PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS

ESCOLA POLITÉCNICA E DE ARTES

GRADUAÇÃO EM CIÊNCIAS DA COMPUTAÇÃO

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE O FIREWALL SONICWALL

DANIEL SOARES MASUDA

GOIÂNIA,

2025

DANIEL SOARES MASUDA

SEGURANÇA DE REDES DE COMPUTADORES: UM ESTUDO SOBRE FIREWALL SONICWALL

Trabalho de Conclusão de Curso apresentado à Escola politécnica, da Pontifícia Universidade Católica de Goiás, como parte dos requisitos para obtenção do título de Bacharel em Ciência da Computação

Orientadora:
Profa. Dra. Solange daSilva.
Banca Examinadora:
Prof. Me. Rafael Leal Martins
Prof. Me. Anibal Rodrigues Jukemura

GOIÂNIA,
2025

DANIEL SOARES MASUDA

FIREWALL SONICWALL PARA SEGURANÇA DE REDES DE COMPUTADORES DOMÉSTICAS E CORPORATIVAS

Trabalho de Conclusão de Curso aprovado em sua forma final pela Escola Politécnica e de Artes, da Pontifícia Universidade Católica de Goiás, para obtenção do título de Bacharel em Engenharia da Computação, em: 02/12/2025.

Banca Examinadora:

_____

Orientadora: Profa. Dra. Solange da Silva

_____

Prof. Me. Rafael Leal Martins

_____

Prof. Me. Anibal Rodrigues Jukemura

GOIÂNIA

2025

AGRADECIMENTO

Agradeço primeiramente a **Deus**, por me dar forças para continuar minha caminhada acadêmica, mesmo diante dos desafios.

À minha mãe, **Josevânia Soares Da Silva Masuda**, pelo apoio incondicional e pelos ensinamentos que sempre me motivaram a seguir em frente. Seu incentivo e dedicação foram fundamentais para que eu chegasse até aqui.

À **PUC GO**, pelo programa de bolsa de estudos social, que me proporcionou a oportunidade de estudar em uma instituição de grande prestígio, aliviando parte dos desafios financeiros dessa jornada.

À minha estimada orientadora, **Profa. Dra. Solange da Silva**, pela paciência, conhecimento compartilhado e por todo o suporte ao longo deste trabalho. Sua orientação foi essencial para meu crescimento acadêmico e profissional.

Aos meus familiares e amigos, que estiveram ao meu lado nos momentos difíceis, oferecendo palavras de incentivo e apoio incondicional.

E a todos que, direta ou indiretamente, contribuíram para que este trabalho fosse concluído com sucesso. Meu sincero agradecimento!

RESUMO

O objetivo geral deste trabalho foi identificar e descrever as funcionalidades do *firewall* SonicWall, destacando sua aplicação na segurança de redes corporativas. Para alcançar esse objetivo, realizou-se uma pesquisa bibliográfica fundamentada em normas e estudos anteriores, além da implementação prática em um *firewall* físico do modelo SonicWall TZ570. Quanto aos aspectos metodológicos, esta pesquisa, em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental.

Durante o desenvolvimento do trabalho, foram executadas configurações práticas no SonicWall, envolvendo desde a definição de um IP fixo para acesso à interface administrativa até a aplicação de políticas de segurança como filtragem de conteúdo e controle de aplicativos. Em seguida, foram realizados testes para validar essas configurações, incluindo tentativas de acesso a sites bloqueados, utilização de aplicativos restritos e simulações de ataques externos. Os resultados comprovaram a eficácia do *firewall* na aplicação das políticas de segurança definidas, garantindo controle granular sobre o tráfego e aumentando a proteção da rede. O estudo permitiu concluir que *firewall*s de próxima geração, como o SonicWall, desempenham papel fundamental na segurança da informação, oferecendo não apenas inspeção de pacotes, mas também funcionalidades integradas de filtragem e prevenção contra ameaças. Além disso, constatou-se que a aplicação de normas como a ISO/IEC 27000 é essencial para estabelecer diretrizes de segurança consistentes. No entanto, uma limitação do estudo foi a não utilização de testes em ambientes com alta demanda ou redes distribuídas, o que poderia ampliar a avaliação sobre o desempenho do dispositivo em cenários complexos. Além disso, conclui-se da importância da utilização de ferramentas robustas e devidamente configuradas para proteger redes corporativas.

Palavras-chave: *Firewall*, SonicWall, segurança da informação, filtragem de conteúdo, Segurança de Redes.

ABSTRACT

The main objective of this study was to identify and describe the functionalities of the SonicWall *firewall*, emphasizing its application in corporate network security. To achieve this goal, a bibliographic research was conducted based on standards and previous studies, alongside the practical implementation of a physical SonicWall TZ570 firewall. This process made it possible to understand how advanced resources such as *Content Filtering Service* (CFS), *App Control*, NAT and *Geo-IP Filtering* can be applied to mitigate cyber risks and protect data against unauthorized access, malware and distributed attacks (VIEIRA, 2021). During the development of the study, practical configurations were carried out on the SonicWall, starting from the definition of a fixed IP address for administrative access to the application of security policies such as content filtering and application control. Tests were then performed to validate these configurations, including attempts to access blocked websites, the use of restricted applications and simulations of external attacks. The results confirmed the effectiveness of the firewall in enforcing the defined security policies, ensuring granular control over traffic and increasing network protection. The study concluded that next-generation firewalls such as SonicWall play a fundamental role in information security, offering not only packet inspection but also integrated filtering and threat prevention functionalities. It was also verified that the application of standards such as ISO/IEC 27000 is essential to establish consistent security guidelines. However, a limitation of this study was the absence of tests in high-demand or distributed network environments, which could further evaluate the device's performance in complex scenarios. Nevertheless, the importance of using robust and properly configured tools to protect corporate networks is reinforced.

Keywords: Firewall, SonicWall, information security, content filtering, Network Security.

LISTA DE SIGLAS

Sigla	Significado
ABNT	Associação Brasileira de Normas Técnicas
CFS	*Content Filtering Service*
CIA	Confidencialidade, Integridade e Disponibilidade
DDoS	*Distributed Denial of Service*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DPI	*Deep Packet Inspection*
DMZ	*Demilitarized Zone*
HTTP	*HyperText Transfer Protocol*
HTTPS	*HyperText Transfer Protocol Secure*
IDS	*Intrusion Detection System*
IPS	*Intrusion Prevention System*
IP	*Internet Protocol*
IPSec	*Internet Protocol Security*
ISO/IEC	*International Organization for Standardization / International Electrotechnical Commission*
LAN	*Local Area Network*
NGFW	*Next Generation Firewall*
PNAD	Pesquisa Nacional por Amostra de Domicílios
QoS	*Quality of Service*
SGSI	Sistema de Gestão de Segurança da Informação
SSL	*Secure Sockets Layer*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TCC	Trabalho de Conclusão de Curso
TZ	SonicWall TZ Series
UTM	*Unified Threat Management*
VPN	*Virtual Private Network*

Sigla	Significado
WAN	*Wide Area Network*
X0 / X1	Interfaces padrão do SonicWall (LAN/WAN)

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Redes de computadores são um conjunto de dispositivos conectados por uma tecnologia que permite a troca de informações entre eles. Quando dois ou mais computadores estão conectados e trocando informações, já se pode considerar uma rede. Essa conexão pode ocorrer por meio de cabos físicos ou tecnologias sem fio, como redes ópticas, ondas de infravermelho e satélites. Existem redes de diversas formas e modelos, cada um operando sob suas próprias regras. Quando interligadas, essas redes formam estruturas maiores, sendo a Internet o maior exemplo de uma rede global (Molina, Silveira & Rodrigues, 2019).

Conforme Santos (2021), a Segurança da Informação (SI) refere-se ao conjunto de práticas e estratégias para proteger dados contra acessos não autorizados, garantindo que as informações permaneçam íntegras e disponíveis apenas para usuários autorizados. Em um cenário onde ataques cibernéticos são cada vez mais frequentes, proteger esses dados é essencial para evitar prejuízos tanto financeiros quanto operacionais.

Um *firewall* é um dispositivo de segurança essencial nesse contexto, pois monitora o tráfego de entrada e saída de uma rede e decide permitir ou bloquear pacotes de dados com base em regras predefinidas pelo administrador (CISCO, 2023). *Firewall*s são amplamente utilizados em redes domésticas e corporativas para impedir acessos não autorizados e evitar vulnerabilidades que possam comprometer sistemas e dados sensíveis (Molina, 2018).

Com o avanço da tecnologia, o uso da Internet se tornou indispensável para diversas atividades, como transações bancárias, comunicação corporativa e armazenamento de informações críticas. Isso aumentou a dependência humana da tecnologia e, consequentemente, os riscos de ataques cibernéticos (Silva, 2010). Para mitigar esses riscos, a implementação de soluções de segurança eficazes, como *firewall*s, tornou-se uma necessidade primordial para empresas e usuários individuais (Dourado, 2022).

O SonicWall é um dos *firewalls* mais utilizados no mercado, sendo amplamente empregado em ambientes corporativos devido às suas funcionalidades avançadas, como filtragem de pacotes, prevenção contra intrusões (IDS/IPS), configuração de VPNs seguras e monitoramento de tráfego em tempo real. Sua implementação garante uma camada extra de proteção contra ataques e acessos indevidos,

permitindo que as organizações tenham maior controle sobre sua infraestrutura de rede.

A SonicWall é uma precursora da segurança cibernética com mais de 30 anos de experiência e um foco incansável em seus parceiros. Com a capacidade de criar, dimensionar e gerenciar a segurança em ambientes de nuvem, híbridos e tradicionais em tempo real, a SonicWall pode fornecer soluções de segurança específicas de forma rápida e econômica para qualquer organização em todo o mundo.

Com base em dados de seu próprio centro de pesquisa de ameaças, a SonicWall oferece proteção perfeita contra os ataques cibernéticos mais evasivos e fornece inteligência de ameaças acionável para parceiros, clientes e a comunidade de segurança cibernética.

Além disso, a escolha do SonicWall como objeto deste estudo se justifica tanto por sua ampla adoção no ambiente corporativo quanto pelo equilíbrio entre funcionalidades avançadas e custo-benefício. No mercado de firewalls de próxima geração, dispositivos como Fortinet FortiGate, Cisco Firepower, Sophos XG Firewall e soluções *open source* como PfSense também são amplamente utilizados.

Entretanto, o SonicWall destaca-se por oferecer uma combinação de desempenho, facilidade de administração, variedade de recursos de segurança integrados (como CFS, *App Control* e Geo-IP Filtering) e um custo geralmente mais acessível quando comparado a concorrentes diretos da categoria corporativa. Enquanto soluções como Cisco *Firepower* e Fortinet costumam apresentar valores mais elevados devido ao licenciamento e à complexidade de implantação, o SonicWall entrega funcionalidades semelhantes com menor investimento inicial e manutenção mais simples, sendo frequentemente escolhido por empresas de médio porte que buscam um firewall robusto, escalável e com boa relação entre custo e desempenho.

Dessa forma, a análise do SonicWall torna-se relevante não apenas por sua presença no mercado, mas também por representar uma alternativa viável e economicamente competitiva em comparação às demais opções disponíveis.

Justifica-se estudar este tema porque a segurança da informação é um dos pilares fundamentais das infraestruturas de TI modernas, e os *firewall*s de nova geração, como o *SonicWall*, desempenham papel essencial na prevenção de ataques e no controle de tráfego de rede. Diante do aumento constante de ameaças cibernéticas, compreender as funcionalidades e as formas de configuração desse

equipamento é essencial para garantir a integridade, disponibilidade e confidencialidade dos dados corporativos. Além disso, o estudo contribui para a formação de profissionais capacitados a implementar soluções eficazes de segurança, promovendo boas práticas e fortalecendo a proteção das redes empresariais.

Diante deste contexto, este trabalho visa responder a seguinte questão de pesquisa: - **Quais são as funcionalidades do *firewall* SonicWall 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* SonicWall e sua aplicação na segurança de redes de computadores.

Os Objetivos Específicos são:

- Descrever a configuração inicial do *firewall* Sonicwall.
- Apresentar as funcionalidades do *firewall* SonicWall.
- Implementar e testar funcionalidades como VPN, *Proxy* e Regras de *Firewall* para avaliar sua eficácia.

Espera-se que os resultados deste trabalho possam contribuir:

- Informando aos administradores de redes corporativas sobre a importância do SonicWall como uma solução de segurança eficaz para proteção de redes;
- Trazendo informações sobre configurações e boas práticas de segurança para os usuários de redes de computadores;
- Mostrando a importância da implementação de Políticas de Segurança da Informação dentro de uma empresa e apresentando as normas de segurança existentes.

Quanto aos aspectos metodológicos, esta pesquisa, em relação aos procedimentos técnicos, é uma pesquisa bibliográfica e experimental.

Esta monografia está organizada em 7 capítulos, sendo estruturada da seguinte forma: o Capítulo 1 traz a introdução com o contexto do trabalho, a questão de pesquisa, objetivos e resultados esperados. Capítulo 2 apresenta o referencial teórico com conceitos, definições e trabalhos relacionados ao tema. O capítulo 3 traz os procedimentos metodológicos, explicando como e o que foi feito para atingir o objetivo geral. O capítulo 4 apresenta a descrição do *Firewal* SonicWall, abordando suas funcionalidades e características principais. O capítulo 5 traz a configuração prática do SonicWall, incluindo VPN, *proxy* e regras de *firewall*. O capítulo 6 mostra

os resultados dos testes e validações. Finalmente, o capítulo 7 apresenta as considerações finais.

2. REFERENCIAL TEÓRICO

Este capítulo é composto de duas partes: a primeira apresenta conceitos e definições da área, e a segunda traz alguns trabalhos relacionados ao tema.

2.1 Segurança da Informação

A Segurança da Informação (SI) refere-se à proteção de dados pertencentes a organizações ou indivíduos contra diversas ameaças. Trata-se de um esforço contínuo, que envolve a implementação de medidas para bloquear ataques cibernéticos e garantir a integridade e a confidencialidade das informações (FIA, 2022).

A SI está diretamente relacionada à preservação do valor das informações para uma empresa ou pessoa, garantindo que os dados permaneçam acessíveis apenas para aqueles que possuem autorização. Os princípios fundamentais da Segurança da Informação incluem confidencialidade, integridade, disponibilidade, autenticidade e legalidade (Wikipedia, 2019).

