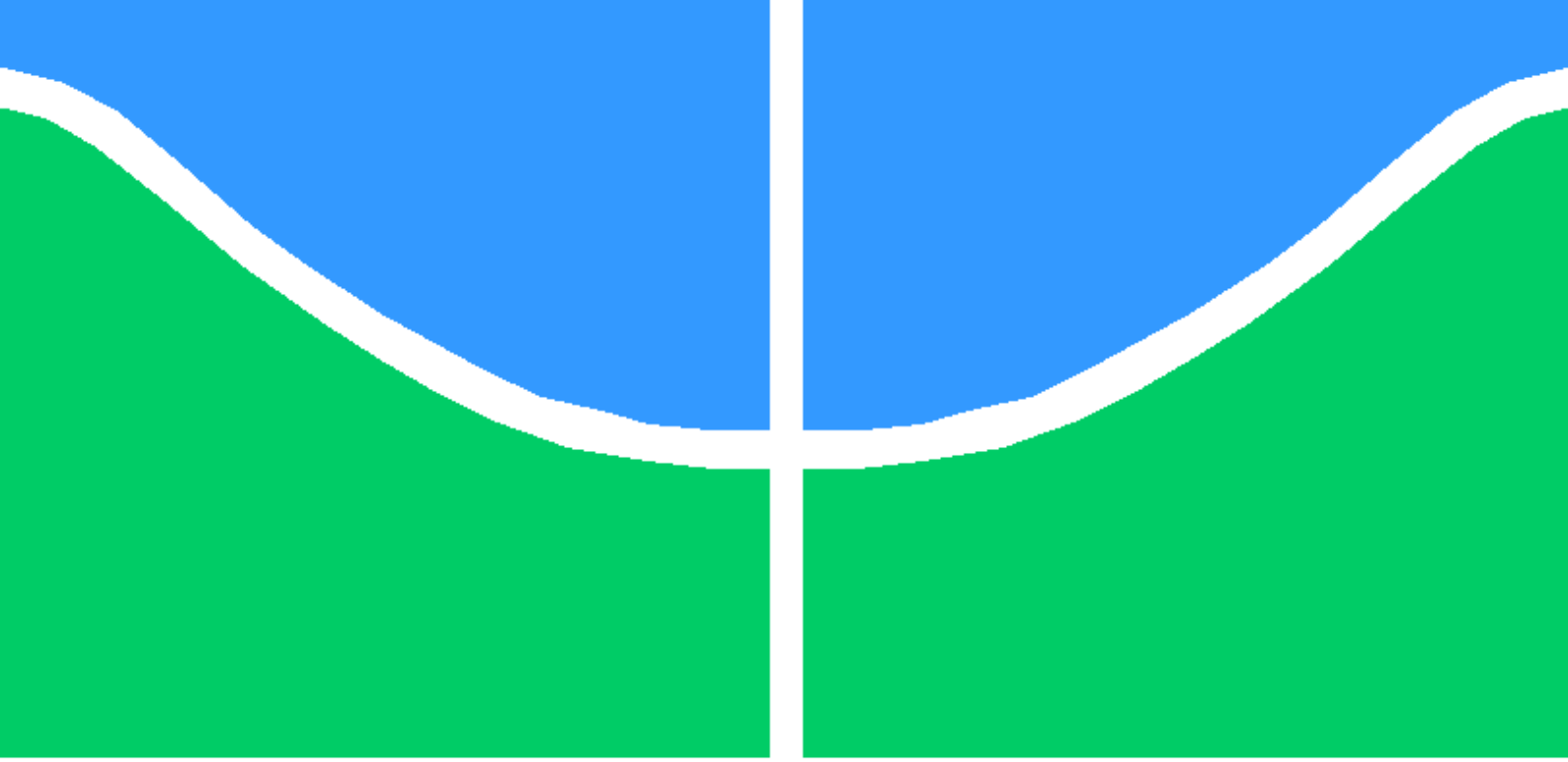


TRABALHO DE GRADUAÇÃO

IMPLEMENTAÇÃO E ANÁLISE DE AUTOMAÇÃO DE REDES EM INFRAESTRUTURAS DE PRÓXIMA GERAÇÃO COM EMPREGO DE SD-WAN

Adrielle da Silva Custódio

Letícia Fernandes Rios

Brasília, Dezembro de 2023

UNIVERSIDADE DE BRASÍLIA

FACULDADE DE TECNOLOGIA

UNIVERSIDADE DE BRASILIA
Faculdade de Tecnologia

TRABALHO DE GRADUAÇÃO

IMPLEMENTAÇÃO E ANÁLISE DE AUTOMAÇÃO DE REDES EM INFRAESTRUTURAS DE PRÓXIMA GERAÇÃO COM EMPREGO DE SD-WAN

Adrielle da Silva Custódio

Letícia Fernandes Rios

Relatório submetido ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Engenheiro de Redes de Comunicação

Banca Examinadora

Prof. Georges Amvame Nze, ENE/UnB _____
Orientador

Prof. Fábio Lúcio Lopes de Mendonça, ENE/UnB _____
Examinador Interno

Hélder Machado, Eng. (EnE/UnB) _____
Examinador Externo

RESUMO

Em uma era digital em constante evolução, a necessidade de uma conexão estável, segura e de qualidade é mais crucial do que nunca. Isso é especialmente verdadeiro ao considerar uma infraestrutura de redes de próxima geração, onde as demandas por largura de banda, velocidade e confiabilidade são ainda mais intensas.

