CONTROLE E MONITORAMENTO INTERNO COM SOFTWARE DE GESTÃO DE REDE LOCAL

João Pedro Cher Benetis dos Santos, E-mail: joaocher@gmail.com
Maria Carolina de Oliveira, E-mail: karolina_olive@hotmail.com

Resumo: A tecnologia está cada vez mais presente em todos os lugares, fazendo parte da vida diária de grande parte da população, sendo utilizada para diversos objetivos. O avanço tecnológico está aumentando e proporcionado vários meios de aperfeiçoamento para diversos setores da sociedade. No ambiente de trabalho, se faz uso de vários sistemas e procedimentos tecnológicos para aumentar o fluxo de tarefas, propiciando maior facilidade de manipulação de informações. Em instituições e empresas que fazem uso de tecnologias para otimizar e aumentar o fluxo de suas rotinas, existe o setor de Tecnologia da Informação, responsabilizado em organizar e monitorar as operações relacionadas a equipamentos e dispositivos de hardware, e sistemas de software, investindo em meios de avaliar e garantir maior performance de segurança dentro do ambiente de trabalho. Visando esta alta performance de uso tecnológico, o monitoramento da rede local é um dos principais fatores que possibilitam a otimização das tecnologias e recursos utilizados por usuários, analisando os dados trafegados e conexões requisitadas através da rede por sistemas e usuários. O monitoramento dentro de uma rede específica permite avaliar e detectar anomalias, permitindo um controle maior sobre recursos, prevendo situações de risco e criando soluções de problemas**.**

Palavras-chave: Conexão, internet, monitoramento, rede, usuários.

CONTROL OF LOCAL NETWORK WITH ANALYSIS SOFTWARE

Abstract: Technology is increasingly present everywhere, being part of the daily life of a large part of the population, being used for various purposes. Technological advancement is increasing and providing various means of improvement for various sectors of society. In the work environment, various systems and technological procedures are used to increase the flow of tasks, making it easier to manipulate information. In institutions and companies that make use of technologies to optimize and increase the flow of their routines, there is the Information Technology sector, responsible for organizing and monitoring operations related to equipment and hardware devices, and software systems, investing in means to evaluate and ensure greater safety performance within the work environment. Aiming at this high performance of technological use, monitoring the local network is one of the main factors that enable the optimization of technologies and resources used by users, analyzing the data transmitted and connections requested through the network by systems and users. Monitoring within a specific network allows evaluating and detecting anomalies, allowing greater control over resources, predicting risk situations and creating problem solutions.

Keywords: Connection, internet, monitoring, network, users.

1. Introdução

Atualmente, a grande maioria das empresas possui uma estrutura de tecnologia que permite um fluxo de trabalho melhor por meio de vários métodos, ferramentas e sistemas. Uma parte importante dessa área é a rede corporativa que, geralmente, se concentra em padrões de rede local com *hardware* sendo *switches*, roteadores, cabeamento *ethernet* e *software* de *firewall* que faz o intermédio das conexões fazendo a validação das requisições de acesso.

Empresas como Cisco, Palo Alto Networks, Linksys, HP Inc. e outras são especializadas em fabricação de equipamentos para redes de alta performance, projetadas para os requisitos das empresas e instituições modernas. Os *switches* e

roteadores possuem como principal função conectar uma rede local à ISPs (*Internet Service Provider*) através de uma infraestrutura remota de fibra óptica ou banda larga, possibilitando transferências de dados em alta velocidade entre hosts locais em um ambiente empresarial. Diversos *hosts* são conectados juntos em uma rede local, compartilhando recursos de conexão com a internet, impressoras e sistemas de *software*.

Entretanto, equipamentos de última geração não garantem sistemas imunes a falhas e ataques, fazendo-se necessário, outros meios de providenciar um maior controle e segurança como *softwares* de *firewall* que estabelecem regras para requisições de usuários e serviços, proibindo navegações em determinados sites. Também é possível exigir conexões de usuários em outros endereços IP (*Internet Protocol*) específicos para serviços internos, sendo necessário um meio de monitoramento, e este é um processo que analisa em tempo real, os recursos que estão sendo utilizados pela rede, possibilitando revelar falhas na performance e disponibilidade de recursos, assegurando uma alta capacidade de fluxo de processos, ou processamento, com o máximo de controle possível.

