ESTUDO DO FIREWALL FORTIGATE DA FORTINET PARA AUXILIAR NA SEGURANÇA DE DADOS DE UMA EMPRESA

Wellington Soares de Moraes, Solange da Silva.

[1]Escola politécnica e de Artes Pontifícia Universidade Católica de Goiás, Goiânia, Goiás, Brasil, *guiton.acre@gmail.com*

[2]Escola politécnica e de Artes Pontifícia Universidade Católica de Goiás, Goiânia, Goiás, Brasil, *solansilva.ucg@gmail.com*

RESUMO: Este trabalho tem como objetivo avaliar a eficácia da solução de *firewall* de próxima geração (NGFW) *Fortigate*, na proteção da privacidade e segurança das informações, diante dos desafios impostos pelo cenário atual de transformação digital e ameaças cibernéticas. Os resultados obtidos com os testes no ambiente real, provou que o *Fortigate* é uma solução eficaz para a proteção de dados empresariais contra uma ampla gama de ameaças cibernéticas. Porém, apesar dos muitos pontos positivos, o estudo também identificou desafios na implementação do *Fortigate*, particularmente em relação à complexidade de configuração em ambientes híbridos ou na nuvem. Empresas com infraestruturas menos tradicionais podem necessitar de assistência adicional para otimizar o uso do *Fortigate*, o que implica a necessidade de treinamento ou a contratação de especialistas em segurança cibernética capacitados. O estudo permitiu concluir que a solução de firewall *Fortigate* da Fortinet mostrou ser uma solução eficiente e robusta para a proteção contra ameaças cibernéticas, oferecendo capacidade para garantir a integridade, confidencialidade e disponibilidade das informações corporativas. No entanto, a eficácia total da implementação depende não apenas da tecnologia em si, mas também de uma abordagem bem planejada e executada para a segurança cibernética em geral.

Palavras chaves: *Segurança de Redes de Computadores, Firewall Fortigate, Segurança Cibernética, Gestão de Segurança Corporativa, Segurança da Informação.*

ABSTRACT: This work aims to evaluate the effectiveness of the next generation firewall (NGFW) solution in protecting privacy and information security, given the challenges posed by the current scenario of digital transformation and cyber threats. The results obtained from testing in a real environment proved that *Fortigate* is an effective solution for protecting business data against a wide range of cyber threats. However, despite the many positive points, the study also identified challenges in implementing *Fortigate*, particularly in relation to the complexity of configuration in hybrid or cloud environments. Companies with less traditional infrastructures may require additional assistance to optimize the use of *Fortigate*, which may require training or hiring capable cybersecurity experts. The study concluded that Fortinet's *Fortigate* firewall solution proved to be an efficient and robust solution for protecting against cyber threats, offering the ability to guarantee the integrity, confidentiality and availability of corporate information. However, the full effectiveness of the implementation depends not only on the technology itself, but also on a well-planned and executed approach to cybersecurity in general.

Keywords: *Computer Network Security, Fortigate Firewall, Cyber Security, Corporate Security Management, Information Security.*

1. Introdução

Segundo a Dell Technologies, pensar no sucesso de um negócio nos dias de hoje está diretamente atrelado ao desempenho digital das organizações. Somente no Brasil, em 2020, de acordo com o Índice de Transformação Digital da Dell Technologies, mais de 85% das empresas decidiram investir em alguma iniciativa relacionada à transformação digital. Nesse contexto, vários termos ganharam espaço no dia a dia das corporações, de forma exponencial, como é o caso da segurança da informação e os seus riscos [1].

Com toda essa transformação digital, a segurança da informação tem emergido como uma prioridade crítica para o setor de Tecnologia da Informação (TI). À medida que os dados se tornam um ativo empresarial valioso, sua proteção contra ameaças tem cada vez mais sofisticadas se faz imperativa. Conforme destacado pela Algar Telecom as inovações tecnológicas, apesar de benéficas, ampliam a possibilidade de ataques cibernéticos. Assim, para garantir a segurança da informação transcende a simples preocupação, figurando como uma necessidade presente nas estratégias de TI. A relevância dessa questão se intensifica com a eminente aplicação da Lei Geral de Proteção de Dados (LGPD), exigindo das empresas uma postura proativa na adoção de soluções avançadas, como Centros de Operações de Segurança (SOCs), para abordar a prevenção, detecção, gestão e resposta a incidentes, além do monitoramento e avaliação de vulnerabilidades. [2].

A Gartner destaca a crescente facilidade e intuitividade no uso da tecnologia, permitindo até mesmo o desenvolvimento de aplicações sem profundo conhecimento técnico, graças à disponibilidade de recursos em plataformas de desenvolvimento na nuvem. Este movimento de democratização do acesso à tecnologia é projetado para se estender além das empresas, alcançando indivíduos em geral [3].

Diante deste contexto, esta pesquisa pretende responder a seguinte questão: - Como proteger a privacidade e segurança das empresas utilizando uma solução NGFW *Fortigate* da Fortinet?

O objetivo geral deste trabalho é avaliar a eficácia da solução de firewall de próxima geração (NGFW) *Fortigate*, desenvolvida pela Fortinet, na proteção da privacidade e segurança das

informações corporativas, diante dos desafios impostos pelo cenário atual de transformação digital e ameaças cibernéticas crescentes.

