UNIVERSIDADE FEDERAL DO PARÁ
CAMPUS UNIVERSITÁRIO DE CASTANHAL
FACULDADE DE COMPUTAÇÃO
CURSO DE BACHARELADO EM SISTEMAS DE INFORMAÇÃO

ROGERIO MACHADO PEREIRA

ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO, PLANEJAMENTO E GERENCIAMENTO DE REDES DE COMPUTADORES.

CASTANHAL – PARÁ – BRASIL

DEZEMBRO / 2018

ROGERIO MACHADO PEREIRA

ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO, PLANEJAMENTO E GERENCIAMENTO DE REDES DE COMPUTADORES.

Trabalho de conclusão de curso submetido à análise da banca examinadora do curso de Bacharelado em Sistemas de Informação como requisito para a obtenção do grau de Bacharelado em Sistemas de informação

Orientador: Prof. Dr. Tássio Costa de Carvalho

ANÁLISE COMPARATIVA DE FERRAMENTAS DE MONITORAMENTO, PLANEJAMENTO E GERENCIAMENTO DE REDES DE COMPUTADORES.

Trabalho de conclusão de curso submetido à análise da banca examinadora do curso de Bacharelado em Sistemas de Informação, como requisito para a obtenção do grau de Bacharelado em Sistemas de Informação.

APROVADA EM: ____ / ____ / ___

BANCA EXAMINADORA:

_____

Prof. Dr. Tássio Costa de Carvalho

(Orientador – FACOMP/UFPA)

_____

Prof. Dr. José Jailton Henrique Ferreira Júnior

(Avaliador Interno – FACOMP/UFPA)

_____

Prof. Msc. Jorge Amaro de Sarges Cardoso

(Avaliador Interno - FACOMP/UFPA)

AGRADECIMENTOS

Agradecer primeiramente a Deus pela oportunidade de ter realizado esse sonho, depois a minha família e namorada que sempre me deram forças para continuar nessa jornada, e a meus professores que me lecionaram, por toda base criada e todo auxílio prestado para moldar meu conhecimento.

A meu orientador Professor Dr.Tássio que foi paciente e ferramenta fundamental nesse trabalho, com todo direcionamento que a mim foi concedido.

Talvez não tenha conseguido fazer o melhor, mas lutei para que o melhor fosse feito. Não sou o que deveria ser, mas graças a Deus, não sou o que era antes.

Martin Luther King

SUMÁRIO

Lista de Figuras

LISTA DE TABELAS

LISTA DE SIGLAS

ARP	Address Resolution Protocol
CPU	Central Process Unit
CMIP	Common Management Information Protocol
DOS	Disk Operating System
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol
GUI	Interface Gráfica de Usuário
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task
ISO	International Organization for Standardization
IP	Internet Protocol
ICMP	Internet Control Protocol
LAN	Local Area Network
MAC	Media Access Control
MIB	Management Information Base
OSI	Open System Interconection
QoS	Quality of Service
RFC	Request fo Comments
SNMP	Simple Network Management Protocol
SDI	Data Interface Serial
SSL	Secure Socket Layer
SPAN	Switched Port Analyzer
TCP	Transmission Control Protocol
TTL	Time To Live

TLS	Transporte Layer Security
UDP	User Datagrama Protocol
URL	Uniform Resource Locator
VPN	Virtual Private Network
WWW	World Wide Web
WAN	Wide Area Network
WLAN	Wireless Local Area Network

RESUMO

Atualmente, pode-se afirmar que as redes de computadores estão ficando cada vez mais complexas e maiores, exigindo uma atenção especial das organizações em aspectos que antes não existia. O alto nível da quantidade de dispositivos exigiu que houvesse integração entre os mesmos, tornando o acompanhamento do desempenho, funcionamento e disponibilidade pontos cruciais a se monitorar em qualquer empresa. Quando pensamos em monitoramento, o principal objetivo é maximizar a eficiência e a produtividade de uma ou mais redes, além de mantê-las estáveis. Ao desenvolver um plano para realiza-lo, se faz necessário ativar funções que possibilitem o controle total da rede e seus serviços, com mecanismos de análise e controle de recursos. Ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa. Já está mais do que comprovado que com um ambiente de TI bem planejado seu negócio tem mais chances de dar certo, mesmo para as empresas em que o principal foco não seja TI, pois todos dependem hoje da Internet e dos serviços que ela disponibiliza. E para isso é necessário utilizar ferramentas de gerenciamento e monitoramento de redes, as quais foram abordadas durante este trabalho, então foi realizada uma análise feita em cenários de redes semelhantes. Essa análise teve por objetivo definir qual ferramenta é a mais adequada, fazendo testes, definindo a que mais obteve gerenciamento de desempenho, todas as ferramentas utilizadas foram testadas na versão demo, são elas; Netflow Analyzer, PRTG, WhtasUp Gold, Wireshark, então foi extraído e coletado dados de cada ferramenta e foi feita a análise e comparação dos resultados.

Palavras Chave: Monitoramento, Gerenciamento de Desempenho, Disponibilidade, Redes de Computadores.

ABSTRACT

Currently, it can be said that computer networks are becoming increasingly complex and larger, requiring special attention from organizations in aspects that did not previously exist. The high level of the number of devices required integration between them, making monitoring performance, operation and availability crucial points to be monitored in any company. When we think of monitoring, the main goal is to maximize the efficiency and productivity of one or more networks, and to keep them stable. When developing a plan to realize it, it is necessary to activate functions that allow the total control of the network and its services, with mechanisms of analysis and control of resources. Having a mapped and monitored environment is critical to the growth process of a business. It is already proven that with a well-planned IT environment, your business is more likely to work, even for companies where the main focus is not IT, because everyone now depends on the Internet and the services it provides. And for this it is necessary to use network management and monitoring tools, which were addressed during this work, then an analysis was done in scenarios of similar networks. This analysis had as objective to define which tool is the most appropriate, doing tests, defining the one that obtained the most performance management, all the tools used were tested in the demo version, they are; Netflow Analyzer, PRTG, WhtasUp Gold, Wireshark, then extracted and collected data from each tool and the results were analyzed and compared.

Key Words: Monitoring, Performance Management, Availability, Computer Network

1. INTRODUÇÃO

A rápida difusão do acesso à internet em diversos tipos de dispositivos que compõe uma rede fez com que aumentasse o nível de complexidade das redes atuais, por consequência exigiu cada vez mais o conhecimento e experiência dos administradores de rede necessitando conhecer detalhadamente o ambiente, com seus valores, suas problemáticas e a capacidade de observar as mudanças positivas e negativas que possa sofrer, a quantidade de dados trafegados e analisáveis fluindo na rede exigem ser gerenciados, e essa gerência pode ser auxiliada e feita por meio de ferramentas de analise de trafego de rede, o uso de ferramentas possibilita a coleta de informações.

Analisar o tráfego, e cada pacote que passa pela rede possibilita detectar o comportamento anômalo seja em um equipamento de comunicação ou algum software que esteja afetando a transmissão das informações na rede.

A maioria das organizações que dependem do uso de redes de computadores, sistemas e processos que necessitem do auxilio da tecnologia de comunicação, precisam ter um bom desempenho nos servidores, equipamentos de rede, assim como softwares, precisam ser eficientes como ativos de redes, pois só assim haverá o sucesso econômico para empresa, de forma especifica ligada ao fluxo de informação, a velocidade e eficiência dos recursos, resultam em confiabilidade e disponibilidade para a transmissão de informações e segurança dos negócios.

Porém, as eventualidades de falhas físicas pelo funcionamento inadequado, insuficiência de softwares, acabam causando sérios prejuízos à organização, e que na maioria das vezes o custo de não ter gerenciado a falha antes de ocorrer, poderia ter evitado um prejuízo que no fim impactou e custaram mais recursos, seja ela financeira ou tempo, mão de obra, investimento, e afetaram drasticamente o funcionamento da empresa.

Para COSTA (2008), ter um ambiente mapeado e monitorado é fundamental para o processo de crescimento de uma empresa, já está mais do que comprovado que um ambiente de T.I bem planejado tem mais chances de dar certo, mesmo para as empresas em que o principal foco seja T.I, pois todos dependem hoje da internet e dos serviços que ela disponibiliza.

Segundo COMER (2001) a utilização de software de gerência de rede é um artificio para que o gerente encontre problemas e possa sanar sua causa. Esses tipos de softwares tem como base o protocolo SNMP, que são capazes de monitorar o estado de serviços e equipamentos da rede.

Conforme TANEMBAUM (2003) geralmente uma rede com baixo desempenho é motivo de reclamação por seus usuários, considerando as variadas soluções possíveis, uma delas é a mais usada e consiste em utilizar um computador que interage com os diversos componentes da rede para deles extrair as informações necessárias ao seu gerenciamento. O gerenciador de rede visa manter o controle de informações estratégicas, controlar a complexidade da rede, obter melhorias nos serviços nos serviços, reduzir ao máximo o tempo de indisponibilidade de sistemas e diminuir os custos com a manutenção de rede.

Porém, para que isso possa acontecer, é necessário o uso de ferramentas de gerenciamento e monitoramento de rede para auxiliar o responsável por essa tarefa de gerenciamento de uma rede. Existem inúmeras tipos no mercado, variando desde ferramentas gratuitas, até as que são comercializadas, sendo de níveis simples como as que identificam ocorrências críticas e as que realizam o *Polling* da rede, como também as mais complexas que auxiliam na detecção de falhas, análise e monitoramento.

O Capitulo 2 é feito um apanhado sobre o estado da arte em Redes de Computadores. A seguir o Capitulo 3 apresenta os trabalhos relacionados que foram essência para análises nesse trabalho, o capitulo 4 faz uma descrição sobre as ferramentas de Gerenciamento e Monitoramento de redes de computadores. Já o Capitulo 5 é realizado os testes e a obtenção dos Resultados, e por fim o capitulo 6 é apresentado as considerações finais.

1.1 Contextualização

Quando uma empresa monitora sua rede utilizando ferramentas, todos os envolvidos pelos processos de TI serão notificados caso alguma eventualidade ocorra na rede, por meio de e-mails pré-programados ou gráficos de saúde da rede, isso faz com que o gerente ou a equipe de TI possa atuar mais precisamente caso possíveis falhas aconteçam.

O desempenho da rede pode ser visualizado de qualquer lugar de forma remota, e caso seja necessário solucionar algum problema o profissional pode agir sem sair de sua casa, as ferramentas proporcionam identificar tendências, ou seja, caso a rede da empresa apresente

diversos problemas de forma isolada ao longo dos anos e passe despercebidos, o software de monitoramento é capaz de identificar padrões nas falhas e consequentemente, entender como está à saúde da rede e planejar melhorias.

Para gerenciar e analisar todos os dados trafegados na rede as organizações precisam se valer de soluções que apoiem a gestão de TI fornecendo formas de visualização destes dados. Por isso o presente trabalho realiza um estudo das principais ferramentas de monitoramento, buscando analisar o desempenho de cada uma, suas características estratégicas na resolução de desafios tecnológicos antes mesmo que eles se apresentem.

1.2 Problematização

A internet obrigou as empresas a buscarem saídas para trabalhar com a grande quantidade de dados. Essa mudança foi tão rápida e radical que o consumo de conteúdos fez com que muitos gestores de organizações se perdessem ao tentar migrar seus sistemas antigos para novos. As perdas significam que possíveis falhas podem ocorrer, gerando paradas em operações, consequentemente, perdas financeiras, transações não concluídas e serviços indisponíveis.

Atualmente, é inevitável uma rede de computadores usarem ferramentas de gerência e monitoramento, o ponto a ser destacado é que mesmo com todo avanço de hardwares e softwares e toda expansão que as redes de computadores sofreram, ainda existe um numero considerável de organizações que deixam de realizar e implantar o monitoramento efetivo de suas redes, gerenciar de forma organizada e satisfatória é um ponto chave para o funcionamento dos serviços, o mercado oferece muitas ferramentas de monitoração e gerenciamento, podendo ser software livre ou proprietário, por conta dos custos envolvidos nos licenciamentos de softwares ou custo de pessoas qualificadas, as empresas temem pelos altos custos e deixam de lado as boas práticas de gerencia de redes.

1.3 Motivação

Nos dias atuais, é muito raro encontrar qualquer organização que seja completamente independente da computação. Os softwares ou sistemas computacionais em larga escala são imprescindíveis no mundo corporativo e em qualquer ambiente, dentro desses ambientes o setor de infraestrutura de redes é responsável por cuidar da rede, colaborando para que a mesma esteja em perfeito funcionamento, mas também com intuito de evitar que as falhas interrompam os processos do negócio. Por isso que o simples fato de um ambiente de redes

possuírem o máximo possível de funcionalidades de rede dentro de suas possibilidades de apoio ao desempenho de tarefas não é o suficiente para desempenhar satisfatoriamente todas as tarefas durante todo tempo.

Segundo Rafael (2014) para uma empresa, seja ela grande ou pequena, uma rede segura e com bom desempenho é um dos critérios essenciais para o sucesso. Geralmente grandes empresas possuem um setor de TI para resolver os problemas que surgem no dia a dia e também para estudar as aplicações que podem trazer benefícios ao seu funcionamento. Já em pequenas empresas, a TI é tratada como uma área secundária, onde normalmente só é chamada para prestar suporte quando já ocorreu algum problema.

1.4 Objetivo

O objetivo geral desse trabalho é analisar, comparar, testar ferramentas de gerenciamento e monitoramento de redes elencando principais pontos das ferramentas; PRTG Network, Wireshark, Netflow Analyzer.

O uso de ferramentas de gerenciamento de redes é essencial para empresas, organizações e usuários comuns, facilitando análises, coletas de informações, tomadas de decisões, mas a escolha de uma ferramenta que apoie ou satisfaça todas as necessidades de gerência a maioria das vezes se torna complicado ao decidir que ferramenta usar, o mercado oferece muitas opções, mas nem todas solucionam as possíveis eventualidades que a rede possa a vim sofre. Este presente trabalho objetiva mostrar algumas ferramentas que o mercado oferece, mostrando suas características, funcionalidades, também realizando comparações das mesmas, por fim as ferramentas que mais se destacaram.

1.4.1 Objetivos Específicos

1. Avaliar a utilização das ferramentas de gerenciamento PRTG Network, Wireshark e Netflow Analyzer, WhatsUP Gold, Sparrow IQ com suas características e funcionalidades e evidenciar qual ferramenta apresenta melhor capacidade na gerencia redes.
2. Avaliar o desempenho de cada ferramenta em um cenário de redes.
3. Indicar a ferramenta mais adequada aos administradores de redes, com base nos resultados provenientes desta análise.
4. Auxiliar as soluções para o ensaio em um ambiente de rede funcional.

CAPÍTULO 2: ESTADO DA ARTE

O surgimento do conceito de redes de computadores teve seus primórdios há muitas décadas atrás, mais ou menos pela década 1960 marcada pelo rápido desenvolvimento da eletrônica aplicada nesse cenário. Foi então que nesse momento a ciência da computação foi uma das mais beneficiadas, várias equipes e desenvolvedores da época reuniram-se para interceptar e decodificar as comunicações e mensagens em códigos cifrados pelo eixo nazifascistas para tentar desvendar estratégias dos inimigos. Mas foi na década seguinte que o conceito se consolidou com a criação da ARPANET, naquele momento eram conectados 30 computadores interligados abrangendo diversas localidades ao redor dos Estados Unidos, incluindo grandes empresas e bases militares.

A Arpanet então revolucionou a tecnologia em redes quando combinou os protocolos TCP e IP em 1973 e ganhou escalabilidade e a capacidade de incluir sistemas de arquitetura diversos, e até hoje o protocolo TCP/IP é o protocolo padrão do Trafego da internet. Esses não foram os únicos fatores que culminaram para o surgimento das redes de computadores, mas é certo que sem eles, as redes como conhecemos nos dias atuais seriam totalmente distintas.

Em questão arquitetural as redes de computadores ficaram distribuídas em camadas, e cada camada é interligada formando uma pilha de protocolos, os protocolos é que determinam o padrão de comunicação para que haja troca de informações. Para TANEMBAUM (2003), a maioria das redes são concebidas e organizadas como pilha de camadas hierárquicas, cuja organização se dá na oferta de serviços para as camadas (Imediatamente) superiores e inferiores, protegendo essas camadas dos detalhes de como os serviços são realmente implementados.

Os modelos de referência *Open System Interconection* (OSI) e TCP/IP são os mais importantes protocolos da arquitetura de redes, assim como cada um tem sua particularidade e diferencial de estruturação e ambos divididos em camadas hierárquicas. O modelo OSI embora seja concreto e amplamente implementado apresenta sete camadas em sua arquitetura, e para TANEMBAUM (2003), estão estruturadas de cima para baixo, sendo elas; Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace e Física. Os princípios do modelo podem ser resumidos na necessidade de cada camada por possuir uma abstração diferente, executar uma função diferente, abranger protocolos padronizados internacionalmente e minimizar os fluxos de informação entre as interfaces.

Diferente do modelo OSI para TANEMBAUM (2003), o protocolo TCP/IP foi criado como descrição dos protocolos já existentes, vindo a ser o padrão de comunicação da internet. Esse modelo integrou camadas por isso tem menos camadas que o outro modelo, são elas: Aplicação, Transporte, Internet e Rede, sendo cada uma responsável pela execução de tarefas distintas, para garantir a integridade e entrega dos dados trafegados.

Sabemos o quanto as redes de computadores beneficiaram, mas para que haja essa interligação os grandes desenvolvedores de dispositivos e software cada vez mais criam novas tecnologias, e para que cada dispositivo queira se conectar na rede, é necessário ter um endereço para que o mesmo possa ser identificado no enlace, à tecnologia chamada de IP, é o fator identificador do dispositivo na rede, essa inovação teve suas versões iniciais, tendo sua ascensão com o IPV4, mas pelo fato da quantidade de dispositivos serem maior que a quantidade de endereços, se fez necessário criar uma nova versão, atualizada para IPV6, essa nova versão oferece um valor ilimitado de endereços IP.

Para ROSS, Júlio (2009), uma rede obedece a uma topologia, ou seja, “Layout Físico” e ao meio de conexão dos dispositivos na rede, como está conectado, esses pontos que fazem parte do meio recebem a denominação de Nós, sendo que estes nós estão sempre associados a um endereço, para que possam se reconhecidos pela rede. A topologia de uma rede depende do projeto das operações, da confiabilidade e do seu custo operacional.

Os mais típicos exemplos de topologia de rede são: Anel; consiste de estações conectadas através de um caminho fechado, Barra; nessa configuração todos os nós se ligam ao mesmo meio de transmissão, Estrela; esse modelo interliga computadores através de um equipamento central concentrador, no entanto, sem nenhuma ligação direta, nem através de outro computador.

Segundo TORRES, Gabriel (2014) existe dois modelos de rede: Ponto a Ponto, que é usada por redes pequenas. E a rede Cliente/Servidor, que pode ser utilizada tanto para redes pequenas quanto em grandes redes, a classificação que a rede recebe é conforme a rede esta montada, e como está a sua configuração em software. Podemos perceber que as redes de computadores são classificadas quanto o seu tipo, e quanto maior for a rede, maior será a forma gerencia-la, obedecendo a arquiteturas, padrões e normas.

Para MIRANDA (2008), uma rede de computadores é um conjunto de computadores (Locais e Remotos) interligados entre si (de forma total ou parcial) de tal maneira de possibilitar a comunicação de dados localmente e/ou remotamente, incluindo todos os

dispositivos, tais como microcomputadores e impressoras. O ideal do autor nos permite inferir que, essa tecnologia possui aplicações e que variam desde comerciais, onde são muito utilizados no compartilhamento de recursos, sejam arquivos, softwares, impressoras, telefonia IP, comercio eletrônico, e também aplicações domesticas como atividades educativas hoje as redes nos permitem fazer atividades intelectuais, pesquisas, jogos, compartilhamento de arquivos, comunicadores instantâneos e outras funcionalidades a mais.

O fato é que estão presentes em todos os segmentos, tendo se tornado vital para praticamente qualquer área do mercado com seu surgimento melhorou a comunicação e o acesso à informação em governos, empresas, escolas e outras instituições, fazendo com que seus trabalhos sejam mais eficientes e ágeis.

Segundo ABREU, Carlos (2012), quando interligamos computadores eles podem trabalhar mais pelos usuários. Pessoas trabalhando em equipes concretizam tarefas inteiras num menor espaço de tempo e com menos esforço. Os benefícios de se conectar os recursos podem significar um avanço incalculável em relação a um micro isolado.