Diante do exposto, com o intuito de melhorar o controle e monitoramento de uma universidade estadual do Paraná, este trabalho teve como foco a análise da rede da unidade em que se encontra a Reitoria, pois possui setores responsáveis pela gestão da instituição tanto na área administrativa quanto na parte de ensino, e que centraliza diversos processos dos demais campis.

O objetivo geral é identificar anomalias e criar possíveis soluções para sanar problemas e aumentar a qualidade da rede local. Para isso, é proposto a utilização de um *software* de gestão e monitoramento alternativo ao meio já existente, almejando aumentar a segurança e controle; o diagnóstico da rede atual, obtendo informações sobre conexões e acesso; e indicar as falhas a partir dos dados obtidos buscando possíveis melhorias na rede.

O *software* de monitoramento Nagios XI foi utilizado para cumprir tais objetivos, buscando demonstrar de maneira simples o estado da rede através do controle do *switch* principal, identificando a situação de conexões estabelecidas. Com uma rede devidamente monitorada, gerida e organizada, o órgão público pode contar com uma segurança e agilidade para que os colaboradores realizem suas rotinas, otimizando o serviço público e evitando possíveis contratempos em relação às conexões.

2. Fundamentação Teórica

Nesta parte serão abordados conceitos sobre as tecnologias utilizadas no trabalho, sendo a subseção 2.1 sobre o tema de redes de computadores, a 2.2 sobre sistemas de controle de tráfego, e por fim a subseção 2.3 sobre o Linux.

2.1 Rede de Computadores

A rede de computador é um sistema que interliga dois ou mais dispositivos e seus periféricos visando comunicação e compartilhamento de dados. Alguns componentes podem constituir na rede sendo eles hardware - equipamento físico como computadores, *switches*, servidores, impressoras e diversos outros eletrônicos; ou componente de *software* - que são aplicações ou recursos utilizados pela rede, como protocolo de transporte de dados TCP/IP (*Transmission Control Protocol/Internet Protocol), HTTP (HyperText Transfer Protocol*), serviço de e-mail (RIBEIRO, 2016).

Os *switches* são dispositivos com várias portas, cada qual pode-se conectar a um computador, fazendo função de interligação das máquinas na rede, atuando como

camada de enlace, repassando pacotes entre equipamentos conectados a ele reconhecendo os endereços de acesso ao meio (MAC) e identificando a origem e destino dos dados (TANENBAUM, 2011).

Os protocolos de rede definem regras que estabelecem um padrão e uma ordem das requisições de dados, guiando ações a serem executadas durante a transmissão e recepção dos dados. Dispositivos que integram uma rede de computadores transmitindo e recebendo dados são denominados de "nós de rede", um ponto de conexão (TANENBAUM, 2011).

Os exemplos de rede de computadores mais comuns são a internet, um sistema global de ligações entre computadores que fazem uso de protocolos para servir usuários de todo o mundo; e a intranet, uma rede privada que usa de protocolos da internet, mas de forma específica de um determinado local, como uma empresa, em que o acesso é feito somente pelos usuários internos.

Existem dois tipos de rede: a física e a lógica. Na rede física é representada a forma da aparência da estrutura da rede, como os nós estão conectados e os meios de conexão dos dispositivos. A rede lógica é a maneira de como as requisições acontecem sobre os meios de rede, como são transmitidos os dados através da ligação física entre dispositivos conectados na rede. A forma que uma rede é estruturada corresponde à topologia. Na Figura 1 podem ser observadas algumas topologias básicas.

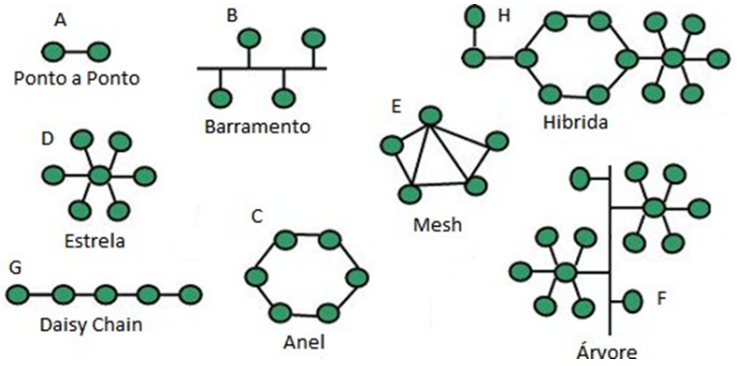

Figura 1 – Topologias de Rede – Adaptado de Tanenbaum (2007)

