CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE LINS PROF. ANTONIO SEABRA
CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

EDUARDO FRANCISCO GOMES

ANÁLISE DA IMPLEMENTAÇÃO DE SD-WAN COM FIREWALL DE PRÓXIMA GERAÇÃO NGFW: UMA ABORDAGEM BASEADA NOS PROTOCOLOS IPSEC E OSPF

LINS/SP
2º SEMESTRE/2025

CENTRO ESTADUAL DE EDUCAÇÃO TECNOLÓGICA PAULA SOUZA
FACULDADE DE TECNOLOGIA DE LINS PROF. ANTONIO SEABRA
CURSO SUPERIOR DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

EDUARDO FRANCISCO GOMES

ANÁLISE DA IMPLEMENTAÇÃO DE SD-WAN COM FIREWALLS DE PRÓXIMA GERAÇÃO NGFW: UMA ABORDAGEM BASEADA NOS PROTOCOLOS IPSEC E OSPF

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de Lins Prof. Antônio Seabra, para obtenção do Título de Tecnólogo(a) em Análise e Desenvolvimento de Sistemas

Orientador: Prof. Dr. Alciano Gustavo Genovez de Oliveira

LINS/SP
2º SEMESTRE/2025

Gomes, Eduardo Francisco

G633a Análise da implementação de SD-WAN com firewall de próxima geração NGFW: uma abordagem baseada nos protocolos IPsec e OSPF / Eduardo Francisco Gomes. — Lins, 2025.

52f.

Trabalho de Conclusão de Curso (Tecnologia em Análise e Desenvolvimento de Sistemas) — Faculdade de Tecnologia de Lins Professor Antonio Seabra: Lins, 2025.

Orientador(a): Dr. Alciano Gustavo Genovez Oliveira

1. SD-WAN. 2. IPSec. 3. OSPF. 4. Firewall. 5. Simulação de Redes. I. Oliveira, Alciano Gustavo Genovez. II. Faculdade de Tecnologia de Lins Professor Antonio Seabra. III. Título.

CDD 004.21

Gerada automaticamente pelo módulo web de ficha catalografica da FATEC Lins mediante dados fornecidos pelo(a) autor(a).

EDUARDO FRANCISCO GOMES

ANÁLISE DA IMPLEMENTAÇÃO DE SD-WAN COM FIREWALL DE PRÓXIMA GERAÇÃO NGFW: UMA ABORDAGEM BASEADA NOS PROTOCOLOS IPSEC E OSPF

Trabalho de Conclusão de Curso apresentado à Faculdade de Tecnologia de Lins Prof. Antônio Seabra, como parte dos requisitos para obtenção do título de Tecnólogo em Análise e Desenvolvimento de Sistemas sob orientação do Prof. Dr. Alciano Gustavo Genovez de Oliveira

Data de aprovação: 12/12/2025

SIGNATÁRIO
Andeson Pazin
Data 03/02/2026 14:36
#d88f42ad012611f1800e42010a2b601f

SIGNATÁRIO
Alciano G. G. de Oliveira
Data 03/02/2026 20:54
#d8982dd7012611f1800e42010a2b601f

Prof. Dr. Alciano Gustavo Genovez de Oliveira

SIGNATÁRIO
Fernando Augusto Garcia Muzzi
Data 03/02/2026 17:24
#d8a27f1e012611f1800e42010a2b601f

Prof. Dr. Fernando Augusto Garcia Muzzi

SIGNATÁRIO
Thiago Galdim Bergamaschi
Data 04/02/2026 09:20
#d8b04dab012611f1800e42010a2b601f

Prof. Thiago Galdim Bergamaschi

DEDICATÓRIA

Dedico este trabalho a Deus, e à minha família, que sempre me apoia em tudo.

Eduardo Francisco Gomes

AGRADECIMENTOS

Agradeço a Deus por sempre me guiar e estar presente em minha vida, à minha família pelo incondicional apoio e a todos os colegas que fizeram parte dessa jornada.

Por fim, registro minha sincera gratidão ao Professor Alciano Gustavo G. de Oliveira. Seu direcionamento técnico preciso, ensinamentos e orientação constante foram cruciais e decisivos para a qualidade e a concretização bem-sucedida deste projeto.

Eduardo Francisco Gomes

RESUMO

A crescente necessidade por redes de transmissão de dados para interconectar de forma segura e eficiente empresas e suas filiais, aliada à utilização intensiva de aplicações em nuvem, tem impulsionado a demanda por arquiteturas de rede mais adaptáveis, escaláveis e seguras. Neste contexto, a tecnologia SD-WAN (Software-Defined Wide Area Network) surge como uma alternativa estratégica a soluções tradicionais, como a infraestrutura MPLS (Multiprotocol Label Switching), que envolvem altos custos e complexidade na implementação. Adiante, a SD-WAN, quando combinada com firewalls de próxima geração e protocolos de segurança e roteamento, como IPsec e OSPF, oferece maior controle, automação e desempenho em redes distribuídas. Este trabalho tem como objetivo analisar a implementação da SD-WAN em ambientes simulados, utilizando firewalls de última geração “NGFWs’, com foco na performance e segurança dos túneis IPsec e no roteamento dinâmico com OSPF. Outrossim, os testes práticos foram realizados com o auxílio do simulador de redes computacionais GNS3. Os resultados obtidos evidenciam as vantagens e desafios da integração dessas tecnologias, oferecendo contribuições significativas para a aplicação de redes inteligentes e seguras.

Palavras-chave: SD-WAN. IPSec. OSPF. Firewall. Simulação de redes.

ABSTRACT

The growing need for data transmission networks to securely and efficiently interconnect companies and their branches, coupled with the intensive use of cloud applications, has driven demand for more adaptable, scalable and secure network architectures. In this context, SD-WAN (Software-Defined Wide Area Network) technology has emerged as a strategic alternative to traditional solutions, such as MPLS (Multiprotocol Label Switching) infrastructure, which involve high implementation costs and complexity. Furthermore, SD-WAN, when combined with next-generation firewalls and security and routing protocols such as IPsec and OSPF, offers greater control, automation and performance in distributed networks. This work aims to analyze the implementation of SD-WAN in simulated environments, using next-generation firewalls (NGFWs), focusing on the performance and security of IPsec tunnels and dynamic routing with OSPF. Practical tests were also carried out using the GNS3 computer network simulator. The results obtained show the advantages and challenges of integrating these technologies, offering significant contributions to the application of intelligent and secure networks.

Keywords: SD-WAN. IPSec. OSPF. Next-generation Firewalls. Network simulation.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ARP – *Address Resolution Protocol*

CLI – *Command-line Interface*

EGP – *Exterior Gateway Protocol*

GNS3 – *Graphical Network Simulator-3*

GUI – *Graphical User Interface*

IETF – *Internet Engineering Task Force*

IGP – *Interior Gateway Protocol*

IP – *Internet Protocol*

IPSec – *IP Security*

LAN – *Local Area Network*

MPLS – *Multiprotocol Label Switching*

NAT – *Network Address Translation*

NETem – *Network Emulator*

NGFW – *Next-Generation Firewall*

OSI – *Open Systems Interconnection*

OSPF – *Open Shortest Path First*

QoS – *Quality of Service*

RFC – *Request for Comments*

SD-WAN – Software-Defined Wide Area Network

SLA – *Service Level Agreement*

VPC – *Virtual PC / Virtual Private Cloud*

VPN – *Virtual Private Network*

WAN – *Wide Area Network*

LISTA DE SÍMBOLOS

% – Porcentagem

s – Segundo

ms – Milissegundo

SUMÁRIO

1 INTRODUÇÃO

A crescente demanda por conexões seguras, eficazes e de alto desempenho entre unidades de negócios, aliada ao uso intensivo de aplicações em nuvem, tem impulsionado a busca por arquiteturas de rede mais flexíveis, escaláveis e seguras. Nesse cenário, modelos tradicionais de interligação, como os baseados em MPLS (Multiprotocol Label Switching), têm revelado limitações severas, principalmente em termos de custo, escalabilidade e complexidade em sua operação (GILL et al., 2019; CISCO, 2020).

As redes WAN tradicionais exigem configurações muito manuais, nas quais rotas entre filiais e matriz são ativadas ou desativadas manualmente pelos administradores de rede. Além disso, cada tecnologia utilizada na interligação (como links dedicados, redes privadas, entre outros) demanda políticas de roteamento diferentes, o que torna a gestão mais difícil e propensa a erros. Esse tipo de cenário necessita de profissionais altamente especializados para operar e manter a infraestrutura, o que contribui para um aumento significativo nos custos operacionais e torna o processo de escalabilidade lento e muito custoso (MEHMOOD et al., 2020).

Em contrapartida, a SD-WAN (Software-Defined Wide Area Network) surge como uma solução moderna, econômica e estratégica. Essa tecnologia cria uma rede lógica (ou virtual) sobreposta à rede física já existente, permitindo que a alternância de rotas entre diferentes links ocorra de forma automática e imperceptível ao usuário final (FERRAZANI; COSTA, 2021). Assim, mesmo em casos de falhas ou congestionamento, o tráfego pode ser redirecionado dinamicamente sem prejuízos na experiência do usuário.

Outro ponto importante é que, com a SD-WAN, as configurações podem ser realizadas de forma centralizada, com menor complexidade e maior controle por parte das próprias empresas, sem depender de provedores de internet. Além disso, a implantação dessa tecnologia apresenta um custo relativamente baixo: basta adquirir roteadores ou firewalls compatíveis com a solução, como os dispositivos FortiGate, da Fortinet, por exemplo, que já integram recursos avançados de segurança e desempenho (FORTINET, 2023).

Com a adoção de firewalls de próxima geração (NGFW), como o FortiGate, a SD-WAN também oferece um controle muito maior do tráfego de rede, permitindo priorizar aplicações críticas (como chamadas de vídeo, acesso a sistemas

corporativos ou videoconferências) em detrimento de aplicações menos relevantes. Esse controle é baseado no desempenho das aplicações e proporciona respostas mais rápidas e conexões mais confiáveis, além de possibilitar uma gestão de desempenho voltada especificamente para as necessidades do negócio (GARTNER, 2022; FORTINET, 2023).

Além disso, a tecnologia fornece relatórios detalhados e completos sobre o tráfego e o desempenho da rede, permitindo que a equipe de TI identifique gargalos, otimize recursos e garanta um melhor nível de serviço (IDG, 2021).

Conforme destaca a Cisco (2025), “a SD-WAN é uma abordagem moderna para redes WAN que oferece uma conectividade mais flexível, segura e econômica, permitindo o uso de múltiplos links de forma inteligente, com gerenciamento centralizado, políticas de segurança integradas e suporte a protocolos como IPsec e OSPF”.

Diante desse contexto, este trabalho tem como objetivo analisar a implementação da SD-WAN em ambientes simulados, utilizando firewalls de última geração com foco na performance dos túneis criptografados via IPsec e no comportamento do roteamento dinâmico com o protocolo OSPF. A pesquisa é conduzida por meio do simulador GNS3.

O estudo visa não apenas destacar os benefícios técnicos da integração entre SD-WAN, firewalls NGFW e protocolos de segurança e roteamento, mas também demonstrar, de forma prática, como essa tecnologia pode ser aplicada em ambientes corporativos para alcançar maior eficiência, segurança e controle. A relevância acadêmica está na análise conjunta de tecnologias contemporâneas de conectividade e proteção de dados, enquanto a contribuição prática recai sobre a avaliação de soluções mais acessíveis, rápidas de implementar e com menor dependência de provedores de internet e infraestrutura tradicional.

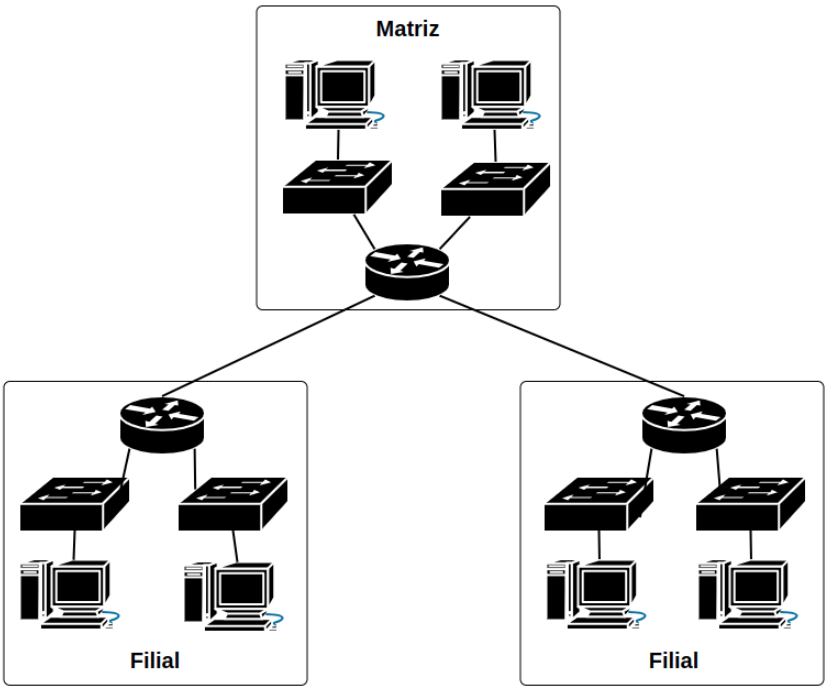
2 CONCEITOS BÁSICOS

Neste capítulo são apresentados os conceitos que serão utilizados e aplicados para nortear este trabalho. São eles: redes WAN e suas limitações tradicionais, o funcionamento e os benefícios da tecnologia SD-WAN, o papel dos firewalls de próxima geração na segurança de redes corporativas, além dos protocolos IPsec e OSPF, que serão utilizados na implementação prática para prover segurança e roteamento dinâmico. A abordagem desses fundamentos teóricos é essencial para compreender os benefícios da proposta deste trabalho, bem como para embasar tecnicamente a arquitetura de rede que será simulada.

