ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP QMB CÉLIO PIRES DE OLIVEIRA JÚNIOR

MONITORAÇÃO DE SISTEMAS: USO DE FERRAMENTAS GRATUITAS PARA GERENCIAR UMA REDE DE COMPUTADORES

Rio de Janeiro
2018

ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS

CAP QMB CÉLIO PIRES DE OLIVEIRA JÚNIOR

MONITORAÇÃO DE SISTEMAS: USO DE FERRAMENTAS GRATUITAS PARA GERENCIAR UMA REDE DE COMPUTADORES

Trabalho acadêmico apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito para a especialização em Ciências Militares com ênfase em Gestão Logística

Rio de Janeiro
2018

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
DECEx - DESMil
ESCOLA DE APERFEIÇOAMENTO DE OFICIAIS
(EsAO/1919)

DIVISÃO DE ENSINO / SEÇÃO DE PÓS-GRADUAÇÃO

FOLHA DE APROVAÇÃO

Autor: **Cap QMB CÉLIO PIRES DE OLIVEIRA JÚNIOR**

Título:

MONITORAÇÃO DE SISTEMAS: USO DE FERRAMENTAS GRATUITAS PARA GERENCIAR UMA REDE DE COMPUTADORES

Trabalho Acadêmico, apresentado à Escola de Aperfeiçoamento de Oficiais, como requisito parcial para a obtenção da especialização em Ciências Militares, com ênfase em Gestão Logística, pós-graduação universitária lato sensu.

APROVADO EM _____/_____/_____ *CONCEITO:* _____

BANCA EXAMINADORA

Membro **Menção Atribuída**

_____
DOUGLAS FRANCISCO RAICOSKI JUNIOR – Ten Cel
Cmt Curso e Presidente da Comissão

_____
JOELSON SUZENA ROSA - Maj
1º Membro e Orientador

_____
ÁTILA ALVES DE SOUZA - Maj
2º Membro

_____
CÉLIO PIRES DE OLIVEIRA JÚNIOR – Cap
Aluno

MONITORAÇÃO DE SISTEMAS:

USO DE FERRAMENTAS GRATUITAS PARA GERENCIAR UMA REDE DE COMPUTADORES

Célio Pires de Oliveira Júnior*

Joelson Suzena Rosa**

Resumo

As organizações necessitam de informação para o desenvolvimento de suas atividades. Na atualidade a informação está disponível para acesso em diversos meios e em diversas partes do mundo. Isso é possível devido o advento e evolução das redes de computadores em conjunto com a evolução tecnológica dos equipamentos que permitem a troca do conhecimento instantaneamente. Esses equipamentos de Tecnologia e Informação e Comunicação (TIC) possuem sistemas, softwares dos mais diversos, que são parte essencial para que o fluxo da informação, pela rede mundial de computadores, ocorra. Para manter os sistemas funcionando, as empresas possuem equipes de TI que utilizam diversas técnicas e ferramentas para monitorar e mapear tudo o que acontece em sua rede. A meta, com o emprego dos softwares de monitoramento, é agir antes que o problema ocorra.

Palavras-chave: Informação, TIC, Tecnologia da Informação, monitoramento, redes de computadores

ABSTRACT

Organizations need information for the development of their activities. At present, the information is available for access in various media and in different parts of the world. This is possible due to the advent and evolution of computer networks in conjunction with the technological evolution of the equipment that allow the exchange of knowledge instantly. These Technology and Information and Communication (ICT) equipment have

systems, most diverse software, which are an essential part for the flow of information, through the worldwide computer network, to occur. To keep systems running, companies have IT teams that use a variety of techniques and tools to monitor and map everything that happens on their network. The goal, with the use of monitoring software, is to act before the problem occurs.

Keywords: Information, ICT, Information Technology, monitoring, computer networks

*Capitão do Quadro de Material Bélico. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2008.

**Capitão do Quadro de Material Bélico. Bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN) em 2004.

1. INTRODUÇÃO

A informação é um recurso intangível. Na atualidade a informação é, cada vez mais, primordial para execução de uma série de tarefas. Seja ela fonte para tomada de decisão ou aquela que uma empresa possui para conduzir suas ações e negócios. Para que uma organização possa usufruir de toda o conhecimento disponível faz-se necessário que a informação esteja disponível, seja confiável e principalmente esteja armazenada em segurança.

> Um dos grandes desafios das organizações no mundo globalizado atual é usar a informação como recurso para competir e manter a vantagem competitiva. Para Beuren (2000) informação é um recurso vital nas organizações, quando devidamente estruturada, integra as funções das várias unidades por meio de diversos sistemas organizacionais, onde o desafio maior da informação é habilitar os gestores a alcançar os objetivos propostos para a organização, por meio do uso eficiente dos recursos disponíveis (Nhasengo e Razzolini, IX Convibra Administração – Congresso Virtual Brasileiro de Administração, 2012)

Com a demanda gerada pelas organizações faz-se necessária a utilização de sistemas informatizados para gerir toda a informação de uma empresa. Tais sistemas visam melhorar processos, agilizar o tramite do conhecimento, evitar falhas humanas e etc. Dessa forma, as organizações, ao aumentarem sua capacidade de gerir e produzir conhecimento, tem um incremento de produtividade. Conseguem realizar com maior eficácia e eficiência suas tarefas diárias.

> A procura de informações por parte das organizações enquadra-se numa perspectiva em que a informação deve estar disponível para os membros da organização, e necessária com melhor precisão não se desligando da qualidade que a informação deve conter para os sistemas de informação. Para reforçar este aspecto, quando as informações estão organizadas e planejadas nos sistemas de informação estas geram informações eficientes e eficazes para a gestão da organização (IX Convibra Administração – Congresso Virtual Brasileiro de Administração, 2012)

Segundo Nhasengo e Razzolini (2012), a tecnologia da informação (TI) é um conjunto de ferramentas indispensáveis neste processo e Foina (2001) a define como conjunto de métodos e ferramentas, mecanizadas ou não, que se propõe a garantir a qualidade e pontualidade das informações dentro da organização. Este

ferramental, funciona como suporte para a tomada de decisão por meio do uso dos sistemas de informação que são recursos fundamentais para o sucesso de uma organização.

Segundo Caiado (2018), no mundo moderno, a Tecnologia da Informação e Comunicação (TIC) está cada vez mais presente na rotina das empresas e da maioria da população urbana. Acerca do vertiginoso aumento da importância das TIC, Porter e Millar (1985) definem a sua relevância na cadeia de valor e apontam que elas geram novos negócios inteiros, muitas vezes de dentro das operações existentes na própria empresa, além de criar vantagens competitivas e mudar a estrutura da indústria, alterando as regras de competição. Tais características foram em grande parte as responsáveis pela propagação das novas tecnologias.

Com essa utilização da informação, cada vez mais dinâmica, por diversos meios eletrônicos, surge também a necessidade de prevenir e mitigar riscos para a organização. Segundo Caiado (2018), a disseminação de uso das TIC, os recursos eletrônicos não estão sendo apenas empregados pelas empresas, mas também sendo mais utilizados na prática de diversos crimes. Com essa disseminação e a falta de regulamentação da rede mundial de computadores, as empresas e organizações se veem inseridas em um ambiente selvagem, ambiente este que é o meio de tramitação da informação entre as partes. Para mitigar os riscos, na atualidade há um aumento no investimento em sistemas que permitam o correto e seguro tramite de dados. As empresas estão se valendo de setores/divisões de TI cada vez mais robustas e qualificadas que empregam ferramentas para garantir o funcionamento adequado dos processos.

O que se vê é um mundo onde a informação trafega por milhares de equipamentos com acesso em vários locais do globo terrestre. Nesse ambiente, por vezes caótico e com regulação ineficaz, existem agentes mal-intencionados que lucram ou se valem de falhas em sistemas computacionais, redes de computadores e outros ativos conectados, para aferir vantagens.

Sendo assim é primordial para uma empresa que sua equipe mantenha todos os sistemas funcionando corretamente, 24 horas por dia, 7 dias por semana. Com um sistema que consiga manter a informação confiável, segura e disponível. Como é humanamente impossível uma equipe ficar o tempo todo olhando cada dispositivo e ou ativo de sua rede. Faz-se necessário a automatização de sistemas de

monitoramento para os diversos processos desenvolvidos nos sistemas de TIC da empresa.

Levando em consideração ainda que o custo de operação de diversos sistemas é um fator que limita, ou pode impactar, o negócio de uma empresa, a equipe de TI deve buscar a utilização de ferramentas que se adequem ao modelo de negócio da empresa com o custo adequado.

1.1 PROBLEMA

As empresas e organizações estão, cada vez mais dependentes dos sistemas de Tecnologia Informação e Comunicações (TIC). O Exército Brasileiro, como organização também faz uso de sistemas para automatizar, gerenciar, acompanhar e melhorar seus processos e informações. Nas Organizações militares do EB, a seção de Informática é a responsável por gerir os recursos de TIC local. Para tanto o dia-a-dia de uma Seção de Informática, exige do gerente de TI, no caso do EB, do **Oficial de Informática** e sua equipe, qualificação e emprego de ferramentas de monitoramento para que este possa identificar e sanar, no menor tempo possível, a pane apresentada, para proporcionar os serviços de maneira correta ao usuário/ operador dos sistemas de informação. O uso dessas ferramentas permite que a Seção de Informática trabalhe de maneira proativa, evitando interrupção dos serviços.

> Art. 45. O oficial de informática é o encarregado das redes de informáticas da unidade é o responsável pela eficiência e continuidade de seu funcionamento.
> Art.46. Ao O Infor incumbe:
> I - controlar os recursos de informática existentes na OM, de acordo com a legislação específica;
> II - zelar pelo cumprimento da legislação em vigor;
> III - organizar e manter atualizada a pasta de licenças de **software**, com os programas em uso na unidade, e em estreita ligação com a Fisc Adm;
> IV - estimular o uso de **software** livre, consoante as orientações do Governo Federal e da Secretaria de Tecnologia da Informação;
> V - propor, difundir e implantar normas de segurança da informação na sua OM, conforme orientações do Cmt U e da Secretaria de Tecnologia da Informação;
> VI - integrar, tanto quanto possível, as atividades de informática e

> comunicações, no preparo e emprego operacional da unidade, em estreita ligação com o O Com Elt;
> VII - na OM em que existir rede local de computadores e/ou computadores com acesso à **Internet**, orientar as atividades ligadas à gerência de redes, principalmente nos aspectos de segurança da informação; e
> VIII - manter atualizados os sítios da **Internet** de responsabilidade de sua OM.
> (BRASIL.EXERCITO. **Regulamento Interno e dos Serviços Gerais – R1(RISG).** SECRETARIA GERAL DO EXERCITO:2013.)

Além do uso de sistemas consagrados e/ou padronizados, o Oficial de Informática, deve buscar sempre melhorar a qualidade do serviço fornecido aos integrantes de sua OM, para isso pode valer de diversos sistemas e outros procedimentos. Tais sistemas podem ser de software livre que diminuem os custos e permitem o uso sem solução de continuidade, se comparado por exemplo a implementações adquiridas por processos licitatórios que, geralmente, dependem de renovação contratual periódica e recursos disponíveis para tal.

