Revista Científica UNAR (ISSN 1982-4920), Araras (SP), v.23, n.1, p.133-152, 2023.
DOI: 10.18762/1982-4920.20230009

MONITORAMENTO E GERENCIAMENTO DE REDE DE COMPUTADORES USANDO AS FERRAMENTAS: NEXT FIREWALL UNTANGLE, LIBRENMS

Danifer Odair Luciano, Prof. Orientador Felipe Cavenaghi

RESUMO

O intuito deste artigo consiste em demonstrar de forma acadêmica, porém prática sobre o gerenciamento e o monitoramento de uma rede de computadores utilizando 02 ferramentas existentes no mercado atual. Assim sendo este estudo demonstra conceitos teóricos juntamente com ilustrações das aplicações práticas simuladas em ambientes de estudos, demostrando a eficácia de duas ferramentas como o Untangle Next Generation Firewall, LibreNMS, utilizando os mesmo para gerenciar, monitorar e mitigar possíveis invasões a rede. É notório que com o crescimento das redes de computadores é necessário ter um maior conhecimento nesta área, para saber como proceder na precisão de uma solução robusta e assertiva num cenário de invasão ou até mesmo em uma instabilidade da rede. Este artigo através das percepções do autor como um usuário das 02 ferramentas, traz também informações de cada ferramentas, suas aplicações, como usar o modo “demo e gratuito” para testar as ferramentas antes de instalá-las e demonstrar através de ilustrações suas usabilidade e facilidades de interpretações de seus *dashboards*, gráficos, mensagens de aviso ou advertências de possíveis intrusões, controle de bandas, bloqueios por firewall, entre outras funcionalidades que cada uma das ferramentas irão apresentar. Desta forma o objetivo principal deste artigo está em despertar nos gestores de rede que a busca por ferramentas pode auxiliar em um gerenciamento e no monitoramento eficaz no dia a dia dos profissionais da Tecnologia da Informação (T.I) e também dos usuários da rede de computadores.

Palavras-chave: Gerenciamento; Monitoramento; Mitigar; Otimização de recursos;

Abstract

The purpose of this article is to provide an academic yet practical demonstration of the management and monitoring of a computer network using two tools currently

available in the market. Thus, this study presents theoretical concepts alongside illustrations of practical applications simulated in study environments, demonstrating the effectiveness of two tools—Untangle Next Generation Firewall and LibreNMS—used for managing, monitoring, and mitigating potential network intrusions. It is evident that, with the growth of computer networks, a deeper knowledge in this area is essential in order to know how to proceed in implementing a robust and effective solution in the event of a breach or even network instability. This article, through the author's experience as a user of both tools, also provides information about each tool, their applications, and how to use the "demo and free" mode to test the tools before installation. It also demonstrates, through illustrations, their usability and ease of interpreting dashboards, graphs, alert messages or warnings of potential intrusions, bandwidth control, firewall blocks, among other features offered by each tool. Thus, the primary objective of this article is to raise awareness among network administrators that the search for such tools can assist in effective management and monitoring in the daily operations of Information Technology (IT) professionals and network users alike.

Keywords: Management; Monitoring; Mitigation; Resource Optimization.

1. INTRODUÇÃO

Atualmente, a segurança dos dados vem sendo tratada de forma mais complexa, e por isso inúmeras empresas do mundo inteiro se dedicam a desenvolver ferramentas que auxiliam no monitoramento e no gerenciamento das redes de computadores, porém este conceito de "rede de computadores" não pode ser considerado apenas, sendo vários computadores conectados a um equipamento que faça a distribuição de internet, uma rede vai muito mais além disso sendo um conjunto de sistemas de computadores e equipamentos conectados todos entre si utilizando um sistema de gerenciamento para esta comunicação, no qual permite que seja feita a troca de dados entre todos os dispositivos nela conectada, seja por um hardware ou um software, por tanto é preciso ter ferramentas eficientes que façam com que essas transações de dados sejam seguras como um antivírus, firewall e também um gerenciador de rede.

Umas das maiores preocupações da sociedade nos dias de hoje, é a proteção dos Ativos (Dados) sem que pessoas má intencionadas conhecidas como ***"hacker" ou "cracker"*** possam tentar invadir a segurança da rede, para descobrir senhas de acesso ou códigos fontes de programas, com fins criminosos ou que haja a divulgação ou repasse não autorizado desses Ativos entre as empresas.

Segundo Ferreira (2021) “Os termos "*hacker*" e *"cracker",* basicamente, servem para designar indivíduos que possuem habilidades com computadores, porém com finalidades diferentes. Enquanto os hackers elaboram e alteram hardwares e softwares de computadores sem causar prejuízos, os *crackers* utilizam seus conhecimentos para praticar o *cracking*, ou seja, quebrar um sistema de segurança.”.

Ter um antivírus nos equipamentos é algo primordial para que haja a proteção dos dados, segundo Skoudis e Liston (2006, apud TANENBAUM, WETHERALL, 2013, p.552), “A melhor maneira de parar um hacker é pensar como um, como os hackers veem uma rede e argumenta que a segurança deve ser uma função do projeto da rede inteira, e não uma reflexão posterior, baseada em uma tecnologia específica. Eles abordam um usuário com a ‘engenharia social’ que tiram proveito desses usuários incautos, que nem sempre estão familiarizados com medidas de segurança do computador.”.