Sendo assim, a busca por tecnologias que ofereçam maior performance, estabilidade e segurança vem se tornando cada vez mais uma preocupação do mercado de TI e reflete diretamente nos desafios emergentes da era digital. O aumento de dispositivos e a utilização extensiva da nuvem destacam a importância de investir em tecnologias e práticas que garantam a integridade, confidencialidade, gerenciamento simplificado e disponibilidade das redes, ao mesmo tempo em que proporcionam uma experiência de usuário otimizada e adaptável às crescentes demandas do cenário tecnológico contemporâneo.

Em vista disso, este projeto propõe realizar o estudo, identificação, implementação e análise de uma arquitetura de redes de campus hipotética da Universidade de Brasília englobando os seus quatro campus localizados em espaços geográficos diferentes, com o emprego da tecnologia SD-WAN para interconexão dos pólos universitários utilizando regras de qualidade de serviço e com a combinação de um serviço de transporte MPLS em seu *backbone* provido por uma operadora para fornecimento de Internet.

Como resultado, a partir da leitura desse projeto de graduação será possível obter conhecimentos referentes às soluções e tecnologias propostas para uma infraestrutura de próxima geração, identificando as melhores práticas de uma rede de campus no que envolve conectividade, redundância e segurança. Além disso, será possível verificar que a implementação deste projeto se dará utilizando vários fornecedores distintos, sendo assim, espera-se que mesmo em um cenário que possui tecnologias heterogêneas, será possível implementar a solução proposta utilizando-se de várias fabricantes do mercado.

Palavras-chaves: SD-WAN, MPLS, segurança, redundância, conectividade

ABSTRACT

In an ever-evolving digital age, the need for a stable, secure and quality connection is more crucial than ever. This is especially true when considering a next-generation network infrastructure, where demands for bandwidth, speed and reliability are even more intense.

Therefore, the search for technologies that offer greater performance, stability and security is increasingly becoming a concern in the IT market and directly reflects the emerging challenges of the digital era. The increase in devices and the extensive use of the cloud highlights the importance of investing in technologies and practices that guarantee the integrity, confidentiality, simplified management and availability of networks, while providing an optimized user experience that is adaptable to the growing demands of the contemporary technological scenario.

In view of this, this project proposes to carry out the study, identification, implementation and analysis of a hypothetical campus network architecture of the University of Brasília, encompassing its four campuses located in different geographic spaces, using SD-WAN technology for interconnection of university centers using quality of service rules and with the combination of an MPLS transport service in their backbone provided by an operator to provide Internet.

As a result, from reading this graduation project it will be possible to obtain knowledge regarding the solutions and technologies proposed for a next generation infrastructure, identifying the best practices of a campus network in terms of connectivity, redundancy and security. Furthermore, it will be possible to verify that the implementation of this project will take place using several different suppliers, therefore, it is expected that even in a scenario that has heterogeneous technologies, it will be possible to implement the proposed solution using several manufacturers on the market.

keywords: SD-WAN, MPLS, security, redundancy, connectivity

SUMÁRIO

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

Acrônimos

ADVPN	*Auto-Discovery VPN*
AS	*Autonomous System*
BDR	*Backup Designated Router*
BGP	*Border Gateway Protocol*
CE	*Customer edge*
CLI	*Command-Line Interface*
CPD	Centro de Processamento de Dados
DNS	*Domain Name System*
DR	*Designated Router*
eBGP	*Exterior Border Gateway Protocol*
FCE	Faculdade de Ceilândia
FGA	Faculdade do Gama
FUP	Faculdade de Planaltina
FTP	*File Transfer Protocol*
FEC	*Forward Equivalent Class*
GNS3	*Graphical Network Simulator*
GUI	*Graphical User Interface*
HSRP	*Hot Standby Router Protocol*
HTTP	*Hypertext Transfer Protocol*
iBGP	*Interior Border Gateway Protocol*
IaaS	*Infrastructure-as-a-Service*
ICMP	*Internet Control Message Protocol*
IDC	*International Data Corporation*
IEEE	Instituto de Engenheiros Eletricistas e Eletrônicos
IoT	*Internet of Things*
IP	*Internet Protocol*
IPsec	*Internet Protocol Security*
LAN	*Local area network*
LDP	*Label Distribution Protocol*
LER	*Label Edge Router*
LFIB	*Label Forwarding Information Bases*