Antigamente as redes eram de difícil instalação e manutenção, exigindo mão de obra altamente qualificada, porém, esta realidade tem se modificado bastante nos últimos anos. Podemos ver o quanto às redes de computadores beneficiaram a vida e a rapidez com que serviços que antes necessitavam de maiores tempos para serem executados, hoje com recurso de interligar dispositivos diminuíram-se as fronteiras espaciais, como também o aumento na acessibilidade para os usuários, seja na busca da realização de uma tarefa ou para recursos mais complexa, como desenvolvimento de novos ideais, aplicações, softwares, etc.

2.1 Gerenciamento de Redes

Gerenciar redes de computadores independe do seu tamanho, é fundamental que mesmo por se tratar de uma rede de pequeno ou grande porte ela deva ser gerenciada, dessa maneira a confiabilidade de eficiência no uso dos recursos e dos serviços oferecidos tenha altos índices de instabilidade. Atualmente quando se pensa em mercado, e grandes organizações, o responsável pela gerência é o Administrador de rede, e para que o mesmo possa ter uma gerência eficiente e de qualidade, é essencial que o mesmo seja auxiliado por ferramentas especificas para esse ambiente.

Para FOROUZAN e MOSHARRAF (2013, p. 693)o gerenciamento de redes pode ser definido como a tarefa de testar, monitorar, configurar e resolver problemas dos componentes

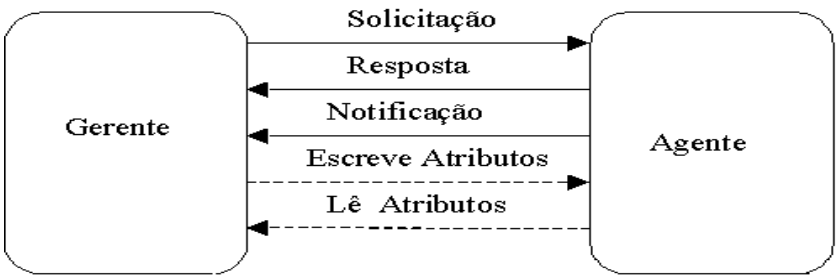
de rede com o objetivo de atender um conjunto de requisitos definidos por uma organização. Com o objetivo de garantir o nível de qualidade de serviço através do monitoramento e controle dos elementos que compõem, tanto físicos, como lógicos.

Segundo FOROUZAN e MOSHARRAF (2013, p. 693), ainda que “um sistema de gerenciamento de rede utiliza hardware, softwares e seres humanos”. Deste modo pode-se inferir e obter informações de como os hardwares e softwares e todos os elementos que compõe a rede foram gerenciados.

Para KUROSE e ROSS (2010, p553) “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”.

O administrador utilizando um conjunto de ferramentas pode gerar dados históricos e estatísticos de seu ambiente computacional, assim como desenvolver ações assertivas no momento de falha ou indisponibilidade. No ambiente de monitoramento não se usa os termos cliente e servidor, mas sim difundidos para Gerente e Agente, sendo que o gerente é o computador que possui o software de gerenciamento de rede e o agente é onde temos a base com os dados a serem analisados e consultados pelo gerente. Conforme a figura a seguir.

Figura 1: Modelo Gerente e Agente



Fonte: Própria do autor.

Para STALLINGS (2005) um sistema de gerenciamento de redes é um conjunto de ferramentas para monitoramento e controle de rede que é integrado, devendo conter uma interface única para o operador e de fácil uso, atendendo as necessidades do gerenciamento diário, sendo que a maior parte da implementação realizada no dispositivo gerenciado.

Para que haja sucesso no gerenciamento o administrador ou desenvolvedor do software deve trabalhar três pontos, são eles: Coleta de dados, esse ponto atua na coleta de informações de todos os recursos que foram gerenciados, através de componentes de softwares são determinados períodos da captura desses dados. Análise, esse item é responsável pela análise das coletas, fazendo inferências desses dados, obedecendo a parâmetros determinados pelo administrador, informando se algo está fora da anormalidade esperada.

Quanto a Ação, após serem realizadas análises sobre os dados coletados, se houver necessidade de ações corretivas ou preventivas, ações como um alarme visual mostrado na interface possam notificar as ações a serem tomadas.

Segundo PANDORA, FMS (2012), a monitoração pode ocorrer de duas formas: Monitoração Local ou Remota. Para que seja de forma Remota tem-se como exemplo o processo executado pelo protocolo SNMP, ou seja, o gerente deve realizar consultar determinadas em períodos ao dispositivo a ser gerenciado, o mesmo enviará dadas respostas, seguindo um modelo Requisição/Resposta sendo um fluxo padrão chamado de Síncrono. Já a monitoração Local tem um módulo de software instalado no dispositivo gerenciado denominado de agente de software, tendo como responsabilidade execução de rotinas e tarefas, neste modelo obtém-se informações mais detalhadas do dispositivo gerenciado.

Basicamente os modelos de gerencia mais aceitos atualmente são o ISO que utiliza o protocolo CMIP e o outro modelo SNMP do IETF (*Internet Engineering Task Force*).

4.2 Modelos Funcionais de Gerenciamento

2.2.1 Modelo ISO

A ISO (*International Organization for Standardization*) é um desenvolvedor de normas, então ela divide o gerenciamento em cinco áreas distintas. Estabelecendo regras para que haja padronização e interoperabilidade entre os processos dentro dos sistemas. Para STALLINGS (2005), a proposta de áreas funcionais são divididas e compostas a seguir, seguindo critérios e normas de gerenciamento.

2.2.1.1 Gerenciamento de falhas

Para ELER (2015, p. 4) define o gerenciamento de falhas com a “função de monitorar os estados dos recursos verificando em qual ponto da rede e quando uma falha ou um erro

pode ocorrer". Ainda é possível inferir que falha é diferente de erro, isso por que, tanto para Eler (2015, p. 4) quanto para Specialski (1999, p. 3), uma falha é uma condição anormal persistente e que causa a total interrupção da rede, como, por exemplo, o rompimento de um cabo; uma falha exige uma ação de gerenciamento imediata. Um erro é uma condição anormal ocasional que pode ser corrigida ou compensada antes que se transforme em uma falha, tendo como exemplo, erro de bits durante uma transmissão.

O gerenciamento de falhas impacta consideravelmente no estado da rede, pois uma eventualidade de erros seria mais difícil fazer previsões de anormalidades, enquanto que uma falha seria mais fácil prever, pois através de dados armazenados historicamente seria possível fazer previsões realísticas. Para Forouzan (2007, p. 875) ainda subdivide o gerenciamento de falhas em "gerenciamento de falhas reativo" e "gerenciamento de falhas proativo".

O gerenciamento de falhas reativo define-se em tomar ações após a ocorrência de eventuais falhas, o administrador da rede então deve localizar o possível ponto de falha e só assim adotar medidas, inicialmente isolando a falha do restante da rede, para que não haja a possibilidade de afetar outros dispositivos, em seguida são tomadas atitudes de correção da falha, e por fim, a documentação desse registro para que possa ser analisado e estudado mais minuciosamente as causas do evento. Já o gerenciamento de falhas Proativo tenta prevenir as possíveis eventualidades de falhas, buscando informações na rede que possam ajuda-lo a impedir que falhas venham a tornarem-se futuros erros.

2.2.1.2 Gerenciamento de Configuração

Para ELER (2015, p. 4), o gerenciamento de configuração "permite manter atualizadas as informações de hardware e software de uma rede, incluindo as informações de configurações de todos os equipamentos". Recurso esse essencial para as redes em decorrência das constantes mudanças que softwares e hardwares sofrem com a evolução dos mesmos. Na eventualidade de uma possível troca de software ou um equipamento da rede a gerencia de configuração deve ser de caráter proativo, seja realizando backups de informações, ou reduzindo o tempo de troca de um dispositivo.

2.2.1.3 Gerenciamento de Contabilização

O gerente da rede deve ser capaz de especificar informações de contabilização de registro de cada nó da rede, mesmo que não haja cobrança interna pela utilização dos recursos, o mesmo deve está habilitado a controlar o uso de cada recurso pelos usuários.

Evitando que grupos ou usuários abusem de privilégios e monopolizem o recurso da rede, consequentemente evitando possíveis incidentes e garantindo o desempenho da rede.

2.2.1.4 Gerenciamento de desempenho

Segundo FOROUZAN (2007, p. 876), o gerenciamento de desempenho tem o objetivo de monitorar e controlar a rede para assegurar que a mesma funcione da forma mais eficiente possível. O gerenciamento consiste em monitorar atividades e controlar recursos realizando possíveis ajustes, avaliando comportamentos de recursos por meio de parâmetros, por exemplo, medição de vasão da rede, perfil de tráfego, nível de utilização, disponibilidades, quanto de pacotes que a rede perdeu e entre outras métricas de medição do desempenho.

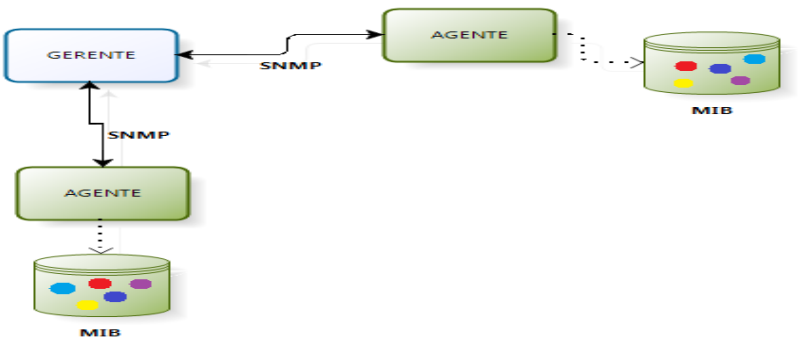
2.2.1.5 Gerenciamento de Segurança

O gerenciamento prover facilidades para proteger recursos, criando politicas de segurança para controlar o acesso à rede, tratando questões como, criação e distribuição de chaves de criptografia, criação de senhas, realizando exames de auditorias para analisar os registros das atividades.

2.2.2 Modelo SNMP

O modelo SNMP do IETF (*Internet Engineering Task Force*) é o padrão mais abordado na atualidade, por ter suportes bases de redes que utilizam o TCP/IP. Os componentes dessa arquitetura são divididos em GERENTE, AGENTE, MIB e Protocolo SNMP, conforme ilustrado na figura a seguir.

Figura 2: Modelo de Gerenciamento SNMP



Fonte: Telcomanager (2018).

2.2.2.1 Gerente (Estação de Gerenciamento)

Neste componente é onde será implantado o software de gerenciamento, devendo constar todos os dados dos agentes facilitando o acesso do administrador ou da equipe de redes na busca de alguma informação. Funcionando equivalente a um cliente na arquitetura cliente-servidor, emitindo pedidos de operações de gestão em nome de um administrador ou de uma aplicação e também recebe armadilhas dos agentes. Um gerente é um servidor executando algum tipo de sistema de *software* que pode lidar com tarefas de gerenciamento de rede

2.2.2.2 Agente

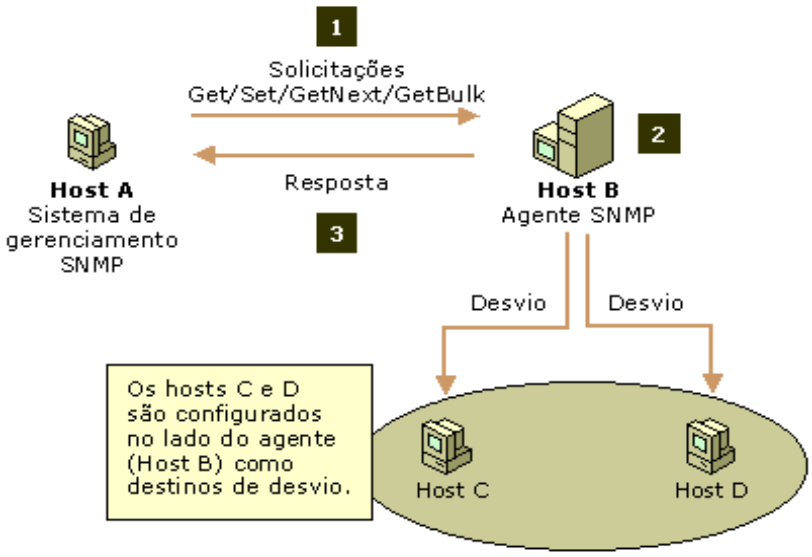
Um agente principal é um pedaço de *software* rodando num componente de rede SNMP, por exemplo, um roteador que responde às solicitações SNMP da estação de gerenciamento. Residindo nas entidades gerenciadas, podendo também enviar uma informação a respeito de alguma situação ocorrida, chamado de mensagens *Trap* caso ocorra uma eventualidade incomum. Essas informações que o agente envia ao gerente são coletadas na MIB onde são devidamente armazenadas.

2.2.2.3 Protocolo SNMP

Segundo COMER (2007) O protocolo SNMP define como gerente e agente se comunicam, conforme define o formato das requisições que um gerente envia a um agente e o formato das respostas que o agente retorna, esse protocolo trabalha o conceito chamado de comunidade (community) o intuito da comunidade seria de atuar como um mecanismo de segurança, a relação ocorre entre o gerente e um grupo de dispositivos gerenciados.

O SNMP é um protocolo não orientado a conexão: não requer ação prévia nem posterior ao envio de mensagens, fazendo com que não haja nenhuma garantia de que as mensagens do protocolo chegarão ao destino. Robusto porque, como não existe conexão, nem o gerente nem o sistema gerenciado necessita um do outro para operar. É um protocolo da camada de aplicação e sua função é facilitar a troca de informações de gerenciamento entre os dispositivos de rede o protocolo mais utilizado no gerenciamento de redes é o TCP/IP. A seguir uma figura ilustrando o modelo de arquitetura do protocolo.

Figura 3: Arquitetura de Gerência SNMP



Fonte: EBAH (2002).

O protocolo SNMP ainda divide-se em três partes:

- Protocolo SNMP: Que define as mensagens que são opções de trocas entre gerentes e agentes, e a forma de procedimentos que irão ser usados na troca de informações.
- Estrutura de Informações de gerencia (SMI): É onde será especificado o formato dos objetos que serão gerenciados pelo SNMP, tipos de objetos, identificação e grupo de informações.
- A base de informações de gerencia (MIB): Um mapa ira descrever a ordem de hierarquia de todos os objetos gerenciados e a forma como serão acessados.

2.2.2.4 MIB

É um dos mais importes componentes na gerencia de redes, pois é a base de informações dos dispositivos gerenciados, especificando quais dispositivos. Para (COMER, 2006) o padrão MIB especifica os itens de dados que um dispositivo gerenciado precisa manter e as operações permitidas em cada um e o seu significado. A MIB pode ser divida em quatro tipos.

- As MIB’s do tipo I e II correspondem as especificações gerais dos dispositivos, por exemplo, o quanto de pacotes foi utilizado por dispositivos, assim como estado de cada interface.

- MIB privada é aquela em que seus componentes fornecem informações específicas dos equipamentos gerenciados, como configuração, colisões e também é possível reinicializar, desabilitar uma ou mais portas de um roteador.
- A MIB experimental é aquela em que seus componentes (objetos) estão em fase de desenvolvimento e teste, em geral, eles fornecem características mais específicas sobre a tecnologia dos meios de transmissão e equipamentos empregados.

2.3 Monitoramento de Redes

Mesmo com os equipamentos de última geração e softwares mais atualizados não há garantia de sistemas imunes a erros, por isso qualquer rede precisa ser monitorada constantemente para evitar interrupções que prejudiquem sua utilização ou possíveis fatores que induzam uma possível falha ao enlace. O monitoramento da rede também torna ações corretivas e preventivas mais rápidas, isso acontece pelo fato da redução do tempo de identificação da falha, ou seja, o administrador é alertado que algo esta ocasionando problemas no funcionamento da rede e que medidas devem ser tomadas.

Para gerenciar e analisar todas as informações trafegadas na rede, tanto para usuários mais simples, quanto para medias e grandes empresas precisam se valer de soluções que apoiem a gestão de TI fornecendo formas de visualizar os dados coletados. Portanto é possível perceber que o monitoramento de redes ajuda a tornar o trabalho de um admistrador de rede ou de uma equipe de TI mais estratégico, criando artifícios que solucionam os desafios tecnológicos antes mesmo que eles possam ocorrer.

Para CHEN (2007) a monitoração e caracterização do trafego de redes são atividades comumente praticadas no gerenciamento de redes. A monitoração de tráfego se preocupa com as características de fluxo de rede, sendo importante para o gerenciamento e planejamento de redes de computadores. O ato de monitorar pode ser realizado de forma mais genérica, atentando-se as métricas que condizem com o tráfego, por exemplo, a quantidade de bytes de fluem em uma determinada interface de um repetidor, outro exemplo de métrica seria a quantidade de erros detectados em uma rede.

Outro conceito importante é o fluxo de redes, Para o CISCO (2006) define fluxo como uma sequencia unidirecional de pacotes entre maquinas de origem e destino. Pode-se dizer em

resumo que o *netflow* provê a sumarização de informações sobre o tráfego de um roteador ou switch. O reconhecimento do dispositivo ocorre tanto por endereço IP quanto pelo endereço de porta da camada de transporte.

Segundo LUCAS (2010) os fluxos, também conhecidos como fluxos de tráfego ou fluxos de dado, são conjuntos de tráfego de redes(aplicativos, protocolos e informações de controle) que possuem atributos comuns, como endereços de origem/destino, tipos de informações, sentido ou informações fim-a-fim.

Para MCCABE (2007), uma das questões mais importantes no monitoramento e gerenciamento baseados em fluxos é a definição de quais tráfegos será necessário analisar, e partindo dessa premissa, é que a localização dos sensores deve ser definida, se possível essa definição deverá ser realizada no gateway do fluxo de tráfego desejado.

Outro quesito importante no monitoramento corresponde ao método de captura da informação. Essas medições podem ser feitas diretamente nos dispositivos onde o tráfego passa naturalmente, ou em equipamentos externos que recebem uma cópia dos pacotes ou informações dos fluxos que fluem pela rede.

As ferramentas disponíveis no mercado para monitoramento de redes permitem realizar uma análise nos processos e seus serviços de forma a identificar o mais cedo possível qualquer falha, buscando assim uma solução do problema antes mesmo que qualquer usuário possa ter notado. Por menor, e mais simples que uma rede de computadores possa ser ela precisa ser monitorado, na intenção de garantir a disponibilidade aos usuários, assim como o desempenho aceitável.

2.3.1 Tráfego de rede

O tráfego de uma Rede TCP/IP consiste de um amplo e multivariado conjunto de dados de pacotes de rede gerados durante as comunicações entre os *hosts*. O processo de coleta do tráfego de rede consiste na captura contínua destes pacotes de rede contendo os dados brutos (em formato hexadecimal), através de uma estação servidora, denominada “sensor do SDI”, com capacidade de disco para armazenamento de um grande volume de dados. Dependendo do objetivo da análise a ser realizada, pode-se ter um sensor do SDI ou posicionado fora ou dentro dos limites de proteção do *firewall* ou dois sensores, um dentro e outro fora dos limites de proteção do *firewall* (BOUZIDA; MARGIN, 2008).

2.3.1.1 Analisadores de Pacotes

Os analisadores de pacotes capturam e apresentam todo o fluxo de dados trafegado decodificando e exibindo o conteúdo dos pacotes para uma análise detalhada (COMER, 2007). Existem diversos tipos de ferramentas que capturam e analisam os pacotes de dados trafegados na rede, incluindo tanto as livres e as proprietárias. Um analisador de pacotes é um software ou hardware que cuja funcionalidade é monitorar, interceptar e capturar o fluxo de tráfego de uma rede.

A segurança de uma rede implica na segurança dos pacotes de dados, A análise de pacotes apresenta o processo de captura e interpretação de dados que flui através de uma rede, a fim de entender melhor o que está acontecendo nela. Essa análise de pacotes é normalmente realizada por uma ferramenta analisadora de pacotes (SANDERS, 2004).

2.3.2. Protocolos de redes

2.3.2.1 ARP (*Address Resolution Protocol*)

"O protocolo ARP é responsável por fazer a conversão entre os endereços IPs e os endereços MAC da rede. Em uma rede grande, os pacotes TCP/IP são encaminhados até a rede de destino através dos roteadores" (TORRES, 2001).

