6 UM ESTUDO ESTATÍSTICO PARA DETECTAR PADRÕES E TENDÊNCIAS NO TRÁFEGO DE UMA REDE DE COMPUTADORES

Ana Nery dos Santos
Graduada em Engenharia de Computação (Faculdade Área 1- Wyden). Concluinte da Pós-graduação em Segurança da Informação. Atualmente trabalho na Prefeitura Municipal de Camaçari, coordenando o Museu de Ciência e Tecnologia - UNICA e Laboratório de Tecnologia de Camaçari - LABTEC. Docente e atuante no fomento da Inovação e Tecnológica regional da Bahia.
E-mail: ananerybahia3@gmail.com

Fábio Rodrigues Santos
Doutor em Modelagem Computacional e Tecnologia Industrial (SENAI/CIMATEC). Mestre em Matemática Pura (UFBA). Graduado em Licenciatura em Matemática (UFSC). Graduado em Bacharelado em Matemática (UFBA). Docente Instituto Federal da Bahia (IFBA/Camaçari).
E-mail: rfabio10@gmail.com

RESUMO

Atualmente a disputa econômica, entre países e empresas, cresce cada vez mais, num processo em que ocorre a difusão de culturas diferentes, hábitos de consumo, e outros costumes de países desenvolvidos que impõe suas marcas mundialmente conhecidas, interligando o mercado mundial. A necessidade de sistemas informatizados, armazenamento, distribuição e controle de informações são indispensáveis, a conectividade que hoje é assistida, através das redes interligadas. Os avanços tecnológicos têm proporcionado às empresas maior eficiência e rapidez na troca de informações e tomadas de decisões. É nesse contexto que esse artigo tem como objetivo analisar e identificar padrões e tendências encontrados em uma rede de computadores, utilizando a ferramenta MRTG para otimizar a infraestrutura de rede, eliminando problemas de desempenho, melhorando a qualidade e disponibilidade de serviço. Análises foram realizadas onde detectou-se anormalidades nos ativos Firewall e Switch, por meio da coleta dos dados, onde foram gerados gráficos que demonstraram falhas de segurança da rede. Também foram realizados estudos estatísticos no desempenho dos ativos, CPU e Memória, onde indicou-se condições favoráveis à sua utilização sem necessidade de procedimentos de intervenções.

Palavras-chave: Gerenciamento de Redes. Tecnologia. MRTG. Estatística.

ABSTRACT

Currently, an economic dispute, between countries and companies, grows more and more, in a process in which there is a diffusion of different cultures, consumption habits and other costumes of countries that affect their world famous brands, interconnecting or world market. The need for computerized systems, storage, distribution and control of information are indispensable, the connectivity that is currently assisted, through interconnected networks. Technological advances have provided companies with greater efficiency and speed in the exchange of information and decision making. It is in this context that this article aims to analyze and identify patterns and trends found in a computer network, using an MRTG tool to optimize a network infrastructure, eliminating performance problems, improving service quality and availability. Analyzes were performed where it detected abnormalities in the Firewall and Switch assets, through data collection, where graphics were generated that demonstrated security flaws in the network. Statistical studies on the performance of assets, CPU and Memory were also carried out, where the conditions indicated are favorable to their use without the need for application procedures.

Keywords: Networks Management. Technology. MRTG. Statistics.

6.1 INTRODUÇÃO

Atualmente a disputa econômica, entre países e empresas, cresce cada vez mais, num processo em que ocorre a difusão de culturas diferentes, hábitos de consumo, e outros costumes de países desenvolvidos que impõe suas marcas mundialmente conhecidas, interligando o mercado mundial. A necessidade de sistemas informatizados, armazenamento, distribuição e controle de informações são indispensáveis, a conectividade que hoje é assistida, através das redes de sociais, permitindo que cidadãos manifestem suas opiniões de maneiras que não eram possíveis anteriormente. Os avanços tecnológicos têm proporcionado às empresas maior eficiência e rapidez na troca de informações e tomadas de decisões, computadores mais rápidos são lançados em curto espaço de tempo. A Internet tem permitido a qualquer empresa praticar o comércio eletrônico, apresentando a um custo baixo, seus produtos para todas as pessoas do mundo inteiro (MOREIRA, 2001).

Com o passar do tempo, percebeu-se que o mercado mundial estava se tornando cada vez mais exigente e competitivo, surgindo a necessidade do uso da Tecnologia da Informação, as empresas começaram a investir de forma agressiva em hardware, software, telecomunicações e banco de dados, esses elementos compõem o que chamamos de infraestrutura de Tecnologia da Informação (TI), e devido a necessidade de trâmite de informação nas redes de computadores, percebeu-se a necessidade de monitorar, gerenciar e controlar esses recursos. Para Fontes (2000) a informação é um bem da organização, e como tal deve ser gerenciado, protegido, possuir regras e políticas de utilização. A medida em que a informação está armazenada no ambiente computacional, ela é cada vez mais necessária para a realização e lucro dos negócios. O Gerenciamento de Rede é essencial dentro da estrutura de uma empresa. Cada vez mais as empresas são dependentes de computadores para a execução de suas atividades, por menor e mais simples que seja uma rede de computadores. Vale aqui mencionar duas importantes redes: Local Área Network (LAN), que são pequenas redes e Wide Area Network (WAN), que são grandes redes distribuídas, tendo a necessidade de definir e manter a proteção diante das ameaças internas e externas garantindo confidencialidade, integridade disponibilidade e autenticidade. À medida que a rede cresce, aumenta-se a complexidade de seu gerenciamento, surgindo a necessidade de ferramentas automatizadas que auxiliem o monitoramento e controle dessa infraestrutura. É neste contexto, que esta pesquisa visa investigar o desempenho de uma rede utilizando a ferramenta *Multi Router Traffic Grapher* (MRTG) que é um software livre (*open source),* para monitorar e controlar através do protocolo *Simple Network Management Protocol*(SNMP) que permite aos administradores da rede gerir

os equipamentos e diagnosticar os problemas existentes. Uma investigação estatística é realizada com o propósito de detectar padrões e tendências no tráfego da rede, indicando possíveis condições anormais de sua infraestrutura, demonstradas através dos gráficos que são refletidos em operações não desejada na rede.

Este artigo está dividido em uma introdução, revisão da literatura, metodologia, resultados e discussões, conclusão e referências.

6.2 REVISÃO DA LITERATURA

6.2.1 Gerenciamento de redes

Nos dias atuais a gerência de redes tornou-se cada vez mais necessária devido ao aumento da utilização das redes de computadores, a integração dos recursos tecnológicos, desde a rede mais simples, como a mais complexa, sendo necessário controlar e monitorar a rede. A heterogeneidade de padrões, sistemas operacionais, equipamentos e outros serviços, requer informações da rede, bem como o tratamento destas informações, para que seja possível se obter um diagnóstico do ambiente da rede, no intuito prevenir e solucionar problemas. Para gerenciar esses recursos, é necessário ferramentas que auxiliem no controle das atividades. A maioria das ferramentas disponíveis para monitoramento de rede são baseadas no conceito do *Multi Router Traffic Grapher* (MRTG) devido a utilização do protocolo SNMP (*Simple Network Management Protocol*) definida na seção 6.2.3.1.