Acrônimos

LSAs	*Link-State Advertisements*
LSP	*Label Switching Path*
LSR	*Label Switching Router*
L3VPN	*Layer 3 Virtual Private Network*
MAC	*Media Access Control*
MP-BGP	*Multiprotocol BGP*
MPLS	*Multi Protocol Label Switching*
MSS	*Maximum Segment Size*
NAT	*Network Address Translation*
NGFW	*Next-Generation Firewall*
OSI	*Open Systems Interconnection*
OSPF	*Open Shortest Path First*
P	*Provider Router*
PDUS	*Protocol Data Units*
PE	*Provider edge*
QEMUs	*Quick Emulators*
QoS	*Quality of Services*
RTT	*Round Trip Time*
SaaS	*Software-as-a-Service*
SCP	*Secure Copy Protocol*
SD-WAN	*Software-Defined Wide Area Network*
SLA	*Service-level Agreement*
SPF	*Shortest Path First*
SSH	*Secure Shell*
STP	*Spanning Tree Protocol*
TCP	*Transmission Control Protocol*
TE	*Traffic Engineering*
TI	Tecnologia da Informação
TLV	*Type-Length-Value*
TTL	*Time to Live*
UDP	*User Datagram Protocol*
UNB	Universidade de Brasília
VIP	*Virtual IP*
VLAN	*Virtual Local Area Network*
VM	*Virtual Machine*
VPN	*Virtual Private Network*
VPNv4	*Virtual Private Network version 4*
VOIP	*Voice Over Internet Protocol*
VRF	*Virtual Routing and Forwarding*
WAN	*Wide Area Network*

Capítulo 1

Introdução

Nos últimos anos, as organizações corporativas se expandem para um modelo de negócios digital, devido, por exemplo, ao aumento do trabalho remoto, crescimento constante no tráfego de dados na rede, adoção de várias nuvens, proliferação da Internet das Coisas (IoT) e busca por otimização e desempenho. Com isso, existe um impacto significativo nas topologias de rede, englobando as áreas de infraestrutura, segurança e utilização da nuvem, o que leva a um crescimento exponencial no número de dispositivos, usuários finais, banda larga, tráfego criptografado e aplicativos na nuvem em redes WANs (TOSTES, 2020).

Dessa maneira, a busca por tecnologias que prometem maior performance e redução de custos vem se tornando cada vez mais uma preocupação do mercado de TI. Atualmente, ainda existem muitas empresas que utilizam a WAN tradicional a partir de circuitos MPLS, para realizar a conectividade entre seus usuários finais presentes nas filiais/campus e seus servidores em *data centers* (NSB, s.d.). Entretanto, esse tipo de infraestrutura reduz a eficiência e performance da rede, pois a WAN não foi projetada para aguentar um número considerável de tráfego, principalmente em um mundo onde as aplicações SaaS (*Software* como Serviço) e IaaS (Infraestrutura como Serviço) em nuvem se tornaram mais comuns.

Sendo assim, é de grande importância a garantia de eficiência na conectividade dos dispositivos de usuários e IoT nas filiais da corporação, além da necessidade de segurança confiável, como também um modelo que gerencie e controle de forma crescente o alto volume de dados. E uma solução ideal para a infraestrutura de TI atual é a implementação do SD-WAN (*Software-Defined Wide Area Network*), no qual aborda a possibilidade de comunicação entre diferentes pontos na topologia WAN utilizando-se do *software* para determinar a melhor forma de disponibilizar os recursos e criar *links* de comunicação seguros entre os *endpoints*, servidores e *data centers* da organização. E assim, obtém-se a garantia de transição de WANs tradicionais e legadas, que possuem uma infraestrutura dedicada com altos custos, SLA's inflexíveis, dificuldade de disponibilidade geográfica, implantação complexa, entre outros fatores, para um infraestrutura flexível e adaptada aos recursos e serviços integrados na nuvem (NSB, s.d.).

Dessa maneira, verificou-se a partir das previsões da *International Data Corporation* (IDC) para o futuro da conectividade, que até 2023, 40% das empresas se beneficiarão de eficiência

operacional otimizada, segurança aprimorada e custos de rede reduzidos, aproveitando-se do SD-WAN, segurança para redes e segurança gerenciadas em nuvem (INFORCHANNEL, 2022). Além disso, segundo pesquisa realizada pela *Global Market Insights*, o mercado mundial de SD-WAN ultrapassou US$1 bilhão em 2019 e deve obter um acréscimo de 60% entre os anos de 2020 e 2026 (NSB, s.d.).

É por isso que as soluções de SD-WAN continuam a ganhar força e serão implantadas cada vez mais com a finalidade de facilitar a entrega de serviços gerenciados de rede e segurança (TOSTES, 2020). Dessa maneira, esta nova forma de implementação e gerenciamento traz solução para três grandes preocupações do mercado de TI: gerenciamento simplificado e eficiente com garantia de melhor performance na utilização da largura de banda, redução de custos e segurança aprimorada.