Na Figura 2(A) está a rede Ponto a Ponto (Peer-to-peer), onde cada um dos "nós" rede atua como cliente quanto servidor, transmitindo e recebendo dados, sem a necessidade de um servidor central. Na rede Barramento todos os dispositivos são interligados em um mesmo barramento físico de dados, onde apenas um dispositivo pode utilizar do barramento por vez – Figura 2(B). Na topologia Anel os dispositivos são conectados em série formando um círculo fechado, onde os dados são transportados de forma unidirecional de "nó" em "nó" até chegar ao destino específico – Figura 2(C). A topologia Estrela é a que possui um elemento centralizado responsável por gerir o fluxo de dados da rede, diretamente conectado a cada "nó" – Figura 2(D). A Malha (Rede Mesh) é uma rede composta por vários "nós" de APs (Access Point) em que os clientes devem utilizá-los para poderem trafegar – Figura 2(E). Por fim, a rede Árvore é composta de interligações que geralmente partem de uma central e se divide em outros ramos menores que se conectam – Figura 2(F).

Existe a topologia Híbrida – Figura 2(H), que é estruturada de forma a comportar o ambiente específico, podendo utilizar mais de uma topologia juntas na mesma estrutura.

A topologia *Daisy Chain* (Rede Encadeada) – Figura 2(G) – é caracterizada por uma estrutura com conexões com cada dispositivo ligado em série com o próximo, onde a

mensagem é retransmitida em sequência, passando por cada "nó" até chegar ao destino (RIBEIRO, 2016).

As redes de computadores são responsáveis por toda a facilidade obtida no nosso cotidiano no que diz respeito à facilidade de comunicação e troca de informações entre pessoas e empresas, tornando-se uma ferramenta tecnológica indispensável.

2.2 Sistemas de Controle de Tráfego

Os sistemas de controle de tráfego agrupam ferramentas de software e hardware que podem analisar diversos aspectos de uma rede, ou seja, utilizando os recursos físicos e lógicos para acompanhar a performance e efetividade da rede, tendo em vista informar, prever, diagnosticar e alertar possíveis erros, demonstrando soluções que podem ser tomadas (JULIO, 2020).

O monitoramento permite obter uma visão geral de dispositivos conectados na rede e como está o tráfego do uso de dados, possibilitando identificar e mediar problemas que podem atrapalhar o desempenho e causar interrupções. Essa gerência é feita por sistemas que disponibilizam ferramentas de monitoramento que reduzem o trabalho das equipes de TI e aumentam a produtividade e segurança (JULIO, 2020).

O monitoramento usa diversos protocolos de rede, como SNMP (Simple Network Management Protocol), que atua na camada de aplicação, validando os status das respostas recebidas dos dispositivos conectados, além de monitorar a configuração do sistema. O ICMP (Internet Control Message Protocol) também é um protocolo que envia informações sobre processos de IP gerando mensagens de erro em caso de falha.

O sistema Nagios possui o protocolo NRPE que permite a execução de *plugins*, que podem ser ferramentas ou extensões associadas a outro programa, a serem executados de outro computador remotamente, podendo monitorar de maneira remota os status (RIBEIRO, 2016).

Esses sistemas de monitoramento que são utilizados na área de TI podem ser transformados para atender um planejamento de forma geral, adequando estratégias para o gerenciamento da rede, documentando informações e organizando em função de ciclo de vida dos serviços executados na instituição.

2.3 Nagios

É uma aplicação de monitoramento de hosts e serviços que alerta sobre eventuais problemas, gerenciando a rede por meio de duas maneiras.

Uma delas é através de conexão entre o servidor Nagios e uma "agente", que pode ser um servidor comum, por exemplo, em que há uma requisição do Nagios para verificar como está o uso da CPU, qual o espaço de armazenamento utilizado ou não, e o uso da memória RAM. Em resposta ao "agente", são enviadas essas informações as quais o Nagios trata e armazena, demonstrando de modo visual as informações do hardware. Assim, o sistema pode gerar alertas sobre as informações recebidas, caso haja algum possível problema, por exemplo, se o limite de armazenamento estiver sendo quase atingido (NAGIOS, 2022).