2.1 REDES CORPORATIVAS

As redes corporativas são infraestruturas de comunicação que interligam computadores, servidores e dispositivos de uma organização, permitindo a troca de informações, o compartilhamento de recursos e o acesso a sistemas internos. Em ambientes distribuídos, é comum que essas redes se estendam para filiais geograficamente separadas, o que exige soluções robustas de conectividade, segurança e gerenciamento (TANENBAUM, 2013).

Figura 2.1 - Redes corporativas



Fonte: Elaborada pelo autor, 2025

2.2 FIREWALLS DE PRÓXIMA GERAÇÃO (NEXT-GENERATION FIREWALLS)

Os firewalls de próxima geração (NGFWs) são dispositivos de segurança avançados que evoluíram dos firewalls tradicionais para oferecer proteção mais robusta e inteligente contra ameaças modernas. Além de realizar a filtragem básica de pacotes, os NGFWs integram uma série de funcionalidades adicionais, como a inspeção profunda de pacotes (DPI), o controle de aplicações, a filtragem baseada em usuários e a integração nativa com VPNs IPsec. Essas características permitem que os NGFWs não apenas bloqueiem tráfego malicioso, mas também detectem e respondam a atividades suspeitas de maneira mais eficiente e dinâmica.

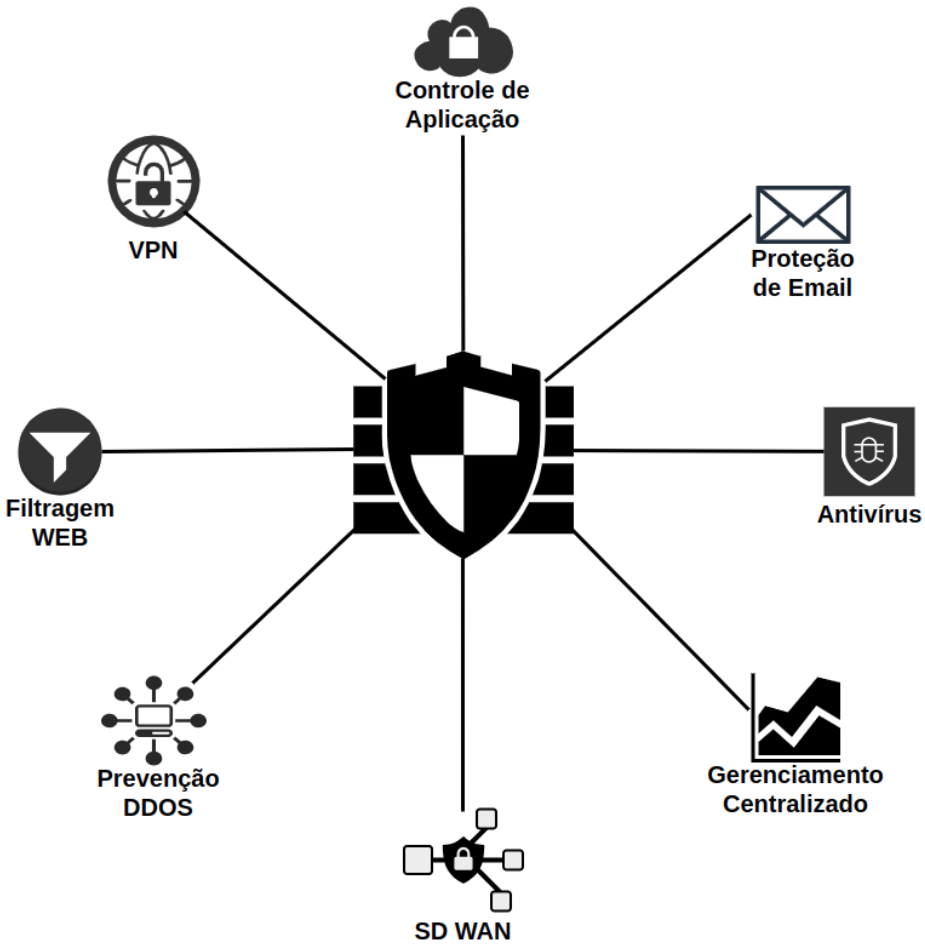
Esses dispositivos são capazes de identificar e bloquear tráfego de aplicações específicas, como redes sociais ou serviços de compartilhamento de arquivos, independentemente da porta ou protocolo utilizados, o que os torna mais eficazes na mitigação de ameaças avançadas, como malware e ataques de dia zero. Além disso, o controle granular de aplicativos possibilita que as organizações definam políticas de

acesso baseadas no comportamento e necessidade dos usuários, otimizando a segurança sem comprometer a produtividade.

De acordo com a Cisco (2020), "os NGFWs são projetados para fornecer visibilidade e controle granulares sobre o tráfego de rede, permitindo a aplicação de políticas de segurança adaptativas e integradas em tempo real". Esses dispositivos também oferecem capacidades de análise de tráfego em tempo real, identificando padrões de comportamento e criando alertas e relatórios detalhados para incidentes de segurança.

Sua utilização é imprescindível em redes empresariais modernas, onde a segurança deve ser aplicada de forma centralizada e com alta visibilidade, especialmente em arquiteturas distribuídas como as implementadas com SD-WAN.

Figura 2.2 - Firewall de Próxima Geração



Fonte: Elaborada pelo autor, 2025

2.3 REDE UNDERLAY

A rede Underlay é a infraestrutura física que transporta o tráfego entre os diferentes dispositivos da rede, incluindo roteadores, switches e links de comunicação. No contexto de SD-WAN, a rede underlay é imprescindível, pois fornece a conectividade básica entre as localidades, mas não é responsável pela inteligência de roteamento ou aplicação de políticas de tráfego. Essa rede pode ser baseada em links privados, como MPLS, ou links públicos, como a internet.

A principal característica da rede underlay é a sua simplicidade. Ela lida com a entrega básica de pacotes entre pontos, sem controlar ou otimizar o tráfego de forma inteligente. No entanto, sua performance e confiabilidade são críticas para garantir o bom funcionamento da SD-WAN. O monitoramento constante da rede underlay, visando detectar falhas e problemas de latência, é essencial para garantir que a rede overlay, que depende da infraestrutura subjacente, funcione de forma eficiente.

2.4 REDE OVERLAY

A rede Overlay é a camada de rede virtualizada que opera acima da infraestrutura física da rede underlay. Em uma implementação de SD-WAN, a rede overlay é responsável por gerenciar o tráfego de dados de forma inteligente, aplicando políticas de roteamento, segurança e qualidade de serviço (QoS) de acordo com as necessidades das aplicações. A rede overlay utiliza a infraestrutura física da rede underlay, mas cria caminhos lógicos independentes para o tráfego, de acordo com as exigências de desempenho e segurança.

No contexto de SD-WAN, a rede overlay permite que a organização tenha controle total sobre as políticas de tráfego, como priorização de aplicações sensíveis (ex: voz e vídeo), controle de largura de banda e roteamento dinâmico em tempo real, sem depender das limitações ou custos impostos pela rede underlay. A flexibilidade da rede overlay é um dos maiores diferenciais da SD-WAN, pois permite adaptar rapidamente o comportamento da rede às necessidades de negócios. Por meio do quadro 2.1 é possível visualizar analise comparativa entre Redes Overlay e Underlay.

Quadro 2.1 - Redes Overlay versus Underlay

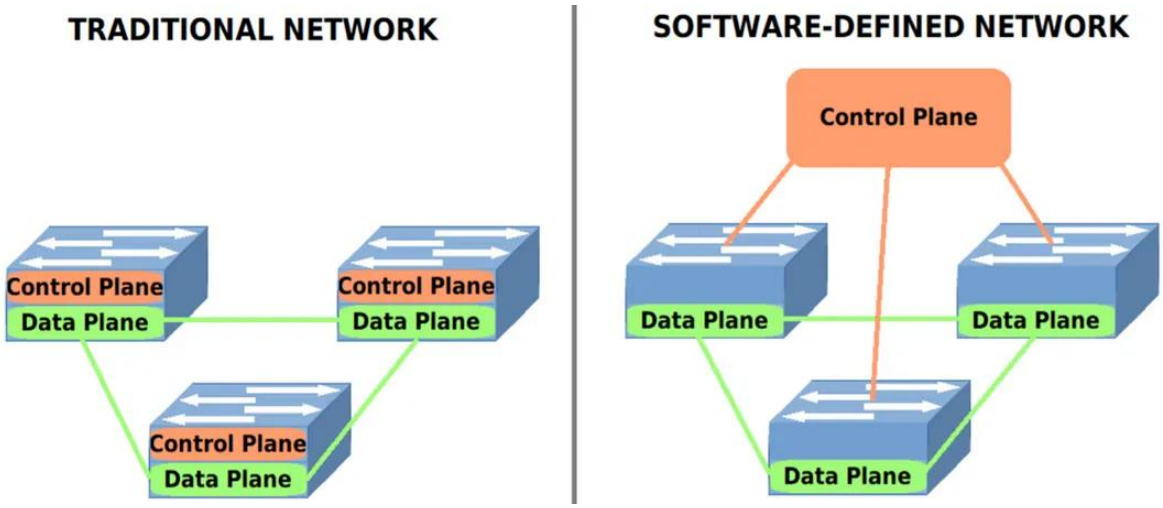
Característica	Underlay	Overlay
Definição	Infraestrutura física real da rede	Rede virtual construída sobre a rede underlay
Componentes	Roteadores, switches, cabos, links físicos	Túneis virtuais, encapsulamento, software de rede
Função	Transportar os dados entre dispositivos fisicamente	Criar redes lógicas para conectar dispositivos isolados
Controle	Normalmente gerenciado por operadoras e administradores de rede	Pode ser controlado por software (SDN, NFV, etc.)
Exemplo	Rede IP tradicional (IPv4/IPv6 com roteamento BGP/OSPF)	VPN, VXLAN, MPLS, SD-WAN

Fonte: Elaborada pelo autor, 2025

2.5 REDES DEFINIDAS POR SOFTWARE (SND – SOFTWARE DEFINED NETWORKING)

Software-Defined Networking (SDN), ou Redes Definidas por Software, é um modelo de arquitetura que visa tornar as redes mais dinâmicas, programáveis e gerenciáveis ao separar logicamente os planos de controle, dados e gerenciamento. Essa abordagem centraliza a tomada de decisão da rede e permite que o comportamento dos dispositivos seja definido por software, tornando a infraestrutura mais flexível e eficiente. Na figura 2.3 é possível entender como uma rede definida por software opera, em comparação com uma rede tradicional.

Figura 2.3 - Redes Definidas por Software



Fonte: Induwara Udanarana, 2023

2.5.1 Plano de Controle (Control Plane)

O Control Plane, ou plano de controle, é responsável por tomar as decisões relacionadas ao roteamento e ao encaminhamento de pacotes. Ele determina o caminho que os dados devem seguir com base em informações como tabelas de roteamento e políticas de rede.

No contexto do SDN, o plano de controle é centralizado em um controlador SDN, que tem uma visão global da rede e toma decisões inteligentes com base em métricas de desempenho, segurança e políticas definidas pela organização. Essa centralização reduz a complexidade dos dispositivos de borda, que deixam de tomar decisões por conta própria e passam a obedecer a comandos emitidos pelo controlador.

2.5.2 Plano de Dados (Data Plane)

O Data Plane, ou plano de dados, também conhecido como plano de encaminhamento, é responsável pelo transporte efetivo dos pacotes de dados entre os dispositivos da rede. Ele atua de forma direta, executando as instruções enviadas pelo plano de controle.

No SDN, switches e roteadores funcionam como dispositivos simples de encaminhamento (forwarding devices), que recebem comandos do controlador SDN e os executam conforme necessário. Isso inclui ações como encaminhar, descartar ou modificar pacotes de acordo com as regras definidas pelo plano de controle.