As empresas de todos os ramos da economia mundial estão preocupando-se em fazer a proteção de seus dados mais sensíveis como dados de funcionários, transações bancárias, lista de clientes, fórmulas industriais, centrais de bancos de dados, entre muitos outros dados, que se por ventura for adquirido por um cracker, este poderá criptografar esses dados para depois chantageá-la para obter a recuperação dos dados novamente, para não vender essas informações para empresas concorrentes, ou também para não fazer a divulgação desses dados em sites ou plataformas especializados de hacker como exemplo a *DeapWeb*, sendo assim as empresas estão sempre procurando inovações no mercado técnologico para fazer a prevenção de perdas de dados, assim sendo, de acordo com Stallings (2020) :

> A prevenção de perda de dados (DLP) é uma tecnologia madura implantada por muitas empresas para dar suporte aos requisitos de segurança da informação. As principais características do DLP também o tornam uma poderosa tecnologia de aprimoramento da privacidade que pode atender a uma ampla gama de requisitos de privacidade de informações. Em essência, DLP é um conjunto de tecnologias integradas que detectam dados sensíveis e impedem o uso não autorizado, liberação ou entrega a destinos ou destinatários específicos, bem como seu armazenamento em locais proibidos. O DLP trabalha em tempo real para identificar informações de identificação

> pessoal e reagir a riscos de privacidade com base no conteúdo dos dados e no contexto dinâmico do ambiente de informações. Assim, o DLP fornece aplicação técnica de termos e condições, ou políticas em geral, para evitar vazamentos de privacidade.

No mercado existem várias ferramentas disponíveis para fazer o gerenciamento e monitoramento da rede e muitas destas ferramentas são capazes de fazer uma análise diária (em tempo real) do comportamento dos equipamentos conectados nos quais trazem diagnósticos sobre a segurança do sistema e auxiliam os gestores em tomadas de decisões sobre medidas de segurança a serem tomadas.

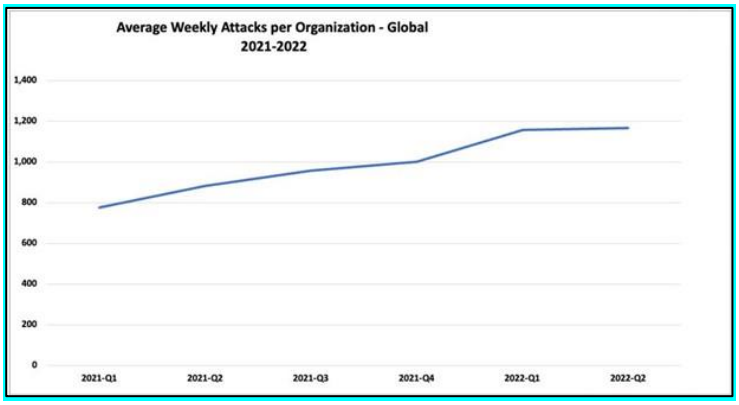
Contudo, o objetivo deste artigo é trazer alguns conceitos que poderão auxiliar os gestores de redes na escolha dessas 02 ferramentas para adotarem em seus ambientes de trabalho.

2. REFERENCIAL TEÓRICO

2.1 Ataques cibernéticos no Brasil

Segundo dados contidos no site da empresa Crypto Id (2022), uma pesquisa feita pelo grupo Check Point Research (CPR), uma divisão de Inteligência em Ameaças da Check Point® Software Technologies Ltd., e uma das fornecedoras líderes de soluções de cibersegurança global, até o segundo trimestre de 2022 houve cerca de 1.540 ataques as organizações brasileiras, um aumento de 46% em ataques cibernéticos semanais tendo um pico histórico. Os ataques cibernéticos globais aumentaram em 32% comparado ao segundo trimestre de 2021, tendo uma média de 1.200 ataques semanais, a Figura 1 demonstra essa evolução de ataques de forma global e, portanto, podemos dizer que as empresas ainda estão muito vulneráveis e suscetíveis a ataques cibernéticos de todos os tipos.

Figura 1 – Média semanal de ataques cibernéticos pelas Organização - Global



Fonte:<https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/ataques-ciberneticos-no-brasil-aumentaram-46-no-segundo-trimestre-de-2022/ >

A vulnerabilidade está presente em todos os setores da economia, porém o setor de Atacados e Varejo lideram um ranking de ataques sofridos no ano de 2022, com um aumento de 182% comparado com o mesmo período do ano de 2021, mas essa vulnerabilidade se espalha por todos os setores onde alguns tem mais défit de segurança que os outros e assim estão sendo mais afetadas por ataques semanais de ransomware de todos os tipos. A Figura 2 demonstra uma tabela feita pelos pesquisadores do site Crypto Id (2022), onde é possível ver quais os setores mais atingidos por invasões do tipo ransomware.

Figura 2 – Tabela sobre o aumento de ataques ransomware por setores econômicos em 2022.

Setor	Organizações impactadas semanalmente	Mudança Ano a Ano
Governo/Militar	1 cada 24	+135%
Educação/Pesquisa	1 cada 30	+83%
Saúde	1 cada 31	+47%
ISP/MSP	1 cada 37	+9%
Finanças/Bancos	1 cada 41	+42%
Comunicação	1 cada 46	+59%
SI/VAR/Distribuidores	1 cada 47	+143%
Manufatura	1 cada 48	+60%
Varejo/Atacado	1 cada 53	+182%
Utilities	1 cada 59	+11%
Transporte	1 cada 70	+28%
Fornecedor Software	1 cada 74	-34%
Lazer/Turismo	1 cada 77	+24%
Fornecedor Hardware	1 cada 78	+48%
Seguro/Jurídico	1 cada 81	+1%
Consultoria	1 cada 87	-17%

Fonte:<https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/ataques-ciberneticos-no-brasil-aumentaram-46-no-segundo-trimestre-de-2022/ >

Baseado em dados apresentados na pesquisa acima, é preciso ter meios de proteger as informações que são trafegadas na rede e uma das opções disponíveis no mercado com alguma ferramenta capaz de trazer mais segurança e de proteger a

rede contra contaminação de vírus, *spyware*, *malwares* entre outras pragas que possam ser instaladas através de anexos de e-mail ou softwares de terceiros.