Uma segunda forma de gerenciamento é a possibilidade de analisar os elementos da rede é por protocolos de serviço de rede, como SNMP, POP3 (*Post Office Protocol*), HTTP, SMTP (*Simple Mail Transfer protocol*), ICMP, NNTP (*Network News Transfer protocol*), além de observar os recursos das máquinas, avaliando o uso e condições, possibilitando o monitoramento remoto por SSH (*Secure Shell*) ou TSL/SSL (*Transport*

Layer Security / Secure Sockets Layer), podendo haver integração com outros plugins, facilitando seu uso pelos usuários e permitindo ligação com outras aplicações por meio de bibliotecas (NAGIOS, 2022).

2.4 pfSense

Um *software* livre baseado no sistema operacional FreeBSD e gratuito de licença BSD – licença de código aberto, utilizado em sistemas Unix – com pacotes adicionais permitindo que ele seja considerado uma central unificado de gerenciamento de ameaças, podendo se gerar relatório em gráficos, modelagem de tráfego e filtragem utilizando de informações em tempo real, possuindo uma interface web fácil de ser utilizada. O pfSense também atua como firewall, servidor (internet, DHCP, NTP, Proxy, etc.), antivírus, antispam, detecção de invasão. É consideravelmente leve com poucos requisitos de hardware, estável que possui dashboard e interfaces configuráveis possibilitando configurações personalizadas e recursos de filtros de informações (4LINUX, 2022).

Este programa apresenta um *dashboard* com informações padrão do sistema – nome da rede, usuário, tipo do sistema, versão da BIOS, configuração da CPU, data e configuração DNS e informações personalizadas com interfaces e gráficos de tráfego. Na parte direita superior há interfaces informando o tipo da rede – LAN, WAN – a velocidade de conexão e a faixa de IP, logo abaixo está o gráfico de tráfego, mostrando dados de entrada e saída de uso da banda de rede, medindo a quantidade de Mb/s e o horário do tráfego de dados (SILVA, 2019).

2.5 Linux

Linux é um Kernel, responsável pelo funcionamento do computador, fazendo a comunicação entre hardware e software, permitindo a execução de aplicações. Esse Kernel é um conjunto de instruções que mantém os componentes físicos e lógicos da máquina, entretanto sendo necessário a utilização de programas adicionais para seu uso efetivo, como interpretadores de comandos e compiladores para possibilitar a criação de novos programas (NEGUS, 2014).

Criador por Richard Stallman, o projeto GNU visava desenvolver um sistema operacional livre baseado em Unix. Stallman criou uma licença de software chamada de GPL, que permitia a modificação livre do código do programa, porém deveriam ser compartilhados da mesma maneira e mantido os créditos dos desenvolvedores.

Assim sendo, Linux é o nome do Kernel e GNU/Linux é do sistema operacional - Kernel com programas adicionais (NEGUS, 2014).

No ambiente de estudo foi utilizado a versão do Ubuntu 20.04 LTS, sendo esta uma derivação do Linux. Existem várias distribuições Linux, que basicamente são compostas de aplicações juntamente do Kernel do sistema, podendo ser comercializadas ou não.

Ubuntu é um sistema operacional de código aberto que se origina da distribuição Debian, baseando-se na estabilidade do desenvolvimento do *software* e utilizando a interface GNOME como área de trabalho da sua versão (UBUNTU, 2022).

3. Procedimentos Metodológicos

Este trabalho foi desenvolvido para coletar dados de forma quantitativa (GIL, 2008) para avaliar o grau de uso da rede local pelos demais setores da unidade da instituição estudada, verificando as informações por *hardware* de compartilhamento de rede, no caso um *switch*.

Realizou-se uma abordagem sobre redes de computadores e as principais tecnologias utilizadas para o desenvolvimento da proposta de intervenção: os sistemas pfSense e Nagios, e o sistema operacional GNU/Linux na distribuição Ubuntu, em relação ao controle e monitoramento de rede. Esta primeira parte do trabalho caracteriza uma revisão de literatura, ou seja, uma pesquisa exploratória para identificar os principais conceitos e funcionalidades das tecnologias citadas de modo a compreender suas aplicações (GIL, 2002).