Cada computador que esteja conectado a rede pode ser reconhecido por dois endereços, um endereço é lógico e o outro físico, sendo este o chamado MAC sendo bastante comparado ao CPF que cada individuo possui, por ser um documento único por pessoa, o endereço MAC é único em cada placa de Rede, e o endereço Lógico é chamado de IP.

Esse protocolo converte os endereços IP e MAC da rede, nas redes de grande porte, os hardwares de rede como roteadores encaminham os pacotes TCP/IP ate o seu destino, então o protocolo ARP identifica para qual placa de rede os pacotes devem ser enviados, pelo fato de nos pacotes conterem apenas o endereço IP de destino e não o endereço MAC da placa de rede.

Segundo OLIVEIRA, S (2013) O ARP age da seguinte forma: manda uma mensagem de *broadcast* para todos os micros da rede perguntando qual deles responde pelo endereço IP ao quais os pacotes são destinados. Assim o micro que possui o endereço de IP requisitado manda seu endereço MAC para que a transmissão de dados seja estabelecida entre as máquinas. Esse protocolo guarda os IP e seus respectivos MAC em uma tabela na memória do

roteador, para não precisar fazer um broadcast se precisar acessar um IP já conhecido, sendo assim não ocupa a rede com broadcasts desnecessários.

2.3.2.2 ICMP (*Internet Control Message Protocol*)

É o protocolo que permite gerenciar informações relativas a erros nas maquinas conectadas, é usado por todos os roteadores da rede para assinalar o problema de entrega.

"Caso um roteador não consiga passar adiante um datagrama recebido por estar congestionado demais ou então por ter zerado o campo Tempo de Vida (TTL, Time to Live) do datagrama, por exemplo, ele precisa informar ao transmissor do datagrama que ocorreu um erro" (TORRES, 2001).

As mensagens de erro ICMP são transportadas na rede sob a forma de datagrama, como qualquer dado. Assim, as mensagens de erro podem elas mesmas estar sujeitas a erros. Contudo, no caso de erro num datagrama que transporta uma mensagem ICMP, nenhuma mensagem de erro é emitida para evitar um efeito 'bola de neve' no caso de incidente na rede.

Abaixo são listadas algumas das principais mensagens ICMP.

2.3.2.2.1 Source Quench

O volume de dados enviado é muito grande, o roteador envia esta mensagem para prevenir que está saturado, para pedir a redução da velocidade de transmissão;

2.3.2.2.2 Eco

Esta mensagem é utilizada quando usamos o comando PING. Ele permite testar a rede, envia um datagrama para um destinatário e pede que ele o restitua.

2.3.2.2.3 Redirecionamento para um hóspede e um serviço dado

O roteador vê que a rota de um computador não é boa para um serviço dado e envia o endereço do roteador a ser acrescentado à tabela de encaminhamento do computador.

2.3.2.2.4 Tempo ultrapassado

Esta mensagem é enviada quando o tempo de vida de um datagrama é ultrapassado. O cabeçalho do datagrama é devolvido de modo a que o usuário saiba que pacote foi destruído.

2.3.2.2.5 Tempo de remontagem do fragmento ultrapassado

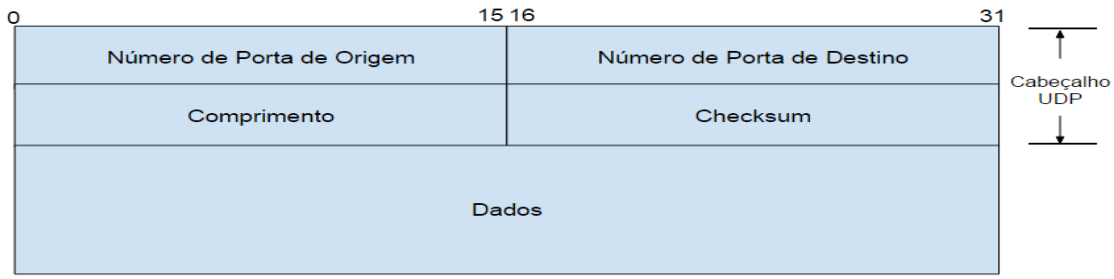
Esta mensagem é enviada quando o tempo de remontagem dos fragmentos de um datagrama é ultrapassado.

2.3.2.3 UDP (*User Data Protocol*)

O protocolo UDP (User Datagram Protocol) é um protocolo não orientado para a conexão da camada de transporte do modelo TCP/IP. Este protocolo é muito simples já que não fornece controle de erros (não está orientado para a conexão). Sua vantagem com relação ao protocolo TCP é a velocidade de transmissão de dados que é bem maior, já que os pacotes enviados são bem menores, seu cabeçalho é menor que um cabeçalho TCP, e como não possui o sistema de verificação de chegada de pacotes (que existe no TCP), a transmissão fica mais rápida, já que o transmissor não precisará receber a confirmação de que o receptor recebeu o pacote para então poder enviar o próximo pacote.

As figuras a seguir podem ver o formato completo de um cabeçalho UDP em redes muito grandes, o uso desse protocolo é completamente desaconselhável, já que a perca de dados pode ser muito grande e a aplicação responsável teria muitas dificuldades para organizar esses dados. Geralmente são usadas em redes onde a taxa de perda de dados não seja um problema e os pacotes enviados sejam pequenos.

Figura 4: Cabeçalho UDP



Fonte: BOSON Treinamentos (2016)

2.3.3 TCP (*Transmission Control Protocol*)

O modelo TCP/IP surgiu como sendo um modelo mais simples e específico para o padrão da Internet. O modelo TCP/IP chama a atenção pela máxima flexibilidade que acontece na camada de aplicação para os desenvolvedores de software.

Segundo DIOGO. R (2013) “protocolo TCP é hoje o mais usado e é o padrão para troca de informações na Internet, sendo um protocolo independente e de fácil adaptação para utilização em outros sistemas de comunicação”. Em contrapartida, pode-se dizer que o protocolo TCP é um protocolo bastante complexo, pois tiveram no seu desenvolvimento objetos de oferecer confiabilidade trabalhando com vários ambientes de rede, com diferentes ferramentas e com muitos aplicativos.

Para realizar o envio dos dados, quando o TCP recebe os pacotes ele divide-os em segmentos, cada segmento é recebe um numero antes de ser enviado. Após estabelecer a conexão com o destinatário, o TCP começa o envio dos pacotes. Os serviços orientados para conexão agrupam três fases. Na fase inicial, criação da conexão, um único caminho entre o terminal origem e o terminal destino é criado.

Assim, os recursos são reservados para garantir um nível consistente de serviço. Na próxima fase, a de transferência de dados, os mesmos são encaminhados em sequência pela conexão estabelecida, encerrando junto ao terminal destino na ordem em que foram enviados. A ultima fase, de encerramento da conexão, serve para encerrar a conexão entre o terminal origem e o terminal destino quando não é mais necessária.

2.3.4 HTTP (*HyperText Transfer Protocol*)

Hypertext Transfer Protocol (HTTP) é o método utilizado para enviar e receber informações na web. A versão mais utilizada atualmente é a 1.1, definida pela especificação RFC 2616. “A Internet não seria a mesma sem o WWW. O “boom” que a internet sofreu nos últimos anos foi graças à criação desse recurso. Um site www consiste em uma série de documentos hipermídia, acessados através de um endereço, também chamado URL (*Uniform Resource Locator*), como, por exemplo, www.seeusite.com.br” (TORRES, 2001).

Seu funcionamento baseia-se em requisições e respostas entre clientes e servidores, o cliente, também chamado de *user agent*, fará a requisição solicitando algum recurso, enviando um pacote de informações contendo alguns cabeçalhos, a um URL especifico. O servidor recebe então estas informações e envia uma resposta, que pode ser um recurso ou simplesmente outro cabeçalho.

CAPITULO 3 – TRABALHOS RELACIONADOS

Este trabalho apresenta um estudo na área de gerência e monitoramento de redes de computadores, tendo como proposta principal realizar testes e análises com as ferramentas de gerenciamento e monitoramento de redes. Dando apoio a pesquisa foi levada em consideração outros trabalhos que propõe análises de ferramentas e estudos.

BUFFONI, Humberto (2013) propõe um estudo sobre ferramentas de gerenciamento e monitoramento, idealizando um cenário de redes com ativos antigos, o objetivo é mapear os problemas relacionados a quedas constantes de acesso à internet e ao seu desempenho em empresa dentro da universidade. No trabalho foram utilizadas ferramentas de gerência de rede tais como CACTI, MRTG e PRTG que foram implementadas para a análise gráfica do comportamento de ativos de redes.

Proposta semelhante de SCAPIM, Alex (2015) onde utiliza às ferramentas Zabbix, Nagios e MRTG, a ideia principal do trabalho é mostrar os dados coletados com bases históricas de forma clara e eficaz, e mostrar as informações dos ativos de redes. O trabalho enfatiza a instalação e configuração correta de todos os softwares, até criando um passo a passo para cada uma, sabemos que uma configuração feita de modo errado ou ineficiente gera falhas, que muitas vezes são financeiramente caro para uma organização, então gerenciar corretamente a configuração é um ponto chave no monitoramento.

BUENO, Edimilson (2012) utiliza ferramentas de softwares livre para realizar uma simulação de um cenário de redes, no qual demonstra instalação, as funcionalidades, as configurações e as características do pandora FMS . O uso de softwares livre é muito amplo atualmente, muitos setores e repartições publicas, preferem utilizar softwares livres, por eles disponibilizarem a capacidade de sofrer mudanças, e por serem mais seguros de certa forma, a equipe de TI pode implantar o software sem obedecer regras de fabricantes, isso é o diferencial para boas práticas de configuração.

BLACK, Thomas (2008) o presente trabalho consiste em apresentar e comparar nove ferramentas de redes, so que baseado em RRD, Zenoss, ManageOP Engine, BigBrother , Spice Works Look@LAN, Zabbix e o Nagios. O objetivo do trabalho não foi apontar qual ferramenta seria a melhor, mas sim de auxiliar o pesquisador a tomar mehor escolha de acordo com suas necessidades. Em particular, são observados os parâmetros mais relevantes dentre os procurados pelos administradores de rede: Performance, facilidade de utilização e necessidade de recursos tanto de hardware quanto humanos.

Outra proposta de analise de ferramentas é feita por Majewski (2009) e Braga (2011), onde ambos realizam um estudo comparativo entre as ferramentas Nagios, Cacti e Zabbix, com objetivo também, de apontar funcionalidades, pontos positivos e negativos, sem a intenção de apontar qual delas é a melhor ferramenta.

ATISANO, José (2011) em seu trabalho apresenta de forma simples e direta o PHP *Network Weathermap*, um dos principais plugins do Cacti, que por sua vez é um importante software de monitoramento de redes. Esta ferramenta permite transformar os dados coletados pelo Cacti em mapas, desta maneira, centralizando todas as informações da rede gerenciada em uma única página. Isto possibilita um amplo controle da rede, habilitando o administrador de rede a detectar com facilidade falhas, tráfegos maliciosos, pontos críticos, e principalmente, lhe possibilita ter uma visão geral da saúde de toda a rede.

AMARAL e FARIAS (2013) Fazem um trabalho tentando definir parâmetros para servir de base nessa escolha, esse trabalho faz um estudo de caso comparativo, em uma computacional heterogênea, entre duas ferramentas: o MRTG, escolhido por ser a uma das primeiras ferramentas aplicadas na gerencia de redes e o Cacti que é hoje uma das ferramentas mais usadas para esse fim.

Como conclusão verificou-se que o Cacti mostrou-se superior ao MRTG, apresentando diversas funcionalidades adicionais implementadas em sua instalação padrão. Essa diferença pode ser creditada ao fato do Cacti ser mais novo e que o MRTG, mesmo tendo sua utilização reduzida, continua ativo e operante.

Podemos perceber que todos os trabalhos que estudam ferramentas de gerenciamento e monitoramento, buscam apresentar funcionalidades, realizam testes, dizem os pontos positivos e negativos de cada ferramenta, mas nunca destaca qual seria a melhor ou mais adequada ferramenta.

Sabemos que o mercado dispõe de infinitas opções de softwares, mas é então que surge varias perguntas, por exemplo, essa ferramenta irá suprir todas as necessidades que a organização necessita monitorar, ou que tipo de software usar, software livre ou proprietário, essas perguntas geram incertezas sobre a efetividade e agilidade com que recurso usar para gerenciar com eficiência toda a rede.

CAPITULO 4 - FERRAMENTAS DE GERENCIAMENTO DE REDES

4.1 WIRESHARK

4.1.2 Uma Breve História sobre o Wireshark

O Wireshark tem uma história muito rica. Gerald Combs, um pós-graduado de ciência da computação da Universidade de Missouri, em Kansas City, originalmente o desenvolveu fora de suas necessidades. A primeira versão do aplicativo Combs, chamado Ethereal, foi lançado em 1998 sob a GNU Public License (GPL). Oito anos depois de lançar o Ethereal, Combs deixou seu trabalho para perseguir outras oportunidades na carreira. Infelizmente, o seu empregador na época tinha plenos direitos sobre a marca Ethereal, e Combs não conseguiu chegar a um acordo que lhe permitiria controlar a marca Ethereal. Em vez disso Combs e o resto da equipe de desenvolvimento, rebatizaram o projeto como Wireshark, em meados de 2006.

4.1.3 Protocolos Suportados

O Wireshark suporta mais de 850 protocolos, estes protocolos como o IP e o DHCP são os mais comuns que os mais avançados protocolos proprietários, como o AppleTalk e BitTorrent. Isso porque o Wireshark é desenvolvido no âmbito de um modelo de codigo fonte aberta, o suporte de um novo protocolo é adicionado a cada atualização. Caso exista algum protocolo que o Wireshark não suporte, basta codificá-lo e submeter seu código aos desenvolvedores do Wireshark para inclusão na aplicação (caso código seja aceito).

4.1.4 Conceitos Iniciais

O Wireshark é uma ferramenta desenvolvida para realizar análise de pacotes que trafegam pela rede. É um software de código livre, (WIRESHARK, 2016) sob a licença GNU GPLv2 que dentre outras normas já difundidas entre os softwares livres, garante que o mesmo permaneça sempre com seu código-fonte aberto. (VIEIRA, 2011). Sendo suportado por uma enorme quantidade de plataformas como o UNIX, Linux, Solaris, FreeBSD, MAC OS X, Windows e outros sistemas, ou seja, praticamente qualquer computador pode utilizar o Wireshark.

Segundo DIEGO. M (2016) Wireshark é uma analisador de protocolos de rede de forma gráfica, que nos permite aprofundar em cada pacote que se move em uma rede. Podendo ser usado para capturar pacotes Ethernet, wireless, *bluetooth* e outros tipos de

tráfego. Ele pode decodificar diferentes protocolos que ele vê então você poderá, por exemplo, reconstruir o áudio de uma ligação Voice over IP (VoIP).

Essa ferramenta permite ao usuário ver todo o trafego que está passando pela rede, colocando a interface de rede em modo promíscuo. A forma padrão do arquivo de rastreamento de rede nativo do Wireshark é o formato Libcap, suportado também por outra biblioteca chamada de Winpcap. Portanto ele pode fazer a leitura de arquivos gerados e capturados por outras ferramentas analisadoras de pacotes, como por exemplo, o Tcdump ou traffic analyzer, que usam o mesmo formato de dados, e as informações coletadas podem ser lidas por esses mesmo softwares que utilizam a Libcap ou a Winpcap para ler os arquivos capturados.

4.1.5 Funcionamento

Segundo ALBERTO. M (2010), para ser capaz de analisar, por exemplo, o ponto de estrangulamento de uma rede envolvido na captura de pacotes com Wireshark é importante entender a estrutura da aplicação, e também como os pacotes recebidos são manipulados por diferentes camadas de um sistema operacional. As limitações impostas pelos componentes físicos do computador também devem ser levadas em consideração.

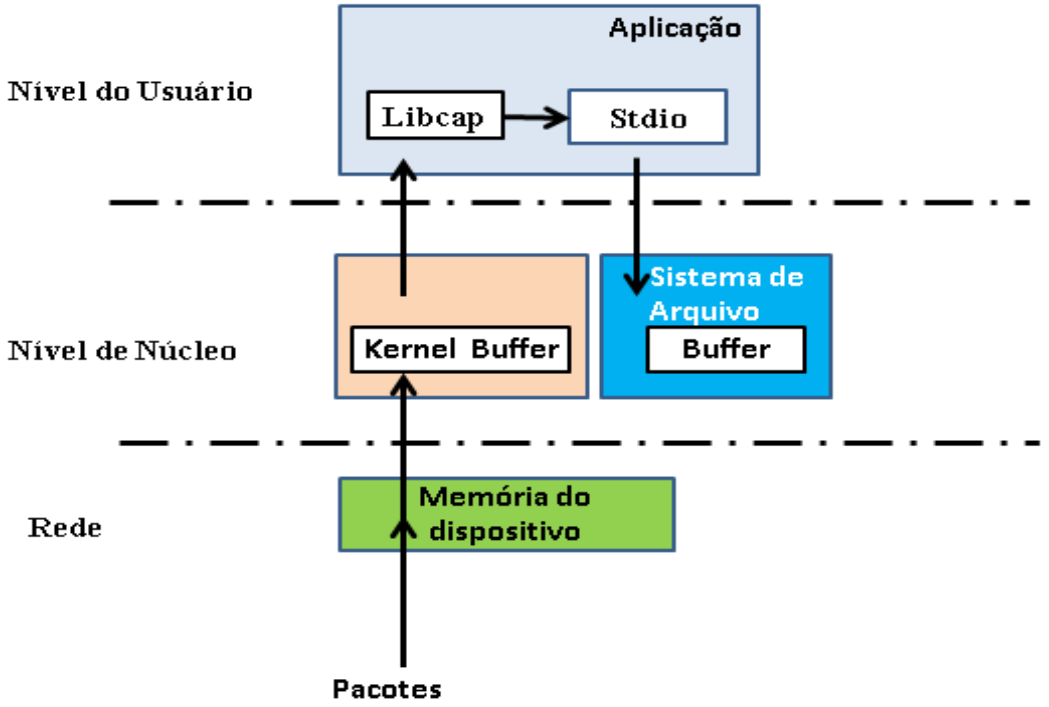
A aplicação Wireshark é o principal executável exposto em GUI (Interface gráfica de usuário) contendo também vários executáveis junto. Nesse conjunto de recursos vem um arquivo executável denominado de Dumpcap, que é uma aplicação da linha de comando que intercepta os pacotes e os carrega diretamente no disco sem realizar qualquer tratamento. Ao iniciar uma sessão de captura na GUI Wireshark, é iniciada uma instância do Dumpcap no console para assim realizar a verdadeira captura dos pacotes.

Em seguida o mesmo informa a GUI Wireshark do arquivo em que está escrevendo os pacotes , então é feito a leitura dos pacotes recém-capturados do arquivo que o Dumpcap está escrevendo, analisa-os, e os informa para o usuário. Para realizar o trabalho de baixo nível o Wireshark utiliza a biblioteca Libcap.

A imagem nº 5 exemplifica um fluxo normal de pacotes que chegam à rede ate o ponto que foi gravado no disco. Essa imagem demonstra um processo chamado de “2-copy”. Inicialmente a NIC (Interface gráfica de Usuário) recebe os pacotes e logo são copiados para a memoria do driver dispositivo. Caso ocorra de os pacotes necessitem ser copiados apenas uma vez antes da aplicação do usuário acessa-los, então um processo ”1-copy” foi obtido. Na

maioria das vezes essa copia realizada no processo seria um Buffer de Kernel que a aplicação do usuário também pode acessar.