Pode-se destacar as principais áreas de gerenciamento de redes, proposta pela International Organization for Standardization (ISO):

- Gerenciamento de configuração
- Gerenciamento de contabilização
- Gerenciamento de desempenho
- Gerenciamento de falhas
- Gerenciamento de segurança

Gerenciamento de segurança: Proteger os objetos gerenciados, propor uma política de segurança robusta e efetiva, garantindo que o sistema de gerenciamento de segurança seja seguro, controlando os acessos da rede de acordo com a política definida.

Gerenciamento de contabilização: Permitem que os recursos estabeleçam taxas para o uso dos objetos gerenciados e identifiquem os custos para uso desses objetos gerenciados. O

administrador da rede deve estar habilitado para controlar o uso dos recursos por usuário ou grupo de usuários, evitando o mesmo abuse de seus privilégios de acesso.

Gerenciamento de falhas: O objetivo do gerenciamento de falhas é registrar, detectar e reagir às condições de falha de rede.

Gerenciamento de configuração: Alguns recursos podem ser configurados para executar diferentes serviços, gerando relatórios de configuração, que são gerados periodicamente ou em resposta às requisições de usuários, atualizando ou modificando os recursos de rede.

Gerenciamento de desempenho: Monitoração das atividades da rede, controle dos recursos através de ajustes e trocas. Verificação do tráfego excessivo, tempo de resposta, quantificar, medir, informar, analisar e controlar o desempenho, garantindo que a rede opere em conformidade e qualidade, são algumas características, do gerenciamento de desempenho.

6.2.2 Ferramentas de gerenciamento

Um sistema de gerência de rede pode ser definido como uma coleção de ferramentas integradas para a monitoração e controle da rede. Essas ferramentas de gerenciamento auxiliam na gestão da rede, garantindo uma melhor qualidade dos seus serviços. Os sistemas oferecem interface única com informações sobre a rede e pode oferecer também um conjunto poderoso e amigável de comandos que são usados para executar quase todas as tarefas da gerência da rede (STALLINGS, 1998).

6.2.3 A infraestrutura do gerenciamento de redes

Um dispositivo gerenciado é um nó de rede que possui um agente SNMP instalado e se encontra em uma rede gerenciada. Estes dispositivos coletam e armazenam informações de gerenciamento e mantém estas informações disponíveis para sistemas Network Management Systems (NMS) através do protocolo SNMP. Dispositivos gerenciados, também às vezes denominados de dispositivos de rede (COMER, 2006).

Podemos observar na Figura 1 uma entidade gerenciadora, objeto gerenciado e um protocolo de gerenciamento de rede. Esses a componentes conceitualmente formam uma arquitetura de gerenciamento. A comunicação entre o gerente e as aplicações são possíveis através da utilização das (API) *Application Program Interface*, que é conjunto de funções que fazem o intermédio na execução de comandos entre um programa.

Figura 1 - Mensagens em um Protocolo de Gerência de Redes

Fonte: KUROSE; ROSS, 2010.

Para que ocorra a troca de informações entre gerente e agentes, é necessário que eles falem a mesma linguagem, essa interpretação é o protocolo de gerência que permite operações de monitoramento (leitura) e controle (escrita).

Gerentes e agentes podem trocar informações, mas não qualquer tipo de informação. As informações de gerência definem os dados que podem ser referenciados em operações do protocolo de gerência, isto é, dados sobre os quais gerente e agente conversam. Podemos destacar quatro componentes básicos da arquitetura geral dos sistemas de gerência de redes, sendo eles: elementos gerenciados; estações de gerência; protocolos de gerência e informações de gerência.

Definição: **Gerente** é uma entidade gerenciada que pode obter informações atualizadas sobre objetos gerenciados e controlá-los. Com este objetivo, o gerente transmite operações de gerenciamento aos agentes. Controla a coleta, o processamento, a análise e/ou a apresentação de informações de gerenciamento de rede.

Definição: **Agente** é o responsável pela execução de gerenciamento sobre objetos gerenciados. O agente também tem possibilidade de transmitir ao gerente as notificações emitidas pelos objetos gerenciados, ou seja, um agente tem o conhecimento das informações de gerenciamento locais e traduzem estas informações para um formato compatível com o protocolo SNMP.

Definição: **Objeto Gerenciado** é a entidade que representa um recurso que poderá ser gerenciado. Um dispositivo gerenciado pode ser um hardware, software, serviços de redes, como por exemplo, um roteador, uma ponte, um switch, uma impressora ou um modem. Esses objetos gerenciados têm informações associadas a eles que são coletadas dentro de uma Base de Informações de Gerenciamento.

6.2.3.1 Protocolo SNMP

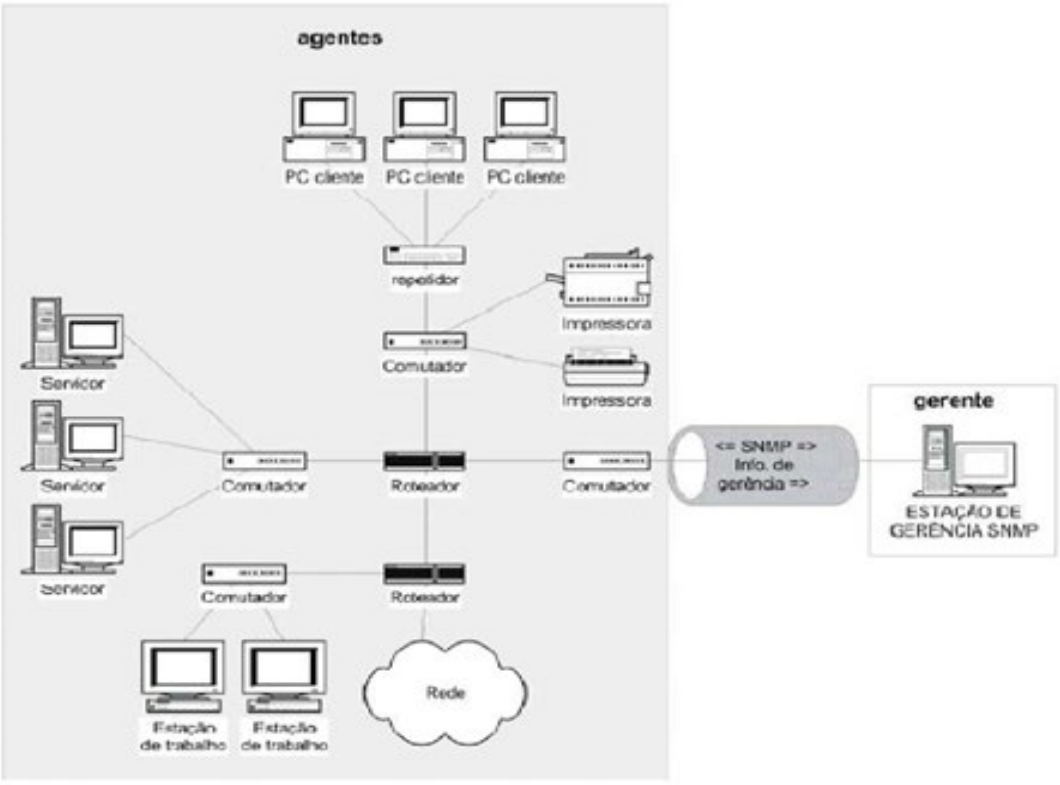
Um dos objetivos da gerência de redes é prevenir e solucionar problemas, o *Simple Network Management Protocol* (SNMP) é a estrutura do gerenciamento de rede mais amplamente usada e disseminada na rede. É um protocolo de gerência típica de redes *Transmission Control Protocol* / Internet Protocol (TCP/IP), da camada de aplicação que facilita o intercâmbio de informações, entre os dispositivos de rede, onde utiliza informações dos agentes que se encontram em uma rede TCP/IP, utiliza o protocolo *User Datagram Protocol* (UDP), para enviar mensagens da rede, onde os gerentes enviam requisições a seus agentes para obtenção dos dados (STALLINGS, 2005).