Existem diversas ferramentas disponíveis para se monitorar os recursos de TIC. A combinação delas ou sistematização do seu uso é primordial, além da escolha da ferramenta que mais se adequa àquela OM. Vale ressaltar que seu emprego deve ser dimensionado de acordo com a demanda, não é útil que o sistema de monitoramento seja mais oneroso que o serviço fornecido. Como dito anteriormente, o objetivo deve ser sempre fornecer a informação confiável em tempo oportuno.

Depois da escolha e configuração da(s) ferramenta(s), para acompanhar a disponibilidade dos sistemas, processos simples de verificação de alertas são implementados para que a equipe possa agir. Esses alertas podem ser por e-mail, SMS, telefone e outros. Esse fato aumenta a agilidade na resolução do problema. Tudo isso visa facilitar o trabalho e permite que a equipe tenha tempo para implementar outras soluções ou resolver outros problemas.

As seções de informática costumam agir de maneira reativa. Trabalham o problema apresentado de maneira corretiva, ou seja, reagem a um evento que compromete o fornecimento do serviço para os usuários. Diversas hipóteses são testadas para saber onde está o problema. Esse processo demanda tempo e exige muito da equipe.

Ferramentas modernas fornecem, além da simples monitoração de sistemas, levantamento de estatísticas de eventos e “sugestões”, passo a passo, para a resolução de incidentes. Com essas informações, contando também com a expertise da equipe, é possível que as seções se tornem mais proativas e parem de reagir ao problema.

> A meta de qualquer organização de TI é garantir que tudo, da infraestrutura subjacente aos aplicativos, esteja funcionando de maneira que os usuários finais possam concluir suas tarefas de forma eficiente. Para ajudá-los, as organizações de TI sempre dependeram de ferramentas de monitoramento de sistemas para alertar sobre problemas ocorridos em seu ambiente, mas as tendências do monitoramento de sistemas apontam para uma evolução rumo à análise, à automação e à correção. Por sua vez, essa evolução permitiu que as organizações de TI passassem de reativas a proativas, evitando assim situações de "combate a incêndios", que tendem a ser muito comuns.(Paap, Chris 2016)

Nesse cenário quais seriam as características ideais de uma ferramenta, de software livre, e quais seriam as vantagens e desvantagens de um possível emprego dessa ferramenta de monitoração gratuita, em conjunto com outras aplicações, para a implementação dos processos, e consequente melhoria dos serviços fornecidos, por uma equipe de gestão de equipamentos de Tecnologia Comunicação e Informação (TIC)?

1.2 OBJETIVOS

OBJETIVO GERAL

- Analisar ferramentas de monitoração de redes gratuitas para o emprego por uma Seção de Informática de uma Organização Militar para melhorar o fornecimento dos serviços de TIC e garantir que a informação seja confiável e esteja sempre disponível.

OBJETIVOS ESPECÍFICOS

- Testar ferramentas de monitoração capazes de gerar alertas e soluções para as panes;

- Pesquisar e apresentar as ferramentas mais comuns usadas pelos gerentes de TI em suas organizações;

- Destacar as vantagens do emprego de determinadas ferramentas em detrimento de outras, possibilitando assim uma comparação qualitativa das ferramentas

- Apresentar o software NAGIOS.

- Apresentar uma experiência de emprego do software BRASILFW.

1.3JUSTIFICATIVAS

- A disponibilidade dos serviços de informática como um todo é um fator primordial em qualquer organização que empregue tecnologia na gerência de seus ativos. Assim uma OM tem que manter os serviços funcionando ininterruptamente para a correta e eficiente condução dos trabalhos.

- Com o uso de uma aplicação que atenda aos interesses da instituição a Seção de Informática poderá manter /ou melhorar a confiabilidade de seus serviços, podendo por exemplo, identificar qual o momento adequado para substituição de determinado componente.

- Devido a melhora do suporte fornecido pela Seção de informática, o trabalho poderá ser realizado com maior agilidade e segurança.

2. METODOLOGIA

Com o escopo de alcançar uma solução para a problemática apresentada, foi realizado uma pesquisa bibliográfica em livros, publicações técnicas, sites especializados, “fóruns’ de discussão e periódicos, após isso foram testadas algumas ferramentas para que se determine suas funcionalidades, principalmente, vantagens e desvantagens.

Para que se tenha uma noção do ambiente ao qual as informações estão expostas, foi realizada uma pesquisa para levantar principais riscos e problemas que podem ocorrer com uma organização, que se utiliza de sistemas informatizados como meio para conduzir suas atividades.

A pesquisa realizada foi basicamente documental, porém algumas ferramentas apresentadas, foram utilizadas pelo autor no período de 2015 a 2017 para gerenciar uma rede, com aproximadamente 80 dispositivos, desse 8 servidores, que forneciam todos os serviços que uma Organização Militar utiliza corriqueiramente mais os

serviços necessários a atividade de inteligência, este atinente apenas as Agencias de Inteligência. Com essa experiência o trabalho vai apresentar algumas vantagens e desvantagens do software livre BRASILFW observadas ao longo do período de utilização. Visando também apresentar outras soluções, foi realizada uma pesquisa em publicações técnicas para se apresentar algumas formas de utilização do software NAGIOS.

Quanto aos objetivos gerais podemos afirmar que a pesquisa é exploratória visando proporcionar maior familiaridade com o tema e utilizando o procedimento técnico da pesquisa documental.

2.1 REVISÃO DE LITERATURA

A cartilha de segurança do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (Cartilha de segurança, disponível em: https://cartilha.cert.br/redes/, acesso em 05 de novembro de 2017) ilustra bem a situação das redes de computadores atuais.

> Inicialmente, grande parte dos acessos à Internet eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um modem e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede.
>
> Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que atualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e a velocidades que podem chegar a até 100 Mbps1. Conexão à Internet também deixou de ser um recurso oferecido apenas a computadores, visto a grande quantidade de equipamentos com acesso à rede, como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio.

Diante de todo esse avanço dos recursos de TIC, faz-se necessário detalhar alguns conceitos básicos para que se entenda a real dimensão dessa evolução tecnológica**.** Trataremos de alguns conceitos gerais importantes para o desenvolvimento do trabalho em questão. Assim será possível o entendimento do sistema proposto e sua aplicação.

2.1.1 Rede de Computadores

As redes de computadores é a interligação de uma ou mais máquinas (computadores) para a troca de informações ou compartilhamento de recursos. Segundo TANENBAUM (2011), "..é um conjunto de computadores autônomos interconectados por uma única tecnologia".

Uma rede deve fornecer serviços a todos os usuários. Segundo TANENBAUM (2011),"...a questão aqui é o compartilhamento de recursos, e o objetivo é tornar todos os programas, equipamentos e especialmente dados ao alcance de todas as pessoas na rede, independentemente da localização física do recurso e do usuário.

A internet é uma rede de computadores que envolve diversos meio de comunicação, que por sua vez interligam diversas redes de computadores. Existem na bibliografia diversos conceitos para a classificação das redes de computadores. Neste trabalho utilizaremos a mais tradicional que é a classificação quanto a geografia e quanto à hierarquia.

2.1.1.1 Quanto à extensão geográfica

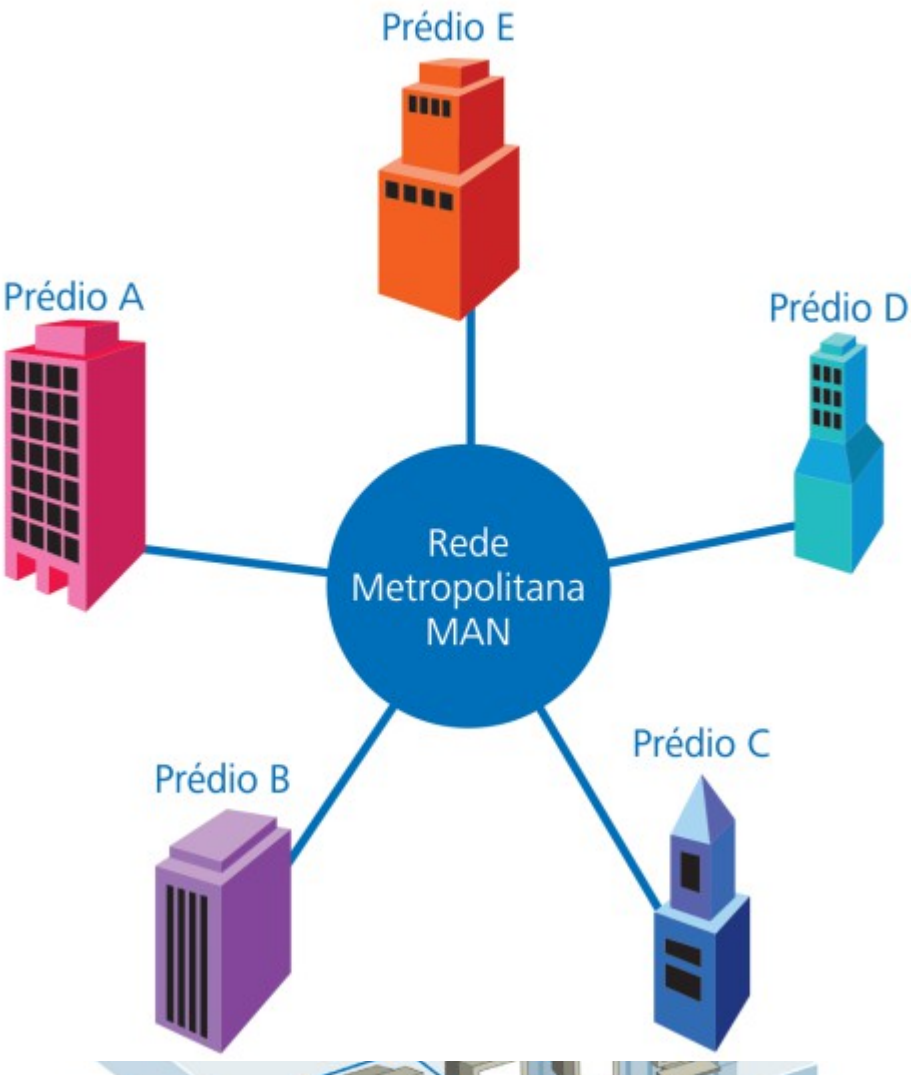
Neste aspecto as redes são classificadas de acordo com o alcance das mesmas. Alguns tipos são:

a) *LAN (Local Area Network):* é uma rede de computadores local, com alcance limitado, interligados entre-si por dispositivos que proporcionam também a comunicação com outros aparatos tecnológicos como impressoras, scanners entre outros.

Figura 1: *LAN*

b) *MAN (Metropolitan Area Network:* rede de área metropolitana é a rede que envolve diversas redes LANs, considerada de média dimensão. A figura a seguir ilustra esse tipo de rede.

Figura 2: *MAN*



Fonte: Rede de computadores. Universidade Federal de Santa Maria: 2014.

c) *WAN (Wide Area Network)* ou rede de longa distância: é uma rede de computadores que abrange grandes distancias, cidades, países e continentes, por exemplo. Engloba as redes *MANs*, que por sua vez engloba as redes *LAN*s.