A fim de fazer um levantamento sobre o monitoramento da rede da Universidade Estadual do Norte do Paraná (UENP) - especialmente nos setores atrelados à Reitoria do campus de Jacarezinho/PR - elencando suas possíveis falhas, utilizou-se de uma pesquisa descritiva quantitativa e qualitativa (KNECHTEL, 2014). Para isso, foi acessado o sistema pfSense, já utilizado pela instituição, e foi observado em tempo real a movimentação do tamanho da banda de entrada e saída de dados na rede. Os dados analisados foram os pacotes de dados e o tamanho da banda medidos em unidades de bits e megabits por segundo. Analisando o tráfego na rede e comparando a quantidade de pacotes de rede consumidos, verificando anomalias como picos elevados de pacotes atingidos durante um tempo, podendo causar lentidão na rede, porém esse monitoramento é feito de uma maneira menos abrangente pelo pfSense, não especificando e detalhando muito a conexão do ambiente de rede gerenciado.

Por fim, é feita uma sugestão de implantação do sistema de monitoramento Nagios, caracterizando uma proposta de intervenção. Esta proposta tem por base a especificação das oportunidades e das possíveis melhorias identificadas diante do diagnóstico da rede, os pontos que demonstram sua viabilidade, sua implantação e a análise dos resultados com a sua aplicação, remetendo a uma metodologia experimental definida por Shull e Travassos (2001).

Desta forma, este trabalho foi desenvolvido para coletar dados de forma a avaliar o grau de uso da rede local pelos setores da unidade da instituição estudada.

4. Resultados

A coleta de dados foi realizada pelo setor de T.I., obtendo as informações que chegam de todos os dispositivos conectados à rede, passados através do *switch* principal.

Primeiramente foi feita análise sobre a interface do *software* pfSense, verificando o gráfico de tráfego durante um período de 1 semana de segunda-feira a sexta-feira, analisando 6 horas de maneira alternada, monitorando em horário de expediente que consiste das 08:00 horas até 17:00 horas, observando de modo limitado ao programa expondo de modo automático os IPs de host que estão consumindo certa quantidade de banda de rede.

Na Figura 2 é demonstrado o tráfego na rede LAN por algumas máquinas no sistema pfSense. No topo da imagem está um filtro de informações do gráfico, sendo possível indicar o tipo de gráfico da rede – LAN ou WAN – ordenando por tamanho da banda de entrada ou saída, filtrando por rede local ou remota, no filtro tela pode- se escolher nome da máquina, endereço IP do *host*. Logo abaixo, observa-se a quantidade de banda de entrada e saída – bandwidth in e out - utilizada por determinados hosts. Ao lado esquerdo da imagem, está localizado o gráfico referente ao tráfego da rede no período das 11:00 horas até às 13:00 horas, sendo que em azul estão os dados correspondentes ao tamanho da entrada de dados passando pela rede de computadores, e em laranja estão os dados correspondentes ao fluxo de saída de dados. Dispostas ao lado direito, estão as informações dos IPs das máquinas e o consumo de banda da rede em bits por segundo.