Para elucidação deste artigo iremos tratar de alguns tópicos relevantes que serão a base para entendimento do leitor sobre a abordagem do tema.

- Modelos de gerenciamento;
- Gerenciamento da rede com Untangle NG Firewall;
- Monitorando a rede com LibreNMS;

2.2 Modelos de Gerenciamento

A ISO 27033-33 é voltada especificamente para segurança da informação relacionada a redes de computadores, e assim sendo traz um modelo a gestão e quais os meios para se ter um rede segura. Conforme descrito por Lima (2021, p. 8 e 10) do livro Introdução ao Gerenciamento de Redes esta ISO criou um modelo de gerenciamento dividido em 5 (cinco) partes, sendo:

- **Gerenciamento de falhas (Fault):** o objetivo desse gerenciamento é registrar, detectar e notificar os administradores sobre os problemas que há na rede para assim fazer tomadas de decisões para sanar a falha;
- **Gerenciamento de configuração (Configuration):** Faz uma varredura na rede e assim o administrador da rede saberá quais são os hosts (equipamentos) compõe a rede e todas as suas configurações seja de forma física (hardwares) ou lógica (softwares);
- **Gerenciamento de contabilização (Account):** esse tipo de gerenciamento serve para garantir que os recursos da rede estão sendo utilizados de forma correta e assim especificar, notificar e gerenciar o acesso de usuários e dispositivos aos recursos da rede, como quotas de impressão, uso de banda, quantidade de megas para downloads entre outros tipos de controles;
- **Gerenciamento de desempenho (Performance):** serve para quantificar, controlar e notificar sobre o desempenho de diferentes componentes de rede;
- **Gerenciamento de segurança (Security):** auxilia na detecção antecipada de um evento que possa causar uma ocorrência na rede;

De acordo com Toquica (2021), apud (Saydam, 1996, p.345-348)

> Gerenciamento de rede inclui a implementação, 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 a um custo razoável.

Não adianta ter uma rede bem estruturada e que seja funcional de forma operacional na infraestrutura, se os serviços que rodam nela ou os dados que são trafegados não estão seguros ou disponíveis quando necessário.

2.3 Gerenciamento da rede com Untangle NG Firewall

Seguindo as diretrizes da ISO 27033-33, para este estudo foi utilizada a ferramenta de gerenciamento Untangle Next Generation Firewall para efetuar esses gerenciamentos da rede, pois segundo informações da contido no site da empresa FC Brasil (segundo semestre de 2022), responsável pelo fornecimento e distribuição desta ferramenta no Brasil, o Untangle Next Generation Firewall traz uma segurança completa de forma simples porém flexível para diversos tipos de empresas (desde de pequenos escritórios a empresas de grande portes, escolas com vários campus). Esta ferramenta é capaz de fazer uma varredura em toda rede em tempo real e por isso é capaz de proteger toda a rede contra intrusões não autorizadas, possui um Filtro Web que auxilia no controle de navegação na web, também possui um poderoso sistema de bloqueio contra ataques por vírus no qual é atualizado constantemente de forma online, e conta com um bloqueador de Spam para que não haja um ataque por Denial of Service (DoS) ou Distributed Denial of Service (DDoS), e essa ferramenta é capaz de fazer um Balanceamento de Carga na rede, e o que facilita sua usabilidade aos usuários é a sua interface fácil de ser compreendida no qual possibilita configurar e gerenciar as políticas e direcionar as soluções de forma rápida.

2.4 Monitorando a rede com LibreNMS

Neste artigo será tratado sobre a utilização do software LibreNMS que é uma ferramenta para fazer o monitoramento da rede, pois essa ferramenta apresenta inúmeras vantagens que auxiliam aos administradores da rede a terem tomadas de decisões mais assertivas referente ao seu trabalho de análise.

Segundo o site oficial do fabricante Librenms.org (2022) o LibreNMS é uma ferramenta muito utilizada no mercado empresarial devido ser um sistema de monitoramento de rede completo que oferece muitos recursos e suportes aos usuários, como monitoramento de largura de banda, tempo de utilização da CPU espaço de armazenamento em disco local (se está crítico ou não), uso da memória. Este sistema traz inúmeras vantagens aos seus usuários, pois se houver uma possível falhas na rede o que se denomina de reação a incidentes a ferramenta irá tentar restabelecer o serviço automaticamente executando rotinas automáticas para restauração, porém se o serviço não for restabelecido o LibreNMS irá emitir alertas de formas programadas por SMS ou e-mails, mensagens instantâneas aos administradores da rede para que fiquem cientes e tomem as atitudes cabíveis para resolução.

Esta ferramenta também auxilia os administradores da rede a analisar quais são os recursos computacionais que estão tendo gargalhos ou sobrecargas, e também poderá auxiliar aos gestores gerando gráficos e relatórios para descobrir quais são os setores que mais tem chances de ter uma contaminação por *Phishing* no qual é uma forma que um criminoso usa para enganar um indivíduo para obter determinadas informações confidenciais, ou então qual setor tem mais chances de sofre um ataque por *DDoS* onde um hacker ou cracker invade um computador e através deste, invade outros computadores tornando-os escravos e assim faz com que esses computadores escravos acessem um determinado serviço ou recurso em um servidor simultaneamente para que possam sobrecarregá-lo e travar suas aplicações.

