PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA E DE ARTES

GRADUAÇÃO EM ENGENHARIA DE COMPUTAÇÃO

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE FIREWALL FORTIGATE EM AMBIENTES CORPORATIVOS

WILLIAN MIRANDA MENDES

GOIÂNIA

2026

WILLIAN MIRANDA MENDES

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE FIREWALL FORTIGATE EM AMBIENTES CORPORATIVOS

Trabalho de Conclusão de Curso apresentado à Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para a obtenção do título de Bacharel em Engenharia de Computação.

Orientadora: Profa. Dra. Solange da Silva
Banca examinadora:

Prof Me. Anibal Santos Jukemura

Prof Me. Rafael Leal Martins

GOIÂNIA

2026

WILLIAN MIRANDA MENDES

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE FIREWALL FORTIGATE EM AMBIENTES CORPORATIVOS

Este Trabalho de Conclusão de Curso foi julgado adequado para obtenção o título de
Bacharel em Engenharia de Computação, e aprovado em sua forma final pela Escola
Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, em 12/06/2026.

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Me. Anibal Santos Jukemura

_____

Prof. Me. Rafael Leal Martins

GOIÂNIA
2026

AGRADECIMENTO

Agradeço primeiramente a Deus, pela sabedoria, força e perseverança concedidas ao longo desta trajetória acadêmica, permitindo-me superar os desafios e alcançar meus objetivos.

Aos meus pais, Luciene Cristina Miranda Mendes e Wainer Neves Mendes, pelo amor, incentivo e apoio incondicional em todas as etapas desta caminhada. Seus exemplos de dedicação e coragem foram fundamentais para a concretização desta conquista.

À minha orientadora, Profa. Dra. Solange da Silva, pela paciência, comprometimento e pelos ensinamentos compartilhados durante o desenvolvimento deste trabalho. Sua orientação foi essencial para o meu crescimento acadêmico e profissional.

À Pontifícia Universidade Católica de Goiás (PUC GO), pela oportunidade de aprendizado e pelo suporte institucional que contribuíram de maneira significativa para minha formação.

Ao meu sênior no trabalho, André Luiz da Silva, pela orientação, confiança e pelos ensinamentos que me ajudaram a evoluir pessoal e profissionalmente.

Aos meus amigos e familiares, pela compreensão, incentivo e presença constante, fundamentais para manter a motivação e o equilíbrio ao longo desta jornada.

E, por fim, a todos que, de alguma forma, contribuíram para a realização deste trabalho, deixo registrado meu mais sincero agradecimento.

RESUMO

Este trabalho teve como objetivo identificar e descrever as funcionalidades do *firewall* FortiGate e sua aplicação na segurança de redes corporativas. Metodologicamente, a pesquisa caracteriza-se como exploratória, com abordagem bibliográfica e experimental, complementada por análise documental e por estudo comparativo de custo-benefício entre soluções de *firewall* para pequenas e médias empresas. A etapa prática foi desenvolvida em ambiente corporativo real, contemplando a implantação de dois appliances FortiGate 60F, um na matriz e outro na filial. Os resultados demonstraram a viabilidade da solução por meio da segmentação lógica da infraestrutura, da interligação segura entre as unidades via VPN IPsec, da redundância de conectividade e da utilização de recursos de monitoramento e visibilidade operados pelo FortiOS. A análise comparativa indicou que a solução adotada apresentou melhor equilíbrio entre desempenho, abrangência funcional, simplicidade de administração e custo total de implementação. Conclui-se que o FortiGate constitui uma plataforma eficaz para proteção perimetral, organização lógica da rede e apoio à governança da segurança em pequenas e médias empresas, desde que corretamente configurado, monitorado e integrado às políticas institucionais de segurança da informação.

Palavras-chave: FortiGate. Segurança de redes. *Firewall* de próxima geração. Segmentação de rede. VPN IPsec.

ABSTRACT

This project aimed to identify and describe the functionalities of the FortiGate firewall and its application in corporate network security. Methodologically, the research is characterized as exploratory, with bibliographic and experimental approaches, complemented by documentary analysis and a comparative cost-benefit study between firewall solutions for small and medium-sized enterprises. The practical stage was carried out in a real corporate environment, involving the deployment of two FortiGate 60F appliances, one at the headquarters and the other at the branch office. The results demonstrated the feasibility of the solution through logical infrastructure segmentation, secure interconnection between units via IPsec VPN, connectivity redundancy, and the use of monitoring and visibility resources operated by FortiOS. The comparative analysis indicated that the adopted solution presented a better balance between performance, functional coverage, ease of administration, and total implementation cost. It is concluded that FortiGate constitutes an effective platform for perimeter protection, logical network organization, and support for security governance in small and medium-sized enterprises, provided that it is properly configured, monitored, and integrated with institutional information security policies.

Keywords: FortiGate. Network security. Next-generation firewall. Network segmentation. IPsec VPN.

LISTA DE SIGLAS

Sigla	Significado
ASIC	*Application-Specific Integrated Circuit*
CAPES	Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CFTV	Circuito Fechado de Televisão
CIDA	Confidencialidade, Integridade, Disponibilidade e Autenticidade
CFS	*Content Filtering Service*
CLI	*Command-Line Interface*
CP	*Content Processor*
CPU	*Central Processing Unit*
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*Demilitarized Zone*
DNS	*Domain Name System*
DPI	*Deep Packet Inspection*
FTP	*File Transfer Protocol*
GUI	*Graphical User Interface*
HTTP	*Hypertext Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IA	Inteligência Artificial ou *Artificial Intelligence*
IBM	*International Business Machines*
IDS	*Intrusion Detection System*
IEC	Comissão Eletrotécnica Internacional
IP	*Internet Protocol* ou Protocolo de Internet
IPS	*Intrusion Prevention System*
IPsec	*Internet Protocol Security*
ISO	Organização Internacional para Padronização
Java EE	*Java Platform, Enterprise Edition*
LAN	*Local Area Network* ou Rede Local
MAN	*Metropolitan Area Network* ou Rede Metropolitana
NAT	*Network Address Translation*
NGFW	*Next-Generation Firewall*
NP	*Network Processor*
OSI	*Open Systems Interconnection*
PDCA	*Plan-Do-Check-Act*
P2P	*Peer-to-Peer*
SI	Segurança da Informação
SGSI	Sistemas de Gestão de Segurança da Informação
SMTP	*Simple Mail Transfer Protocol*
SQL	*Structured Query Language*
SSL	*Secure Sockets Layer*
SPU	*Security Processing Units*
TCC	Trabalho de Conclusão de Curso
TCP	*Transmission Control Protocol*

Sigla	Significado
TI	Tecnologia da Informação
TLS	*Transport Layer Security*
UDP	*User Datagram Protocol*
URL	*Uniform Resource Locator*
UTM	*Unified Threat Management*
UTP	*Unified Threat Protection*
VPN	*Virtual Private Network*
WAF	*Web Application Firewall*
WAN	*Wide Area Network*
XSS	*Cross-Site Scripting*

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1 INTRODUÇÃO

As redes de computadores tornaram-se fundamentais no ambiente corporativo moderno, viabilizando a comunicação e o compartilhamento de informações entre dispositivos interconectados. Entretanto, juntamente com os benefícios da conectividade, surgem desafios relacionados à proteção dessas redes contra uma variedade cada vez maior de ameaças cibernéticas.

Em um cenário no qual incidentes de segurança são cada vez mais frequentes e sofisticados, a segurança de redes de computadores desponta como uma prioridade estratégica para organizações de todos os portes, pois visa garantir a confidencialidade, integridade e disponibilidade dos dados corporativos mesmo diante de tentativas de ataque maliciosas (Thapa e Paul, 2024).

Diversos estudos destacam que ferramentas avançadas de cibersegurança – como *firewalls* de nova geração, sistemas de detecção de intrusão e plataformas de monitoramento – são essenciais para proteger ativos e informações sensíveis contra acessos não autorizados. Essas soluções, oferecidas por empresas líderes em tecnologia (Cisco, IBM, Fortinet etc.), possibilitam às organizações salvaguardar seus ambientes de Tecnologia da Informação (TI) e assegurar conformidade com normas regulatórias.

Por outro lado, apresentam desafios de complexidade, custo e necessidade de configuração adequada, reforçando a importância da gestão de riscos e da capacitação em cibersegurança (Thapa e Paul, 2024).

Entre os mecanismos de defesa em segurança de redes, destaca-se o *firewall*, amplamente reconhecido como a primeira linha de proteção de perímetro. Um *firewall* monitora o tráfego de entrada e saída de uma rede e decide permitir ou bloquear pacotes de dados com base em um conjunto de regras previamente definidas pelo administrador (Cisco, 2023).

Essas ferramentas podem ser implementadas em nível de *hardware*, *software* ou combinação de ambos, e tornaram-se onipresentes tanto em ambientes domésticos quanto empresariais devido à sua eficácia em mitigar riscos básicos de segurança (Dourado, 2022).

Todavia, a evolução das ameaças cibernéticas expôs limitações dos *firewalls* tradicionais, que operavam majoritariamente por inspeção superficial de pacotes (analisando endereços e portas) e regras estáticas.

Atacantes passaram a explorar tais limitações camuflando ataques em meio a tráfego aparentemente legítimo ou usando portas não convencionais e criptografia para escapar do filtro básico dos *firewalls* convencionais (Patel, 2024). Como resposta, surgiram os chamados *firewalls* de próxima geração (NGFWs) a partir de meados dos anos 2000, projetados justamente para superar essas deficiências dos modelos tradicionais (Patel, 2024).

No mercado atual de segurança de redes, diversas soluções de *firewall* de nova geração se destacam. Dentre elas, o FortiGate, da fabricante Fortinet, figura como um dos equipamentos líderes e mais utilizados em ambientes corporativos. O FortiGate tem sido reconhecido pela literatura e órgãos independentes por oferecer funcionalidades avançadas e alto desempenho na proteção de redes empresariais.

Por exemplo, em avaliações comparativas recentes, as soluções Fortigate obtiveram as maiores pontuações em casos de uso como data centers corporativos, bordas de redes distribuídas e pequenas/médias empresas, evidenciando sua eficácia em diferentes cenários (Shah e Abid, 2022).

Justifica-se, portanto, a escolha do FortiGate como objeto de estudo neste trabalho em virtude de sua relevância no mercado de Segurança da informação (SI) e de seu amplo emprego em empresas, o que implica que conhecer suas funcionalidades e configurações é de grande interesse prático para profissionais da área.

Diante deste contexto, este trabalho visa responder à seguinte questão de pesquisa: **Quais são as funcionalidades do *firewall* FortiGate e como ele pode ser configurado para garantir segurança em redes corporativas?**

Este trabalho tem como objetivo geral identificar e descrever as funcionalidades do *firewall* FortiGate e sua aplicação na segurança de redes corporativas.

Os objetivos específicos são:

- Descrever a estrutura de implantação do firewall FortiGate 60F e sua integração lógica à rede corporativa;

- Apresentar e detalhar as principais funcionalidades de segurança oferecidas pelo FortiGate, explicando seus propósitos e modos de operação;
- Mostrar funcionalidades selecionadas do FortiGate 60F em ambiente corporativo real, com foco na interligação segura entre matriz e filial por VPN, segmentação lógica da infraestrutura, redundância de conectividade e recursos de monitoramento, a fim de avaliar a viabilidade da solução na proteção e organização da rede corporativa;
- Comparar, sob a perspectiva de custo-benefício, a solução FortiGate com outra solução de *firewall* avaliada pela empresa, considerando fatores técnicos, operacionais e financeiros.

Espera-se que os resultados deste trabalho possam contribuir:

- Informando administradores de rede corporativa sobre a importância do FortiGate como solução de segurança eficaz e reforçando suas vantagens como *firewall* de nova geração;
- Fornecendo orientações gerais sobre estruturação, configuração e boas práticas de segurança, auxiliando profissionais e usuários de TI na implementação correta de políticas de proteção em suas redes;
- Destacando a relevância de uma política de segurança da informação nas empresas, bem como a aderência a normas e diretrizes de segurança reconhecidas, de forma a reduzir a vulnerabilidades e aprimorar a gestão de riscos.

Quanto aos aspectos metodológicos, esta pesquisa caracteriza-se como pesquisa secundária de natureza exploratória, utilizando uma abordagem bibliográfica e experimental.

Esta monografia está organizada em sete capítulos. O capítulo 1 apresenta a Introdução, contextualizando o tema, definindo o problema de pesquisa, objetivos, justificativa e metodologia empregada. O capítulo 2 contém o Referencial Teórico, abordando os conceitos fundamentais de segurança da informação e de redes de computadores, os tipos de *firewall* e suas evoluções, além de trabalhos relacionados sobre *firewalls* de próxima geração e gestão de segurança em redes corporativas. No

capítulo 3, são descritos os Procedimentos Metodológicos, detalhando a classificação da pesquisa, o ambiente e os métodos de coleta e análise de dados adotados para atingir os objetivos propostos. O Capítulo 4 é dedicado exclusivamente ao *firewall* FortiGate, apresentando as características técnicas do modelo FortiGate 60F utilizado e suas principais funcionalidades de segurança. No capítulo 5 é apresentado uma análise de custo e benefício entre o FortiGate e o *SonicWall*, outro modelo de *firewall*. O Capítulo 6 apresenta a estrutura de implantação, o funcionamento e os resultados observados com o FortiGate no ambiente corporativo real. Finalmente, o Capítulo 7 traz as conclusões finais.

2 REFERENCIAL TEÓRICO

Este capítulo apresenta os conceitos fundamentais que embasam o estudo sobre segurança de rede de computadores com foco em *firewall* FortiGate em ambientes corporativos. São abordados inicialmente os princípios de Segurança da Informação, seguidos dos conceitos essenciais de redes de computadores, situando o contexto no qual os *firewalls* operam.

Em seguida, discute-se o conceito de *firewalls*, seus tipos e a evolução para os *firewalls* NGFW. Posteriormente, são apresentadas as normas da série da Organização Internacional para Padronização em conjunto com a Comissão Eletrotécnica Internacional (ISO/IEC) 27000 relevantes (27001, 27002, 27003, 27004), que estabelecem diretrizes para gestão da segurança da informação. O aprofundamento específico sobre a arquitetura e as funcionalidades do FortiGate é desenvolvido no Capítulo 4.

Por fim, são discutidos trabalhos relacionados, evidenciando pesquisas e estudos recentes correlatos ao tema deste trabalho.

2.1 SEGURANÇA DA INFORMAÇÃO

SI diz respeito à proteção dos dados e sistemas contra acessos não autorizados, uso indevido, divulgação, interrupção, modificação ou destruição. De acordo com a norma ISO/IEC 27000, SI é definida como “a preservação da confidencialidade, integridade e disponibilidade da informação” (ISO, 2018, p. 4).

Embora essa definição normativa apresente a base clássica formada pela confidencialidade, integridade e disponibilidade, abordagens institucionais recentes também incorporam a autenticidade como propriedade essencial da segurança da informação, formando o modelo Confidencialidade, Integridade, Disponibilidade e Autenticidade (CIDA) (BRASIL, [s.d.]; LNCC, 2024).

Esses quatro elementos formam os pilares CIDA da segurança da informação, ilustrados na Figura 1, sendo fundamentais para orientar políticas, controles e práticas de proteção em ambientes corporativos. A confidencialidade refere-se à garantia de que a informação seja acessível somente por pessoas autorizadas. A integridade assegura que os dados permaneçam confiáveis e não sejam alterados indevidamente. A

disponibilidade significa que as informações e serviços estarão acessíveis aos usuários autorizados quando necessário e a autenticidade busca assegurar que a informação, o acesso ou a ação realizada possam ser atribuídos a uma origem legítima, como um usuário, sistema, equipamento ou entidade autorizada (IBM, 2023; LNCC, 2024).

Figura 1 - Quatro pilares da confidencialidade, integridade, disponibilidade e autenticidade da segurança da informação

Fonte: Autoria própria, 2026

Nesse contexto, o modelo CIDA amplia a compreensão tradicional da segurança da informação, pois não basta apenas proteger o sigilo, a exatidão e o acesso aos dados. Também é necessário garantir que a origem das informações e das ações realizadas no ambiente tecnológico seja verificável.

Em redes corporativas, essa característica é especialmente relevante, pois mecanismos de autenticação de usuários, controle de acesso, VPN, certificados digitais, registros de eventos e políticas de *firewall* contribuem diretamente para reforçar a autenticidade e a confiabilidade das operações realizadas na infraestrutura de TI.

A importância da SI cresceu significativamente nos últimos anos devido ao aumento de ameaças cibernéticas e incidentes de vazamentos de dados. Empresas e organizações têm enfrentado ataques cada vez mais sofisticados, incluindo *malware*, *ransomware* e violações de dados confiáveis (IBM, 2023). Um relatório da *International Business Machines* (IBM) de 2023 indicou que o custo médio global de uma violação de dados atingiu US$ 4,45 milhões, representando um aumento de aproximadamente 15% no triênio de 2020 a 2023. Nesse cenário, investir em SI tornou-se fundamental.

Os princípios e boas práticas de segurança ajudam as organizações a mitigar riscos e proteger seus ativos informacionais. Por exemplo, a série ISO/IEC 27000 fornece um *framework* global para implementação de Sistemas de Gestão de Segurança da Informação (SGSI), como discutido na seção 2.4 deste capítulo.

Em suma, SI envolve um conjunto de políticas, processos, controles e tecnologias destinados a proteger os dados contra ameaças, garantindo a continuidade dos negócios e a minimização de impactos em caso de incidentes.