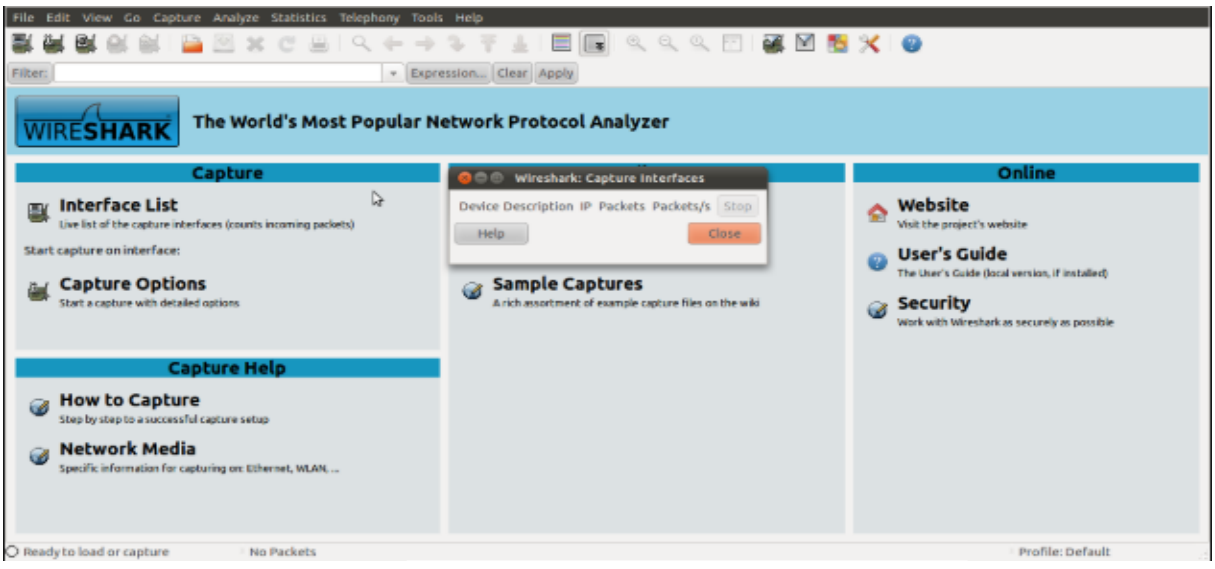
Figura 6: Fluxo de Pacotes



Fonte: Adaptada de Flow of packets [Dabir e Matrawy (2007)]

Tela de Funcionamento do Wireshark

Figura 5: Interface Inicial do Wireshark.



Fonte: Wireshar.org (2017)

4.1.6 Modo Promíscuo

Antes que você possa capturar os pacotes em uma rede, você precisará de um cartão de interface de rede (NIC) que suporte um driver de modo promíscuo. É o modo promíscuo que permite uma NIC ver todos os pacotes que atravessam o sistema de cabeamento. Quando uma placa de rede não está no modo promíscuo, ela geralmente vê uma grande quantidade broadcast e outros tráfegos que não é dirigida a ela, que serão descartados. Quando está no modo promíscuo, ela captura tudo e passa todo o tráfego que recebe para a CPU, basicamente ignorando as informações que se encontram na camada 2. Seu farejador (sniffing) de pacotes agarra todos os pacotes para dar lhe um relato completo e preciso de todos os pacotes no sistema.

4.2 Funcionalidades do Wireshark

4.2.1 Uso de Filtros

Uma vez iniciada a captura, é possível filtrar os pacotes capturados de acordo com a necessidade de quem está analisando, outro ponto a ter em mente é que, como os pacotes são obtidos de acordo com o filtro aplicado, é possível obter toda a sequência do pacote completo, se necessário. Existe uma grande variedade para aplicar de acordo com a necessidade.

A figura a seguir mostra um exemplo de filtragem a fim de reconhecer quais servidores foram conectados por solicitação de DNS. Os filtros são muito úteis e podem ser aplicados juntos como parte de operações lógicas. Eles podem ser usados na captura ou especificados anteriormente**,** para que eles capturem apenas o que é especificado no próprio filtro. Esse tipo de ferramenta não é usado apenas na análise de *malware,* mas também no estudo de protocolos de rede, na busca de vulnerabilidades e outros aplicativos.

4.2.2 Tipos de Filtros

4.2.2.1 Filtrar por IP de origem:

No inicio do campo do filtro selecione o protocolo, no caso desse tipo de filtro será o IP, deve ser colocado o tipo IP (Protocolo de Internet) caso seja Ipv4 ou Ipv6, criar a relação lógica e definir o pacote a ser capturado ou o IP’s que se deseja interceptar e filtrar.

4.2.2.2 Filtrar por Requisições GET do HTTP

Ao selecionar o tipo de filtro de requisições GET deve ser especificado que apenas as mensagens HTTP capturadas serão exibidas na janela de listagem de pacotes. A figura a seguir mostra o funcionamento.

4.2.2.3 Filtra por Requisições POST

Assim como nas requisições GET o método POST deve ser especificado que apenas as mensagens HTTP capturadas na janela de listagem dos pacotes. A figura a seguir mostra o funcionamento

4.2.2.4 Filtrar pela porta TCP

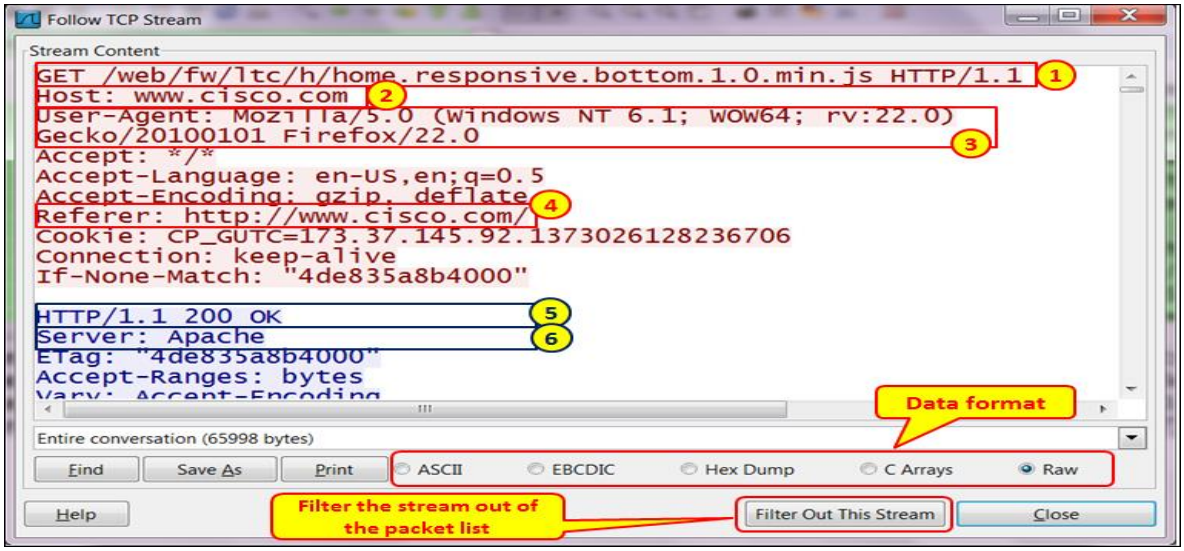
A filtragem de Porta TCP é como os exemplos anteriores, bastando apenas que no campo de filtragem seja indicada a relação de filtragem e indicando qual ou quais portas devem ser capturadas, podendo filtrar tanto a porta de origem, quanto a de destino. Dessa forma origem (tcp.srcport) ou destino (tcp.dstport).

4.2.3 Follow TCP Stream

Outra funcionalidade que o Wireshark dispõe é de poder seguir os fluxos do Protocolo, pode ser muito útil ver o protocolo da maneira que a camada de aplicativo o vê. Caso um usuário esteja procurando senhas em um fluxo Telnet ou esteja tentando entender um fluxo de dados. Talvez você só precise de um filtro de exibição para mostrar apenas os pacotes em um fluxo TLS ou SSL. Se assim for, a capacidade do Wireshark de seguir fluxos de protocolo será essencial.

Para fazer essa operação basta selecionar um pacote, seja TCP, UDP, TLS ou HTTP na lista de pacotes stream e conexão que deseja fazer a analise, então selecione o item de Follow TCP Stream no menu Wireshark Tools, o wireshark então irá configurar um filtro de exibição apropriado e abrir uma caixa de diálogo com todos os dados do fluxo TCP dispostos em ordem.

Figura 7: Tela, Fallow Tcp Stream



Fonte: DevMedia (2011)

4.2.3.1 Detalhes do Fluxo

- O GET - É marcado no número **1**.
- Solicitado o HOST – É marcado no número **2.**
- O tipo de Cliente, MOZILA FIREFOX – É marcado no número **3**.
- O Referenciador, neste caso, CISCO- É marcado no número **4.**
- A resposta HTTP ok – Marcado no número **5**.
- Tipo de SERVIDOR – Marcado no número **6**.

4.2.4 Informação Especializada

O Infos especialista é um recurso quer faz o registro de anomalias encontradas pelo Wireshark em um arquivo de captura, a principal ideia dessa funcionalidade é de melhorar a exibição de comportamento de Rede ”Incomum” ou basicamente mais transparente e notável. Contudo, tanto usuários iniciantes quanto os mais experientes identificaram com mais rapidez prováveis problemas de rede, ao se comparar com a varredura de lista de pacotes feita “Manualmente”. A tabela a seguir mostra algumas entradas de informações especialistas e seus detalhes.

Tabela 1: Entrada, informação Especializada.

Pacote #	Gravidade	Grupo	Protocolo	Resumo
1	Nota	Seqüência	TCP	ACK duplicado (# 1)
2	Bate-papo	Seqüência	TCP	Conexão redefinida (RST)
8	Nota	Seqüência	TCP	Mantenha vivo
9	Advertir	Seqüência	TCP	Retransmissão rápida (suspeita)

Fonte: Manual Guide Wireshark, Adaptada.

4.2.4.1 Detalhes da Tabela

4.2.4.1.1 Gravidade

Todas as informações de especialistas têm um nível de gravidade específico. Os seguintes níveis de severidade são usados, entre parênteses estão às cores nas quais os itens serão marcados na GUI, por exemplo, *Erro (vermelho)***:** problema grave, por exemplo, [Malformed Packet], *Avisar (amarelo)*: aviso, por exemplo, aplicativo retornou um código de erro "incomum" como um problema de conexão**,** *Bate-papo (cinza)*: informações sobre o fluxo de trabalho normal, por exemplo, um pacote TCP com o conjunto de sinalizadores SYN , *Nota (ciano)* **:** coisas notáveis, por exemplo, um aplicativo retornou um código de erro "normal" como HTTP 404.

4.2.4.1.2 Grupo

Existem grupos de informações especialistas, por exemplo, *Malformado***:** pacote malformado ou dissecador tem um erro, dissecação deste pacote abortado, ou *Remontar***:** problemas ao remontar, por exemplo, nem todos os fragmentos estavam disponíveis ou ocorreu uma exceção durante a remontagem, *Sequência* **:** sequência de protocolo suspeita, por exemplo, sequência não foi contínua ou foi detectada uma retransmissão Esses são exemplos de grupos, mas há uma vasta quantidade de outros exemplos de grupos que a ferramenta contem.

4.2.4.1.3 Protocolo

Especificar o protocolo no qual as informações de especialistas foram causadas.

4.2.4.1.4 Resumo

O resumo é uma parte adicional onde conterá as informações especializadas explicando as ocorrências de cada informação especialista na tabela.

4.2.5 Selos de Tempo

Marcadores de tempo, quando cada pacote que o Wireshark captura é carimbado com a hora que foi capturada, esses carimbos de hora serão salvos no arquivo de captura, assim eles estarão disponíveis para analise. Segundo Chris. S (2010) O tempo é essencial, especialmente na análise de pacotes, tudo o que acontece em uma rede é sensível ao tempo, Wireshark reconhece a importância do tempo e nos fornece várias opções configuráveis que lhe digam respeito.

Referências de tempo de um pacote permite que um usuário configure todos dos cálculos de tempo subsequente sejam feitos em relação a um pacote especifico.

4.2.6 Remontagem de Pacotes

Os protocolos de rede geralmente precisam transportar grandes blocos de dados completos, por exemplo, ao transferir um arquivo. O protocolo subjacente pode não ser capaz de lidar com esse tamanho de bloco (por exemplo, limitação do tamanho do pacote de rede) ou é baseado em fluxo como o TCP, que não sabe nada dos dados, por isso o protocolo de rede deve impor e manipular limites para cada bloco, distribuindo em pacotes menores.

Faz-se necessário determinar os limites de bloco no lado do recebimento, esse mecanismo chama-se Remontagem. Esse mecanismo é implementado para localizar, decodificar e exibir os dados fragmentados, encontrando cada fragmento de pacote correspondente deste fragmento, e mostrara os dados combinados como paginas adicionais no painel “Packet Bytes”.

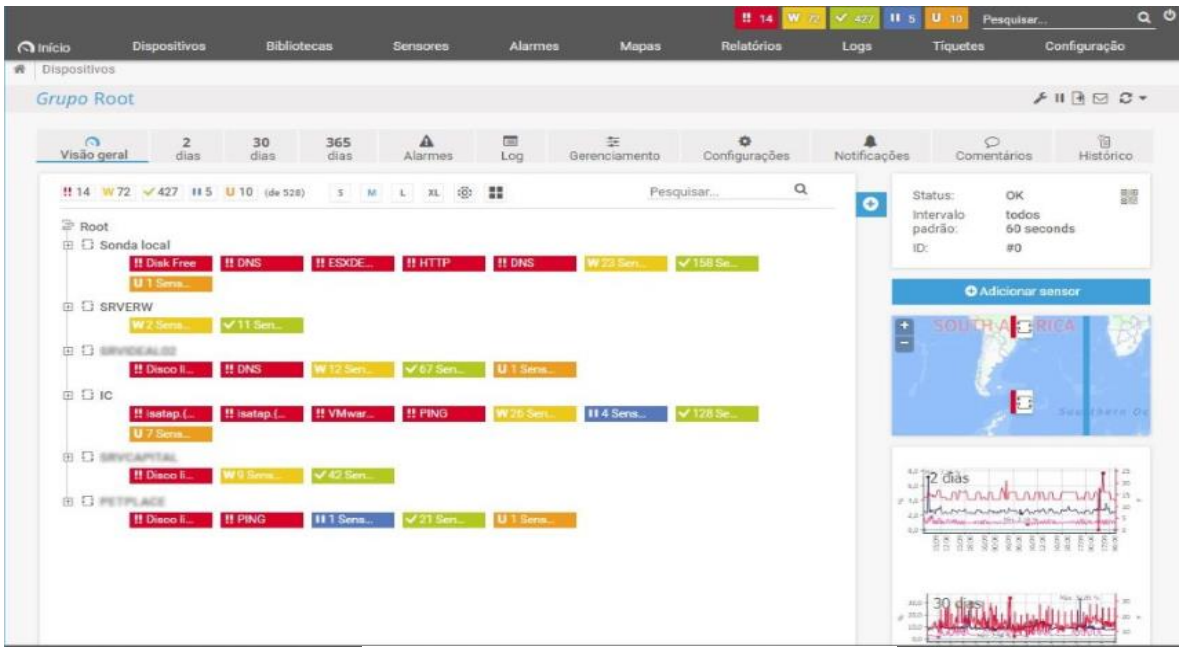
4.3 PRTG (*Paessler Router Traffic Grapher*)

É uma ferramenta de monitoramento de redes, baseada na plataforma Windows de sistemas operacionais, adequado para pequenas, medias e redes de grande porte, sendo capaz de monitorar LANs, WANs, VPNs e WLANs, na disponibilidade de rede e de como está ocorrendo o uso da banda, bem como fazer análises na qualidade de serviço, medir a carga de memoria, uso da CPU, assim como os principais outros hardwares da rede, como roteadores, servidores e sistemas.

É um software cheio de recursos, todos os dados coletados pelos protocolos de gerência de redes são armazenados em um banco de dados interno que podem ser revisados e analisados em longo prazo e fazer analises do estado atual ou um histórico da rede. O PRTG suporta protocolos SNMP (*Simple Network Management Protocol*), WMI (*Windows Management instrumentations*), *packet sniffer, NetFlow, sFlow, jFlow*.

O Monitoramento das informações é feita por meio de gráficos específicos gerados de acordo com o tipo de informação que se deseja. Este aplicativo é capaz de controlar e expor em gráficos personalizáveis informações sobre taxa de uso de hardware, tráfego de diversos protocolos, taxa de uso de banda de rede, assim como pode gerenciar componentes de rede, realizar conexões remotas a uma determinada máquina e também é útil para produzir mapas de conexões a partir de uma imagem da estrutura física da rede.

Figura 8: Interface Inicial PRTG



Fonte: Paessler (2018)

4.3.1 Estrutura do PRTG

Essa ferramenta de analise de rede é formada por módulos diferentes, e que podem ser divididas em três categorias, são elas; As Interfaces básicas de Administração, partes do Sistema e as Interfaces de Controle, cada parte dessas corresponde à infraestrutura que o PRTG foi desenvolvido e seu desempenho depende da integração das mesmas.

4.3.2 Interfaces Básicas de Administração

4.3.3 Partes do Sistema

Server Core: Como próprio nome já induz, seu funcionamento é comparado ao de um coração do PRTG, contendo todas as informações de armazenamentos dos dados, sendo também responsável por executar processos essenciais, como; Gestão de *Clauster*, Gestão e configuração de *Probes* conectadas, Banco de Dados no monitoramento de resultados, Gerar Relatórios, Gerar conta de Usuários, e muitos outros processos do sistema.

Probe(s): Sensores são configurados pelo Administrador, que fazem o monitoramento de todos os dispositivos do sistema e ao coletar todas essas informações, as mesmas são enviadas ao Server Core.

4.3.4 Interfaces de Controle

Servidor Web: Motor de relatórios e notificações do sistema, usado para realizar configurações no Server Core, como criar Login de Administrador, Fazer o endereçamento IPs do servidor web e de porta, assim como o idioma em que o sistema funcionará e outras.

PRTG Probe: A sonda, como é chamada, ela que faz o acompanhamento real, monitorada pelo Server core. E também usado para outras configurações mais básicas, como o nome da Probe, e configurações de conexão com o servidor.

Web Interface: É uma aplicação executada no browser Windows GUI, onde um aplicativo Windows comunica-se com o servidor núcleo usando API Ferramentas do Administrador para a configuração de senha/login e IP’s do servidor WEB.

Ajax Web Interface: A interface web baseada em Ajax é usada para configuração de dispositivos e sensores, bem como para a análise dos resultados da monitoração. Também é utilizada para administração do sistema de modo geral, e o gerenciamento de usuários e grupos.

4.3.5 Sistema de Notificações

O sistema de notificações é uma das principais funcionalidades do PRTG, pois caso ocorra qualquer eventualidade a integridade e funcionamento da rede, alertas são enviados ao administrador ou automaticamente a ferramenta executa ações de correção ou prevenção, como exemplos de eventos que mais ocorrem são a falha de sensores ou lentidão.

4.3.6 Licenças do PRTG

4.3.6.1 Freeware Edition

Este tipo de licença é indicado para redes que não necessitam de um alto grau de complexidade, sendo mais básica, para uso pessoal, podendo suportar até 10 sensores, no entanto esta licença suporta todos os tipos de sensores.

4.3.6.2 Trial Edition

Esta licença é voltada para clientes que queiram e desejam analisar a ferramenta PRTG, ou seja, no intuito de testar e avaliar o software com intenção de aquisição de licenças comerciais. Essa licença tem como características poder monitorar um numero ilimitado de sensores, suportando todos os tipos de sensores, diminuindo o intervalo de monitoramento para um segundo, quando na normalidade seria de no mínimo de dez segundos.

4.3.6.3 Special Edition

Esta licença proporciona ampliar o numero de sensores, passando a ter todos os sensores das licenças consideradas mais básicas e adicionando uma considerável quantidade de sensores adicionais.

4.3.6.4 Commercial Editions

Licença Comercial, voltada para redes maiores e mais complexas, e ainda oferecendo outras variações de acordo com a robustez e tamanho da rede, permite um numero ilimitado de sensores, permite instalação de Cluster Failover, composto por dois nós.

4.4 WHATSUP GOLD

É um software de uso simples para gerenciamento de redes produzido pela Ipswitch, Inc. A arquitetura expansível e escalável do WhatsUp Gold permite detectar, mapear e gerenciar toda a infraestrutura de TI: dispositivos de rede, servidor, aplicativos, recursos virtuais, configurações e tráfego de rede.

4.4.1 Funcionalidades

4.4.1.1 Análise do tráfego

Facilita a visibilidade detalhada do tráfego da sua rede para ver quais usuários, aplicativos e protocolos estão consumindo largura de banda. Essa percepção permite configurar políticas de uso de largura de banda, maximizar o retorno sobre os custos de ISP e garantir largura de banda adequada para aplicativos e serviços de negócios críticos.

4.4.1.2 Planejamento de capacidade de largura de banda

A capacidade de ver as tendências históricas de uso de largura de banda permite que o administrador fique à frente do planejamento da capacidade, ter a visibilidade de quais aplicativos estão gerando o consumo permite que o seja feito demonstração de um gerenciamento eficaz da largura de banda.