Os objetivos específicos são:

- Identificar as principais vulnerabilidades e ameaças cibernéticas que as empresas enfrentam no contexto atual de transformação digital, com ênfase na importância da segurança da informação.
- Analisar as características e funcionalidades do *Fortigate*, em sua capacidade de atender às necessidades de segurança de informação das empresas. Isso inclui a inspeção de tráfego criptografado e a automação de respostas a incidentes, aspectos fundamentais para a proteção de dados.
- Examinar a integração do *Fortigate* dentro do conceito *Security Fabric* da Fortinet, para promover uma arquitetura de segurança coesa e inteligente.
- Avaliar o impacto do uso do *Fortigate* na experiência do usuário e na continuidade dos negócios, considerando sua performance superior alimentada por processadores de segurança especialmente projetados com *Security Processing Unit* (SPU) que oferecem capacidades de inspeção de tráfego sem comprometer a velocidade da rede.

Espera-se que os resultados deste trabalho possam contribuir:

- Apresentando as funcionalidades do *Fortigate*, servindo como recurso informativo para administradores de segurança da informação. Isso permite que os gestores façam escolhas mais atualizadas ao selecionar soluções de segurança para suas organizações.
- Avaliando a eficácia do *Fortigate* e sua integração com o *Security Fabric* da Fortinet, trazendo evidências práticas que podem auxiliar as organizações na escolha e implementação de soluções de firewall de próxima geração. Estas evidências são cruciais para justificar investimentos em segurança da informação e para adaptar as estratégias de segurança às necessidades específicas de cada empresa.
- Trazendo recomendações práticas para a implementação eficaz do *Fortigate* em ambientes corporativos, visando maximizar a proteção contra ameaças cibernéticas e garantir a integridade, confidencialidade e disponibilidade das informações críticas.
- Informando aos administradores de segurança da informação de uma ferramenta que possibilita aplicar as melhores práticas de segurança do mercado.
- Fornecendo evidências práticas que podem auxiliar as organizações na escolha e implementação de soluções de firewall de próxima geração, como o *Fortigate* da Fortinet.

2. REFERENCIAL TEORICO

Essa seção apresenta alguns conceitos e definições sobre o tema e detalha sobre as funcionalidades do *Fortigate*.

2.1 Firewall

O firewall pode ser definido como um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança. Os *firewalls* têm sido a linha de frente da defesa na segurança de rede há mais de 25 anos. Eles colocam uma barreira entre redes internas protegidas e controladas que podem ser redes externas confiáveis ou não, como a Internet [4].

Nesse contexto, o *Fortigate* nada mais é do que um *firewall* de proteção de rede de computadores, que usa processadores de segurança capazes de identificar uma atividade suspeita antes mesmo dela solicitar acesso ao dispositivo [5].

O *firewall Fortigate* foi desenvolvido pela Fortinet, empresa referência em gestão e segurança de redes, além de líder do conceito *Unified Threat Management* (UTM) ou Gerenciamento Unificado de Ameaças. Esse modelo de firewall representa uma evolução para os demais, visto que torna o processo de identificação de ameaças mais rápido, prático e visual [5].

Como o nome indica, o UTM é capaz de integrar em uma só plataforma recursos como Firewall *Next Generation Firewall* (NGFW), *Virtual Private Netowork* (VPN), controle de aplicações, prevenção de intrusos, bem como o filtro web. Por meio dessas competências interconectadas, o *Fortigate* faz uma "curadoria" de segurança, identificando aplicações, ou, permitindo e/ou bloqueando o tráfego [5].

O diferencial do *Fortigate* que fazem com que esse firewall se destaque no mercado é, possuir o conceito de Gerenciamento Unificado de Ameaças. Essa condição faz com que a proteção oferecida pela ferramenta seja, sobretudo, dotada de algumas características em especial, amplitude, Proteção de alto nível, gerenciamento simplificado, geração de relatórios qualificados, otimização de custos, redução da complexidade com visualização unificada dos aplicativos, usuários e redes.

Além disso, os produtos *Fortigate* são diferenciados por contarem com processadores FortiASIC, que atendem, de forma separada, aos recursos de um equipamento. Desta forma, mesmo em caso de sobrecarga do serviço do firewall, ainda haverá uma possibilidade de trabalho e acesso à central de gerenciamento [5].

De forma complementar, por meio de seu sistema operacional denominado de FortiOS e de outras características, como a utilização de inteligência artificial, os *Fortigate* realizam inspeção de desempenho de tráfego de texto nos modelos cripto ou não criptografados [5].

Portanto, os *Fortigate* representam importantes *appliances* de segurança, que atuam contra-ataques conhecidos e desconhecidos, por meio de um serviço completo de segurança de rede e informação. É uma solução indicada para quem deseja transformar a estratégia desse segmento de TI nas empresas [5].

2.2 Ameaças cibernéticas

As ameaças cibernéticas são formas de grupos de sujeitos ou de apenas ação de sujeito individual, de modificar, expor, roubar informações pertencentes às organizações ou outras pessoas. Assim, há diversas formas de invasões, como *Denial of Service* (DoS), utilizado com o objetivo de bloquear a entrega dos serviços pertencentes ao fornecedor. Diante disso, ele realiza a requisição de um dispositivo, resultando na sobrecarga de processamento, banda, memória e a *Central Processing Unit* (CPU) do computador [6].