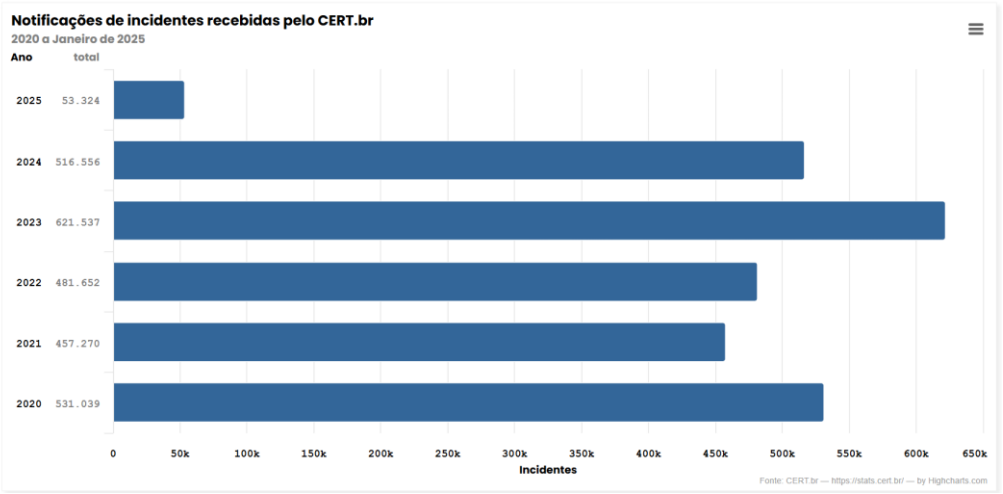
A tríade Confidencialidade, Integridade e Disponibilidade (CIA) é o modelo central da Segurança da Informação, complementado por outros aspectos como não-repúdio, autenticidade e conformidade. Com o avanço do comércio eletrônico e a crescente digitalização da sociedade, a privacidade também se tornou uma preocupação fundamental.

Os principais atributos da Segurança da Informação, segundo padrões internacionais como a ISO/IEC 17799:2005, são:

- Confidencialidade: Restringe o acesso às informações apenas para entidades autorizadas.
- Integridade: Garante que os dados permaneçam inalterados, protegidos contra modificações indevidas ao longo de seu ciclo de vida.
- Disponibilidade: Assegura que as informações estejam acessíveis sempre que necessário para usuários legítimos.
- Autenticidade: Certifica que os dados provêm de uma fonte confiável e não sofreram alterações durante a transmissão (Wikipedia, 2019).

A Figura 1 apresenta o número de incidentes reportados ao CERT.br entre 2014 e 2025, evidenciando o crescimento constante dos ataques cibernéticos ao longo dos anos.

Figura 1 – Número de incidentes reportados ao CERT.br entre 2014 e 2025



Fonte:cert.br, 2025

De acordo com o gráfico, observa-se um crescimento significativo no número de pessoas com acesso à Internet, evidenciando a crescente importância da segurança da informação e da proteção de redes.

2.2 *Firewall*

Um *firewall* é um dispositivo de segurança de rede que controla o tráfego de entrada e saída, decidindo permitir ou bloquear pacotes com base em um conjunto de regras predefinidas. Essa tecnologia tem sido a linha de defesa primária para redes corporativas e domésticas há mais de 25 anos, estabelecendo uma barreira entre redes internas protegidas e redes externas, como a Internet. *Firewalls* podem ser implementados em *hardware*, *software* ou em uma combinação de ambos (Cisco Systems Inc., 2023).

Existem dois principais tipos de *firewalls*: *stateless* e *stateful*, que adotam abordagens distintas para a filtragem de pacotes em uma rede. A principal diferença entre eles está na forma como lidam com as conexões e analisam os pacotes de dados. O *firewall stateless* (sem estado) trata cada pacote de forma independente, sem manter qualquer registro das conexões estabelecidas. Isso significa que ele avalia cada pacote isoladamente, analisando apenas seu cabeçalho e sem considerar o contexto geral da comunicação. O firewall *stateful* (com estado) utiliza

uma tabela de estados para armazenar informações sobre conexões ativas. Isso permite que ele avalie não apenas os endereços e portas, mas também o estado da conexão, oferecendo uma filtragem mais inteligente e eficiente (OSTEC, 2020).

A abordagem *stateful* oferece vantagens significativas, como a redução do número de regras, maior eficiência na validação de pacotes e, principalmente, maior segurança. Ao manter um histórico das conexões, o *firewall* pode analisar dados adicionais, proporcionando uma filtragem mais precisa. Embora o *firewall stateful* seja uma evolução natural do *stateless*, ambos ainda são amplamente utilizados e desempenham papéis essenciais na segurança da informação (OSTEC, 2020).

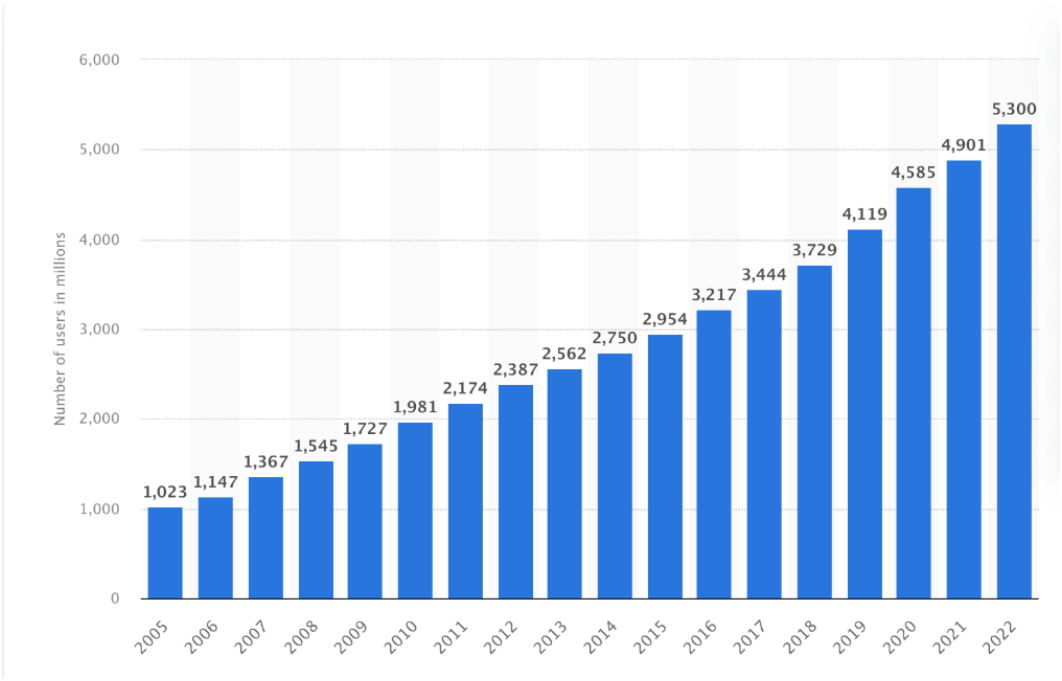
2.3 Redes de Computadores

Uma rede doméstica segura é um aspecto essencial da segurança na Internet. Redes vulneráveis podem ser exploradas por *hackers* para a realização de diversos tipos de ataques, como instalação de *malware*, roubo de dados e identidade, criação de *botnets* e outros crimes cibernéticos (Kaspersky, 2023).

Em 2021, o número de domicílios com acesso à Internet no Brasil chegou a 90%, segundo dados da Pesquisa Nacional por Amostra de Domicílios (PNAD). Isso representa 65,6 milhões de domicílios conectados, um aumento de 5,8 milhões em comparação com 2019 (GOV, 2022).

A Figura 2 apresenta a estimativa de pessoas com acesso à Internet no mundo, demonstrando o crescimento exponencial do uso de redes de computadores. Em 2022, o número de usuários globais chegou a 5,3 bilhões, evidenciando a necessidade de segurança cibernética cada vez mais eficiente (CERT.br, 2023).

Figura 2 - Estimativa de pessoas com acesso à Internet no mundo.



Fonte:cert.br, 2025

2.3.1 ISO/IEC 27000

A *International Organization for Standardization* (ISO) é uma organização internacional que tem como objetivo desenvolver e promover normas, testes, padronizações e certificações que facilitam as relações entre diferentes nações. Fundada em 1947, a ISO conta atualmente com membros de 165 países. No Brasil, é representada pela Associação Brasileira de Normas Técnicas (ABNT).

A ISO 27000 é um conjunto de certificações voltadas para segurança da informação e proteção de dados, destinadas a empresas e órgãos públicos. Essas normas servem como base para a criação de um Sistema de Gestão de Segurança da Informação (SGSI) em organizações de pequeno, médio e grande porte (PUCPR, 2021).

A primeira versão dessa norma foi lançada em 2005, baseada em um padrão britânico de segurança da informação. Atualmente, a versão vigente é a ISO/IEC 27000:2018, que estabelece diretrizes fundamentais para a proteção de dados. Os principais princípios da norma são: confidencialidade, integridade, disponibilidade e autenticidade (PUCPR, 2021).

2.3.2 ISO/IEC 27001

A ISO/IEC 27001 define os requisitos necessários para a implantação de um SGSI. A implementação desse sistema pode ser resumida em cinco fases principais:

- Entender o contexto da organização – Avaliação do nível de maturidade da empresa em relação à segurança da informação.
- Avaliação de riscos – Identificação de riscos e oportunidades, além da conscientização dos colaboradores sobre a importância da segurança da informação.
- Controles operacionais – Implementação de medidas para controlar, eliminar ou reduzir os riscos identificados.
- Análise de eficácia – Auditoria interna para verificar a efetividade dos controles implementados.
- Melhoria contínua – Monitoramento constante do SGSI, com avaliações periódicas para garantir conformidade e eficiência (PUCPR, 2021).

2.3.3 ISO/IEC 27002

De acordo com Rodrigues (2021), a ISO/IEC 27002 funciona como um código de práticas para os controles de segurança da informação. Ela fornece diretrizes para a seleção, implementação e gerenciamento de controles, considerando o ambiente de risco de cada organização.

A adoção da ISO 27002 traz diversas vantagens para as empresas, incluindo:

- Maior conscientização sobre segurança da informação entre os colaboradores.
- Melhor controle de ativos e proteção de informações confidenciais.
- Implementação estruturada de políticas de controle de segurança.
- Identificação e correção de deficiências nos processos internos.
- Redução dos riscos legais e regulatórios por não conformidade.
- Diferencial competitivo para empresas que desejam conquistar clientes que valorizam boas práticas de segurança.
- Maior organização e eficiência operacional, com processos bem definidos.
- Redução de custos ao prevenir incidentes de segurança da informação.

- Além disso, a norma garante conformidade com legislações e regulamentações aplicáveis à segurança da informação.

2.3.4 ISO/IEC 27003

A ISO/IEC 27003 fornece diretrizes essenciais para a implementação de um SGSI, abrangendo desde a concepção do projeto até a elaboração de planos para sua implantação.

As principais etapas recomendadas pela norma incluem:

- Obtenção da aprovação da alta administração para iniciar o projeto.
- Definição do escopo, políticas e limites do SGSI.
- Identificação dos requisitos de segurança da informação da organização.
- Realização da avaliação de riscos e definição das estratégias para mitigá-los.
- Implementação do SGSI, garantindo conformidade com as diretrizes da norma (IRKO, 2021).

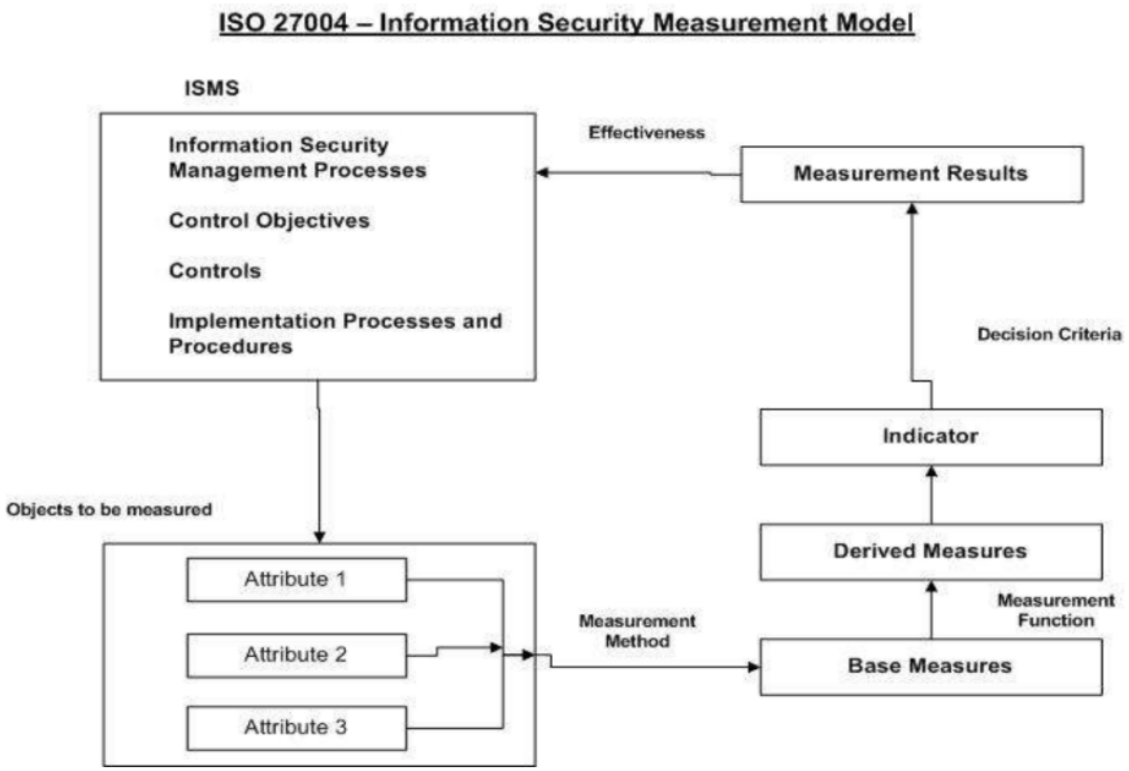
2.3.5 ISO/IEC 27004

A ISO/IEC 27004 estabelece métricas para a gestão da segurança da informação, permitindo que as organizações avaliem a eficácia das medidas aplicadas. Seu conteúdo é dividido em várias seções, incluindo:

- Justificativa – Explica a importância da medição no contexto da segurança da informação.
- Características – Define quais métricas devem ser monitoradas, quem será responsável por medi-las e com que frequência.
- Tipos de medidas – Apresenta métricas para avaliação do desempenho e da eficiência dos controles de segurança.
- Processos – Orientações sobre o desenvolvimento, implementação e aplicação das métricas.
- Anexos – Exemplos práticos de modelos de medição, métricas e fórmulas matemáticas aplicáveis.

A Figura 3 apresenta um exemplo desse modelo, detalhando as etapas do processo de medição da segurança da informação.