4.4.1.3 Monitoramento do desempenho de aplicativos

A ferramenta dispõe da funcionalidade de monitorar os aplicativos que compõe a rede, oferecendo perfis de monitoramento, com recomendações de práticas de uso, assim como o usuário pode criar seus perfis de monitoração. Com auxílio de alertas para definição de estados de aviso para cada situação que aplicativos possam a vir ocorrer.

4.4.1.4 Gerenciamento de configuração de dispositivos

Ações como Backup de configuração de rede, alertas de mudança de configuração, auditoria de conformidade com politicas, são funcionalidades que a ferramenta disponibiliza. O recurso Gerenciamento de configurações do WhatsUp Gold pode alertar os administradores de rede para alterações na configuração.

O *Configuration Management* alerta sobre quaisquer alterações detectadas toda vez que varre seu banco de dados de configuração. As verificações podem ser programadas para serem executadas automaticamente para encurtar a janela entre quando uma alteração é feita e quando um alerta é emitido.

4.1.1.5 Monitoramento de Nuvens

Os relatórios dos provedores de serviços na nuvem não são capazes de ajudar você a visualizar seus recursos baseados na nuvem dentro do contexto da sua infraestrutura geral. Isso gera lacunas de monitoramento de visibilidade. O WhatsUp Gold permite monitorar e enviar alertas e relatórios sobre o status e o desempenho de cada métrica disponível por meio das APIs da AWS ou do Azure, além de integrar esses dados em seu mapa de infraestrutura, central de alertas e dashboards.

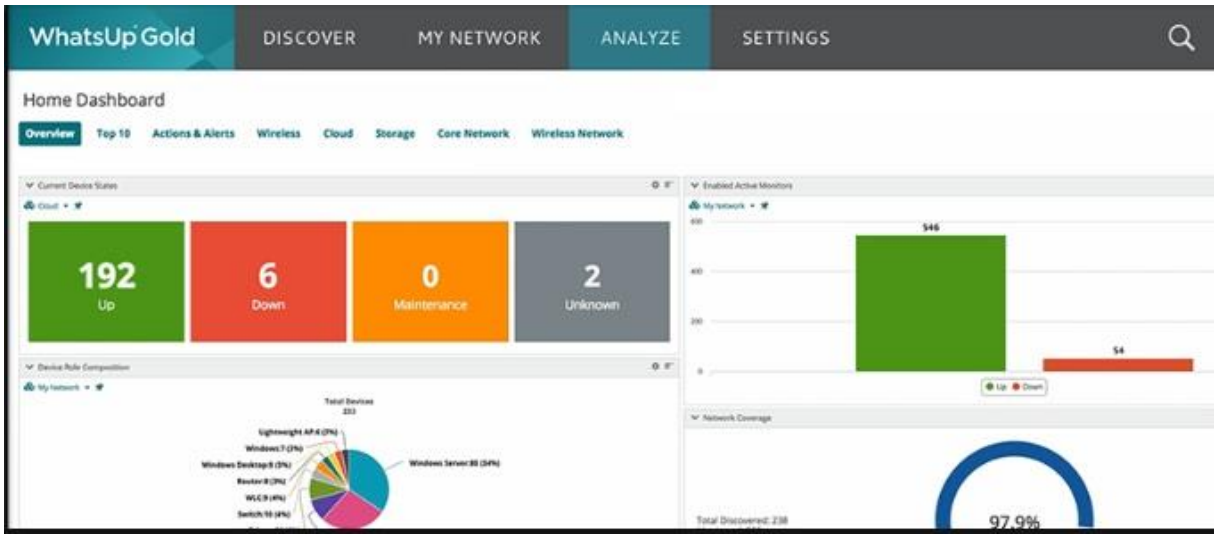
4.1.1.6 Licenças do WhatsUp Gold

WhatsUp Gold é vendido em três edições diferentes:

1. WhatsUpGold Premium
2. WhatsUpGold Standard
3. WhatsUpGold Distributed

Tela Interface WhatsUp Gold

Figura: Tela WhatsUp Gold



Fonte: WhatsUp.Com

4.5 SPARROW IQ

O SparrowIQ é uma solução de análise de tráfego baseada em pacotes e de monitoramento de desempenho de rede que fornece aos gerentes de rede visibilidade de tráfego quase em tempo real sobre o uso da rede com base em conversas, aplicativos, usuários e classe de serviço.

4.4.1Características principais

Controle Flow Analysis: O painel personalizado fornece estatísticas de uso de rede e é fácil de entender as outras principais funcionalidades desse recurso.

Uso de tráfego de rede através de vários pontos de dados, tais como:

1. Resumo geral do tráfego / estatísticas
2. Melhores Classes de Serviço
3. Uso de largura de banda por taxa
4. Volume de tráfego.
5. Relatórios de longo prazo baseados em fluxo.
6. Dashboard flexível e filtragem de relatórios.
7. Configuração de alerta personalizada para largura de banda e volume de tráfego.
8. Rastrear o uso de todo o departamento por meio de agrupamento de IP.

4.4.2 Requisitos

Para o SparrowIQ funcionar oferecendo todos os seus recursos para a rede, é necessário enviar uma cópia do tráfego da rede para a maquina SparrowIQ, através da técnica de SPAN (*Switched Port Analyzer*) espelhamento para uma porta que esteja livre, essa porta será chamada de Network Tap. Se estiver usando um Tap, as portas de entrada e saída precisam ser conectadas para permitir a passagem dos dados.

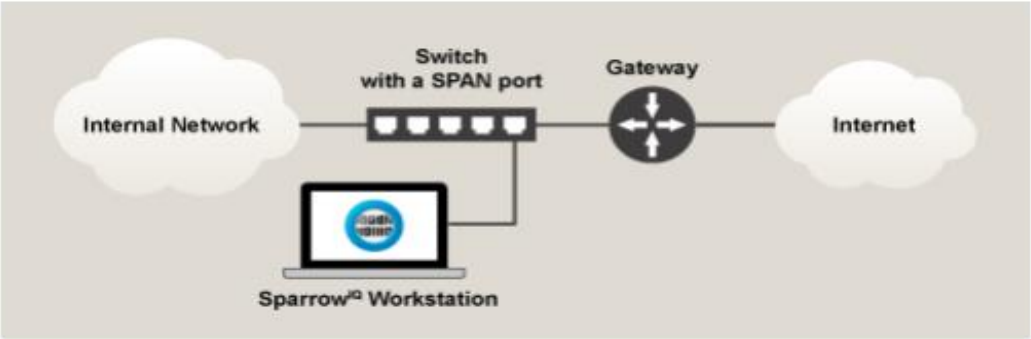
4.4.3 Ilustrando o Funcionamento

4.4.3.1Usando o comutador SPAN

Neste cenário de implantação, a estação de trabalho SparrowIQ é conectada diretamente a um comutador ou roteador que suporte o espelhamento de portas. Muitos dispositivos, até mesmo switches baratos, suportam recurso de alguma forma, embora possa ser conhecido como espelhamento de porta, SPAN (usado principalmente pela Cisco), ou

RAP (usado principalmente pelo equipamento da 3Com). Muitos fornecedores populares suportam este modelo. A figura exemplifica o funcionamento.

Figura 11: Funcionamento do Sparrow



Fonte: Sparrow Manual Guide

4.4.4 Funcionalidades do Sparrow IQ

4.4.4.1 Filtros

Esse recurso permite que o usuário concentre os resultados dos gadgets do painel selecionando determinados critérios nos quais executarem a análise. A ferramenta dispõe de modos de filtragem.

4.4.4.1.1 Endpoint

Através do endereço IP ou um endereço de host que foi adicionado à tabela de mapeamento, o usuário basta selecionar qualquer entrada no mapeamento, e inserindo parte do nome ou endereço e a busca é realizada automaticamente.

4.4.4.1.2 Grupo IP

Através de uma faixa de endereços IPv4 especificados são criados grupos com a interface Grupos no Página de configurações. Uma vez criados, esses grupos podem ser selecionados como filtros.

4.4.4.1.3 Aplicativos

Qualquer aplicativo encontrado na tabela de mapeamento de portas ou qualquer número de porta válida pode ser selecionado como um filtro de aplicativo. Observe que o preenchimento automático permite que o usuário selecione aplicativos de uma lista de correspondências.

4.4.4.1.4 Classe de serviço

Um filtro de classe de serviço seleciona dados com base em sua classe de serviço, conforme definido no cabeçalho de todos os pacotes IPv4.

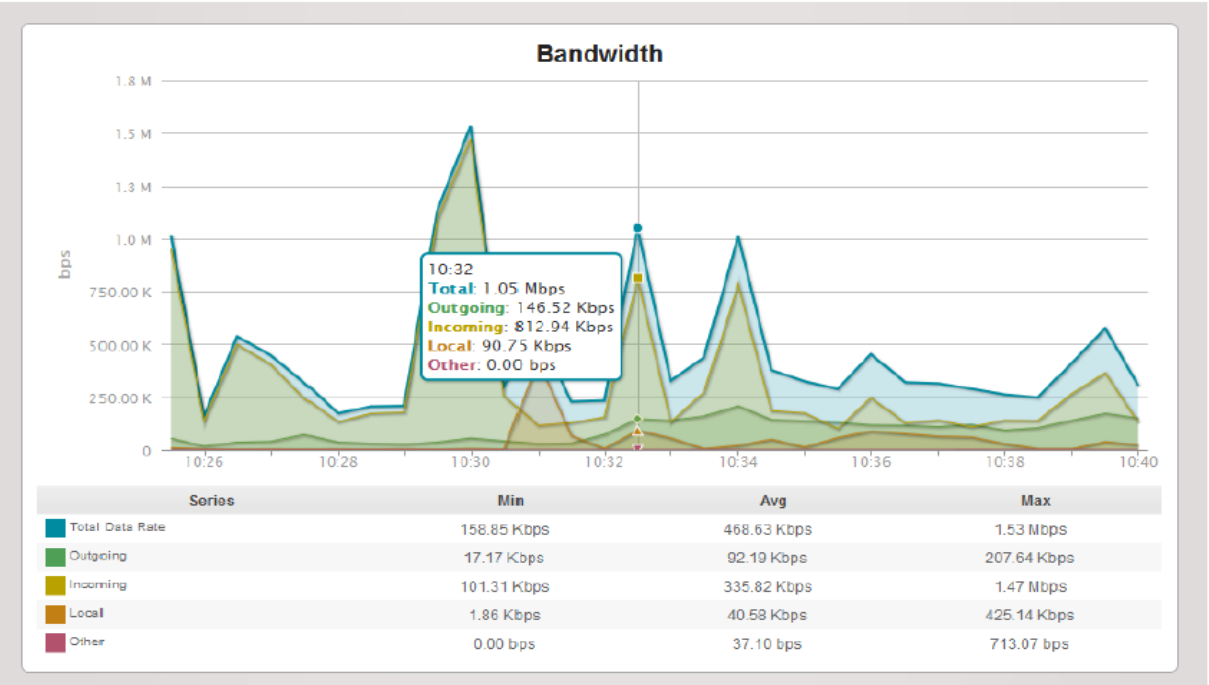
4.4.5 Path QoS

O recurso Path QoS é usado para monitorar e analisar a qualidade de uma conexão de rede entre o host SparrowIQ e outro host, seja em uma rede local ou global. Esta informação é útil para diagnosticar problemas com comunicações em tempo real, como VoIP, videoconferência ou streaming. Este widget permite configurar até 10 caminhos, dependendo da versão paga do SparrowIQ. Cada caminho analisa a rota do SparrowIQ host para o alvo configurado enviando fluxos de dados de teste para o destino e analisando as características de tempo das respostas.

4.4.6 Taxa de Largura de Banda

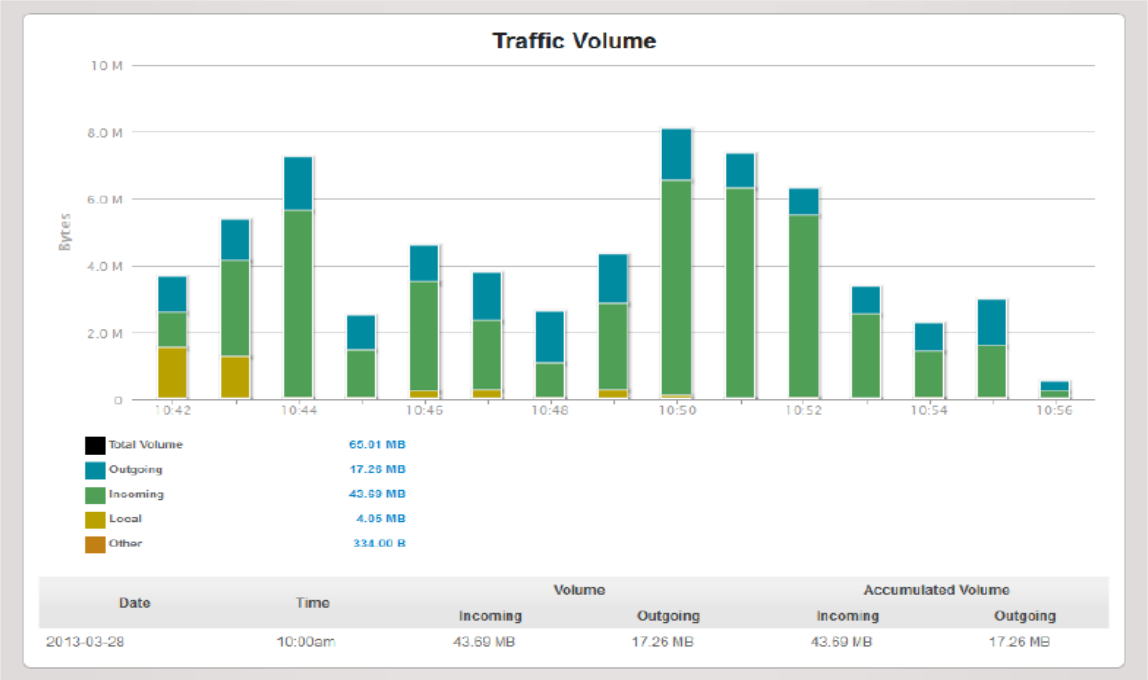
A taxa da largura de banda é exibida através de um gadget no qual exibe a largura geral medida no Gateway, essa funcionalidade exibe toda a taxa de trafego geral que a rede esta consumindo. A ferramenta mostra através de graficos bem detalhados todas as eventualidades da rede, a figura a seguir exemplifica todo o tráfego monitorado em uma fatia de tempo, e quais mudanças foram sofridas.

Figura 12: Painel de largura de banda



4.4.7 Volume de Tráfego

O gadget de volume de tráfego exibe o volume de tráfego na rede se o monitoramento do gateway tiver sido ativado e configurado, então o volume de tráfego será dividido para exibir as diferentes seções de entrada e saida do trafego. Essa funcionalidde gera gráficos que nos proporcionam mensurar e realizar analise da quantidade de volumes de dados trafegados



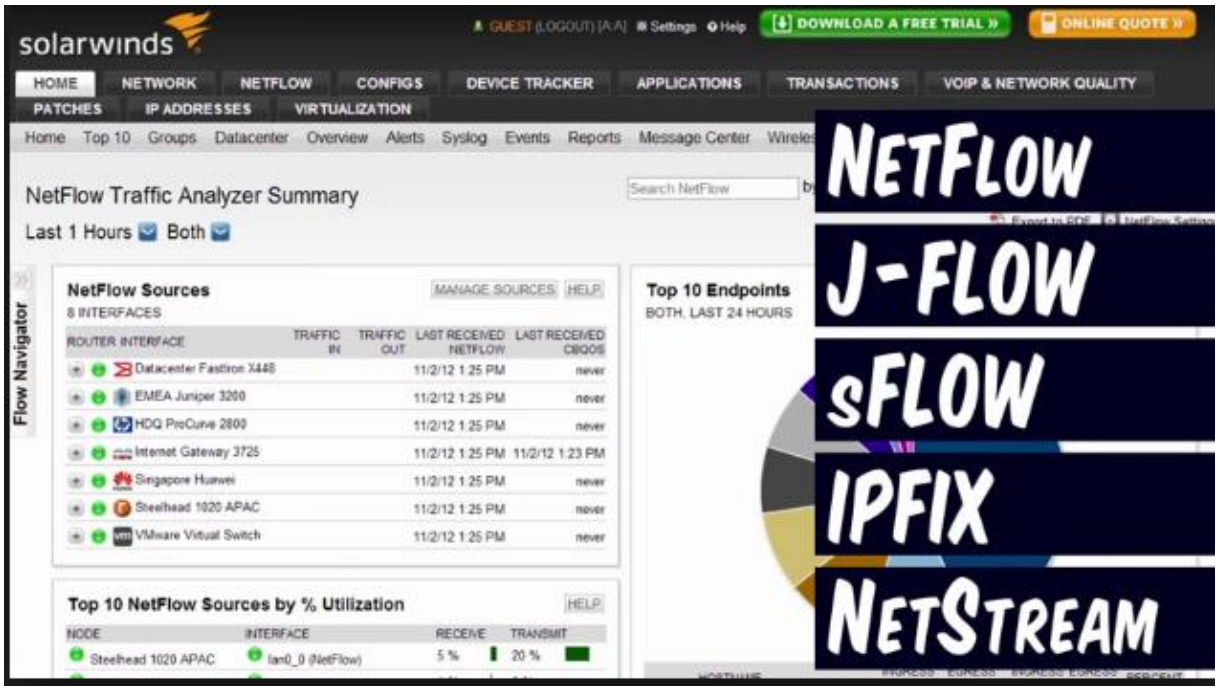
Fonte: Sparrow Manual

4.6 NETFLOW ANALYZER

O NetFlow Analyzer é uma ferramenta de monitoramento de largura de banda baseada na Web que realiza análises detalhadas de tráfego usando dados exportados dos fluxos *NetFlow ™ / Netflow ™ / cflowd ™ / J-Flow ™ / sFlow ™ / IPFIX ™ / AppFlow* . Esses dados fornecem detalhes granulares sobre o tráfego de rede que passou por uma interface. O NetFlow Analyzer processa essas informações para mostrar quais aplicativos estão usando a largura de banda, quem está usando e quando.

Gráficos extensos e relatórios intuitivos facilitam a análise dessas informações e também ajudam a acelerar o processo de solução de problemas. A ferramenta vem pré-carregado com um conjunto de recursos que fornecem estatísticas detalhadas de uso de largura de banda e permite que você faça uma busca detalhada para ver mais detalhes sobre tráfego, aplicativo ou conversa de largura de banda, etc. Este recurso também inclui outras opções administrativas que ajudam no gerenciamento redes corporativas e utilização de largura de banda com facilidade.

Figura 14: Interface Netflow Analyzer



Fonte: Solar Winds(2017)

A partir de sua instalação no roteador Cisco, o NetFlow passa a identificar os pacotes de dados não mais isoladamente, como outras tecnologias, mas como fluxos, com início, meio

e fim. Quando os fluxos são identificados, eles são armazenados no NetFlow Cache para caracterização e compreensão do tráfego da rede. Após 30 minutos são apagados da memória.

4.5.2 Os benefícios da tecnologia NetFlow

4.5.2.1. Identificação das aplicações na rede

Pode-se saber quais são as aplicações que estão utilizando a rede e identificá-las, visando otimizar o fluxo de informações para que os processos mais importantes recebam maior banda.

4.5.2.2 Detecção de Anomalias

Muitas anomalias nas redes comprometem a velocidade de operação e, consequentemente, o trabalho do usuário. Com o NetFlow é possível detectar essas anomalias e reduzir sua ação, melhorando o fluxo de dados e a velocidade da rede.

4.5.2.3 Verificação de instabilidades

As instabilidades da rede também são causas de atrasos em processos internos, deixando os usuários ociosos ou improdutivos. Ao instalar a tecnologia NetFlow nos roteadores, a equipe de TI pode verificar tais instabilidades e mitigar as causas, melhorando a qualidade do serviço.

4.5.2.4 Leitura do uso dos recursos na rede

O NetFlow é eficaz na identificação do uso dos recursos na rede, segmentando as aplicações que mais consomem sua velocidade. Tendo essa informação em mãos, fica mais fácil adequar os processos e direcionar o fluxo de dados de acordo com a necessidade, tornando a rede mais estável e segura.

4.5.2.5 Identificação de impactos na rede

Causas estranhas que impactam na rede podem ser descobertas através do NetFlow com facilidade, permitindo que a equipe de TI atue em cima do problema para que seja solucionado o mais rápido possível.