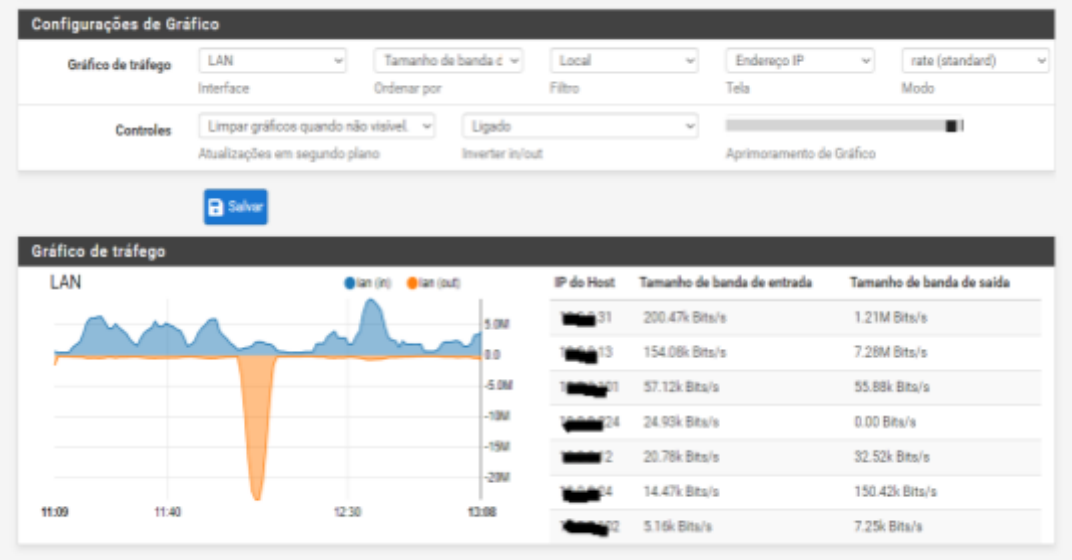

Figura 2 – Gráfico de Tráfego gerado pelo pfSense

Através do gráfico pode-se perceber que houve um grande uso da rede entre 11:40 horas e 12:30 horas em que determinados hosts utilizaram mais da rede no tráfego de saída de dados em 7.28 e 1.21 *Megabits* por segundo, sendo que comumente se percebe dados entre 10 kbits e 300 kbits quando analisada em suas condições normais. Sem mais opções para detalhamento nessa interface para analisar rede interna de computador percebe-se que o sistema tal acaba tendo desvantagens em relação a outros sistemas, como o Nagios XI.

4.1 Sugestão de aplicação – Nagios XI

O Nagios XI é apresentado como uma alternativa que visa um melhor monitoramento da rede de maneira mais simplificada visando identificar acessos desconhecidos e/ou com uso incomum da rede, pois oferece um maior detalhamento de maneira simples sobre a situação da rede, permitindo identificar no *dashboard* da interface do equipamento a ser monitorado.

Na Figura 3 é demonstrada a interface de monitoramento do *switch* de modo geral.

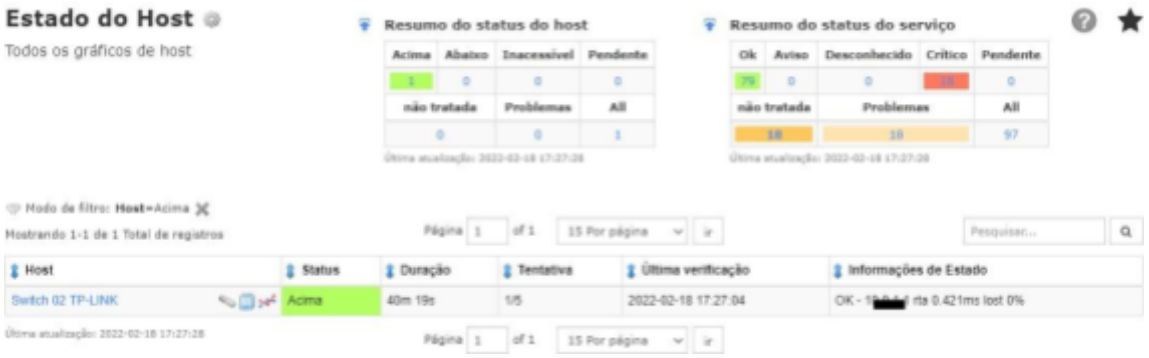

Figura 3 – Nagios interface *switch*

A interface permite identificar o status do serviço, duração e as tentativas de conexão caso tenha ou haja queda de sinal, além de permitir a visualização de um resumo de status do serviço que informa o número de serviços monitorados e avisos de alerta caso haja um problema com alguma porta do *switch*. Então, nessa interface, temos o resumo do status do host, permitindo a visão de "Acima" de quantos *hosts* estão funcionando corretamente, "Abaixo" são hosts que apresentam algum problema e não estão

funcionando ou funcionam com alguma restrição, "Inacessível" *hosts* que o sinal não consegue alcançá-los na rede e "Pendente" hosts com alerta de algum ajuste a ser feito, quanto ao resumo do status do serviço, relaciona os serviços dos hosts monitorados.