Com isso, ao adotar a tecnologia SD-WAN observamos diversas vantagens para o gerenciamento de TI e para a empresa como um todo, pois ela oferece alta disponibilidade, atendimento automático às políticas de aplicativos, tráfego de rede com roteamento dinâmico, trazendo maior inteligência, melhores custos operacionais, incluindo conexões VPNs seguras, tráfego seguro para a Internet e nuvem, fluxos de trabalho otimizados, painel de gerenciamento centralizado além de diversas melhorias nas aplicações e desempenho de WAN (NSB, s.d.).

1.1 Problemática

Com o alto desenvolvimento tecnológico e adoção da nuvem nas organizações de forma integral ou híbrida, observa-se que a busca por eficiência, desempenho, baixa latência, velocidade, segurança e menores custos de implantação e manutenção se tornam constantes e aceleradas. Porém, muitas empresas foram projetadas considerando um modelo tecnológico de outra época, no qual sua utilização não está sendo ideal atualmente, pois o *backhaul* de todo o tráfego, incluindo o destinado à nuvem, entre as filiais e a matriz, introduz latências e prejudica diretamente no desempenho das aplicações, e assim as organizações encontram certos desafios para absorver o crescente tráfego da WAN, necessitando de ajustes em sua infraestrutura.

Com este cenário, é essencial entender a importância para a implementação de um modelo ideal com a utilização da tecnologia SD-WAN a fim de realizar uma arquitetura que permita que as organizações aproveitem qualquer combinação de serviços de transporte, como o MPLS, por exemplo, para conectar os diferentes tipos de usuários a aplicativos com segurança, garantia de desempenho, resiliência consistente, onde há a automatização no direcionamento de tráfego de maneira orientada por aplicativos com base nos propósitos de cada empresa, trazendo assim melhorias nos quesitos de segurança e também uma simplificação da arquitetura WAN.

Para isso, além dos investimentos na projeção desta arquitetura, é necessário seguir algumas etapas para uma implementação de SD-WAN bem-sucedida (VENKO, 2022), como por exemplo: requisitos do ambiente e identificação de perfis de conectividade, fluxos de tráfego de aplicativos, qualidade de serviço (QoS), qualidade de experiência, largura de banda e segurança, como também a determinação do modelo SD-WAN.

1.2 Objetivos

1.2.1 Objetivos Gerais

Este trabalho traz como objetivo geral a promoção do conhecimento em redes ao expor os estudos e análises realizados na implementação de uma infraestrutura de rede SD-WAN, em um ambiente controlado a fim de conectar as filiais de uma organização, como também na implementação de uma arquitetura WAN possui a conexão MPLS como serviço de transporte legado presente no *backbone*, no qual disponibiliza acesso à Internet aos usuários.

1.2.2 Objetivos Específicos

- Realizar estudos relacionados à uma infraestrutura de redes SD-WAN;
- Identificar o melhor método e arquitetura de implementação de infraestrutura MPLS com SD-WAN;
- Realizar a implementação de uma infraestrutura de rede com tecnologia SD-WAN a partir da topologia física presente na Universidade de Brasília (UnB), no qual conta com quatro campus. Sendo eles: Campus Darcy Ribeiro, localizado no Plano Piloto, Faculdade de Ceilândia (FCE), Faculdade do Gama (FGA) e Faculdade de Planaltina (FUP);
- Realizar a implementação de uma arquitetura WAn com a tecnologia MPLS L3VPN;
- Encontrar as características de desempenho e qualidade de serviço para identificação do melhor *link* para encaminhamento dos dados;
- Identificar as melhores práticas de segurança para cada um dos perfis de usuário;

1.3 Estrutura Documental

Este documento visa o estudo, implementação e análise de resultados da tecnologia SD-WAN com a integração de uma topologia WAN legada que utiliza o serviço de transporte MPLS para o tráfego de dados. Assim, este documento se encontra segmentado em 6 capítulos, sendo que:

- O primeiro capítulo se refere à introdução, que descreve as motivações, primeiros estudos, alguns conceitos e objetivos do trabalho;
- O segundo capítulo se refere à fundamentação teórica, no qual é apresentado a base teórica necessária para toda a concepção deste estudo;
- O terceiro capítulo é dedicado à descrição das ferramentas utilizadas para a produção da infraestrutura a partir de um emulador virtualizado, detalhando cada serviço implementado juntamente com suas funcionalidades e configurações de operação e ajuste técnico;

- O quarto capítulo retrata a arquitetura do projeto, o desenho topológico físico e lógico e a implementação dos serviços e tecnologias propostas;
- O quinto capítulo apresenta os resultados e análises obtidas para cada uma das etapas propostas no quarto capítulo;
- O sexto capítulo apresenta uma análise conclusiva sobre os resultados comportamentais obtidos após a implementação da topologia. Além disso é apresentado sugestões de trabalhos futuros relacionados a este estudo, mas não sendo este o limitante para novas contribuições.