Dentro da Arquitetura de gerenciamento SNMP encontramos o modelo do gerenciamento de rede que é usado para o SNMP que inclui os seguintes elementos chaves:

- Estação de gerenciamento, ou gerenciador;
- Agente;
- Base de informações de gerenciamento;
- Protocolo de gerenciamento de rede.

Podemos observar na Figura 2 em que cada dispositivo gerenciado um agente de gerenciamento de rede, um processo que é executado no dispositivo gerenciado, que se comunica com a entidade gerenciadora e que executa ações locais nos dispositivos gerenciados sob o comando e o controle da entidade gerenciadora.

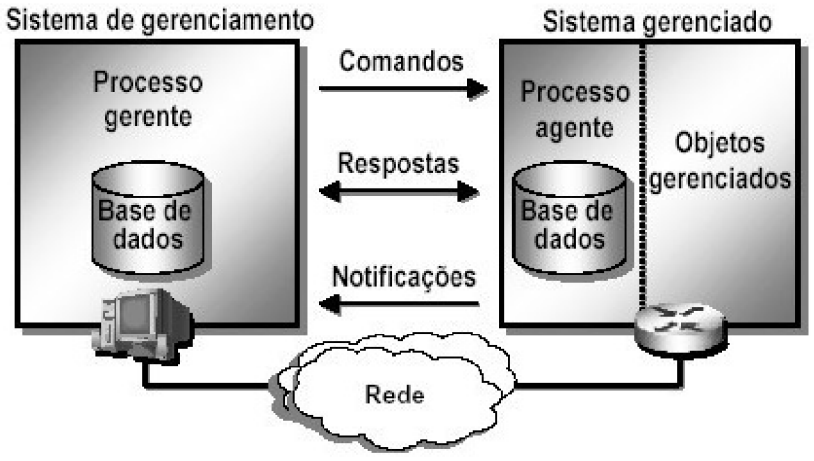
Figura 2 - Imagem esquemática de gerenciamento de redes



Fonte: COSTA, 2008.

O gerenciamento da rede através do protocolo SNMP permite o acompanhamento em tempo real, da rede, podendo ser utilizado para gerenciar hardware e software. Por tanto, o SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB (*Management Information Base*) e a aplicação de gerência como também é o nome desta solução de gerência.

Figura 3 - Modelo do protocolo SNMP



Fonte: PORTUGAL, 2006.

Podemos observar na Figura 3 o SNMP é o nome do protocolo no qual as informações são trocadas entre a MIB e a aplicação de gerência como também é o nome deste modelo de gerência. O protocolo SNMP fornece uma base de objetos gerenciados (MIB) que procuram abranger todas as informações necessárias para a gerência da rede (PORTUGAL, 2006).

6.2.3.2 MIB *(MANAGEMENT INFORMATION BASE)*

O conjunto de todas as informações expostas por um elemento de rede é chamado de MIB do elemento de rede, ou seja, é o modelo conceitual que contém informações sobre o elemento gerenciado, ou seja, procura obter todas as informações necessárias para a gerência da rede.

Essa base de informação gerencial que é um conjunto de objetos gerenciados definidos segundo um padrão estruturados em grupos hierárquicos, na qual coleta informações necessárias para o gerenciamento da rede baseada nas regras do SMI (*Structure of Management Information*). O SNMP Utiliza uma linguagem para definição da MIB, conceitualmente, a MIB é independente de protocolo.

Os objetos gerenciados possuem um valor que representa o estado de um objeto real em um determinado instante. Muito esforço é empregado no desenvolvimento de uma MIB/Agente, portanto ela deve ser estável ao longo do tempo, entretanto, podemos destacar que a MIB é um contrato entre agente e aplicações de gerenciamento. Na sua arquitetura o monitoramento da rede, primeiramente é necessário que o agente esteja ativo no equipamento gerenciado para que seja possível a obtenção dos valores da MIB II via SNMP (PORTUGAL, 2006).

A seguir apresenta-se as principais funcionalidades da MIB:

- Checar a abrangência do sistema de gerenciamento ou operações de infraestrutura suportadas;
- Categorizar e agrupar funções diferentes;
- Identificar casos de uso e cenários a serem analisados para verificar a interdependência entre diferentes tarefas e suas interfaces.
- Estabelecer uma terminologia comum entre agente e gerente;
- Nome da informação gerenciada e seu tipo;
- Nomenclatura utilizada para cada instância desta informação;
- Mantida pelo agente (equipamento);
- Organizada como Objetos Gerenciáveis: *Management Objects* (MO).

6.3 METODOLOGIA

Para Marconi (1999, p. 29) a caracterização do problema define e identifica o assunto em estudo, ou seja, um problema muito abrangente torna a pesquisa mais complexa. Quando bem delimitado, simplifica e facilita a maneira de conduzir a investigação. Neste artigo foi realizado uma pesquisa bibliográfica, buscando informações em livros, apostilas, artigos e material disponibilizado na internet. Os dados experimentais foram extraídos do Laboratório de Tecnologia de Camaçari (LABTEC), vinculado ao Museu UNICA, pertencente a Secretaria de Cultura de Camaçari. a fim de detalhar o conhecimento da ferramenta de monitoramento MRTG definida na seção 3.1.

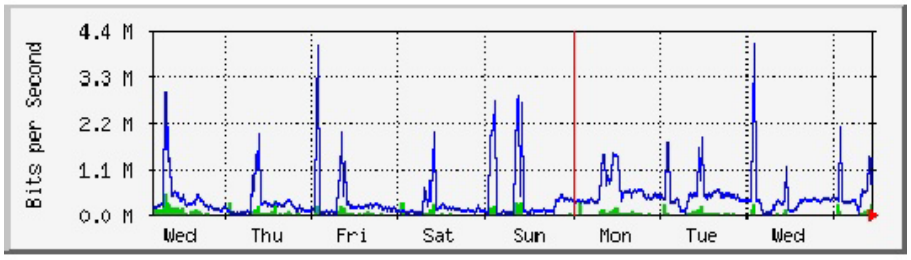
6.3.1 MRTG (*MULTI ROUTER TRAFFIC GRAPHER*)

O MRTG é um software livre com sua distribuição aberta, licenciado sob a GNU *General Public License* (GPL) (MRTG, 2018). Que tem como proposta, auxiliar os administradores no monitoramento do tráfego, bem como verificar desempenho dos hardwares, através das coletas dos dados. Também é possível verificar o tempo de paralisação dos dispositivos numa rede. Essa ferramenta gera páginas *HyperText Markup Language*(HTML) contendo imagens gráficas que possibilitam uma apresentação do estado real deste tráfego. Baseado na linguagem de programação Perl e C, a ferramenta faz a coleta dos dados via protocolo SNMP ou script, podendo monitorar qualquer equipamento que ofereça o suporte a este protocolo ou script.

