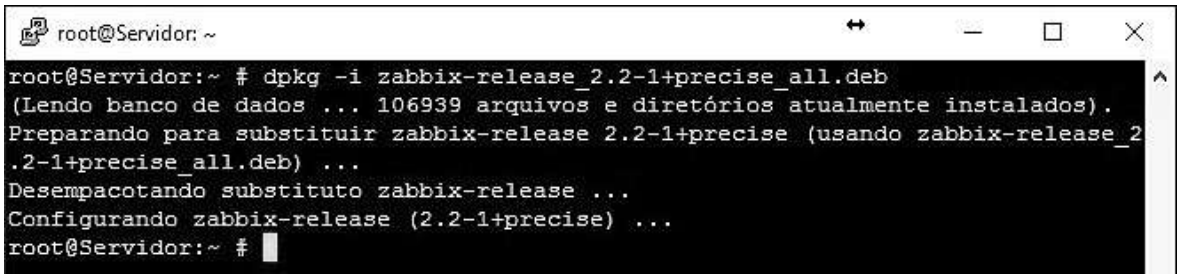
Execute o comando “dpkg -i zabbix-release_2.2-1+precise_all.deb”, conforme na Figura A 2, para instalar o pacote e em seguida atualize a lista de pacotes com “apt-get update”, ilustrado na Figura A 3.

Figura A 1: Download do pacote de configurações

Fonte: Autoria própria

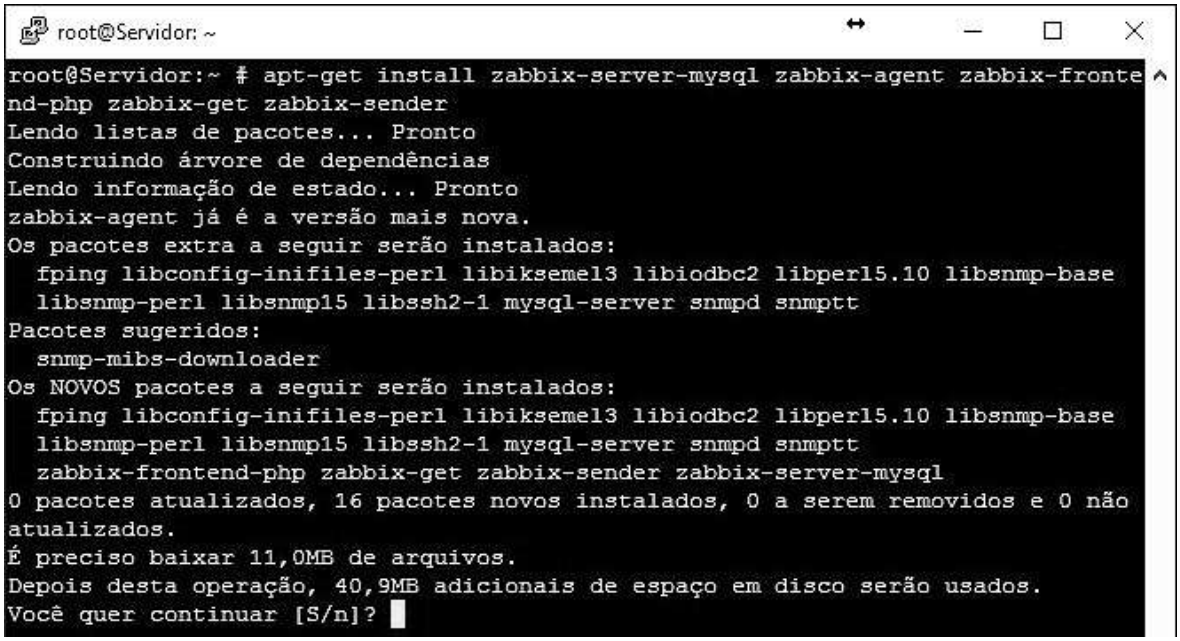
[9] https://www.youtube.com/watch?v=BekcRg21TYU
[10] http://zabbixbrasil.org/files/Tutorial_de_instalacao_do_Zabbix_Server_2-2_Hernandes_Martins.pdf