2.5 Motivos para monitorar a rede de computadores

Com o atual cenário mundial, a proteção dos Dados é algo de extrema necessidade, sendo que em diversos países foram instituídas leis que regularizam o uso e o tratamentos que são dados aos Dados. Conforme relatado no portal oficial do governo brasileiro o Gov.br, no Brasil entrou em vigor em 14 de agosto de 2020 a

Lei nº 13.709/2018 chamada Lei Geral de Proteção de Dados Pessoais, esta lei impõe limites para coletas e o seu devido tratamento referente a dados/informações pessoais, e o descumprimento desta lei é passível a advertência ou multas severas que podem chegar no valor de até R$ 50 milhões de reais, sendo assim as empresas ou instituições, estão procurando de todas as formas se proteger contra invasões, para não sofrerem sanções legais por perdas ou vazamento de dados, e para garantir sua segurança estão contratando especialistas da área e investindo com infraestruturas para terem uma rede de comunicação segura.

Muitas empresas veem sofrendo ataques no mundo todo, e aqui no Brasil podemos citar os casos como do Hospital Albert Einstein:

- Em novembro de 2020, o Hospital Albert Einstein foi alertado pelo Procon-SP para explicar o vazamento de uma lista que permitia o acesso aos prontuários pessoais e médicos de pacientes testados, diagnosticados e internados para covid-19 e expostos na internet por um mês de informações. O vazamento ocorreu depois que um cientista de dados do Hospital Albert Einstein de St. Paul postou uma lista de nomes de usuários e senhas em um fórum que permitia o acesso aos dados de assuntos de teste. O hospital obteve a informação graças a um projeto com o ministério. Após a denúncia, a unidade informou que a chave de acesso havia sido alterada, e o hospital abriu um processo para investigar o caso.

De acordo com artigo de Berardi et al. (2023) ataques de Ransoware é uma ameaça cibernética mais predominante na infraestrutura digital, onde os invasores usam diversas técnicas para obter os dados ou recursos dos usuários para depois exigir resgate de forma física (dinheiro) ou virtual (criptomoeda no qual é um método de pagamento não rastreável).

Para manter hábitos comportamentais nos indivíduos da empresa é necessário criar normas e regras que irão ditar suas condutas, sendo assim conforme determina a **ISO 27001 anexo A** é preciso criar um documento de Políticas de Segurança da Informação também conhecido como PSI, nesse documento deverá ter um conjunto de diretrizes obrigatórias para proteger os dados e informações e devem ser adotadas por todos usuários da empresa para garantir a confidencialidade, integridade e disponibilidade da informação. Com a implantação de uma PSI e com

o gerenciamento de rede dentro de uma empresa, provavelmente haverá algumas mudanças em relação as atitudes comportamentais dos usuários da rede, e assim sendo os gestores sempre terão que se questionar, sobre: “Como atuar de uma forma ativa em busca de uma solução para proteger a rede? Como evitar que a rede fique indisponível por fadiga ou desgaste de hardware? Quais são as ferramentas necessárias para isso?

3. ANALISE E DISCUSSÃO DOS RESULTADOS

3.1 Metodologia

A fim de atingir os objetivos delineados para o trabalho, foi necessário fazer um levantamento bibliográfico para a base conceitual para o cenário proposto. O levantamento bibliográfico contou com a pesquisa em livros, revistas especializadas, e pesquisas na Internet.

Respondendo as questões iniciais proposta na problemática, esse documento irá demonstrar através de um estudo de caso com as aplicações funcionando em um ambiente criado para testes. Foram implementadas possíveis soluções para que seja feita um monitoramento em rede de forma sucinta e objetiva, utilizando as ferramentas citadas (Next Firewall Untangle e LibreNMS) como apoio para este estudo.

3.2 Análise e resultado

Para elaboração deste artigo, foi desenvolvido um cenário de rede para a instalação das ferramentas sugeridas, sendo assim nos próximos tópicos serão tratadas as percepções do autor como um usuário do sistema.

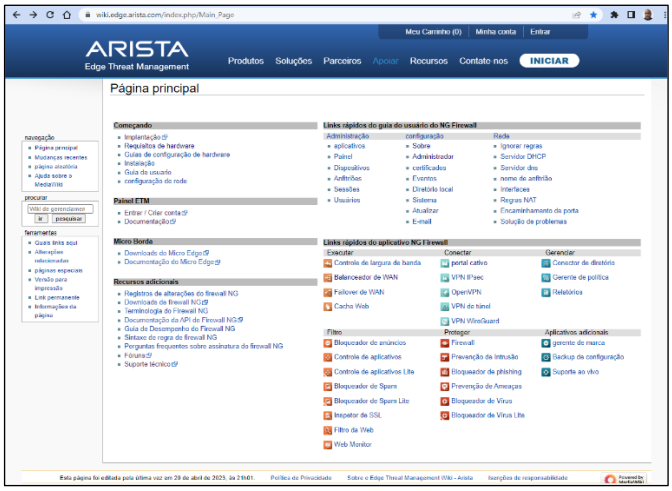
3.2.1 Untangle Next Generation Firewall.

Atualmente existem tantas opções de ferramentas de proteção com firewall a ser considerar no mercado como o Zenarmor (Sensei), Cisco Secure Firewall, Sophos Firewall, Ponto de verificação quântica, Fornalha, Barracuda CloudGen Firewall, Série SonicWall NSA, Parede lisa, Software PFSense, entre muitos outros, o

Untangle Next Generation Firewall se destaca por sua facilidade de utilização e por também ser uma plataforma semelhante a uma loja de aplicativos onde seus usuários podem escolher quais aplicativos ou módulos irão utilizar em seu computador Servidor, Desktop, ou até mesmo no Smartphone.

O site Arista Edge Threat Management é uma Wikipédia desenvolvida por funcionários da empresa Arista Edge Threat Management no qual é umas das empresas responsáveis pela distribuição da ferramenta pelo mundo, e traz vários tópicos que irão auxiliar o usuário a administrar a ferramenta, tendo nele uma vasta documentação que servirá para consulta de instalação até como utilizar a ferramenta por completo.