2.2 REDES DE COMPUTADORES

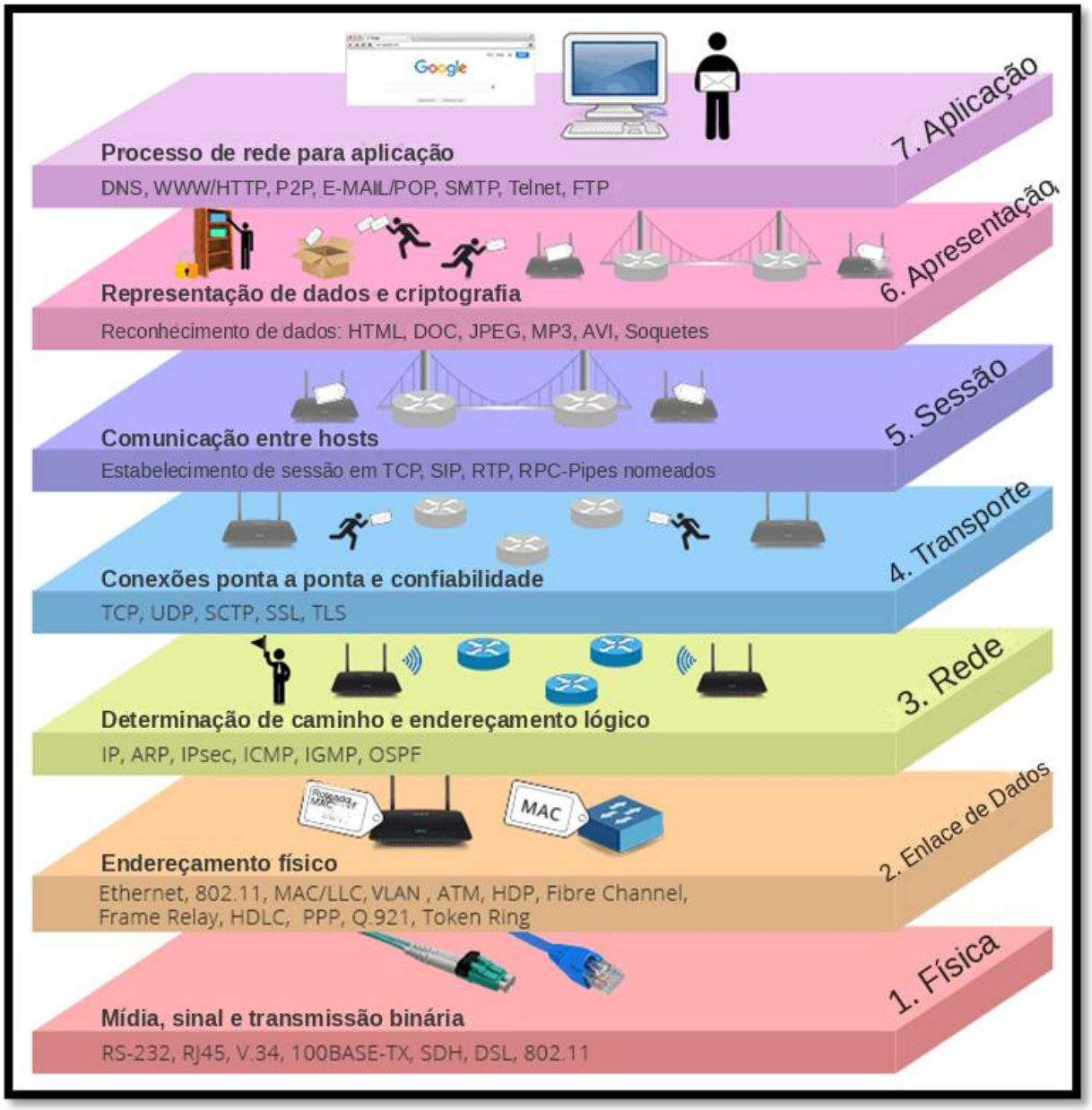
Redes de computadores constituem a base da comunicação digital corporativa, permitindo a interligação de sistemas e o compartilhamento de recursos. Uma rede de computadores pode ser definida como um conjunto de dispositivos autônomos interconectados que trocam informações e compartilham recursos entre si (Kurose e Ross, 2020). Em outras palavras, envolve múltiplos computadores, servidores, roteadores, *switches* e outros equipamentos conectados por meio de enlaces de comunicação (cabos, enlaces sem fio etc.), de forma a possibilitar a transmissão de dados.

Segundo Tanenbaum, Feamster e Wetherall (2021, p. 2), uma rede de computadores pode ser entendida como “uma coleção de dispositivos computacionais autônomos e interconectados”. Essas interconexões podem variar em escala e alcance, desde redes locais (LANs) dentro de um escritório, passando por redes metropolitanas (MANs), até redes de longa distância (WANs) que cobrem regiões geográficas extensas ou interligam filiais de uma empresa em diferentes localidades.

As redes modernas operam em arquiteturas hierárquicas por camadas, seguindo modelos como Protocolo de Controle da Transmissão/Protocolo de Internet (TCP/IP)

ou o modelo *Open Systems Interconnection* (OSI), ilustradas na Figura 2, nos quais cada camada do protocolo realiza funções específicas para viabilizar a comunicação de dados. Por exemplo, há camadas responsáveis pelo endereçamento e roteamento dos pacotes (camada de rede), pelo controle de conexões fim a fim (camada de transporte) e pela interface com as aplicações do usuário (camada de aplicação) (Kurose e Ross, 2020).

Figura 2 - Modelo de referência em camadas *Open Systems Interconnection* e *Transmission Control Protocol/Internet Protocol* para comunicações em rede.



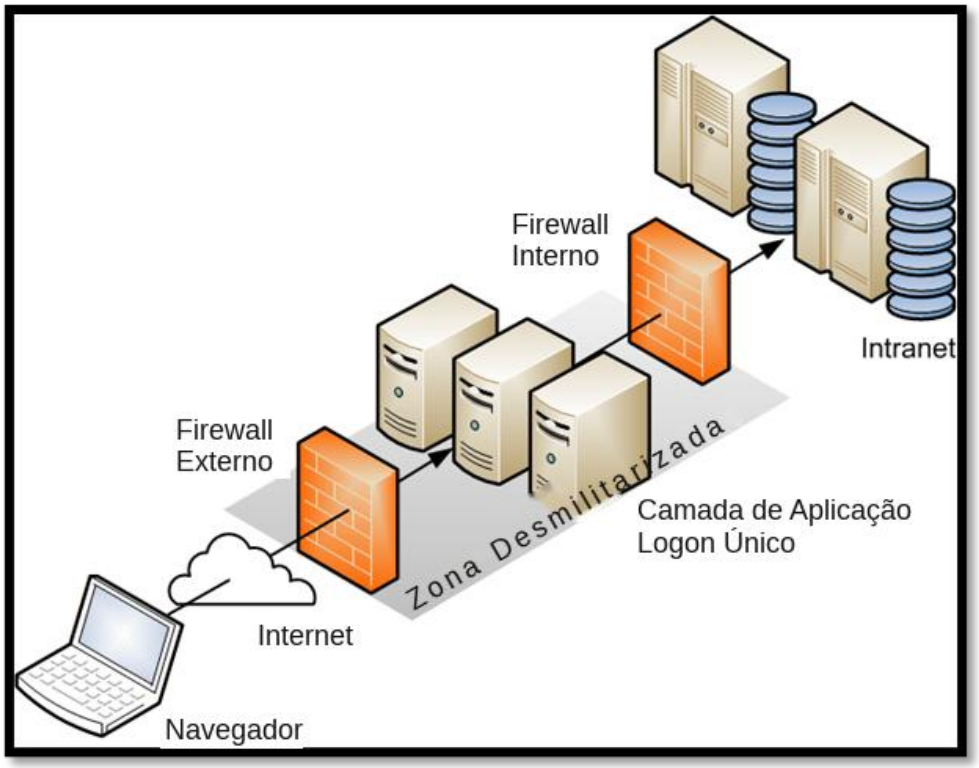
Fonte: Traduzido de CISCO, 2023

Essa estrutura de camada torna as redes flexíveis e escaláveis, mas também introduz diversos vetores de ataque exploráveis por agentes maliciosos. Com o aumento da interconectividade e da dependência das organizações em relação a sistemas em rede, a segurança de redes tornou-se componente crítico da infraestrutura

de TI corporativa. Uma brecha de segurança em uma rede pode permitir que invasores acessem dados sensíveis ou interrompam serviços essenciais (NIST, 2009).

É importante ressaltar que rede corporativas geralmente são segmentadas em domínios de segurança com diferentes níveis de confiança, como rede interna (privadas), zonas desmilitarizadas (DMZs), voltadas a servidores de aplicações públicas) e a própria Internet (rede externa não confiável), apresentado na Figura 3. Essa segmentação visa limitar o alcance de eventuais incidentes e facilitar a aplicação de controles de segurança (Cisco, 2025; NIST, 2016).

Figura 3 - Segmentação de rede com zona desmilitarizada (DMZ) protegida por *firewall* de perímetro.



Fonte: Traduzido de HOOGENRAAD, 2023

Mecanismos de proteção de rede, notadamente os *firewalls,* são empregados tipicamente nos pontos de fronteira entre essas redes de diferentes níveis de confiança (por exemplo, entre a rede interna e a Internet, ou entre a DMZ e a rede interna).

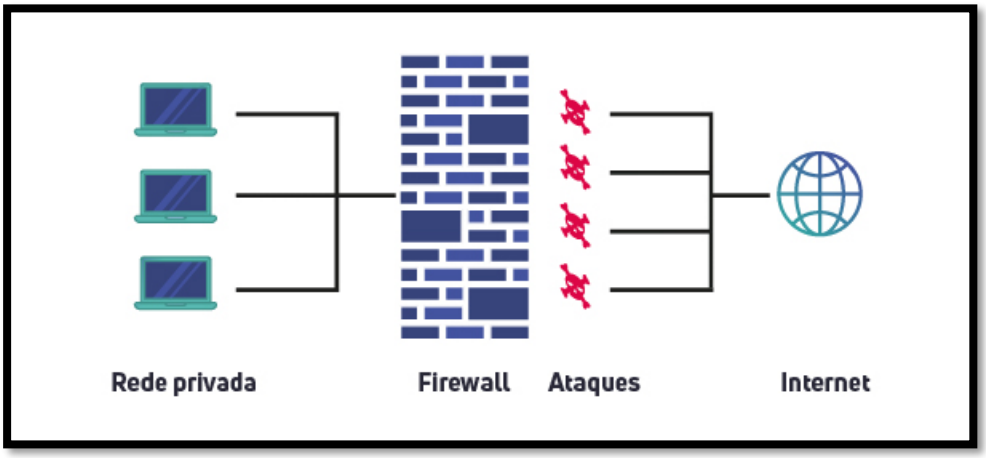
Dessa forma, as redes de computadores e a segurança estão intimamente ligados. A mesma infraestrutura que possibilita comunicação e negócios traz também riscos que precisam ser gerenciados. A próxima seção detalha o papel dos *firewalls*, que há décadas constituem uma das principais linhas de defesas para proteger redes corporativas (NIST, 2009).

2.3 *FIREWALLS*: CONCEITO, TIPOS E EVOLUÇÃO NGFW

O *firewall* é um dos pilares da segurança de redes, atuando como uma barreira de proteção entre uma rede confiável (interna) e redes não confiáveis (externas). De forma geral, um *firewall* é definido como um dispositivo (ou serviço) de segurança de rede projetado para monitorar, filtrar e controlar o tráfego de dados que sai e entra de uma rede, com base em um conjunto de regras de segurança pré-definidas (Fortinet, 2023a).

Seu objetivo principal é bloquear tráfegos maliciosos ou não autorizados e, simultaneamente, permitir que o tráfego legítimo necessário às operações da organização flua normalmente, mostrado na Figura 4. Os *firewalls* existem há mais de 25 anos e desde então têm sido a primeira linha de defesa em segurança de redes, estabelecendo um perímetro seguro que impede que usuários ou sistemas externos acessem a rede interna sem autorização (Cisco, 2023).

Figura 4 - O que é *Firewall*



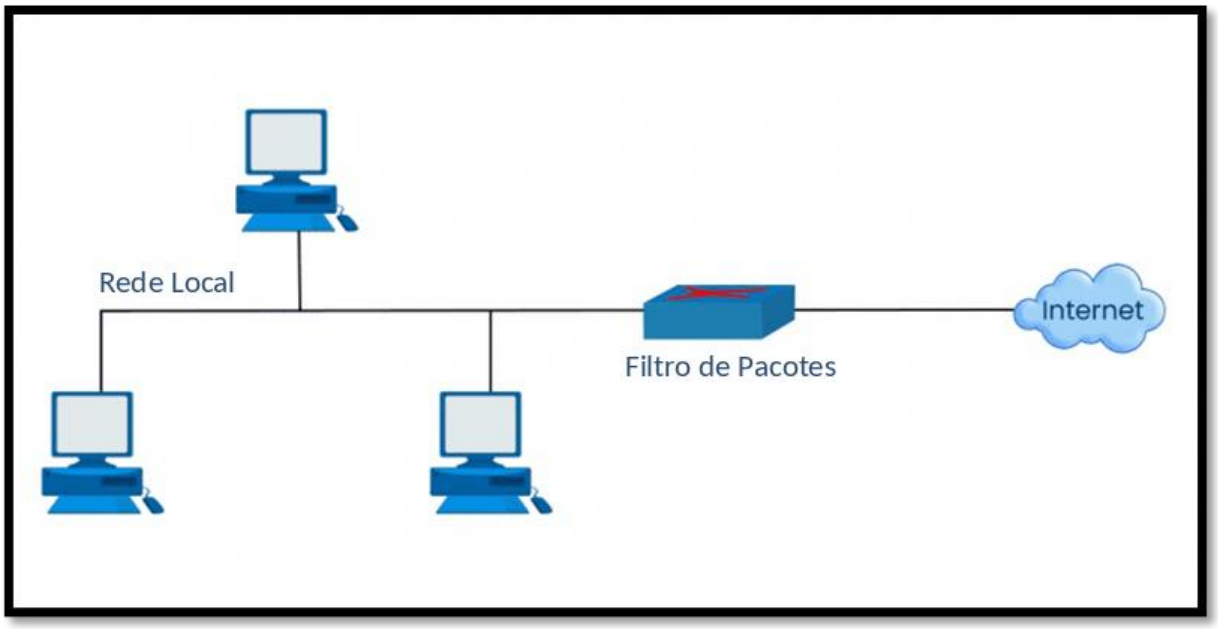
Fonte: BORN, 2021

Tipos de *firewalls*: Historicamente, os *firewalls* evoluíram em suas técnicas de filtragem e camada de atuação. Podem-se classificar diferentes tipos ou geração de *firewalls.*

2.3.1 FIREWALL DE FILTRO DE PACOTES (CAMADA DE REDE)

É o tipo mais básico, conhecido também como *firewall* de camada de pacote. Opera principalmente na camada de rede (endereços IP) e transporte (portas TCP e Protocolo de Datagrama do Usuário, UDP) do modelo OSI, inspecionando cabeçalhos dos pacotes e aplicando regras estáticas de acordo com endereços de origem/destino, portas e protocolo. Esse tipo de *firewall* (às vezes chamado de *stateless*) não mantém estado de conexões e está apresentada na Figura 5.

Figura 5 - *Firewall* de Filtro de Pacote



Fonte: Traduzido de RIBEIRO, [s.d.]

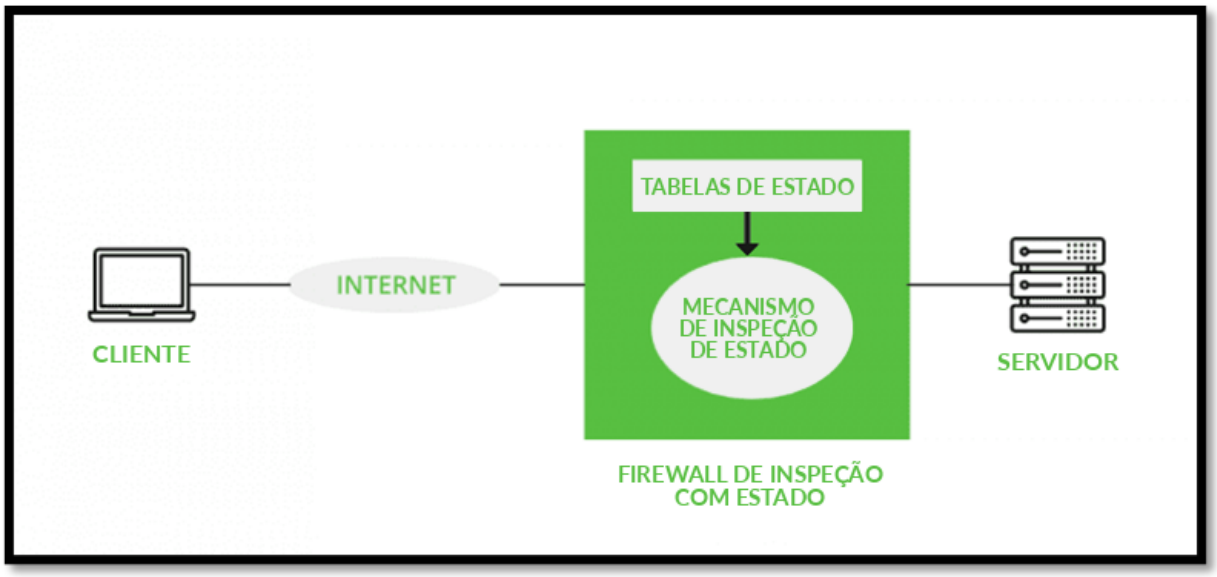
Cada pacote é examinado isoladamente. *Firewalls* de filtro de pacotes surgiram no final dos anos 1980 e foram os primeiros a estabelecer o conceito de fronteira de rede protegido (Bhartiya e Jindal, 2021). Embora eficientes para

bloquear ou permitir tráfego básico, eles não inspecionam o conteúdo dos pacotes e podem ser burlados por ataques que utilizam portas/protocolos permitidos.

2.3.2 *FIREWALL* DE INSPEÇÃO DE ESTADO (NÍVEL DE CIRCUITO)

Chamado de *stateful firewalls*, foram uma evolução nos anos 1990. Além de considerar os critérios do filtro de pacotes, eles mantêm informações sobre o estado das conexões ativas (por exemplo, acompanham sessões TCP estabelecidas). Assim, podem permitir automaticamente pacotes de retorno de conexões iniciadas internamente, bloqueando tráfego inesperado. Esse tipo de *firewall* atua como uma espécie de *gateway* de circuito, monitorando o *handshake* das conexões e garantindo que cada pacote pertença a uma conexão válida, mostrado na Figura 6.