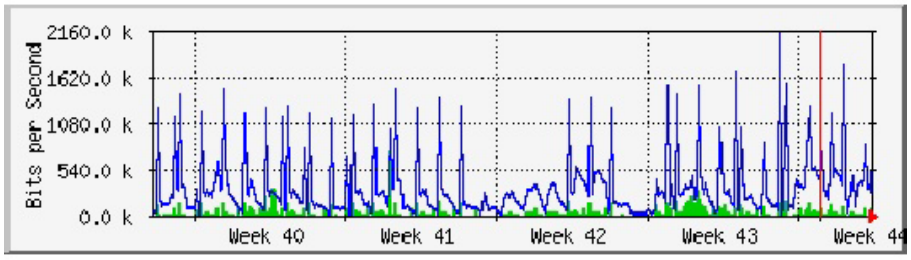
Essa ferramenta fornece gráficos que podem ser visualizados através de qualquer navegador web, sendo possível monitorar mais de 100 links de rede de quaisquer dispositivos que oferecem suporte ao protocolo SNMP ou scripts. Acumular duas ou mais fontes de dados em um único gráfico, enviar e-mails para os administradores da rede fornecendo informações pré-estabelecidas, e desempenho dos dispositivos monitorados são algumas das características do MRTG.

É possível monitorar diversos tipos de dispositivos, como: Servidores Web, DHCP, de Impressão, DNS, E-mail, de Arquivos; Firewall; Roteadores; Switch; Quantidade de bits que entram e saem de uma interface; Quantidade de pacotes que entram e saem de uma interface; Utilização de uma CPU(*Central Processing Unit*); Estado do enlace físico de uma interface e Utilização da memória. Na Figura 4, verifica-se alguns exemplos construídos pelo MRTG.

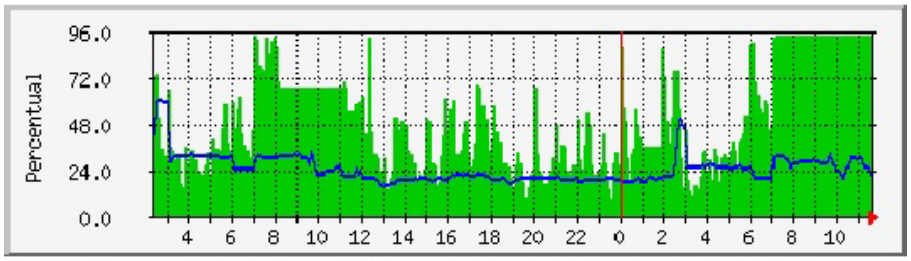
Figura 4 - Imagem ilustrativa gerada pelo MRTG



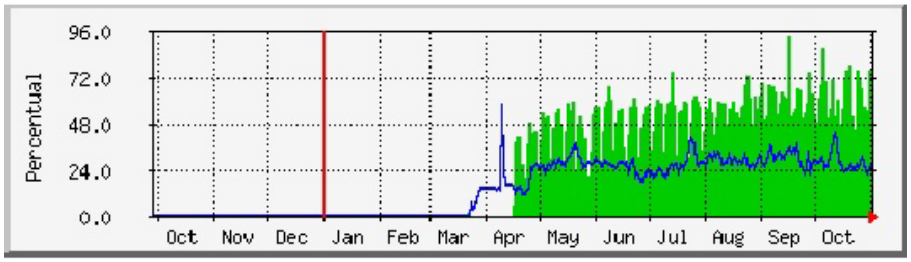
(Uso da Placa de rede na semana, em verde: tráfego recebido. Em azul: tráfego enviado)



(Uso da Placa de rede no mês, em verde: tráfego recebido. Em azul: tráfego enviado)



(Uso da Memória e CPU nas últimas 24hs, em verde: CPU ocupada. Em azul: memória ocupada)



(Uso da Memória e CPU no ano, em verde: CPU ocupada. Em azul: memória ocupada)

Fonte: SCRIBD, 2005.

O monitoramento e status dos equipamentos da rede é feito através da variável SNMP ou scripts, com base na leitura das MIBs, pode-se citar alguns exemplos, como memória, CPU, disco, fabricante, contato, versão etc. Essa leitura é possível, porque cada dispositivo tem uma MIB com suas informações.

6.3.2 Vantagens do MRTG

- Faz o uso SNMP para coletar os dados ou por meio de script.
- Geram gráficos e dos ativos da rede.
- Medição de dois valores, no caso de tráfego, podem ser entradas e saída.
- Coleta de dados a cada 5 minutos por padrão, mas o tempo pode ser modificado.
- Geram gráficos através de páginas em HTML para visualização (diário, mensal, semanal e anual).
- Medição de dois valores, no caso de tráfego, podem ser entrada e saída.
- Configuração através de arquivos de texto.
- O MRTG pode avisar caso o gráfico atinja um valor preestabelecido, através do envio de e-mail para o administrador informando o ocorrido.
- Coleta de dados a cada 5 minutos por padrão, mas o tempo pode ser aumentado.
- Utilização da ferramenta para gerar uma página de índice para os casos em que muitos itens são monitorados: INDEXMAKER
- Utilização da ferramenta para gerar os arquivos de configuração CFGMAKER

O monitoramento de uma rede local com o uso desta ferramenta nos permite uma análise de como anda o tráfego da rede, por meio os dados coletados, como desempenho, falhas, estatísticas, possibilitando a análise e gerenciamento da rede, contribuindo para um planejamento de ações que otimizem tanto na performance como na segurança e crescimento da rede.

6.3.3 Metodologia experimental por meio da ferramenta MRTG

Como vimos na seção 6.2.1, importância do gerenciamento de redes, monitorar, administrar e controlar os ativos da rede não é uma tarefa nada fácil para o administrador de rede. Com isso recomenda se a utilização de um sistema de gerenciamento inteligente de monitoramento de redes. Após realizar várias pesquisas no intuito de encontrar ferramentas de fácil configuração e instalação, o MRTG foi escolhido por diversas características que forma aqui esplanadas além de ter um ambiente amigável, gratuito e difundido no mercado.

6.3.3.1 Implantação

A instalação foi realizada no computador com a distribuição de código aberto do Linux, CentOS 6.3 onde foi configurado como sendo servidor de monitoramento. Feito a instalação e configuração foi realizado testes de monitoramento e desempenho dos seguintes os ativos da rede: Switch, Firewall, CPU e Memória. Entendesse como ativos dispositivos gerenciados ou monitorados que possui um agente SNMP instalado e se encontra na rede gerenciada.