Figura 3 – Site da Arista Edge Threat Management



Fonte: < https://edge.arista.com/ng-firewall/>

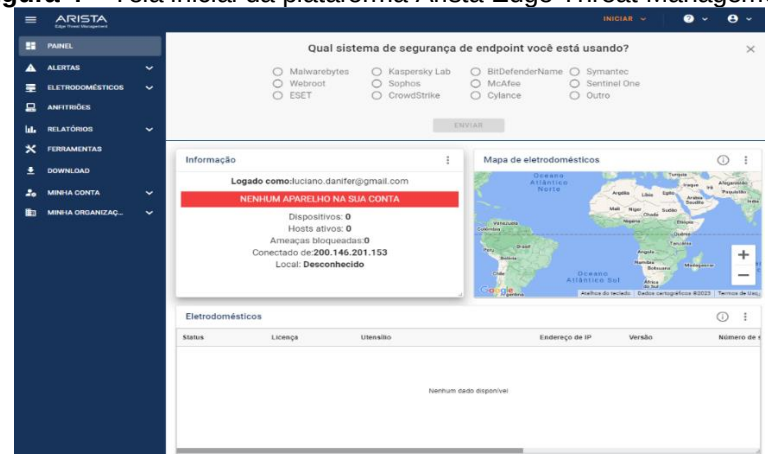
A instalação do Untangle NG Firewall é baseada em software, isso significa que pode ser instalado em qualquer desktop ou servidor que se encaixe no projeto. No site do fornecedor Arista Edge Threat Management é possível se cadastrar e testar a ferramenta por 14 dias de forma gratuita, basta ter um e-mail ativo e seguir os passos solicitados.

Quando clicar na opção “COMECE COM UM TESTE GRATUITO”, o usuário será redirecionado para uma página onde deverá preencher alguns dados como o

seu e-mail, instituição, nome completo, área de atuação, e logo após será lhe encaminhado um e-mail confirmando seu cadastro.

Após se cadastrar com um e-mail e uma senha, o usuário terá acesso a algumas das ferramentas do sistema, porém será necessário fazer a configuração de cada funcionalidade no qual irá utilizar.

Figura 4 – Tela inicial da plataforma Arista Edge Threat Management



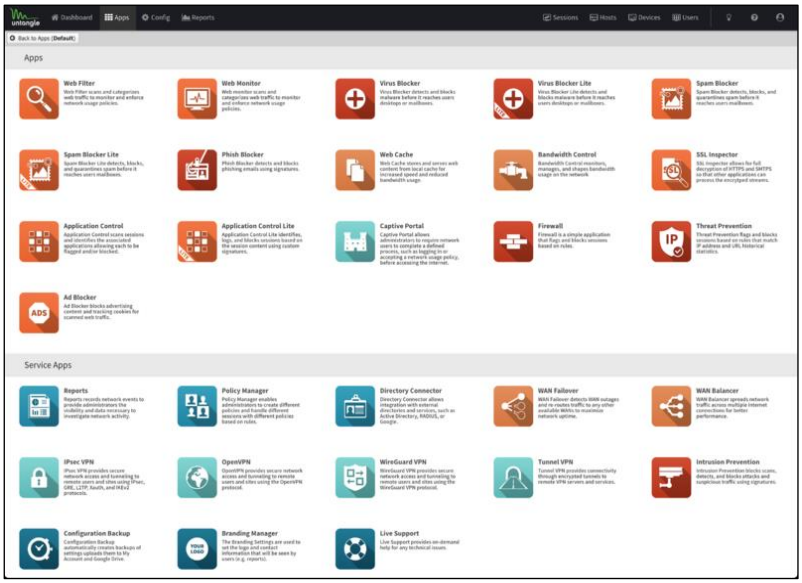
Fonte: < https://edge.arista.com/ng-firewall/>

Quando estiver tudo configurado será possível fazer algumas análises na plataforma, e assim como já mencionado anteriormente é possível adicionar as funcionalidades que forem pertinentes ao monitoramento da empresa. Para esse estudo foram instaladas algumas ferramentas do Untangle como exemplo:

- Web Filter,
- Virus Blocker,
- Web Monitor,
- Spam Blocker Lite para Controle de Banda,
- Balanceamento de Carga,
- Ad Blocker,
- Vírus Blocker,
- Web Cache,
- SSL Inspector,
- Captive Portal,
- Conexão remota segura via VPN,
- Além de funções de firewall,
- IDS (Sistemas de Detecção de Intrusão) e IPS (Sistemas de Prevenção de Intrusão);

Devido sua tecnologia Integrated Rules EngineTM, é possível que todos os programas e aplicativos instalados funcionem juntos, mesmo estes aplicativos sendo de funções diferentes, pois esse integrador faz com que todos o sistema se reconheça como por exemplo o aplicativo de filtragem de spam com o de prevenção de infecções por vírus.