Figura 6 - *Firewall* de Inspeção de Estado



Fonte: Traduzido de RIBEIRO, [s.d.]

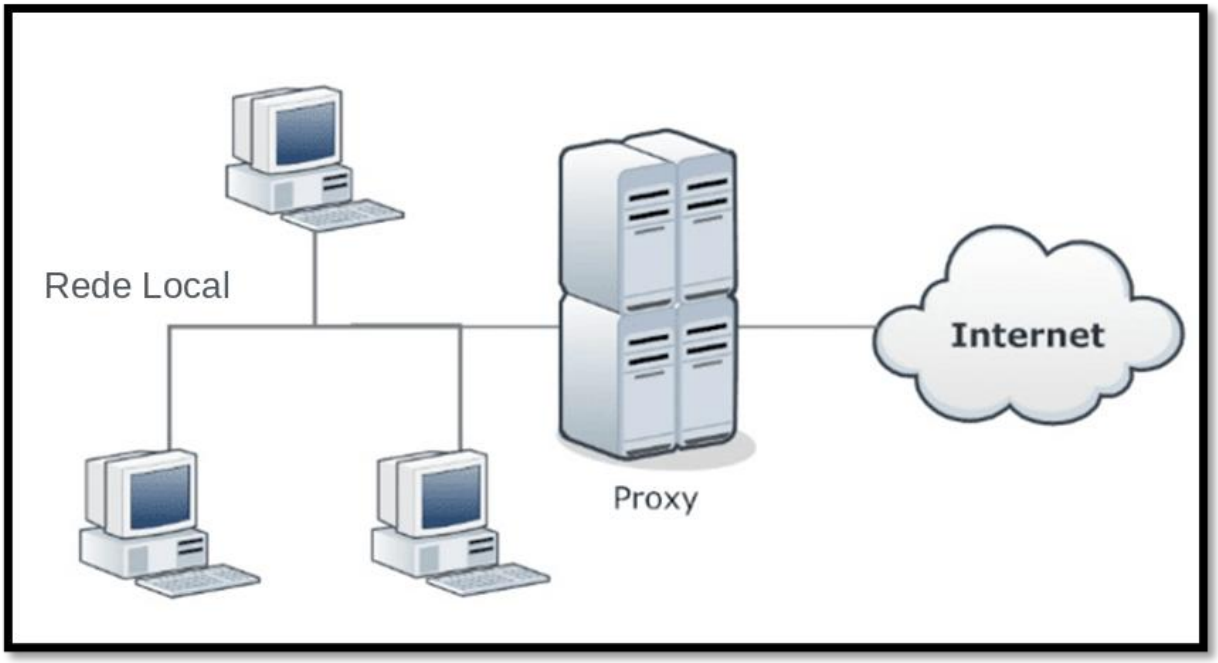
Firewall stateful, conseguem distinguir tráfegos legítimos (por exemplo, respostas a requisições internas) de tentativas não solicitadas de entrada, aumentando a segurança em relação ao *stateless*. Ainda assim, *firewalls* de

inspeção de estado operam majoritariamente até a camada de transporte e não analisam o conteúdo da carga útil das aplicações (Bhartiya e Jindal, 2021).

2.3.3 FIREWALL DE CAMADA DE APLICAÇÃO/SERVIDOR *PROXY*

Esse tipo aprofunda a inspeção até a camada de aplicação (Camada 7 do modelo OSI). São *firewalls* capazes de entender protocolos de aplicação (HTTP, FTP, SMTP etc.) e filtrar conteúdo específico. Um exemplo é o *firewall proxy*, que atua intermediando a comunicação entre cliente interno e servidor externo – o cliente se conecta ao *proxy*, que por sua vez conecta-se ao destino externo, repassando (e filtrando) as informações, destacado na Figura 7.

Figura 7 - *Firewall Proxy*



Fonte: Traduzido de RIBEIRO, [s.d.]

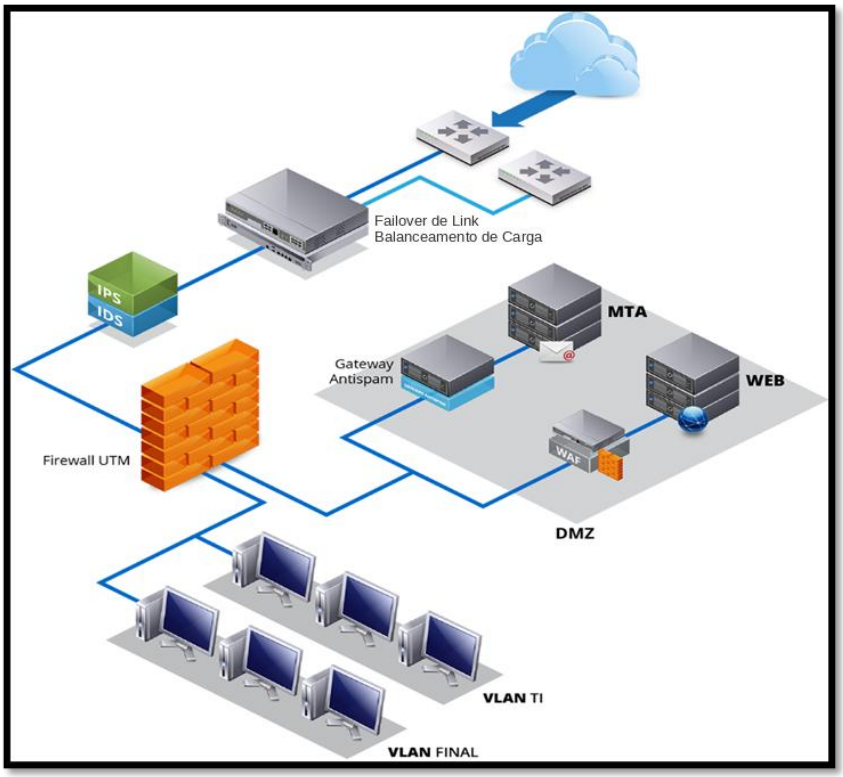
Firewalls de aplicação podem bloquear comandos maliciosos em protocolos *web* ou *email*, por exemplo, e realizar inspeção mais granulada. Devido à natureza detalhada da análise, tendem a exigir mais processamento e podem introduzir latência, mas oferecem controle mais rigoroso. Tecnologias de *Web Application Firewall* (WAF)

também se enquadram aqui, focadas em proteger aplicações *web* específicas, filtrando ataques como *Structured Query Language* (SQL) *Injection*, *Cross-Site Scripting* (XSS) etc. (Kurose e Ross, 2020; Tanenbaum, Femstrer e Wetherall, 2021).

2.3.4 FIREWALL UTM (GERENCIAMENTO UNIFICADO DE AMEAÇAS)

O termo *Unified Threat Management* (UTM) surgiu nos anos 2000 para designar dispositivos de segurança que consolidam múltiplas funções além do *firewall* tradicional. Um *firewall* UTM típico, além de filtrar pacotes e manter estado, inclui funcionalidades de IDS/IPS (sistema de detecção e prevenção de intrusões), *antimalware*, filtro de conteúdo *web*, VPN, entre outros, em uma única plataforma integrada (Fortinet, 2023a; ESR/RNP, 2022), apresentados na Figura 8.

Figura 8 - *Firewall* de gerenciamento unificado de ameaças



Fonte: Traduzido de ASER, [s.d.]

Esse modelo unificado simplifica o gerenciamento e amplia a cobertura de segurança, pois um único *appliance* passa a executar diversos serviços de proteção (antes realizados por equipamentos separados). A Fortinet foi uma das pioneiras no conceito UTM e consolidou-se no mercado com dispositivos que combinem essas múltiplas defesas (ESR/RNP, 2022).

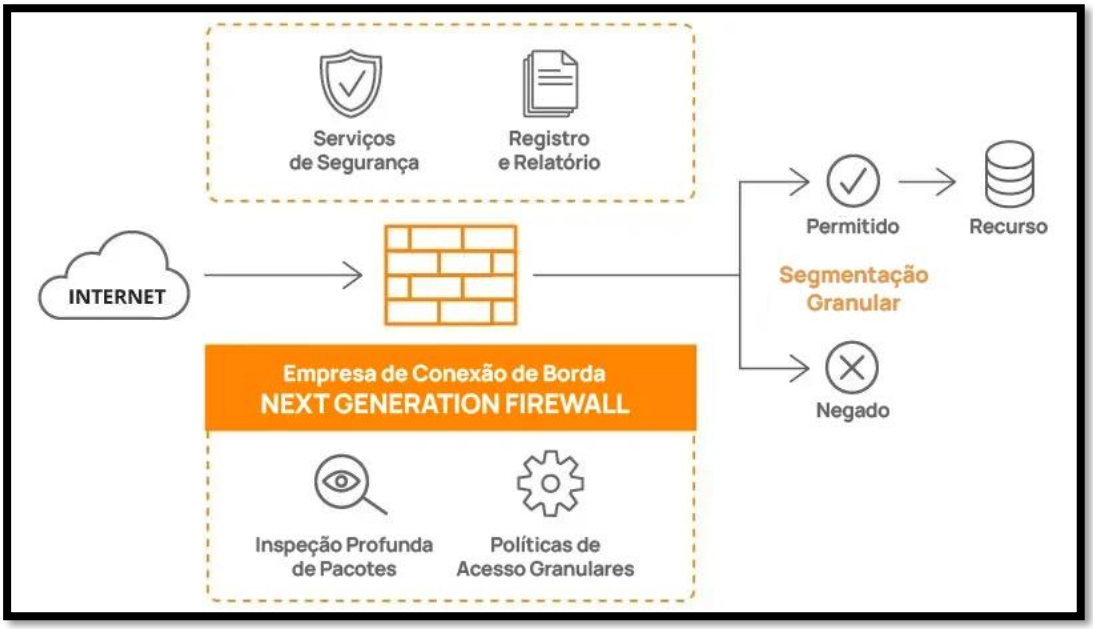
2.3.5 FIREWALL DE PRÓXIMA GERAÇÃO (NGFW)

Os NGFW representam a evolução mais recente em tecnologias de *firewall*, englobando características dos *firewalls* tradicionais, UTM e adicionando capacidades avançadas, especialmente a inspeção de pacotes profunda (DPI) e o reconhecimento de aplicações.

Diferentemente dos *firewalls* legados, os NGFW conseguem inspecionar não apenas cabeçalhos, mas também o conteúdo dos pacotes em tempo real, identificando a aplicação ou serviço trafegando (mesmo que use porta ou protocolo fora do padrão) (Patel, 2024). Isso permite, por exemplo, distinguir tráfego legítimo de HTTP/HTTPS de tráfego de aplicações indesejadas tuneladas na porta 80/443. Com a consciência de aplicação (*application awareness)*, o *firewall* de próxima geração pode aplicar políticas mais granulares – por exemplo, bloquear acesso a redes sociais ou *streaming*, permitir determinado aplicativo corporativo e negar outro, independentemente da porta utilizada (Patel, 2024).

Além disso, NGFWs tipicamente incluem IPS integrado, filtro de URL, inspeção de tráfego criptografado (SSL/TLS) e outras defesas contra ameaças avançadas, mostrado na Figura 9.

Figura 9 - *Firewall* de próxima geração



Fonte: PRONNUS, [s.d.]

A motivação para o surgimento dos NGFWs veio das limitações dos *firewalls* tradicionais frente às ameaças modernas. Ataques passaram a encapsular códigos maliciosos em tráfegos aparentemente legítimos (por exemplo, malware trafegando via Protocolo de Transferência de Hipertexto e Protocolo de Transferência de Hipertexto Seguro (HTTP/HTTPS), que em *firewalls* antigos passariam despercebidos) (Patel, 2024). Assim, por volta de meados dos anos 2000, fornecedores como Palo Alto *Networks*, *Check Point* e Fortinet impulsionaram o conceito de *next-generation firewall*, combinando *firewall* com inspeção profunda e controle de aplicação.

Essa evolução se mostra crucial num ambiente em que aplicações usam portas dinâmicas, comunicações são frequentemente cifradas e ameaças sofisticadas burlam facilmente filtros simples (Ahmed, Khan e Rahman, 2021). NGFWs são projetados para operar em tempo real, analisando o comportamento dos dados e aplicações, e prevenir ataques complexos que passariam pelas defesas legadas (Patel, 2024).

Em suma, a principal diferença entre um NGFW e um *firewall* tradicional está na visibilidade e inteligência aplicadas ao tráfego: enquanto o *firewall* clássico enxerga endereços e portas, o NGFW “entende” o que está sendo acessado (aplicação, conteúdo) e quem está acessando (usuário, dispositivo), permitindo aplicar políticas de segurança muito mais específicas e eficazes.

2.4 NORMAS DA SÉRIE ORGANIZAÇÃO INTERNACIONAL PARA PADRONIZAÇÃO / COMISSÃO ELETROTÉCNICA INTERNACIONAL (ISO/IEC) 27000 (27001, 27002, 27003, 27004)

Para estruturar e respaldar as práticas de SI nas organizações, uma série de normas internacionais foi desenvolvida no âmbito da ISO/IEC, destacando-se a família ISO/IEC 27000, que abrange padrões SGSI.

Entre essas, merecem ênfase as normas ISO/IEC 27001, 27002, 27003 e 27004, pelas orientações diretas que fornecem à implementação, operação e melhoria da SI corporativa. A seguir, apresenta-se cada uma dessas normas e seu escopo.

2.4.1 ISO/IEC 27001

SGSI é o principal padrão da família e o único certificável. A ISO/IEC 27001 estabelece os requisitos para criar, implementar, manter e aprimorar continuamente um SGSI. Nela estão especificados os controles de segurança que a organização deve considerar (listados no Anexo A da norma) e as cláusulas para gestão de riscos, políticas, organização da segurança, controle de acessos, criptografia, continuidade, conformidade etc. (ISO, 2022a).

O foco da 27001 é dizer “o quê” deve ser feito para proteger as informações (por exemplo, deve-se realizar análise de riscos, deve-se ter controle de acesso, deve-se ter planos de resposta a incidentes), sem detalhar “como” implementar cada controle. As organizações podem buscar a certificação ISO 27001 por entidades independentes, demonstrando assim a clientes, parceiros e reguladores que seguem as melhores práticas internacionais de SI (ISO, 2022a).

2.4.2 ISO/IEC 27002

Código de Práticas para Controles de Segurança da Informação: Trata-se de um guia complementar à 27001. Enquanto a ISO 27001 define o que é necessário (requisitos), a ISO 27002 foca em como implementar os controles de segurança sugeridos. A ISO/IEC 27002 fornece orientações para seleção, implementação e gerenciamento dos controles de segurança com base na avaliação de riscos do SGSI (ISO, 2022b).

A versão 2022 da ISO 27002 reorganizou os controles em 4 grandes temas (controles organizacionais, de pessoas, físicos e tecnológicos), totalizando 93 controles, incluindo novos relacionados a ameaças atuais (como prevenção a ataques de engenharia social, segurança de serviços em nuvem, mascaramento de dados, monitoramento de atividades etc.).

Em resumo, a ISO 27002 serve como um catálogo de boas práticas e sugestões de medidas de segurança (por exemplo, como deve ser um procedimento de *backup*, políticas de criptografia, controles de registro de eventos, segurança de dispositivos móveis, dentre outros), que a organização pode adotar para cumprir os objetivos de controle elencados na ISO 27001. Embora não seja certificável, a 27002 é amplamente utilizada como referência para implementação prática de um SGSI e frequentemente citada em auditorias como evidência de boas práticas.

2.4.3 ISO/IEC 27003

Guia para Implementação de SGSI: A norma ISO/IEC 27003 fornece orientações para implementar um SGSI conforme os requisitos da ISO 27001 (ISO, 2017). Ou seja, é um documento voltado a auxiliar organizações no planejamento e implantação inicial do SGSI. Ela cobre aspectos como: obtenção do comprometimento da direção, definição do escopo do SGSI, análise *gap* em relação à 27001, elaboração de cronogramas de projeto, abordagem de análise de riscos, planejamento de tratamento de riscos, estrutura documental (políticas, procedimentos) necessária, entre outros passos para estabelecer o SGSI.

A 27003 funciona como um manual de boas práticas de gestão de projeto para segurança da informação, garantindo que a empresa entenda as etapas e elementos necessários para criar seu sistema de gestão de acordo com a 27001. Essa norma é especialmente útil na fase inicial do projeto, para orientar equipes e *stakeholders* sobre como colocar em prática os controles e processos exigidos, e como integrar o SGSI à cultura organizacional.

Em suma, a 27003 complementa a 27001 detalhando como dar o pontapé inicial em um SGSI eficaz (ISO, 2017).

2.4.4 ISO/IEC 27004

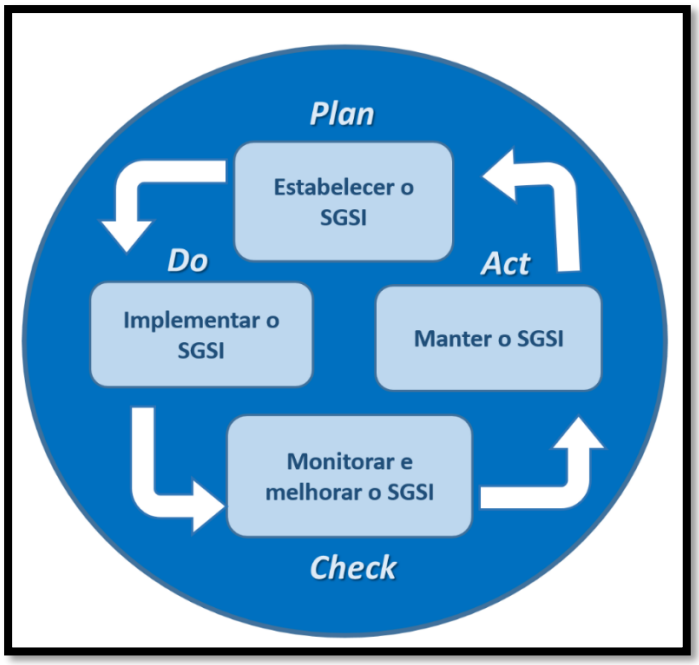
Monitoramento, Medição, Análise e Avaliação do SGSI: A norma ISO/IEC 27004 traz diretrizes para monitorar e medir o desempenho de um SGSI (ISO, 2016).