Figura 3 - Modelo de medição de segurança da informação



Fonte: *Network intelligence, 2025*

2.4 Trabalhos Relacionados

2.4.1. Segurança em Redes Corporativas e Ataques DDoS

O trabalho de VIEIRA (2021) analisou a segurança em redes corporativas com ênfase na prevenção de ataques do tipo DDoS (Distributed Denial of Service). Os autores destacam a importância dos *firewall*s de próxima geração (NGFW), como os da linha SonicWall, por oferecerem inspeção profunda de pacotes (DPI) e controle de tráfego em tempo real. Segundo eles, esses recursos são fundamentais para mitigar ataques distribuídos e garantir maior estabilidade no ambiente de rede.

O estudo também ressaltou que a capacidade de adaptação e resposta rápida dos *firewall*s NGFW às tentativas de exploração de vulnerabilidades é um diferencial significativo no cenário corporativo, onde a disponibilidade e a continuidade dos serviços são cruciais (VIEIRA, 2021).

2.4.2. *Firewall*s em Pequenas Empresas e Filtragem de Conteúdo

Carvalho (2015) investigaram a aplicação de *firewall*s em ambientes de

pequenas empresas, enfatizando a importância de soluções que sejam eficientes e, ao mesmo tempo, acessíveis em termos de custo-benefício.

Os autores argumentam que *firewall*s modernos, como o SonicWall, oferecem proteção contra *malwares*, filtros de conteúdo por categorias e integração com serviços de segurança em nuvem, sendo ideais para empresas com recursos limitados.

O estudo demonstrou que a presença de recursos como *Content Filtering Service* (CFS) contribui significativamente para a redução de vulnerabilidades em redes pequenas, ao impedir o acesso a sites maliciosos ou inapropriados e ao limitar a exposição a ameaças online comuns (Carvalho, 2015).

2.4.3. *Firewall*s e Redes sem Fio em Ambientes Corporativos

Rodrigues, Gonçalves, Castilho e Martins (2020) exploraram a evolução das soluções de segurança em redes wireless, destacando a importância da integração entre *firewall*s e tecnologias sem fio. De acordo com os autores, a utilização de *firewalls* com suporte a inspeção e filtragem em tempo real, como o SonicWall com *App Control* e *Geo-IP Filtering*, é essencial para detectar e bloquear tentativas de intrusão antes que comprometam a integridade da rede.

Eles também apontam que a combinação entre visibilidade de tráfego, controle de aplicativos e segmentação de rede proporciona uma barreira eficiente contra ameaças internas e externas, especialmente em ambientes empresariais onde a mobilidade e a conectividade são cada vez mais exigidas (Rodrigues et al, 2020).

2.4.4. Desempenho de *Firewall*s sob Alta Demanda

No trabalho de Pereira (2019), foi avaliado o desempenho de diferentes soluções de *firewall* sob cenários de alta demanda e tráfego intenso. A análise evidenciou que soluções comerciais que utilizam inspeção profunda de pacotes (DPI), como o SonicWall, são capazes de manter altos níveis de desempenho mesmo durante ataques de negação de serviço (DoS).

O autor concluiu que a eficiência dessas ferramentas se dá pela capacidade de processamento de conexões simultâneas e pela aplicação de políticas de segurança em camadas, o que reduz os impactos de ataques cibernéticos sobre a rede e

melhora a resiliência do ambiente protegido (Pereira, 2019).

2.4.5. Comparação entre *Firewalls Open Source* e Comerciais em Magalhães (2020) realizaram uma comparação entre *firewall*s de código aberto, como o PfSense, e soluções comerciais, como o SonicWall, em termos de eficácia, suporte e atualizações. Os autores concluíram que, embora ferramentas *open-source* possam ser eficazes em determinados contextos, as soluções comerciais oferecem vantagens significativas, como atualizações automáticas, suporte técnico especializado e integração com serviços de inteligência contra ameaças.

Essa constatação reforça a importância de se adotar soluções consolidadas em ambientes críticos, onde a disponibilidade dos serviços e a segurança da informação são prioridades. Além disso, destacaram que a facilidade de gerenciamento dos equipamentos comerciais também contribui para a tomada de decisão por parte das empresas (Magalhães, 2020).

3. MÉTODO

Quanto à natureza, esta pesquisa é um resumo de assunto, que consiste em explicar de forma clara e organizada um determinado tema, abordando seus conceitos, evolução e aplicações práticas, a partir da análise de informações coletadas em diferentes fontes bibliográficas (Wazlawick, 2014).

Quanto aos objetivos, trata-se de uma pesquisa exploratória e descritiva. A pesquisa exploratória tem como finalidade proporcionar maior familiaridade com o problema, tornando-o mais explícito e permitindo o aprimoramento de ideias ou a descoberta de novas perspectivas sobre o tema estudado (Gil, 2017, p. 41).

Já a pesquisa descritiva busca observar, registrar e analisar fatos sem interferir neles, com o intuito de descrever as características de um fenômeno ou de uma população, identificando possíveis relações entre variáveis (Gil, 2017, p. 44).
Quanto aos procedimentos técnicos, esta 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 CAPES. Segundo Gil (2017, p. 59-85), “a pesquisa bibliográfica permite reunir conhecimentos já existentes sobre o tema, servindo como base teórica para a parte prática do estudo.”

De acordo com Gil (2017), as etapas da pesquisa bibliográfica são:

a) Formulação do problema: Quais as funcionalidades do software de segurança SonicWall?

b) Levantamento bibliográfico preliminar: Foram realizadas buscas nas bases de dados da CAPES e no Google para embasar a definição do problema.

c) Busca das fontes: A pesquisa foi realizada em artigos acadêmicos, TCCs, sites especializados, blogs e nas bases de periódicos da CAPES, além de livros relevantes sobre segurança de redes e *firewall*s.

d) Fichamento: Foram realizados resumos dos materiais lidos, destacando as informações mais importantes para o desenvolvimento da pesquisa.

e) Redação do texto: Escrita do TCC.

A pesquisa experimental tem como objetivo avaliar o desempenho e as funcionalidades do *firewall* SonicWall em situações de configuração e testes práticos. Segundo Gil (2017, p. 93-101), ‘’esse tipo de pesquisa consiste em manipular variáveis e observar os efeitos que produzem sobre o objeto de estudo, controlando

os fatores que possam interferir nos resultados.”

As etapas da pesquisa experimental, segundo Gil (2017) incluem:

a) Formulação do problema: Quais são as funcionalidades do *firewall* SonicWall e como ele se comporta em diferentes cenários de segurança de rede?

b) Definição do plano experimental: Foram descritas as configurações e funcionalidades desse *firewall*, como regras de *firewall*, VPN, controle de tráfego e proteção contra ataques. Configurações como a criação de regras de filtragem de tráfego, definição de políticas de segurança e análise de logs foram realizadas.

c) Determinação do ambiente: O ambiente experimental foi detalhadamente configurado em um *firewall* físico SonicWall TZ570, conectado à Internet pela interface WAN (X1) e à rede interna pela interface LAN (X0). Foram utilizadas máquinas clientes físicas e virtuais para simular diferentes perfis de usuários e cenários de tráfego. O *gateway* padrão das máquinas foi definido para roteamento pelo SonicWall. Foram simulados acessos à web, uso de aplicativos e tentativas de conexão remota, com o intuito de validar as políticas implementadas.

d) Coleta de dados: Foram realizados os seguintes testes práticos:

Teste de NAT: Verificação do redirecionamento de portas para permitir acesso a um servidor interno via internet.

Teste de CFS: Tentativas de acesso a sites classificados como redes sociais, jogos e conteúdo adulto, para validar o bloqueio de páginas indevidas.

Teste de App Control: Bloqueio de aplicativos como WhatsApp Web e serviços de streaming, visando reduzir consumo de banda e riscos à segurança.

Teste de Geo-IP Filtering: Simulação de acessos externos oriundos de localizações geográficas não autorizadas, como forma de validar o bloqueio por região.

Teste de VPN: Configuração e validação de uma conexão remota via VPN SSL, verificando autenticação, criptografia e estabilidade do túnel de comunicação.

Esses testes tiveram como propósito avaliar a resposta do sistema, a eficácia das regras aplicadas e o desempenho do SonicWall diante de diferentes cenários de segurança.

e) Análise e interpretação dos dados: Os resultados obtidos foram analisados para verificar a eficácia das configurações implementadas e o desempenho do SonicWall nas situações de segurança simuladas.

f) Redação do relatório: Escrita do TCC.

4. FUNCIONALIDADES DO SONICWALL

Este capítulo tem como objetivo apresentar as principais funcionalidades do *firewall SonicWall*, uma solução amplamente utilizada para proteger redes de computadores contra ameaças cibernéticas. Este capítulo foca na descrição teórica dessas funcionalidades, preparando o leitor para sua implementação prática no Capítulo 5, baseada em um *appliance SonicWall* (Sonicwall, 2024).

Como um *firewall* de próxima geração ou *Next Generation Firewall* (NGFW), o *SonicWall* oferece recursos avançados que combinam hardware e software para garantir segurança em tempo real em redes domésticas e corporativas. O *SonicWall* é reconhecido por sua experiência de mais de 30 anos em segurança cibernética, oferecendo uma plataforma flexível e escalável que atende desde redes residenciais até infraestruturas corporativas complexas. Diferentemente dos *firewall*s tradicionais, que se limitam à filtragem básica, o SonicWall integra tecnologias avançadas, como análise de tráfego em camadas superiores e proteção contra ameaças emergentes.

A seguir, são detalhadas suas principais funcionalidades, que o posicionam como uma ferramenta essencial para administradores de rede (Fortinet, 2019).

4.1 Inspeção Profunda de Pacotes ou *Deep Packet Inspection* (DPI)

A DPI é uma funcionalidade central do SonicWall, permitindo a análise detalhada do conteúdo dos pacotes de dados, além de seus cabeçalhos. Essa tecnologia identifica e bloqueia ameaças ocultas, como *malwares* em tráfego criptografado (ex.: SSL/TLS), oferecendo uma proteção mais robusta que a filtragem convencional. Estudos destacam que o DPI é essencial para detectar ataques que exploram vulnerabilidades em aplicativos, uma capacidade crítica em ambientes corporativos (Carvalho, 2015).

4.2 Prevenção de Intrusões ou *Intrusion Detection and Prevention System* (IDS/IPS)

O SonicWall incorpora um sistema de IDS/IPS, que monitora o tráfego em tempo real para identificar e neutralizar tentativas de exploração de vulnerabilidades. Com assinaturas de ameaças atualizadas regularmente, ele bloqueia ataques como

injeções de SQL e *buffer overflows* antes que causem danos. Pesquisas apontam que sistemas IDS/IPS baseados em DPI aumentam significativamente a segurança contra ameaças conhecidas e emergentes (Rodrigues et al., 2020).

4.3 Controle de Aplicativos (*App Control*)

O *App Control* permite ao SonicWall monitorar e restringir o uso de aplicações específicas, como redes sociais ou serviços de *streaming*, otimizando a produtividade e reduzindo riscos de segurança. Essa funcionalidade utiliza assinaturas para identificar o tráfego de aplicativos, oferecendo controle granular sobre o uso da rede. Segundo estudos, o gerenciamento de aplicativos é vital para prevenir a entrada de *malwares* por meio de softwares não autorizados (Fortinet, 2019).

4.4 Filtragem de Conteúdo ou *Content Filtering Service* (CFS)

O CFS do SonicWall bloqueia o acesso a sites perigosos ou inadequados, como os que hospedam *phishing* ou conteúdo impróprio, utilizando categorias personalizáveis. Essa funcionalidade é amplamente aplicada em redes corporativas para cumprir políticas de uso e em ambientes domésticos para proteção de usuários. A literatura destaca que a filtragem de conteúdo reduz a exposição a ameaças baseadas na web, como ataques de engenharia social (OSTEC, 2020).

4.5 Rede Privada Virtual ou *Virtual Private Network* (VPN)

O SonicWall suporta VPNs seguras, utilizando protocolos como Segurança do Protocolo da Internet ou *Internet Protocol Security* (IPsec) e Camada de Soquetes Seguros ou *Secure Sockets Layer* (SSL) VPN, para garantir conexões criptografadas entre dispositivos remotos e a rede interna. Essa funcionalidade é crucial para empresas com equipes distribuídas, permitindo acesso seguro a recursos corporativos. Pesquisas confirmam que VPNs baseadas em *firewalls* NGFW são essenciais para proteger dados em redes públicas (VIEIRA, 2021).

4.6 Gerenciamento de Tráfego e *Quality of Service* (QoS)

O gerenciamento de tráfego e QoS do SonicWall permite priorizar aplicações críticas, como videoconferências, enquanto limita o uso de banda por serviços menos importantes. Essa funcionalidade melhora o desempenho da rede em cenários de alta demanda, garantindo uma experiência consistente para os usuários. Estudos apontam que o QoS é fundamental para otimizar redes corporativas com tráfego diversificado (Pereira, 2019).

4.7 Proteção contra Ameaças Avançadas

O SonicWall oferece proteção contra ameaças avançadas por meio do *Capture Advanced Threat Protection* (Capture ATP), que utiliza *sandboxing* para analisar arquivos suspeitos em um ambiente isolado. Esse recurso detecta *malwares* de dia zero e *ransomwares*, complementado por atualizações em tempo real. A literatura enfatiza que soluções de *sandboxing* são eficazes contra ameaças que evadem detecções tradicionais (Magalhães, 2020).

4.8 Monitoramento em Tempo Real e Relatórios

O monitoramento em tempo real do SonicWall fornece visibilidade detalhada do tráfego por meio de dashboards e logs, permitindo aos administradores identificarem tentativas de intrusão e analisar o uso da rede. Relatórios gerados auxiliam em auditorias e tomadas de decisão. Pesquisas destacam que o monitoramento contínuo é essencial para resposta rápida a incidentes de segurança (Rodrigues et al., 2020).

4.9 Segmentação de Rede

A segmentação de rede no SonicWall cria zonas de segurança (ex.: LAN, DMZ), isolando dispositivos para limitar a propagação de ameaças. Essa funcionalidade é especialmente útil em ambientes corporativos com múltiplos departamentos ou

serviços. Estudos indicam que a segmentação reduz o impacto de ataques ao confinar ameaças a áreas específicas da rede (Vieira, 2021).

4.10 Flexibilidade e Escalabilidade

O SonicWall é projetado para atender a diferentes cenários, com modelos como TZ Series para pequenas redes e NSa/NSsp para grandes empresas. Sua compatibilidade com ambientes híbridos (*on-premise* e nuvem) o torna adaptável às demandas modernas de TI. A literatura reforça que *firewall*s escaláveis são indispensáveis para organizações em crescimento ou com infraestruturas complexas (Pereira, 2019).