Figura 5 – Plataforma de aplicativos do Untangle

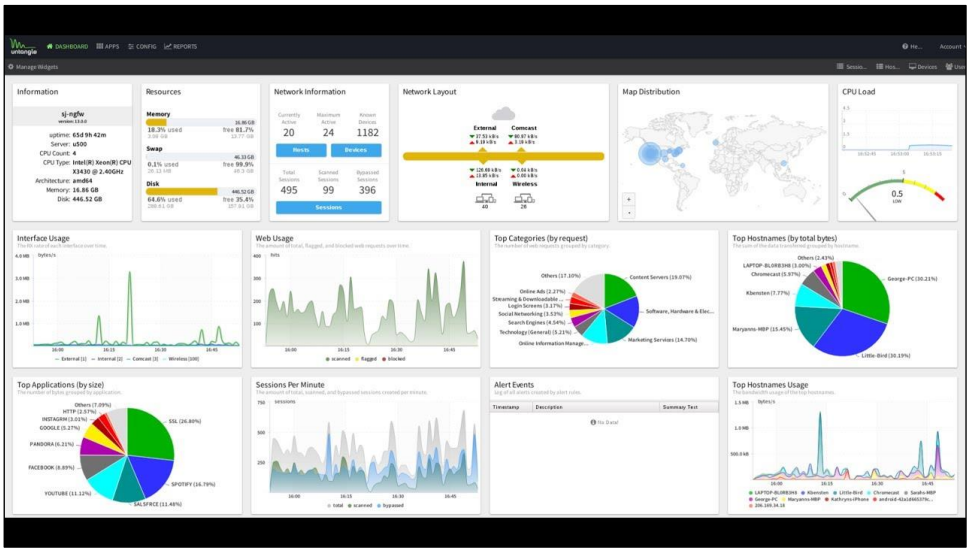


Fonte: < https://edge.arista.com/ng-firewall/ >

Com uma plataforma modular, é possível instalar ou remover os aplicativos de conforme a necessidades da empresa e por isso tem um ótimo papel na economia em valores financeiros, pois o usuário paga somente pelo que está utilizando.

Devido ter uma interface web intuitiva, ele permite que seja configurado as políticas e fazer o gerenciamento das soluções com facilidade. Contudo também é possível visualizar tudo o que está acontecendo na rede utilizando as ferramentas de relatórios de forma detalhada e visualizar vários dashboard diferentes, nos quais possam trazer informações complementares ao gerenciador de rede, sendo assim ao mesmo tempo que está visualizando os recursos (consumo de memória, uso de swap, uso de disco) é possível ver um gráfico de uso de sites navegados pelos usuários ou até mesmo ver qual é o consumo de banda por cada usuário por nome de hostname conforme demonstrado na Figura 9.

Figura 6 – Dashboard criados no Untangle



Fonte: < https://edge.arista.com/ng-firewall/>

A ferramenta Untangle traz inúmeros recursos, porém não serão abordados nesse artigo, mas para estão disponíveis na opção teste online da ferramenta ou para os administradores de rede que decidirem adquirir a ferramenta completa para uso em sua empresa.

Esta poderosa ferramenta de monitoramento Untangle NG Firewall está disponível no mercado e é uma das opções sugeridas para se fazer um monitoramento efetivo na rede.

3.2.2 LibreNMS

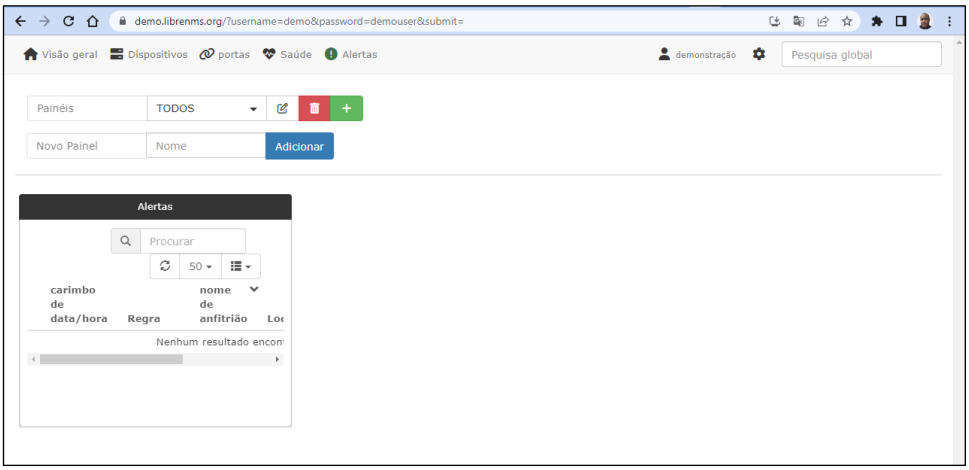
O LibreNMS é um sistema de monitoramento de rede baseado em PHP, MYSQL e protocolo SNMP, e inclui a descoberta automáticas de equipamentos na rede através de varreduras automáticas os protocolos CDP, FDP, LLDP, OSPF, BGP, SNMP e o ARP,e também possui inúmeros recursos e suporte aos dispositivos da rede. Este sistema opera em diversos sistemas operacionais de rede como exemplo FreeBSD, Cisco, e em Linux e suas diversas versões.

No site oficial da empresa LibreNMS (librenms.org/) é possível fazer o teste de demonstração da ferramenta antes de instalá-la e assim o usuário poderá experimentar diversas funcionalidades de forma simplificada, e aprender a criar templates, dashboards e painéis para fazer o monitoramento, e não para fazer esse

teste não é preciso se cadastrar, é só clicar no botão “ABRIR DEMONSTRAÇÃO” na página princial.

Entrar na página de demonstração será preciso configurá-la criando os dashboard e inserindo as informações para que seja feito o monitoramento da rede.