Outra forma de ataque são os *malwares*, de caráter malicioso, sendo que o mais conhecido é o ataque *ransonware*, sendo que sua principal função é a extração de informações, que são criptografadas. Em seguida, é solicitado um resgate, para que o usuário tenha acesso aos dados. Sendo assim, essa ação é considerada um sequestro digital, que rouba dados que podem ser vitais e essenciais de organizações [7].

Além de extorquirem os dados, os criminosos virtuais também vendem essas informações diretamente para os provedores, evitando a necessidade de negociar com terceiros, o que poderia complicar a negociação e potencialmente expor o esquema de roubo. [7].

2.3 Principais ferramentas de firewall de rede

Segundo o quadrante mágico Gartner que define o mercado de *firewall* de rede que usam inspeção de tráfego com estado bidirecional (para saída e entrada) para proteger redes. Os

firewalls de rede são aplicados por meio de hardware, dispositivos virtuais e controles nativos da nuvem. *Firewalls* de rede são usados para proteger redes. Podem ser redes locais, híbridas (no local e na nuvem), em nuvem pública ou em nuvem privada. Os produtos de firewall de rede oferecem suporte a diferentes casos de uso de implantação, como perímetros, empresas de médio porte, *data centers*, nuvens, escritórios distribuídos e nativos da nuvem [8].

Como mostrado na Figura 1, Gartner coloca 4 principais *firewalls* que se enquadram no quadrante magico, sendo eles *Fortigate*: NGFW da Fortinet ocupando a primeira colocação e classificado como a melhor escolha dos clientes, *Check Point Quantum* da *Check Point Software Technologies* ocupando o segundo colocado no rank, *PA-Series* da *Palo Alto Networks* ocupando a terceira posição e *Cisco Secure Firewall* da Cisco que ocupa a quarta e última posição do quadrante [8].

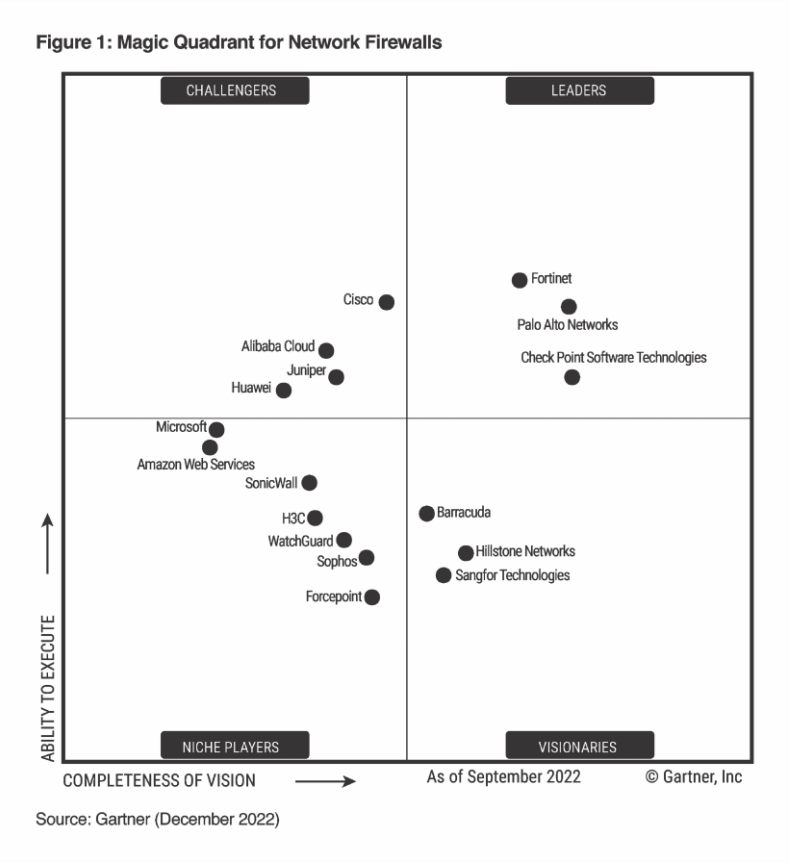


Figura 1 – Quadrante Magico de Gartner [7].

3. Materiais e Métodos

Essa pesquisa, quanto à natureza, caracteriza-se como um resumo de assunto, já que se baseia em apenas organizar uma área de conhecimento, indicando sua evolução histórica e estado de arte [9].

Quanto aos objetivos essa pesquisa é exploratória, aquela em que o autor não tem necessariamente uma hipótese ou objetivo definido em mente. Ela pode ser considerada, muitas vezes, como o primeiro estágio de um processo de pesquisa mais longo [9].

Referente aos procedimentos técnicos, trata-se de uma pesquisa bibliográfica, documental e experimental.