No caso, nota-se 97 serviços ao todo, onde 79 serviços estão sendo executados de forma normal, 0 (zero) serviços estão sobre "Aviso" ou alerta de limitação de uso e 18 estão em estado "Crítico", ou seja, não estão com conexão e o serviço não está sendo executado. Na parte inferior da interface encontra-se o host monitorado informando o status – Acima ou Abaixo -, a "Duração" que é o tempo que o dispositivo está sendo monitorado, as "Tentativas" de reconectar ao módulo, caso o sinal seja perdido e informações de estado em geral do *host*.

Na Figura 4 é possível observar a situação das portas físicas e lógicas do *switch* e o gráfico de tráfego de rede de uma porta específica.

Serviço	Status	Duração	Tentativa	Última verificação	Informações de Estado
Porta9 Status	Critical	34m 19s	5/5	2022-02-18 17:25:55	CRITICAL: Interface port 9: Gigabit Copper (index 9) is down.
Porta9 Bandwidth	Ok	38m 18s	1/5	2022-02-18 17:26:56	OK - Current BW in: 0Mbps Out: 0Mbps
Porta8 Status	Ok	38m 24s	1/5	2022-02-18 17:26:50	OK: Interface port 8: Gigabit Copper (index 8) is up.
Porta8 Bandwidth	Ok	38m 30s	1/5	2022-02-18 17:26:44	OK - Current BW in: 0Mbps Out: 0Mbps
Porta7 Status	Critical	34m 40s	5/5	2022-02-18 17:25:34	CRITICAL: Interface port 7: Gigabit Copper (index 7) is down.
Porta7 Bandwidth	Ok	38m 39s	1/5	2022-02-18 17:26:35	OK - Current BW in: 0Mbps Out: 0Mbps
Porta6 Status	Ok	38m 45s	1/5	2022-02-18 17:26:29	OK: Interface port 6: Gigabit Copper (index 6) is up.
Porta6 Bandwidth	Ok	38m 52s	1/5	2022-02-18 17:26:22	OK - Current BW in: 0Mbps Out: 0Mbps
Porta5 Status	Critical	35m 2s	5/5	2022-02-18 17:30:12	CRITICAL: Interface port 5: Gigabit Copper (index 5) is down.
Porta5 Bandwidth	Ok	39m 4s	1/5	2022-02-18 17:26:11	OK - Current BW in: 0Mbps Out: 0Mbps

Figura 4 – Nagios interface porta do *host*

Na Figura 4, notam-se todas as portas monitoradas no equipamento *Switch* 02 TP-LINK, visualiza-se os serviços, em questão são as portas do *switch*, o estado em que se encontra sendo "Ok" para funcionamento normal e "Critical" que acusa algum erro ou problema que é descrito em "Informações de Estado", a duração do tempo que está sendo monitorada com as tentativas de reconexão caso haja queda no sinal, com informações de estado de maneira a informar o tipo de conexão da porta, o *status* e a banda de rede consumida.

Na parte de serviço desta interface, existe a chamada para outra interface que demonstra um gráfico de rede de uma porta específica, indicando o fluxo de dados do tamanho de banda de rede de computadores sendo consumida pelo *host* da porta determinada.

Figura 5 – Nagios interface gráfica de porta específica

Na Figura 5 é permitido visualizar um gráfico de tráfego da porta 4 do *switch*, demonstrando a quantidade de banda usada no momento da análise, informando a entrada e saída em Mbits por segundo em média no eixo x e o horário no eixo y.

4.2 Fases de Implantação

A implantação do *software* Nagios XI em um sistema GNU/LINUX foi realizada com o mínimo de configurações feitas no SO. Instalação rápida foi feita a partir de um comando no terminal de console do sistema:

root#: curl https://assets.nagios.com/downloads/nagiosxi/install.sh | sh

Também podendo ser feita de modo manual:

root#: cd /tmp

root#: wget https://assets.nagios.com/downloads/nagiosxi/xi-latest.tar.gz root#: tar xzf xi-latest.tar.gz

root#: cd nagiosxi root#: ./fullinstall

Após a instalação, é disponibilizado o endereço para acessar a interface web do Nagios, onde é feita uma configuração básica do serviço, definindo a URL, idioma do sistema, timezone, o tipo de licença da versão e usuário e senha para administrador. Feita instalação e pré configuração da aplicação, pode-se acessar o serviço. A interface principal apresenta a situação dos serviços e hosts geridos e as ferramentas de gestão, disponibilizando as configurações para adicionar o serviço e/ou equipamento a ser monitorado.