Figura 3: *WAN*

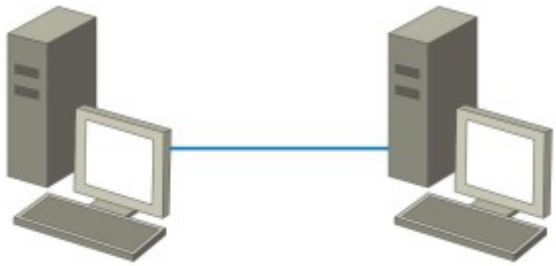
Fonte: Rede de computadores. Universidade Federal de Santa Maria: 2014.

2.1.1.1 Quanto à hierarquia

A classificação quanto a hierarquia se refere ao modo como as maquinas s comunicam dentro de uma determinada rede. Dentre os diversos tipos destacaremos dois:

a) Redes ponto-a-ponto: redes onde há a conexão direta entre as máquinas, nesse tipo de rede há o compartilhamento de arquivos e recursos.

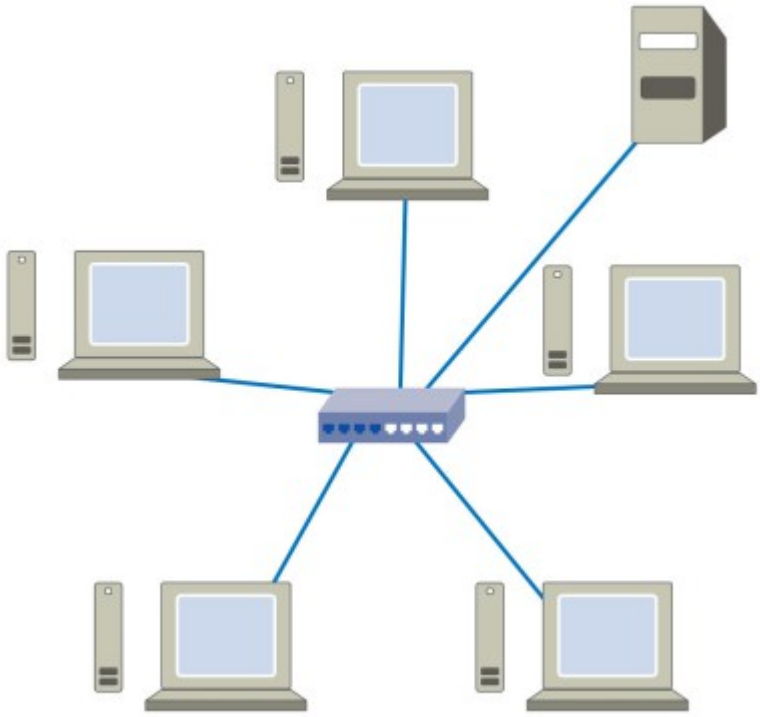
Figura 4: Redes ponto-aponto



Fonte: Rede de computadores. Universidade Federal de Santa Maria: 2014.

b) Redes cliente-servidor: São redes que possuem clientes (computadores) ligados a servidores, responsáveis por fornecer serviços e recursos aos clientes da rede.

Figura 5: Redes cliente-servidor



Fonte: Rede de computadores. Universidade Federal de Santa Maria: 2014.

2.1.2 Principais componentes, ativos e serviços de rede

Uma rede de computadores visa, além de interligar computadores, permitir o compartilhamento de serviços e recursos através de componentes com características especificas.

> Uma rede de computadores é formada por diversos dispositivos, equipamentos, entre outros, para que a mesma possa funcionar corretamente e cumprir o objetivo geral de uma rede: a troca de informações e o compartilhamento de recursos, sejam eles recursos de hardware ou software.

(Roberto Franciscatto, Fernando de Cristo, Tiago Perlin, 2014, P.22)

2.1.2.1 Servidores

O servidor é um hardware que desempenha diversas tarefas, e fornece diversos serviços. Os servidores também são responsáveis por executar serviços de maneira centralizada, facilitando assim a distribuição de serviços.

> Um servidor na rede pode conter funcionalidades de diferentes naturezas. Alguns tipos de servidores/serviços de rede são:
>
> • O servidor FTP: que é o servidor onde os usuários têm acesso a arquivos em rede;
>
> • O servidor web: é responsável por aceitar pedidos HTTP (*Hypertext Transfer Protocol*) de clientes, servindo com páginas web e arquivos de site;
>
> • O servidor DNS: que é responsável pela distribuição de nome de redes, convertendo nomes em IPs;
>
> • O servidor de arquivos: que é responsável por armazenar arquivos de clientes;
>
> • O servidor Webmail: que é responsável pelo envio/recebimento de contas eletrônicas e armazenamento de e-mails;
>
> • O servidor de Proxy: que é o responsável pelo armazenamento dos endereços de sites acessados, funcionando como um cache.
>
> (Renata Aparecida Benini e Marcelo Santos Daibert, Monitoramento de Redes de Computadores - Artigo Revista Infra Magazine 1. 2017)

Vale ressaltar que qualquer máquina pode ser utilizada como servidor. Porém deve ser ter em conta quando da implementação da quantidade de clientes, e por consequência a quantidade de requisições serão realizadas. Segundo (FRANCISCATTO; CRISTO; PERLIN, 2014, P.22) o servidor deve ser um computador preparado para exercer esta função, tanto no hardware com que é composto quanto ao software que é empregado no mesmo, ou seja, um servidor deve ter um hardware específico para suportar as atividades de servidor e deve também conter um sistema operacional que forneça à máquina capacidade de prover serviços específicos de servidores.

2.1.2.1 Dispositivos de rede

Diante dos conceitos já apresentados sobre as redes de computadores e os servidores, trataremos agora sobre alguns conceitos relativos aos dispositivos que permitem a interligação dos diversos ativos de uma rede, por serem diversos, trataremos daqueles mais comuns que merecem maior atenção para o correto funcionamento da mesma. São eles:

a) Clientes: são as estações de trabalho cliente que utilizarão ou processarão as informações. Como exemplo podemos citar computadores, notebooks, smartphones entre outros;
b) Interface de rede: são as placas de redes dos computadores clientes que permitem a conexão com a rede de computadores;
c) *Switch:* é o responsável por interligar um cliente com o destino. Serve como concentrador, recebe a informação e entrega ao destino,
d) Roteador: é um dispositivo que tem como característica selecionar a rota mais apropriada para transferir e receber protocolos na rede. É utilizado para fazer a comunicação entre diferentes redes de computadores provendo a comunicação entre computadores distantes entre si

2.1.3 Monitoramento de redes

Quando da utilização de uma rede de computadores muitos se esquecem, ou não tem a real noção, da quantidade de fluxo de informação. Em uma rede comum de uma empresa a quantidade de clientes, servidores e serviços disponíveis é gigantesca, o que no remete a pergunta como gerenciar tudo isso? Para responder parte dessa pergunta podemos nos valer das soluções de monitoramentos de sistema, mais especificamente, monitoramento de redes.

Assim monitorar a rede é tarefa fundamental para obter uma consciência situacional do real estado da rede. Com o monitoramento é possível planejar as ações manter todos os serviços funcionando aumentando a capacidade de trabalho de uma organização, sem solução de continuidade.

Em um ambiente de rede é necessário verificar a eficiência de cada componente da rede e serviços existentes. O normal de uma rede é o crescimento, ao longo do tempo, uma vez que a informação produzida é armazenada e novas soluções são implementadas. No dia a dia, situações de “lentidão da rede” são comuns – nesse ponto vale uma ressalva, por mais que se tenha um ambiente completamente estruturado, os serviços de banda contratados são limitadores, quanto mais clientes menor vai ser a banda disponível. A situação ideal é monitorar o fluxo de dados e monitorar os possíveis problemas antes que o usuário perceba o problema. A melhor maneira é monitorar tudo.

Para Ernando (2015) o administrador deve ir melhorando seu sistema para poder reagir pro-ativamente aos incidentes.

> Controlar reativamente um sistema fazendo ajustes de acordo com as modificações ocorridas em seu ambiente e gerenciar pro-ativamente, possibilita detectar tendências ou anomalias que permitam executar ações antes que surjam problemas mais graves. Uma das funções do administrador de redes é justamente evitar ou responder de forma rápida a quaisquer tipos de anomalia. Para tal, deve-se possuir conhecimento suficiente e dispor de ferramentas que indique as falhas, e com isso, tomar atitudes necessárias a fim de manter a rede ativa e os serviços disponíveis. (Ernando, 2015, p. 20)

Segundo Benini e Daibert (2017), monitorar rede é verificar o funcionamento de cada serviço e equipamento disponível. Para isso é necessário utilizar ferramentas que verificam o funcionamento adequado dos equipamentos e serviços, enviando relatórios e alertas aos administradores, prevenindo falhas, e fazendo com que sejam corrigidas antes que sejam notadas pelo usuário.

Os sistemas e/ou ferramentas de monitoramento devem possuir características que atendam às necessidades do administrador da rede. Segundo COUTO (2012), a arquitetura geral dos sistemas de gerenciamento de redes apresenta 4 componentes básicos:

- Elementos Gerenciados: são denominados agentes e são implementados por um software que permite o monitoramento e o controle do equipamento.
- Estações de Gerencia: interage diretamente com os agentes para monitorá-los e gerenciá-los.
- Protocolo de Gerencia: é a interface entre a estação de gerencia e o agente por meio de uma normatização das operações de monitoramento (leitura) e controle (escrita).
- Informações de Gerencia: são os dados que podem ser referenciados em operações do protocolo de gerencia, que podem ser: estáticos, dinâmicos e estatísticos.