Figura 7 - Pagina do site LibreNMS.org



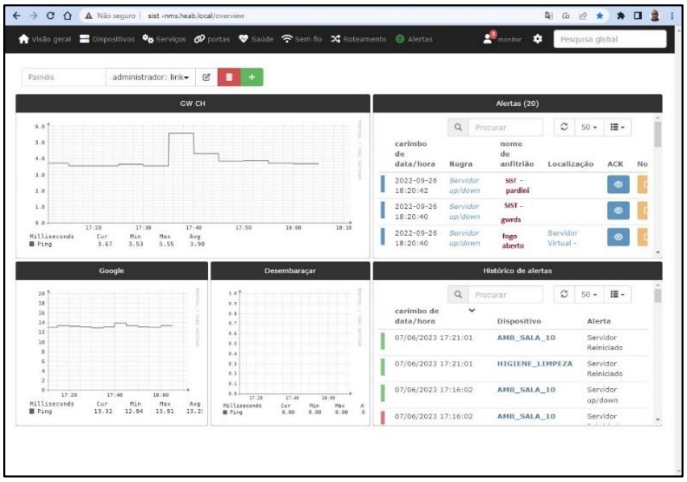
Fonte: < https://demo.librenms.org/?username=demo&password=demouser&submit=>

Apesar de ser instalado no sistema operacional Linux, é possível visualizar suas operações de qualquer máquina da rede, pois sua interface gráfica pode ser visualizada através de qualquer browser.

Para este estudo foi criado uma máquina virtual com o sistema operacional Linux versão Ubuntu-22-04 e feito a instalação da ferramenta com a configuração para que buscasse os dados da rede que foi desenvolvida para este trabalho.

Após a instalação, tem que ser feito a configuração dos painéis onde será visualizado as ações da rede como os links de fornecimento de internet, pode ser feito o monitoramento da banda e tráfego, os servidores físicos e os virtuais, e criar diversos dashboards para monitorar todo o ambiente da rede, através de gráficos, alertas, mapas.

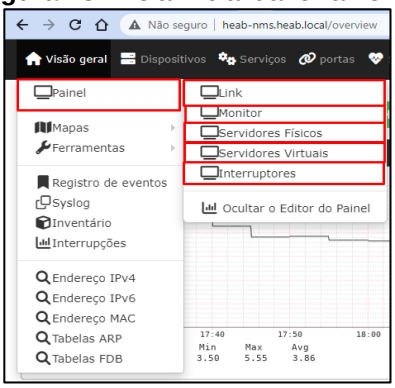
Figura 8 - Tela inicial da ferramenta



Fonte: própria do autor

No LibreNms tem a possibilidade de criar vários painéis com diferentes funcionalidades e personalizá-lo para visualização de um único usuário ou compartilhar com outros usuários:

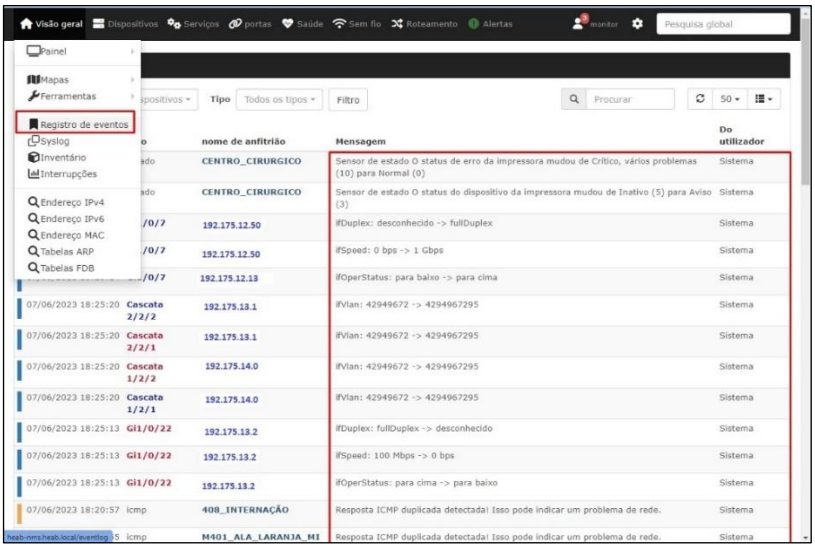
Figura 13 - Tela inicial da ferramenta



Fonte: própria do autor

Com as configurações feitas, é possível verificar os registros de eventos que ocorrem na rede, facilitando ao gerenciador da rede entender oque esta acontecendo na rede e qual foi o tipo de falha ou evento ocorrido.

Figura 9 - Eventos de registro do LibreNMS



Fonte: própria do autor

O gerenciador da rede usando o LibreNMS poderá criar vários controles para monitorar todos os eventos da rede, criando e programando os Widgets é possível verificar as notificações em uma única tela se for preciso, e esses acessos serão feitos de forma online utilizando um browser para ver todas as analises, os gráficos sobre a tráfego na rede, os alertas de eventos, gráficos de uso dos Links de internet, estatísticas sobre uso do CPU, armazenamento e uso da memórias do servidores, entre muitos outros monitoramentos que podem ser programados de acordo com versão do LibreNMS que for instalado.

Figura 10 -Visão panoramica de vários painéis de monitoramento

Fonte: < https://www.serverion.com/pt_br/solucoes/librenms/ >

Com todas ações acima descritas e demonstradas com as figuras, o LibreNMS se torna uma opção assertiva, para quem deseja fazer o monitoramento da rede com uma ferramenta com facilidade e praticidade de configurar e utilizar.

4. CONSIDERAÇÕES FINAIS

O uso das ferramentas LibreNMS e Untangle Next Generation Firewall juntas podem fornecer uma abordagem abrangente para a segurança de rede e proteção contra ameaças cibernéticas.

Enquanto Untangle Next Generation Firewall é uma solução de firewall abrangente que oferece recursos avançados de segurança de rede. Ele protege sua rede contra ameaças externas, como ataques de hackers, malware e intrusões indesejadas.

Por outro lado, complementando com o LibreNMS no qual é uma plataforma de monitoramento de rede de código aberto que permite monitorar e gerenciar dispositivos de rede, como roteadores, switches e servidores. Ele oferece recursos abrangentes de monitoramento, incluindo o monitoramento de desempenho, disponibilidade de dispositivos, tráfego de rede, acompanhamento do status e a saúde da rede, identifica os problemas de desempenho e muito mais.