Foi realizada uma revisão bibliográfica sobre as estratégias para garantir a segurança de dados em ambientes empresariais, com um foco particular na utilização do *firewall Fortigate*. Foi analisada a eficácia desta tecnologia contra uma variedade de ameaças cibernéticas, incluindo invasões, *phishing*, *ransomware* e ataques distribuídos de negação de serviço (DDoS). Através de um estudo detalhado de literatura existente, que inclui trabalhos acadêmicos, Teses de Conclusão de Curso (TCCs) e artigos científicos. Este trabalho destaca como o *Fortigate* se diferencia de outros *firewalls*, especialmente em sua capacidade de oferecer proteção em camadas e defesa contra ameaças avançadas e persistentes.

A pesquisa sublinha a importância dos *firewalls* de próxima geração (NGFWs) como uma ferramenta essencial na arquitetura de segurança de informações de uma empresa, demonstrando como soluções integradas e abrangentes são cruciais para enfrentar o panorama dinâmico e cada vez mais complexo de ameaças cibernéticas.

A revisão bibliográfica envolve a análise de materiais já publicados, como livros, teses, recursos online e revistas, entre outros. Sua principal vantagem é permitir uma abordagem mais ampla de diversos fenômenos, além do que seria possível se pesquisasse diretamente [10].

A pesquisa documental é uma abordagem metodológica semelhante à pesquisa bibliográfica, mas se diferencia principalmente pelas fontes utilizadas [10].

De acordo com Gil [10], a pesquisa documental também tem etapas, mas este estudo se concentrará em apenas uma delas, que é:

a) Análise e interpretação dos dados: Analisar os documentos da *Fortigate* da Fortinet e interpretar seus dados, para assim descrever de forma objetiva, detalhada e com qualidade o conteúdo completo.

Foi realizado experimentos e testes em uma empresa real que usa o *Fortigate* para verificar e alcançar os objetivos deste trabalho, cujo resultados estão mostrados na Seção 4.

4. Resultados e Discussão

Este segmento do estudo concentra-se nos resultados da análise das funcionalidades e eficácia do *firewall Fortigate*, desenvolvido pela Fortinet, como uma solução de segurança cibernética para empresas. A avaliação abrange diversos aspectos técnicos e operacionais do *Fortigate*, proporcionando uma visão de como este dispositivo pode auxiliar na segurança de dados corporativos em um cenário de crescentes ameaças digitais.

4.1 Ambiente de Teste do Firewall Fortigate

Para atingir os objetivos desse trabalho foi utilizado o *firewall Fortigate* de uma empresa real que é uma instituição financeira, possuindo aproximadamente 1500 estações de usuários, incluindo servidores, *desktops*, *switch*, *firewalls* e *nobreaks*. Os testes foram autorizados e aprovados pela instituição e não resultaram em prejuízo para a mesma. A configuração específica do *Fortigate* 400F foi escolhida por sua capacidade de lidar com volumes elevados de tráfego e suas funcionalidades avançadas de segurança. Esta ferramenta, conforme mostrado na Figura 1, apresenta indicadores da solução e o *dashboard*, mostrando uma visibilidade abrangente, com painéis que incluem estatísticas em tempo real, logs de eventos, análises de tráfego, e muito mais. Esses recursos são não só vastos em número, mas também são organizados de maneira intuitiva, facilitando a navegação e a operação mesmo para usuários que não possuem especialização técnica profunda.

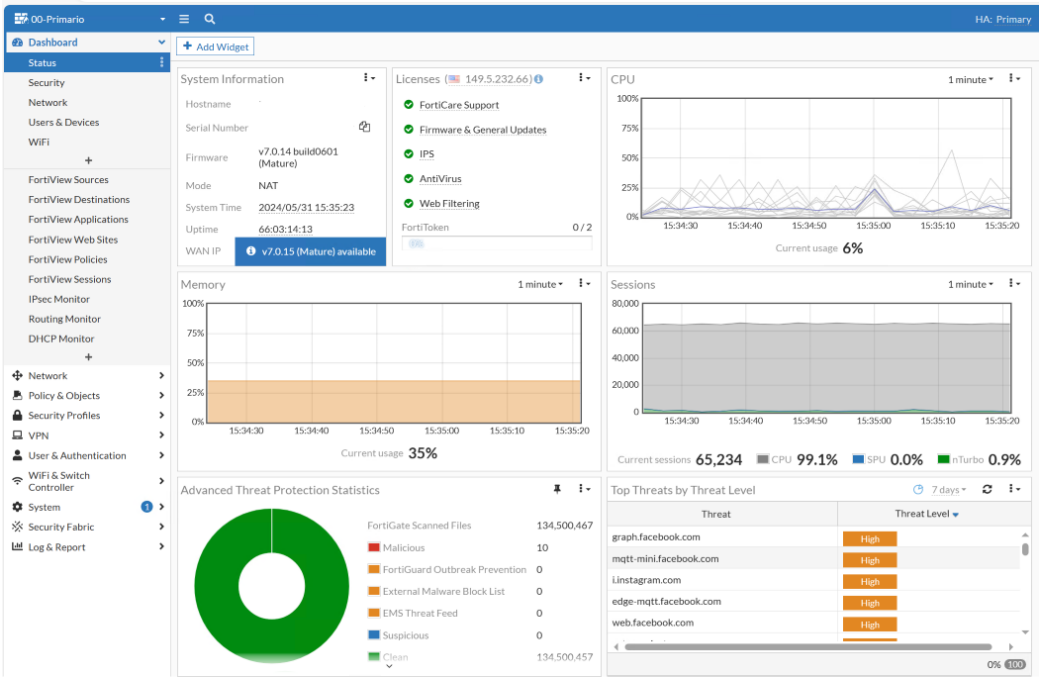


Figura 2 – Dashboard *Fortigate* [Autoria própria].