2.5.3 Plano de Gerenciamento (Management Plane)

O Management Plane, ou plano de gerenciamento, é responsável pela configuração, monitoramento e administração da rede. Ele atua em conjunto com o plano de controle para implementar mudanças na topologia da rede, aplicar atualizações, monitorar desempenho e gerar relatórios.

Em uma arquitetura SDN, o plano de gerenciamento é altamente automatizado e baseado em interfaces de programação (APIs) que permitem a integração com sistemas de orquestração, ferramentas de monitoramento e aplicações de segurança. Isso viabiliza uma gestão mais ágil e inteligente, reduzindo o tempo de resposta a falhas e otimizando o uso dos recursos de rede.

2.6 SD-WAN (SOFTWARE-DEFINED WIDE AREA NETWORK)

A tecnologia SD-WAN (Software-Defined Wide Area Network) é uma aplicação prática dos princípios das Redes Definidas por Software (SDN), voltada especificamente para ambientes de redes WAN. Assim como o SDN separa os planos de controle e de dados em redes locais e data centers, a SD-WAN implementa essa separação em redes geograficamente distribuídas, permitindo uma gestão centralizada, dinâmica e inteligente do tráfego entre filiais, datacenters e aplicações em nuvem.

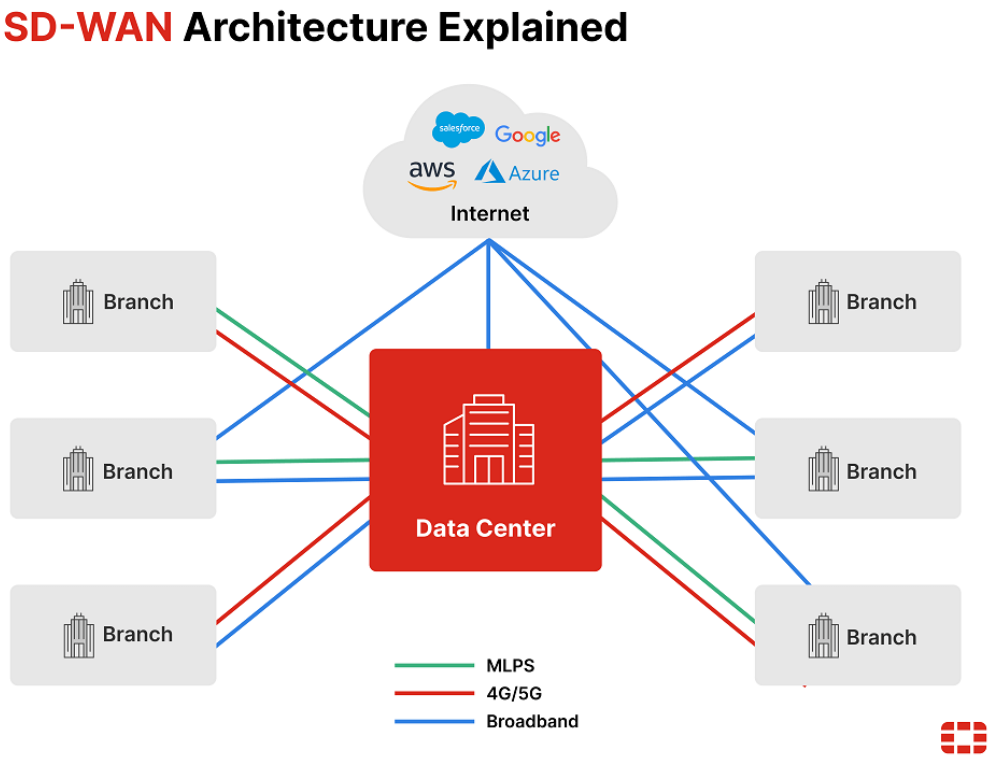
A SD-WAN é uma arquitetura baseada em software que separa o plano de controle do plano de dados na rede WAN. Essa separação possibilita o gerenciamento e o roteamento do tráfego de maneira dinâmica, com base em políticas definidas pelo administrador da rede, considerando critérios como tipo de aplicação, qualidade dos links e prioridade de serviço.

Segundo a Fortinet (2021), "a SD-WAN permite que empresas substituam circuitos MPLS caros por conexões de banda larga mais acessíveis, sem sacrificar a

qualidade, confiabilidade ou segurança do serviço". Essa abordagem oferece maior visibilidade e controle sobre o tráfego, reduz a dependência de enlaces dedicados, aumenta a resiliência da rede ao permitir múltiplos caminhos de comunicação (como links de Internet comum, MPLS e redes LTE), e ainda possibilita priorizar aplicações ou serviços críticos em tempo real.

Além disso, a centralização do controle por meio de um controlador SD-WAN facilita a configuração, a aplicação de políticas e o monitoramento em tempo real, reduzindo a complexidade operacional e aumentando a agilidade na resposta a falhas ou mudanças na rede corporativa. Como será abordado nos capítulos seguintes, essas características fazem da SD-WAN uma solução eficiente e segura para organizações que dependem cada vez mais de aplicações em nuvem e conectividade entre unidades remotas.

Figura 2.4 - SD-WAN

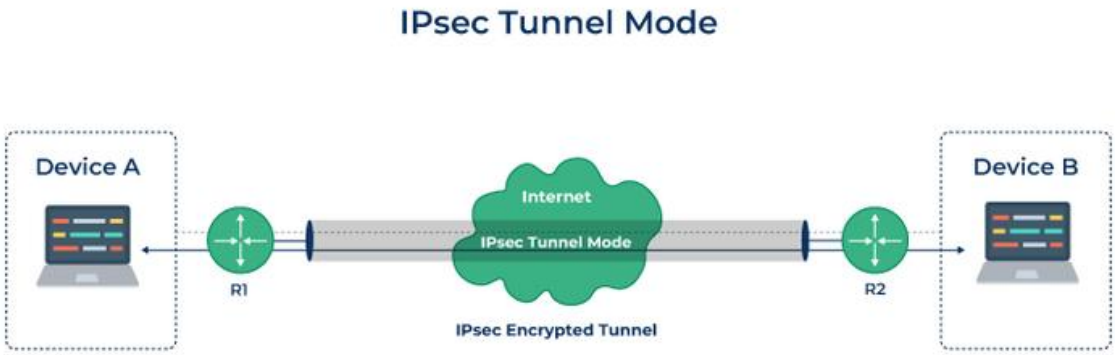


Fonte: Fortinet, 2025

2.7 IPSEC (INTERNET PROTOCOL SECURITY)

O IPsec é um conjunto de protocolos usados para proteger comunicações na camada de rede do modelo OSI, sendo essencial para fornecer confidencialidade, integridade e autenticidade ao tráfego IP (RFC 4301, IETF). É composto por dois protocolos principais: o Authentication Header (AH), focado na integridade, e o Encapsulating Security Payload (ESP), que é o protocolo preferencial por incluir a criptografia (confidencialidade) dos dados. Em soluções de rede distribuída, o IPsec é utilizado no Modo Túnel para encapsular e criptografar o pacote IP original, estabelecendo as VPNs de site-a-site que criam a rede Overlay segura sobre a infraestrutura pública (Tanenbaum, 2013).

Figura 2.5 - IPSec



Fonte: GeeksForGeeks, 2025

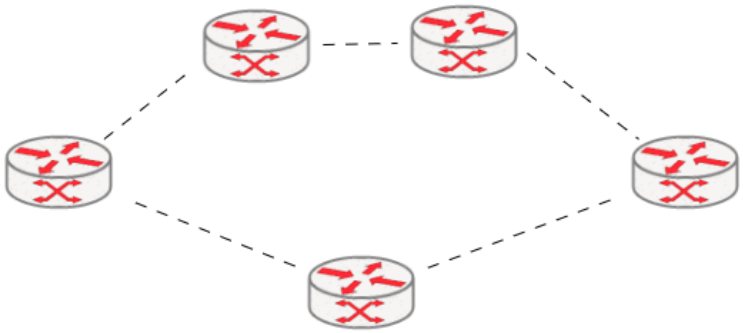
2.8 PROTOCOLOS DE ROTEAMENTO

Os protocolos de roteamento são responsáveis por determinar os melhores caminhos para o tráfego de dados entre diferentes redes. Eles permitem que os dispositivos de rede, como roteadores, troquem informações sobre a topologia e atualizem dinamicamente suas tabelas de roteamento com base em mudanças na rede.

Esses protocolos se dividem em duas grandes categorias: internos (IGPs – Interior Gateway Protocols) e externos (EGPs – Exterior Gateway Protocols). Dentre os protocolos internos, destacam-se o RIP (Routing Information Protocol), que utiliza algoritmos de vetor de distância com atualização periódica das rotas, e o OSPF (Open Shortest Path First), que se baseia no estado de enlace e constrói uma visão topológica completa da rede, permitindo decisões mais eficientes — este último será detalhado no Capítulo 3.

Além disso, o protocolo BGP (Border Gateway Protocol), classificado como EGP, é amplamente utilizado para troca de rotas entre sistemas autônomos, como acontece na Internet. Em ambientes corporativos com múltiplas filiais e conexões WAN, a escolha e a correta configuração dos protocolos de roteamento são essenciais para garantir desempenho, redundância e resiliência no tráfego de dados.

Figura 2.6 - Protocolos de roteamento



Fonte: Elaborada pelo autor, 2025

2.9 LARGURA DE BANDA

Largura de banda refere-se à capacidade máxima de transmissão de dados entre dois pontos da rede durante um intervalo de tempo. Medida em megabits ou gigabits por segundo (Mbps, Gbps), ela indica o volume de dados que pode ser trafegado simultaneamente. Esse parâmetro é essencial para avaliar o desempenho de redes corporativas.

Figura 2.7 - Largura de banda

Fonte: Liquid Web, 2025

2.10 VELOCIDADE DE TRANSMISSÃO

A velocidade de transmissão está relacionada à taxa efetiva com que os dados são enviados e recebidos na rede. Diferente da largura de banda teórica, a velocidade real pode ser afetada por latência, congestionamentos, jitter e perdas de pacotes. A ferramenta Wireshark será utilizada para observar esses fatores em tempo real, permitindo a identificação de gargalos e análise da qualidade dos túneis IPsec e rotas configuradas. Conforme definido na RFC 6349, o desempenho de uma rede deve considerar fatores como tempo de ida e volta (RTT), perda de pacotes e capacidade de throughput efetivo para avaliar a qualidade da transmissão de dados (GEORGE et al., 2011).

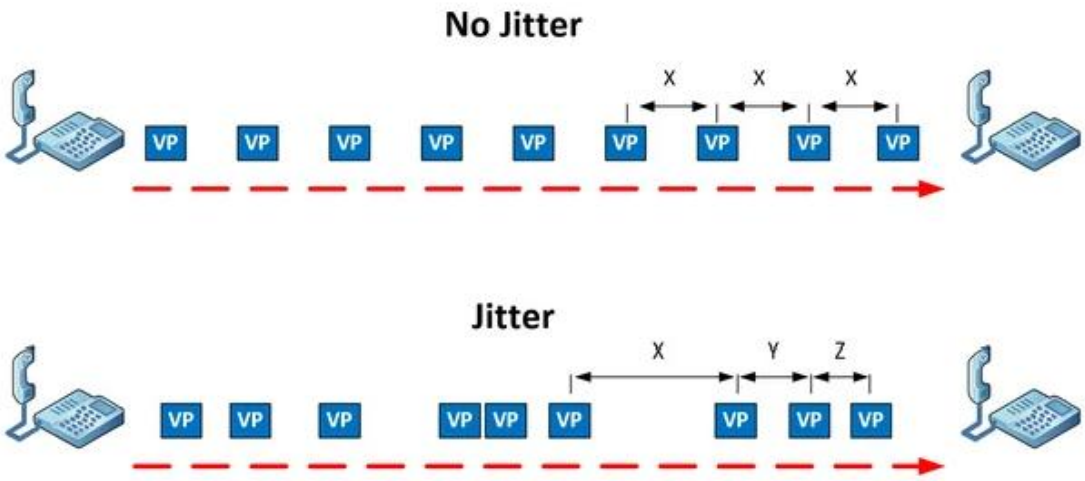
2.11 VARIAÇÃO DE ENTREGA DE PACOTES (JITTER)

Jitter é a variação no tempo de entrega dos pacotes em uma rede. Em aplicações como voz sobre IP (VoIP) e videoconferência, essa oscilação pode comprometer a qualidade da comunicação, causando atrasos, cortes de áudio ou imagem distorcida, conforme pode ser observado na figura 2.7.

Valores elevados de jitter indicam instabilidade na rede e afetam diretamente serviços sensíveis ao tempo. Por isso, soluções como a SD-WAN monitoram

constantemente o jitter, redirecionando o tráfego automaticamente para links com melhor desempenho, garantindo uma comunicação mais estável.