As funcionalidades descritas neste capítulo evidenciam que o SonicWall constitui uma solução abrangente para a segurança de redes, oferecendo ferramentas avançadas para proteção, controle e otimização do tráfego. Desde a inspeção profunda de pacotes, passando por mecanismos de prevenção contra intrusões, controle de aplicações, filtragem de conteúdo, VPNs seguras e políticas de segmentação, até recursos de escalabilidade e gerenciamento centralizado, o firewall se mostra adequado para atender diferentes necessidades organizacionais.

Dessa forma, o entendimento teórico dessas funcionalidades fornece a base necessária para a aplicação prática apresentada no capítulo seguinte, no qual são demonstradas as etapas de configuração do SonicWall e a validação de seus recursos em um ambiente real.

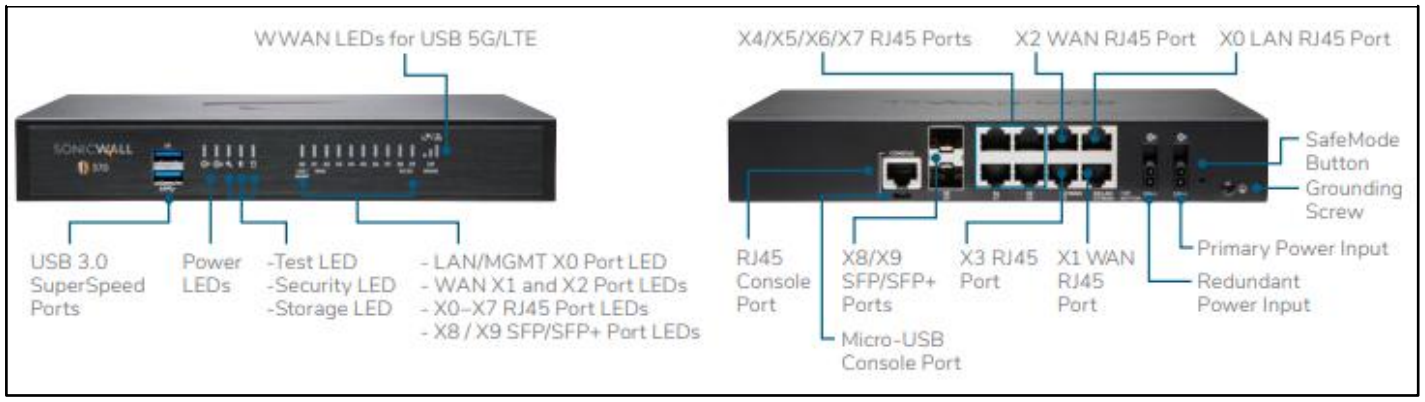
5. CONFIGURACAO PRATICA DO SONICWALL

Este capítulo apresenta a configuração prática do *firewall* SonicWall TZ570, com o objetivo de demonstrar passo a passo como realizar sua configuração inicial e aplicar políticas de segurança em um ambiente corporativo.

A configuração foi realizada utilizando um equipamento real numa empresa real, permitindo a captura de telas (prints) e a validação prática dos procedimentos.

A Figura 4 apresenta os painéis frontal e traseiro de um dispositivo de rede SonicWall, utilizado para gerenciamento de segurança e conectividade. funcionalidade e as opções de conectividade do dispositivo.

Figura 4 - SonicWall TZ570 series



Fonte: www.sonicwall.com, 2025

O painel frontal exibe LEDs indicadores de status, como WWAN para USB 5G/LTE, LEDs de energia, teste, segurança, armazenamento e portas LAN/MGMT, WAN e SFP/SFP+. O painel traseiro mostra as portas de conexão, incluindo portas RJ45 (X4 a X7), portas SFP/SFP+ (X8 e X9), uma porta WAN RJ45 (X1), uma porta LAN RJ45 (X0), portas de console (RJ45 e micro-USB), entradas de energia (primária e redundante), botão SafeMode e parafuso de aterramento. Essa ilustração destaca a funcionalidade e as opções de conectividade do dispositivo.

5.1 Acesso inicial ao SonicWall

Para acessar o *firewall* pela primeira vez, é necessário conectar-se diretamente

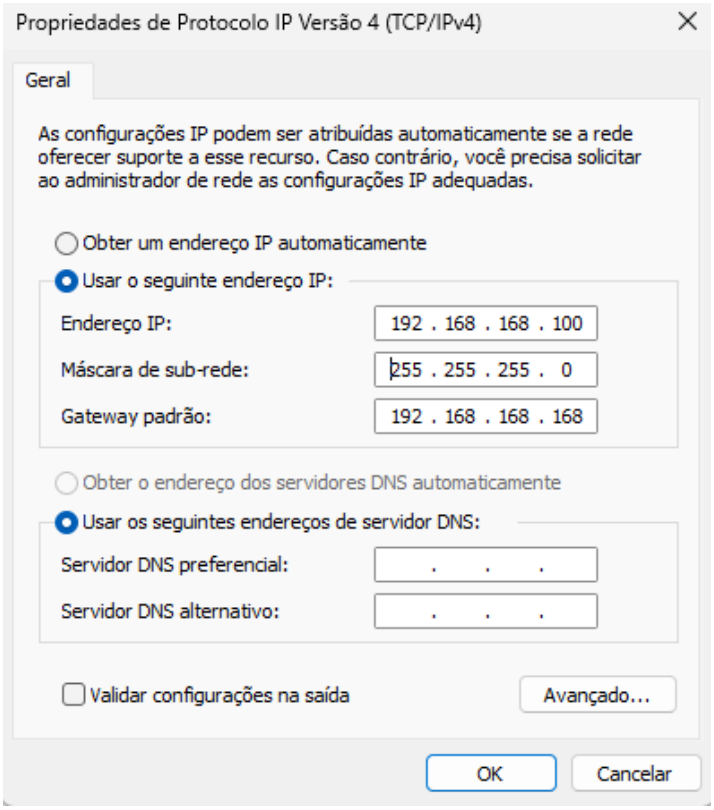
a uma de suas portas LAN via cabo de rede, utilizando um computador. Antes disso, é fundamental configurar um endereço IP fixo no computador, pertencente à mesma sub-rede da interface de gerenciamento do SonicWall.

Por padrão, o SonicWall TZ570 possui o IP 192.168.168.168 na interface X0 (LAN). Portanto, o IP do computador deve ser configurado manualmente com um IP da mesma rede, como 192.168.168.100, com máscara de sub-rede 255.255.255.0 e gateway 192.168.168.168 (SonicWall, 2024).

Painel de Controle > Rede e Internet > Conexões de Rede > Propriedades de Ethernet > Protocolo IP Versão (TCP/IPv4)

A Figura 5 ilustra a janela "Propriedades do Protocolo IP Versão 4 (TCP/IPv4)" no Painel de Controle do Windows, usada para configurar manualmente o endereço IP de um computador.

Figura 5 - Configuração Manual do IP no Protocolo TCP/IPv4



Fonte: Elaborado pelo autor (2025)

Por padrão, o SonicWall TZ570 possui o IP 192.168.168.168 na interface X0 (LAN). Assim, o IP do computador foi configurado como 192.168.168.100, com

máscara de sub-rede 255.255.255.0 e gateway 192.168.168.168, garantindo compatibilidade com a rede do dispositivo SonicWall. Essa configuração é acessada via Painel de Controle > Rede e Internet > Conexões de Rede > Propriedades de Ethernet > Protocolo IP Versão 4 (TCP/IPv4), conforme recomendado pelo SonicWall (2024).

5.2 Acesso via navegador e autenticação

Após configurar o IP fixo, o próximo passo é abrir um navegador web e digitar o endereço IP do *firewall* (https://192.168.168.168). Por padrão, o SonicWall utiliza HTTPS para acesso à interface de gerenciamento.

Na primeira tela de login, é utilizado o usuário padrão:

Usuário: admin

Senha: password

A Figura 6 apresenta a tela inicial de login do *firewall* SonicWall TZ570, acessada via navegador web pelo endereço HTTPS https://192.168.168.168.

Figura 6 - Tela de Login Inicial do *Firewall* SonicWall TZ570

Fonte:www.sonicwall.com

A interface exibe os campos para inserção das credenciais padrão (usuário: admin, senha: password), que são solicitadas no primeiro acesso.

Após o login, o sistema requer a alteração da senha padrão, seguindo as boas práticas de segurança recomendadas pela fabricante e alinhadas à norma ISO/IEC 27001 (ISO, 2013). Essa etapa é essencial para proteger o dispositivo contra acessos não autorizados.

5.3 Utilização do assistente de configuração inicial (*Setup Wizard*)

Após o primeiro login e alteração da senha de administrador, o SonicWall TZ570 apresenta o *Setup Wizard*, um assistente de configuração que facilita o processo de inicialização do equipamento. O assistente permite configurar rapidamente os aspectos básicos como zona de rede, interfaces, configuração da WAN, e credenciais administrativas.

Durante o uso do assistente, recomenda-se seguir as etapas abaixo:

- Configuração do nome do dispositivo (*hostname*): nomear o *firewall* com uma identificação clara, como fw-matriz ou sonicwall-main, facilitando a organização futura.
- Fuso horário: selecionar a zona horária correta, como GMT -3:00 para o horário de Brasília.
- Configuração da interface WAN (X1): definir se será IP dinâmico (DHCP), IP fixo ou PPPoE, dependendo do provedor de internet.
- Configuração da interface LAN (X0): definir o IP interno do *firewall*, como por exemplo 10.0.0.1, que será o gateway da rede interna.

5.4 Configuração das interfaces de rede

No SonicWall, cada interface física (X0, X1, X2 etc.) pode ser associada a uma zona lógica (LAN, WAN, DMZ, VPN etc.). A configuração correta das interfaces é essencial para o funcionamento do *firewall* e a aplicação de políticas de segurança.

Interface X0 – LAN

A interface X0, por padrão, é configurada como LAN. Esta será a interface que conectará a rede interna ao *firewall*.

Para configurá-la, conforme mostrada na Figura 7:

Acesse o menu *Network* > Interfaces.

Clique no lápis ao lado da interface X0.

Por exemplo defina os seguintes parâmetros:

Zone: LAN

IP *Assignment: Static*

IP *Address* Ex: 192.168.1.123

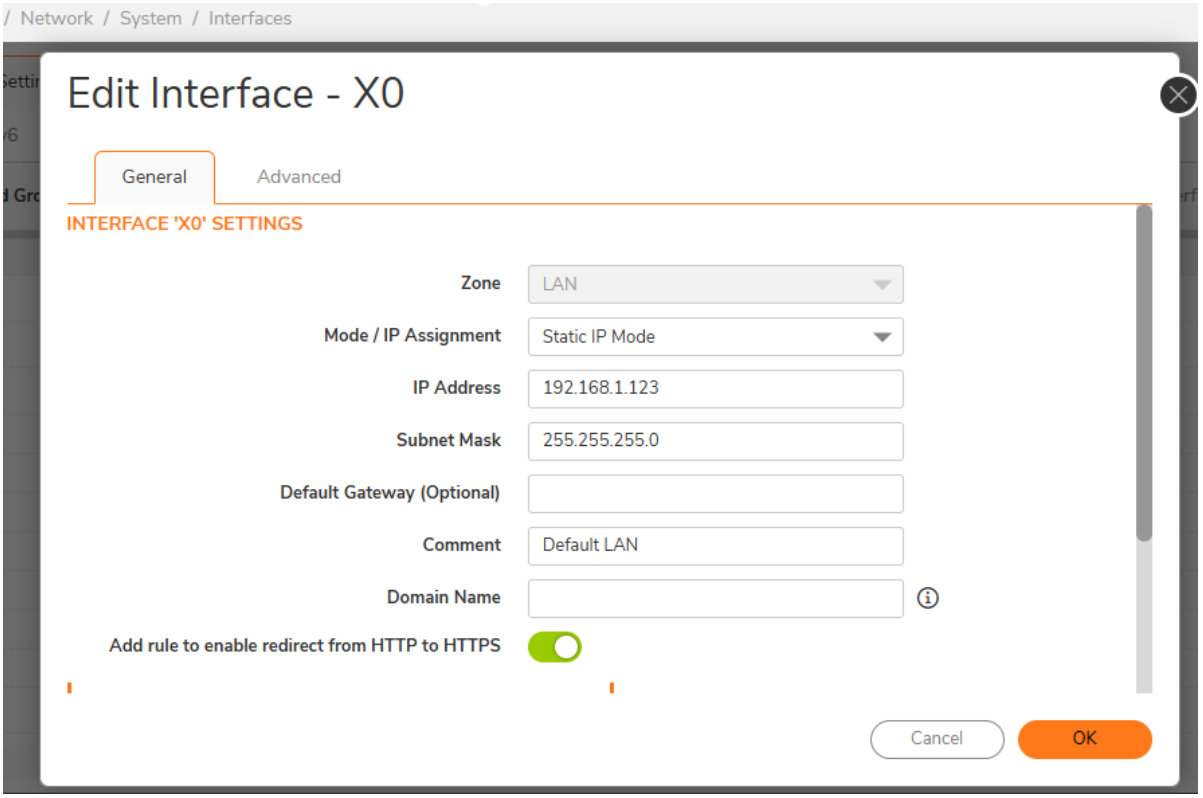
Subnet Mask Ex: 255.255.255.0

Gateway: deixe em branco nesta etapa

Clique em "OK" para salvar.

A Figura 7 mostra a janela de edição da interface X0 no *firewall* SonicWall TZ570, acessada via seção "*Network / System / Interfaces*".

Figura 7 - Configuração da Interface X0 no *Firewall* SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

A configuração exibe a zona definida como LAN, o modo de atribuição de IP configurado como *Static IP Mode*, com o endereço IP 192.168.1.123 e máscara de

sub-rede 255.255.255.0. O campo "*Default Gateway*" está opcional e em branco, enquanto o comentário "*Default LAN*" foi adicionado. Também é possível habilitar uma regra para redirecionar de HTTP para HTTPS, conforme indicado pelo interruptor ativado. Essa interface permite personalizar as configurações de rede do dispositivo.

Com essa configuração, todos os dispositivos internos que estiverem na faixa 192.168.1.0/24 poderão se comunicar com o *firewall* através da porta X0.

Interface X1 – WAN

A interface X1 é geralmente utilizada como WAN, sendo conectada diretamente ao modem do provedor de internet.

Para configurar:

Ainda no menu Network > Interfaces, clique no lápis da interface X1.