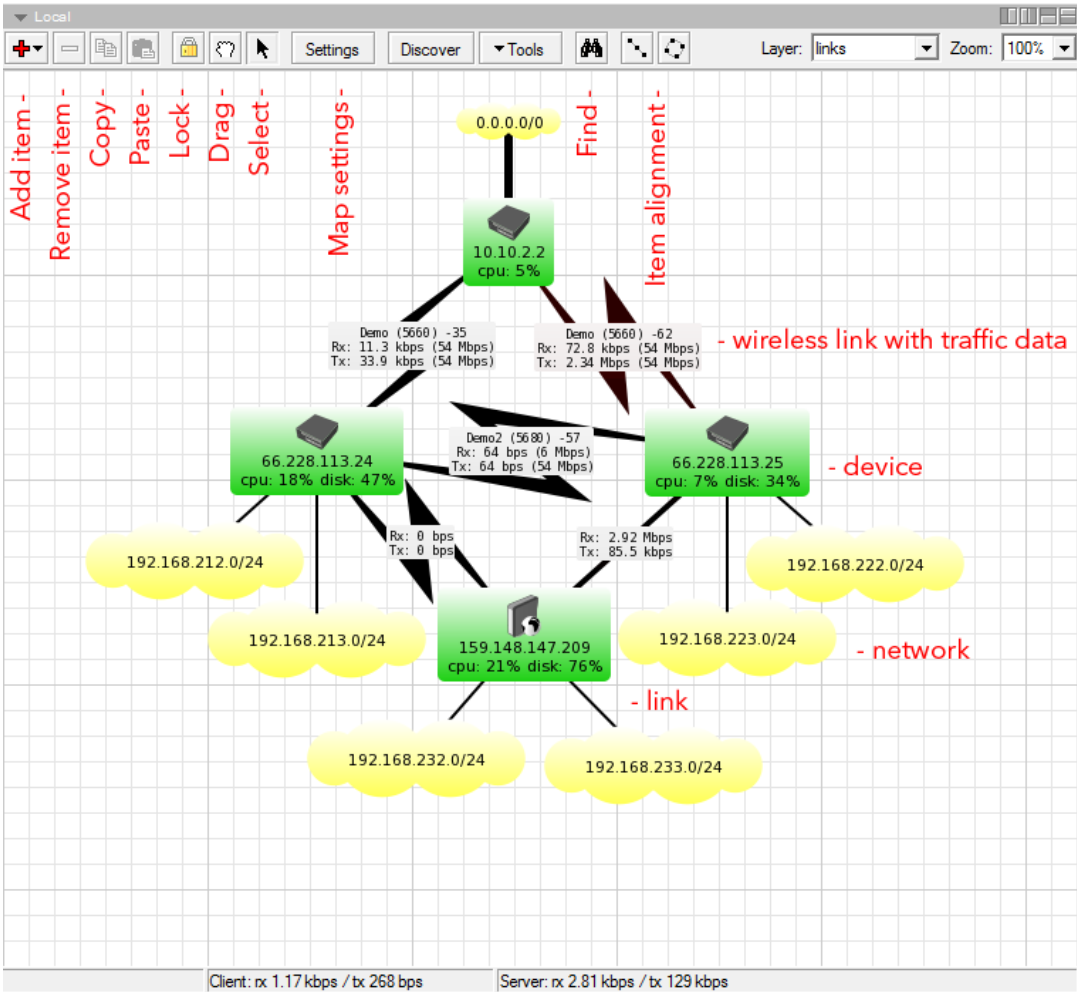
2.2 FERRAMENTAS DE MONITORAMENTO DE REDE

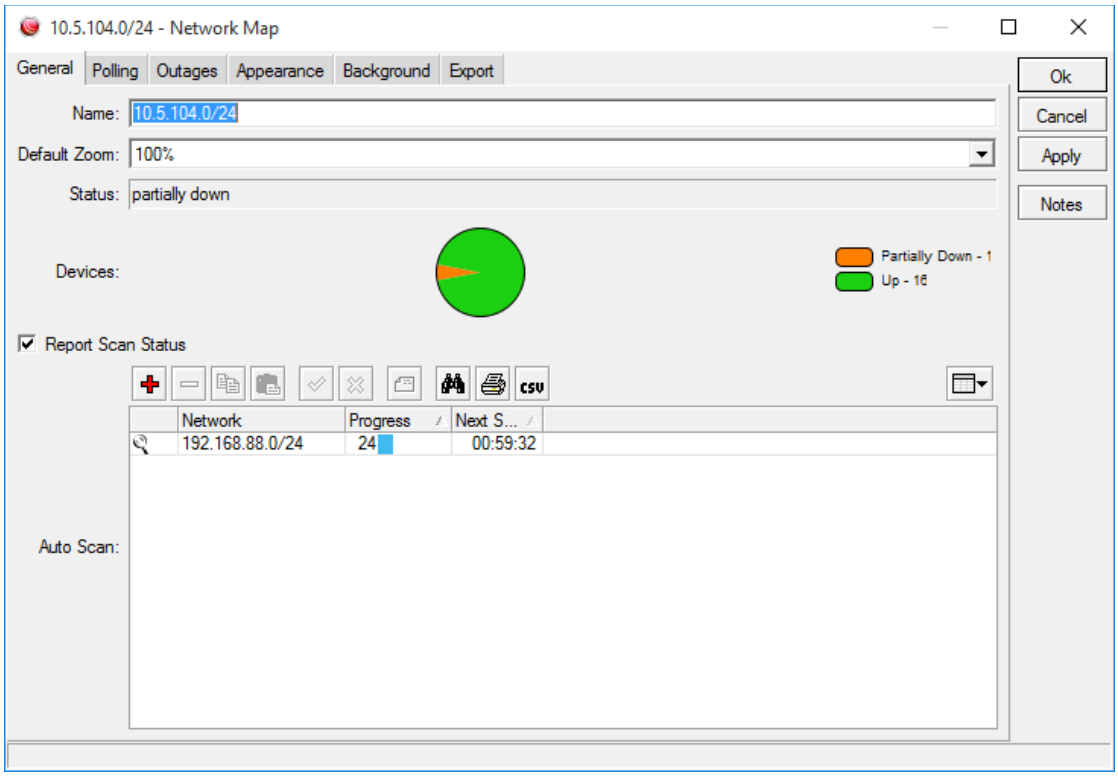
As ferramentas de monitoramento de rede permitem que se visualize todos os ativos que estejam conectados à rede, assim como todos os serviços disponíveis nela. Nesta parte do trabalho iremos apresentar algumas ferramentas disponíveis apresentando suas principais características e funcionalidades. As ferramentas serão The Dude, WhatsUP e Nagios.

2.2.1 The DUDE

A ferramenta de monitoramento de rede *The DUDE* permite que se faça um levantamento de toda a rede monitorando todos os dispositivos conectados. Fornece informações acerca de quedas e restabelecimentos, serviços, assim como uso de recursos de equipamentos. Permite o mapeamento da rede com gráficos da topologia da rede. Notificações via audio/vídeo/email acerca de eventos. Gráfico de serviços mostrando, latência, tempos de resposta de DNS, utilização de banda, informações físicas de links, entre outros. A ferramenta é totalmente gratuita e pode ser instalada em diversos sistemas operacionais

Figura 6: Mapeamento The DUDE





Fonte: Desenvolvedor(disponível em:https://mikrotik.com/img/mtv2/dude2.PNG)

Figura 7: Mapeamento de Rede com The DUDE

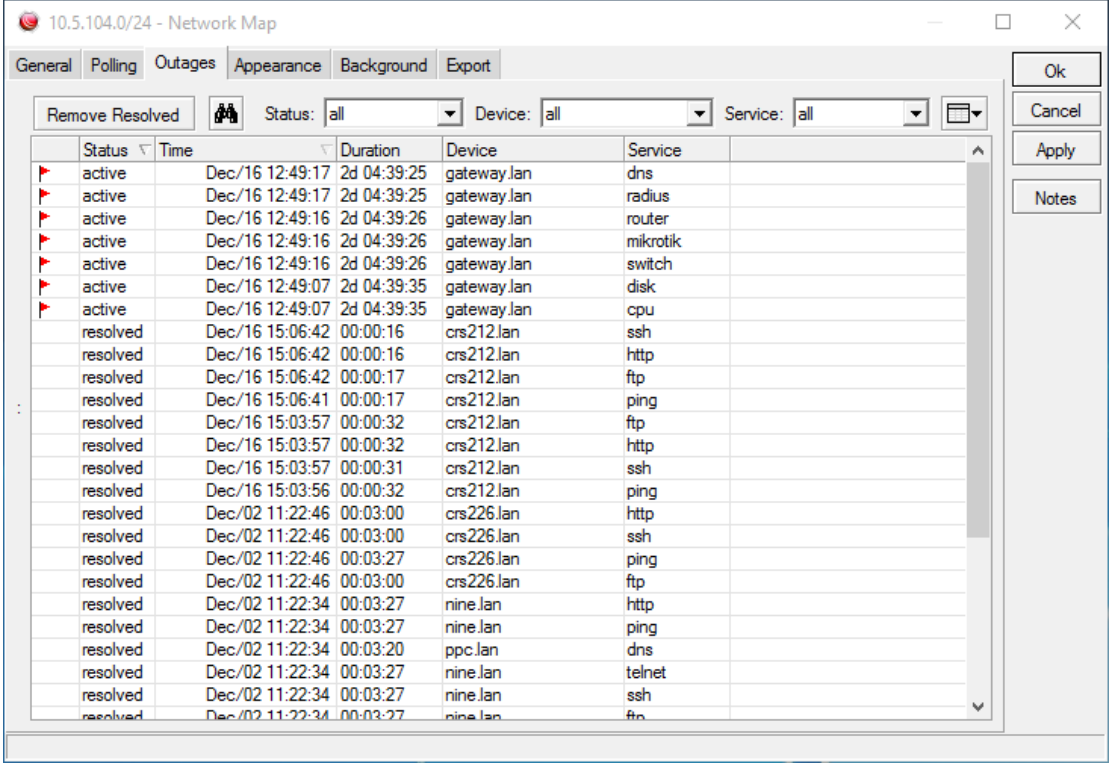


Figura 8: Mapeando IPs da rede

A ferramenta possui uma interface simples e intuitiva de uso. Tem a facilidade de ser completamente gratuita e poder ser instalada em diversos sistemas operacionais.

2.2.2 WhatsUP

É um software que permite o gerenciamento de uma rede através de recursos gráficos para mapear e monitorar. A aplicação permite o envio de notificações. Possui uma versão gratuita sendo sua versão comercial mais usual, versão essa conhecida como WhatsUP GOLD.