Figura 2.8 - Variância de pacotes (jitter)



Fonte: IR Team, 2025

2.12 SEGURANÇA DA INFORMAÇÃO EM REDES DE COMPUTADORES

A segurança da informação em redes busca proteger os dados contra acesso indevido, modificação não autorizada e indisponibilidade. Essa proteção é baseada nos princípios da confidencialidade, integridade e disponibilidade (tríade CIA), e é aplicada por meio de políticas, autenticação, criptografia e ferramentas como os firewalls de próxima geração. As VPNs (Virtual Private Network), especialmente quando implementadas com IPsec, tem um papel fundamental nesse cenário, pois criam canais seguros de comunicação sobre redes públicas, preservando a privacidade e a autenticidade das informações que trafegam nesse túnel. A integração entre SD-WAN, NGFWs e VPNs fortalece as defesas das redes corporativas distribuídas, promovendo um ambiente mais seguro e confiável.

3 TECNOLOGIAS

Este capítulo aborda as principais tecnologias e protocolos específicos empregados na implementação do projeto. O foco é a integração entre os componentes de segurança (FortiGate, IPsec), a inteligência de rede (SD-WAN) e o

roteamento dinâmico (OSPF), que viabilizam a comunicação segura, eficiente e gerenciável entre as unidades organizacionais.

3.1 FIREWALL DE PRÓXIMA GERAÇÃO (NGFW) FORTIGATE (HUB-AND-SPOKE)

A solução FortiGate, da Fortinet, foi utilizada como o Firewall de Próxima Geração (NGFW), atuando como o principal Edge Device da topologia Hub-and-Spoke. No contexto do projeto, sua relevância reside na sua capacidade de consolidar múltiplos serviços: segurança de borda, suporte nativo à tecnologia SD-WAN e funcionalidade de roteamento via IPsec e OSPF. O FortiGate é o ponto de controle central responsável por monitorar o desempenho dos links WAN e aplicar as regras de Service Level Agreement (SLA) para o roteamento inteligente de tráfego, garantindo uma gestão centralizada de políticas de segurança e conectividade para a Matriz e Filiais (Fortinet, 2021).

Figura 3.1 - Linha de comando Fortigate

```
#conf_file_ver=283768489312446
#buildno=0444
#global_vdom=1
config system global
    set alias "FortiGate-VM64-KVM"
    set hostname "FortiGate-VM64-KVM"
    set timezone 04
end
config system accprofile
    edit "prof_admin"
        set secfabgrp read-write
        set ftviewgrp read-write
        set authgrp read-write
        set sysgrp read-write
        set netgrp read-write
        set loggrp read-write
        set fwgrp read-write
        set vpngrp read-write
        set utmgrp read-write
        set wanoptgrp read-write
        set wifi read-write
    next
end
--More--
```

Fonte: Elaborada pelo autor, 2025

3.2 ROTEADORES CISCO

Os roteadores Cisco foram empregados na simulação para representar a infraestrutura Underlay (a camada física de transporte) que interconecta as unidades da organização. Utilizaram-se dois Roteadores Cisco 7200, que operam como roteadores de Camada 3 e atuam como Provedores de Serviço WAN distintos (Link A e Link B). Sua principal função é simular os múltiplos caminhos e a segregação de tráfego na WAN, sendo que um dos roteadores também é responsável por fornecer conectividade à Internet ao ambiente simulado através de NAT. A interconexão entre os FortiGates e a matriz é realizada através das portas WAN dos roteadores (Gigaethernet 2/0, 3/0 e 4/0), garantindo o roteamento básico para que o FortiGate (a camada Overlay de controle) possa monitorar a qualidade de cada link e aplicar suas regras de SD-WAN de forma inteligente.

Figura 3.2 - Linha de comando Cisco

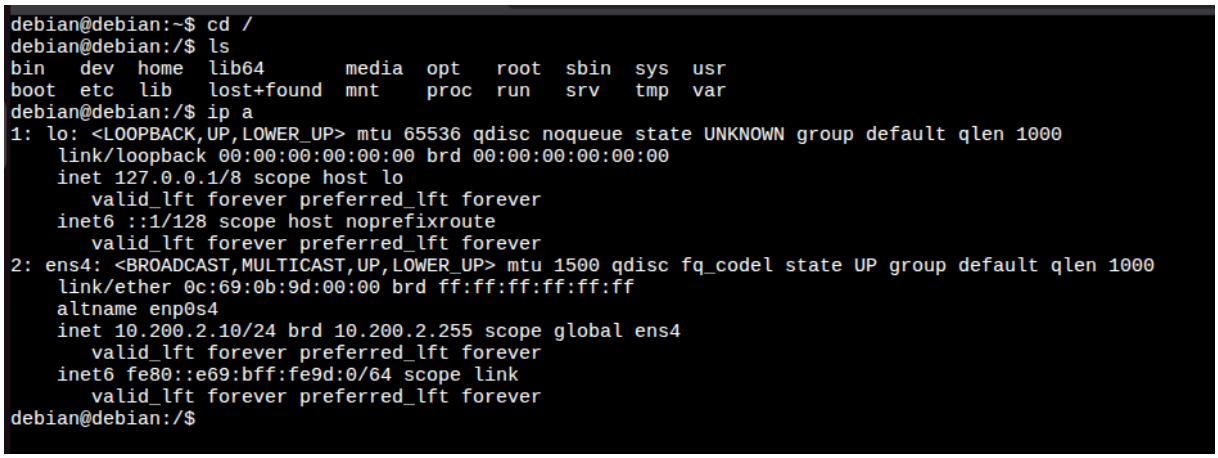
```
ISP111#show ip interface brief
Interface                  IP-Address      OK? Method Status                Protocol
Ethernet0/0                unassigned      YES NVRAM  administratively down down
GigabitEthernet0/0         11.0.0.253      YES NVRAM  up                    up
GigabitEthernet1/0         11.0.0.1        YES NVRAM  up                    up
GigabitEthernet2/0         11.0.0.5        YES NVRAM  up                    up
GigabitEthernet3/0         11.0.0.9        YES NVRAM  up                    up
GigabitEthernet4/0         11.0.0.13       YES NVRAM  up                    up
GigabitEthernet5/0         unassigned      YES NVRAM  administratively down down
GigabitEthernet6/0         192.168.1.191   YES NVRAM  up                    up
NVI0                       11.0.0.253      YES unset  up                    up
ISP111#
```

Fonte: Elaborada pelo autor, 2025

3.3 PCS VIRTUAIS DEBIAN

Foram utilizadas Máquinas Virtuais baseadas no Debian, uma distribuição Linux robusta, para simular os clientes finais (hosts) de cada site. As VPCs Debian atuaram como hosts nas simulações, sendo cruciais para a geração e recebimento de tráfego e para a validação da conectividade e das políticas da SD-WAN. Sua utilização permitiu testar as regras de priorização de tráfego (SLA) do FortiGate de ponta a ponta.

Figura 3.3 - Linha de comando Debian

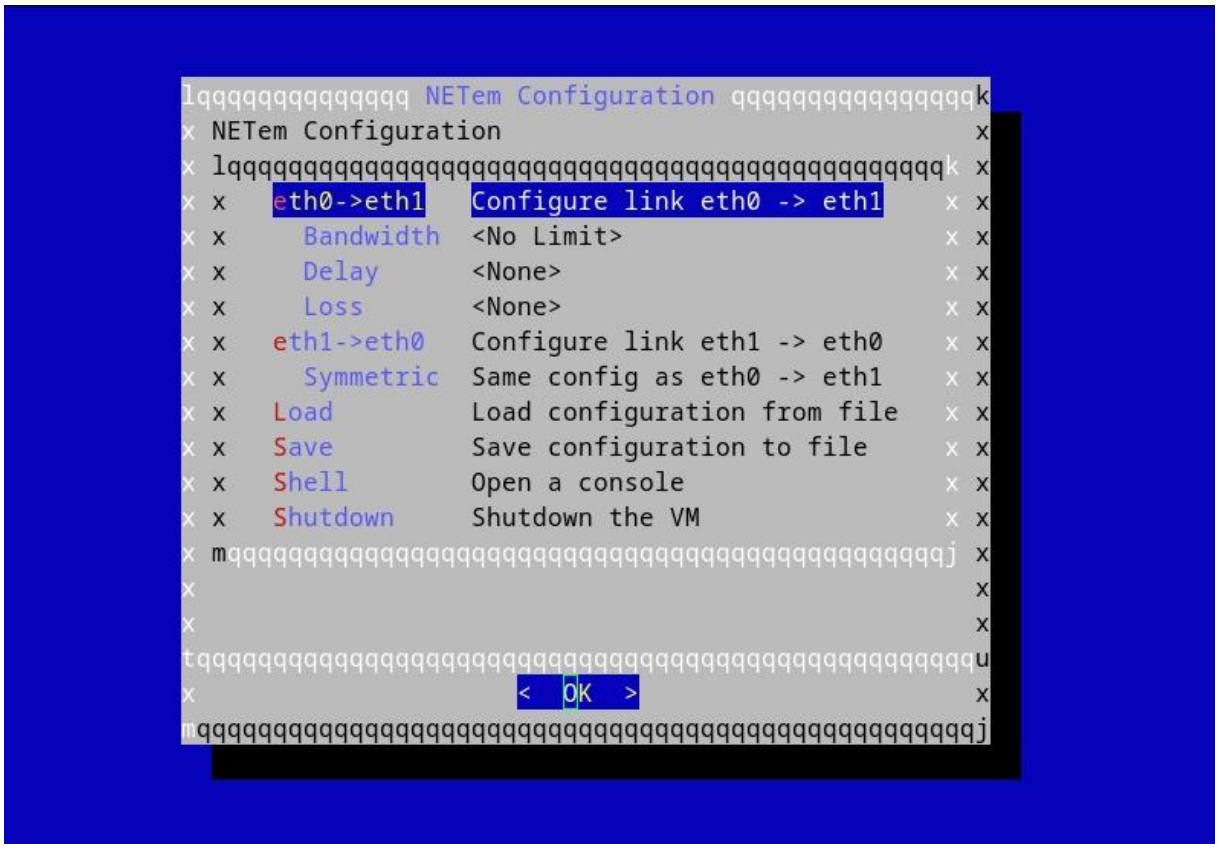


Fonte: Elaborada pelo autor, 2025

3.4 LINUX NETEM

O Linux NETEM (Network Emulator) foi utilizado em máquinas virtuais Linux para simular condições de rede adversas, como aumento de latência, jitter e perda de pacotes. Isso permitiu avaliar o desempenho da SD-WAN em cenários realistas e verificar a resposta da infraestrutura configurada a essas variações.

Figura 3.4 - Interface GNU/Linux NETem

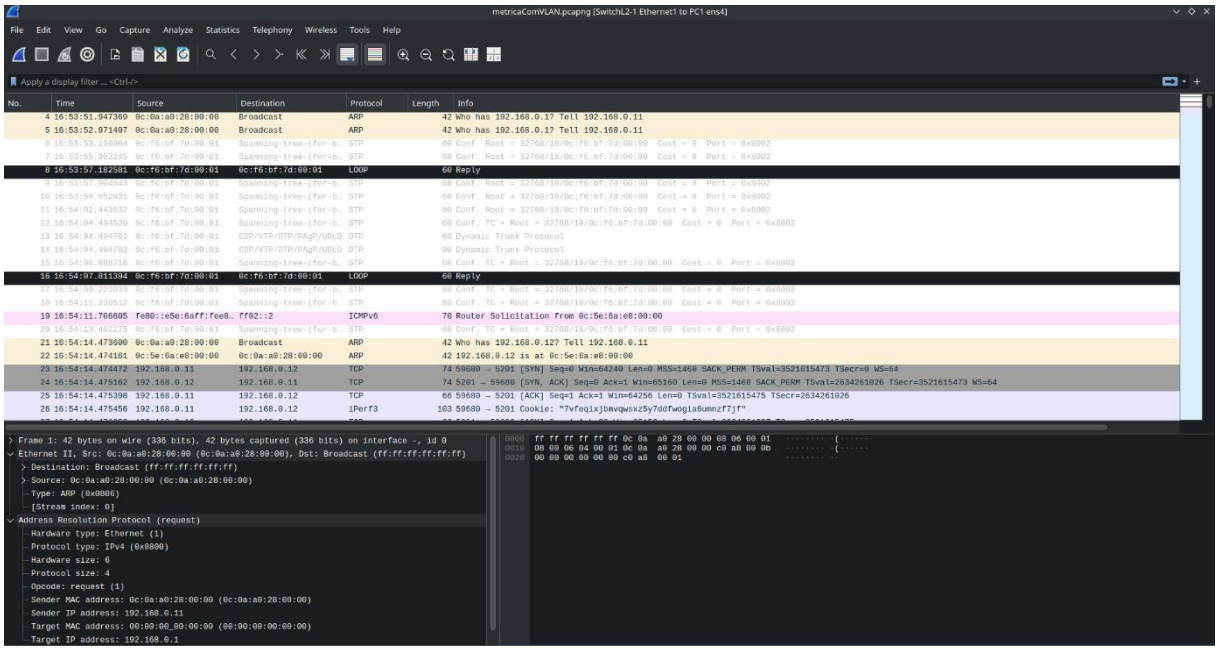


Fonte: Elaborada pelo autor, 2025

3.5 WIRESHARK

O Wireshark é uma ferramenta de captura e análise de pacotes amplamente utilizada em redes de computadores. Ele permite inspecionar protocolos em diferentes camadas, identificar problemas de comunicação e validar o funcionamento de túneis IPsec, protocolos de roteamento como o OSPF e o comportamento do tráfego em ambientes SD-WAN. Sua utilização foi essencial para validar os resultados obtidos nas simulações realizadas no GNS3.