Análise dos experimentos:

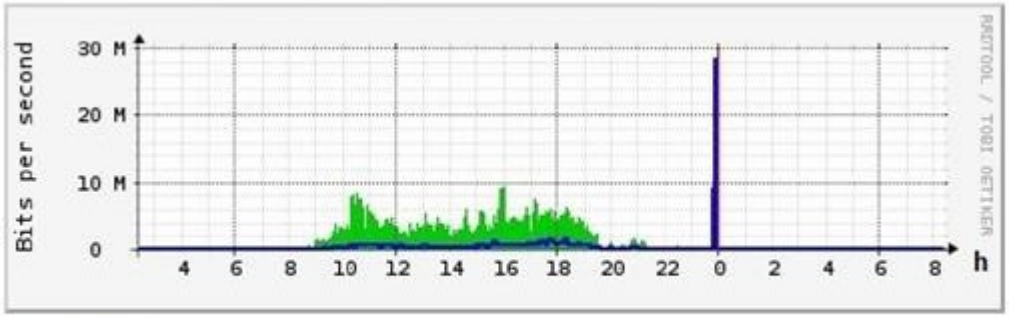
- Análise de monitoramento de cargas: Firewall e Switch.
- Análise de desempenho: CPU e Memória.

6.4 RESULTADOS

A importância da gerência de redes, desde a rede mais simples como a mais complexa, o administrador tem que estar atento ao que está acontecendo na sua infraestrutura, para tal as ferramentas de monitoramento é de grande importância para um melhor desempenho e maior segurança da rede.

A seguir serão realizadas as análises estatísticas em busca de identificar padrões e tendências que reflitam irregularidades ou falhas na utilização da rede.

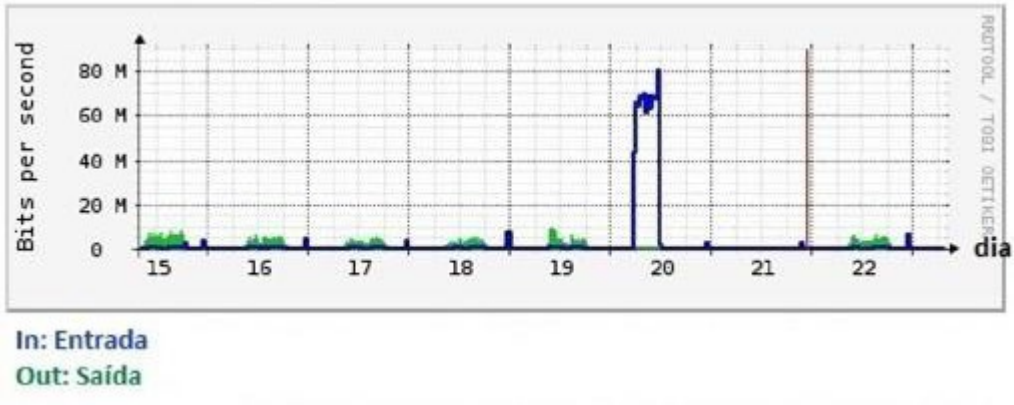
Figura 5 - MRTG monitorando o tráfego diário do Firewall



A Figura 5 ilustra o monitoramento diário do Firewall sobre a quantidade de bits e pacotes que entram e saem da interface, tendo o gráfico diário traçado a cada 5 minutos e possui abscissa com aproximadamente 24 horas. Podemos observar um fluxo de entrada estável,

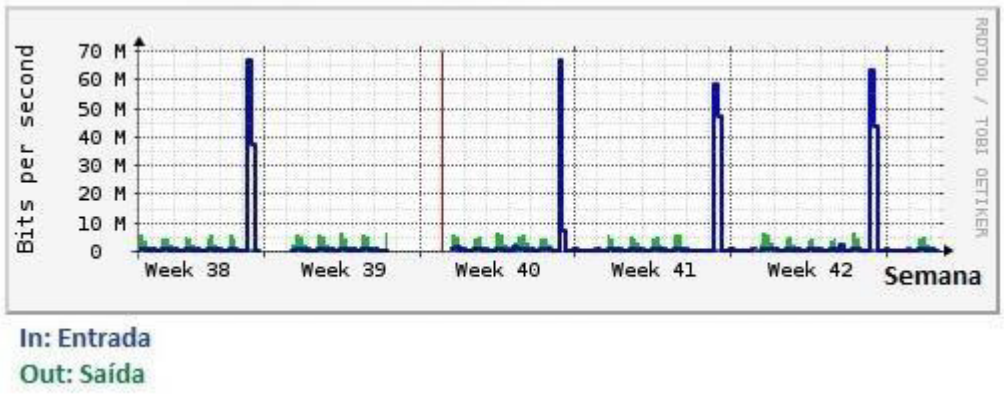
apresentando uma discrepância às 00:00h, neste dia, enquanto a demanda de saída apresenta uma variação em torno de 10M (megas) aceitável para o horário comum ao expediente.

Figura 6 - MRTG monitorando o tráfego semanal do Firewall



A Figura 6 ilustra o monitoramento semanal do firewall sobre a quantidade de bits e pacotes que entram e saem da interface tendo o gráfico semanal traçado a cada 30 minutos possuindo uma abscissa com aproximadamente oito dias. Podemos observar no gráfico que no dia 20 foi constatado um pico anormal do tráfego da rede na entrada em relação aos outros dias. Desta forma alertou-se para tamanha discrepância. A partir daí foi necessário utilizar uma ferramenta de controles de acessos, o SQUID, que tem como característica armazenar páginas da Web e arquivos (FTP) *File Transfer Protocol*, constatando a utilização da rede para acessar plataformas de serviços streaming. O fluxo de saída mostrou-se aceitável em conformidade à análise da Figura 5.

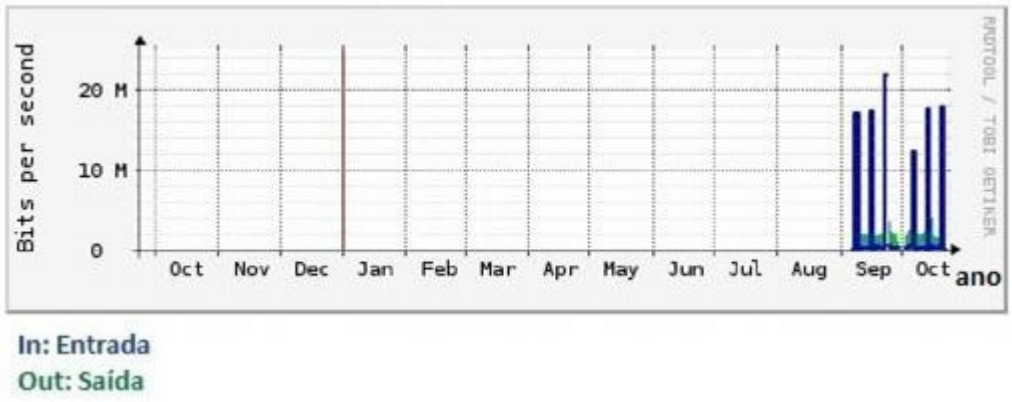
Figura 7 - MRTG monitorando o tráfego mensal do firewall



A Figura 7 ilustra o monitoramento mensal do firewall sobre a quantidade de bits e pacotes que entram e saem da interface, tendo o gráfico mensal traçado a cada 2 horas e possui

abscissa com aproximadamente cinco semanas. Observa-se no gráfico que foi constatado eventos anormais na entrada de dados em dois dias específicos nas semanas, em quatro semana das cinco de realização das leituras. Permanecendo sem discrepância na saída de dados conforme as análises anteriores.