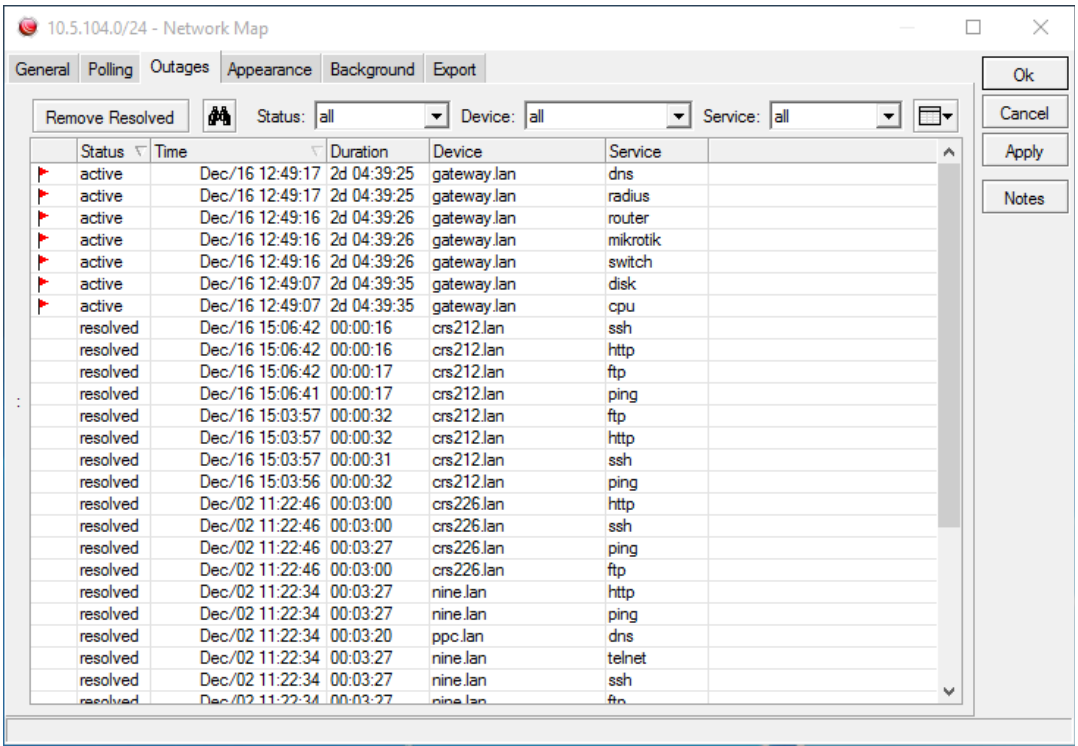
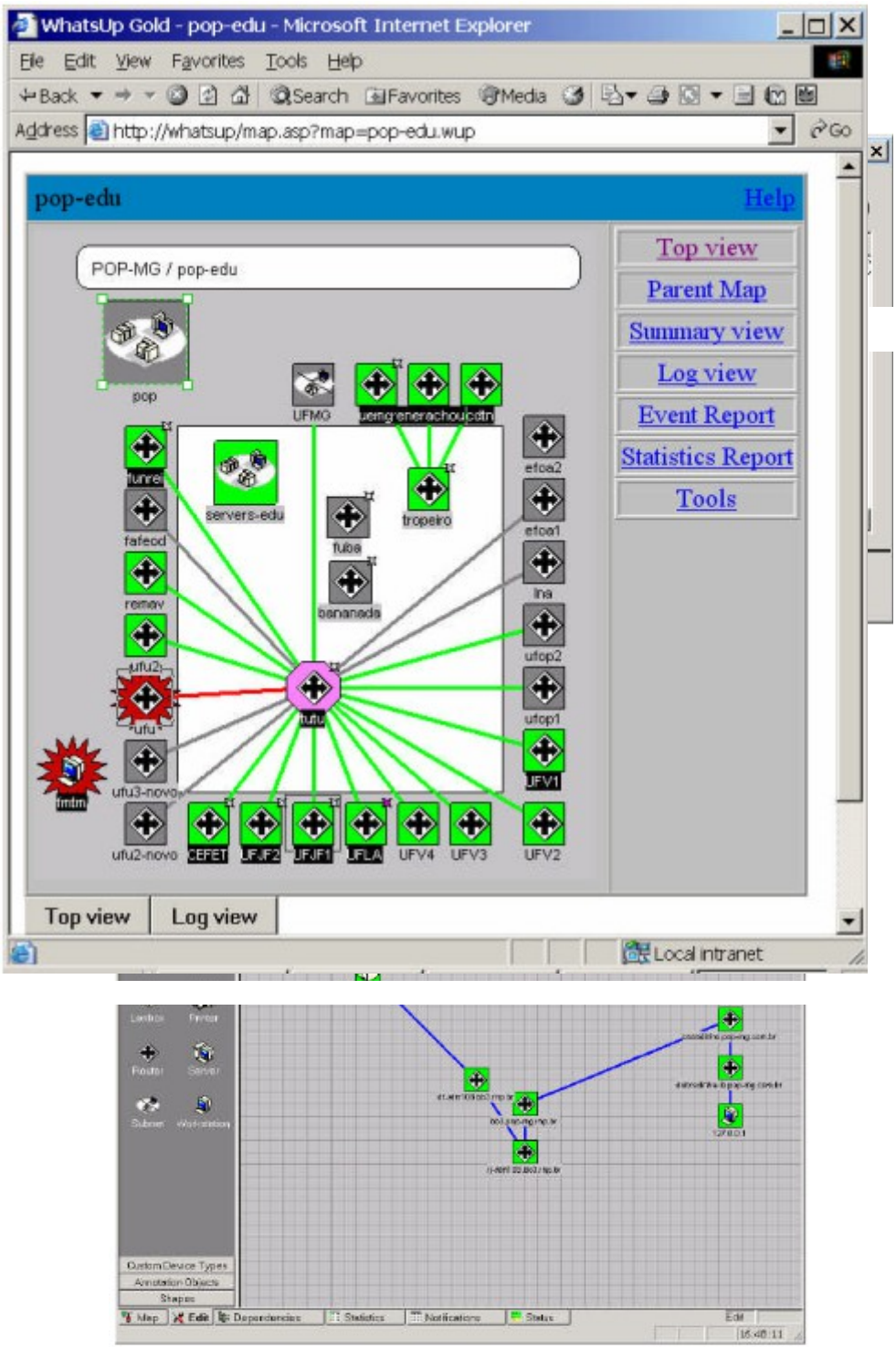


Figura 9: *Varredura com WhatsUp*

Figura 10: Mapa da rede**,** *WhatsUP*

A ferramenta permite a monitoração de equipamentos e serviços; Receber notificações de problemas; Mapear a rede; Gerar relatórios de disponibilidade, desempenho e capacidade; Permite o gerenciamento via aplicação WEB.

Figura 11: *Mapa de uma rede com WhatsUP*



2.2.3 Nagios

O NAGIOS é uma ferramenta de monitoração de rede de código aberto distribuída sobre a licença GPL. Ela permite que monitore os clientes (dispositivos/hosts) e serviços. Ela gera alertas quando problemas são apresentados**.** A ferramenta é conhecida mundialmente, sendo também disponibilizadas em versões pagas.

Suas principais funcionalidades são: o monitoramento de serviços de rede como tráfego de dados de host e serviços que podem ser definidos pelo administrador da rede, além de monitorar serviços como SMTP (*Simple Mail Transfer Protocol*), POP3 (*Post Office Protocol*), HTTP (*HyperText Transfer Protocol*), NNTP (*Network News Transfer Protocol*), ICMP (*Internet Control Message Protocol*) e SNMP (*Simple Network Management Protocol*).

Na versão gratuita a ferramenta possibilita a visualização web. Porém a configuração deve ser feita em seus arquivos de configuração, manualmente arquivo por arquivo. Em sua versão paga possui interface de configuração que facilita o processo.

Devido a ampla difusão da ferramenta é uma ferramenta excelente para uso por ter diversos documentos de suporte. Os fóruns disponíveis possibilitam a resolução de problemas relativos a utilização do NAGIOS.

Figura 12: Interface principal *NAGIOS*

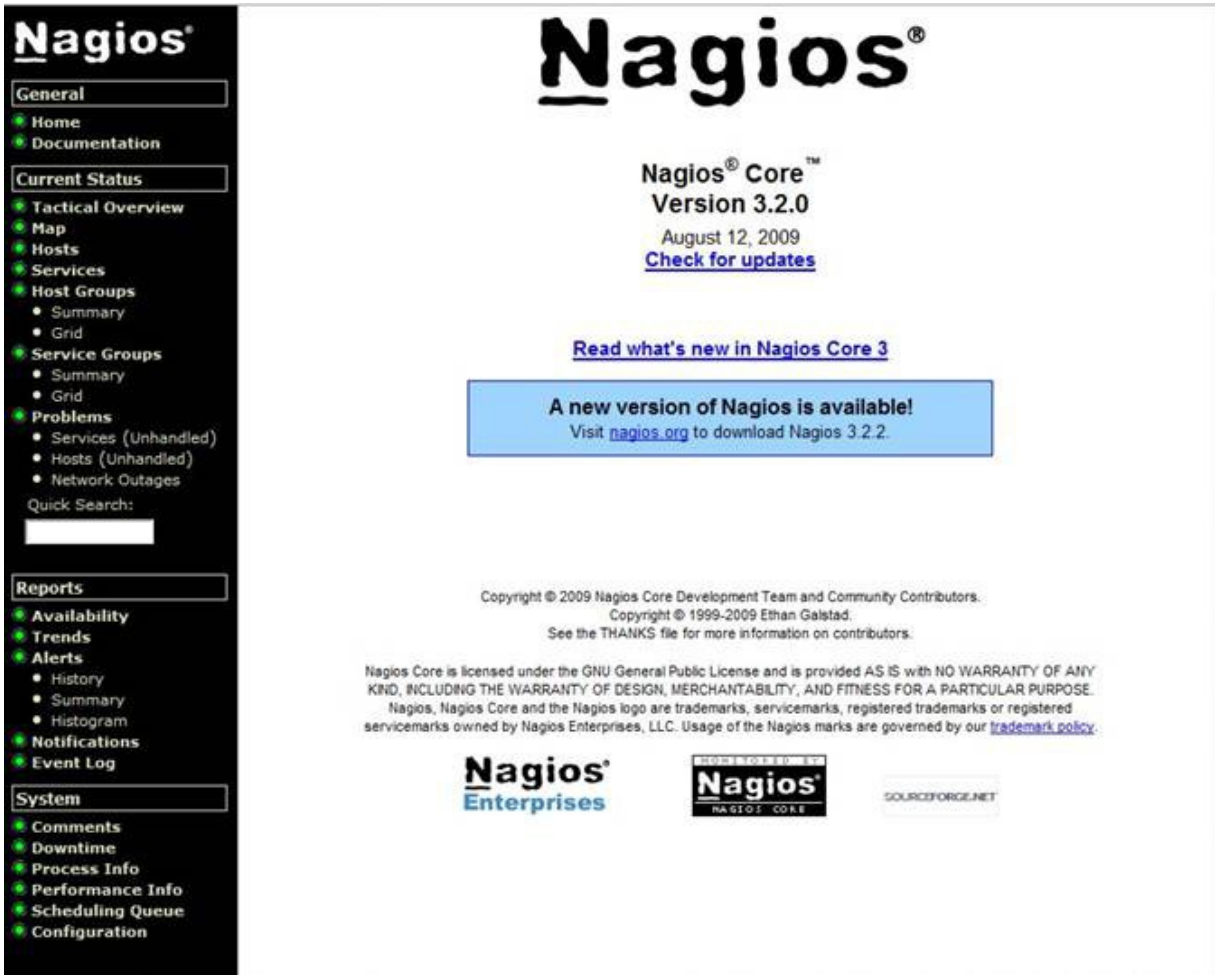
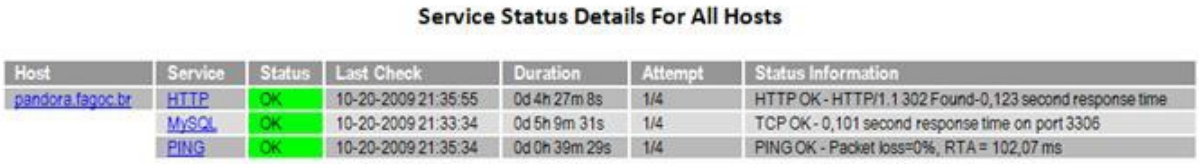


Figura 13: *Varredura de dispositivos conectados*

Como exemplo de um relatório temos a FIGURA 13, que a presenta uma interface principal, no menu *Current Status*, ao acessar a opção *Services* é exibido o nome do servidor (*Host*), os serviços que estão sendo monitorados (*Service*), a última verificação informando a data e a hora (*Last Check*), a duração da verificação (*Duration*), as tentativas de verificação (*Attempt*), além de informar o estado do serviço durante a verificação (*Status Information*),

Figura 14: *Interface de status*



Service Status Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Status Information
pandora.fagoc.br	HTTP	OK	10-20-2009 21:35:55	0d 4h 27m 8s	1/4	HTTP OK - HTTP/1.1 302 Found-0,123 second response time
	MySQL	OK	10-20-2009 21:33:34	0d 5h 9m 31s	1/4	TCP OK - 0,101 second response time on port 3306
	PING	OK	10-20-2009 21:35:34	0d 0h 39m 29s	1/4	PING OK - Packet loss=0%, RTA = 102,07 ms

Em sua versão *open source* a configuração é trabalhosa o que demanda tempo e conhecimento dos sistemas UNIX.