4.2 Identificação das Principais Vulnerabilidades e Ameaças Cibernéticas

As principais vulnerabilidades e ameaças cibernéticas "Top 10 Threats Worldwide" segundo a FortiGuard que as empresas enfrentam no contexto atual de transformação digital. Este segmento irá explorar como essas ameaças específicas refletem os riscos comuns e emergentes no cenário digital [11].

1. Vulnerabilidades do Microsoft Office e Oracle Java

    - MSOffice/CVE_2018_0798.BOR!exploit e MSExcel/CVE_2017_0199.DDOC!exploit: Explorações de vulnerabilidades no software da Microsoft que podem permitir a execução remota de código.

    - Oracle Java JRE CVEs (2022-21619, 2022-21624, 2022-21626, etc.): Uma série de vulnerabilidades no *Java Runtime Environment* que podem permitir ataques de execução remota de código e *buffer overflow*, destacando a necessidade de atualizações regulares e patches

2. Ataques Baseados em Protocolos e Serviços

    - SIPVicious.SIP.Scanner e HTTP.Suspicious.Headers.With.Special.Characters: Ataques que exploram protocolos específicos (SIP e HTTP) para identificar vulnerabilidades ou realizar ataques de injeção.

    - DNS.PTR.Records.Scan e IP.Land: *Scans* maliciosos que tentam explorar informações de configuração de rede para facilitar ataques ou mapeamento de rede.

3. Propagação de *Malware* e Controle de *Bootnets*

    - Zeroaccess.Botnet, Andromeda.Botnet, Prometei.Botnet: Estes *botnets* demonstram a capacidade dos atacantes de controlar grandes redes de máquinas infectadas para realizar atividades maliciosas, como ataques DDoS, *spamming* e mineração de criptomoedas.

- TorrentLocker.Botnet e Mozi.Botnet: Especificamente envolvidos em *ransomware* e ataques de negação de serviço, respectivamente, estes *botnets* são exemplos de como os cibercriminosos monetizam seu controle sobre redes infectadas.

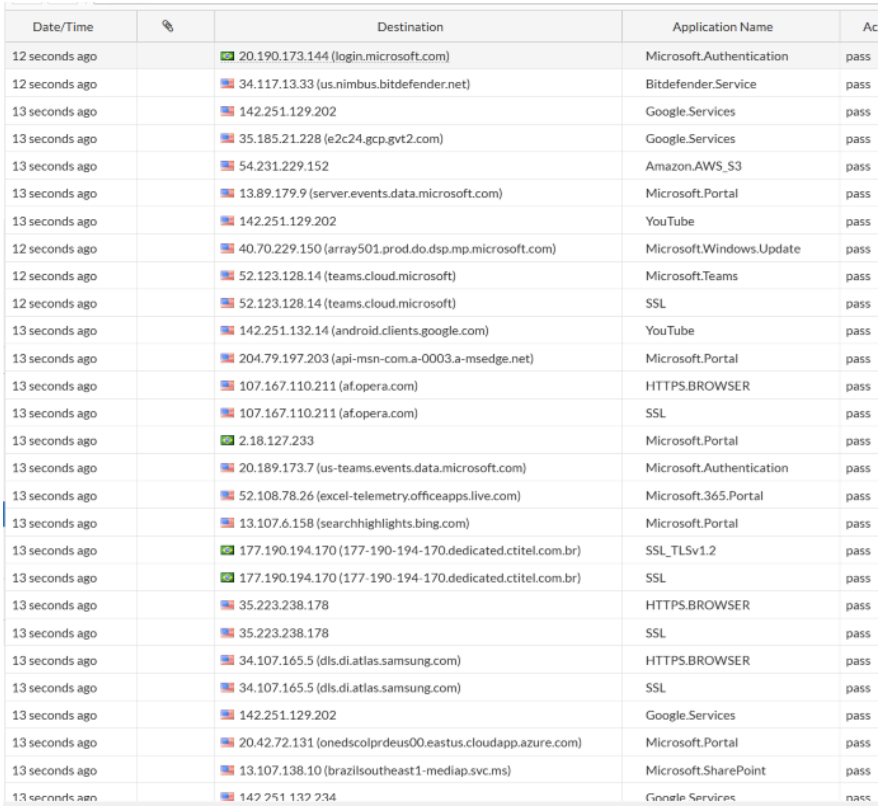
4. Explorações de Segurança Emergentes e Ameaças Desconhecidas

    - Unknown Threats: A categoria *'Unknown'* com o maior volume de incidência destaca o desafio constante de enfrentar novas ameaças que ainda não foram plenamente identificadas ou entendidas.

    - Apache log4net CVE-2018-1285 XML External Entity Vulnerability: Vulnerabilidades em bibliotecas de terceiros, como a Apache log4net, mostram o risco de componentes de software que podem ser explorados para ataques de injeção de entidade externa XML.