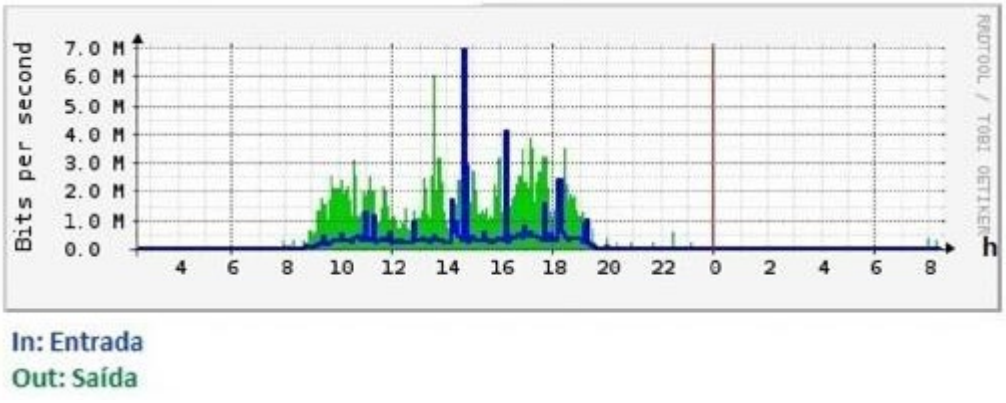
Figura 8 - MRTG monitorando o tráfego mensal do firewall



A Figura 8 ilustra o monitoramento anual do firewall sobre a quantidade de bits e pacotes que entram e saem da interface, tendo o gráfico anual traçado a cada um dia, e possuindo abscissas com aproximadamente um ano. Observa-se neste gráfico que o monitoramento anual evidencia a eficácia da ferramenta nesta análise a partir do mês de setembro, período onde se deu a implantação do MRTG. Nesta investigação, persiste as discrepâncias das entradas de dados detectadas nas investigações anteriores.

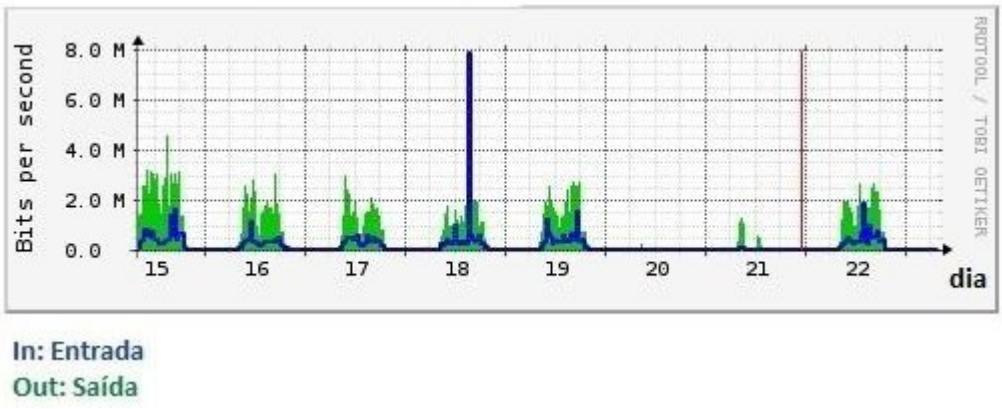
A seguir é mostrado o estudo estatístico através do dispositivo switch.

Figura 9 - MRTG monitorando o tráfego diário do switch



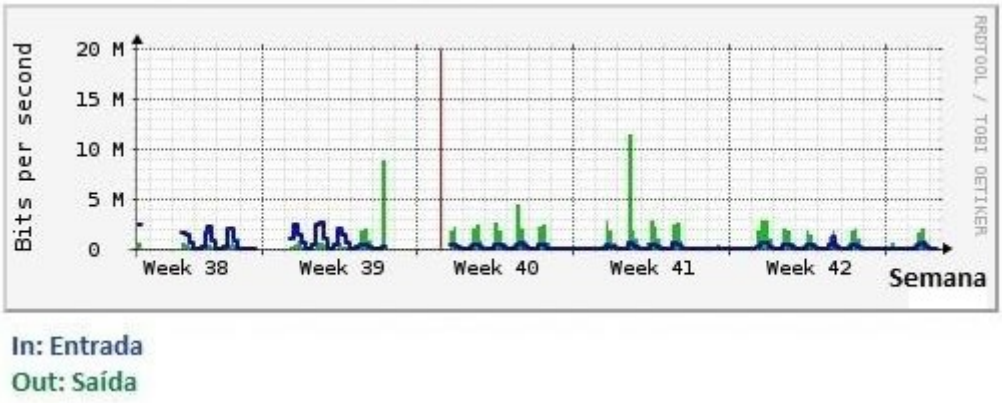
A Figura 9 ilustra o monitoramento diário do switch sobre a quantidade de bits e pacotes que entram e saem da interface, tendo o gráfico diário traçado a cada 5 minutos e possui abscissa com aproximadamente 24 horas. Observa-se que em alguns momentos o tráfego do switch aumenta de forma anormal. Ao verificar o que estava acontecendo na rede, através da ferramenta de controles de acessos, SQUID, foi constatado o uso indevido da rede para realizar downloads em sites que não estavam em lista de bloqueio. Já o fluxo de saída apresentou um comportamento satisfatório do uso da rede, no período das 08:00h às 20:00h, conforme com o período de expediente.

Figura 10 - MRTG monitorando o tráfego semanal do switch



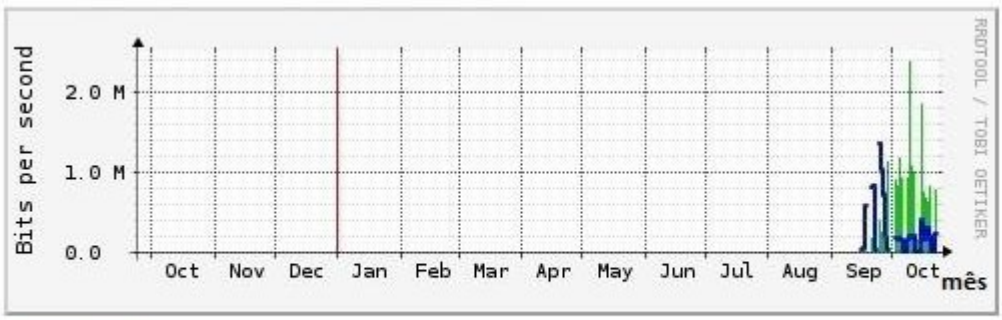
A Figura 10 ilustra o monitoramento semanal do switch sobre a quantidade de bits e pacotes que entram e saem da interface, tendo o gráfico semanal é traçado a cada 30 minutos e possui abscissa com aproximadamente oito dias. Nesta análise, no dia 18 indica a utilização indevida da rede pelo usuário, persistente a entrada de dados.