  Este projeto conta, além dos seis capítulos apresentados, 22 anexos referentes as configurações dos equipamentos utilizados na topologia proposta.

Capítulo 2

Fundamentação Teórica

Este capítulo apresenta os conceitos fundamentais utilizados para o desenvolvimento deste trabalho.

2.1 WAN

Primeiramente, a Rede de Longa Distância (WAN), do inglês *Wide Area Network*, abrange uma grande área geográfica no qual interliga um conjunto de redes locais (LANs) ou outras redes privadas que se comunicam entre si, conforme ilustrado na Figura 2.1, sendo considerada então, uma "rede de redes" (KOVACS, 2023). Dessa forma, as WANs permitem que as empresas, faculdades, escolas e até mesmo órgãos públicos conectem filiais remotas a *data centers* e forneçam os aplicativos e serviços necessários para executar suas funções de negócios.

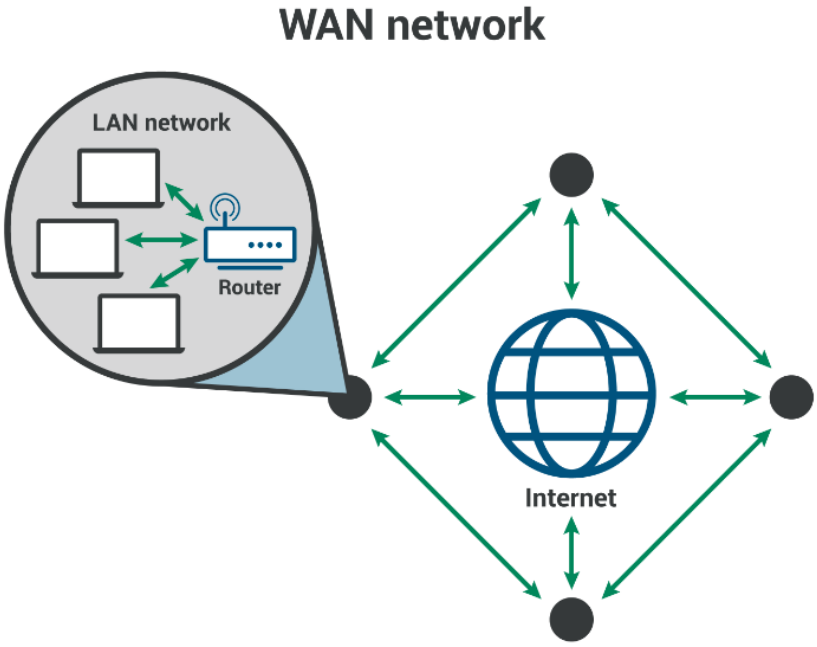


Figura 2.1: Ilustração de uma WAN. Fonte: (CLOUDFLARE, W., s.d.)

As LANs, diferentemente das WANs, são redes menores que utilizam uma tecnologia de conexão única, sendo assim, possuem capacidades limitadas, mas com alta velocidade e baixa latência, além disso, possuem maior facilidade de implantação e com menor custo de configuração e gerenciamento (AWS, W., s.d.). Dessa forma, as WANs detém de alta capacidade, mas com restrições de largura de banda e latência, o que causa problemas de desempenho, além disso, apresenta dificuldades em sua implantação e gerenciamento por se tratar de uma rede ampla com diversas conexões.

Ainda, podem ser utilizados diferentes tipos de tecnologias para estabelecer a conexão entre as LANs (AWS, W., s.d.), como:

- **Linhas Alugadas/Dedicadas**: conexão de rede direta de uma LAN à outra sendo física ou virtual, visto que esta conectividade WAN é alugada de um provedor de rede juntamente com serviços de acesso à Internet;
- **Tunelamento**: método de transportar os dados entre as LANs a partir do encapsulamento de pacotes de maneira criptografada garantindo maior segurança. Esta conexão é frequentemente utilizada nas redes privadas virtuais (VPNs);
- ***Multiprotocol Label Switching* - MPLS**: tecnologia de tráfego de dados baseado em rótulos/etiquetas pré-determinados para cada pacote na comunicação, no qual proporciona encaminhamento e comutação eficiente de forma mais rápida;
- **WANs definidas por *software* - SD-WAN**: evolução da tecnologia MPLS, no qual abstrai as funções MPLS em uma camada de *software*, oferecendo gerenciamento flexível;

Este trabalho terá como foco o estabelecimento de comunicação entre as LANs a partir de um *backbone* WAN legado que utiliza o serviço de transporte MPLS para fornecimento de conectividade com a Internet, juntamente com a tecnologia SD-WAN na borda da rede, para obter maior controle e gerenciamento dos caminhos alternativos entre os diferentes sites, a partir de relatórios avançados baseados em qualidade de serviço, além de convergência facilitada e automatizada, alta flexibilidade, combinação de conexões, criptografia e grande segurança no tráfego *overlay*.