Existem uma infinidade de ferramentas disponíveis na rede mundial de computadores, a intenção deste trabalho não visa falar sobre todas elas, nem tampouco ser um manual de uso para emprego de tais ferramentas. Após as ferramentas escolhidas de maneira bem sucintas, este trabalho vai detalhar o emprego apresentando as funcionalidades de um software que, não é necessariamente uma ferramenta de monitoração de rede. Ele é um firewall e roteador que permite a configuração, manutenção e visualização do que acontece com a rede. Serão apresentadas as características do software e impressões do seu uso (como dito anteriormente, o autor utilizou o software durante aproximadamente 4 anos).

3. RESULTADOS E DISCUSSÃO

Visando responder a problemática apresentada, este trabalho apresentará as vantagens e desvantagens do software testado, o software BRASILFW. Serão apresentadas as definições, vantagens e desvantagens da aplicação.

As definições apresentadas, neste trabalho, referentes ao projeto BRASILFW, podem ser encontradas no site do desenvolvedor do projeto. Disponível em: https://wiki.brazilfw.com.br.

3.1 Projeto BRASILFW

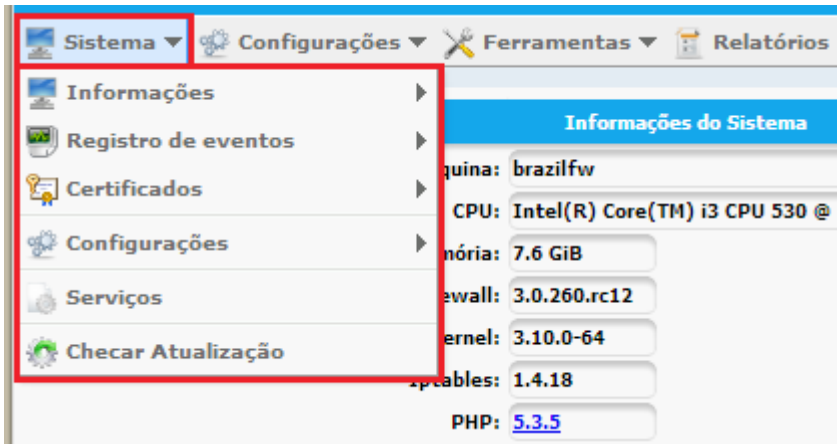
O BrazilFW *Firewall and Router*' é uma mini distribuição Linux que se destina a ser um Firewall e Roteador. Ele é uma mini versão de um sistema operacional que foi concebido para funcionar em maquinas com pouco recurso de hardware, por ser leve. Para se ter uma noção dos requisitos para se instalar esse sistema, a equipe de desenvolvimento aponta como requisitos mínimos: Processador 1 GHZ / 1 GB de memória RAM / 10 GB de HD. Características essas facilmente encontradas em computadores já obsoletos.

O BRASILFW funciona como uma “parede” entre a rede interna *(LAN ou MAN),* fazendo o gerenciamento dos dispositivos da rede interna, com a rede externa a ele (*MAN* ou *WLAN).*

3.1.1 Sistema

Na figura a seguir é demonstrada uma tela de informações do sistema no qual o software está instalado.

Figura 15: Informações do Sistema BRASILFw

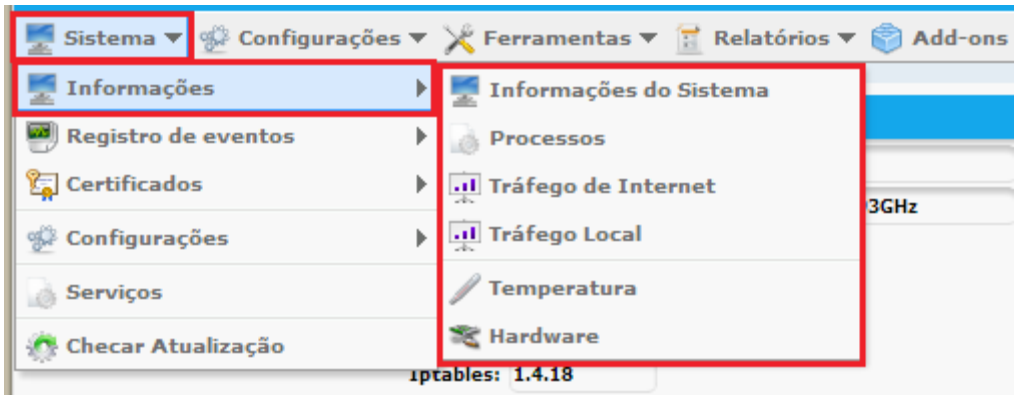


Fonte:htTps://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-01-pt-br.png

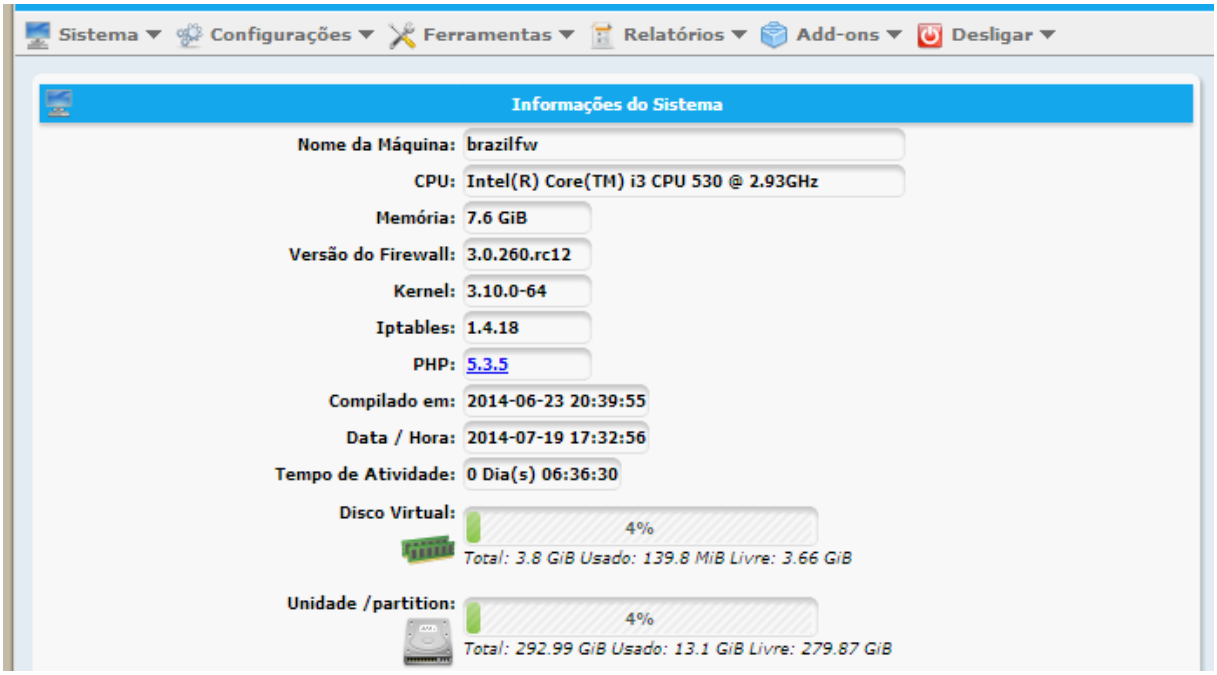
3.1.2 Informações

Nas figuras 16 e 17 veremos, na aba informações, algumas características do software, processos, trafego de internet entre outras.

Figura 16: Informações do Sistema

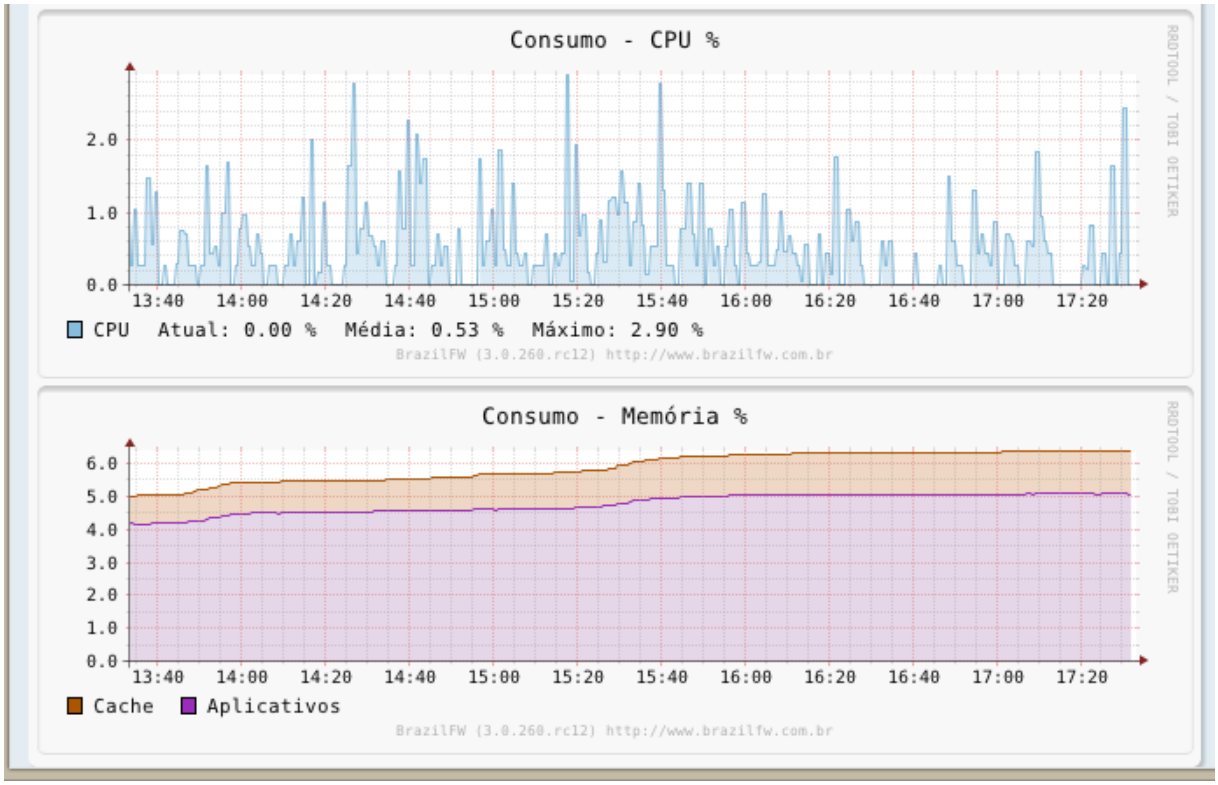


Fonte: https://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-02-pt-br.png