Figura 11 - MRTG monitorando o tráfego mensal do switch



A Figura 11 ilustra o monitoramento mensal do switch sobre a quantidade de bits e pacotes que entram e saem da interface tendo o gráfico mensal traçado a cada 2 horas e possui abscissa com aproximadamente cinco semanas. Neste gráfico detectou-se um padrão para o uso da rede para entrada e saída de dados, não indicando inconformidades expressivas.

Figura 12 - MRTG monitorando o tráfego anual do switch

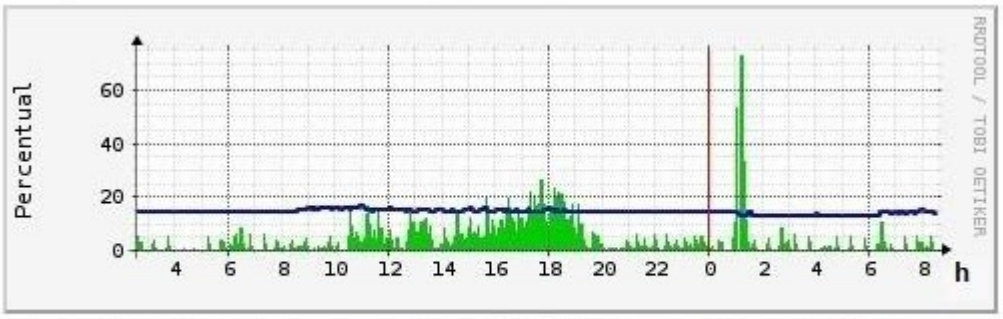


In: Entrada
Out: Saída

A Figura 12 ilustra o monitoramento anual do switch sobre a quantidade de bits e pacotes que entram e saem da interface tendo o gráfico anual traçado a cada um dia e possui abscissa com aproximadamente um ano. Neste gráfico, o monitoramento começa em setembro, período este de implantação da ferramenta. Indicando também a eficácia do MRTG para este ativo.

Os gráficos seguintes mostram o monitorado sobre os registros dos históricos do uso da CPU e memória do servidor.

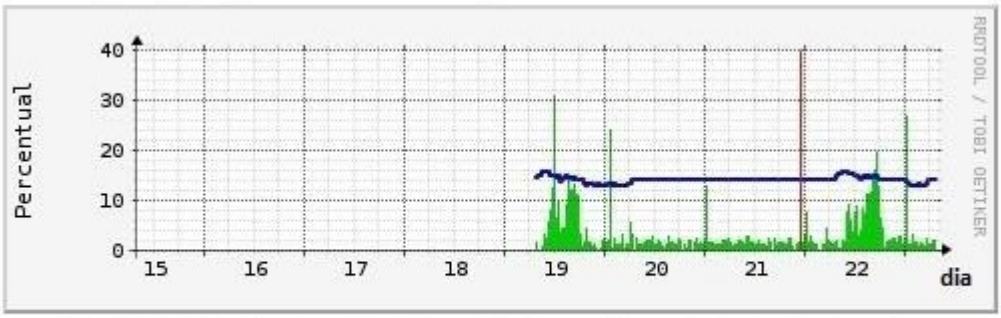
Figura 13 - MRTG monitorando o desempenho diário da CPU e memória



Max CPU 72.7 % (72.7%) Average CPU 4.4 % (4.4%) Current CPU 0.1 % (0.1%)
Max Mem 16.2 % (16.2%) Average Mem 14.1 % (14.1%) Current Mem 13.8 % (13.8%)

A Figura 13 ilustra o monitoramento diário de desempenho do CPU e memória, onde o gráfico diário é traçado a cada 5 minutos e possui abscissa com aproximadamente 24 horas. A memória apresenta baixa variação entre as medidas máxima, média e instantânea indicando um comportamento satisfatório de uso abaixo de 20%. Segue o mesmo comportamento para CPU, tendo uma exigência maior entre 10:00h e 20:00h. Entre as 00:00h e 02:00h percebeu-se um pico na utilização da CPU onde foi indicado, após verificação, que era o horário de realização do backup no servidor.

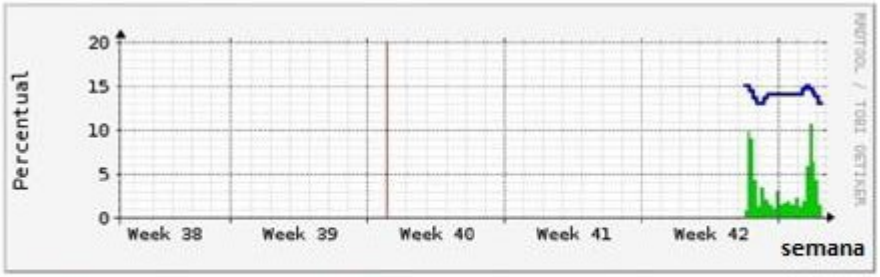
Figura 14: MRTG monitorando o desempenho semanal da CPU e memória



Max CPU 30.6 % (30.6%) Average CPU 3.3 % (3.3%) Current CPU 1.7 % (1.7%)
Max Mem 15.8 % (15.8%) Average Mem 14.0 % (14.0%) Current Mem 14.0 % (14.0%)

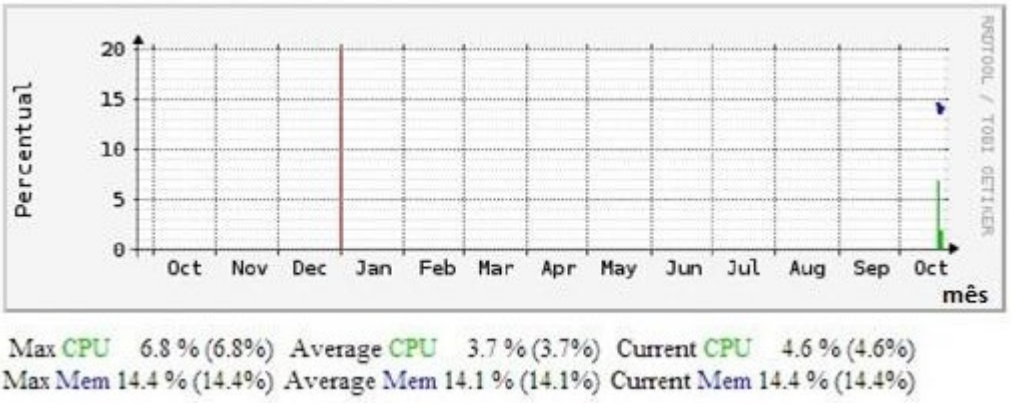
A Figura 14 ilustra o monitoramento semanal do desempenho da CPU/Memória onde o gráfico é traçado a cada 30 minutos e possui abscissa com aproximadamente oito dias. Neste gráfico, persistiu de forma análoga as mesmas conclusões estatísticas representadas pela Figura 13, a partir do dia 19, período este de início de implantação da ferramenta.