Figura A 2: Instalação do pacote



Fonte: Autoria própria

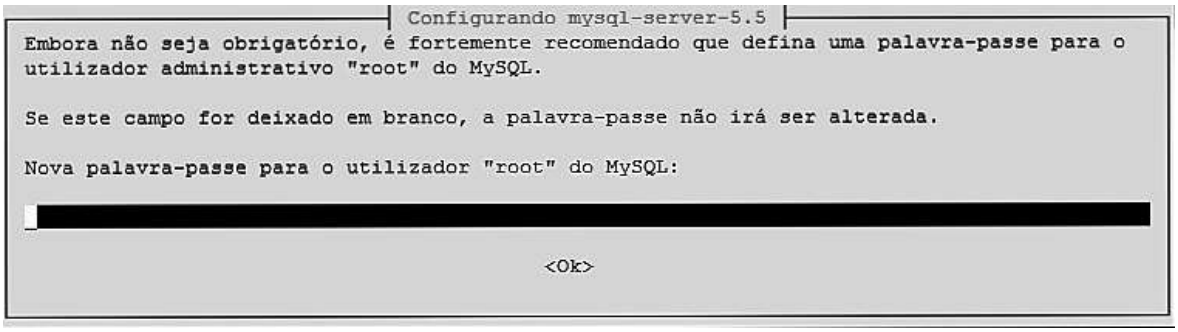
Figura A 3: Instalação do Zabbix



Fonte: Autoria própria

Durante o processo de instalação conforme na Figura A 3 será necessário criar e informar as senhas do banco de dados MySQL, conforme demonstrado na Figura A 4 neste caso foi utilizado à senha “123456”.

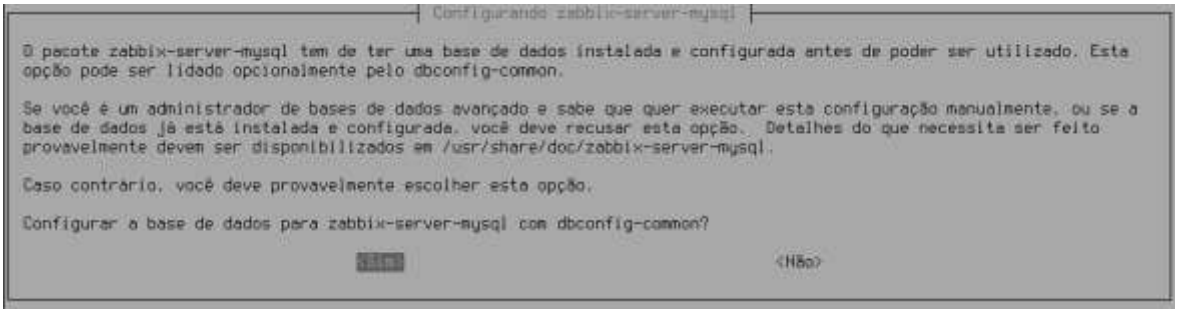
Figura A 4: Instalação do MySQL



Fonte: Autoria própria

Depois de instalado e configurado o MySQL surgirá uma pergunta “Configurar a base de dados para zabbix-server-mysql com dbconfig-common?”, selecione “<Sim>”, conforme ilustrado na Figura A 5 então será solicitada a senha root do MySQL, a mesma cadastrada anteriormente conforme na Figura A 4, após informada será solicitado para criar a senha para o Zabbix acessar o banco de dados MySQL, neste caso foi utilizado “123456” novamente.

Figura A 5: Configuração do usuário e senha do Zabbix no MySQL



Fonte: Autoria própria

Terminado o processo acima basta reiniciar o serviço web com o comando “service apache2 restart” e o Zabbix Server este instalado, sendo acessível com qualquer navegador utilizando o endereço “http://ip-do-servidor/zabbix”, uma tela de “Bem-vindo” será exibida, conforme Figura A 6 em seu primeiro acesso, algumas informações serão conferidas, será necessário fazer a conexão com o banco de dados MySQL, conforme exemplo na Figura A 7 com o usuário e senha cadastrados anteriormente, depois de inseridos os dados basta prosseguir até o último passo, conforme Figura A 8 após clicar no botão “*Finish*” a tela principal

será exibida, conforme mostrado na Figura A 9 que por padrão vem configurado com usuário “admin” e senha “zabbix”, conectado será exibida a tela principal conforme na Figura 8.