Com isso, o modelo SD-WAN não exclui o uso do MPLS. Na realidade, estas duas tecnologias são complementares, sendo que uma solução híbrida pode fornecer à empresa uma solução ideal. Enquanto o MPLS é utilizado na Internet Pública, ou seja, na rede da provedora, para fornecer um controle mais granular para onde os pacotes irão fluir obtendo maior eficiência na transmissão dos dados, o SD-WAN utilizado na borda da rede do cliente, permitirá automatização, controle, gerenciamento e alta disponibilidade no direcionamento de tráfego com base nos propósitos da empresa.

2.2 SD-WAN

Antigamente utilizavam-se de um modelo convencional de tráfego de *backhaul* por meio de uma rede corporativa central a fim de conectar as filiais a um *data center*. Entretanto, este tipo de

comunicação não atende os usuários de maneira eficiente devido ao desperdício de largura de banda e alta latência, obtendo consequentemente baixo desempenho e baixo controle no gerenciamento. Dessa forma, as WANs tradicionais não foram desempenhadas para atender um alto controle de dados a partir do aumento considerável no tráfego em uma grande área geográfica.

Atualmente, há a necessidade da utilização de aplicações SaaS - *Software* como serviço, do inglês *Software-as-a-Service* e IaaS - Infraestrutura como serviço, do inglês *Infrastructure-as-a-Service* em várias nuvens, como também encontrar uma melhor maneira de realizar o envio de dados diretamente pela Internet mantendo as diretrizes de segurança.

Com isso, a Rede de Longa Distância Definida por *Software* (SD-WAN), do inglês *Software-Defined Wide Area Network*, é uma abordagem de rede WAN que conecta ambientes distantes de forma não tradicional, a partir da automatização de tráfego, no qual define o melhor canal de comunicação com base em fatores estabelecidos previamente pela empresa como, custo de transmissão, nível de segurança e agilidade no encaminhamento de pacotes (MOBILIT, 2022) a fim de conectar usuários a aplicativos com maior agilidade, otimização e segurança. A Figura 2.2 mostra um comparativo da arquitetura existente em redes WAN tradicionais e redes WAN que utilizam SD-WAN.

Além disso, a tecnologia SD-WAN oferece facilidade na implantação, simplicidade no gerenciamento ao desacoplar o *hardware* de rede de seu mecanismo de controle e monitoramento centralizado para direcionar o tráfego de forma segura e inteligente. Permite, também, que as empresas implementem WANs de alto desempenho substituindo parcialmente ou totalmente tecnologias WANs tradicionais, garantindo, portanto, melhor experiência ao usuário.

Por fim, o SD-WAN possibilita uma conectividade que prioriza a nuvem a fim de garantir roteamento e comutação mais ágil com maior largura de banda, baixa latência e baixo custo, obtendo desempenhos de alto nível, maior confiabilidade, resiliência e segurança.

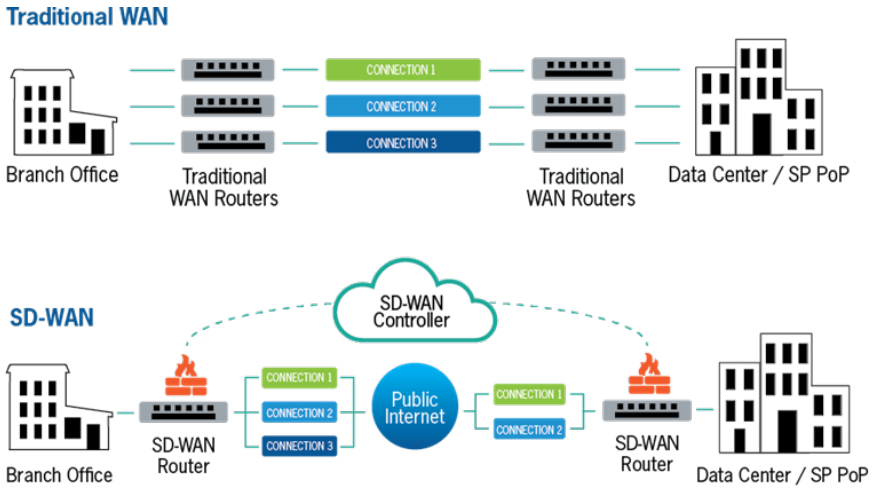


Figura 2.2: Comparação ilustrativa de uma rede tradicional WAN e rede SD-WAN. Fonte: (TECNOLOGIA, 2019)

2.3 MPLS

O MPLS, do inglês *Multiprotocol Label Switching*, foi desenvolvido com o objetivo de atender a demanda de usuários e variedade de aplicações. Esta tecnologia se refere a um protocolo de roteamento baseado em pacotes rotulados, onde cada rótulo indica um índice na tabela de roteamento do próximo roteador, ou seja, eles quem irão determinar como um pacote deve viajar entre uma origem e destino, criando portanto, uma rede privada (AUGUSTINE, 2022). Dessa forma, os pacotes de dados são encaminhados com base no conteúdo dos rótulos, evitando o processo de pesquisa do roteamento convencional (BIANCA, 2017).