Seu objetivo é auxiliar as organizações a avaliarem a eficácia do SGSI e dos controles implementados (conforme 27001) por meio de métricas e indicadores quantificáveis. A 27004 orienta na definição de métricas de segurança, na coleta de dados, na análise desses dados e na geração de relatórios que apoiem decisões gerenciais (ISO, 2016). Por exemplo, a organização pode estabelecer métricas como número de incidentes de segurança por mês, tempo médio de resposta a incidentes, porcentagem de servidores em conformidade com *patches* de segurança, entre outras.

A norma discute como garantir que essas medições sejam relevantes para os objetivos de segurança, como interpretá-las e como reportá-las a interessados (diretoria, auditoria etc.).

Em síntese, a ISO 27004 busca instituir uma cultura de melhoria contínua no SGSI, através do ciclo *Plan-Do-Check-Act* (PDCA), ilustrado na Figura 10: planejar controles, implementá-los, medi-los (fase "*Check*" que a 27004 detalha) e então agir para corrigir ou melhorar com base nos resultados. A edição atual é ISO/IEC 27004:2016, e uma nova edição alinhada às revisões de 2022 pode estar em desenvolvimento. Ao aplicar as orientações da 27004, as empresas conseguem quantificar quão bem estão protegendo suas informações e identificar pontos fracos para ajustes (ISO, 2016).

Figura 10 - Ciclo *Plan-Do-Check-Act* aplicado ao Sistema de Gestão de Segurança da Informação.



Fonte: PALMA, 2016

Ao adotar essas normas, as organizações conseguem alinhar suas práticas de segurança a padrões internacionalmente reconhecidos, obter melhoria contínua na proteção de dados e, não raro, cumprir exigências regulatórias ou de mercado que demandam conformidade com boas práticas (ISO, 2022a; ISO, 2022b).

Para o contexto deste trabalho, é relevante notar que a implementação de um *firewall* FortiGate em uma empresa deve idealmente fazer parte de um SGSI abrangente conforme essas normas, por exemplo, controles de rede e comunicações (Anexo A da ISO 27001) preveem o uso de *firewalls*, sistemas de detecção de intrusão e segmentação de redes como medidas de segurança.

Assim, as normas ISO/IEC 27000 oferecem a estrutura macro na qual soluções tecnológicas como o FortiGate se inserem para compor a estratégia de defesa corporativa.

2.5 TRABALHOS RELACIONADOS

2.5.1 SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE *FIREWALL SONICWALL*

O objetivo geral de Masuda (2025) foi identificar e descrever as funcionalidades do *firewall SonicWall* e sua aplicação na segurança de redes de computadores.

Desenvolveu uma pesquisa bibliográfica aliada a uma demonstração prática, configurando um equipamento *SonicWall* (TZ570) em ambiente real. As etapas incluíram acesso e autenticação seguros, configuração de interfaces LAN/WAN, serviços de *Domain Name System* (DNS) e *Dynamic Host Configuration Protocol* (DHCP), criação de políticas de NAT e regras de *firewall*, além de ativação de serviços como *Content Filtering Service* (CFS) e *App Control*.

O autor concluiu-se que o *SonicWall* se apresenta como solução versátil e robusta, com recursos integrados (DPI, CFS, *App Control*) que contribuem para elevar a proteção e a visibilidade do tráfego em redes corporativas.

2.5.2 UM ESTUDO DOS SOFTWARES ENDIAN *FIREWALL* E PFSENSE *FIREWALL*

O objetivo geral de Dourado (2022) foi identificar e descrever as funcionalidades dos *firewalls* pfSense e Endian utilizados em redes de computadores

Realizou-se uma pesquisa de caráter descritivo, com levantamento bibliográfico e análise comparativa das funcionalidades e características dos dois *softwares*.

Concluiu que ambas as soluções oferecem recursos adequados para proteção de redes em diferentes cenários, e que a escolha entre *pfSense* e *Endian* deve considerar necessidades específicas do ambiente (perfil de uso, facilidade de configuração, recursos requeridos), cumprindo o objetivo de mapear e comparar as funcionalidades essenciais.

2.5.3 ESTUDO SOBRE VULNERABILIDADES E IMPLEMENTAÇÃO DE UM CENÁRIO DE SQL *INJECTION*

O objetivo geral da autora Machado (2021) foi identificar e descrever algumas das formas de ataques mais conhecidas aos dados corporativos, apresentando os principais pontos de vulnerabilidade e propondo medidas preventivas para mitigá-las.

Ela realizou uma pesquisa bibliográfica e experimental, abordando ataques como *Port Scanning*, *Phishing*, *Spoofing*, *Sniffing* e *SQL Injection*. Além da parte teórica, a autora desenvolveu um experimento prático de *SQL Injection* utilizando um banco de dados fictício implementado com PostgreSQL e uma aplicação *web* em *Java Platform, Enterprise Edition* (*Java* EE), demonstrando como a exploração de falhas pode comprometer a integridade e confidencialidade das informações.

A autora concluiu que não existe uma única solução capaz de eliminar todas as vulnerabilidades de segurança da informação. No entanto, práticas como o uso de *firewalls*, antivírus, VPNs, treinamento de usuários e a aplicação das normas ISO/IEC 27001 e 27005 são essenciais para fortalecer a segurança das organizações. A pesquisa evidenciou ainda que a conscientização e a implementação de políticas de segurança são tão importantes quanto o uso de ferramentas tecnológicas.

3 PROCEDIMENTOS METODOLÓGICOS

Quanto à natureza é uma pesquisa secundária ou bibliográfica, pois busca obter informações em trabalhos já publicados, como livros, artigos, normas, Trabalhos de Conclusão de Curso e documentações técnicas relacionadas à segurança de redes e firewalls (Wazlawick, 2022).

Quanto aos objetivos esta pesquisa é exploratória. “As pesquisas exploratórias têm como propósito proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito ou a construir hipóteses” (Gil, 2022, p. 42).

Quanto aos procedimentos técnicos: A pesquisa é bibliográfica e experimental.

A pesquisa bibliográfica envolve a análise de artigos, livros, teses, sites e outras fontes de conteúdo publicadas e indexadas em bases de dados, como os periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES). De acordo com Gil (2022), as etapas da pesquisa bibliográfica são:

a) Formulação do problema: Quais são as funcionalidades do *firewall* FortiGate e como ele pode ser configurado para garantir segurança em redes corporativas?

b) Levantamento bibliográfico preliminar: Foram realizadas buscas em Periódicos CAPES e motores acadêmicos para delimitar a importância e a relevância prática do tema.

c) Busca das fontes: Para pesquisa foram selecionados artigos indexados, Trabalhos de Conclusão de Curso (TCC) relacionados, sites técnicos especializados, documentação oficial Fortinet e normas ISO/IEC 27000 pertinentes.

d) Fichamento: Foram realizados resumos analíticos dos materiais, com extração de conceitos-chave e evidências empíricas relevantes ao FortiGate e à segurança de redes.

e) Redação do texto: Refere-se à escrita do TCC.

Pesquisa experimental: A pesquisa experimental visou avaliar o FortiGate 60F em um ambiente corporativo real, por meio da observação das configurações implantadas, da estrutura lógica da rede e dos resultados práticos de funcionamento da solução.

De acordo com Gil (2022), as etapas da pesquisa experimental incluem:

a) Formulação do problema: Foi definido como problema experimental verificar de que forma a implantação do FortiGate 60F poderia contribuir para a organização, proteção, conectividade e monitoramento de uma rede corporativa real, considerando a segmentação lógica da infraestrutura, a interligação segura entre matriz e filial, a redundância dos links externos e a visibilidade operacional proporcionada pela solução.

b) Definição do plano experimental: Foram especificados e documentados os procedimentos de implantação e os critérios de verificação aplicados em ambiente corporativo real, considerando a implantação dos equipamentos FortiGate 60F na matriz e na filial da empresa X. O plano contemplou a análise das configurações aplicadas ao ambiente, com ênfase em políticas de *firewall*/NAT, VPN IPsec entre as unidades, segmentação lógica das redes, controle de tráfego, redundância dos links externos e monitoramento por meio de painéis e visualizações nativas do FortiGate, considerando também a aderência da plataforma às funcionalidades de segurança estudadas no referencial teórico, como IPS, *Web Filtering*, *Application Control* e inspeção SSL/TLS. Também foram definidos critérios para verificar a coerência das políticas aplicadas, a comunicação segura entre matriz e filial, a separação adequada dos segmentos de rede, a disponibilidade dos links externos e a visibilidade operacional do ambiente, relacionando as funcionalidades estudadas no referencial teórico com sua aplicação prática no ambiente analisado, sem exposição de regras específicas ou parâmetros sensíveis.

c) Determinação do ambiente: A implementação foi conduzida em ambiente real da empresa X, aproveitando a infraestrutura existente de rede corporativa. O ambiente inclui um FortiGate 60F físico conectado a segmentos internos (LAN), uma zona desmilitarizada (DMZ) e uma interface WAN para acesso à Internet. Foram considerados servidores, estações de trabalho e serviços reais já existentes no ambiente corporativo, permitindo observar o funcionamento da solução em condições reais de uso.

d) Coleta de dados: As informações foram obtidas por meio de painéis, dashboards e visualizações nativas do FortiGate, observando-se o estado do equipamento, o comportamento do tráfego, as sessões ativas, o uso de recursos, a conectividade entre unidades e a disponibilidade dos links externos. A análise

concentrou-se na verificação qualitativa do funcionamento da solução, sem exposição de logs, regras, endereços ou parâmetros sensíveis do ambiente real.

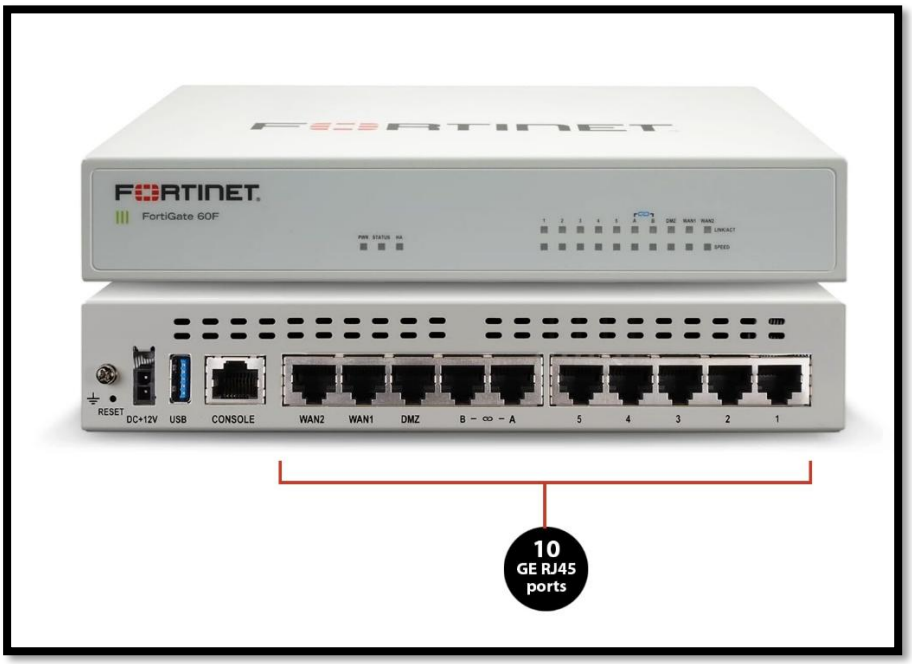
e) Análise e interpretação dos dados: Os resultados obtidos foram analisados para verificar a aderência da solução às necessidades do ambiente corporativo, considerando a organização lógica da rede, a comunicação segura entre unidades, a redundância de conectividade e a visibilidade operacional proporcionada pelo FortiGate 60F.

f) Redação do relatório: redação do TCC.

4 FORTIGATE: ARQUITETURA E FUNCIONALIDADES

O FortiGate é a família de *firewalls* de próxima geração da empresa Fortinet, amplamente utilizada em ambientes corporativos de diversos portes. A Fortinet, fundada em 2000, destacou-se no mercado de segurança ao adotar a arquitetura UTM em seus dispositivos e, nos últimos anos, figura consistentemente como líder em soluções *firewall* corporativo segundo relatórios do *Gartner Magic Quadrant* (Shah e Abid, 2022). Em essência, o FortiGate, exibido na Figura 11, é um *appliance* que combina múltiplas funções de segurança de rede em um único equipamento, operando sobre um sistema operacional próprio, o FortiOS.

Figura 11 - Visão frontal do *firewall* Fortinet FortiGate 60F (*appliance* físico)



Fonte: AMAZON, [s.d.]

Os *firewalls* FortiGate diferenciam-se por uma arquitetura unificada e otimizada por *hardware* especializado. Todos os recursos de segurança (filtro de pacotes, inspeção de conteúdo, VPN, etc.) são gerenciados de forma centralizada pelo FortiOS, o que simplifica a administração e garante integração entre as diversas funções. Além disso, os FortiGates empregam ASICs proprietários, denominados FortiASIC ou *Security Processing Units* (SPUs), para acelerar em *hardware* tarefas intensivas, como inspeção de tráfego em alta velocidade e criptografia. Essa estratégia de *offload* para

chips dedicados permite que o FortiGate mantenha alto *throughput* e baixa latência mesmo com múltiplos serviços de segurança ativados simultaneamente.

Em outras palavras, enquanto muitos *firewalls* concorrentes baseados apenas em CPU enfrentam degradação de desempenho ao habilitar funções como inspeção SSL ou IPS, o FortiGate lida com essas cargas de forma mais eficiente graças aos seus processadores de rede (NP) e de conteúdo (CP) integrados (Fortinet, 2023b). Por exemplo, a quinta geração de SPUs da Fortinet (SP5) consolidou processamento de rede e conteúdo em um único *chip*, oferecendo *firewall* de camada 7 e inspeção avançada com desempenho otimizado e baixo consumo de energia (Fortinet, 2023b).

A arquitetura do FortiGate também se integra ao conceito de *Security Fabric* da Fortinet, apresentada na Figura 12, uma malha de segurança que conecta diversas soluções da marca (*firewall*, *endpoint*, *sandbox*, WI-FI etc.) para compartilhar inteligência e coordenar defesas.

Figura 12 - Diagrama circular do *Security Fabric*

Fonte: Traduzido de FORTINET, 2025

Adicionalmente, o FortiGate possui recursos robustos de alta disponibilidade, permitindo configurar dois ou mais aparelhos em *cluster* redundante (modo ativo-passivo ou ativo-ativo) para garantir que falhas em um dispositivo não interrompam a proteção da rede. Essa capacidade de *failover* automático reforça a confiabilidade da solução em ambientes críticos.

Funcionalidades de segurança: Como um *firewall* de próxima geração, o FortiGate fornece um conjunto extenso de funcionalidades, combinando os papéis antes desempenhados por múltiplos sistemas especializados. Dentre as principais funções e recursos integrados, destacam-se:

4.1 *FIREWALL* E NAT

Filtragem de pacotes *stateful* (inspeção de estado) em todas as interfaces de rede, com políticas configuráveis pelo administrador para permitir, negar ou inspecionar tráfego conforme endereços, portas, protocolo, usuário ou aplicação. Suporte a *Network Address Translation* (NAT) para tradução de endereços, criação de DMZs e segmentação de rede (Fortinet, 2023c).

4.2 VPN

Suporte nativo a VPNs tanto de *site-to-site* (por exemplo, IPsec VPN conectando matrizes e filiais) quanto de acesso remoto (SSL VPN para usuários móveis). O FortiGate provê criptografia forte e autenticação para tunelamento seguro de dados através da *Internet*, permitindo extensão segura da rede corporativa (Fortinet, 2023c).

4.3 IPS

Sistema de prevenção de intrusões integrado, capaz de detectar e bloquear *exploits*, ataques e atividades anômalas na rede em tempo real. O FortiGuard IPS fornece assinaturas atualizadas regularmente para identificar desde varreduras de porta até ataques complexos conhecidos, enquanto o mecanismo de inspeção heurística do FortiGate ajuda a flagrar comportamentos suspeitos desconhecidos (Shah; Abid, 2022). Assim, tráfegos maliciosos podem ser interrompidos antes de alcançar seu destino na rede interna.

4.4 *ANTIMALWARE* (ANTIVÍRUS DE BORDA)

Inspeção *antimalware* do tráfego, analisando arquivos e fluxos de dados em busca de vírus, *trojans*, *spyware* e outras pragas digitais. O FortiGate pode bloquear ou quarentenar conteúdos infectados em trânsito, usando assinaturas de antivírus e técnicas de detecção proativa para ameaças *zero-day* (Shah; Abid, 2022). Essa função amplia a defesa além do perímetro, servindo como uma linha adicional além dos antivírus em *endpoints*.

4.5 *WEB FILTERING* (FILTRO WEB)

Controle de acesso à *web* por categorias de URL. O FortiGate mantém uma base de categorias (atualizada via FortiGuard) que classifica sites como maliciosos, de *phishing*, conteúdos impróprios, redes sociais, *streaming*, etc. Políticas de filtro *web* permitem bloquear, monitorar ou restringir o acesso dos usuários a determinados sites conforme as políticas corporativas (Fortinet, 2023d).

Isso contribui tanto para a segurança (bloqueando sites maliciosos ou de *phishing*) quanto para a produtividade e conformidade (impedindo navegação indevida).

4.6 *APPLICATION CONTROL* (CONTROLE DE APLICAÇÕES)

Capacidade de identificar e controlar aplicações específicas dentro do tráfego de rede, independentemente da porta ou protocolo utilizados. O FortiGate reconhece milhares de aplicações (de serviços corporativos a aplicativos *web* e de rede *peer-to-peer*) (P2P), e permite ao administrador criar regras para bloquear, permitir ou limitar o uso de determinadas aplicações (Fortinet, 2023e).