Figura 3.5 - Interface do Wireshark



Fonte: Elaborada pelo autor, 2025

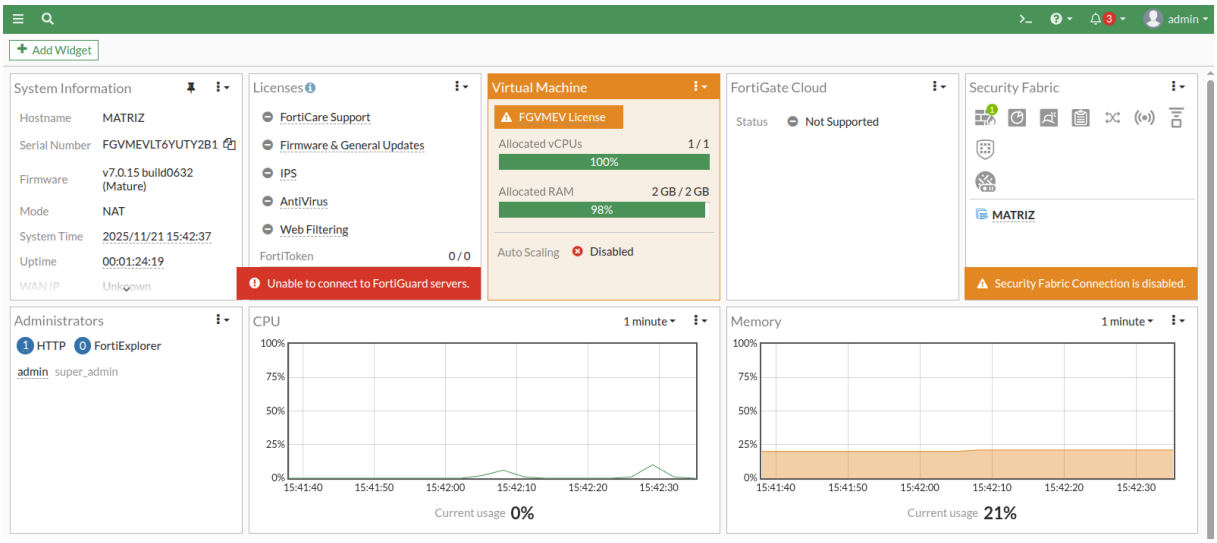
3.6 OSPF (OPEN SHORTEST PATH PROTOCOL)

O OSPF é um protocolo de roteamento dinâmico que permite a troca de informações de topologia entre roteadores. Ele utiliza o algoritmo Dijkstra para calcular o caminho de menor custo entre os dispositivos da rede. No cenário simulado, o OSPF foi utilizado para propagar rotas internamente entre os dispositivos FortiGate, promovendo maior eficiência e resiliência na troca de dados.

3.7 SD WAN

A implementação prática da SD-WAN no projeto foi realizada por meio do FortiGate, que permitiu integrar múltiplos enlaces WAN e definir regras de roteamento baseadas em métricas como latência, jitter e perda de pacotes. Foram criadas políticas para priorização de tráfego crítico e rerroteamento automático em caso de falhas. A SD-WAN foi validada em cenários simulados com diferentes tipos de tráfego, destacando sua eficiência em ambientes corporativos distribuídos.

Figura 3.6 - Interface gráfica do firewall Fortigate

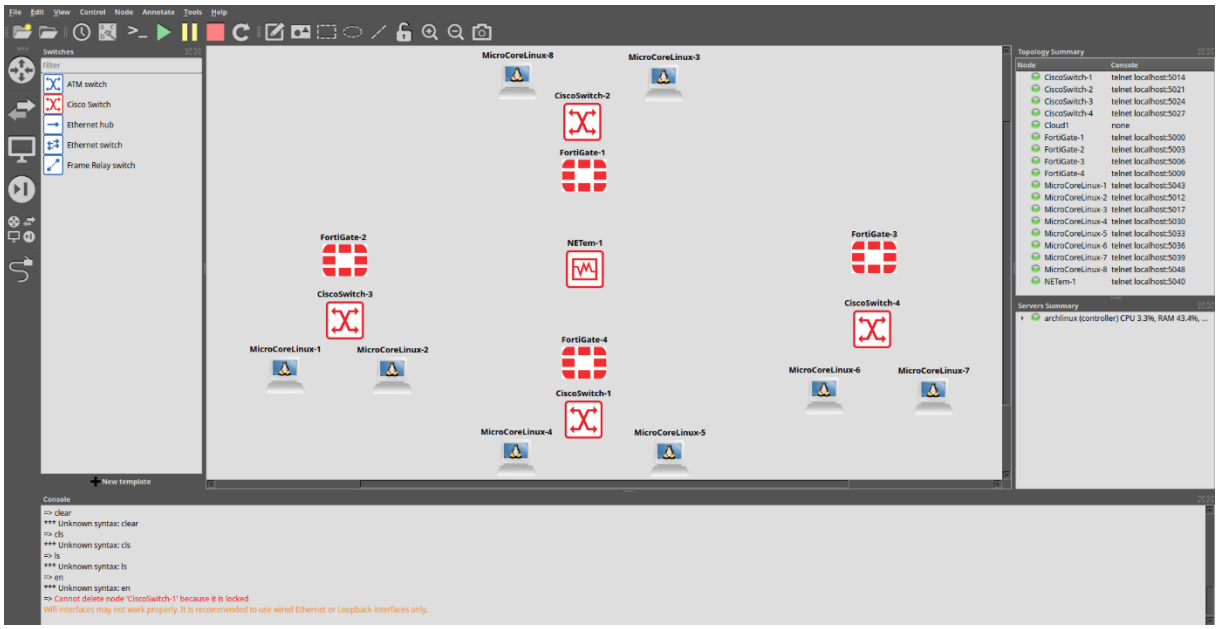


Fonte: Elaborada pelo autor, 2025

3.8 GNS3

Para a validação prática do projeto, foi utilizado o simulador GNS3 (Graphical Network Simulator-3), que permite a emulação de dispositivos reais em um ambiente virtual. O GNS3 possibilita a integração com imagens de firewalls FortiGate e roteadores Cisco, além de máquinas virtuais com Linux para testes de comunicação e captura de pacotes. Essa abordagem foi essencial para a realização de testes de conectividade, performance e segurança.

Figura 3.7 - Interface do GNS3



Fonte: Elaborada pelo autor, 2025

4 IMPLEMENTAÇÃO

Esta seção detalha a metodologia de construção do ambiente de simulação e apresenta a análise da performance do SD-WAN, comprovando a eficácia da integração com os túneis IPsec e o roteamento OSPF.

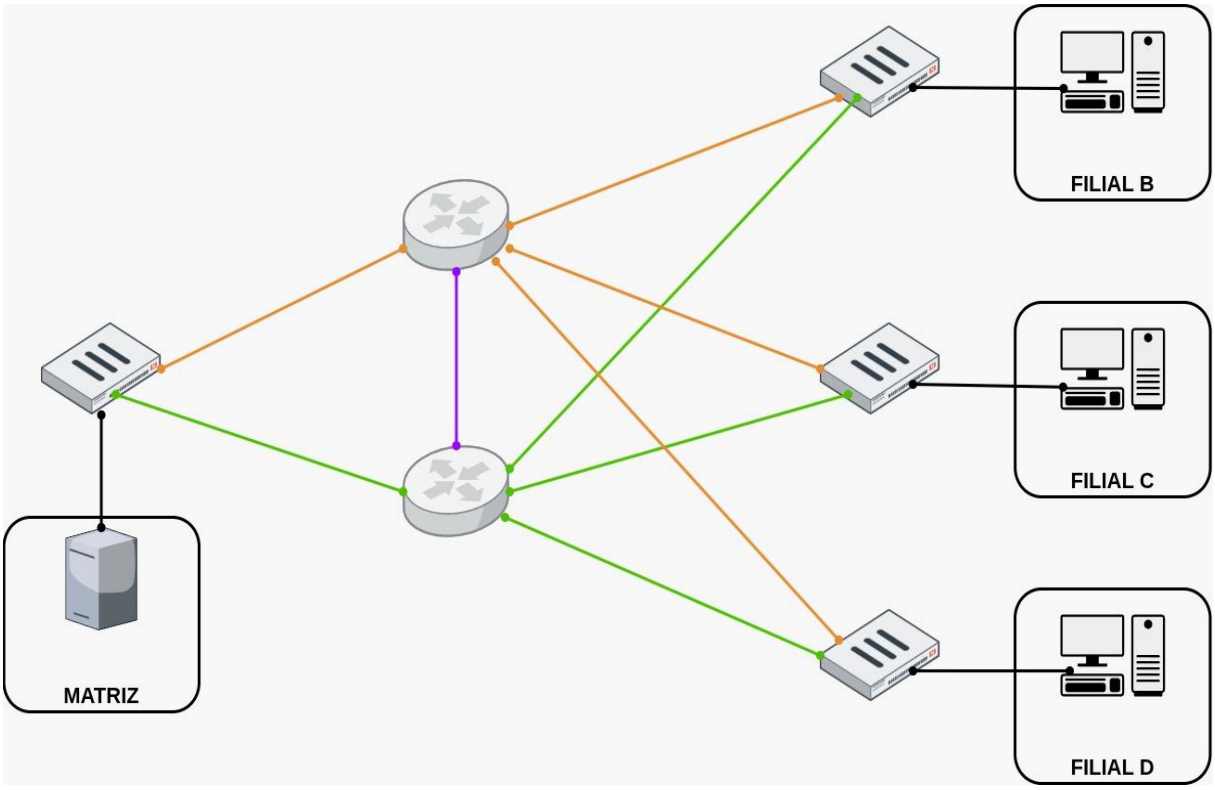
4.1 METODOLOGIA E CONFIGURAÇÃO DA TOPOLOGIA

O ambiente de testes foi construído no simulador GNS3, utilizando quatro FortiGates e dois Roteadores Cisco 7200 para emular a rede distribuída. O sucesso da implementação depende de uma base de endereçamento IP elucidativa e concisa, que garante a conectividade Underlay para o funcionamento da camada Overlay (Fortinet, 2021).

4.2 ARQUITETURA E ENDEREÇAMENTO IP

O ambiente de testes foi implementado no simulador GNS3, utilizando quatro FortiGates (Matriz e três Filiais) e dois Roteadores Cisco 7200 para simular os múltiplos links WAN (Underlay). A conectividade de gerenciamento foi garantida por uma Bridge Linux no sistema operacional host. O endereçamento IP foi segmentado para isolar as redes LAN e WAN, conforme detalhado na Tabela 4.1.