4.3 Eficácia do Fortigate em Ambientes Corporativos

Conforme apresentado na Figura 2 os resultados obtidos destacam a capacidade superior do *Fortigate* em identificar e mitigar ameaças cibernéticas complexas, incluindo ataques de *phishing*, *ransomware* e DDoS. Por exemplo na Figura 2 notasse que o *Fortigate* inspeciona todos os pacotes separando em aplicação com a resolução dos IPs e a geolocalização das aplicações. Uma característica notável do *Fortigate* é a sua capacidade de inspeção profunda de pacotes, que permite uma análise detalhada do tráfego de dados, identificando atividades suspeitas antes que possam causar danos significativos. Esta funcionalidade é essencial, visto que muitos ataques modernos são altamente sofisticados e podem evadir sistemas de segurança menos avançados.



Date/Time		Destination	Application Name	Ac
12 seconds ago		20.190.173.144 (login.microsoft.com)	Microsoft.Authentication	pass
12 seconds ago		34.117.13.33 (us.nimbus.bitdefender.net)	Bitdefender.Service	pass
13 seconds ago		142.251.129.202	Google.Services	pass
13 seconds ago		35.185.21.228 (e2c24.gcp.gvt2.com)	Google.Services	pass
13 seconds ago		54.231.229.152	Amazon.AWS_S3	pass
13 seconds ago		13.89.179.9 (server.events.data.microsoft.com)	Microsoft.Portal	pass
13 seconds ago		142.251.129.202	YouTube	pass
12 seconds ago		40.70.229.150 (array501.prod.do.dsp.mp.microsoft.com)	Microsoft.Windows.Update	pass
12 seconds ago		52.123.128.14 (teams.cloud.microsoft)	Microsoft.Teams	pass
12 seconds ago		52.123.128.14 (teams.cloud.microsoft)	SSL	pass
13 seconds ago		142.251.132.14 (android.clients.google.com)	YouTube	pass
13 seconds ago		204.79.197.203 (api-msn-com.a-0003.a-msedge.net)	Microsoft.Portal	pass
13 seconds ago		107.167.110.211 (af.opera.com)	HTTPS.BROWSER	pass
13 seconds ago		107.167.110.211 (af.opera.com)	SSL	pass
13 seconds ago		2.18.127.233	Microsoft.Portal	pass
13 seconds ago		20.189.173.7 (us-teams.events.data.microsoft.com)	Microsoft.Authentication	pass
13 seconds ago		52.108.78.26 (excel-telemetry.officeapps.live.com)	Microsoft.365.Portal	pass
13 seconds ago		13.107.6.158 (searchhighlights.bing.com)	Microsoft.Portal	pass
13 seconds ago		177.190.194.170 (177-190-194-170.dedicated.ctitel.com.br)	SSL_TLSv1.2	pass
13 seconds ago		177.190.194.170 (177-190-194-170.dedicated.ctitel.com.br)	SSL	pass
13 seconds ago		35.223.238.178	HTTPS.BROWSER	pass
13 seconds ago		35.223.238.178	SSL	pass
13 seconds ago		34.107.165.5 (dls.di.atlas.samsung.com)	HTTPS.BROWSER	pass
13 seconds ago		34.107.165.5 (dls.di.atlas.samsung.com)	SSL	pass
13 seconds ago		142.251.129.202	Google.Services	pass
13 seconds ago		20.42.72.131 (onedscolprdeus00.eastus.cloudapp.azure.com)	Microsoft.Portal	pass
13 seconds ago		13.107.138.10 (brazilsoutheast1-mediap.svc.ms)	Microsoft.SharePoint	pass
13 seconds ago		142.251.132.234	Google.Services	pass

Figura 3 – *Fortigate* fazendo inspeção de tráfego de rede [Autoria própria].

A integração do *Fortigate* com a plataforma *Security Fabric* da Fortinet também foi destacada como um diferencial. Esta integração permite que o *Fortigate* compartilhe informações de segurança em tempo real com outros dispositivos na rede, criando uma defesa coordenada e mais eficaz contra-ataques. A capacidade de operar de maneira sincronizada com outros componentes de segurança amplia significativamente a visibilidade e o controle sobre a segurança da rede, um fator importante para empresas que operam em ambientes digitais complexos.

4.4 Impacto na Performance da Rede e Usabilidade

Outro resultado significativo da análise, conforme apresentado na Figura 3, foi a observação de que o *Fortigate* mantém uma alta performance de rede, mesmo sob carga pesada, graças aos processadores de segurança (SPUs) especializados. Esses processadores ajudam a minimizar a latência e garantem que as operações críticas de negócios não sejam prejudicadas por medidas de segurança, atendendo às demandas de empresas que necessitam de uma solução que equilibre segurança e performance.

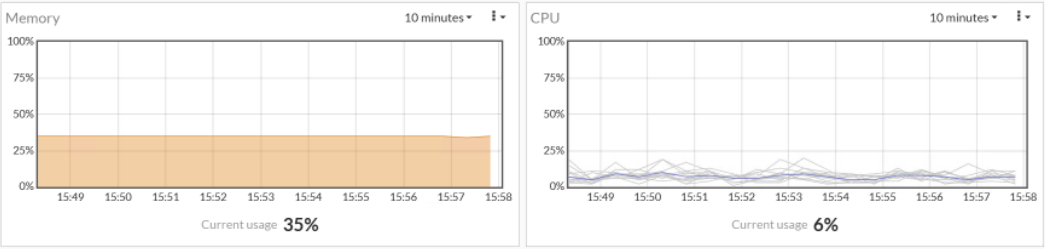


Figura 4 – *Fortigate* fazendo inspeção de tráfego de rede [Autoria própria].