Por exemplo, é possível bloquear aplicativos de compartilhamento de arquivos P2P ou mensageria instantânea, ou priorizar o tráfego de um aplicativo crítico de negócio. Esse controle granular é um dos atributos chave dos NGFWs e está plenamente presente no FortiGate.

4.7 SSL/TLS *DEEP INSPECTION* (INSPEÇÃO DE TRÁFEGO CRIPTOGRAFADO)

Com a crescente adoção de criptografia, o FortiGate pode atuar ativamente inspecionando comunicações SSL/TLS. Mediante configuração adequada (instalação de certificado de autoridade nas máquinas cliente, por exemplo), o FortiGate realiza decriptação intermediária do tráfego HTTPS ou VPN SSL, analisa o conteúdo em busca de ameaças, e então recriptografa e encaminha ao destino (Fortinet, 2023f; Lekoutovich, 2025).

Graças aos seus processadores de segurança dedicados (SPUs), o FortiGate consegue realizar inspeção profunda de TLS com desempenho altamente superior ao de *firewalls* baseados somente em CPU tradicional (Fortinet, 2023b; Lekoutovich, 2025), reduzindo o "ponto cego" que comunicações criptografadas costumam representar para outras ferramentas de segurança.

4.8 SANDBOX E INTELIGÊNCIA ARTIFICIAL

Integrado ao ecossistema Fortinet, o FortiGate pode encaminhar arquivos suspeitos para análise em *sandbox* (Shah e Abid, 2022). Nessa análise dinâmica, arquivos desconhecidos são executados em ambiente controlado para observar comportamento malicioso, com uso de técnicas de IA/*machine learning* para detecção de ameaças de dia-zero.

As informações de ameaças descobertas são então retornadas ao FortiGate e compartilhadas via FortiGuard para todos os clientes, melhorando continuamente a proteção (Lekoutovich, 2025). O FortiGate também aplica inteligência artificial em outras frentes, como na análise de padrões de tráfego (identificação de *botnets*, anomalias etc.) e otimização de atualização de assinaturas.

Todas essas funcionalidades são geridas através de uma interface unificada de administração (FortiGate GUI/CLI) o que simplifica a operação. Relatórios e logs abrangentes também são fornecidos, permitindo auditoria de eventos de segurança e monitoramento do uso da rede (tentativas de ataque bloqueadas, *websites* acessados, largura de banda consumida etc.).

Conforme destaca a literatura, o FortiGate se sobressai por oferecer ampla cobertura de proteção, gerenciamento simplificado, alto desempenho e visibilidade

unificada de aplicativos, usuários e rede (ESR/RNP, 2022). Em testes independentes, os *firewalls* FortiGate frequentemente alcançam eficácia de segurança próxima a 100% nas categorias avaliadas e *throughput* superior a soluções concorrentes equivalentes, graças aos seus diferenciadores de arquitetura e integração de serviços (Fortinet, 2023b).

Em suma, o FortiGate representa uma solução completa de segurança de rede para ambientes corporativos. Sua arquitetura robusta, com *hardware* customizado (ASICs, FortiASIC) e *software* otimizado (FortiOS), aliada a um portfólio extenso de funcionalidades de NGFW/UTM, permite às empresas implementarem políticas de segurança em profundidade sem renunciar ao desempenho da rede.

Por essas razões, o FortiGate foi definido como objeto central deste trabalho, sendo analisado teoricamente e aplicado em ambiente corporativo real para verificar como suas funcionalidades contribuem para a proteção, organização e conectividade de redes corporativas.

5 ANÁLISE DE CUSTO-BENEFÍCIO ENTRE FORTIGATE E SONICWALL

A análise de custo-benefício foi realizada com foco no contexto de pequenas e médias empresas, nas quais as decisões de investimento em segurança de rede devem considerar não apenas o custo inicial de aquisição, mas também fatores como desempenho, funcionalidades, facilidade de administração, continuidade operacional e custo total ao longo do tempo.

A análise apresentada neste capítulo foi baseada em documentos comerciais recebidos pela Empresa X durante o processo de avaliação e aquisição da solução, preservando-se as informações sensíveis e os dados de identificação das empresas envolvidas.

A empresa X está consolidada no mercado regional há mais de três décadas. Trata-se de uma organização de médio porte, com aproximadamente 300 colaboradores e estrutura composta por uma matriz e uma filial, inserida em um contexto com alta demanda de serviços contínuos de rede, segurança de informação pessoal e transacional e estabilidade na estrutura de TI.

Para fins de padronização da análise comparativa, todos os valores foram apresentados em dólar americano (US$). No caso da proposta de locação originalmente apresentada em reais, foi utilizada como referência a cotação de venda do dólar de setembro de 2025, correspondente a R$ 5,3928 por US$ 1,00.

Na proposta da solução deste trabalho, foram considerados dois *appliances* do modelo FortiGate 60F acompanhados de duas licenças *Unified Threat Protection* (UTP) com validade de 3 anos, totalizando US$ 4.849,88, considerando o mês de setembro de 2025. Na composição detalhada, cada equipamento apresentou um valor unitário de US$ 875,85, enquanto suas licenças trienais ficaram em US$ 1.549,09.

A outra solução estudada e levantada foi o SonicWall TZ370. Foram considerados dois *appliances* também com licenciamento trienal para cada equipamento, totalizando US$ 5.090,00, considerando o mês de agosto de 2025. Na composição detalhada, cada equipamento apresentou valor unitário de US$ 490,00.

Além disso, para cada *appliance*, foram consideradas uma licença trienal *Advanced Protection*, no valor unitário de US$ 1.770,00, e uma licença trienal *SonicWall Analytics Software*, no valor unitário de US$ 285,00. Assim, o total de US$ 5.090,00

resulta da soma de dois equipamentos de US$ 490,00, duas licenças *Advanced Protection* de US$ 1.770,00 e duas licenças *SonicWall Analytics Software* de US$ 285,00.

Contudo, é importante ressaltar que o valor da solução *SonicWall* estava vinculado a uma condição comercial específica de substituição do equipamento antigo TZ350 pelo modelo TZ370, por meio de um programa de fidelização do fabricante. Esse programa prevê um preço especial para upgrade, crédito pelo *appliance* antigo, reduzindo o custo de modernização da infraestrutura.

Adicionalmente, para os dois *appliances* FortiGate 60F, foi apresentada uma alternativa de locação por 36 meses, no valor de R$ 2.909,57 mensais. Para fins de comparação em moeda única, esse valor foi convertido para dólar americano com base na cotação de venda de setembro de 2025, correspondente a R$ 5,3928 por US$ 1,00. Assim, a locação mensal correspondeu a aproximadamente US$ 539,53, resultando em um custo total aproximado de US$ 19.423,03 ao final de 36 meses.

Embora essa opção oferecesse serviços agregados como suporte 24x7x365, monitoramento e licenças UTP, o custo acumulado ao longo do período mostrou-se significativamente superior ao investimento de aquisição.

Assim, a decisão não foi tomada apenas pelo preço nominal, mas pela relação entre custo total, desempenho, abrangência funcional e facilidade de operação. A comparação em dólar evidenciou que, embora a locação incluísse serviços adicionais, seu custo acumulado em 36 meses foi aproximadamente quatro vezes superior ao valor de aquisição dos equipamentos FortiGate 60F com licenças trienais.

Dessa forma, a escolha pela solução FortiGate foi justificada pela melhor relação entre investimento, recursos de segurança, administração centralizada, visibilidade de tráfego e aderência ao ambiente corporativo real analisado neste estudo.

Para pequenas e médias empresas, essa escolha tende a ser mais vantajosa porque esse perfil organizacional geralmente necessita de soluções que conciliem proteção robusta com simplicidade de operação.

O Quadro 1 apresenta um resumo comparativo das duas propostas analisadas, evidenciando os principais aspectos financeiros, técnicos e operacionais observados em cada solução.

Quadro 1 - Comparação de custo-benefício entre as soluções avaliadas

CRITÉRIO	SOLUÇÃO FORTIGATE 60F	SOLUÇÃO SONICWALL TZ370
Custo de aquisição	Valor competitivo considerando equipamento + licença UTP por 3 anos	Valor próximo, porém, condicionado a programa de troca do equipamento antigo
Licenciamento	Licença trienal já prevista na proposta	Licenciamento trienal composto por módulos separados, com valores unitários por *appliance*: *Advanced Protection* e *SonicWall Analytics Software*.
Desempenho	Alto desempenho com aceleração por *hardware* dedicado	Desempenho adequado, porém, sem o mesmo destaque de aceleração por *hardware* no estudo
Abrangência funcional	Forte integração entre *firewall*, VPN, IPS, filtro *web*, *Application Control* e inspeção SSL/TLS	Conjunto robusto de segurança, mas dependente da composição dos módulos licenciados
Facilidade de administração	Administração centralizada e boa visibilidade de tráfego e eventos	Gestão funcional, porém, com menor aderência ao ambiente analisado
Condição comercial	Proposta direta de aquisição	Valor favorecido por programa de *upgrade*/troca do equipamento anterior
Principais desvantagens	Reconfiguração total do novo *firewall* e investimento inicial mais sensível quando comparado à locação mensal	Dependência de condição comercial específica para alcançar o valor apresentado

Fonte: Autoria própria, 2026

Analisando as 2 propostas a solução escolhida pela Empresa X foi o FortiGate. Essa decisão não foi fundamentada apenas pelo valor financeiro, mas principalmente na melhor relação entre desempenho, integração de funcionalidades de segurança, de administração e aderência ao cenário operacional da empresa.

6 CONFIGURAÇÕES E RESULTADOS DO FUNCIONAMENTO DO FORTIGATE

Este capítulo apresenta a implementação prática da solução baseada em FortiGate 60F no ambiente corporativo estudado, com foco nas configurações adotadas, na organização lógica da infraestrutura e nos resultados observados durante o funcionamento da plataforma.

O ambiente foi observado pelo período de 9 meses, durante o qual foram analisados o comportamento da solução implantada, a conectividade entre as unidades, a segmentação lógica da rede, a disponibilidade dos links externos e os recursos de monitoramento e visibilidade do FortiGate.

Para preservar a segurança da empresa analisada, não são expostos neste capítulo endereços IP públicos ou privados, nomes internos de objetos de configuração, credenciais, parâmetros sensíveis de autenticação ou qualquer informação que possa comprometer a integridade do ambiente real da empresa X.

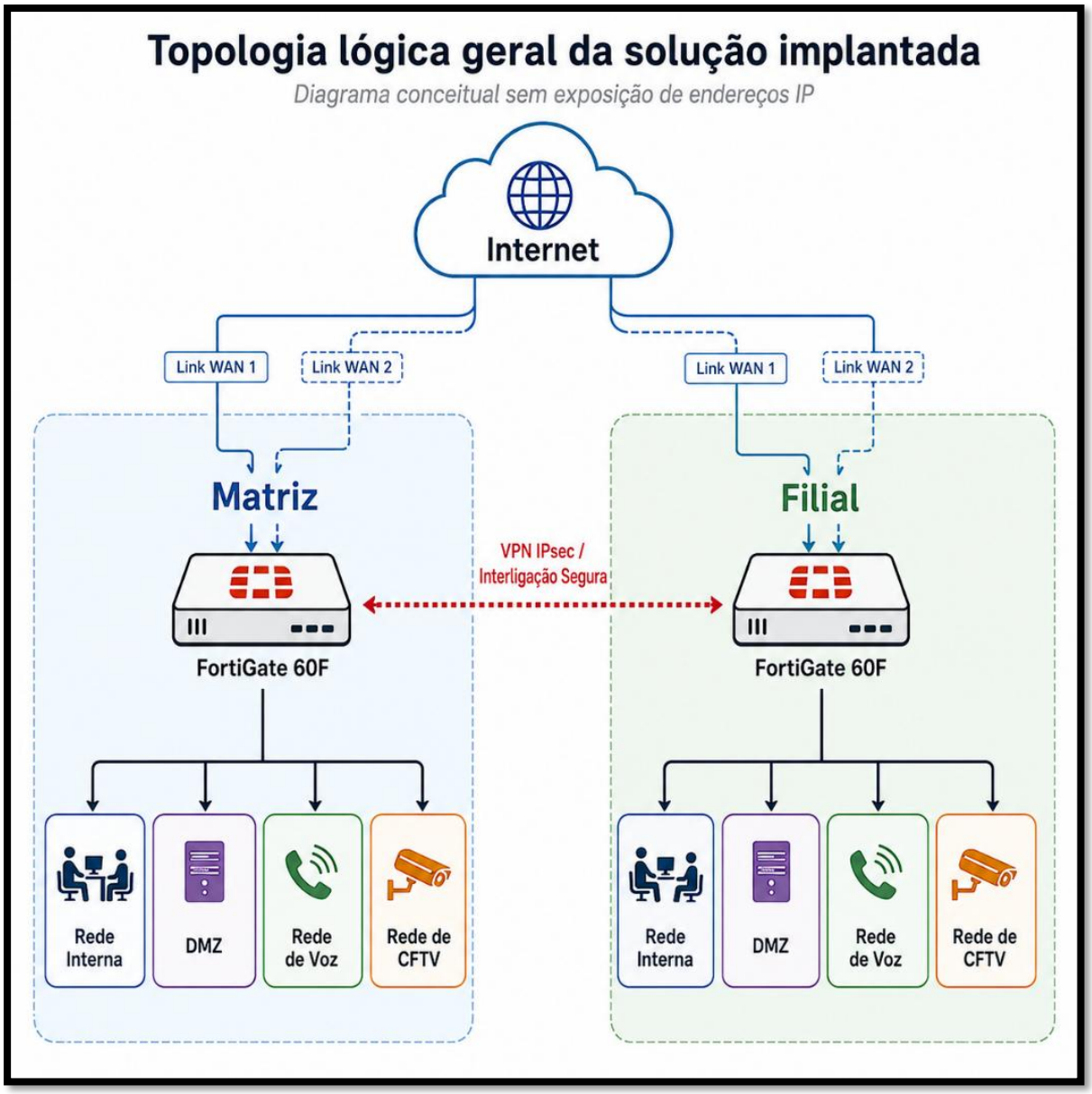
Ainda assim, a descrição técnica foi mantida com nível de detalhamento suficiente para demonstrar a coerência entre o planejamento apresentado no TCC e a implantação efetivamente realizada.

A implementação envolveu dois equipamentos FortiGate 60F, sendo um instalado na unidade principal e outro na unidade filial. A estrutura foi organizada de forma a atender requisitos típicos de pequenas e médias empresas com operação distribuída, como segmentação de redes internas, separação de serviços críticos, comunicação segura entre unidades, conectividade com múltiplos links de Internet e recursos de monitoramento operacional.

Os resultados apresentados a seguir demonstram que o ambiente passou a contar com uma arquitetura mais organizada, maior capacidade de visibilidade sobre o tráfego e melhores condições para aplicação de políticas de segurança de forma centralizada e consistente.

A visão consolidada dessa arquitetura inicial pode ser observada na Figura 13, na qual se destacam a matriz, a filial, os segmentos internos, a DMZ, os links WAN e a interligação segura entre as duas unidades.

Figura 13 - Topologia lógica geral da solução implantada, com matriz, filial, redes internas, zona desmilitarizada, links de rede externa e interligação segura entre unidades



Fonte: Autoria própria, 2026

6.1 ESTRUTURA GERAL DA IMPLEMENTAÇÃO

A implantação foi estruturada em dois pontos principais de segurança perimetral, correspondentes à matriz e à filial. Em ambos os casos, o FortiGate foi configurado como equipamento central de borda, assumindo funções de controle de tráfego, separação lógica de redes, roteamento entre segmentos, suporte à comunicação segura e observabilidade do ambiente.

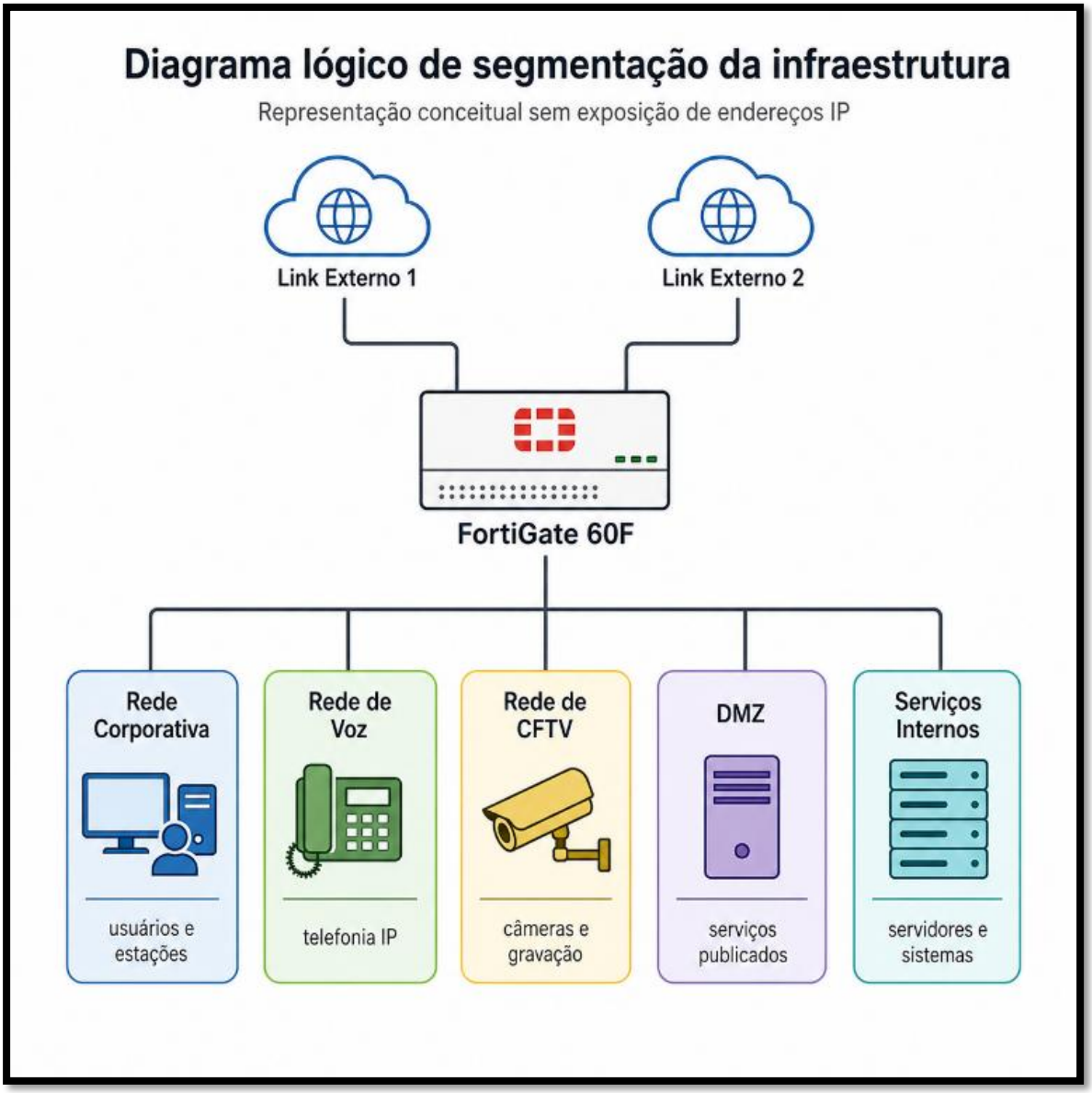
Essa abordagem reforça um dos principais diferenciais da solução: a capacidade de concentrar, em um único equipamento, múltiplas funções que tradicionalmente seriam distribuídas entre diferentes dispositivos de rede e segurança.