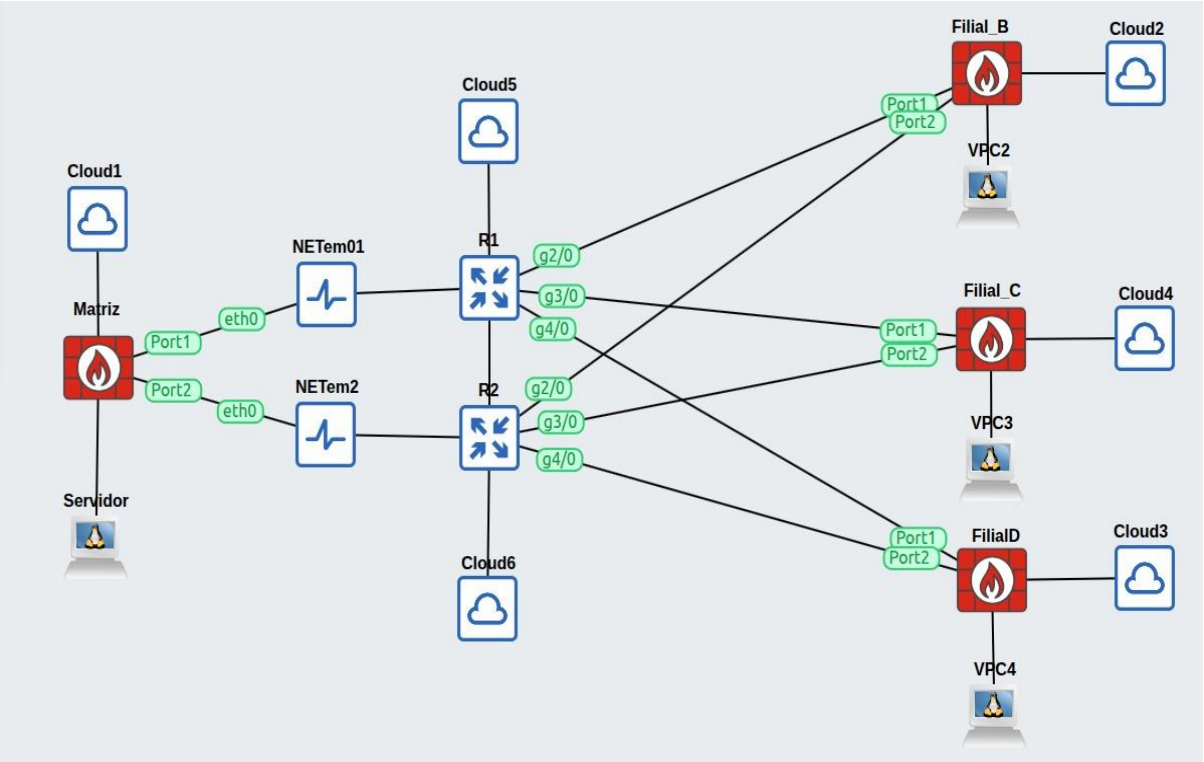
Figura 4.1 - Topologia Lógica da Arquitetura SD-WAN (Hub-and-Spoke)



Fonte: Elaborada pelo autor, 2025

Em seguida, a Figura 4.2 apresenta o ambiente de emulação físico construído no GNS3, detalhando o hardware virtual utilizado — quatro FortiGates, dois Roteadores Cisco 7200, os PCs Debian (VPCs), as clouds, 2 linux NETem — e a interconexão das interfaces (ex: FortiGate Port1 e Port2 conectadas aos roteadores).

Figura 4.2 - Ambiente de Emulação Físico no GNS3



Fonte: Elaborada pelo autor, 2025

Para garantir a rastreabilidade e a segregação de tráfego, o endereçamento IP foi rigorosamente planejado para isolar as redes de Gerenciamento, LAN e WAN. A Tabela 4.1 apresenta o detalhamento completo de cada interface e dispositivo, desde os endereços de Gerenciamento (192.168.1.x/24) até os IDs de túnel VPN (100.64.x.x/32), fornecendo a base técnica exaustiva necessária para a replicação do ambiente simulado.

Tabela 4.1 - Endereçamento IP da Topologia

Tipo de Rede	DIspositivo	Interface	Endereço IP
LAN (Acesso)	Matriz	Port3	10.10.0.1/24
LAN (Acesso)	Filial B	Port3	10.200.2.1/24
LAN (Acesso)	Filial C	Port3	10.200.3.1/24
LAN (Acesso)	Filial D	Port3	10.200.4.1/24
Gerenciamento	Matriz	Port4	192.168.1.101/24
Gerenciamento	Filial B	Port4	192.168.1.102/24

Gerenciamento	Filial C	Port4	192.168.1.103/24
Gerenciamento	Filial D	Port4	192.168.1.104/24
WAN Link A (Underlay)	Matriz	Port1	11.0.0.2/30
WAN Link A (Underlay)	Filial B	Port1	11.0.0.6/30
WAN Link A (Underlay)	Filial C	Port1	11.0.0.10/30
WAN Link A (Underlay)	Filial D	Port1	11.0.0.14/30
WAN Link B (Underlay)	Matriz	Port2	22.0.0.2/30
WAN Link B (Underlay)	Filial B	Port2	22.0.0.6/30
WAN Link B (Underlay)	Filial C	Port2	22.0.0.10/30
WAN Link B (Underlay)	Filial D	Port2	22.0.0.14/30
VPN (Túnel 1)	Matriz	VPNPSK1	100.64.1.1/32
VPN (Túnel 2)	Matriz	VPNPSK2	100.64.2.1/32
VPN (Túnel 1)	Filial B	VPNHUB1	100.64.1.2/32
VPN (Túnel 2)	Filial B	VPNHUB2	100.64.2.2/32
VPN (Túnel 1)	Filial C	VPNHUB1	100.64.1.3/32
VPN (Túnel 2)	Filial C	VPNHUB2	100.64.2.3/32
VPN (Túnel 1)	Filial D	VPNHUB1	100.64.1.4/32
VPN (Túnel 2)	Filial D	VPNHUB2	100.64.2.4/32
Loopback (Router ID)	Matriz	Loopback10	10.255.0.1/32
Loopback (Router ID)	Filial B	Loopback10	10.255.0.2/32
Loopback (Router ID)	Filial C	Loopback10	10.255.0.3/32
Loopback (Router ID)	Filial D	Loopback10	10.255.0.4/32
Interconexão ISP	R1	G0/0	11.0.0.253/30
Interconexão ISP	R2	G0/0	11.0.0.254/30
Internet (NAT)	R1	G6/0	192.168.1.191/24
Internet (NAT)	R2	G6/0	192.168.1.194/24

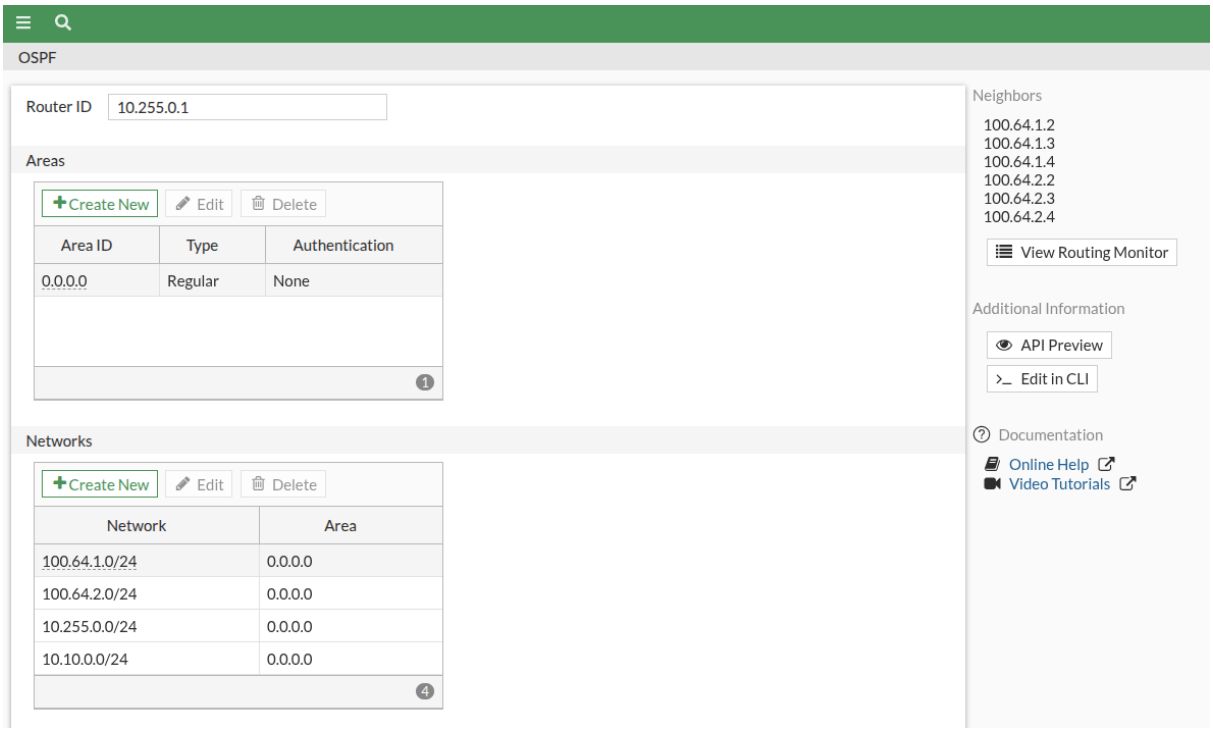
Fonte: Elaborada pelo autor, 2025

4.3 CONFIGURAÇÃO DE ROTEAMENTO OSPF

Para garantir o roteamento dinâmico das redes internas (LANs) de forma resiliente, o protocolo OSPF foi configurado para rodar sobre os túneis IPsec estabelecidos. Essa abordagem garante que as rotas de acesso às sub-redes da Matriz e das Filiais sejam propagadas e atualizadas de forma automática, utilizando o

túnel VPN como um link de transporte. O OSPF foi essencial para o failover ocorrer de forma transparente na camada de roteamento.

Figura 4.3 - Visão geral do OSPF do Firewall Matriz

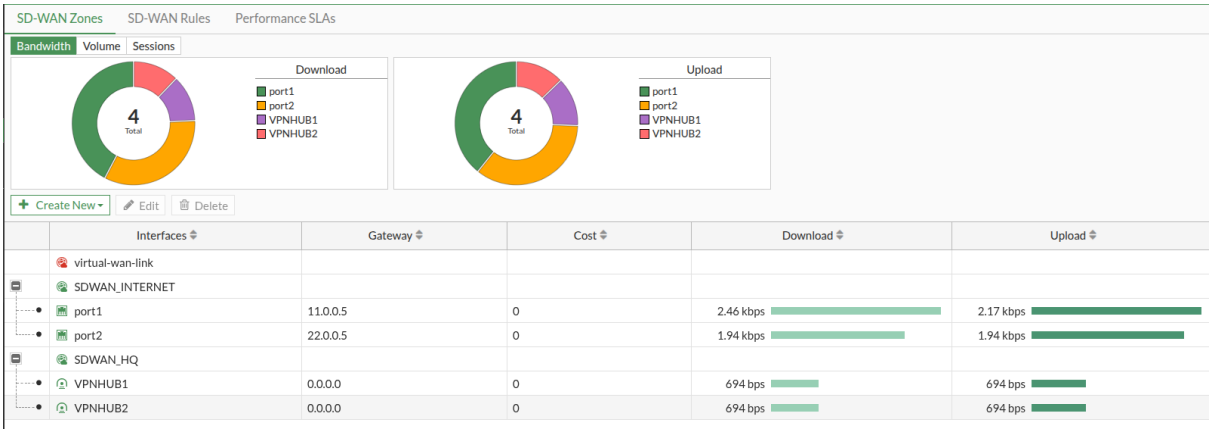


Fonte: Elaborada pelo autor, 2025

4.4 CONFIGURAÇÃO DA ZONA SD-WAN E TÚNEIS IPSEC

A inteligência da rede foi implementada através da configuração de duas Zonas SD-WAN na Matriz e em suas Filiais, refletindo a necessidade de segregação e controle distinto sobre os fluxos de tráfego (Fortinet, 2021). Uma zona, denominada INTERNET, foi estabelecida para agrupar as interfaces físicas WAN (port1 e port2), dedicando-se ao tráfego geral de saída para a Internet sob regras específicas de NAT. Em contrapartida, a zona HQ foi criada especificamente para agrupar os túneis VPN IPsec (identificados como VPNHUB1 e VPNHUB2), sendo dedicada exclusivamente ao tráfego interno e seguro entre a Filial e a Matriz. Essa segregação permite um controle de políticas mais granular e a aplicação da segurança do túnel VPN, que, por sua vez, cria a rede Overlay segura (RFC 4301), garantindo a confidencialidade e integridade dos dados corporativos que transitam sobre o Underlay público (Tanenbaum, 2013).

Figura 4.4 - Zonas SD-WAN e seus respectivos membros



Fonte: Elaborada pelo autor, 2025

4.5 CONFIGURAÇÃO DE POLÍTICAS DE FIREWALL

As políticas de firewall foram estabelecidas para controlar o fluxo de dados (Gartner, 2022). Políticas distintas foram criadas para as zonas: LAN-to-HQ (VPN) com NAT desabilitado, permitindo a comunicação interna, e LAN-to-INTERNET com NAT habilitado, para a navegação web e acesso externo.