4.5.2.6 Redução de vulnerabilidades

Com a identificação do tráfego que passa pela rede, caracterização das aplicações e fluxo de dados, é possível reduzir as vulnerabilidades da rede e evitar a entrada de agentes estranhos que possam impactar na banda ou na própria rede.

4.5.3 As principais vantagens de utilização do Netflow são:

1. Funcionamento como cache para acelerar os *lookups* nas tabelas de roteamento;
2. Dispensa a verificação de tabelas de *access-list* (apenas de entrada) toda vez que um pacote chega, ficando mais eficiente o processo de roteamento;
3. Permite a exportação das informações de fluxo utilizadas pelo cache do Netflow, facilitando a coleta de dados para futuras análises sem a necessidade de colocar um analisador em cada enlace.

4.5.4 Principais Motivos para Uso da Ferramenta

1. Entender o comportamento de trafego da rede da Organização
2. Identificar a origem dos problemas ocasionados ou gerados por anomalias do tráfego.
3. Validar o impacto das mudanças planejadas na rede.
4. Identificar a causa-raiz do congestionamento da rede.
5. Medir consumo de links de cada aplicação ou usuário.
6. Identificar quais são as aplicações que mais consomem banda

4.5.5 Simplificando a Definição da Ferramenta

Na prática, o Netflow é um software que caracterizar a operação da rede, sendo fundamental para mapear o comportamento da rede, incluindo: aplicação e uso, eficiência e utilização dos recursos, impacto de mudanças e alterações, anormalidades e vulnerabilidades. A ferramenta cria um ambiente com ferramentas para compreender “quem”, “o que”, “quando” e “como” o tráfego flui pela rede, permitindo melhorias nos processos e adequações do ambiente às necessidades de negócio.

A capacidade de caracterizar o tráfego IP e entender “onde” e “como” ele flui é fundamental para o desempenho da rede, disponibilidade e solução de problemas. O monitoramento dos fluxos de tráfego IP facilita o planejamento de capacidade e assegura que os recursos sejam utilizados de forma adequada e em apoio às metas organizacionais. Ajudando a determinar onde aplicar o QoS, otimizar o uso de recursos e desempenha um papel vital na segurança da rede ao detectar ataques de negação de serviço (DoS), propagação de *worms* e outros eventos indesejáveis na rede

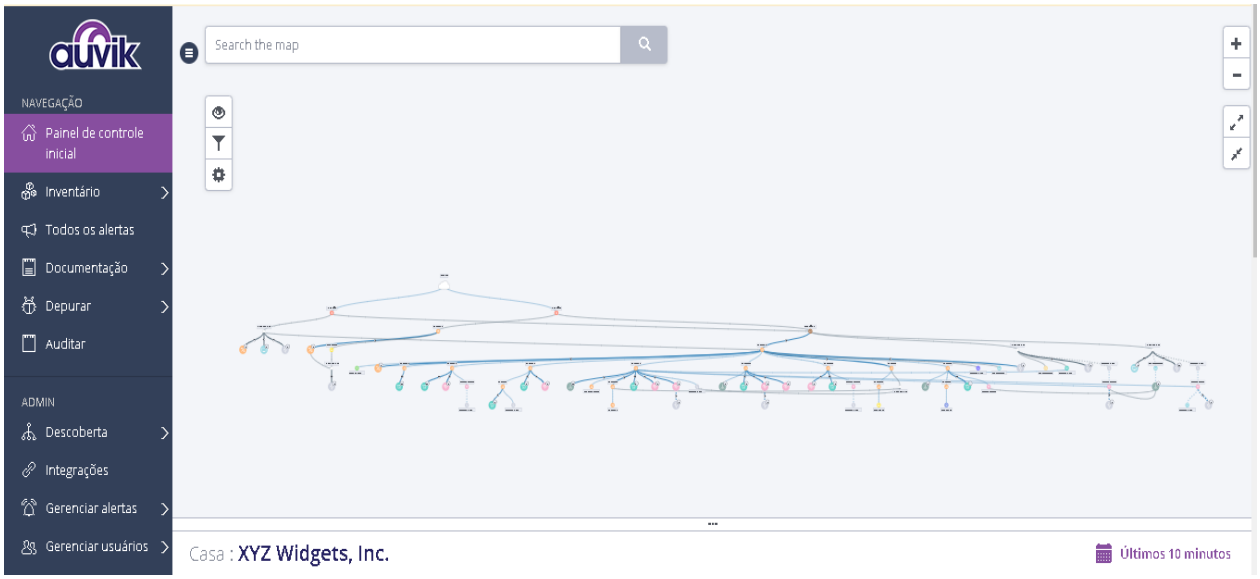
CAPITULO 5 – TESTES E ANÁLISES DOS RESULTADOS

Os testes abordados neste trabalho tiveram propósito de coletar as informações em cada ferramenta, no cenário em estudo, e visualizar os gráficos de consumo de CPU, Memória, disco, Tráfego entrada e saída, destacar as funcionalidades de cada uma, e destacando as ferramentas que seriam mais adequadas, consideradas “Melhores” para o Gerenciamento e Monitoramento de redes.

5.1.2 Netflow Analyzer integrado a plataforma AUVIK serviço em nuvem.

Para o cenário de testes da ferramenta Netflow Analyzer foi necessário ser realizado em nuvem, utilizando uma versão Demo de validade de 14 dias para testes, a Empresa AUVIK disponibiliza essa versão para que usuários possam testar a ferramenta seja em sua rede domestica, empresarial, podendo tambem simular redes para realização de teste, para a realização deste trabalho foi escolhido por realizar o teste por simulação de uma rede de Medio porte com 77 dispositivos, mas o teste foi realizado em uma sub rede contendo 7 computadores, todos possuem a mesma configuração, a ferramenta de disponibiliza configurar esse tipo de informação (Sistema Operacional, Memóra, Processador e aramazenamento) na plataforma, o teste entao consiste em coletar os dados da rede num periodo de 10 minutos. A imagem a seguir mostra como ficou configurada a topologia da rede para o cenario de testes na plataforma.

Figura 15: Interface de Topologia da rede



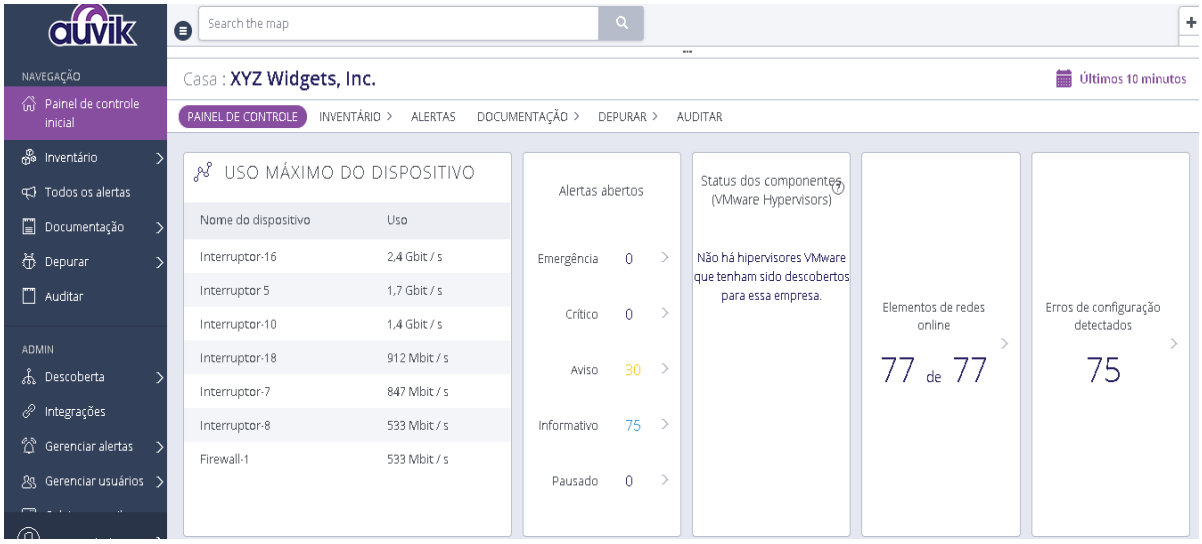
Fonte: Própria do Autor

A tela a seguir mostra que ao realizarmos uma busca de dispostivos que mais estão consumindo, a ferramenta ainda dispõe da função Alerta, e ao realizar uma busca ela nos informa os alertas abertos.

5.1.2 Taxa de Uso Máximo Por Dispositivo

Para a análise de consumo por dispositvo a ferramenta oferece um Ranking de dispositvos que apresentam um alto consumo, ao realizar a busca a ferramenta nos mostra quais dispostivos mais consumiram.

Figura 16: Tela de Uso dos Dispositivos



Fonte: Própria do autor.

A ferramenta então detecta que dispositivos estão com consumos elevados, são eles;

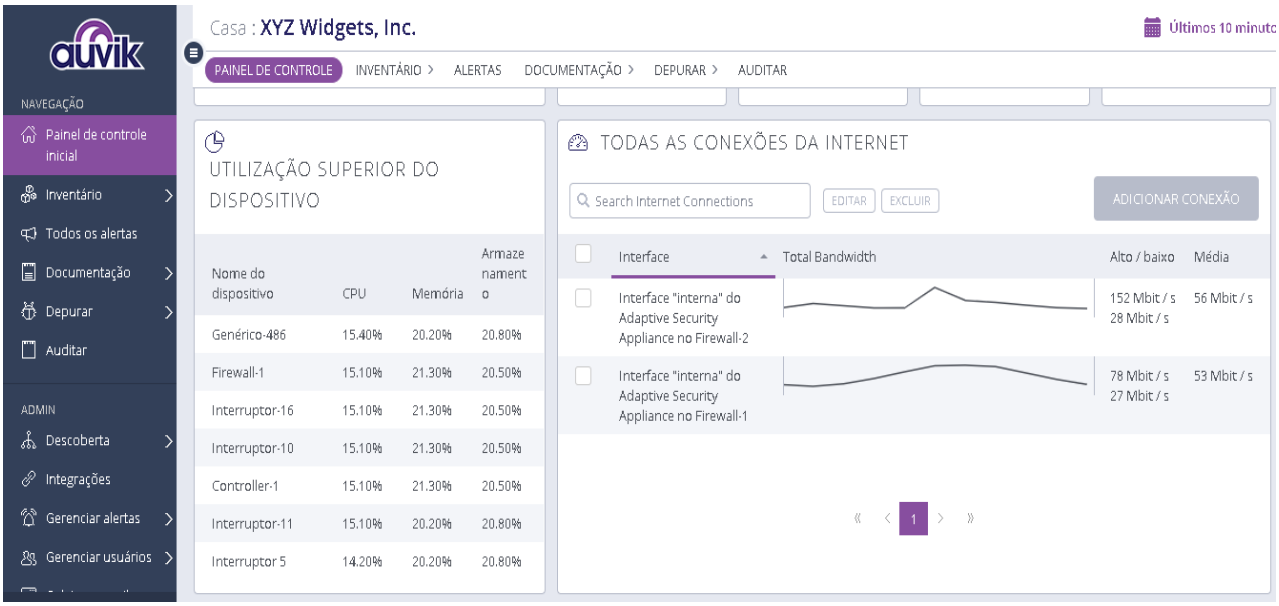
1. Computador 16 com consumo médio de 2,4 Gbits/s.
2. Computador 5 com consumo médio de 1,7 Gbits/s.
3. Computador 10 com consumo médio de 1,4 Gbits/s.
4. Computador 18 com consumo médio de 920 Mbit/s.
5. Computador 7 com consumo médio de 850 Mbit/s.
6. Computador 8 com consumo médio de 533 Mbits/s.
7. Computador 1 com consumo de 533 Mbits/s

Ainda na mesma tela podemos observar quais alertas estão em aberto e qual o nível identificado, a ferramenta define os níveis de alerta em: Emergência, Critico, Aviso, Informativo e Pausado.

5.1.3 Taxa de Uso da CPU, Memória e Armazenamento.

A tela a seguir mostra os resultados obtidos ao realizar uma busca na rede, e identificar quais dispositivos mais consomem CPU, Memória e Armazenamento, na mesma tela podem ser visualizadas todas as conexões de internet.

Figura 17: Interface de Utilização do Dispositivo



Fonte: Própria do autor.

A tabela a seguir mostra os resultados obtidos ao ser feita a busca dos dispositivos quanto ao seu consumo de CPU, Memória e Armazenamento. É importante destacar que a ferramenta informa o consumo que cada dispositivo apresenta na rede, mas para exemplificar e idealizar o proposito dos testes foi capturado apenas o consumo de sete dispositivos.

Tabela 2: Coleta dos Dados Netflow Analyzer

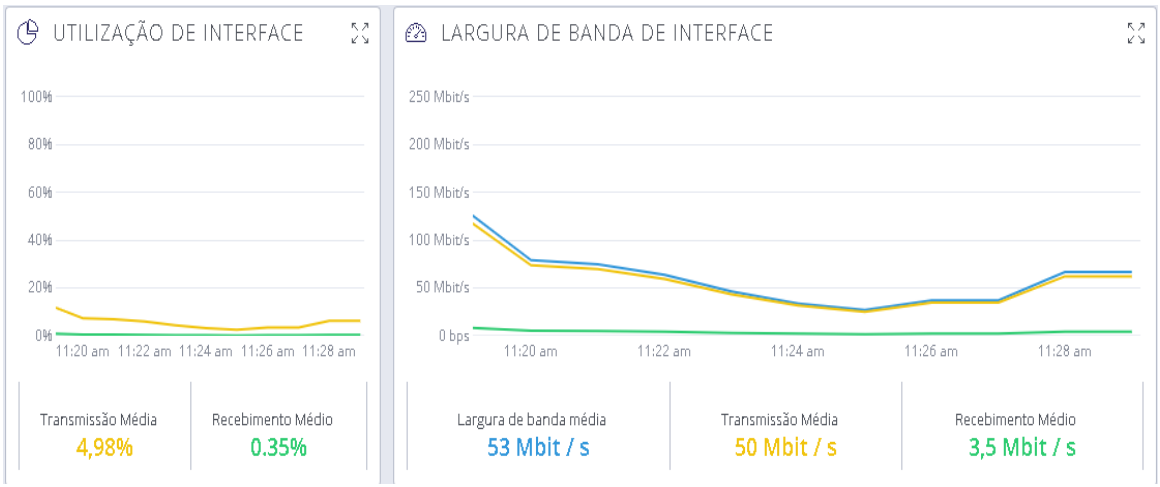
Nome do Dispositivo	CPU	Memória	Armazenamento Interno
Genérico 495	17,20%	20,20%	20,90%
Firewall	18,10%	20,30%	20,90%
Interruptor 16	19,40%	21,30%	20,90%
Interruptor 10	15,10%	21,10%	20,90%
Controller 1	20,10%	21,30%	20,90%
Interruptor 11	18,10%	20,20%	20,90%
Interruptor 5	14,20%	20,20%	20,90%

Fonte: Própria do Autor.

5.1.4 Mudança do Comportamento da Conexão de Internet

Para o teste foi usada uma conexão de internet, a ferramenta possibilita adicionar ainda mais conexões dependendo da eventualidade, e analisadas em um espaço de tempo de 10 minutos. É possível analisar no gráfico de variação o quanto a rede oscilou nesse período.

Figura 18: Largura de Banda e Utilização de interface.



Fonte: Própria do Autor

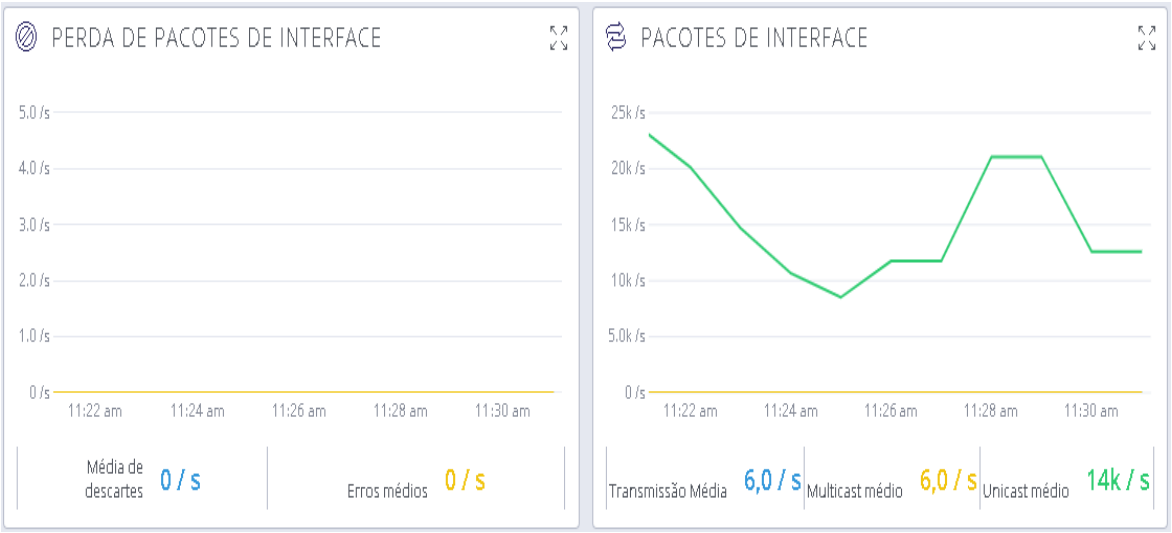
Os gráficos mostram o quanto à rede variou nesse período de tempo, saindo de um ponto alto de envio de banda, e reduzindo consideravelmente no decorrer da transmissão, tendo como média 50 Mbits/s de envio e uma taxa de 3,5 Mbits/s de recebimento. Ainda no

painel ao lado podemos ver a taxa de utilização da interface, com uma taxa de transmissão média de 4,98% e o recebimento médio de 0.35%.

5.1.5 Perda de Pacotes

Pelo fator tempo definido ser pequeno as perdas foram zero, contudo podemos ver a variação dos pacotes de interface no gráfico da direita, onde oscilou com uma transmissão média de 6,0/s, Multicast médio de 6,0/s e o Unicast médio foi de 14K/s. Dentro de uma organização que queira mensurar as perdas que a sua rede vem sofrendo, esses dados são essenciais, para que possa ser tomadas decisões e prevenções de melhorias na transmissão sem que haja um alto índice de perdas.

Figura 19: Perda de Pacotes



Fonte: Própria do Autor

5.2 Coletas de dados e análise com a ferramenta PRTG

Inicialmente instalado a ferramenta PRTG cria dois arquivos, a CONSOLE e PRTG networking Monitor, esse recurso então funciona via browser no caso a versão DEMO usada neste trabalho, caso seja para projetos mais complexos que explorem ainda mais recursos, há a versão paga desse software, oferecendo um conjunto ilimitado de sensores.

Para este cenário de teste, foi usada uma rede semelhante a que foi usada no cenário da ferramenta Netflow analizer, com a mesma quantidade de computadores, nas mesmas condições, para observar as mudanças que a mesma rede sofreu, só que com os dados

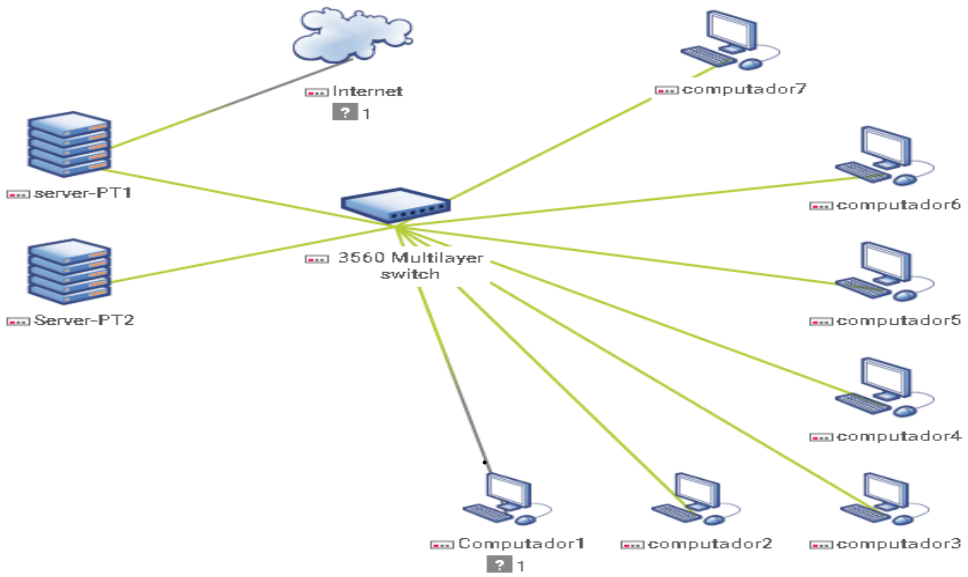
estatísticos usados com a ferramenta PRTG, os gráficos a seguir mostram a coleta dos dados e variação da rede.