Na prática, a implementação seguiu uma arquitetura corporativa típica, em que o *firewall* não atua apenas como barreira de entrada e saída da rede, mas também como elemento organizador da infraestrutura interna.

A presença de múltiplos segmentos lógicos, túneis entre unidades e painéis nativos de monitoramento confirma que a solução foi implantada de maneira aderente ao ambiente real da empresa e ao objetivo do estudo, que consiste em analisar como o FortiGate pode ser configurado para garantir segurança em redes corporativas.

A organização geral apresentada se desdobra, no plano lógico, na segmentação da infraestrutura, como mostrado na Figura 14. Nela, é possível perceber a separação dos principais domínios de serviço e o papel do *firewall* como elemento central dessa arquitetura.

Figura 14 - Diagrama lógico de segmentação da infraestrutura em rede corporativa, voz, circuito fechado de televisão, zona desmilitarizada e links externos



Fonte: Autoria própria, 2026

Essa representação reforça que a segmentação adotada não foi apenas uma decisão técnica, mas também funcional, pois distribui os serviços de acordo com sua finalidade operacional e favorece a aplicação de controles mais específicos entre os diferentes ambientes.

6.2 ORGANIZAÇÃO DAS INTERFACES E SEGMENTAÇÃO DA INFRAESTRUTURA

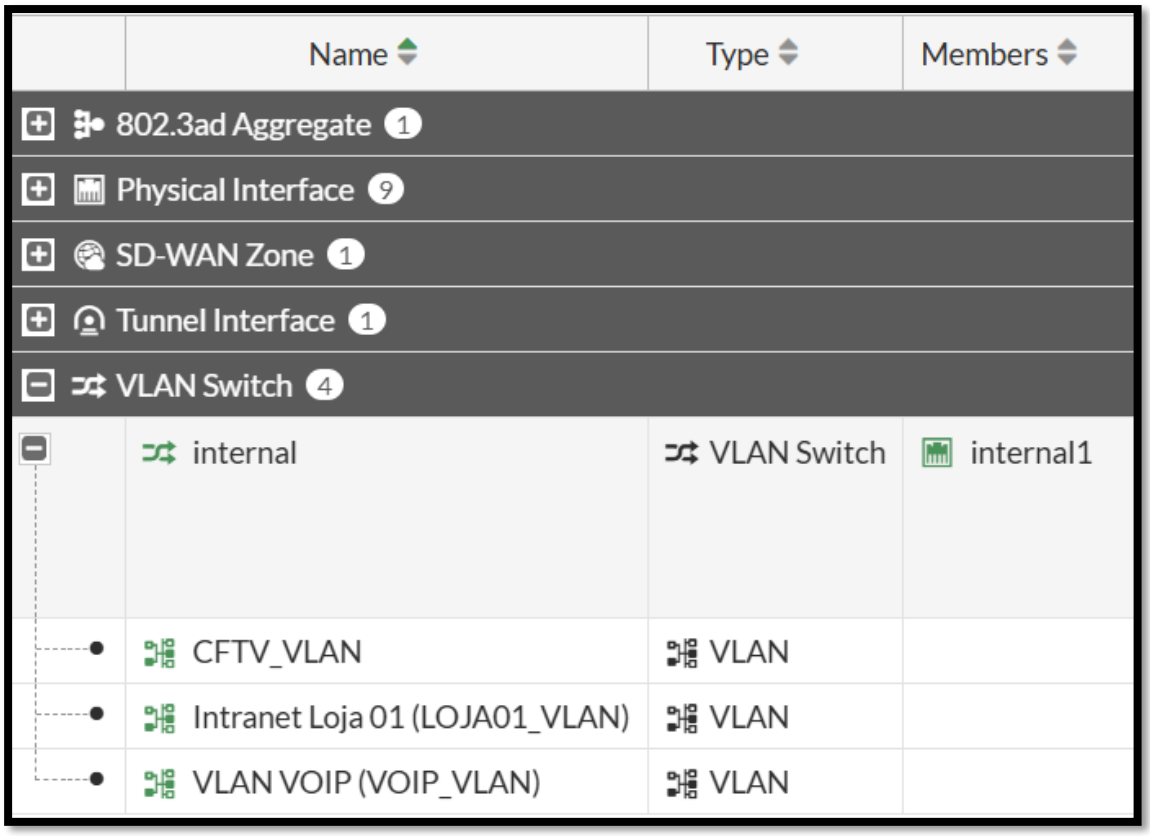
Um dos principais resultados práticos observados foi a adoção de uma política de segmentação lógica da rede. Em vez de concentrar todos os ativos em uma única rede plana, a implantação separou os serviços por finalidade operacional, criando domínios distintos para a rede corporativa principal, comunicação de voz, sistema de videomonitoramento, área desmilitarizada e enlaces de comunicação externa.

Essa segmentação melhora o controle de tráfego, reduz a propagação de incidentes entre setores diferentes e facilita a aplicação de políticas específicas de acesso e segurança.

Do ponto de vista técnico, essa organização mostra aderência às boas práticas discutidas no referencial teórico, especialmente no que se refere à separação por níveis de confiança e à limitação do alcance de possíveis falhas ou ataques.

Em ambientes com múltiplos serviços simultâneos, como dados corporativos, telefonia IP, Circuito Fechado de Televisão (CFTV) e acesso à Internet, essa separação é especialmente importante para manter previsibilidade operacional e reduzir interferências entre os serviços, como visto na Figura 15. Assim, o *firewall* deixa de ser apenas uma barreira perimetral e passa a exercer também o papel de elemento estruturante da rede interna.

Figura 15 - Exemplo da tela de interfaces do FortiGate com os segmentos lógicos já organizados



Fonte: Autoria própria, 2026

A disposição das interfaces no equipamento acompanha a lógica de segmentação descrita anteriormente, reforçando a aderência entre o planejamento da solução e sua implementação efetiva. Essa organização também contribui para simplificar a administração do ambiente e tornar mais clara a aplicação das políticas por segmento.

6.3 REDUNDÂNCIA DE CONECTIVIDADE E DISPONIBILIDADE OPERACIONAL

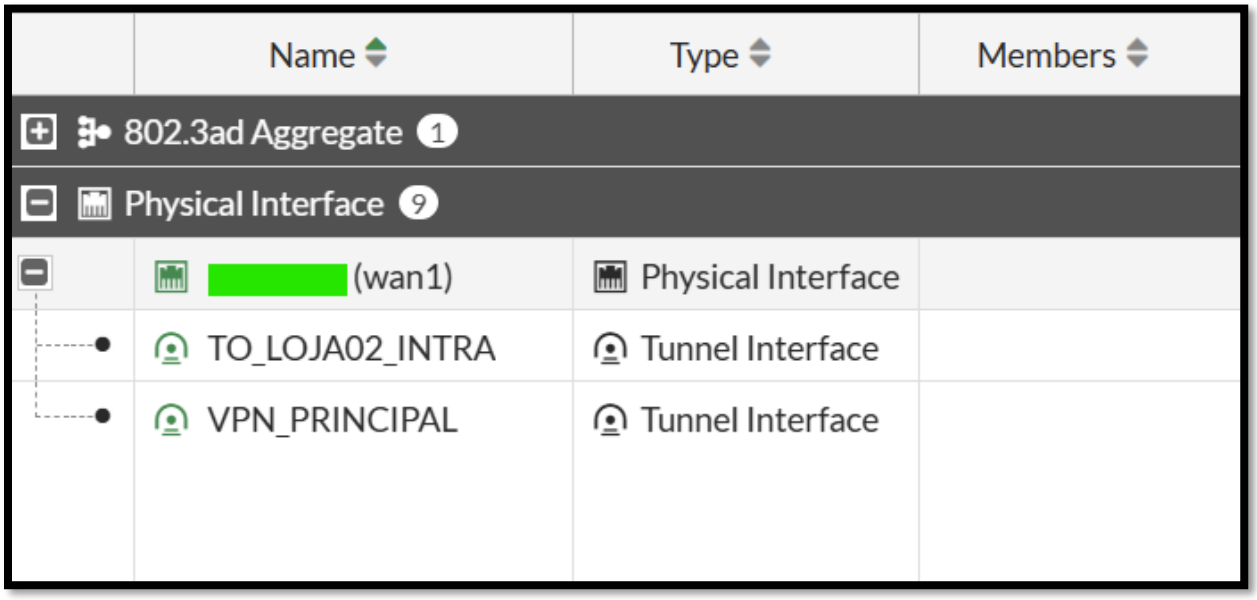
A implementação também contemplou uma estrutura de múltiplos links de Internet, permitindo que cada unidade operasse com mais de uma possibilidade de saída externa. Em cenários corporativos, essa redundância é relevante porque reduz a dependência de um único provedor e amplia a capacidade de continuidade operacional em caso de indisponibilidade parcial.

No caso estudado, a coexistência de dois enlaces WAN por unidade representa uma estratégia coerente com a necessidade de manter serviços administrativos, comerciais e de comunicação em funcionamento contínuo.

Além da existência dos dois links, a configuração também indica o uso de mecanismos de acompanhamento do estado da conectividade, o que reforça a capacidade do equipamento de avaliar a saúde dos enlaces e apoiar o roteamento de tráfego de forma mais inteligente.

A organização das interfaces de rede externa pode ser observada na Figura 16, que apresenta a tela de configuração das interfaces utilizadas para a conectividade externa do FortiGate.

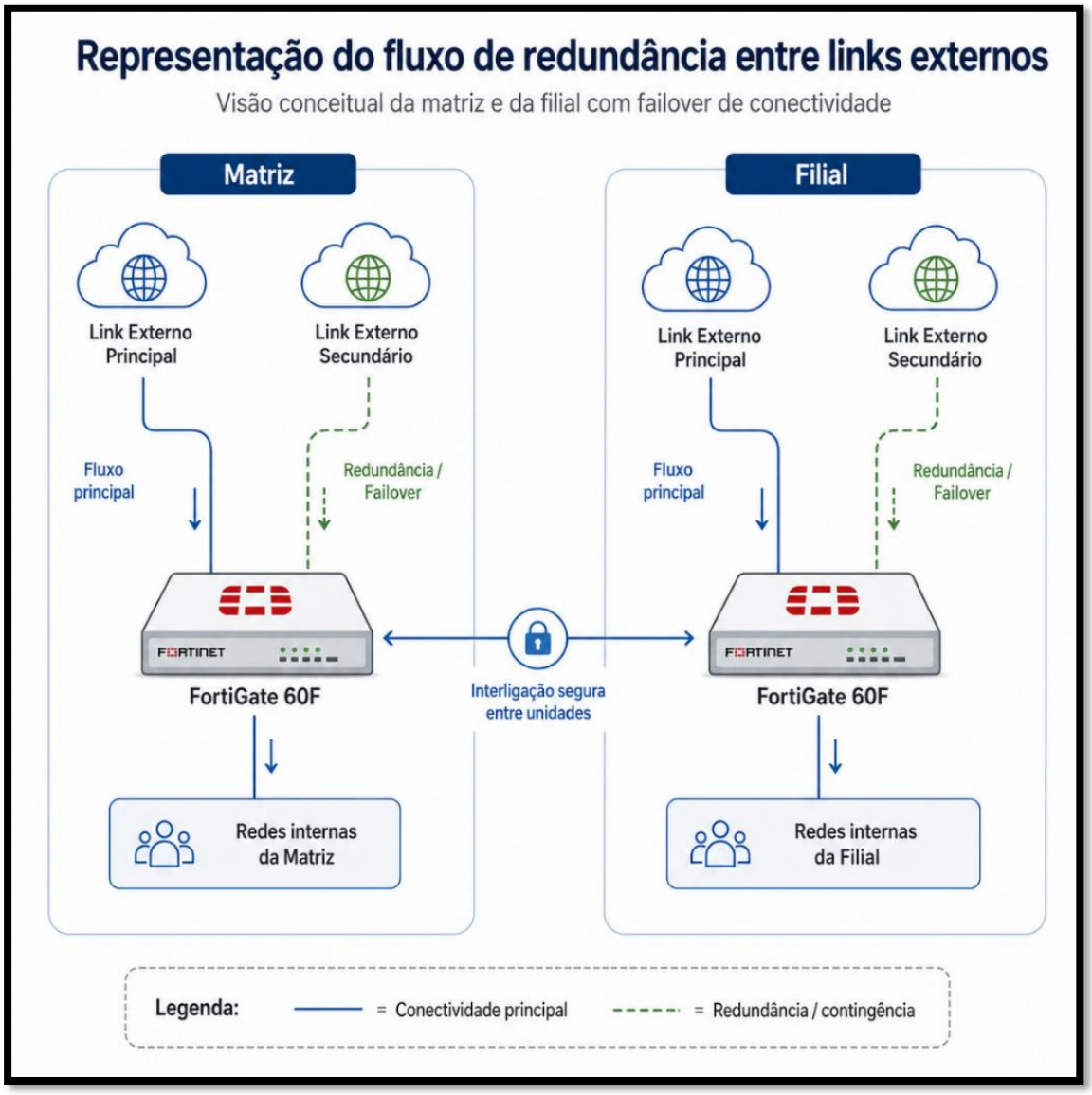
Figura 16 - Tela de configuração das interfaces de rede externa do FortiGate



Fonte: Autoria própria, 2026

De forma complementar, a Figura 17 sintetiza o fluxo de redundância entre os links externos da matriz e da filial, evidenciando a lógica de contingência utilizada para ampliar a disponibilidade operacional do ambiente.

Figura 17 - Representação do fluxo de redundância entre links externos na matriz e na filial.



Fonte: Autoria própria, 2026

A conectividade foi estruturada com foco em continuidade de operação, reduzindo a dependência de um único enlace e oferecendo melhores condições de resiliência para os serviços corporativos em caso de falha parcial.

6.4 COMUNICAÇÃO SEGURA ENTRE MATRIZ E FILIAL

Outro resultado importante foi a implementação de comunicação segura entre as duas unidades da empresa por meio de túneis VPN *site-to-site*. Essa configuração permitiu interligar matriz e filial de forma criptografada, garantindo troca de informações internas sem exposição direta dos dados na Internet pública.

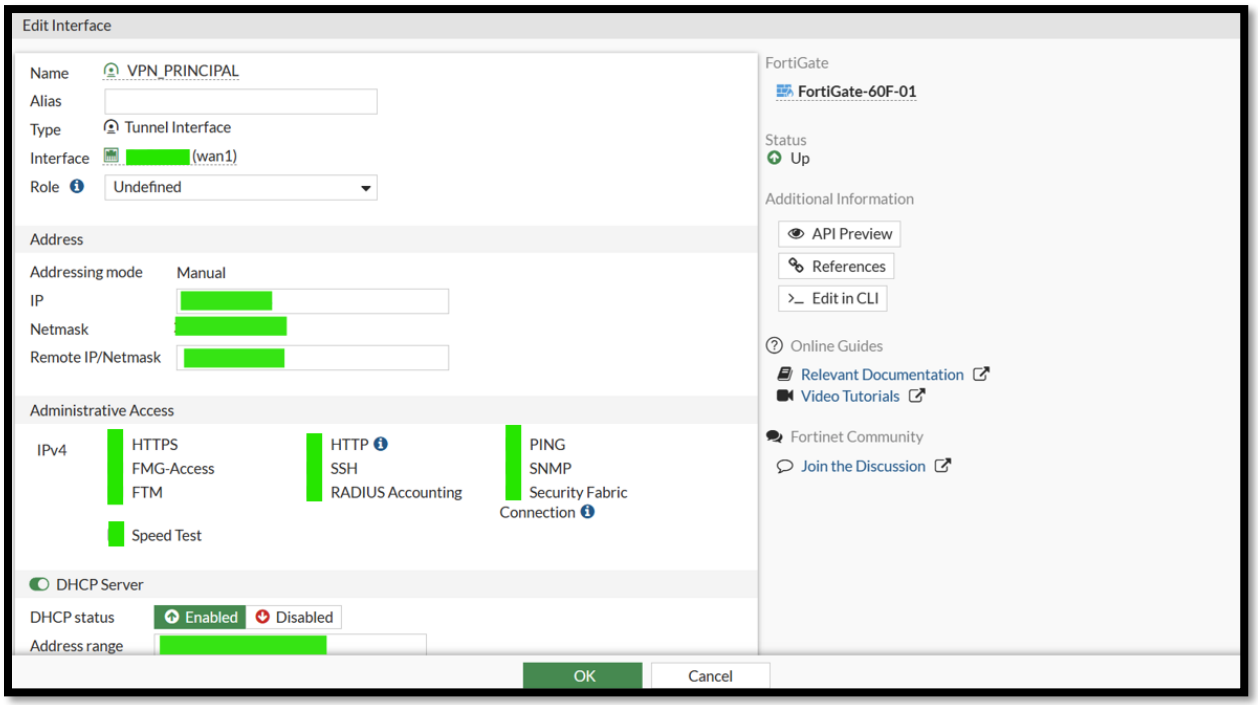
A presença dessa comunicação segura era um dos objetivos operacionais centrais do projeto, pois a empresa depende da integração entre unidades para funcionamento de sistemas, compartilhamento de recursos e padronização de políticas de segurança.