Figura 4.5 - Políticas de Firewall

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
POLICY_LAN_TO_HQ	port3	SDWAN_HQ	NETWORK_10.200.0.0/16	GROUP_NETWORK_PRIVATE	always	ALL	ACCEPT	Disabled
POLICY_LAN_TO_INTERNET	port3	SDWAN_INTERNET	NETWORK_10.200.0.0/16	all	always	ALL	ACCEPT	Enabled
POLICY_PERMIT_ANY	any	any	all	all	always	ALL	ACCEPT	Disabled
Implicit Deny	any	any	all	all	always	ALL	DENY	

Fonte: Elaborada pelo autor, 2025

4.6 ANÁLISE E RESULTADOS DE DESEMPENHO

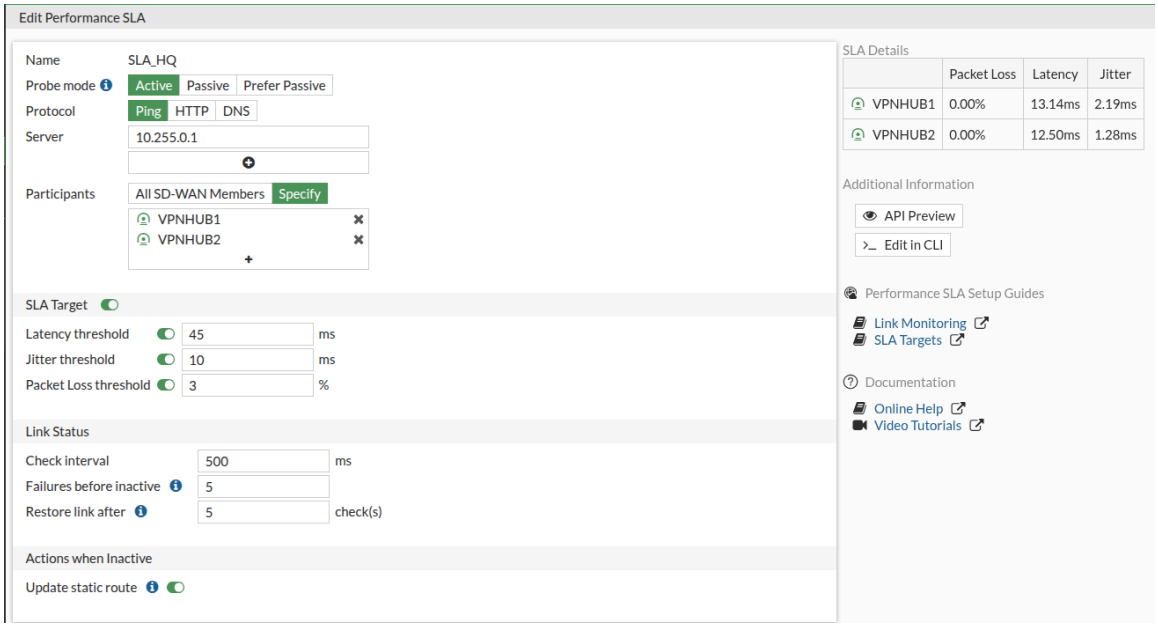
Esta seção abrange os procedimentos de teste e apresenta a análise da solução, comprovando que a SD-WAN é capaz de gerenciar a qualidade do serviço e reagir a degradações de link, validando a eficácia da arquitetura proposta.

4.6.1 Definição e Monitoramento do Service Level Agrement

O controle de tráfego foi estabelecido por meio do Link Health Monitoring, um recurso essencial do SD-WAN, configurado para monitorar a latência, jitter e perda de pacotes de cada link WAN (Link A e Link B). Regras de SLA (Service Level Agreement) foram definidas com limiares específicos (ex: Latência Máxima) para que o FortiGate tomasse decisões de traffic steering em tempo real.

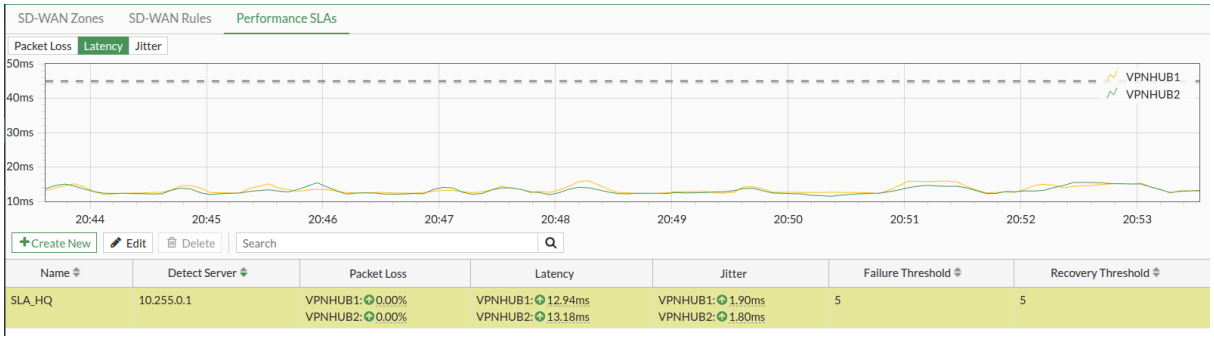
A Figura 4.6 exibe a configuração estática dos parâmetros de SLA definidos para a Matriz e Filiais. Em seguida, a Figura 4.7 demonstra o monitoramento em tempo real do Link Health, atestando o desempenho de cada Underlay antes da simulação de falha.

Figura 4.6 - Definição do SLA



Fonte: Elaborada pelo autor, 2025

Figura 4.7 - Monitoramento Dinâmico da Saúde do Link



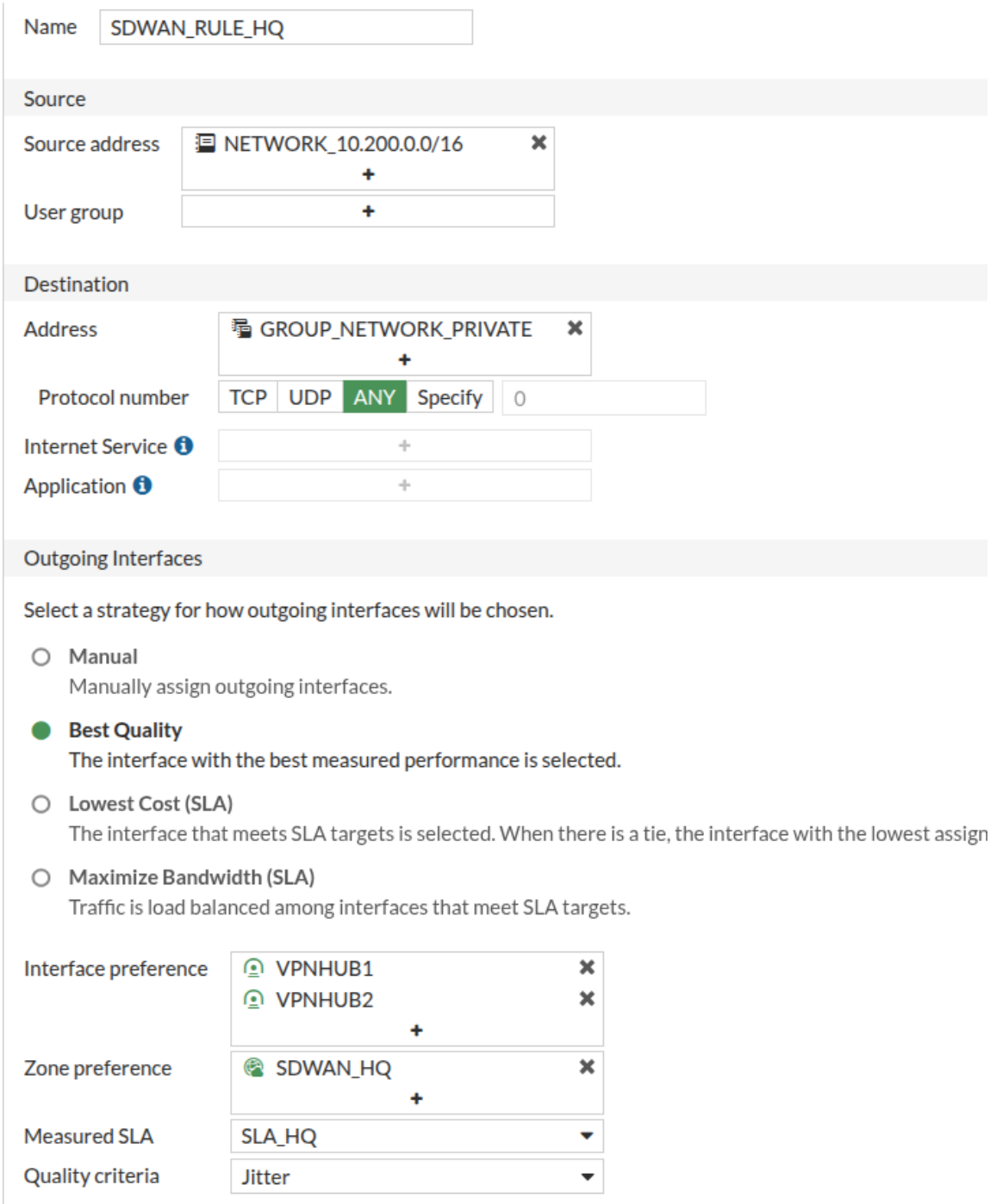
Fonte: Elaborada pelo autor, 2025

4.6.2 Regras SD-WAN (Service Rules)

As regras de serviço do SD-WAN foram criadas para definir a política de roteamento da rede Overlay. A regra principal estabeleceu que o tráfego crítico, destinado à Zona HQ (VPNs), deveria sempre priorizar o link que estivesse abaixo do SLA de latência (best quality).

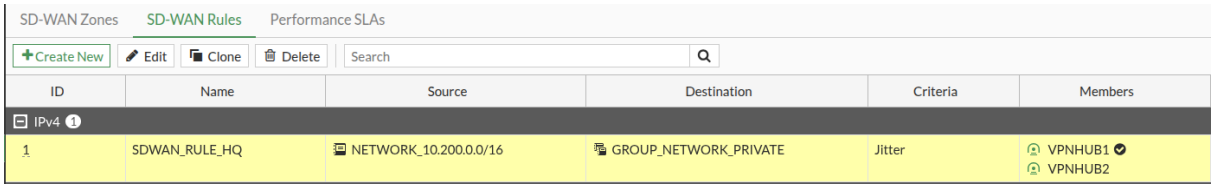
A Figura 4.8 exibe a configuração detalhada da regra de serviço, mostrando os critérios de seleção e a ordem de prioridade dos membros (túneis VPN). Em seguida, a Figura 4.9 demonstra o status inicial da regra e a seleção do túnel, mostrando que o VPNHUB1 já estava ativo e em uso para o tráfego da Zona HQ antes da degradação do link principal.

Figura 4.8 - Configuração Detalhada da Regra de Serviço do SD-WAN



Fonte: Elaborada pelo autor, 2025

Figura 4.9 - Status Inicial da Regra

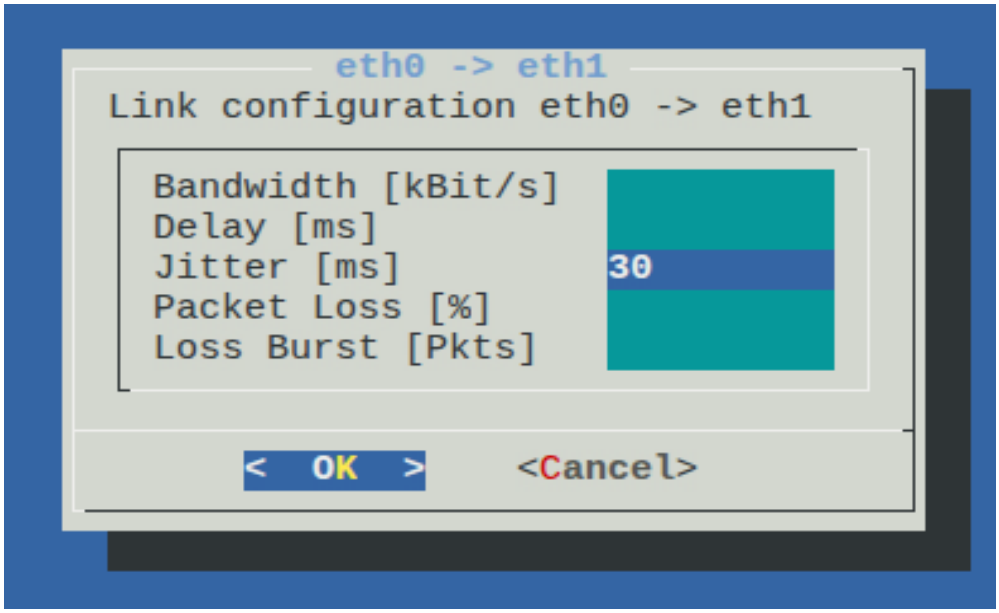


Fonte: Elaborada pelo autor, 2025

4.6.3 Cenário de Emulação de Falhas e Degradação de Link

Para demonstrar a eficácia das regras de SLA, o Linux NETem foi aplicado no Link A para simular um cenário de congestionamento. Esta ferramenta foi crucial para manipular as condições da rede Underlay (Ferrazani; Costa, 2021). Os seguintes parâmetros de degradação foram aplicados: Latência aumentada para 30ms e Jitter (Variação) para 10ms. A Figura 4.10 demonstra a aplicação desses comandos na interface de rede.