Figura A 6: Primeiro acesso ao Zabbix

Fonte: Autoria própria

Figura A 7: Conexão do Zabbix com o banco de dados MySQL

Fonte: autoria própria

Figura A 8: Instalação do Zabbix completa

Fonte: Autoria Própria

Figura A 9: Tela de conexão do Zabbix

Fonte: Autoria própria

APÊNDICE B – Instalação e configuração do Squid

O Squid foi instalado utilizando a mesma versão Linux que o Zabbix e sua instalação é muito simples, bastou executar uma linha de comando, “apt-get install squid”, depois de instalado tem que configurar as ACL de acordo com as políticas de acesso definidas pela empresa.

O controle de sites do governo será feito pela seguinte ACL “acl sites_gov dstdomain .gov.br”, redes sociais será “acl rede_social dstdomain .youtube.com .twitch.tv .meebo.com .facebook.com .facebook.com.br .vagalume.com.br”.

Com a configuração dos valores acordados na política nas ACL’s a configuração da liberação ou bloqueio será por meio do “http_access” e conforme descrito no item 3.3.3, a ordem influência no resultado, então para que todos os sites do governo não fossem bloqueados, deveriam estar antes de qualquer bloqueio, deixando a configuração da seguinte forma:

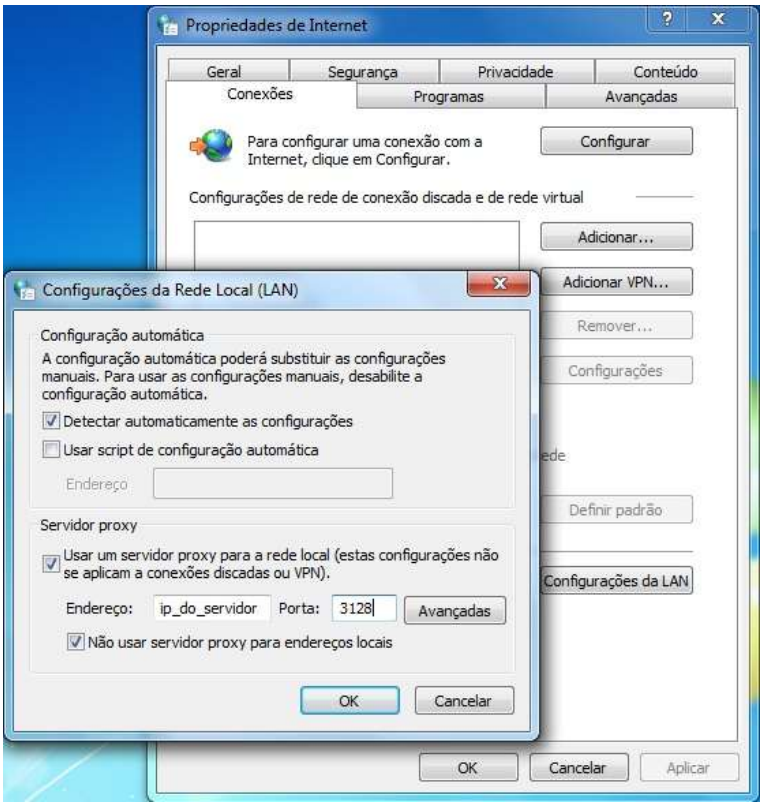
http_access allow all sites_gov

http_access allow all !rede_social

http_access deny all

Definidas as regras, configurada a sua execução, a próxima etapa é a configuração do Proxy nos micros dos usuários da rede, esta configuração precisa ser feita em cada micro, conforme Figura B 1: Configuração do Proxy no usuário fazendo com que toda requisição do usuário a uma página, seja solicitado ao servidor Proxy e ele deverá analisar se aquele endereço é ou não liberado, conforme explicado no item 3.1 e demonstrado na Figura 11.

Figura B 1: Configuração do Proxy no usuário



Fonte: Autoria própria