Além disso, a experiência do usuário com o *Fortigate* foi avaliada positivamente, especialmente em termos de gestão e geração de relatórios. A interface do usuário é intuitiva e fornece relatórios detalhados que ajudam os administradores de rede a entenderem o panorama de segurança da empresa de forma clara e precisa. Esses relatórios são fundamentais para o monitoramento contínuo e para a tomada de decisões baseadas em evidências.

4.5 Desafios e Considerações para Implementação do Fortigate

Apesar dos muitos pontos positivos, o estudo também identificou desafios na implementação do *Fortigate*, particularmente em relação à complexidade de configuração em ambientes híbridos ou na nuvem. Empresas com infraestruturas menos tradicionais podem necessitar de assistência adicional para otimizar o uso do *Fortigate*, o que implica a necessidade de treinamento ou a contratação de especialistas em segurança cibernética capacitados.

Os resultados obtidos com os testes no ambiente real, provaram que o *Fortigate* é uma solução eficaz para a proteção de dados empresariais contra uma ampla gama de ameaças cibernéticas. A integração do *Fortigate* com o *Security Fabric*, juntamente com a capacidade de inspeção profunda de pacotes e a alta performance dos SPUs, fazem dele uma escolha apropriada para empresas que buscam uma defesa cibernética avançada e integrada. Apesar da solução *Fortigate* 400F ser cara, é crucial que as empresas entendam a necessidade desse investimento, que trará retorno significativo em segurança. Para empresas menores, existem outras soluções como o *Fortigate* 40F, que é adequado para pequenas empresas com pouco tráfego e um custo mais acessível. Contudo, é importante que as organizações considerem os desafios de implementação e operação, assegurando que tenham os recursos necessários para maximizar os benefícios desta tecnologia.

4.6 Recomendações para Implementação Efetiva do Fortigate

Com base nos resultados e discussões deste estudo, várias recomendações podem ser formuladas para auxiliar as empresas na implementação efetiva do *Fortigate* como uma ferramenta de segurança cibernética:

- **Capacitação Técnica**: As empresas devem investir na capacitação técnica de suas equipes de TI, especialmente em aspectos relacionados à configuração e gerenciamento do *Fortigate*. Isso inclui treinamento em características específicas do produto, como a inspeção de tráfego criptografado e as funcionalidades avançadas de detecção e resposta a ameaças.

- **Planejamento de Segurança Integrada**: Adotar uma abordagem integrada de segurança é crucial. O *Fortigate* deve ser parte de uma estratégia de segurança mais ampla que inclua outras ferramentas e práticas. A utilização do *Security Fabric* da Fortinet é recomendada para maximizar a integração e a comunicação entre diferentes dispositivos de segurança na rede.

- **Avaliação de Necessidades de Segurança**: Antes da implementação, as empresas devem realizar uma avaliação detalhada de suas necessidades de segurança. Isso inclui entender os tipos de dados mais críticos que precisam de proteção, as principais vulnerabilidades da infraestrutura existente e os requisitos regulatórios específicos que podem influenciar as escolhas de segurança.

- **Monitoramento e Avaliação Contínua**: Após a implementação do *Fortigate*, é essencial estabelecer processos de monitoramento e avaliação contínua para garantir que o sistema esteja funcionando conforme esperado e adaptar-se a novas ameaças. Isso também ajudará a identificar rapidamente qualquer necessidade de ajuste ou atualização na configuração do firewall.

- **Gerenciamento de Mudanças**: As empresas devem desenvolver um robusto processo de gerenciamento de mudanças para a introdução do *Fortigate* em suas redes. Isso minimiza o impacto operacional e garante que todas as partes interessadas entendam as mudanças e suas implicações para a segurança da rede.

- **Consulta com Especialistas em Segurança**: Recomenda-se que as organizações consultem especialistas em segurança cibernética para uma implementação personalizada e otimizada do *Fortigate*. Isso é particularmente importante para ambientes complexos ou altamente regulamentados.

5. Conclusão

Este artigo tem como objetivo responder a seguinte questão de pesquisa e com o objetivo: "Como proteger a privacidade e segurança das empresas utilizando uma solução NGFW *Fortigate* da Fortinet?''

O estudo permitiu concluir que a solução de firewall *Fortigate* da Fortinet mostrou ser uma solução eficiente e robusta para a proteção contra ameaças cibernéticas, oferecendo amplas capacidades para garantir a integridade, confidencialidade e disponibilidade das informações corporativas. No entanto, a eficácia total da implementação depende não apenas da tecnologia em si, mas também de uma abordagem bem planejada e executada para a segurança cibernética em geral.

Os resultados obtidos com os testes no ambiente real provaram que o *Fortigate* é uma solução eficaz para a proteção de dados empresariais contra uma ampla gama de ameaças cibernéticas. Porém, apesar dos muitos pontos positivos, o estudo também identificou desafios na implementação do *Fortigate*, particularmente em relação à complexidade de configuração em ambientes híbridos ou na nuvem. Empresas com infraestruturas menos tradicionais podem necessitar de assistência adicional para otimizar o uso do *Fortigate*, o que implica a necessidade de treinamento ou a contratação de especialistas em segurança cibernética capacitados.