Figura 4.10 - Aplicação de Latência e Jitter via Linux NETem

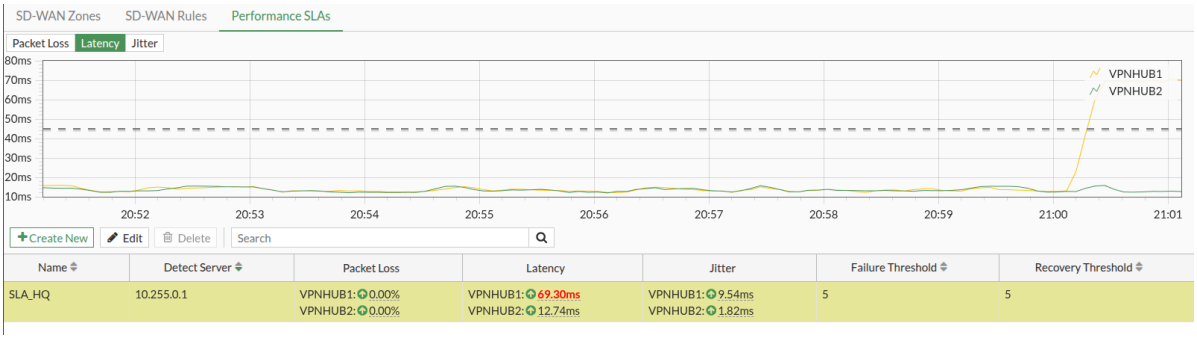


Fonte: Elaborada pelo autor, 2025

4.6.4 Comprovação do Failover e Análise Final

Com a degradação intencional do Link A via Linux NETEM, as regras de SD-WAN foram acionadas. O aumento da latência e do jitter elevou as métricas do Link A acima dos limiares de SLA configurados, resultando na sua imediata violação. A Figura 4.11 comprova que o status do Link A (Underlay) foi alterado para abaixo do SLA, acionando o processo de traffic steering.

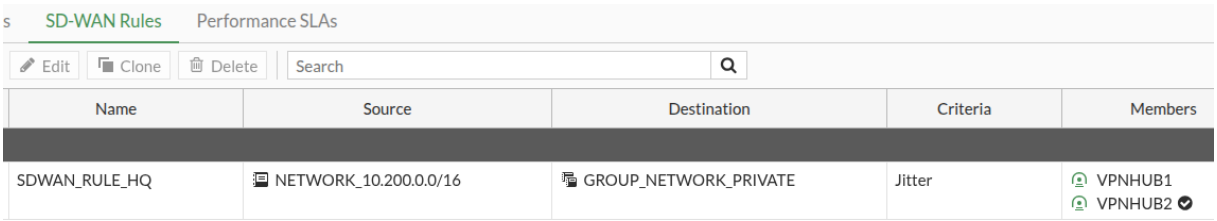
Figura 4.11 - Comprovação da Violação do SLA



Fonte: Elaborada pelo autor, 2025

Em resposta à violação do SLA, o FortiGate acionou a regra SD-WAN, que exige a priorização do caminho de melhor qualidade. Automaticamente, o tráfego crítico da Zona HQ foi desviado para o caminho secundário. A Figura 4.12 demonstra o sucesso deste processo, exibindo a VPNHUB2 (túnel IPsec sobre o Link B) como o túnel ativo e selecionado pela regra de serviço.

Figura 4.12 - Ativação da VPNHUB2 (Link B)



Fonte: Elaborada pelo autor, 2025

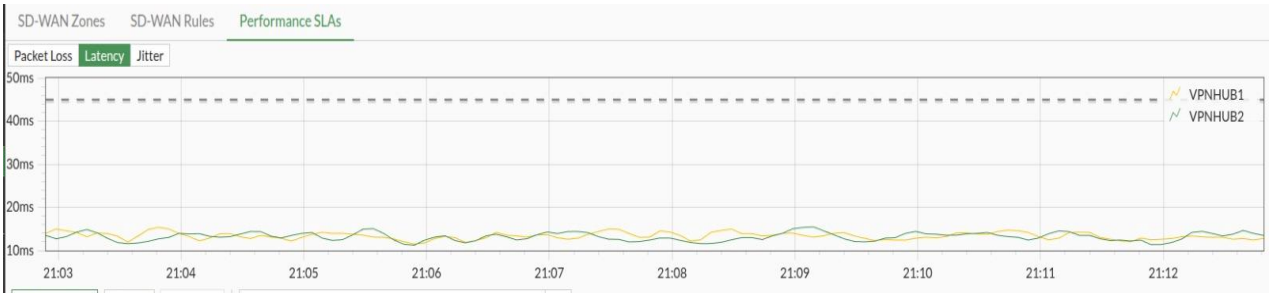
4.7 ANÁLISE DE DADOS DE TELEMETRIA E QUANTIFICAÇÃO DE GANHOS

Atendendo à necessidade de validação quantitativa dos resultados, foram extraídos os dados de telemetria nativa gerados pelo subsistema de monitoramento do FortiGate (SD-WAN Analytics). Esta análise permite comparar o comportamento das métricas de qualidade em condições normais versus condições de estresse, comprovando a precisão do gatilho que acionou a troca de rotas demonstrada anteriormente.

Inicialmente, é fundamental estabelecer a linha de base operacional da rede. A Figura 4.13 apresenta o monitoramento do Link A em operação padrão, antes da

aplicação dos testes. O gráfico evidencia a estabilidade da conexão, com a métrica de latência operando confortavelmente abaixo do limite estabelecido no SLA, qualificando o link como apto para o tráfego corporativo.

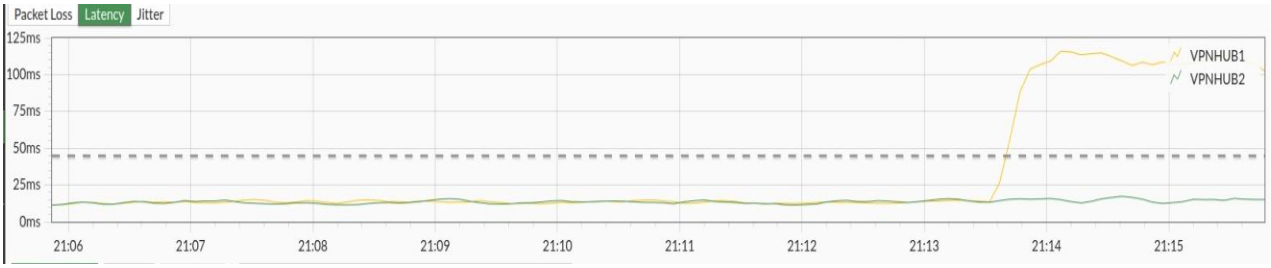
Figura 4.13 - Telemetria de SLA: Registro do aumento de latência no Link A



Fonte: Elaborada pelo autor, 2025

Em contrapartida, o momento exato da injeção de falhas via ferramenta NETEM é registrado na Figura 4.14. A análise comparativa entre os cenários comprova que a latência sofreu uma elevação abrupta, ultrapassando o limiar de 30ms. O sistema identificou a violação instantaneamente, alterando o status do membro para inoperante.

Figura 4.14 - Telemetria de SLA: Registro de pico de latência e violação do limiar



Fonte: Elaborada pelo autor, 2025

A comparação entre as duas figuras valida o mecanismo de decisão da arquitetura. A detecção precisa da anomalia, evidenciada na Figura 4.14, foi o fator determinante que obrigou o FortiGate a desviar o tráfego para a VPNHUB2 (Link B), conforme verificado na Figura 4.12. Desta forma, comprova-se que a solução oferece um ganho significativo de visibilidade e automação, eliminando a subjetividade no diagnóstico de falhas de rede.

5 CONSIDERAÇÕES FINAIS

O presente trabalho validou a SD-WAN como uma tecnologia essencial à volatilidade do mercado, substituindo a infraestrutura WAN estática e dispendiosa por uma rede inteligente e automatizada. A urgência por agilidade e resiliência nas operações dos empreendimentos modernos confere a este tema uma relevância crucial, provando que a solução é uma questão de sobrevivência e eficiência corporativa.

5.1 CONCLUSÃO E COMPROVAÇÃO DE ARQUITETURA

A pesquisa atingiu seu objetivo ao demonstrar que a integração do firewall FortiGate, utilizando os protocolos IPsec e OSPF, resulta em uma arquitetura robusta e ágil. Os testes de estresse, simulados com o Linux NETEM, confirmaram que a degradação do Link A (VPNHUB1) elevou as métricas de latência e jitter acima do limiar de SLA configurado. Em resposta, o FortiGate acionou o failover, desviando automaticamente o tráfego crítico para o Link B (VPNHUB2), mantendo a qualidade do serviço. O OSPF, operando sobre os túneis IPsec, garantiu a atualização e o reaprendizado rápido das rotas internas no novo caminho, com um tempo de failover de 1000 milissegundos, validando a resiliência comportamental da arquitetura. Conclui-se, portanto, que a SD-WAN implementada com roteamento dinâmico constitui uma alternativa de alta performance e baixo custo operacional para a interconexão de unidades de negócios.

5.2 CONTRIBUIÇÕES E SUGESTÕES PARA O FUTURO

Este projeto oferece uma metodologia de laboratório replicável utilizando ferramentas acessíveis e gratuitas (GNS3 e Linux NETEM) para análise empírica de SD-WAN, sendo esta a principal contribuição prática do trabalho. Para dar continuidade à pesquisa, sugere-se a expansão do projeto focando na integração de ferramentas de gerenciamento e análise de segurança. Isso inclui a implementação da solução FortiManager para a centralização da administração, configuração e escalabilidade da arquitetura Hub-and-Spoke, e a utilização do FortiAnalyzer para a coleta, correlação e análise aprofundada dos logs de segurança e desempenho da

SD-WAN, com o objetivo de melhorar a observabilidade e diminuir o tempo de resposta a incidentes.

REFERÊNCIAS

CISCO. **Cisco SD-WAN: A better way to WAN**. Cisco Systems, 2020. Disponível em: https://www.cisco.com. Acesso em: 24 jun. 2025.

CISCO. **Next-Generation Firewall (NGFW)**. 2020.

CISCO. **SD-WAN: A Beginner's Guide**. Disponível em: https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/sd-wan/nb-06-sd-wan-ebook-cte-en.html. Acesso em: maio 2025.

COMBS, Gerald et al. **Wireshark User's Guide**. The Wireshark Team, 2023. Disponível em: https://www.wireshark.org/docs/wsug_html_chunked/. Acesso em: 24 jun. 2025.

FERRAZANI, G.; COSTA, M. Software-Defined Wide Area Network (SD-WAN): Uma revisão sobre arquitetura e desafios. **Revista Brasileira de Redes de Computadores e Sistemas Distribuídos**, v. 9, n. 1, p. 45-60, 2021.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. 5. ed. São Paulo: McGraw-Hill, 2017.

FORTINET. **FortiGate Secure SD-WAN Solution Guide**. Fortinet, 2023. Disponível em: https://www.fortinet.com. Acesso em: 24 jun. 2025.

FORTINET. **Fortinet Secure SD-WAN**. 2021. Disponível em: https://www.fortinet.com/br/products/sd-wan. Acesso em: maio 2025.

FORTINET. **FortiOS Handbook**: SD-WAN. 2023. Disponível em: https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/19246/sd-wan. Acesso em: 17 jun. 2025.

GARTNER. **Magic Quadrant for WAN Edge Infrastructure**. Gartner, 2022.

GILL, H. et al. Understanding WAN Transformation with SD-WAN. **IEEE Communications Magazine**, v. 57, n. 3, p. 96–102, 2019.

HEMMINGER, Stephen. Network Emulation with NetEm. In: **Linux Conf Au**. 2005. Disponível em: https://www.ibm.com/docs/en/linux-on-systems?topic=tools-netem. Acesso em: 17 jun. 2025.

IDG. **SD-WAN Market Trends and Benefits Report**. IDG Communications, 2021.

RFC 4301: Security Architecture for the Internet Protocol. Internet Engineering Task Force, 2005.

MEHMOOD, Y. et al. A Comprehensive Survey on Software-Defined Networking. **IEEE Access**, v. 8, p. 195651–195673, 2020.

SANDERS, Chris. **Practical Packet Analysis**: Using Wireshark to Solve Real-World Network Problems. 3. ed. San Francisco: No Starch Press, 2017.

STALLINGS, William. **Criptografia e Segurança de Redes**: Princípios e Prática. 7. ed. São Paulo: Pearson, 2017.

STALLINGS, W. **Cryptography and Network Security**: Principles and Practice. 8. ed. Pearson, 2020.

TAHENNI, A.; MERAZKA, F. **SD-WAN over MPLS**: A Comprehensive Performance Analysis and Security with Insights into the Future of SD-WAN. 2023. Disponível em: https://arxiv.org/abs/2401.01344. Acesso em: 12 maio 2025.

TANENBAUM, Andrew S.; WETHERALL, David J. **Redes de Computadores**. 5. ed. São Paulo: Pearson, 2011.