Em conjunto, o uso dessas ferramentas pode melhorar significativamente a segurança da sua rede. O LibreNMS monitora o desempenho e a disponibilidade da rede e o Untangle Next Generation Firewall garante a segurança e o controle do tráfego. É importante ressaltar que a implementação e a configuração corretas dessas ferramentas são cruciais para garantir sua eficácia, porém além dessas três ferramentas é necessário implementar outras práticas recomendadas de segurança, como manter os sistemas operacionais atualizados, fazer backup regular dos dados e educar os usuários sobre boas práticas de segurança.

REFERÊNCIAS

FERREIRA, Sarah Pereira. Crimes cibernéticos: a ineficácia da legislação brasileira. 2021.

STALLINGS, Guilherme. Prevenção de perda de dados como uma tecnologia de aprimoramento da privacidade. **Journal of Data Protection & Privacy** , v. 3, n. 3, pág. 323-333, 2020.

Lei Geral de Proteção de Dados Pessoais (LGPD) Disponível em <https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd> **Acessado em:** 27 de maio de 2023 às 13:20 hs.

O que é cracker? **Disponível em** <https://www.tecmundo.com.br/o-que-e/744-o-que-e-cracker-.htm> **Acessado em:** 25 de setembro de 2022 às 09:20 hr.

Oque é Phishing **- Disponível em**: < https://br.malwarebytes.com/phishing/ > **Acessado em:** 13 de outubro de 2022 às 17:05 hr.

RESHMI, TR. Violações de segurança da informação devido a ataques de ransomware - uma revisão sistemática da literatura. **International Journal of Information Management Data Insights** , v. 1, n. 2, pág. 100013, 2021.

Procon-SP notifica Hospital Albert Einstein. **Disponível em:** <https://www.procon.sp.gov.br/procon-sp-notifica-hospital-albert-einstein/ > **Acessado em:** 17 de maio de 2023

LIMA, E. Profº - Introdução ao Gerenciamento de Redes. - t1º Ed., Cardoso, 2021.

Ataques Cibernéticos no Brasil aumentaram 46% no segundo trimestre de 2022- CRYPTOID **Disponível em:** < https://cryptoid.com.br/criptografia-identificacao-digital-id-biometria/ataques-ciberneticos-no-brasil-aumentaram-46-no-segundo-trimestre-de-2022/ > **Acessado em:** 18 de maio de 2023 às 16:30 hr.

BERARDI, D.; GIALLORENZO, S.; MELIS, A.; MELLONI,S.; ONORI,L.; PRANDINI, M.; **Data Flooding against Ransomware: Concepts and Implementations**, Computers & Security, 2023, **Disponível em:** <https://www.sciencedirect.com/science/article/abs/pii/S0167404823002055> **Acessado em:** 20 de maio de 2023.

Untangle: Firewall de Próxima Geração - **Disponível em:** <https://www.fcbrasil.com.br/desembaracar-proxima-geracao-firewall/ >**Acessado em:** 03 de março de 2023 às 10:05 hr.

Untangle – Next Generation Firewall. **Disponível em:** <https://www.fcbrasil.com.br/untangle-desenvolvimento/>**Acessado em:** 20 de maio de 2023 às 22:10 hr.

Wikipédia Arista Edge Threat Management - Disponível em: <https://wiki.edge.arista.com/index.php/Main_Page > Acessado em: 02 de maio de 2023 às 12:50 hr.

Figuras 3 a 6 – Imagem do Site da Arista Edge Threat Management
Disponível em:< https://edge.arista.com/ng-firewall/>**Acessado em:** 01 de junho de 2023 às 22:10 hr.

Figura 7 – Imagem do Site Oficial LibreNMS
Disponível em: <https://demo.librenms.org/?username=demo&password=demouser&submit=>
Acessado em: 01 de junho de 2023 às 22:15 hr.

Figura 10 – Visão panorâmica de vários painéis de monitoramento
Disponível em: < https://www.serverion.com/pt_br/solucoes/librenms/ > **Acessado em:** 01 de junho de 2023 às 22:15 hr.

LibreNMS DocsName- **Disponível em:** < https://docs.librenms.org/Support/Features/ > **Acessado em:** 23 de maio de 2023 às 09:25 hr.

LibreNMS-AWS EC3 **- Disponível em:** <https://www.linkedin.com/pulse/librenms-aws-ec2-bruno-oliveira/?originalSubdomain=pt > **Acessado em:** 25 de maio de 2023 às 18:20 hr.

Tudo o que precisa saber sobre a ISO 27001 e segurança da informação. **Disponível em:** <https://certificacaoiso.com.br/tudo-o-que-precisa-saber-sobre-a-iso-27001-e-seguranca-da-informacao/> Acessado em: 27 de maio de 2023 às 19:05 hr.

COSTA M. B. O que é DoS e DDoS? **Disponível em:** <https://canaltech.com.br/produtos/o-que-e-dos-e-ddos/> **Acessado em:** 28 de outubro de 2022 às 17:30 hr.

AGUILAR TOQUICA, Cristhian Alejandro et al. Gerenciamento de rede em nuvem: um passo em direção ao SDWAN. (Apud. **SAYDAM, T.; MAGEDANZ, T**. “From Networks and Network Management into Service and Service Management”. Journal of Networks and System Management, v.4, n.4 (dez. 1996), p. 345–348.)

KUROSE, J. F. e ROSS, K. - Redes de Computadores e a Internet –6a Ed., Pearson, 2010.

SKOUDIS, E. e **LISTON, T.** Counter Hack Reloaded, 2.ed., Upper Saddle River, NJ: Prentice Hall, 2006.