Para a continuidade desta pesquisa sugere-se os seguintes trabalhos futuros:

- Realizar uma análise de longo prazo do desempenho do *Fortigate* em diferentes tipos de ambientes empresariais, incluindo sua eficácia em ambientes de nuvem versus *on-premises*.

- Investigar os impactos da inteligência artificial e aprendizado de máquina incorporados no *Fortigate* e como essas tecnologias podem avançar a segurança cibernética no futuro.

5. Referências Bibliográficas

1. Dell Technologies.: Índice de Transformação Digital 2020 (DT Index 2020). Acesso em: 7 março de 2024. Disponível em: https://www.dell.com/pt-br/dt/perspectives/digital-transformation-index.htm
2. Algar Telecom.: As tendências para a área de TI em 2020. Acesso em: 7 março de 2024. Disponível em: https://blog.algartelecom.com.br/tendencias/as-tendencias-para-a-area-de-ti-em-2020/
3. Gartner. Gartner Top 10 Strategic Technology Trends for 2020. Acesso em: 7 março de 2024. Disponível em: https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/
4. CISCO.: O que é um firewall?. Acesso em: 23 maio 2024. Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html
5. Escola Superior de Redes.: O que é *Fortigate* e qual sua importância para a Segurança Corporativa?. Acesso em: 7 março de 2024. Disponível em: https://esr.rnp.br/seguranca/o-que-e-fortigate/
6. Bonguet, A., Bellaiche, M.: A Survey of Denial-of-Service and Distributed Denial of Service Attacks and Defenses in Cloud Computing. Future Internet; 9(3), 43; (2017).
7. Fornasier, M.O.; Spinato, T.P., Ribeiro, F.L.: Ransomware e cibersegurança: a informação ameaçada por ataques a dados. Revista Thesis Juris, Acesso em: 7 março 2024; 9(1). Disponível em: https://periodicos.uninove.br/thesisjuris/article/view/16739/
8. Gartner.: Network Firewalls Reviews and Ratings. Acesso em: 7 março de 2024. Disponível em: https://www.gartner.com/reviews/market/network-firewalls/
9. Wazlawick, R.S.: Metodologia de Pesquisa para Ciência da Computação. 2ª ed. Rio de Janeiro: Elsevier; 2014. cap.4, p. 21 – 26.
10. Gil, A.C.: Como Elaborar Projetos de Pesquisa. 6ª ed. São Paulo: Editora Atlas Ltda.; 2017.
11. FORTIGUARD LABS.: Top 10 Threats Worldwide. Fortinet, 2024. Acesso em: 23 maio 2024. Disponível em: https://www.fortiguard.com/threat-research/threat/

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
GABINETE DO REITOR

Av. Universitária, 1069 • Setor Universitário
Caixa Postal 86 • CEP 74605-010
Goiânia • Goiás • Brasil
Fone: (62) 3946.1000
www.pucgoias.edu.br • reitoria@pucgoias.edu.br

RESOLUÇÃO n° 038/2020 – CEPE

ANEXO I

APÊNDICE ao TCC

Termo de autorização de publicação de produção acadêmica

O estudante Wellington Soares de Moraes do Curso de Ciência da Computação, matrícula: 20181002804516, telefone: (62) 98217-5073, e-mail: guiton.acre@gmail.com, na qualidade de titular dos direitos autorais, em consonância com a Lei nº 9.610/98 (Lei dos Direitos do Autor), autoriza a Pontifícia Universidade Católica de Goiás (PUC Goiás) a disponibilizar o Trabalho de Conclusão de Curso intitulado ESTUDO DO FIREWALL FORTIGATE DA FORTINET PARA AUXILIAR NA SEGURANÇA DE DADOS DE UMA EMPRESA, gratuitamente, sem ressarcimento dos direitos autorais, por 5 (cinco) anos, conforme permissões do documento, em meio eletrônico, na rede mundial de computadores, no formato especificado (Texto(PDF); Imagem (GIF ou JPEG); Som (WAVE, MPEG, AIFF, SND); Vídeo (MPEG, MWV, AVI, QT); outros, específicos da área; para fins de leitura e/ou impressão pela internet, a título de divulgação da produção científica gerada nos cursos de graduação da PUC Goiás.

Goiânia, 25 de JUNHO DE 2024.

Assinatura do autor: WELLINGTON SOARES DE MORAES:75359006153

Assinado de forma digital por WELLINGTON SOARES DE MORAES:75359006153
DN: c=BR, o=ICP-Brasil, ou=AC SOLUTI Multipla v5, ou=09461647000195, ou=Videoconferencia, ou=Certificado PF A1, cn=WELLINGTON SOARES DE MORAES:75359006153
Dados: 2024.06.25 22:27:58 -03'00'

Nome completo do autor: Wellington Soares de Moraes

Assinatura do professor–orientador: ___

gov.br Documento assinado digitalmente
SOLANGE DA SILVA
Data: 26/06/2024 07:00:53-0300
Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: __ SOLANGE DA SILVA _____