A interligação foi estruturada de modo segmentado, contemplando comunicação entre redes equivalentes das duas unidades e respeitando a separação lógica dos serviços. Essa organização aumenta o controle sobre o que trafega entre matriz e filial e reduz a exposição desnecessária de segmentos que não precisam de comunicação direta.

Em termos práticos, isso significa que a VPN não foi implementada apenas como um túnel genérico, mas como um mecanismo alinhado à arquitetura da empresa, permitindo acesso interunidades de forma mais precisa e segura.

Um dos elementos associados à comunicação segura entre as unidades pode ser observado na Figura 18, que apresenta a tela de edição da interface de túnel utilizada na estrutura de VPN do FortiGate. A configuração completa da VPN *site-to-site*, incluindo parâmetros de Fase 1 e Fase 2, não é exposta neste trabalho, a fim de preservar informações sensíveis do ambiente real.

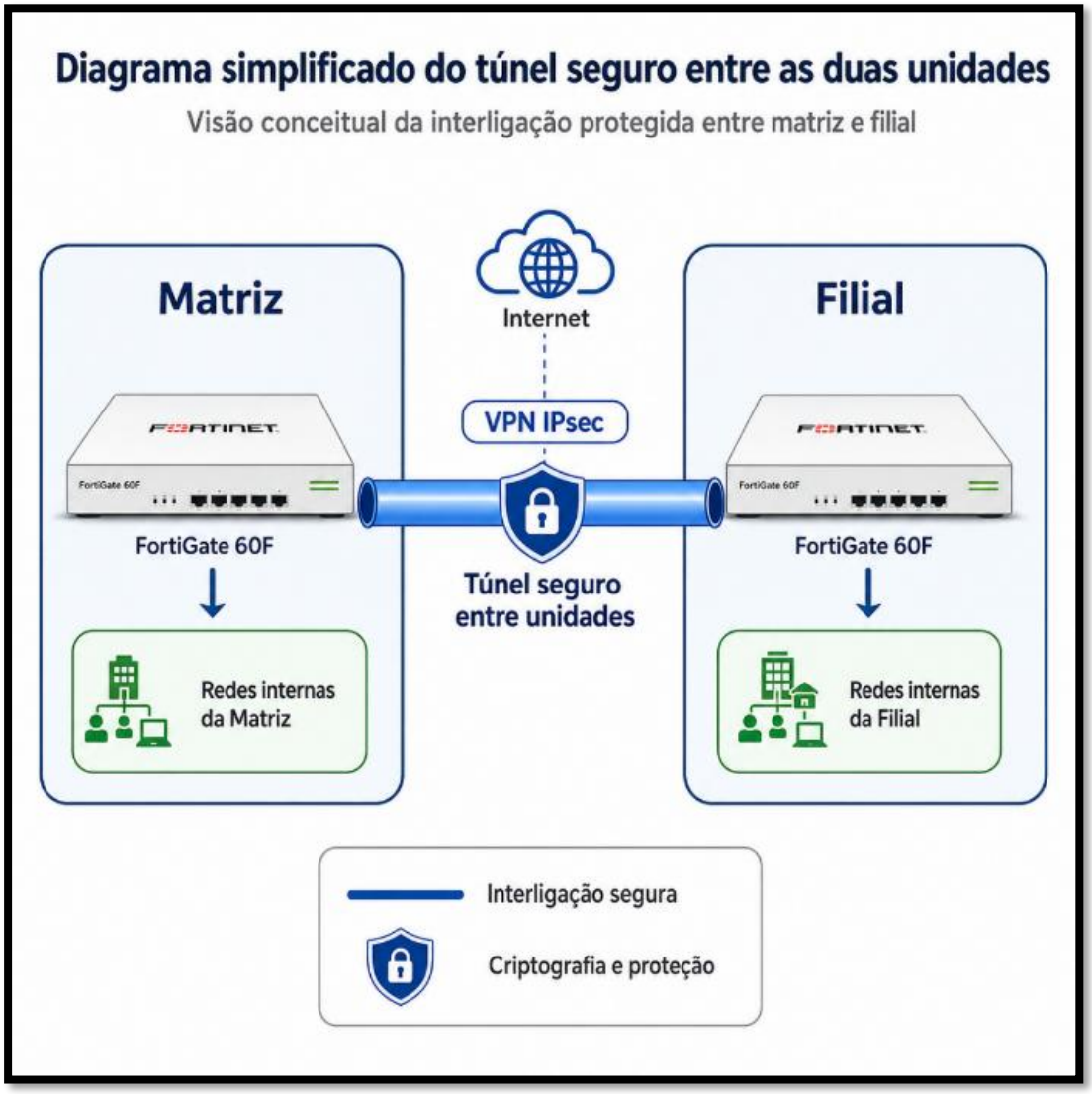
Figura 18 - Tela de edição de interface de túnel utilizada na estrutura de VPN do FortiGate.



Fonte: Autoria própria, 2026

Já a Figura 19 apresenta uma representação simplificada do túnel seguro estabelecido entre matriz e filial, destacando a função da VPN como mecanismo de interligação protegida entre as duas unidades.

Figura 19 - Diagrama simplificado do túnel seguro entre as duas unidades.



Fonte: Autoria própria, 2026

6.5 ADMINISTRAÇÃO CENTRALIZADA E PAINÉIS DE MONITORAMENTO

A implementação evidenciou também o uso dos recursos nativos do FortiOS para acompanhamento do funcionamento da rede e dos eventos de segurança. Os equipamentos foram configurados com *dashboards* que permitem visualização do estado geral do dispositivo, uso de CPU, memória, sessões ativas, conectividade de VPN, comportamento da rede, inventário de dispositivos e painéis voltados à segurança e ao tráfego.

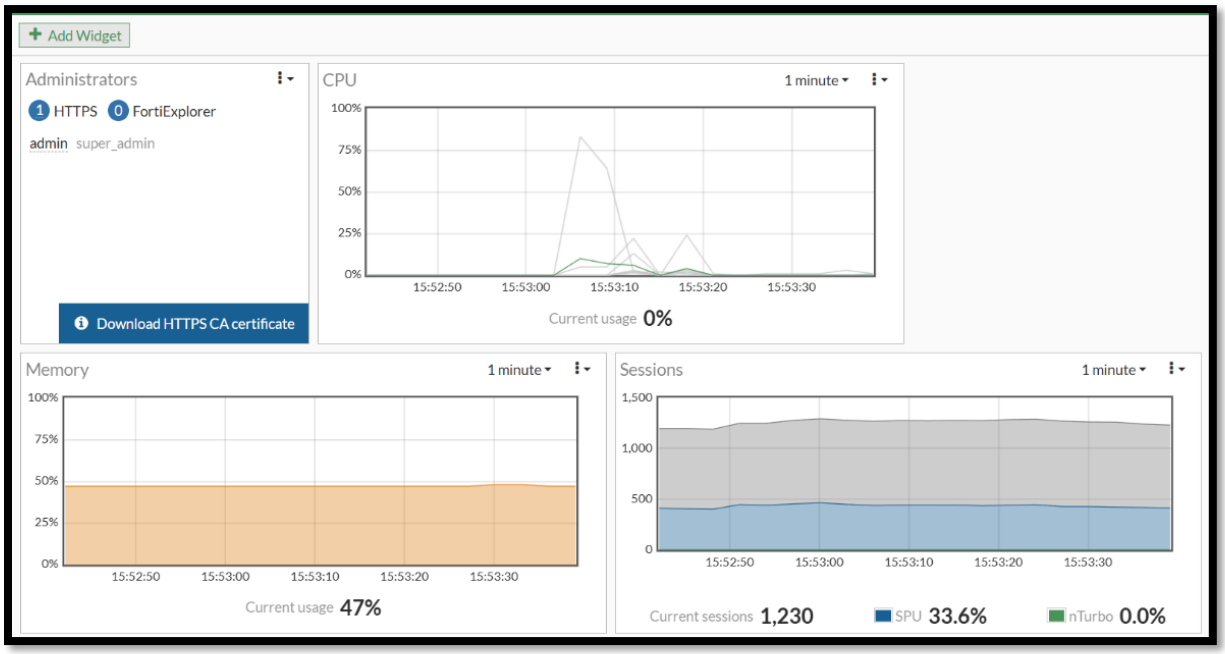
Esse conjunto de recursos é relevante porque transforma o *firewall* em um ponto central de observabilidade da infraestrutura, permitindo que o administrador identifique tendências, anomalias e impactos das políticas aplicadas.

A presença de painéis do tipo *FortiView*, voltados à análise por origem, destino, aplicações, *websites*, políticas e sessões em tempo real, reforça a visibilidade operacional da solução. Em pequenas e médias empresas, isso representa uma vantagem importante, pois a equipe de TI costuma ser mais enxuta e necessita de ferramentas que concentrem diagnóstico, monitoramento e gestão em uma mesma interface.

Desse modo, a implementação confirma, na prática, uma das premissas do TCC: o FortiGate não atua apenas como equipamento de bloqueio de tráfego, mas como uma plataforma completa de controle e acompanhamento do ambiente de rede.

Os recursos de administração e visibilidade descritos nesta subseção podem ser observados a partir da Figura 20, que evidencia informações operacionais relevantes do equipamento em tempo real.

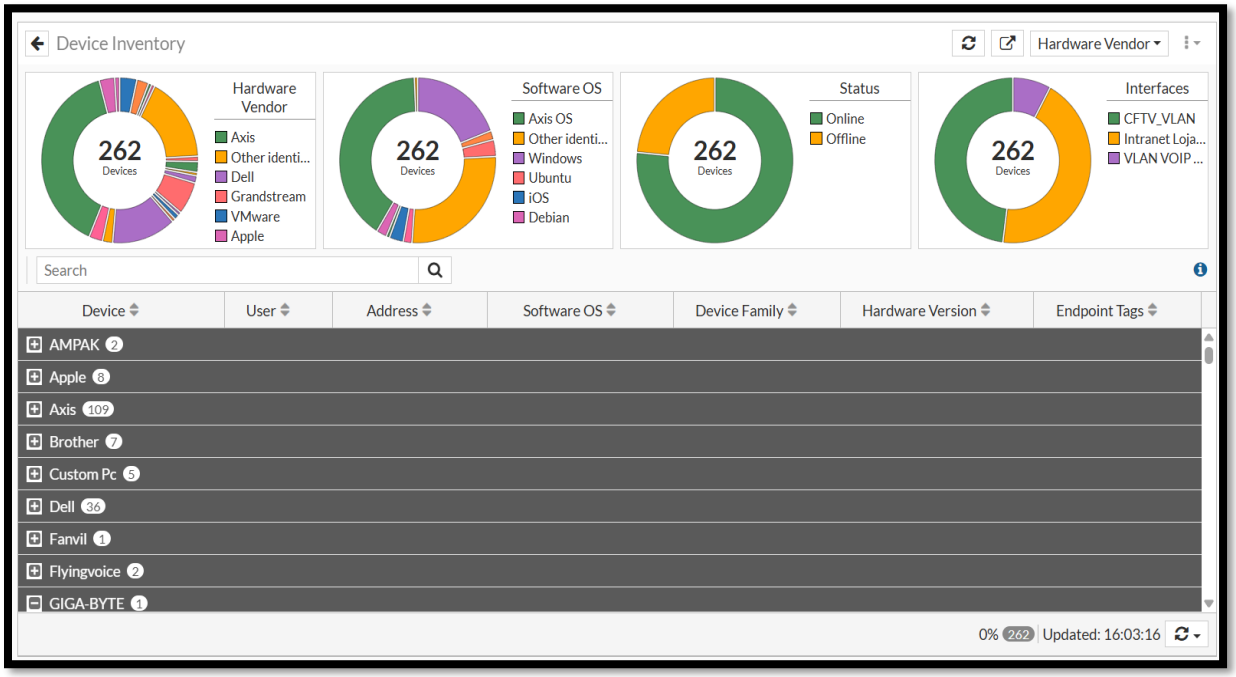
Figura 20 - *Dashboard* de status do FortiGate com uso de unidade central de processamento, memória e sessões.



Fonte: Autoria própria, 2026

Na sequência, a Figura 21 complementa essa visão ao apresentar informações relacionadas aos usuários e softwares identificados na rede, ampliando a capacidade de acompanhamento do ambiente.

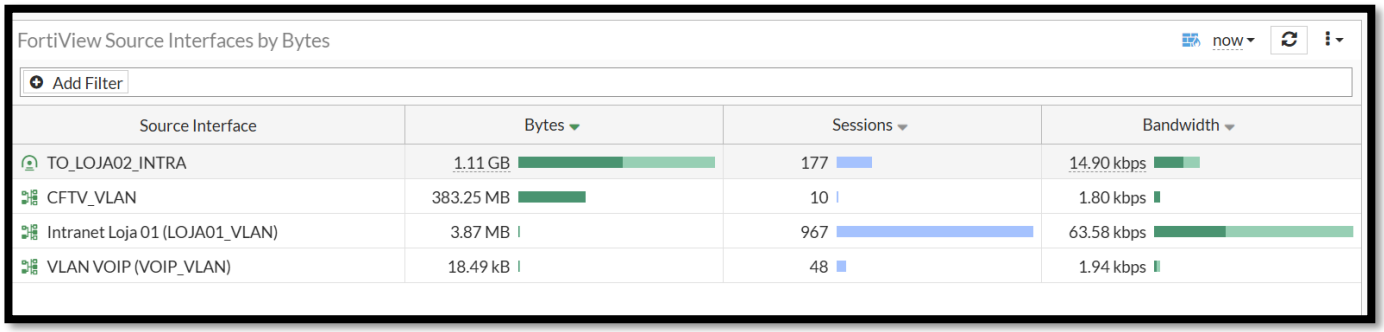
Figura 21 - *Dashboard* de usuários e *softwares* identificados na rede



Fonte: Autoria própria, 2026

Por sua vez, a Figura 22 destaca o comportamento do tráfego por interface, permitindo visualizar a distribuição do uso de banda e a atividade dos enlaces monitorados.

Figura 22 - *Dashboard* de uso de b*ytes* por interface



Fonte: Autoria própria, 2026

O FortiGate, no ambiente implantado, não atua somente como elemento de filtragem, mas também como plataforma de observabilidade, reunindo informações operacionais que apoiam o diagnóstico, o monitoramento e a tomada de decisão administrativa.

6.6 FUNCIONALIDADES OBSERVADAS NO AMBIENTE IMPLANTADO

As configurações analisadas confirmam que o ambiente foi preparado para utilizar, além das funções básicas de roteamento e segmentação, recursos avançados do próprio FortiGate. Entre eles, destacam-se o suporte a políticas de filtragem, o uso de túneis seguros, o acompanhamento de tráfego por meio de *dashboards* e o preparo da plataforma para operar com funcionalidades mais amplas de segurança já discutidas no referencial teórico, como controle de aplicações, inspeção de tráfego e visibilidade detalhada por serviço.

Ainda que o capítulo não exponha regras específicas nem políticas sensíveis, a estrutura observada demonstra que o equipamento foi implantado de modo compatível com o uso corporativo real e com o perfil de segurança exigido pela empresa.

Do ponto de vista de funcionamento, os principais ganhos observados foram: maior organização da rede, controle mais claro sobre os serviços internos, comunicação segura entre unidades, capacidade de monitoramento centralizado e melhor base para futuras ações de segurança.

Esses resultados não significam que a proteção depende exclusivamente do equipamento, mas mostram que a configuração adotada cria condições mais adequadas para aplicação consistente de políticas e para resposta mais rápida a problemas operacionais ou incidentes de segurança.

6.7 RESULTADOS PRÁTICOS OBSERVADOS

Sob a perspectiva dos resultados, a implementação demonstrou que o FortiGate 60F atendeu ao objetivo de estruturar uma solução de segurança funcional para uma empresa de pequeno e médio porte com duas unidades.

A segmentação lógica da infraestrutura, a interligação segura entre matriz e filial e a disponibilidade de painéis operacionais representam evidências concretas de que a solução foi corretamente incorporada ao ambiente real.

Além disso, a presença de recursos de monitoramento e administração centralizada indica que o equipamento oferece não apenas proteção, mas também governança operacional sobre a rede.