O MPLS é considerado uma rede de trânsito, ou seja, transporta pacotes entre pontos de entrada e saída, dessa forma, é necessário, para sua implantação, grande planejamento e investimentos. Além disso, trata-se de um multiprotocolo, pois possui compatibilidade com qualquer outro protocolo da camada de rede. Entretanto, é importante observar que o MPLS não realiza roteamento, e sim comutação de circuitos virtuais. Com isso, este protocolo é considerado presente entre as camadas de rede e enlace (SANTA CATARINA, 2023).

Sendo assim, a tecnologia MPLS possibilita o encaminhamento e comutação eficiente de fluxos de tráfego de dados através da rede, visando diminuir o processamento nos equipamentos e interligar com maior eficiência redes de tecnologia distintas. O processo consiste em dividir a informação em classes de serviço, atribuindo os rótulos em cada pacote, e por fim, encaminhar os dados por meio das rotas estabelecidas pelas classes, realizando apenas a comutação (BIANCA, 2017).

Dessa forma, quando um pacote entra na rede, ele será recebido por um LER, do inglês *Label Edge Router*, responsável por atribuir o rótulo ao pacote. Esse rótulo é utilizado para representar um FEC, do inglês *Forward Equivalent Class*. Esse termo descreve um conjunto de pacotes com características semelhantes ou até mesmo idênticas que podem estar vinculados ao mesmo rótulo MPLS. Diferentemente do protocolo IP, onde a tabela de encaminhamento é analisada a cada roteador para verificar o próximo salto, o MPLS analisa o FEC apenas no momento de atribuir um rótulo ao pacote. A partir disso, os rótulos são anexados ao pacote, no qual seguem por um LSP, do inglês *Label Switching Path*, ou seja, os dados serão encaminhados por um determinado caminho definido pelos roteadores de borda da rede (LERs). No momento em que o pacote chega ao próximo nó, seu rótulo será analisado e substituído por outro, que então dará continuidade ao caminho. O processo de funcionamento do MPLS pode ser visualizado na Figura 2.3. Além disso, os nós em uma rede MPLS são conhecidos por LSRs, do inglês *Label Switching Router* (DUARTE, s.d.).

O protocolo LDP, do inglês *Label Distribution Protocol*, permite que os roteadores se comuniquem em uma rede MPLS a partir da distribuição de rótulo, ou seja, esse protocolo permite que os LSRs troquem informações e estabeleça caminhos LSPs e associem estes caminhos a FECs específicos (DUARTE, s.d.). No momento em que uma sessão entre dois roteadores é estabelecida, eles são denominados LDP *peers* e iniciam as trocas de informações de mapeamento LSP/FEC, indicando os endereços que um LSR alcança associados a rótulos, de maneira bidirecional.

É importante mencionar que o MPLS resultou em grandes avanços nas áreas de redes de

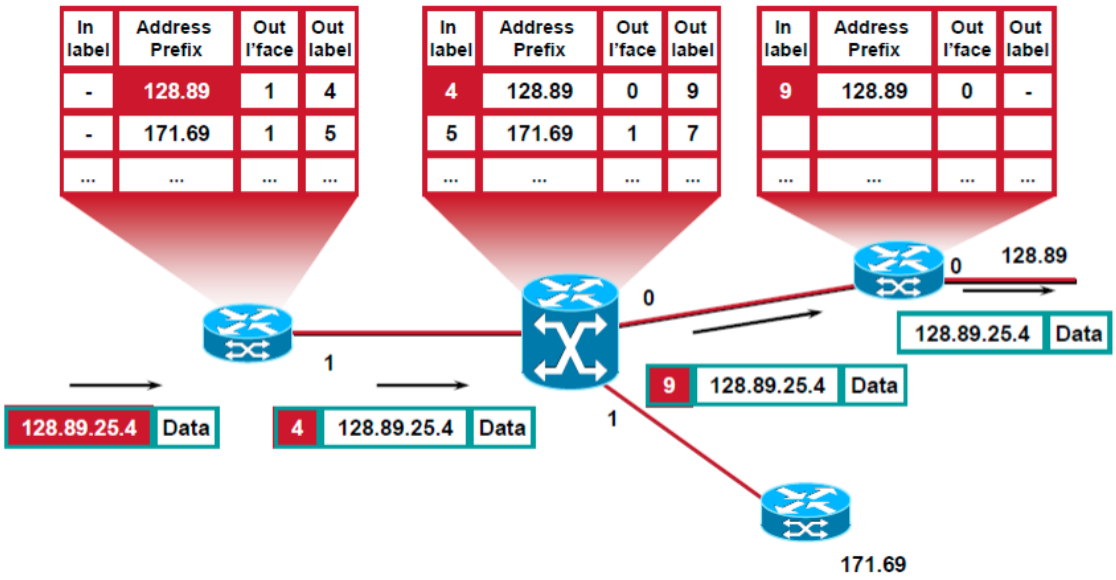


Figura 2.3: Funcionamento de uma rede MPLS. Fonte:(FONSECA, 2019)