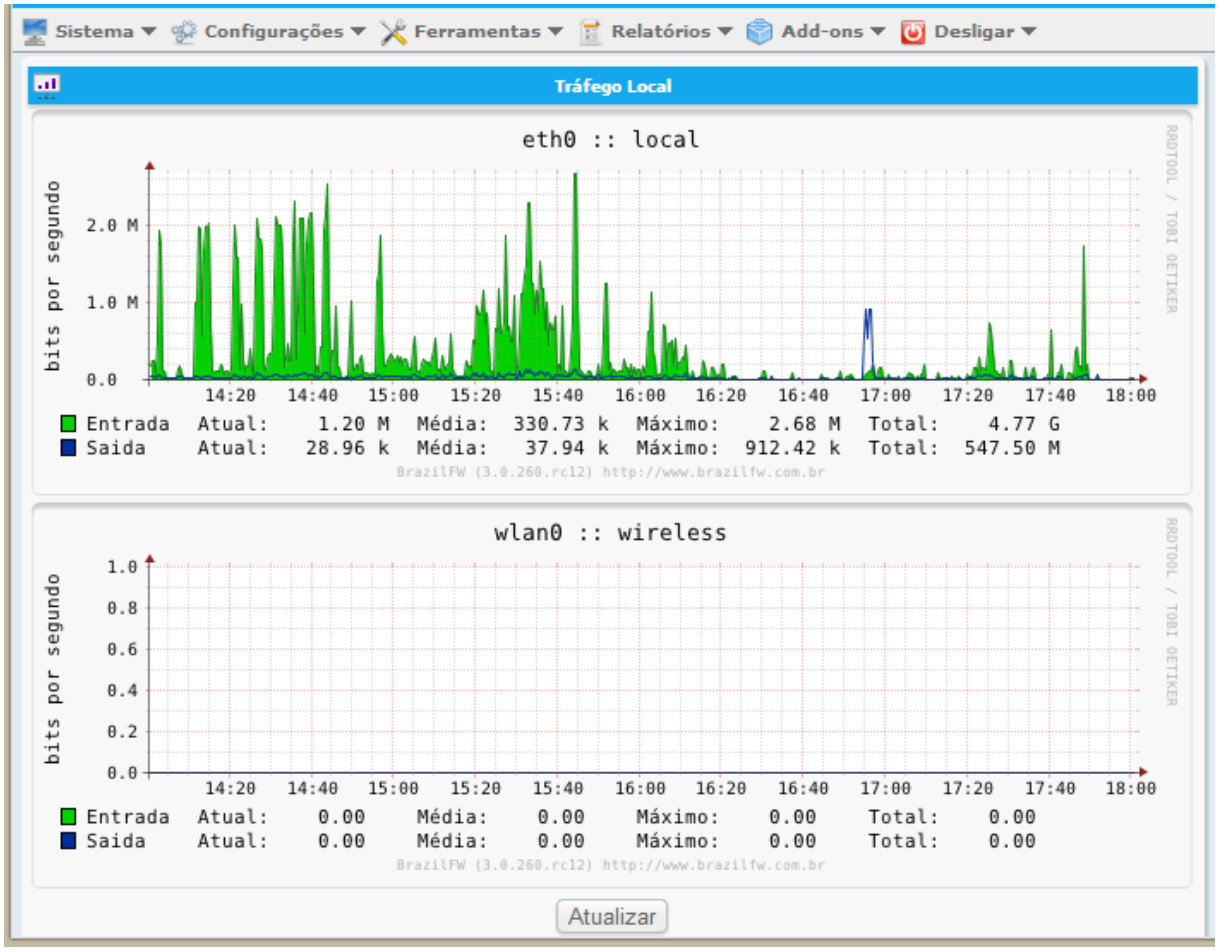
Fonte: https://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-03-pt-br.png

Figura 18: Informações de consumo de recursos



Fonte:https://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-04-pt-br.png

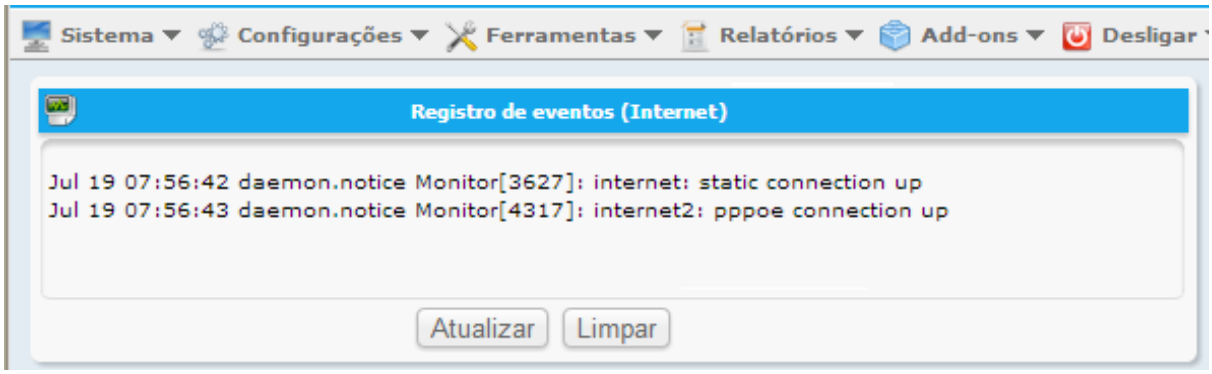
Figura 19: Trafego de rede nas interfaces de rede



Fonte: https://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-07-pt-br.png

Na figura abaixo podemos ver as informações do nosso link com a internet. Essa informação é essencial para sabermos se a rede interna recebe internet e se está distribuindo para os usuários da rede.

Figura 19: Trafego de rede nas interfaces de rede



Fonte: https://wiki.brazilfw.com.br/lib/exe/detail.php?id=system&media=wiki:system-13-pt-br.png

Todas essas informações se referem à máquina em que está “rodando” o BRASILFW. Elas são uteis para saber se o dispositivo está funcionando corretamente. Vale ressaltar que o software for sua facilidade de aplicação pode ser instalado em uma máquina virtual. Passaremos agora a apresentar algumas funcionalidades do sistema com suas respectivas análises. Não serão tratados aqui os parâmetros de configuração, uma vez que são simples e estão bem explicados no site do desenvolvedor do projeto.

3.2 Principais Funcionalidades

3.2.1 Consumo de internet

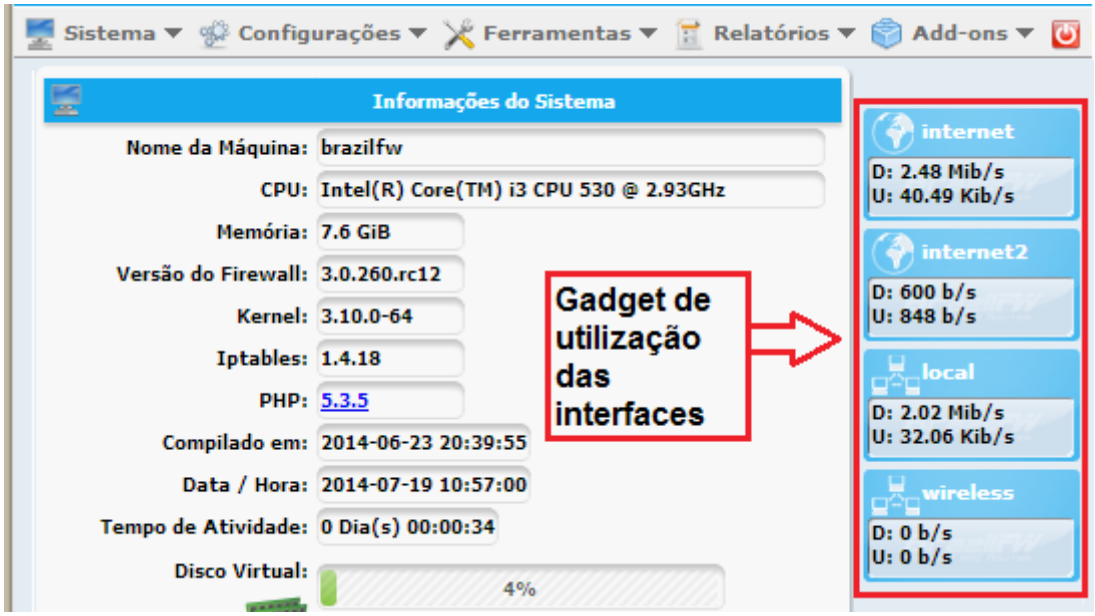
Exibe a tela de consumo das interfaces de rede. A velocidade de cada link/interface é atualizada cada 15 segundos. Esta tela permite saber se o link de internet contratado é adequado.

Como podemos observar, como o sistema permite gerenciar sub-redes e controlar o fluxo de cada placa.

Aqui cabe salientar, como mostraremos mais a frente, que o fluxo de rede pode ser interrompido pelo administrador, isso poderia ser feito por exemplo para limitar o acesso à internet durante o horário de expediente. Se houver um bloqueio

ativo ou algum problema com a conexão dos dados da “internet” estarão com o valor ZERO.

Figura 20: Estado dos *links* rede

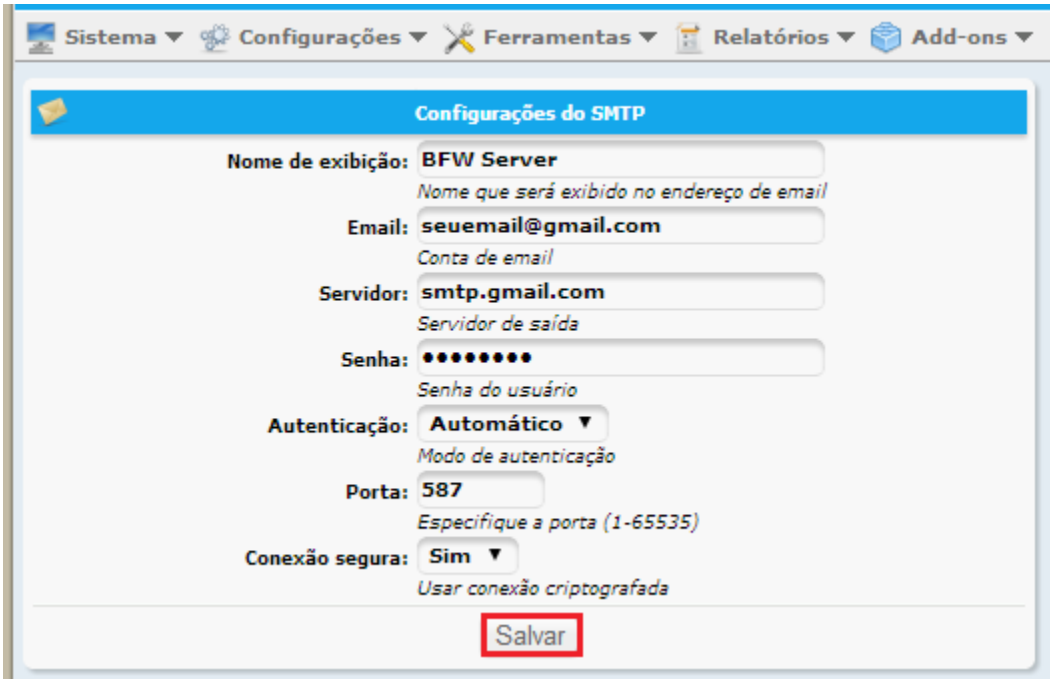


Fonte:ttps://wiki.brazilfw.com.br/lib/exe/detail.php?id=system_configuration&media=wiki:system-config-06-pt-br.png

3.2.2 Serviço de e-mail SMTP

O software permite que configuremos um e-mail para notificação de eventos críticos. O desenvolvedor possui uma serie de possibilidades.