O diferencial da ferramenta PRTG foi poder adicionar mais sensores para coletar mais dados da rede. Os sensores adicionados foi o de tráfego de entrada/saída. O PRTG tal como a ferramenta Netflow Analyzer e Sparrow IQ apresenta o tráfego em forma de gráficos, porém destaca-se por apresentar tabelas integradas aos gráficos com dados numéricos sobre o tráfego passado em cada estação.

5.2.1 Topologia Lógica da rede

Para o teste com a ferramenta PRTG foi criado uma rede com 7 computadores, todos utilizando o sistema operacional Windows, todas as maquinas tem a mesma configuração de memória, processador e armazenamento, na rede então foi posto dos servidores, e um hub para fazer a conexão das maquinas e a conexão de internet é um link de 5 Mb/s dedicados.

Figura 20: Topologia lógica da rede



Fonte: Própria do Autor

5.2.2 Dados coletados pela ferramenta PRTG

A tabela a seguir mostra os dados coletados pela ferramenta, em dez minutos de tráfego, as informações contidas na tabela são; O tráfego de entrada máximo que computador teve na rede, assim como o tráfego de saída mínimo, o quanto foi usado de CPU por cada ativo na rede, e o uso da memória, para esse teste foi adicionado o sensor de coleta de trafego,

SNMP traffic, a ferramenta destacou-se por ter essa gama de sensores, que facilitam o administrador de redes a identificar uma ocorrência na rede, sendo avisado por alertas que são emitidos a cada evento na rede.

Tabela 3: Dados Coletados pela Ferramenta PRTG

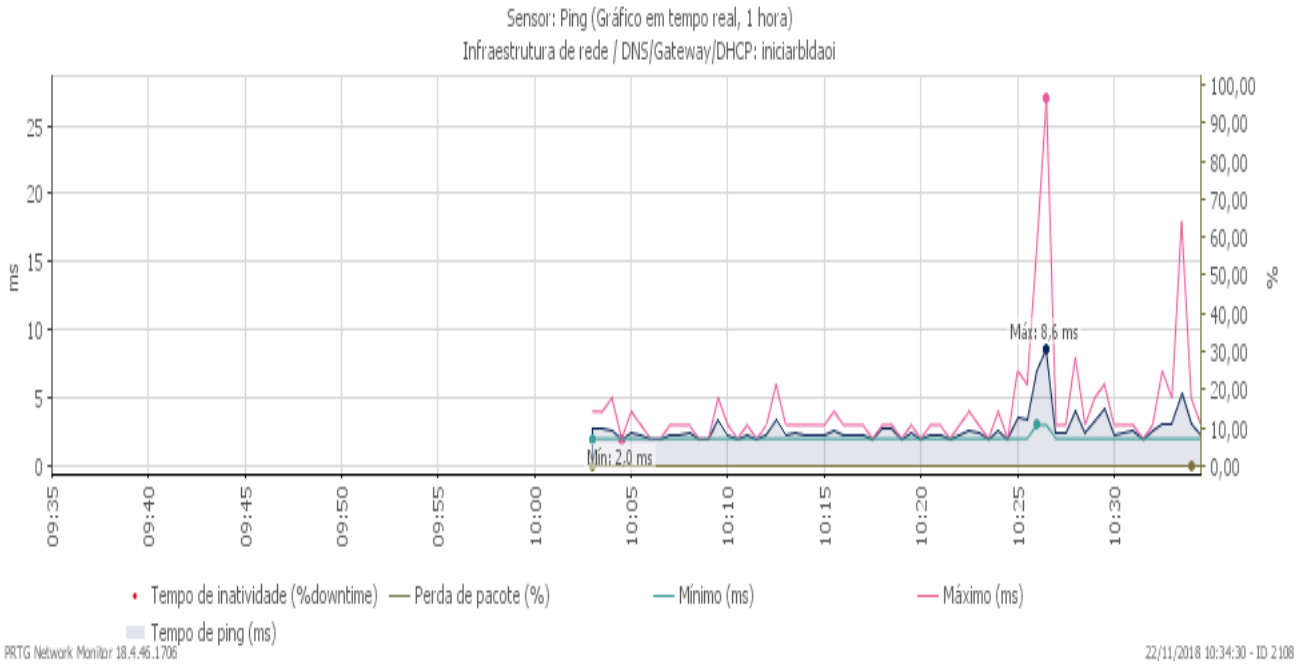
Ativo	Tráfego de entrada Máximo KB/s	Tráfego de Saída Mínimo KB/s	Uso da CPU	Uso da Memória
Computador 1	77,1	4,1	15,20%	18,20%
Computador 2	48,2	3,2	15,10%	14,10%
Computador 3	80,4	28,4	15,40%	20,40%
Computador 4	34,9	24,7	14,10%	18,10%
Computador 5	67,8	16,5	15,20%	18,20%
Computador 6	74,6	44,8	15,10%	17,10%
Computador 7	45,7	3,9	14,20%	15,40%

Fonte Própria do Autor

5.2.2.1 Gráficos dos Sensores Adicionados a Rede

5.2.2.2 Gráfico de PING

Figura 21: Gráfico de coletas de Ping.



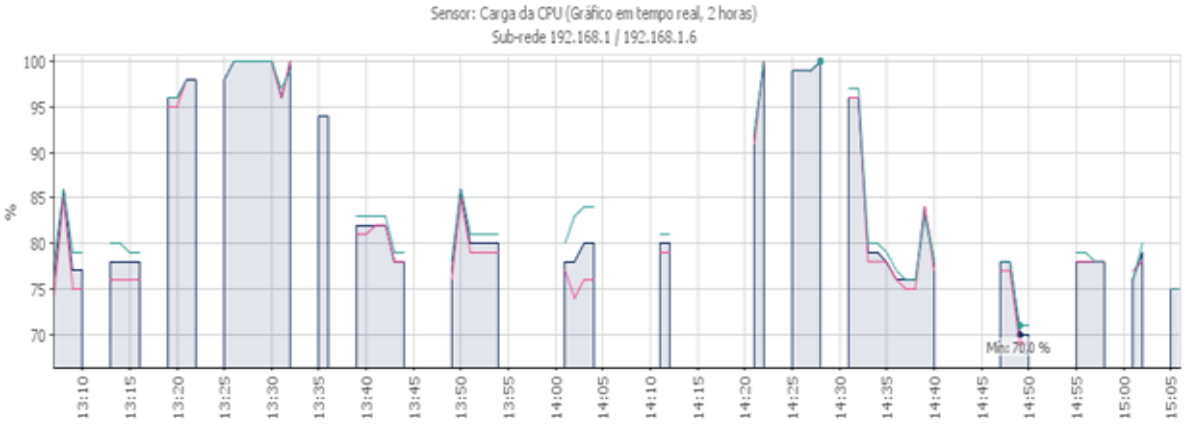
Fonte própria do Autor

O gráfico mostra a variação de Ping dos ativos de redes, as legendas mostram as informações de cada linha do gráfico, a cor vermelha mostra o tempo de inatividade da rede, a cor preta informa a perda de pacotes, a cor azul define o mínimo em (ms) a variação de ping, e a cor lilás mostra o máximo de atingido pela rede, por fim a cor cinza mostra o tempo de ping da rede.

Os dados coletados pelo gráfico são que a média do tempo dos 7 ativos de rede são de 6ms e o tempo mínimo foi de 2ms, já o valor máximo da média que a rede atingiu de ping foi de 20ms, com a perda de pacotes média de 1%. A ferramenta ainda mostra esses dados individuais de cada ativo que faz parte da rede, o gráfico então ilustra média dos valores coletados. Então podemos perceber que todos os dispositivos da rede estão disponíveis.

5.2.2.2.1 Gráfico de Carga da CPU

Figura 22: Gráfico de carga de CPU, sensor de carga.



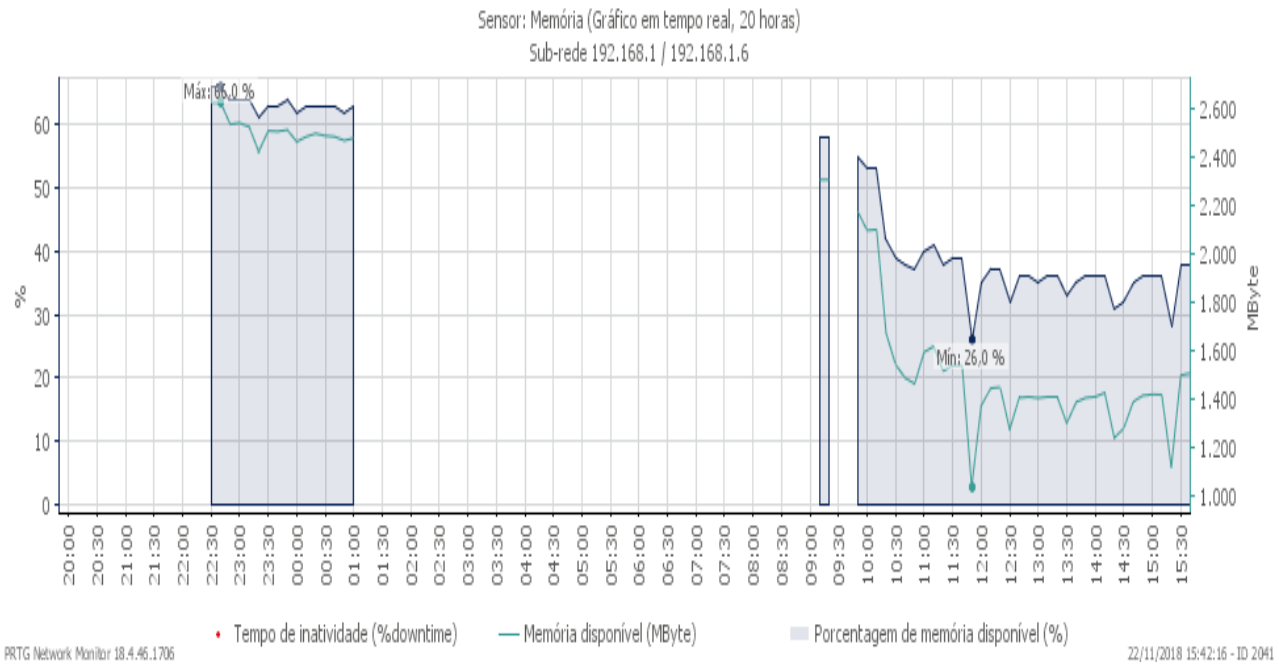
Fonte: Própria do Autor

O gráfico da carga de CPU média da rede permite mostrar o quanto foi o consumo médio da rede, podemos ver no gráfico o consumo médio de cem por cento, a linha azul representa os consumos máximos que a rede chegou, e a linha vermelha significa o mínimo de consumo, para o consumo máximo, a média foi de 86 %, para o consumo mínimo a média foi de 70 %, o diferencial do sensor utilizado é que, quando o consumo está muito alto, são enviados alertas para o administrador de que algo está errado, no painel ainda é informados que ativos ou quais fatores estão causando aumento do nível de consumo, assim como as ações a serem feitas.

Quanto aos dados gerados pelo gráfico, a ferramenta dispõe o gráfico de dois, trinta até trezentos e sessenta e cinco dias com os dados coletados nesse período, mas caso o administrador queira analisar um determinado tempo, a software divide o tempo de coleta em fatias de cinco em cinco minutos.

5.2.2.2.2 Gráfico de Memória

Figura 23: Gráfico da Memória PRTG



Fonte: Própria do autor

O gráfico mostra os períodos em que a rede mais consumiu memória, podemos ver que as fatias de tempo no gráfico estão divididas, ao realizar a coleta de dos dados, foi configurado na ferramenta, mostrar no gráfico em que período do dia teria o maior consumo, assim como o menor. Como a ferramenta funciona em tempo real, podemos ver que entre as 22:30 e 00:30 houve o consumo máximo de 65,0 % de memória, e entre as 10:00 e 15:30 do dia seguinte foi o momento em que menos houve consumo 26,0%. Quanto à porcentagem geral de memória disponível foi constatada que 46% disponíveis, podemos ver que mais de 50% da memoria geral da rede estava sendo consumida.

5.2.3 Teste e Dados Coletados com a ferramenta WhatsUp Gold

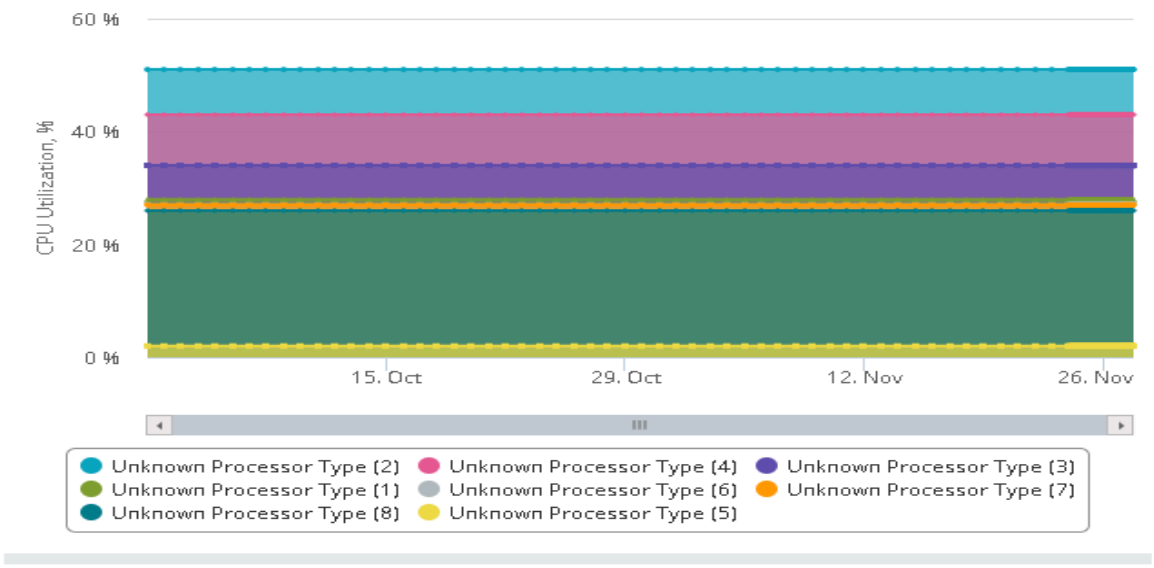
Para o teste com essa ferramenta, o cenário de redes foi o mesmo utilizado com as ferramentas PRTG NETWORK e NETFLOW ANALYZER afim de análises do uso das mesmas nos mesmos cenários e métricas de análises, para esse teste foi desenvolvida e configurada a rede na plataforma WhatsUp Gold, como é uma ferramenta que funciona na tecnologia de Computação em Nuvens, o cenário do teste pode ser configurado de acordo com as outras ferramentas já citadas nesse trabalho.

Essa ferramenta é uma que teve um bom destaque, pois apresenta uma gama de recursos para o gerenciamento de redes, os dados coletados por ela são mantidos salvos em um banco de dados interno da ferramenta, nela o administrador pode ver toda infraestrutura da rede, assim como executar uma vasta quantidade de funcionalidades, ações de prevenção, dados analisáveis por meio de painéis e gráficos. Pelo fato da ferramenta ter sido testada na versão Demo, ficou limitada para alguns recursos, mesmo assim ela proporcionou gerar informações plausíveis e consistentes para ser implantado em grandes empresas, um exemplo é a Petrobrás, grande organização que utiliza esse software em suas redes.

Os dados coletados pela ferramenta são ilustrados por gráficos que mostram o quanto foi as variações da rede.

5.2.3.1 Gráfico da Carga da CPU

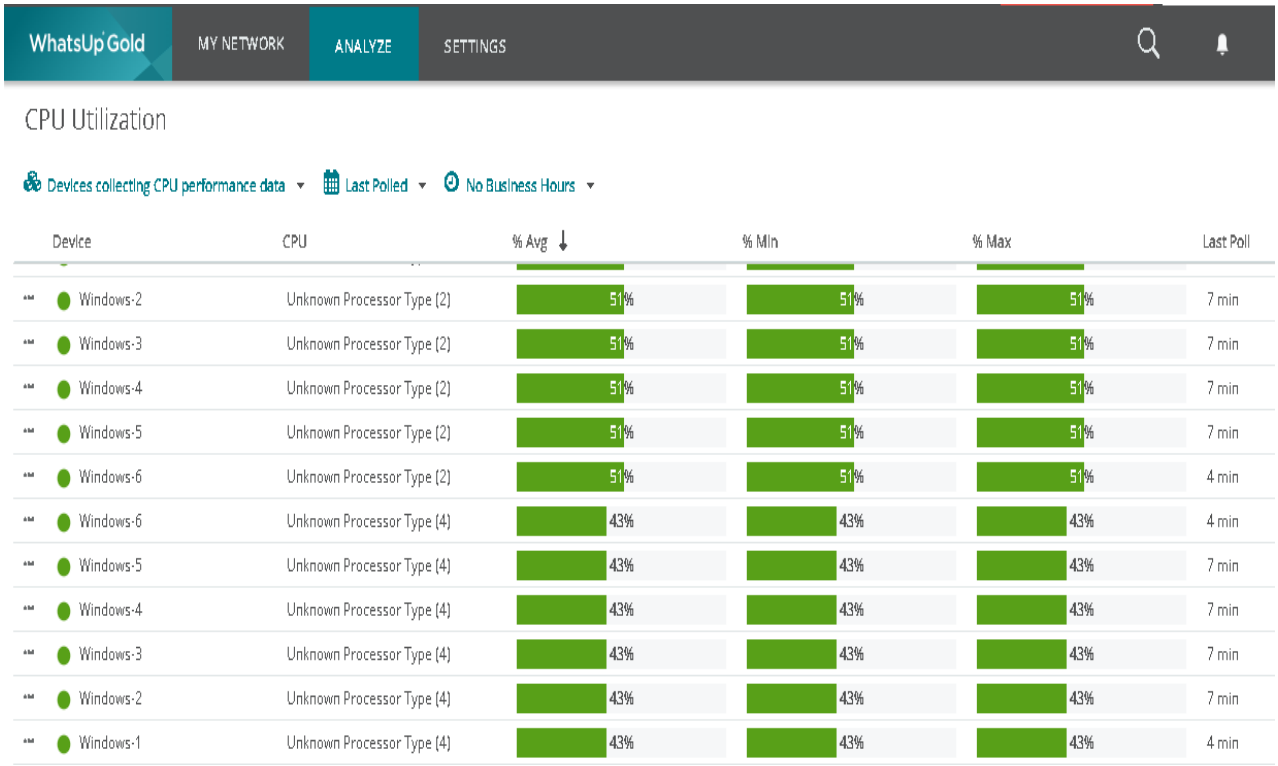
Figura 24: Gráfico da CPU WhtasUp Gold



Fonte: Própria do Autor

A ferramenta proporciona gerar o gráfico de carga de CPU onde cada consumo gerado por cada ativo da rede é informado por uma cor no gráfico, podemos visualizar que o consumo não foi excessivo, e não passou de 60%, podemos ver também de acordo com os dias na parte inferior do gráfico que o consumo manteve-se constante. No painel a seguir as informações de consumo são mais detalhadas. Mostrando o tempo de coleta, o máximo e mínimo de consumo de cada ativo da rede.