Defina os seguintes parâmetros:

Zone: WAN

IP Assignment: Static ou DHCP (dependendo do provedor)

IP Address: conforme fornecido pelo provedor

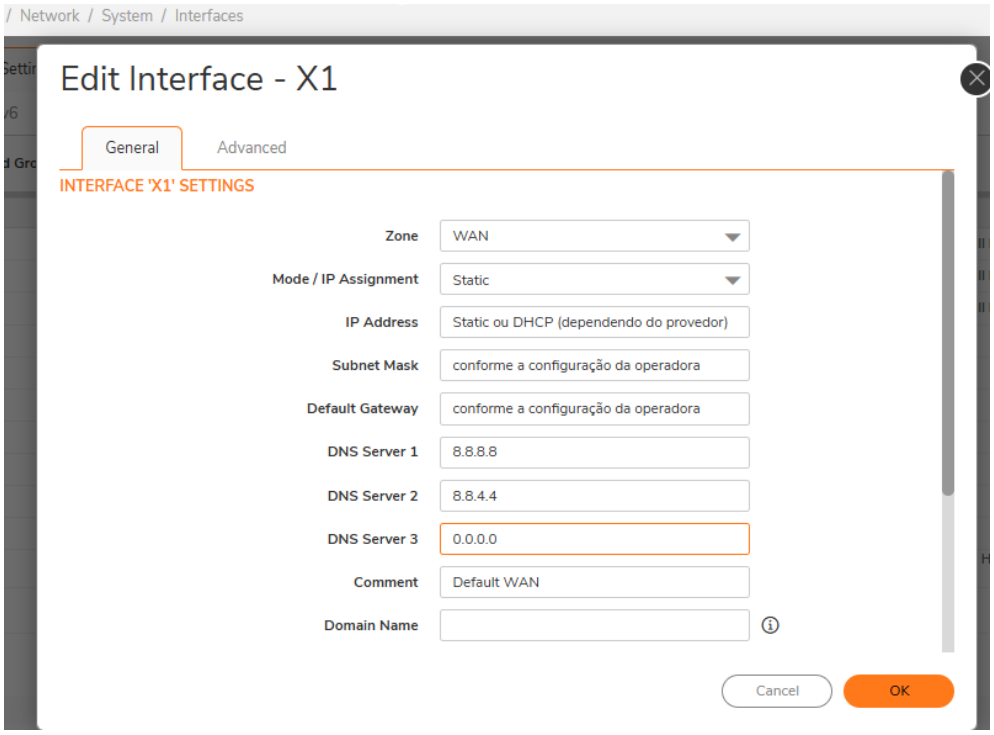
Subnet Mask e Gateway: conforme a configuração da operadora

Clique em "OK".

A Figura 8 exibe a janela de edição da interface X1 no *firewall* SonicWall TZ570, localizada na seção "*Network / System / Interfaces*". A interface está configurada na zona WAN, utilizando o modo "*Static* ou DHCP (dependendo do provedor)".

Os servidores DNS estão definidos como 8.8.8.8 (DNS Server 1) e 8.8.4.4 (DNS *Server* 2), enquanto o campo DNS Server 3 está zerado (0.0.0.0). O comentário "*Default WAN*" foi adicionado para identificação. Essa configuração permite que a interface X1 gerencie a conexão com a rede externa, ajustando-se automaticamente ao método de atribuição de IP do provedor de Internet.

Figura 8 - Configuração da Interface X1 no *Firewall* SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

Essa interface permitirá a saída para a internet e a publicação de serviços internos, caso necessário.

A interface X1 conectará o SonicWall à internet. As configurações dessa interface dependem do tipo de serviço oferecido pelo provedor:

IP Dinâmico (DHCP):

Selecionar IP *Assignment*: DHCP.

Essa configuração é típica para conexões residenciais ou de pequenos escritórios com modens em modo *router*.

IP Estático:

Selecionar IP Assignment: Static.

Preencher os campos:

IP Address: fornecido pelo provedor (ex: 187.16.52.10).

Subnet Mask: normalmente /30 (255.255.255.252) ou /29.

Default Gateway: IP do roteador do provedor.

Essa é a opção mais comum em conexões corporativas.

PPPoE:

Utilizado em conexões ADSL.

Informar o usuário e senha PPPoE do provedor.

Após configurar a interface X1, pode-se testar a conectividade clicando em *Diagnostics* > *Ping* e tentando alcançar, por exemplo, 8.8.8.8 (Google DNS).

Referência: SonicWall. (2024). *Configuring* WAN *Interfaces on SonicOS 7*. Disponível em: https://www.sonicwall.com/support/technical-documentation/

5.5 – Configuração de DNS e DHCP

Após configurar a interface LAN (X0), é essencial definir os serviços básicos de rede como DNS e, se necessário, DHCP.

Domain Name System ou Sistema de Nomes de Domínio (DNS)

A configuração dos servidores DNS permite que os dispositivos internos realizem a resolução de nomes de domínio corretamente:

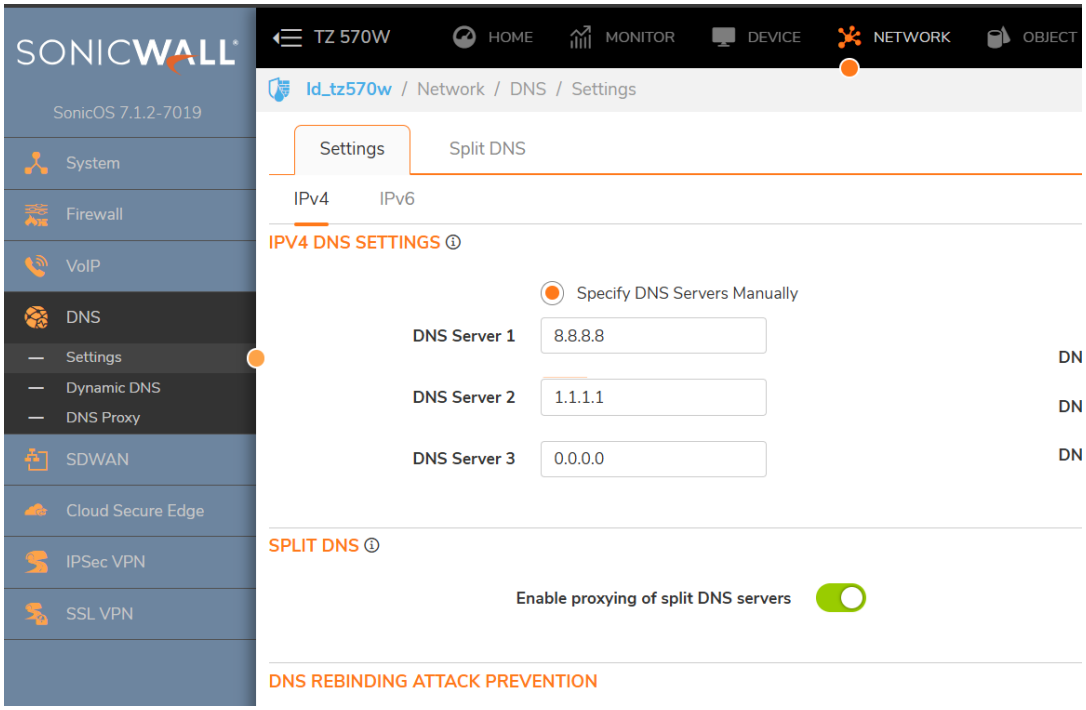
1. Acesse Network > DNS.
2. Marque a opção *Enable DNS Proxy* para que o SonicWall intermedie as requisições DNS.
3. Em DNS Server 1 e 2, insira servidores públicos ou privados, como:
    - 8.8.8.8 (Google)
    - 1.1.1.1 (Cloudflare)
4. Clique em Apply.

A Figura 9 ilustra a janela de configurações de DNS IPv4 na interface do SonicWall TZ570, acessada via "Network / DNS / Settings". A opção "Specify DNS Servers Manually" está selecionada, com os servidores DNS configurados como 8.8.8.8 (DNS Server 1), 1.1.1.1 (DNS Server 2) e 0.0.0.0 (DNS Server 3, desativado).

A seção "Split DNS" está habilitada com a opção "Enable proxying of split DNS servers" ativada, enquanto a "DNS Rebinding Attack Prevention" está disponível para reforçar a segurança.

Essa configuração permite gerenciar manualmente os servidores DNS e proteger contra ataques de reescrita de DNS.

Figura 9 - Configuração de Servidores DNS na Interface IPv4 do SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

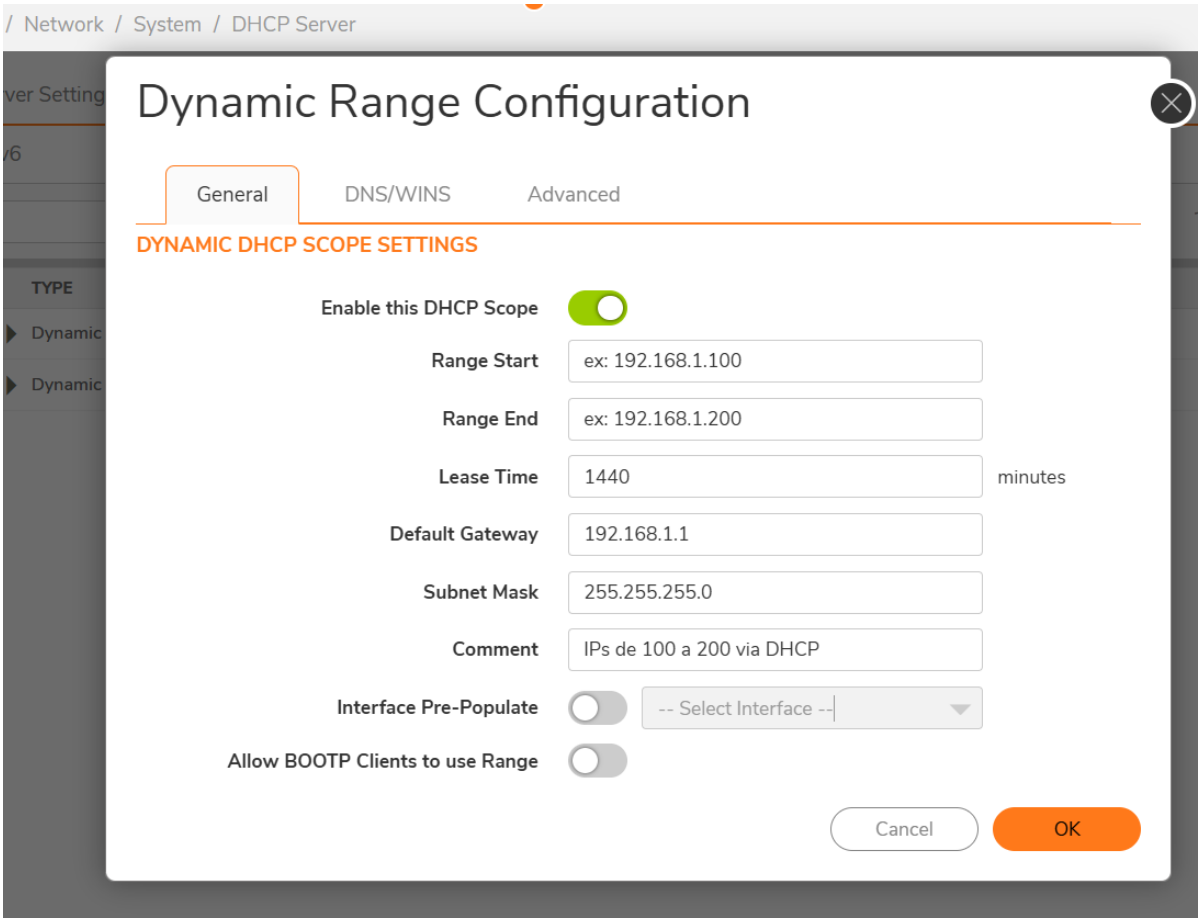
Dynamic Host Configuration Protocol ou Protocolo de Configuração Dinâmica de Host (DHCP)

Se a rede local não possuir um servidor DHCP ativo (como um Windows Server), o SonicWall pode atuar como servidor:

1. Acesse Network > DHCP Server > DHCP Server Lease Scopes.
2. Clique em Add Dynamic.
3. Configure:
    - Interface: X0 (LAN)
    - Start IP / End IP: 192.168.1.100 – 192.168.1.200
    - Lease Time: 1440
    - Subnet Mask: 255.255.255.0
    - Gateway: 192.168.1.1
    - Primary DNS: 8.8.8.8
4. Clique em OK para ativar o serviço.

A Figura 10 apresenta a janela de configuração de escopo dinâmico DHCP no SonicWall TZ570, acessada via "*Network / System / DHCP Server*".

Figura 10 - Configuração de Escopo Dinâmico DHCP no SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

A seção *"Dynamic DHCP Scope Settings"* está habilitada, com o intervalo de IPs definido de 192.168.1.100 (*Range Start*) a 192.168.1.200 (Range End), tempo de concessão de 1440 minutos (*Lease Time),* gateway padrão 192.168.1.1 (*Default Gateway*) e máscara de sub-rede 255.255.255.0 (*Subnet Mask*). O comentário "IPs de 100 a 200 via DHCP" foi adicionado. A interface pré-preenchida e o uso por clientes BOOTP estão desativados, permitindo a alocação automática de endereços IP na rede.

5.6 – Atualização do *firmware* e registro do dispositivo

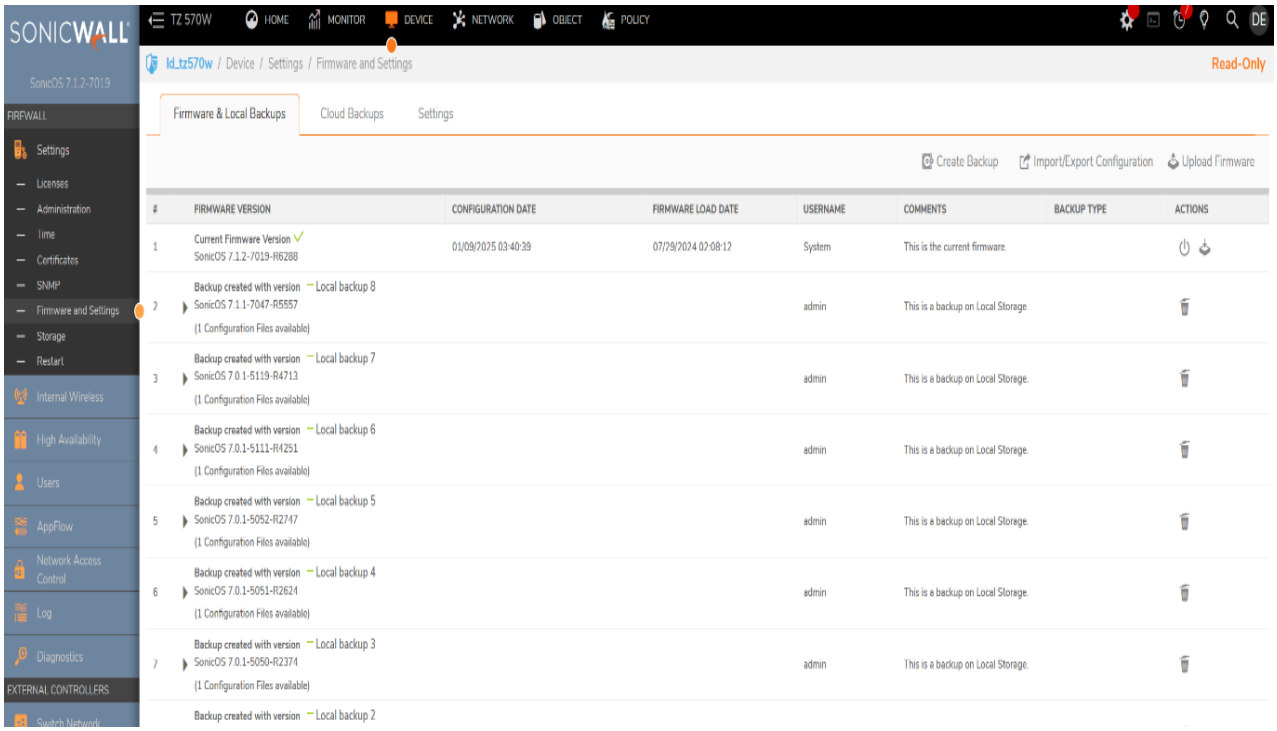
Manter o firmware atualizado garante mais segurança, estabilidade e acesso a novas funcionalidades.