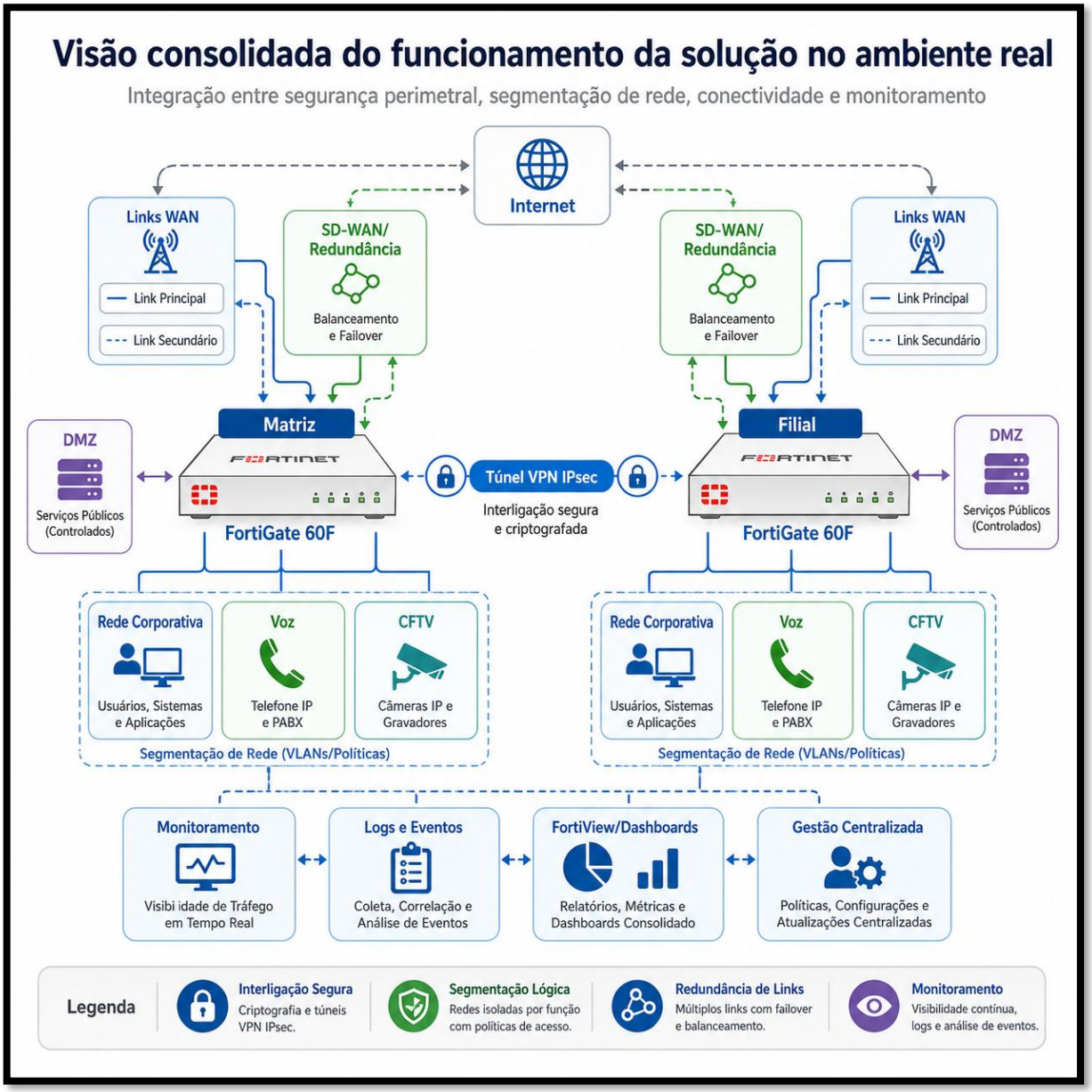
Também se observou que a solução implantada possui potencial para apoiar etapas futuras de análise quantitativa, uma vez que a plataforma oferece base para coleta de logs, eventos, sessões, comportamento de aplicações e indicadores de uso dos recursos do equipamento.

Portanto, mesmo preservando informações sensíveis, é possível afirmar que os resultados do funcionamento confirmam a viabilidade do FortiGate como solução de segurança e conectividade para pequenas e médias empresas que necessitam integrar unidades, segmentar serviços e manter maior controle sobre sua infraestrutura de rede.

A síntese dos principais elementos descritos ao longo deste capítulo pode ser observada na Figura 23, que apresenta uma visão consolidada do funcionamento da solução no ambiente real.

Ressalta-se que os resultados apresentados possuem caráter qualitativo e estrutural, pois se concentram na validação da implantação, da segmentação lógica, da interligação segura, da redundância de conectividade e da visibilidade operacional. A análise quantitativa aprofundada de desempenho, bloqueios, eventos históricos e comportamento de aplicações foi reservada como possibilidade de continuidade do estudo.

Figura 23 - Visão consolidada do funcionamento da solução no ambiente real.



Fonte: Autoria própria, 2026

Dessa forma, a figura finaliza o capítulo ao integrar, em uma única visão, os aspectos de segurança perimetral, segmentação lógica, conectividade entre unidades, redundância de links e monitoramento contínuo, evidenciando a coerência entre o projeto proposto, a implementação realizada e os resultados observados no funcionamento da solução.

7 CONCLUSÃO

Este trabalho teve como finalidade responder à seguinte questão de pesquisa: **quais são as funcionalidades do *firewall* FortiGate e como ele pode ser configurado para garantir segurança em redes corporativas?** A partir da revisão teórica, da análise comparativa entre soluções de mercado e da implementação prática em ambiente corporativo real, foi possível concluir que o FortiGate constitui uma solução robusta, tecnicamente consistente e adequada para atender às demandas de segurança, conectividade e administração de redes em pequenas e médias empresas.

No referencial teórico, verificou-se que o FortiGate reúne, em uma única plataforma, recursos típicos de *firewalls* de próxima geração, como filtragem *stateful*, inspeção profunda de pacotes, controle de aplicações, VPNs seguras, prevenção e detecção de intrusões, filtro *web* e inspeção de tráfego criptografado, além de mecanismos avançados de visibilidade e administração centralizada.

Esses recursos, aliados à arquitetura baseada em FortiOS e aceleração por hardware dedicado, confirmam sua relevância como solução de segurança perimetral e de segmentação lógica em ambientes corporativos.

A análise de custo-benefício desenvolvida no Capítulo 5 também reforçou a coerência da escolha da solução adotada. Embora ambas as propostas avaliadas apresentassem características técnicas relevantes, a alternativa escolhida demonstrou melhor equilíbrio entre custo de aquisição, abrangência funcional, facilidade de operação, previsibilidade de investimento e aderência ao cenário real da empresa analisada.

Para organizações de pequeno e médio porte, esse equilíbrio é particularmente importante, pois a decisão tecnológica precisa considerar não apenas o preço nominal, mas também a sustentabilidade operacional e a simplificação da gestão da infraestrutura de TI.

No plano prático, os resultados observados no Capítulo 6 demonstraram que a implementação do FortiGate 60F atendeu ao objetivo de estruturar uma solução funcional de segurança para uma empresa com duas unidades. A segmentação lógica da infraestrutura, a comunicação segura entre matriz e filial, a presença de redundância

de conectividade e a utilização de painéis operacionais confirmaram que o equipamento foi incorporado ao ambiente de forma coerente com os requisitos da organização.

Além disso, a implantação evidenciou que o FortiGate não atua apenas como barreira de proteção perimetral, mas também como elemento organizador da rede, apoiando o controle dos serviços internos, a visibilidade do tráfego e a administração centralizada do ambiente.

Outro aspecto relevante é que a solução implementada demonstrou potencial para apoiar atividades contínuas de monitoramento e governança da segurança, uma vez que oferece base para acompanhamento de sessões, visualização de tráfego, análise de comportamento de aplicações e consulta futura a logs e eventos, sem necessidade de exposição de informações sensíveis do ambiente.

Mesmo sem expor dados sensíveis ou detalhes confidenciais da configuração real, os resultados apresentados são suficientes para demonstrar a viabilidade do FortiGate como solução de segurança e conectividade em cenários corporativos distribuídos, especialmente quando há necessidade de integrar unidades, segmentar serviços e manter controle operacional mais amplo sobre a rede.

Dessa forma, conclui-se que o objetivo geral do trabalho foi alcançado, uma vez que foi possível identificar, descrever e analisar as funcionalidades do FortiGate, bem como demonstrar sua aplicação prática em um ambiente corporativo real. O estudo também evidencia que a eficácia dessa solução não depende exclusivamente do equipamento em si, mas da forma como ele é configurado, monitorado e integrado às políticas de segurança da organização.

Assim, o FortiGate mostrou-se não apenas uma ferramenta tecnológica de proteção, mas uma plataforma estratégica para o fortalecimento da segurança da informação em redes corporativas.

Para continuidade deste trabalho, sugerem-se como trabalhos futuros:

- Ampliar a análise quantitativa do ambiente implantado, explorando indicadores de desempenho sob carga, latência, consumo de recursos do equipamento e comportamento da rede em diferentes cenários de uso;

- Avaliar o comportamento de aplicações específicas, verificando como políticas de *Application Control*, filtro *web* e inspeção de tráfego impactam diferentes tipos de serviços utilizados no ambiente corporativo;
- Analisar estatísticas históricas de eventos de segurança, considerando registros de tentativas de acesso indevido, bloqueios realizados, alertas gerados e ocorrências identificadas pelos mecanismos de proteção do FortiGate;

Esses desdobramentos podem aprofundar a compreensão sobre o uso do FortiGate em ambientes corporativos reais e fortalecer sua avaliação comparativa com outras soluções de *firewall* de próxima geração.

REFERÊNCIAS

AHMED, U.; KHAN, S.; RAHMAN, A. ***Case of Palo Alto and Fortigate Firewall: performance analysis of Next-Generation Firewalls*.** 2021. Disponível em: < https://www.researchgate.net/publication/365435690_Study_to_analyse_compare_and_evaluate_the_performance_of_next_general_firewalls_Case_of_Palo_Alto_and_Fortigate_Firewall>. Acesso em: 28 set. 2025.

AMAZON. ***FortiGate-60F Firewall Appliance - 10 Gigabit Ethernet RJ45 Ports, Includes DMZ, WAN & Internal Ports (Appliance Only, No Subscription) (FG-60F)***. [s.d.]. Disponível em: <https://www.amazon.com/Fortinet-FortiGate-Firewall-Throughput-Protection/dp/B07ZZMFWJ7>. Acesso em: 6 abr. 2026.

ASER. ***Firewall* UTM – Aser *Security***. Disponível em: <https://www.aser.com.br/servicosgerenciaveis/firewall-utm/>. Acesso em: 11 nov. 2025.

BHARTIYA, D.; JINDAL, A. ***Advanced Network Security Solutions***. [S.l.]: Springer, 2021.BORN, Amanda. **O que é *firewall* e seu papel na segurança da informação**. Disponível em: <https://vcx.solutions/o-que-e-firewall-e-seu-papel-na-seguranca-da-informacao/>. Acesso em: 27 out. 2025

BRASIL**. Política Nacional de Segurança da Informação**. [s.d.]. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategias-e-politicas-digitais/politica-nacional-de-seguranca-da-informacao>. Acesso em: 11 jun. 2026.

CISCO SYSTEMS, INC. **O que é um *firewall*?** 2023. Disponível em: <https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 21 set. 2025.

CISCO SYSTEMS, INC. **Protocolos básicos de rede na compreensão do modelo OSI.** Disponível em: <https://community.cisco.com/t5/artigos-gerais/protocolos-b%C3%A1sicos-de-rede-na-compreens%C3%A3o-do-modelo-osi/ta-p/4802414>. Acesso em: 27 out. 2025.

CISCO SYSTEMS, INC. ***Understand the Zone-Based Policy Firewall Design***. 2025. Disponível em: <https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/98628-zone-design-guide.html>. Acesso em: 28 set. 2025.

DOURADO, R. S. **Um estudo dos softwares *Endian Firewall* e *PFSense Firewall***. Monografia (Graduação em Segurança da Informação) – Escola Politécnica, Pontifícia Universidade Católica de Goiás, Goiânia, 2022.

ESR/RNP – Escola Superior de Redes / Rede Nacional de Ensino e Pesquisa. **O que é FortiGate e qual sua importância para a Segurança Corporativa?** 2022. Disponível em: <https://esr.rnp.br/seguranca/o-que-e-fortigate/>. Acesso em: 28 set. 2025.

FORTINET. **Application Control (Admin/Docs)**. 2023e. Disponível em: https://docs.fortinet.com. Acesso em: 28 set. 2025.

FORTINET. **FortiGate *Next-Generation Firewalls*.** 2023. Disponível em: <https://www.fortinet.com/products/next-generation-firewall>. Acesso em: 21 set. 2025.

FORTINET. **Fortinet *Secure Processors* (SPU)**. 2023b. Disponível em: <https://www.fortinet.com/products/fortigate/fortiasic>. Acesso em: 28 set. 2025.

FORTINET. **FortiGate VPN *capabilities* (Admin/Docs)**. 2023c. (Documento técnico/guia do produto). Disponível em: <https://docs.fortinet.com>. Acesso em: 28 set. 2025.

FORTINET. **Glossário: Definição de *firewall***. 2023a. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/firewall>. Acesso em: 28 set. 2025.

FORTINET. **Security Fabric**. Disponível em: <https://www.fortinet.com/br/solutions/enterprise-midsize-business/security-fabric>. Acesso em: 27 out. 2025.

FORTINET. **SSL/TLS *Inspection* (Admin/Docs)**. 2023f. Disponível em: <https://docs.fortinet.com>. Acesso em: 05 set. 2025.

FORTINET. ***Web Filtering* (Admin/Docs)**. 2023d. Disponível em: <https://docs.fortinet.com>. Acesso em: 28 set. 2025.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 7. ed. Rio de Janeiro: Editora Atlas Ltda, 2022.

HOOGENRAAD, Wim. **O que é uma zona desmilitarizada (DMZ)?** Disponível em: <https://pt.itpedia.nl/2023/01/28/wat-is-een-demilitarized-zone-dmz/>. Acesso em: 27 out. 2025.

IBM SECURITY; PONEMON INSTITUTE. ***Cost of a Data Breach Report*** 2023. IBM, 2023.

ISO. *ISO/IEC 27000:2018 —* ***Information technology — Security techniques — Information security management systems — Overview and vocabulary*****. Genebra: International Organization for Standardization**, 2018.

ISO. *ISO/IEC 27001:2022 —* ***Information Security Management Systems — Requirements*****. Genebra: International Organization for Standardization**, 2022a.

ISO. *ISO/IEC 27002:2022 —* ***Information security controls*****. Genebra: International Organization for Standardization**, 2022b.

ISO. *ISO/IEC 27003:2017 —* ***Information Security Management Systems — Guidance*****. Genebra:** ***International Organization for Standardization***, 2017.

ISO**.** *ISO/IEC 27004:2016 —* ***Information Security Management — Monitoring, measurement, analysis and evaluation***. Genebra: International Organization for Standardization, 2016.

KUROSE, J. F.; ROSS, K. W. ***Computer Networking: A Top-Down Approach***. 8. ed. Boston: Pearson, 2020.

LEKOUTOVICH, M. ***Key Features & Benefits of FortiGate Firewalls: and how a Managed Service maximizes them***. 2025. Disponível em: <https://balanced.plus/key-features-benefits-of-fortigate-firewalls/>. Acesso em: 28 set. 2025.

LNCC - LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA. **Os quatro pilares da segurança da informação – Confidencialidade, Disponibilidade, Integridade e Autenticidade.** 2024. Disponível em: <https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-

informacao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade>. Acesso em: 11 jun. 2026.

MACHADO, B. C. **Estudo sobre vulnerabilidades e implementação de um cenário de SQL *Injection***. 2021. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) – Escola Politécnica, Pontifícia Universidade Católica de Goiás, Goiânia, 2021.

MASUDA, D. S. **Segurança de redes de computadores: um estudo sobre *firewall SonicWall***. 2025. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) — Pontifícia Universidade Católica de Goiás, Goiânia, 2025.

NIST. SP 800-41 Rev. 1: ***Guidelines on Firewalls and Firewall Policy***. Gaithersburg, MD: *National Institute of Standards and Technology*, 2009. Disponível em: <https://csrc.nist.gov/pubs/sp/800/41/r1/final>. Acesso em: 28 set. 2025.

NIST. SP 800-125B: ***Secure Virtual Network Configuration for VM Protection***. Gaithersburg, MD: *National Institute of Standards and Technology*, 2016. Disponível em: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-125b.pdf>. Acesso em: 28 set. 2025.

PALMA, Fernando. **Sistema de Gestão de Segurança da Informação (SGSI)**. Disponível em: <https://www.portalgsti.com.br/2016/12/sistema-de-gestao-de-seguranca-da-informacao-sgsi.html>. Acesso em: 27 out. 2025.

PATEL, U. ***The Role of Next-Generation Firewalls in Modern Network Security: A Comprehensive Analysis*. *International Journal of Advanced Research in Engineering and Technology (IJARET)***, v. 15, n. 4, p. 135-154, 2024.

PRONNUS. **O que é Next Generation *Firewall* e Quais são Suas Vantagens?** Disponível em: <https://pronnus.com.br/blog/o-que-e-next-generation-firewall-e-quais-sao-suas-vantagens/>. Acesso em: 11 nov. 2025.

RECEITA FEDERAL DO BRASIL. **Tabelas para conversão de dólar em 2025**. 2025. Disponível em: <https://www.gov.br/receitafederal/pt-br/assuntos/meu-imposto-de-renda/tabelas/conversao/2025>. Acesso em: 11 jun. 2026.

RIBEIRO. **Quais os Tipos de *Firewall***. Disponível em: <https://blog.qd7.com.br/quais-os-tipos-de-firewall/>. Acesso em: 11 nov. 2025.

SHAH, N.; ABID, M. ***Fortinet scores highest in three use cases in the 2022 Gartner critical capabilities report for network firewalls***. Fortinet Blog, 31 jan. 2022. Disponível em: <https://www.nomios.com/news-blog/fortinet-gartner-networks-firewalls-report/>. Acesso em: 21 set. 2025.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. ***Computer Networks***. 6. ed. Harlow: Pearson, 2021.

THAPA, R. M.; PAUL, S. ***Cybercrime Management: The Role of Cybersecurity Education and Training***. *International Journal of Innovative Science and Research Technology*, v.9, n.11, p.650-657, 2024.

WAZLAWICK, R. S. **Metodologia de pesquisa para ciência da computação**. [S. l.]: Elsevier Editora Ltda., 2022.

ANEXO B – Termo de autorização de publicação de produção acadêmica

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 Willian Miranda Mendes do Curso de Engenharia de Computação, matrícula 20212003300272, telefone: (62) 99826-4569, e-mail willian.mendes3131@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 SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE FIREWALL FORTIGATE EM AMBIENTES CORPORATIVOS , 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, 28 de MARÇO de 2026.

Documento assinado digitalmente
gov.br WILLIAN MIRANDA MENDES
Data: 28/03/2026 19:59:20-0300
Verifique em https://validar.iti.gov.br

Assinatura do autor: _____

Nome completo do autor: Willian Miranda Mendes

Assinatura do professor–orientador: _____ Documento assinado digitalmente gov.br SOLANGE DA SILVA Data: 02/06/2026 19:22:55-0300 Verifique em https://validar.iti.gov.br _____

Nome completo do professor-orientador:Solange da Silva_