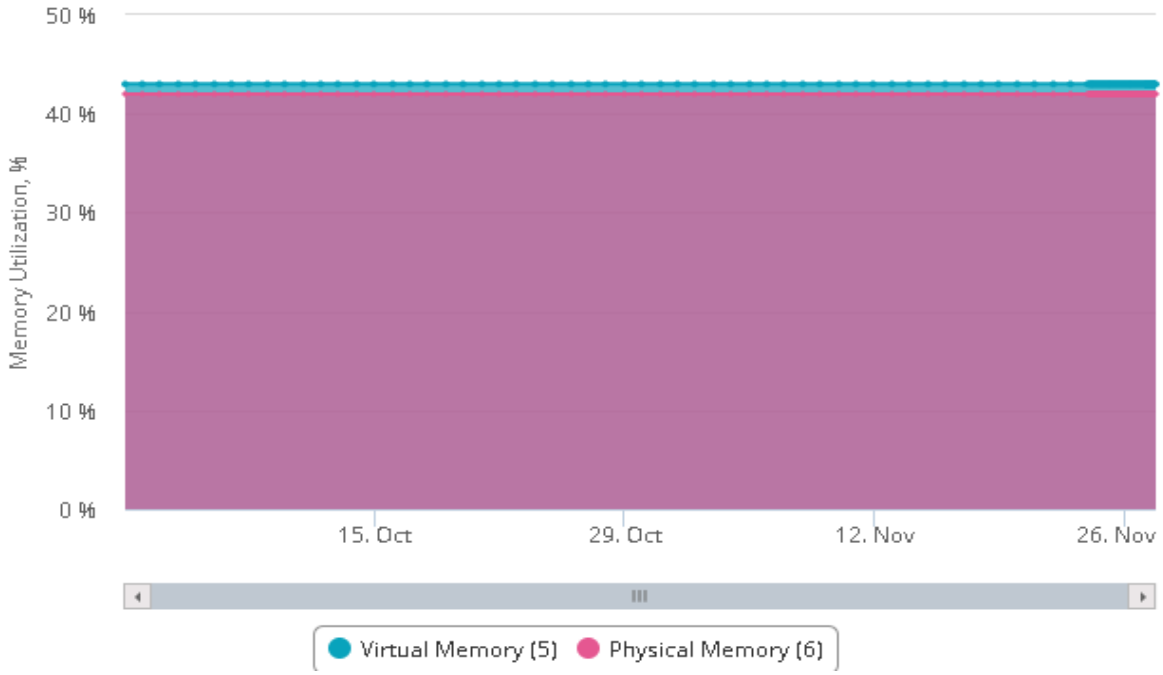
Figura 25: Painel de utilização da CPU



Fonte: Própria do Autor

5.2.3.2 Gráfico do Consumo de Memória

Figura 26: Consumo da Memória



Fonte: Própria do autor

Os consumos de memória podem perceber que no geral foi aceitável pelo fato da rede não ser tão robusta e complexa, o software distingue a parte lilás como a memória física que realmente foi consumida pela rede, e a parte azul foram à quantidade de memória virtual utilizada.

5.3 Análise e Comparação dos resultados das ferramentas Netflow Analyzer e PRTG

As figuras 5 e 6 ilustram como as ferramentas detectaram que o ativo Interruptor 16 realizou maior consumo a rede, ao realizar uma análise minuciosa no dispositivo foi possível detectar que o mesmo, realizou vários acessos a sites de jogos, filmes, realizou downloads, então foi possível coletar essas informações.

As duas ferramentas foram bem objetivas em detectar qual dispositivo da rede consumia mais banda, mas a ferramenta PRTG foi mais prática, apresenta um pacote de sensores que facilitam o trabalho de um administrador de redes, foi então que a ferramenta PRTG se destacou, foi utilizados sensores de consumo de banda, latência, de carga e uso de alertas, foi então que a ferramenta foi bem ágil em descobrir que o interruptor 16 seria o ativo que mais realizava solicitações de download.

O Netflow Analyzer permite descobrir todos os dados a respeito da CPU, Armazenamento de memoria e Perda e pacotes, mas se for para uma analise de outras métricas de medição da rede, a ferramenta deixa a desejar, em relação a ferramenta PRTG que na versão DEMO utilizada neste trabalho, onde o desenvolvedor oferece 100 sensores de testes nessa versão gratuita, enquanto que se optar pela versão paga, ela disponibiliza mais de cinco mil sensores. A cada sensor adicionado a rede, é possível realizar análises de gráficos de consumo de acordo com cada sensor instalado.

5.4 Resultados com a ferramenta Sparrow IQ

Para o cenário de testes com o software Sparrow IQ foi usado o mesmo cenário de testes da ferramenta PRTG, foi instalado o host Sparrow IQ, servidor Server PT 1 ilustrado na topologia do cenário de redes do PRTG, então através das funcionalidades que o software dispões pode ser realizado a coleta e analise dos dados, o tráfego interceptado dos 7 ativos da redes são salvos em uma base de dados, inicialmente foi criado um grupo na funcionalidade *Groups* , e então 8 minutos foram interceptados os dados passados pela rede e o consumo que cada dispositivo nessa fatia de tempo.

Essa ferramenta não precisa de Switches ou roteadores com capacidade de fluxo e independe do tamanho da rede, a conexão do Sparrow na rede só pode ser feita usando dois métodos, Um modo seria utilizar a porta SPAN (Uma porta SPAN se conecta a um dispositivo de monitoramento e recebe uma cópia de todo o tráfego percorrendo um ou muitos dos outros switches que foram marcados para análise. Switches de Rede), a maioria dos dispositivos modernos suporta esse recurso ou usando um Network Tap para fornecer o acesso ao tráfego.

Podemos perceber que esse software assim como os outros estudados neste trabalho, permite coletar as informações de consumo, CPU, Memória e os Registros de Tráfego Máximo e Mínimo de cada ativo na rede, porém por questões de limitação de licenças não pode ser gerado os gráficos de consumo da rede, a licença disponibilizada não oferece esse recurso para usuários simples, mas para empresas que queiram implantar o sistema de gerenciamento completo.

A licença usada no trabalho nos permitiu fazer previsões sobre o tamanho da rede em questão, a plataforma web então disponibilizou acessar os dados em um painel de visualização de estatísticas. Pelo tamanho da rede poremos ver que os consumos não tiveram uma variação fora do normal em relação as outras coletas das ferramentas também estudadas.

Tabela 4: Dados coletados pela ferramenta Sparrow IQ

Ativo	Tráfego de entrada Máximo KB/s	Tráfego de Saída Mínimo KB/s	Uso da CPU	Uso da Memória
Computador 1	91,1	47,1	17,20%	20,20%
Computador 2	60,2	13,2	15,10%	19,10%
Computador 3	47,1	18,4	13,40%	22,40%
Computador 4	50,9	24,3	15,10%	18,10%
Computador 5	32,8	17,5	15,20%	17,20%
Computador 6	97,6	49,8	19,10%	23,10%
Computador 7	45,7	23,9	14,20%	14,40%

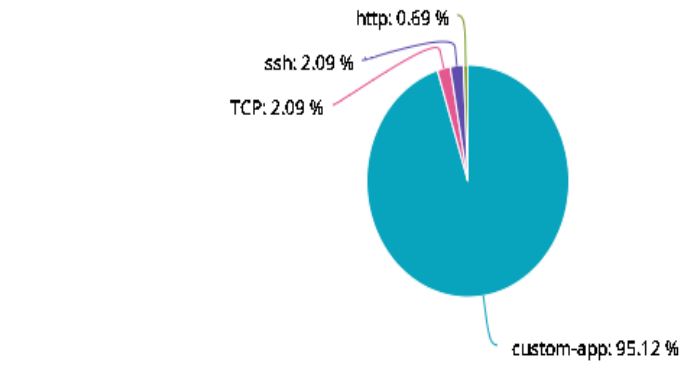
Fonte: Própria do autor

5.5 Dados Coletados e Resultado com a ferramenta Wireshark

Conforme a ilustração do ambiente de redes da figura xxx, a rede possui um Hub Switch que é um ativo que tem por função interligar todas as estações de serviço da rede em questão. Uma das características principais do Hub é receber os dados enviados de um computador e transmitir às outras máquinas. Para que seja feita a interceptação dos pacotes enviados e recebidos pelos ativos que estão sendo monitorados, o wireshark poderia ser instalado em qualquer dispositivo da rede, então foi optado por instalar o wireshark no servidor Server PT 1 pois assim a captura dos pacotes é realizada na própria interface do servidor.

A ferramenta então coletou uma vasta quantidade de informações, todo fluxo de entrada e saída que estava sendo enviado e recebido de pacotes por cada maquina, o principal intuito do teste foi identificar o dispositivo que teve mais alto valor de tráfego, ou as maquinas que tiveram maior nível de tráfego.

Figura 27: Tipos de Aplicações que mais consumiram



Application	Bytes	Bit Rate	Byte Percentage
custom-app	146.25 MB	681.57 Kbps	95.1%
TCP Unclassified	3.22 MB	15.00 Kbps	2.1%
ssh	3.22 MB	15.00 Kbps	2.1%
http	1.07 MB	4.98 Kbps	0.7%

Fonte: Própria do autor

5.6 Análise e Comparação dos resultados das ferramentas Wireshark e Sparrow IQ

As ferramentas Wireshark e Sparrow, são softwares de gerenciamento e monitoramento que apresentam infinitas funcionalidades para qualquer administrador ou empresa utilizar, porém ambas apresentam suas particularidades, enquanto o Wireshark coletas todos os dados e pacotes que trafegam na rede e disponibiliza os mesmos para análise do trafego e organiza-os em protocolos, seus filtros monitoram toda entrada e saída de dados, no teste a ferramenta pode coletar as aplicações que mais consumiram e então foi feito o gráfico das mesmas.

A ferramenta teve bom desempenho, porém não acompanha as outras aqui também estudadas, não possui sensores, nem disponibiliza criar mapas de redes, ou visualizar estatísticas mais avançadas da rede.

A ferramenta Sparrow IQ foi um pouco melhor que o Wireshark por ter mais recursos, ela gera gráficos estatísticos de consumo e registros de dados coletados, infelizmente por

questão de licença não pode ser adicionado os gráficos de consumos, portanto a mesma se sobrepôs em relação o Wireshark.

5.7 Quadro Comparativo entre as Ferramentas de Gerenciamento e Monitoramento

Tabela 4: Comparativo entra as Ferramentas de Gerenciamento e Monitoramento

Ação	PRTG	Wireshark	WhatsapUP	Netflow Analyzer	Sparrow IQ
Monitoramento do tráfego da rede	Permite	Permite	Permite	Permite	Permite
Monitoramento de outras informações de dispositivos	Permite(Além de scripts e consultas SNMP	não Permite	Permite	Permite	Não Permite
incorporação de templates	Permite(Importação)	Permite(Inserção de scripts)	Permite(Importação simples)	Permite(Consulta)	Não Permite
Busca Automática por dispositivos com SNMP	Permite(Uso de Sensores)	não Permite	Permite	Permite	Não Permite
Alertas de Situações definidas	Permite(Atraves de Notificações e Sensores definidos)	Permite(Por meio de Comandos)	Permite(Alertas e Sensores)	Permite(Alertas)	Permite(Por meio de Comandos)
Interface	Interface visual, com menus e Funções	Interface Visual	Interface Visual	Interface Visual	Interface Visual
Alocação e Agrupamento de Dispositivos para visualização	Sistemas de arvores, com possibilidade de Agrupamento	não Permite	Permite	Permite	Permite(Paginas Html individuais)
Monitoramento em tempo real da situação do dispostivo	Permite(Uso de Sensores)	não Permite	Permite(Uso de Sensores)	Permite(Padrão)	Permite(Plugins)
Alteração de informações sobre os gráficos	Permite	não Permite	Permite	Permite	Permite(Licença Paga)

Fonte: Própria do Autor.

A partir dos testes realizados e dados coletados com as ferramentas presentes nesse trabalho pode-se concluir que todas as ferramentas são eficientes, possuem muitas funcionalidades, porém duas tiveram destaque especial, o software PRTG e WhatsUp Gold, pois são ferramentas que evoluíram de acordo com o crescimento e complexidade das redes de computadores, ambas trabalham o conceito de sensores, mapas de rede, disponibilidade e integração com outras plataformas, sendo bastantes utilizadas por grandes empresas, nacionais e internacionais.

Apesar de terem resultados parecidos nas coletas obtidas, as duas mereceram ser destacadas como mais adequadas para pequenas, mediar e grandes redes.

6 CONSIDERAÇÕES FINAIS

Devido ao grande crescimento da complexidade das redes, e aumento da utilização da internet, se faz necessário o uso de equipamentos cada vez mais sofisticados e que suportem a demanda por conexão, para manutenção e funcionamento eficiente da rede e seus ativos.

Deste modo surge a necessidade de tornar o gerenciamento e monitoramento ainda mais efetivos dentro das organizações, independente do tamanho, tornando a realização de tarefas menos exaustivas e mais eficientes, usando ferramentas que apoiem todas as tarefas, assim como simplificando e alertando as eventualidades que possam sair da normalidade.

Este trabalho teve como objetivo realizar um estudo sobre cinco ferramentas de monitoramento e gerenciamento existentes no mercado, sendo elas PRTG, Netflow Analyzer, WhatsUp Gold, Wireshark. Foram realizados testes, assim como comparação das funcionalidades, cada ferramenta foi testada em cenários semelhantes a fim de coletar resultados e analisar as funcionalidades de cada uma, além de destacar qual ferramenta apresentou melhor desempenho.

Com base nos testes feitos em cada ferramenta pode-se perceber que existem muitas semelhanças de funcionalidades entre elas, porem o Wireshark por ser um software que possui muitos recursos, limitou-se pelo fato de não ter a gama de artifícios que as outras ferramentas possuírem, é uma ferramenta que não conseguiu desenvolver-se como as outras ferramentas em estudo.

Tanto o PRTG quanto o WhatsUP Gold apresentam uma constante evolução, isto deve-se ao sucesso que as ferramentas fazem com os usuários e organizações. Ambas se mostram bastante completas quanto as suas funcionalidades, aparentemente são ferramentas com uma usabilidade bem acessível, e muitos recursos disponíveis. Com bases nos testes e funcionalidades as duas ferramentas foram determinadas como solução mais adequada para o cenário apresentado em relação as cinco também utilizadas.

A ferramenta PRTG teve bom desempenho em relação às outras quando analisamos que o consumo de CPU não ultrapassou os 15% de uso, em relação às demais ferramentas, e o baixo uso de memória não ultrapassando os 20% de uso, foram essências para o sucesso da ferramenta.

A capacidade de interação entre os softwares e administrador da rede deve ser bem avaliada, pois é necessário que a rede esteja disponível o maior tempo possível, neste sentido

é importante ressaltar as tecnologias que podem ser utilizadas para gerar alerta, como uso de sensores, presentes em ambas as ferramentas.

A ferramenta Netflow Analyzer apresenta muitos recursos, porém em relação às outras citadas anteriormente, apresenta um número limitado de recursos, não possui tecnologia de sensores, mas possui a funcionalidade de simular uma rede completa em sua plataforma na nuvem.

Para prover um serviço com máximo de eficiência e desempenho é fundamental que a ferramenta possa suprir o máximo de recursos e artifícios possíveis, o administrador precisa que essas ferramentas garantam a qualidade máxima dos serviços, assim como um acesso eficaz e com responsabilidade, este trabalho destaca os recursos que cada software estudado dispõe, mas o objetivo foi encontrar o mais adequado, através de analises e critérios.

Uma das dificuldades encontradas no trabalho foi de ter que simular cada dispositivo que compôs a rede, e de cada particularidade das ferramentas usadas nos testes, todas testadas foram validadas na versão demo, sendo que a ferramenta Sparrow IQ por questões de licenças não liberou o software por completo na versão demo, pois eles priorizam os testes do software para empresas.

Este estudo contribuiu para o desenvolvimento pessoal do autor do trabalho, ampliando os conhecimentos através das pesquisas realizadas e implementadas neste trabalho, possibilitando a aplicação de diversos conteúdos aprendidos ao longo do curso, este trabalho ainda poderá servir de apoio a todos que necessitem fazer estudos sobre as ferramentas analisadas, além de auxilia-los em uma possível implantação de algum software que aqui foi testado.

6.1Trabalhos Futuros

Destacam-se a seguir, os trabalhos futuros a serem executados, aproveitando os estudos obtidos neste trabalho. Realizar a análise de outros fatores das ferramentas também aplicar e utilizar outras métricas para medição do desempenho. Incluir outros dispositivos da rede que não foram monitorados.

Realizar Implementação de uma ferramenta de gerência de redes, justifica-se pelo fato de poder analisar outros fatores o gerenciamento de redes e realizar estudo comparativo com as ferramentas de software Livre.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, F. R.; PIRES H. D. **Gerência de redes**. Universidade Federal Fluminense. Disponível em: < http://www.midiacom.uff.br/~debora/redes1/pdf/trab042/SNMP.pdf> Acesso em: 02 Ago. 2018

ATISANO, José**. Monitoramento de redes com CACTI e PHP Network**. Curitiba 2011.

Disponível em: https://acervodigital.ufpr.br/bitstream/handle/1884/43298/R%20-%20E%20-%20REGINALDO%20JOSE%20ATISANO.pdf?sequence=1&isAllowed=y Acessado em: 09 set 2018.

BARRIVIERA, Rodolfo Msc. **Gerência de Redes de Computadores: Protocolo CMIP**, 2010, Instituto Federal do Paraná – Campus Londrina. Disponível em: . Acesso em: 15 ago. 2016.

BUFFONI, Humberto (2013) **"Uma proposta de Gerência para redes de Computadores"**. Disponível em: https://pantheon.ufrj.br/bitstream/11422/3302/4/HBuffoni.pdf. Acessado em: 19 set 2018

BLACK, Lovis Tomas (2008) "**Comparação de ferramentas de gerenciamento de Rede"**.

Rio de Janeiro: UFRGS Dezembro, Disponível em: http://www.ulbra.inf.br/joomla/images/documentos/TCCs/2011_02/PROJETO_RC_KANAN_ALI_ABDULLA_MOQADI.pdf

BRAGA, J. O. **Estudo sobre o protocolo SNMP e comparativo entre ferramentas**. 2012. 31 fev. Trabalho de Conclusão de Curso (Especialização) - Faculdade de Ciências Exatas e Tecnológica, Universidade Tuiuti do Paraná, Curitiba, 2012.

COSTA, F. (2008) **Ambiente de redes monitorados com Nagios e Cacti.** Rio de Janeiro: Editora Ciência Moderna Ltda.

DIAS, H. L. **A importância do monitoramento de ativos de redes**: **um estudo de caso com o sistema CACIC.** 2008. 67 f. Trabalho de Conclusão de Curso (Bacharelado) - Escola Politécnica, Universidade de Pernambuco, Pernambuco, 2008. Disponível em: <http://tcc.ecomp.poli.br/20082/TCC_Henrique_Dias_2008-2.pdf>.

MENDES, Luís (**2010) "Análise e caracterização de tráfego em redes muni-wi" Disponível em:** http://www.decom.ufop.br/menotti/monoII102/files/BCC391-102-mn-04.1.407LuisAlbertoMoreira.pdf Acessado em 26 de setembro de 2018.

MELODY, Rodrigues **Computação em nuvem: estudo de viabilidade** disponível em: http://repositorio.roca.utfpr.edu.br/jspui/bitstream/1/663/1/CT_TELEINFO_XIX_2011_15.pdf acessado em: 12 out 2018.

MAJEWSKI, R. **Sistemas de monitoração de rede**. Curitiba: Pontifícia Universidade Católica do Paraná, Nov. 2009.

OLIVEIRA, D. T. **Gerência de redes de computadores**: **uma abordagem com o uso do SNMP.** 2002. 85 f. Trabalho de Conclusão de Curso (Bacharelado) - Ciência da Computação,Centro Universitário do Triângulo (Unitri), Uberlândia, 2008. Disponível em: <http://www.computacao.unitri.edu.br/downloads/monografia/28211129405651.pdf>.

POLETO, Olavo F. **Gerenciamento e Monitoramento de Redes II: Análise de Desempenho**, Jan. 2012. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialgmredes2/pagina_2.asp>. Acesso em: 14 out. 2018.

PRTG. Disponível em: <http://www.paessler.com/prtg>. Acesso em: 13.out.2018

ROSA, D. M Da. Suporte a Cooperação em Sistemas de Gerenciamento de rede utilizando Tecnologias Peer-to-peer. 2007. 73 f. Dissertação(Mestrado em Ciência da Computação)-Instituto de Informática, UFRGS, Porto Alegre.

SILVA, João (2016) **"Monitoramento da rede Unirio Tec. através da ferramenta Centreon".** Disponível em**:** http://bsi.uniriotec.br/tcc/textos/201612Calil.pdf. Acessado em: 12 out 2018.

TANENBAUM, Andrew S**. Redes de computadores. 4ª Ed**., Rio de Janeiro: Editora Campus, 2003.

KUROSE, J. F.; ROSS, K. W, **Redes de computadores e a internet: uma abordagem Top-Down**. 5. ed. São Paulo: Pearson, 2010.

KUROSE, J. ROSS, W. K. **Redes de Computadores e a Internet – Uma Abordagem Top Down** 3ª Edição. Pearson. 2005.