1. Atualização do *firmware*:
2. Acesse *Device* > *Settings* > *Firmware and Settings*.
3. Verifique a versão atual.
4. Baixe a versão mais recente no portal oficial: https://mysonicwall.com
5. Faça upload do novo *firmware* clicando em *Upload Firmware*.

Após o *upload*, clique em *Boot* para inicializar com o novo firmware. Obs.: Antes de fazer o boot, faça um *backup* por segurança.

A Figura 11 mostra a interface de gerenciamento de firmware e configurações do SonicWall TZ570, acessada via "*Device* > *Settings* > *Firmware and Settings*".

Figura 11 - Interface de Gerenciamento de Firmware e Configurações do SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

A tela exibe uma lista de backups de firmware e configurações disponíveis, incluindo a versão atual (SonicOS 7.1.2-7019) datada de 03/09/2025 04:39, e

backups locais anteriores criados pelo usuário "admin", com comentários como "*This is the current firmware"* e *"This is a backup on Local Storage".* A interface permite criar novos *backups*, importar/exportar configurações e realizar a atualização de *firmware*, sendo recomendável realizar um backup antes de prosseguir com o boot do novo *firmware*, conforme prática de segurança.

Registro do dispositivo:

1. Acesse *Device* > *Settings*> *Licenses* > *MySonicWall*.
2. Clique em *Synchronize*.
3. Faça login com sua conta *MySonicWall*.
4. O dispositivo será registrado automaticamente.

O registro é necessário para ativar os serviços de segurança como CFS, *App Control*, *Geo-IP Filtering*, etc.

5.7 – Configuração de políticas de NAT e regras de *firewall*

Para que serviços internos sejam acessados externamente, é necessário criar regras de NAT (*Network Address Translation*) e *firewall*.

Exemplo de NAT para servidor web:

1. Acesse *Policy* > NAT *Rules* > clique em *Add NAT Rule*.
2. Configure:
    - Original *Source*: Any
    - Original *Destination*: WAN IP
    - Original *Service*: HTTP (porta 80)
    - *Translated Destination*: IP do servidor interno (ex: 192.168.1.10)
    - *Translated Service*: Original
    - *Inbound* Interface: X1
    - *Outbound* Interface: X0

Criar regra de *firewall*:

1. Vá em *Policy* > *Rules* > *Access Rules*.
2. Adicione uma nova regra de WAN to LAN permitindo:
    - *Source*: Any
    - *Destination*: IP do servidor interno

- *Service*: HTTP
- *Action*: *Allow*

Essas configurações permitem que dispositivos externos acessem o serviço interno com segurança controlada.

5.8 – Serviços como CFS (*Content Filtering*), *App Control, Geo-IP Filtering*

O SonicWall oferece recursos avançados de segurança para controle de conteúdo e tráfego.

CFS (*Content Filtering Service*)

Permite bloquear sites por categoria (ex: redes sociais, pornografia, jogos etc.).

1. Vá em *Security Services* > *Content Filter*.
2. Habilite o CFS.
3. Crie uma *Policy* definindo:
   - Categorias a bloquear.
   - Grupos de usuários afetados.
4. Aplique a política à interface LAN (X0).

App Control Advanced Controla ou bloqueia o uso de aplicações como WhatsApp, Skype, BitTorrent, etc.

1. *Acesse Security Services* > *App Control Advanced*.
2. Habilite o recurso.
3. Escolha uma categoria (ex: IM) e selecione os aplicativos.
4. Defina se será permitido, bloqueado ou monitorado.

Geo-IP Filtering

Bloqueia conexões com base na localização geográfica.

1. Vá em *Security Services* > *Geo-IP Filter*.
2. Habilite o recurso.
3. Escolha países a serem bloqueados ou permitidos.
4. Aplique a política à interface WAN (X1).

Esses serviços ajudam a proteger a rede contra ameaças externas, limitar uso indevido da internet e reforçar a política de segurança.

6.TESTES E VALIDAÇÕES DO *FIREWALL* SONICWALL

Após a configuração prática realizada no *firewall SonicWall TZ570*, descrita no capítulo anterior, foram executados testes para validar o funcionamento correto das políticas de segurança implementadas. Esses testes tiveram como objetivo comprovar a eficácia das configurações aplicadas e demonstrar como elas contribuem para a proteção da rede corporativa contra ameaças externas e internas.

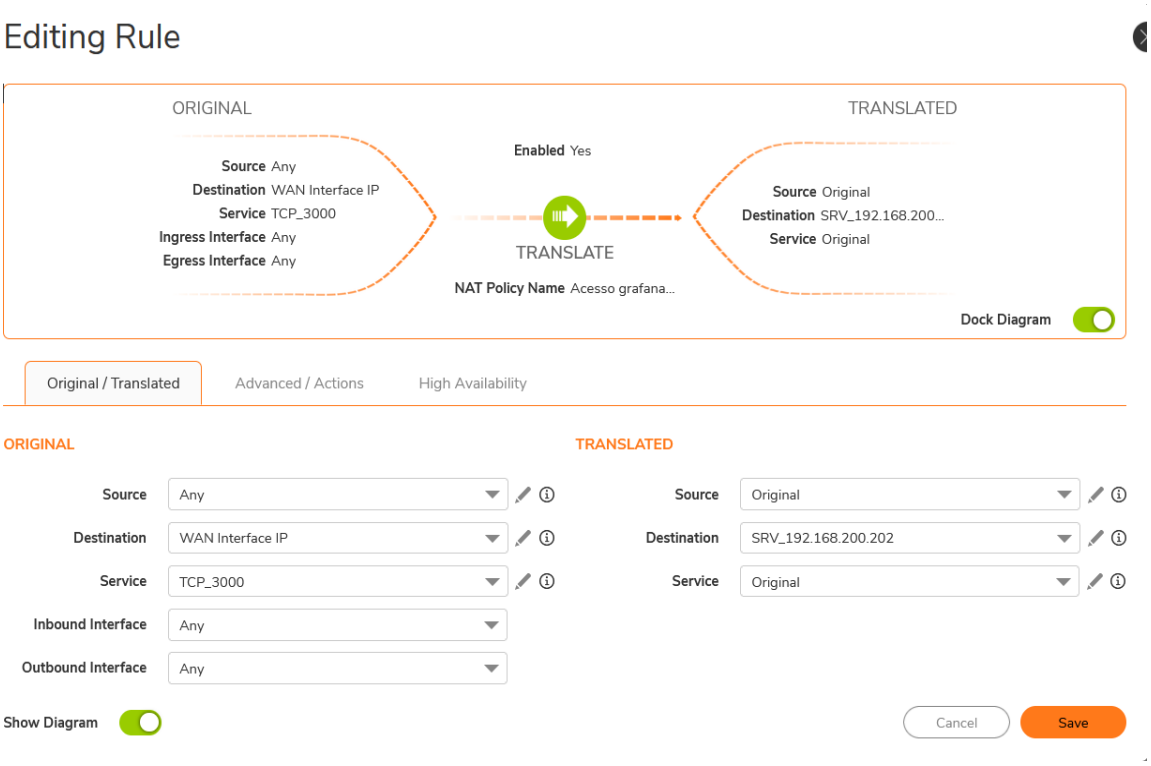
6.1 Teste do Network Address Translation (NAT)

O primeiro teste realizado foi a validação da funcionalidade de NAT, configurada para permitir o redirecionamento de portas (port forwarding) e possibilitar o acesso externo a um serviço interno.

Procedimento detalhado:

- Criou-se uma regra de NAT conforme mostra a Figura 12, para permitir o acesso externo a um serviço interno, utilizando uma porta específica previamente definida.

Figura 12 – Tela de edição da regra de NAT mostrando tradução de destino para o servidor interno.



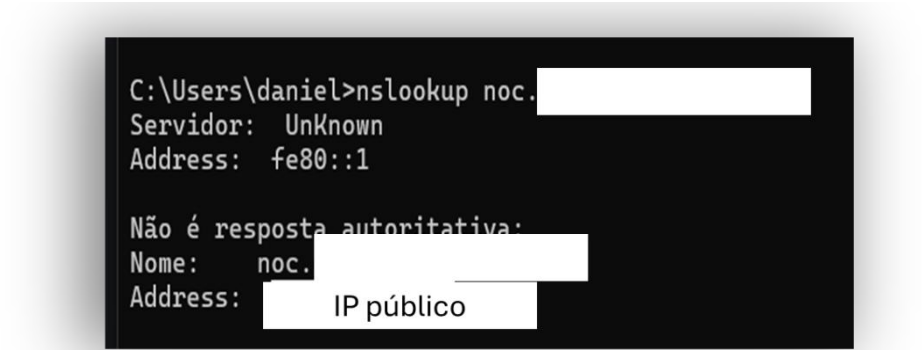
Fonte: Elaborado pelo autor, 2025

- Também foi configurada a respectiva Access Rule, permitindo o tráfego apenas da interface WAN para a LAN, garantindo que somente a porta autorizada estivesse liberada.

Validação:

• Utilizou-se um dispositivo externo para simular uma tentativa de acesso ao serviço publicado por meio da regra de NAT.
• Foi utilizado o comando *nslookup*, conforme apresentado na Figura 13, o qual retornou o IP público configurado, confirmando que o redirecionamento estava funcional. Além disso, verificou-se que somente a porta autorizada estava acessível, enquanto todas as demais permaneceram bloqueadas.

Figura 13 – Consulta DNS (*nslookup*) utilizada para validar o IP público no teste de NAT



Fonte: Elaborado pelo autor, 2025

Esse comportamento confirma a eficácia da política de *NAT* na segmentação e proteção do tráfego, permitindo apenas conexões previamente autorizadas (SonicWall, 2024).

6.2 Teste do Serviço de Filtragem de Conteúdo (Content Filtering Service – CFS)

O Content Filtering Service (CFS) foi configurado com o objetivo de restringir o acesso a categorias de sites consideradas inadequadas ao ambiente corporativo ou que pudessem comprometer a segurança e a produtividade da rede, como conteúdos maliciosos, redes sociais, entretenimento e páginas com material impróprio.

Procedimento detalhado:

- Foi criado um perfil de filtragem de conteúdo no SonicWall por meio da edição do objeto *Edit CFS Profile Object*, conforme apresentado na

Figura 14. Nessa configuração, foram definidas diversas categorias como *Security Risk*, *Human Resource Protections*, *Questionable/Legal*, *Social Media/Internet Communication* e *Entertainment*, todas configuradas com a ação de bloqueio (*Block*), de acordo com a política de segurança adotada pela empresa.

- As categorias relacionadas a conteúdos sensíveis, como malware, phishing, pornografia, violência, armas e redes sociais, foram explicitamente configuradas para bloqueio.
- Após a definição do perfil, a política de CFS foi aplicada à interface LAN (X0), ficando válida para os usuários da rede interna.

A Figura 14 ilustra a tela de configuração do *Edit CFS Profile Object*, evidenciando a seleção e o bloqueio das categorias de conteúdo que não são permitidas no ambiente corporativo, demonstrando o controle granular oferecido pelo SonicWall na filtragem de acessos à web.

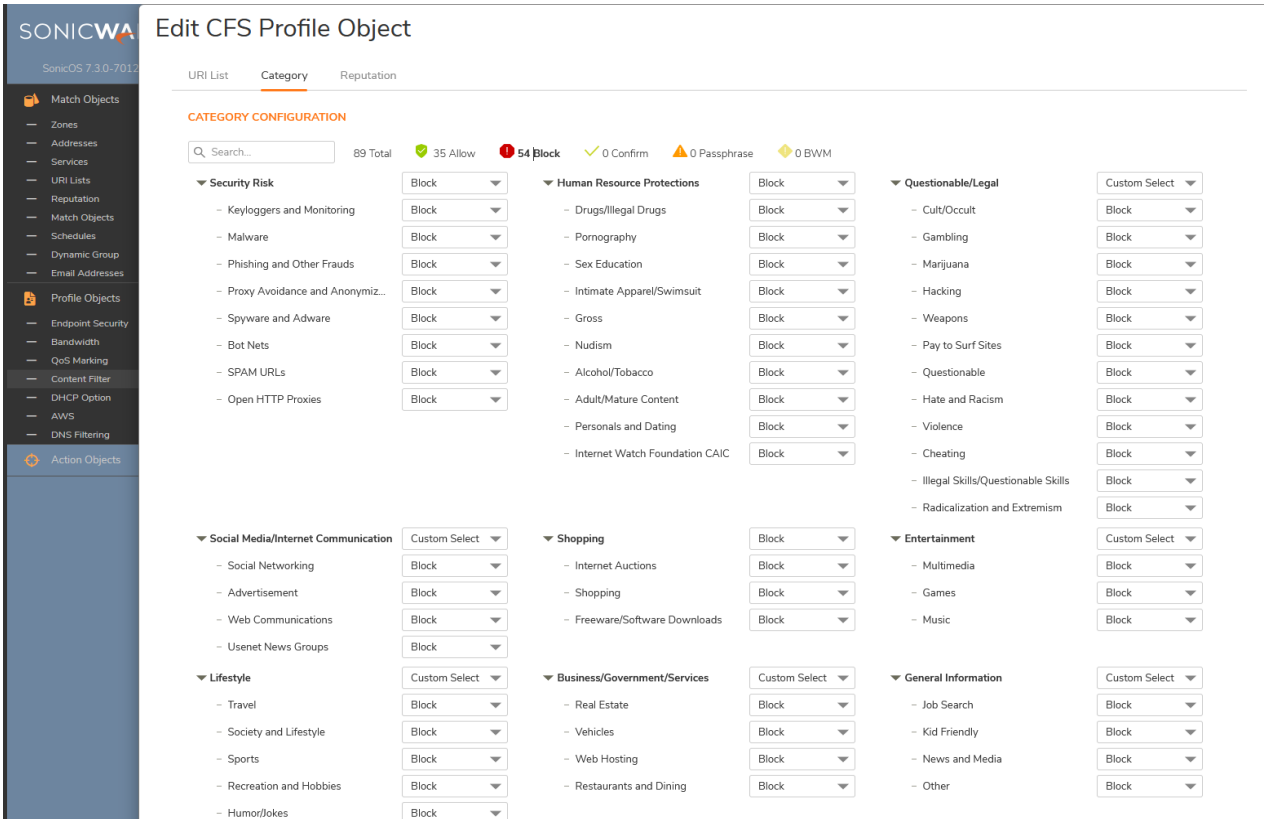
Validação:

- Para validar a configuração, foram realizadas tentativas de acesso a sites classificados em categorias bloqueadas, incluindo páginas com conteúdo violento e sites relacionados à compra de armas.
- Conforme demonstrado na Figura 15, ao tentar acessar um desses endereços, o SonicWall exibiu automaticamente a página padrão de bloqueio, informando que o site foi bloqueado pelo administrador de rede, além de apresentar a categoria associada ao bloqueio, neste caso, *Violence*.