Figura 21: Configuração de e-mail para recebimento de avisos



Fonte:htttps://wiki.brazilfw.com.br/lib/exe/detail.php?id=system_configuration&media=wiki:system-config-08-pt-br.png

3.2.2 Restrição de MAC

Essa funcionalidade é muito útil para configuramos quem vai utilizar a rede. Ela permite ao administrado configurar uma “Lista Branca”, basicamente selecionamos os MAC que poderão usufruir dos recursos da rede. Quando da informação podemos inserir uma série de informações sobre o MAC, por exemplo tipo de máquina e quem é o usuário.

Essa funcionalidade se mostrou muito útil para aumentar a segurança da rede. Principalmente quando a rede possui centenas de dispositivos. Ajudou bastante quando da montagem de redes para determinadas atividades temporárias. Mesmo o usuário sabendo a senha da WI-fi ou conectando um cabo de rede ao seu dispositivo ele não conseguirá o acesso, somente se o administrador liberar o acesso.

Uma das vantagens do sistema é permitir que isso seja feito via aplicação web. Ou seja, mesmo remotamente o administrador pode configurar a listra branca.

3.2.3 Proxy

O BRASILFW também pode instalado um *proxy Squid*. Nele pode ser configurado uma lista de restrições de sites que podem ser acessados sem a necessidade de se implementar um outro sistema para essa finalidade. Essa funcionalidade se deve ao fato de ser uma distribuição Linux e em tal SO é muito comum a utilização do proxy Squid.

Combinada com ferramentas adicionais, pode se configurar horários para acesso a determinadas páginas (essa função não é exclusiva do BRASILFW, está sendo descrita aqui apenas como uma boa pratica a ser adotada).

3.3 Vantagens e desvantagens

O BRASILFW é um software de código aberto, podendo ser implementado por qualquer indivíduo em redes *LAN.* Por ser um programa versátil sua utilização não demanda grande recursos de hardware, o que facilita, por exemplo a utilização de dispositivos que não atendem mais as necessidades do usuário para que se instale o sistema.

O sistema possui uma serie de ferramentas que podem ser instaladas, ferramentas desenvolvidas especificamente para uso como o software. Elas podem ser *scaners* de pacote, ferramentas antivírus e diversas outras que podem ser implementadas de acordo com a necessidade do usuário.

Se compararmos as ferramentas de monitoramento apresentadas, The DUDE, WhatsUp e Nagios – lembrando que o BRASILFW é um firewall que tem funcionalidades e ferramentas para o monitoramento da rede – ele tem a vantagem de ser open *source*, porém as ferramentas possibilitam uma série de configurações de alertas que o BRASILFW não possui por padrão. Se compararmos com a ferramenta Nagios, como dito uma das mais difundida entre administradores de rede, ele carece de uma série de funcionalidade, como desenho da rede, tempo de conexão, visualização de conteúdo acessado pelo usuário em tempo real, entre outros fatore.

Outra desvantagem é a falta de atualizações constantes do sistema como um todo, a última versão disponível é do ano de 2016.

Existem diversos sistemas no mercado ou na rede mundial de computadores, aqui apresentamos mais uma solução para aumentar a segurança dos ativos e, mais importante, da informação gerida e produzida por uma organização com custo monetário zero.

4. CONSIDERAÇÕES FINAIS

Desde sua criação a rede mundial de computadores cresceu de maneira desordena, carecendo de regulamentação e padronização. Assim como os dispositivos e softwares que permitem a interação entre os computadores desde a utilização doméstica até alcançar proporções mundiais. Hoje utilizando o computador podemos utilizar serviços e facilidades fornecidas por empresas, que por sua vez tem seus servidores hospedados a milhares de quilômetros.

Para as organizações esses fatores de crescimento continho, da rede e da informação, gera a possibilidade de interação com uma gama diversificada de colaboradores. Produzindo e trocando informações sensíveis para a condução dos negócios da empresa.

Como vimos ao longo trabalho a evolução constante dos sistemas tecnológicos exige que os responsáveis pelas soluções de TIC estejam sempre buscando aprimorar técnicas métodos e sistema para poder agir pro-ativamente nesse ambiente. Juntamente com esse avanço tecnológico em larga escala cresce a

quantidade informação a ser gerida. Nesse quesito é de extrema importância que a informação seja confiável, armazenada de modo seguro e esteja disponível para que possa agregar valor à organização.

As empresas necessitam, o todo tempo, de conexão com seus colaboradores e acesso a informação para fornecer produtos competitivos. Nesse cenário as equipes de TI dessas organizações devem estar preparadas para garantir a informação nesse e conexão nesse ambiente de máquinas interligadas.

Vale ressaltar que apesar do caráter social da rede mundial de computadores, que possibilita a interação entre seus usuários e permite o acesso a uma gama de conhecimento. Existem também milhares de agentes mal-intencionados que atuam aproveitando as brechas do sistema, a falta de regulação da rede e a inocência dos usuários finais.

Assim as equipes de TI, tem que lidar ainda com o fator segurança da rede. Como infelizmente não existem sistemas extremamente seguros, essas equipes devem buscar soluções que garantam a impenetrabilidade da rede. Não se pode permitir que a informação seja furtada por agentes externos a rede.

O Exército Brasileiro também está inserido nesse contexto. As informações geridas e produzidas são de extrema importância para sua estratégia organizacional.

Assim existe a necessidade de toda estrutura de uma equipe de TI possuir ferramentas que se adequem a organização. Algumas soluções exigem um elevado grau de aporte financeiro para que possam ser implementadas. Por isso, solução de código aberto são uma solução para o bom funcionamento das estruturas de TI, além é claro de uma equipe qualificada para tratar os incidentes.

Ao longo do trabalho podemos conhecer um pouco mais sobre ferramentas consagradas para monitoramento de rede. Ferramentas gratuitas que são de fácil implementação que permite que o administrador de TI possa agir antes que o problema ocorra. Essas ferramentas possuem em sua maioria versões comerciais que implementam funcionalidades a elas.

O sistema BRASILFW é mais um software, firewall e roteador, totalmente gratuito e código fonte aberto que permite, ademais das funções nativas, inserir uma série de funcionalidades ao seu sistema. Essas funcionalidades se assemelham àquelas fornecidas pelas ferramentas aqui apresentadas. Soluções como visualização de dispositivos conectados, tempo de conexão, consumo de cada dispositivo, páginas que estão sendo acessados entre outros serviços.

A organização para seguir com seus trabalhos necessita que seus sistemas de Tecnologia da Informação e Comunicação estejam funcionando corretamente. Por isso valer-se de ferramentas como as apresentadas neste trabalho. Permite que suas equipes de TI possam monitorar, mapear e agir antes que os problemas aconteçam devido os alertas gerados pelas ferramentas.

As ferramentas podem e devem ser utilizadas em conjunto combinadas com boas práticas para gerir a informação.

REFERÊNCIAS

BRASIL.EXERCITO. Regulamento Interno e dos Serviços Gerais – R1(RISG). SECRETARIA GERAL DO EXERCITO:2013.

NHASENGO, Bernardo Cândido David; RAZZOLINI, Edelvino Filho. Monitoramento da informação usando sistemas de informação. IX Convibra Administração – Congresso Virtual Brasileiro de Administração. 2012. Disponivel em:<http://www.convibra.com.br/upload/paper/2012/29/2012_29_4426.pdf> Acesso em: 20 de agosto de 2018.

LOVATTO, Maico. Gerenciamento e Segmentação de Redes: Estudo de caso em empresa do setor alimentício. 40f. Monografia (Especialização Semipresencial em Redes de Computadores) – Universidade Tecnológica Federal do Paraná. Pato Branco: 2015.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. Cartilha de segurança, Disponível em: <https://cartilha.cert.br/redes/>acesso em 05 de novembro de 2017.

TANENBAUM, Andrew S. Redes de computadores. 5ª edição. Amsterdam, Holanda:2011.

ERNANDO, Washington Pereira Benício. Monitoramento e Gerenciamento de Redes Utilizando Zabbix. São Paulo: 2015.

BLACK , Tomas Lovis. Comparação de Ferramentas de Gerenciamento de Redes. Porto Alegre: 2008.

COUTO, ANDRÉ VALENTE DO. Uma abordagem de Gerenciamento de Redes baseado no Monitoramento de Fluxos de Tráfego Netflow com o suporte de Técnicas de Business Intelligence. Dissertação de Mestrado, Publicação PPGENE.DM–107/2012,Departamento de Engenharia Elétrica, Universidade de Brasília: 2012.

GRÜTZMANN, Giales Fischer. Uso da ferramenta Dude para monitoramento de uma rede pequeno porte geograficamente distribuída. Faculdade de Tecnologia Senac Pelotas (FATEC).

BENINI, Renata Aparecida; DAIBERT, Marcelo Santos. Monitoramento de Redes de Computadores - Artigo Revista Infra Magazine 1. Disponível em: < https://www.devmedia.com.br/monitoramento-de-redes-de-computadores-artigo-revista-infra-magazine-1/20815>. Acesso em: 07 março de 2018.

ANTUNES, Anderson Rodrigo. Nagios Trabalhando em Maquina Virtual. Pontifícia Universidade Católica do Paraná. Curitiba: 2010.

MONTEIRO, Murilo Silva. WhatsUp Gold. PoP-MG/DCC/UFMG. UFMG: 2002. Disponível em: < https://memoria.rnp.br/_arquivo/sci/2002/whatsup.pdf>. Acesso em: 01 de setembro de 2018.

FRANCISCATTO, Roberto; CRISTO, Fernando; PERLIN, Tiago. Rede de computadores. Universidade Federal de Santa Maria: 2014.

PRIGGE, Matt. 5 Recursos que todo Sistema de Monitoramento deveria ter. Disponível em:<http://computerworld.com.br/tecnologia/2015/02/16/5-recursos-que-todo-sistema-de-monitoramento-deveria-ter>. Acesso em: 06 de novembro de 2017.

BRASILFW. Disponível em: < https://wiki.brazilfw.com.br>. Acesso em: 7 de novembro de 2017.

Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão, 2Crimes cibernéticos / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília : MPF, 2018