Na Figura 6 é apontada a interface principal da aplicação que informa de maneira resumida a quantidade e situação dos hosts e serviços monitorados.

Figura 6 – Interface principal do *software* Nagios

É demonstrada na interface um resumo geral de todos os hosts "observados", permitindo a identificação de estado do host e dos serviços, no caso existe 1 host operando normalmente e 97 serviços dos quais 79 estão em condições normais e 18 estão em estado crítico podendo ser perda de sinal lógico até rompido físico de cabo.

5. Conclusão

Esse trabalho levantou o uso de tráfego da rede local para uma unidade da Universidade Estadual do Norte do Paraná, a fim de propor a utilização de um programa como alternativa de monitoramento da rede interna, a partir da análise do estado e do fluxo da rede de computadores internamente.

Para se atingir uma compreensão da rede de computadores interna, primeiro foi diagnosticado a rede atual através informações de conexões, depois identificadas falhas por meio dos dados obtidos, e propospo a utilização do *software* de gestão e monitoramento de rede Nagios XI para facilitar a gestão da rede com maior detalhamento de informações.

Com isso, a hipótese do trabalho de que o uso de um *software* de monitoramento alternativo para avaliar o fluxo da rede de computadores se confirmou, por oferecer e prover um maior detalhamento de informações sobre conexões do equipamento que foi estudado na rede, possibilitando a identificação de anomalias no uso da banda de rede.

Sendo assim, ambos permitem uma visão do tráfego de rede, porém o uso do Nagios XI permite o monitoramento do tráfego da rede de forma mais simples e detalhada, identificando de maneira mais precisa anomalias e possíveis erros críticos.

Em pesquisas futuras, pode-se estudar a integração entre o *software* pfSense com o Nagios XI através de bibliotecas de compartilhamento e integração de informações entre esses programas usando SSH.

Referências

4LINUX. O que é pfSense. Site 4LINUX. 2022. Disponível em: https://4linux.com.br/o-que-e-pfsense/. Acesso em: 20 fev. 2023.

GIL, Antônio Carlos. Como Elaborar Projetos de Pesquisa. 4. ed. São Paulo: Atlas, 2002.

JULIO, C. Monitoramento de rede: importância, vantagens e melhores ferramentas. Site Backup Garantido. 2020. Disponível em: https://backupgarantido.com.br/blog/monitoramento-de-rede/. Acesso

em: 21 nov. 2021.

KNECHTEL, Maria do Rosário. Metodologia da pesquisa em educação: uma abordagem teórico-prática dialogada. Curitiba: Intersaberes, 2014.

NAGIOS. Linux Monitoring With Nagios. Site NAGIOS. 2022. Disponível em: https://www.nagios.com/solutions/linux-monitoring/. Acesso em: 12 jan. 2022.

NEGUS, C. Linux A Bíblia. Tradução 8 Ed. ALTA BOOKS Editora. Rio de Janeiro, 2014.

PFSENSE. Open Source Security. 2022. pfSense. Disponível em: https://www.pfsense.org/. Acesso em 10 fev. 2022.

RIBEIRO, T. C. S. C. Fundamentos de rede de computadores. Londrina. Editora e Distribuidora Educacional S. A. 2016.

SHULL, F.; CARVER, J; TRAVASSOS, G. H. *An Empirical methodology for introducing software processes. In: VIII European Software Engineering Conference Held Jointly and XI International Symposium on Foundations of Software Engineering(ACM SIGSOFT)*. New York, USA: ACM, 2001. P. 288-296. Citado nas páginas 25, 64, 87 e 95.

SILVA, D. F. O que é pfSense. 20219. pfSense. Disponível em: http://www.danilosilva.net/2019/09/23/o-que-e-pfsense/. Acesso em 08 mar. 2022.

TANENBAUM, Andrew. S. Rede de computadores. 5ª Edição. 2011.

TANENBAUM, Andrew S. Organização estruturada de computadores. 5. ed. São Paulo: Pearson-Prentice Hall, 2007.

UBUNTU. The Story of Ubuntu. 2022. Siet Ubuntu. Disponíve em: https://ubuntu.com/about/. Acesso em 07 mar. 2022.