A Figura 15 exemplifica o funcionamento do CFS em operação, mostrando a resposta do firewall ao usuário final ao tentar acessar um site não permitido, comprovando a aplicação correta da política configurada.

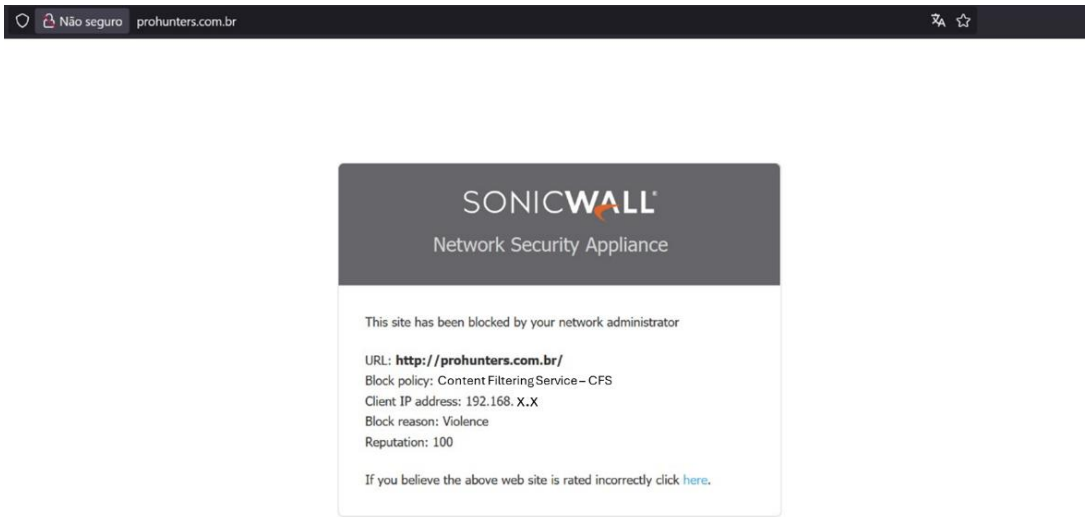
Esses resultados confirmam a eficácia do Content Filtering Service como uma ferramenta essencial para o controle de acesso à internet em ambientes corporativos, contribuindo para a redução de riscos de segurança, prevenção contra conteúdos indevidos e aumento da produtividade dos usuários (Carvalho, 2015).

Figura 14 – Tela de configuração do Edit CFS Profile Object



Fonte: Elaborado pelo autor, 2025

Figura 15 – Bloqueio de site pelo *Content Filtering Service (CFS)* no SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

Exemplo de bloqueio realizado pelo Content Filtering Service (CFS), restringindo o acesso a um site classificado na categoria de violência, não permitida pela política de segurança definida.

6.3 Teste do Controle de Aplicativos (App Control Advanced)

Outro recurso testado foi o App Control Advanced, utilizado para controlar e bloquear aplicações que poderiam consumir largura de banda excessiva ou representar riscos à segurança da rede corporativa, como mensageiros instantâneos, aplicativos de entretenimento e ferramentas de compartilhamento de arquivos.

Procedimento detalhado:

- O recurso App Control Advanced foi ativado no SonicWall e configurado para aplicar políticas de bloqueio a aplicações pertencentes às categorias *Messaging* e *File Sharing*.
- Entre os aplicativos incluídos na política de bloqueio estavam TikTok, WhatsApp Web, Skype, aplicações de torrent e serviços de armazenamento em nuvem.
- A política foi aplicada à interface LAN, tornando o bloqueio válido para os usuários da rede interna.

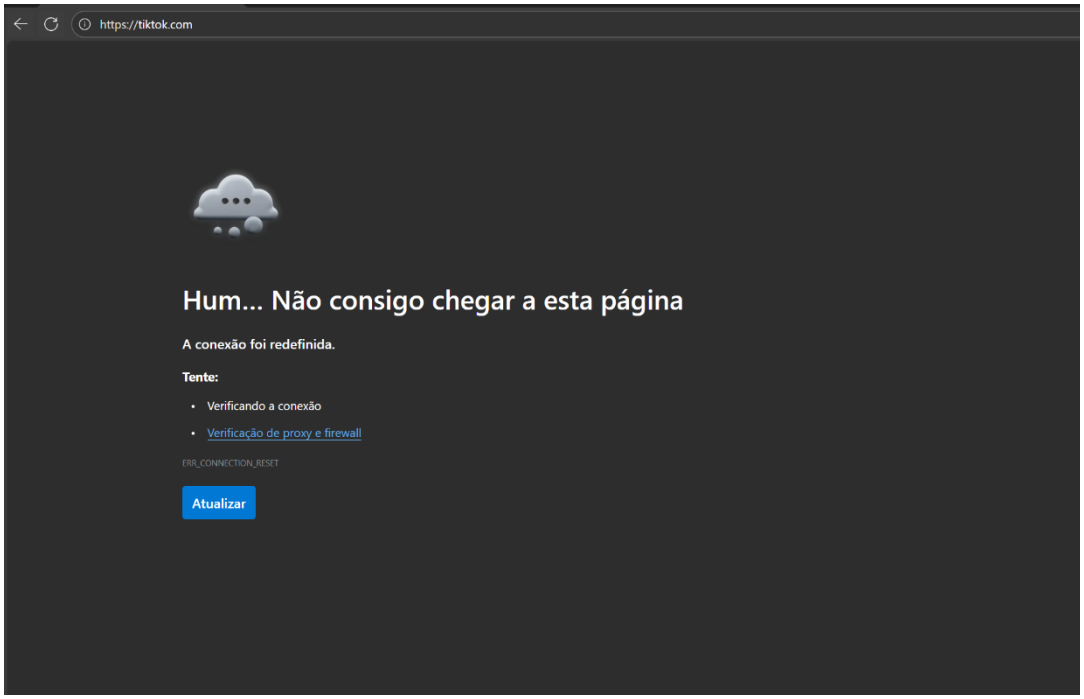
Validação:

- Para validar a configuração, tentou-se acessar o aplicativo TikTok por meio de um navegador web.
- Conforme demonstrado na Figura 16, o acesso foi imediatamente interrompido pelo firewall, resultando na exibição da mensagem “Hum... Não consigo chegar a esta página”, indicando que a conexão foi redefinida pelo controle de aplicações do SonicWall.
- O evento também foi registrado nos logs do firewall como *“Application blocked by policy”*, confirmando a atuação correta da regra configurada.

A Figura 16 apresenta a tela exibida ao usuário final no momento da tentativa de acesso ao TikTok, evidenciando o bloqueio imposto pelo App Control Advanced conforme a política definida.

Os resultados obtidos demonstram a eficácia do App Control Advanced como uma ferramenta fundamental para ambientes corporativos, pois contribui para a redução de vulnerabilidades, evita o uso indevido da banda de internet e reforça a aplicação das políticas de segurança da informação (Rodrigues et al., 2020).

Figura 16 – Bloqueio de acesso ao aplicativo TikTok pelo *App Control Advanced* no SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

Tela exibida ao tentar acessar o aplicativo TikTok, bloqueado conforme regra definida no *App Control Advanced.*

6.4 Teste do Geo-IP Filtering

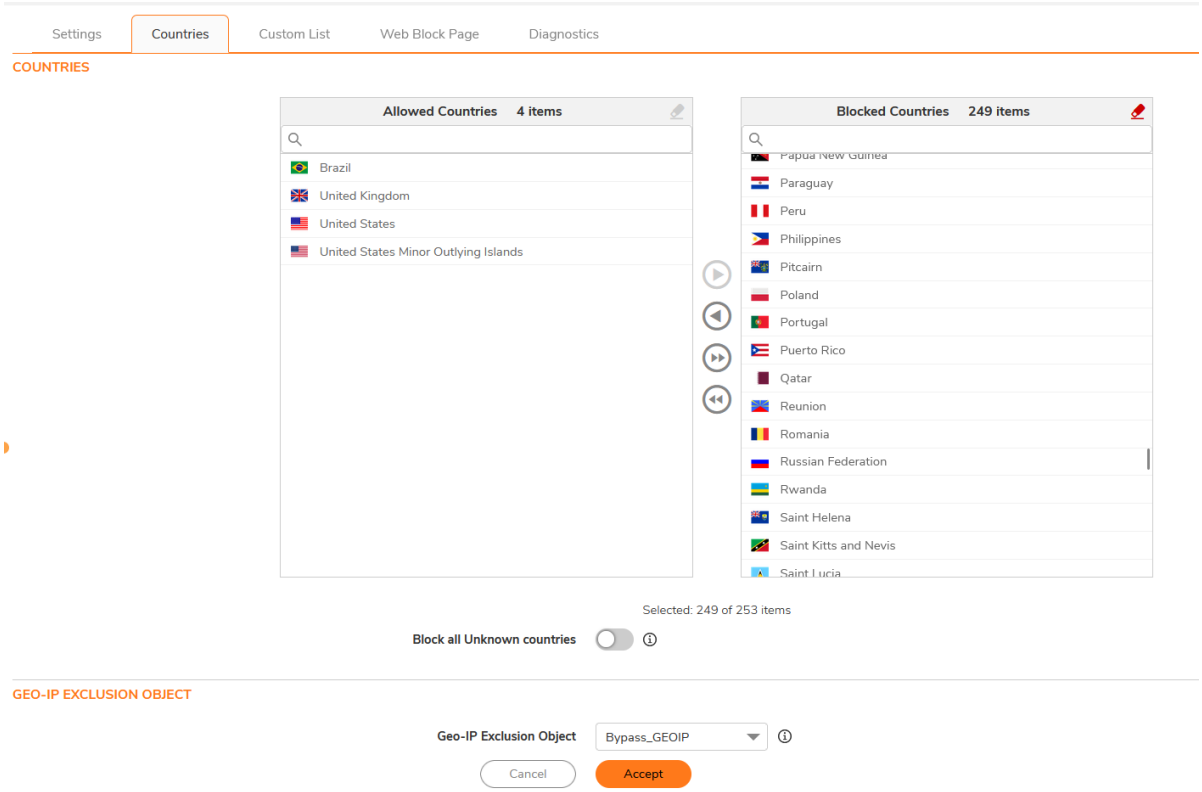
O teste de Geo-IP Filtering teve como objetivo validar o bloqueio de acessos à rede com base na localização geográfica, impedindo conexões provenientes de países considerados de alto risco ou que não possuem relação com as operações da empresa.

Procedimento detalhado:

- O recurso Geo-IP Filtering foi configurado no firewall SonicWall, definindo uma lista de países permitidos e bloqueando aqueles considerados não autorizados, conforme apresentado na Figura 17.
- Entre os países bloqueados destacam-se China, Rússia e Coreia do Norte, enquanto apenas países previamente autorizados permaneceram liberados para comunicação com a rede.
- A política foi aplicada para que qualquer tentativa de acesso originada dos países bloqueados fosse automaticamente negada pelo firewall.

A Figura 17 ilustra a tela de configuração do Geo-IP Filtering no SonicWall, evidenciando a separação entre países permitidos e países bloqueados, bem como a aplicação da política de restrição geográfica adotada no ambiente corporativo.

Figura 17 – Configuração de países permitidos e bloqueados no Geo-IP Filtering do SonicWall



Fonte: Elaborado pelo autor, 2025

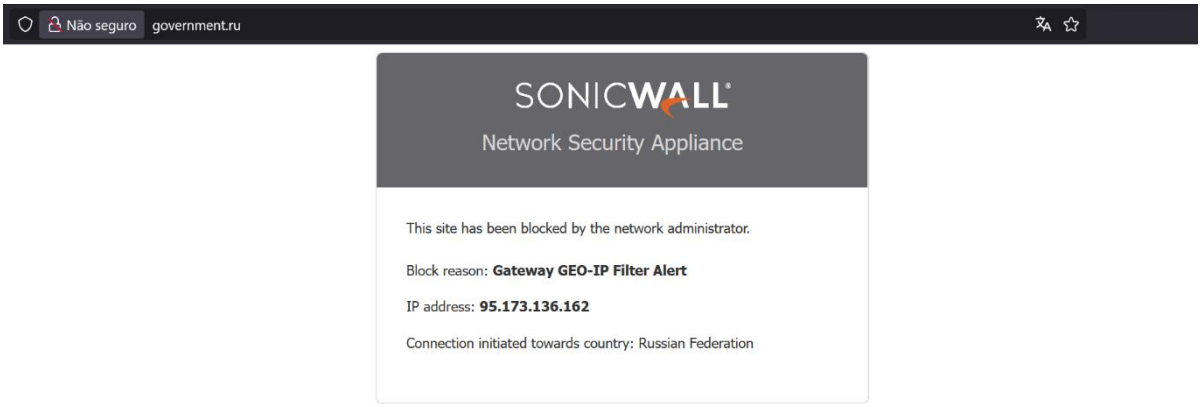
Validação:

- Para validar a configuração, foi realizada uma simulação de acesso a um site hospedado na Federação Russa, conforme demonstrado na Figura 18.
- Ao tentar estabelecer a conexão, o SonicWall bloqueou imediatamente a solicitação, exibindo a página de bloqueio com a mensagem *“Gateway GEO-IP Filter Alert”*, informando que a conexão foi negada em razão da origem geográfica do endereço IP.