Figura 15 - MRTG monitorando o desempenho mensal da CPU e memória, traçado a cada 2 horas e possui abscissa com aproximadamente cinco semanas



Max CPU 10.5 % (10.5%) Average CPU 3.2 % (3.2%) Current CPU 1.6 % (1.6%)
Max Mem 15.1 % (15.1%) Average Mem 14.0 % (14.0%) Current Mem 13.7 % (13.7%)

Figura 16 - MRTG monitorando o desempenho anual da CPU e memória, traçados a cada um dia e possui abscissa com aproximadamente um ano



As Figuras 15 e 16, indicam um funcionamento também satisfatório para memória e CPU. Na figura 16, percebeu-se uma influência modesta destes parâmetros apenas no mês de outubro, mês este de implantação do MRTG para tais ativos.

6.5 CONSIDERAÇÕES FINAIS

O MRTG obteve um resultado satisfatório de acordo com o gerenciamento de rede, que tem como um dos objetivos utilizar ferramentas inteligentes, capazes de monitorar, administrar e controlar a rede, melhorando disponibilidade, segurança e desempenho da infraestrutura. Após análises foram detectadas anormalidades nos ativos (Firewall, Switch), por meio da coleta dos dados, onde foram gerados gráficos que demonstraram falhas na segurança da rede.

Na Figura 6, constatou-se no dia 20 um pico anormal do tráfego da rede na entrada em relação aos outros dias, o que indicou uma utilização não autorizada na rede para acessar plataformas de serviços streaming, persistindo a mesma tendência em uma investigação mais refinada em um dia (às 00:00h) como mostra a Figura 5. A Figura 7, mostrou o mesmo evento anormal na entrada em quatro semanas das cinco analisadas, todavia, refletindo na utilização indevida da rede em repetidas semanas, dias e horários.

As Figura 9 e Figura 10 indicam a utilização indevida da rede pelo usuário, persistente a entrada de dados, em dia e horários específicos, o que foi possível identificar a causa e local de onde originou-se tais tendências indevidas. Já o monitorando do desempenho da CPU e da memória nas Figuras 13, 14, 15 e 16 mostraram padrões e tendência favoráveis a sua utilização no servidor, não indicando nenhum tipo de problema que necessitasse de procedimentos de intervenção.

Conclui-se assim que a ferramenta MRTG é bastante satisfatória para análises em monitoramento, carga de tráfegos, medição de valores e layout gráficos. para detecção de padrões e tendências em redes de computadores, sendo possível encontrar soluções de problemas com maior eficiência.

REFERÊNCIAS

COMER, D. E. **Interligação de redes com TCP/IP**. 1. ed. [S.l.: s.n.], 2006.

COSTA, F. **Ambiente de redes monitorados com nagios e cacti.** 1. ed. [S.l.]: Ciência Moderna Ltda, 2008.

FONTES, E. **Vivendo a segurança da informação? Orientações práticas para pessoas e organizações.** 1. ed. [S.l.]: Sicurezza, 2000.

KUROSE, J.; ROSS, K. **Redes de computadores e a internet**: uma abordagem top-down. [s.n.], 2010. ISBN 9788588639973. Disponível em: http://books.google.com.br/books?id=raZtQwAACAAJ. Acesso em: 26 jun. 2020.

MARCONI, M. d. A. **Técnicas de pesquisa.** 1. ed. [S.l.]: Atlas S.A, 1999.

MOREIRA, N. S. **Segurança mínima**: uma visão corporativa da segurança de informações. [S.l.]: Axcel Books do Brasil, 2001.

MRTG. **MRTG** site oficial. 2018. Disponível em: https://oss.oetiker.ch/mrtg/. Acesso em: 26 jun. 2020.

PORTUGAL, A. G. **DFAPrognósticos**: um software para medir correlacões de longo alcance dos acordos de níveis de serviços baseados na análise de flutuação sem tendências. Dissertação (Mestrado Interdisciplinar em Modelagem Computacional) - Fundação Visconde de Cairu, Salvador, 2006.

STALLINGS, W. **Redes e sistemas de comunicação de dados.** Elsevier, 2005. Disponível em: http://books.google.com.br/books?id=fw9rAAAACAAJ. Acesso em: 26 jun. 2020.

_____. **SNMP, SNMPv2, SNMPv3 and RMON1 and 2.** 3. ed. [S.l.]: Addison Wesley, 1998.

MINI CURRÍCULO E CONTRIBUIÇÕES AUTORES

TITULO DO ARTIGO	**UM ESTUDO ESTATÍSTICO PARA DETECTAR PADRÕES E TENDÊNCIAS NO TRÁFEGO DE UMA REDE DE COMPUTADORES**
RECEBIDO	01/07/2020
AVALIADO	24/07/2020
ACEITO	24/07/2020

AUTOR 1	
PRONOME DE TRATAMENTO	Sra.
NOME COMPLETO	Ana Nery dos Santos
INSTITUIÇÃO/AFILIAÇÃO	Prefeitura Municipal de Camaçari
CIDADE	Camaçari
ESTADO	Bahia
PAÍS	Brasil
RESUMO DA BIOGRAFIA	Graduada em Engenharia de Computação (Faculdade Área 1-Wyden). Concluinte da Pós-graduação em Segurança da Informação. Atualmente trabalho na Prefeitura Municipal de Camaçari, coordenando o Museu de Ciência e Tecnologia - UNICA e Laboratório de Tecnologia de Camaçari - LABTEC. Docente e atuante no fomento da Inovação e Tecnológica regional da Bahia.
CONTRIBUIÇÃO DO AUTOR NO ARTIGO	Autoria
AUTOR 2	
PRONOME DE TRATAMENTO	Sr.
NOME COMPLETO	Fábio Rodrigues Santos
INSTITUIÇÃO/AFILIAÇÃO	Instituto Federal da Bahia - IFBA
CIDADE	Camaçari
ESTADO	Bahia
PAÍS	Brasil
RESUMO DA BIOGRAFIA	Doutor em Modelagem Computacional e Tecnologia Industrial área de Sistemas complexos (SENAI/CIMATEC - 2019). Mestre em Matemática Pura área de Sistemas Dinâmicos (UFBA - 2004). Graduado em Licenciatura em Matemática (UFSC - 2002). Graduado em Bacharelado em Matemática (UFBA - 1999). Docente Instituto Federal da Bahia (IFBA/Camaçari)
CONTRIBUIÇÃO DO AUTOR NO ARTIGO	Coautoria

Endereço de Correspondência dos autores	**Autor 1:** Rua do Telégrafo, s/n, Natal - Camaçari-BA - CEP. 42809-000 **Autor 2:** Loteamento Espaço Alfa s/n, Tv., Limoeiro - Camaçari-BA CEP. 42.800-605