A Figura 18 apresenta a tela exibida ao usuário final no momento do bloqueio, comprovando que o acesso foi impedido devido à política de Geo-IP Filtering aplicada.

Os resultados obtidos demonstram que o recurso Geo-IP Filtering agrega uma camada adicional de proteção à infraestrutura de rede, prevenindo acessos provenientes de regiões consideradas de alto risco e reduzindo a superfície de ataque contra tentativas externas indevidas (Pereira, 2019).

Figura 18 – Bloqueio de conexão internacional pelo *Geo-IP Filtering* no SonicWall TZ570



Fonte: Elaborado pelo autor, 2025

Tela exibida ao tentar acessar um endereço hospedado na Federação Russa, bloqueado conforme regra configurada no recurso *Geo-IP Filtering.*

6.5 Resultados Obtidos

Com base nos testes realizados, verificou-se que todas as funcionalidades implementadas no firewall SonicWall TZ570 — NAT, Content Filtering Service (CFS), App Control Advanced e Geo-IP Filtering — operaram conforme o esperado.

O NAT possibilitou a publicação controlada de serviços internos por meio de *port forwarding*; o CFS bloqueou corretamente as categorias de conteúdo previamente definidas, exibindo a página padrão de bloqueio; o App Control Advanced impediu o uso de aplicações não autorizadas, registrando os eventos correspondentes nos logs; e o Geo-IP Filtering bloqueou conexões oriundas de países restritos, sem impacto perceptível sobre o tráfego legítimo da rede.

Esses resultados validam a eficácia do conjunto de políticas aplicadas, evidenciando a redução de riscos e o aumento do controle sobre o tráfego de rede (Magalhães, 2020).

De forma consolidada, os testes demonstram que a utilização de um firewall de próxima geração, com mecanismos de inspeção e controles integrados, contribui para a mitigação de ameaças comuns, como acessos não autorizados, uso indevido de largura de banda, exposição indevida de serviços internos e tentativas de conexão provenientes de regiões consideradas de alto risco. Além disso, a adoção dessas políticas está alinhada às boas práticas e às normas de segurança da informação, em especial às diretrizes da família ISO/IEC 27000.

Por fim, recomenda-se que as políticas de segurança sejam continuamente acompanhadas por meio da análise de logs, geração de relatórios e revisões periódicas, de modo a garantir a aderência contínua aos requisitos do negócio e à conformidade com as normas de segurança da informação (Magalhães, 2020).

7.CONCLUSAO

Este trabalho teve o intuito de responder à seguinte questão de pesquisa: Quais são as funcionalidades do *firewall* SonicWall e como ele pode ser configurado para garantir segurança em redes corporativas?

O objetivo geral deste trabalho foi identificar e descrever as funcionalidades do *firewall* SonicWall, destacando sua aplicação na segurança de redes corporativas.

Para alcançar esse objetivo, realizou-se uma pesquisa bibliográfica fundamentada em normas e estudos anteriores, além da implementação prática em um *firewall* físico do modelo SonicWall TZ570. Esse processo possibilitou compreender como recursos avançados, como *Content Filtering Service* (CFS), *App Control*, *NAT* e *Geo-IP Filtering*, podem ser aplicados para mitigar riscos cibernéticos e proteger dados contra acessos não autorizados, *malwares* e ataques distribuídos (VIEIRA, 2021).

Durante o desenvolvimento do trabalho, foram executadas configurações práticas no SonicWall, envolvendo desde a definição de um IP fixo para acesso à interface administrativa até a aplicação de políticas de segurança como filtragem de conteúdo e controle de aplicativos. Em seguida, foram realizados testes para validar essas configurações, incluindo tentativas de acesso a sites bloqueados, utilização de

aplicativos restritos e simulações de ataques externos. Os resultados comprovaram a eficácia do *firewall* na aplicação das políticas de segurança definidas, garantindo controle granular sobre o tráfego e aumentando a proteção da rede.

O estudo permitiu concluir que *firewall*s de próxima geração, como o SonicWall, desempenham papel fundamental na segurança da informação, oferecendo não apenas inspeção de pacotes, mas também funcionalidades integradas de filtragem e prevenção contra ameaças. Além disso, constatou-se que a aplicação de normas como a ISO/IEC 27000 é essencial para estabelecer diretrizes de segurança consistentes. No entanto, uma limitação do estudo foi a não utilização de testes em ambientes com alta demanda ou redes distribuídas, o que poderia ampliar a avaliação sobre o desempenho do dispositivo em cenários complexos.

Além disso, conclui-se da importância da utilização de ferramentas robustas e devidamente configuradas para proteger redes corporativas.

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

- a análise comparativa entre *firewall*s comerciais, como SonicWall, Fortinet e Cisco, e soluções *open source*, como *PfSense*, a fim de verificar diferenças em termos de custo, desempenho e escalabilidade.
- explorar a integração do SonicWall com sistemas de monitoramento, como SIEMs.
- implementação de políticas avançadas de *Zero Trust* para ampliar o nível de segurança.

REFERÊNCIAS

ABNT. *ABNT NBR ISO/IEC 27002: tecnologias da informação - técnicas de segurança.* In: Profjefer.files.wordpress.com, 8 ago. 2005. Disponível em: https://profjefer.wordpress.com/wp-content/uploads/2013/10/nbr_iso_27002-para-impressc3a3o.pdf sso em: 19 mar. 2025.

VIEIRA, A. M. Mecanismo de prevenção de ataque DDoS em redes SDN [S. l.], 2021. Disponível em: https://ri.ufs.br/bitstream/riufs/15014/2/ALFREDO_MENEZES_VIEIRA.pdf. Acesso em: 1 abr. 2025.

AO KASPERSKY LAB. Como configurar uma rede doméstica segura. [S. l.], 2023. Disponível em: https://www.kaspersky.com.br/resource-center/preemptive-safety/how-to-set-up-a-secure-home-network. Acesso em: 23 mar. 2025.

CISCO SYSTEMS, INC. O que é um firewall? In: O que é um firewall? [S. l.], 2023. Disponível em: https://www.cisco.com/c/pt_br/products/security/firewalls/what-is-a-firewall.html. Acesso em: 1 abr. 2025.

MAGALHÃES B. Qual a diferença entre um Firewall corporativo e Open-Souce. [S. l.], 2020. Disponível em: https://ti.3up.tech/qual-a-diferenca-entre-um-firewall-corporativo-e-opensource/ . Acesso em: 5 abr. 2025.

DOURADO, R. S. Um estudo dos softwares Endian Firewall e PFSense Firewall. Segurança da informação, PUC Goiás, 9 dez. 2022. Disponível em: : Um estudo dos softwares endian firewall e pfsense firewall. Acesso em: 19 mar. 2025.

ENDIAN. Endian Firewall Community. [S. l.], 2023. Disponível em: https://www.endian.com/en/community/. Acesso em: 9 abr. 2025.

FIA BUSINESS SCHOOL. Segurança da informação: o que é, 5 pilares e como garantir nas empresas? Segurança da informação, fia.com.br, 16 dez. 2022. Disponível em: https://fia.com.br/blog/seguranca-da-informacao/?utm_term=&utm_campaign=INSANE+-+Rebranding+%23Topo&utm_source=adwords&utm_

medium=ppc&hsa_acc=8114508637&hsa_cam=23229832751&hsa_grp=&hsa_ad=&hsa_src=x&hsa_tgt=&hsa_kw=&hsa_mt=&hsa_net=adwords&hsa_ver=3&gad_source=1&gad_campaignid=23229857663&gbraid=0AAAAAD821FZEzoSrxBwPhEJm2i8oPPPl_&gclid=CjwKCAiAz_DIBhBJEiwAVH2XwNV-7KIQr83loR4qe11OQoIYHyMad2aQpmxA9trpEAj0XQT9J0J2-hoC8iEQAvD_BwE. Acesso em: 19 mar. 2025.

FIREWALL DEFINIÇÃO. Aprimore seus conhecimentos sobre segurança. [S. l.], 2020. Disponível em: https://ostec.blog/seguranca-perimetro/firewall-definicao/. Acesso em: 13 out. 2025.

FORTINET. What is deep packet inspection (DPI)? [S. l.], 2019. Disponível em: https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection. Acesso em: 1 abr. 2025.

GIL, A. C. *Como elaborar projetos de pesquisa.* 7. ed. São Paulo: Editora Atlas Ltda., 2017.

GOV.BR. 90% dos lares brasileiros já tem acesso à internet no Brasil, aponta pesquisa: segundo a Pesquisa Nacional por Amostra de Domicílios, isso significa 65,6 milhões de domicílios conectados, portanto, 5,8 milhões a mais do que em 2019. [S. l.], 2022. Disponível em: https://www.gov.br/casacivil/pt-br/assuntos/noticias/2022/setembro/90-dos-lares-brasileiros-ja-tem-acesso-a-internet-no-brasil-aponta-pesquisa. Acesso em: 25 mar. 2025.

FREUND, G. P., KARPINSKI, C., & MACEDO, D. D. J. O contexto histórico da produção científica sobre Segurança da Informação, 14 out. 2023. Disponível em: https://ojs.uel.br/revistas/uel/index.php/informacao/article/view/43684. Acesso em: 19 mar. 2025.

IRKO. Cybersecurity: quais são as principais normas e qual sua relação com a LGPD? [S. l.]: IRKO, 2021. Disponível em: https://site.irko.com.br/blog/cybersecurity/ . Acesso em: 26 mar. 2025.

ISO. *ISO/IEC 27001: information security management.* [S. l.], 2013. Disponível em: https://www.iso.org/standard/54534.html. Acesso em: 25 mar. 2025.

MOLINA, D.; SILVEIRA, S. R.; RODRIGUES, F. B. Um estudo de caso sobre a implantação de um ambiente de segurança de redes de computadores. *Revistas .unifacs.br*, 1 jun. 2019. Disponível em: https://revistas.unifacs.br/index.php/rsc/article/viewFile/5904/3808 . Acesso em: 19 mar. 2025.

CARVALHO, R. J. SEGURANÇA DA INFORMAÇÃO DE PEQUENAS E MÉDIAS EMPRESAS: Proposta de implantação de firewall. [S. l.], 2015. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/936/1/20152S_CARVALHORobsonJose_CD2510.pdf. Acesso em: 1 abr. 2025.

OSTEC. Firewall definição: aprimore seus conhecimentos sobre segurança. [S. l.], 2020. Disponível em: https://ostec.blog/seguranca-perimetro/firewall-definicao/. Acesso em: 1 abr. 2025.

PEREIRA, L. A. Desempenho de firewalls em cenários de alta demanda. [S. l.], 2019. Disponível em: https://repositorio.ufmg.br/bitstream/1234/56789/1/CC_Pereira_2019.pdf Acesso em: 1 abr. 2025.

PROMOVESOLUCOES. ISO 27002: o que é e qual sua importância para a LGPD? [S. l.]: Rafael Rodrigues, 2021. Disponível em: https://promovesolucoes.com/iso-27002-o-que-e-e-qual-sua-importancia-para-a-lgpd/. Acesso em: 26 mar. 2025.

PUCPR. ISO 27000: tudo o que você precisa saber para se destacar na segurança da informação. [S. l.]: Olívia Baldissera, 2021. Disponível em: https://posdigital.pucpr.br/blog/iso-27000. Acesso em: 25 mar. 2025.

RODRIGUES, A. F.; GONÇALVES, J. P.; CASTILHO, M. V.; MARTINS, H. P. SEGURANÇA EM REDES SEM FIO: principais formas de ataques, testes de invasão e modelos de segurança. [S. l.], 2020. Disponível em: https://ric.cps.sp.gov.br/bitstream/123456789/10155/1/redesdecomputadores_2021_1_alinerodrigues_segurancaemredessemfio.pdf. Acesso em: 1 abr. 2025.

SILVA, D. G. Segurança da informação por meio de redes neurais artificiais. [S. l.], 10 out. 2021. Disponível em: https://www.nucleodoconhecimento.com.br/tecnologia/artificiais. Acesso em: 19 mar. 2025.

SONICWALL. *Datasheet: SonicWall TZ series gen 7.* [S. l.], 2025. Disponível em: https://www.sonicwall.com/resources/datasheet/datasheet-sonicwall-tz-series-gen-7. Acesso em: 1 abr. 2025.

SONICWALL. *Guia do usuário do SONICWALL NSa 4700 network security appliance.* [S. l.], 2022. Disponível em: https://manuals.plus/sonicwall/sonicwall-nsa-4700-network-security-appliance-manual. Acesso em: 1 abr. 2025.

SONICWALL. SonicWall next-generation firewalls: technical documentation. [S. l.], 2025. Disponível em: https://www.sonicwall.com/support/technical-documentation/. Acesso em: 1 abr. 2025.

WAZLAWICK, R. S. *Metodologia de pesquisa para ciência da computação.* [S. l.]: Elsevier Editora Ltda., 2014.

WIKIPEDIA. Segurança da informação. In: Segurança da informação. [S. l.], mar. 2019. Disponível em: https://pt.wikipedia.org/wiki/Seguran%C3%A7a_da_informa%C3%A7%C3%A3o. Acesso em: 12 dez. 2025.

SANTOS, G. B. Segurança da informação em ambientes corporativos. [S. l.], 2021. https://repositorio.sis.puc-campinas.edu.br/bitstream/handle/123456789/15028/ceatec_ppggrt_me_Gevanildo_BS_parcial.pdf?sequence=1&isAllowed=y. Acesso em: 2 de abr. 2025.

SILVA, C. E. M. A Segurança em redes Wi-Fi Corporativas: Estudo de caso na Marinha do Brasil. [S. l.], 2010. Disponivel em: https://pantheon.ufrj.br/bitstream/11422/3352/1/CSilva.pdf. Acesso em: 4 de mar. 2025.

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 Daniel Soares Masuda do Curso de Ciencia da Computação, matrícula 20202002800207, telefone: +55 (62) 98207-0867 e-mail danielmasuda123@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 O FIREWALL SONICWALL, 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, 16 de Setembro de 2025.

Assinatura do autor: gov.br Documento assinado digitalmente DANIEL SOARES MASUDA Data: 16/09/2025 18:54:46-0300 Verifique em https://validar.iti.gov.br

Nome completo do autor: Daniel Soares Masuda

Assinatura do professor–orientador: gov.br Documento assinado digitalmente SOLANGE DA SILVA Data: 16/09/2025 19:34:56-0300 Verifique em https://validar.iti.gov.br

Nome completo do professor-orientador: Solange da Silva