computadores e telecomunicações, como: Sistemas de Qualidade de Serviços (QoS), do inglês *Quality of Services*; Tecnologias de plano de controle; Engenharia de tráfego (TE), do inglês *Traffic Engineering*, com ênfase na otimização da rede a partir da menor latência e alta taxa de transmissão; Redes Privadas Virtuais (VPNs), do inglês *Virtual Private Network*, como também, gerenciamento de conexões em redes ópticas.

2.4 MPLS L3VPN

O MPLS L3VPN é um tipo de tecnologia L3VPN e se refere a junção do MPLS, para encaminhar pacotes VPN em *backbones* de provedores de serviços com alta disponibilidade e resiliência, com o protocolo de roteamento dinâmico BGP (*Border Gateway Protocol*), utilizado para obter conectividade entre o roteador de borda da provedora/operadora, conhecido como PE (do inglês, *Provider edge*) e o roteador do cliente, conhecido como CE (do inglês, *Customer edge*), ou seja, o BGP é utilizado para anunciar as rotas VPN. Ainda há a separação do tráfego WAN do cliente dentro do *backbone* da operadora de forma transparente a partir da implementação de VRFs (do inglês, *Virtual Routing and Forwarding*) (ORTEGA, 2017).

Além disso, para obter uma rede MPLS funcional, é necessário que os roteadores do *backbone* sejam capazes de realizar roteamento entre eles, dessa forma, neste projeto será utilizado o roteamento OSPF para obter comunicação entre os roteadores da provedora. Além disso, o LDP é o responsável por gerar e distribuir os *labels* MPLS entre os roteadores (ORTEGA, 2017).

A Figura 2.4 abaixo exemplifica um diagrama de rede esquemático para a tecnologia MPLS L3VPN juntamente com os parâmetros necessários:

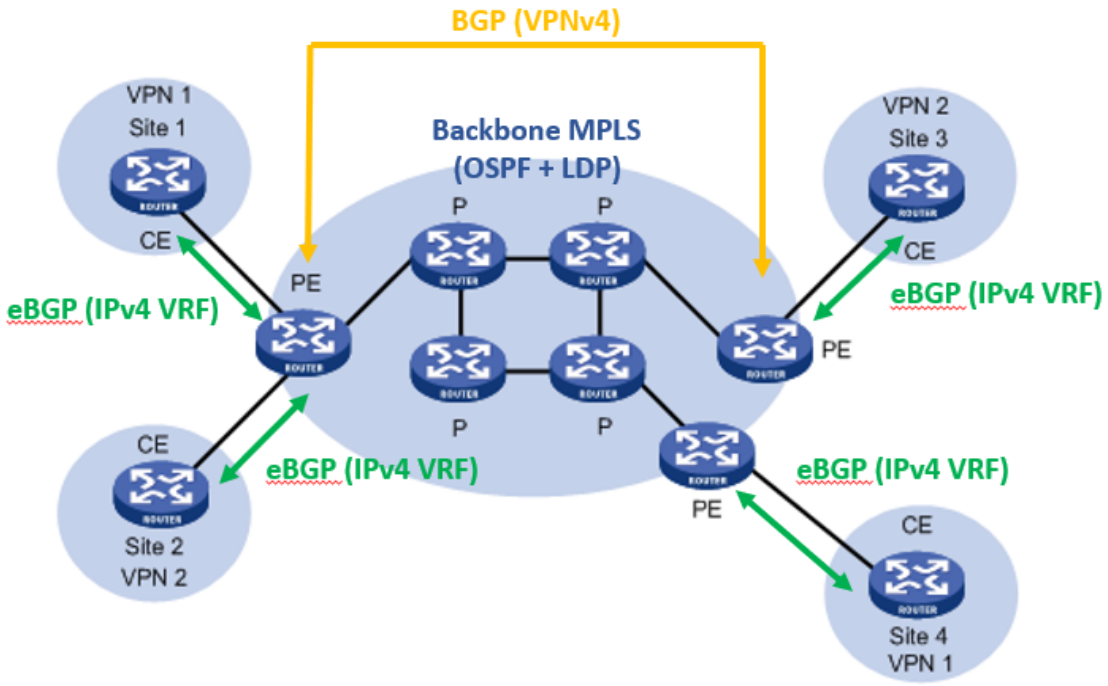


Figura 2.4: Diagrama de rede para o modelo MPLS L3VPN. Fonte: (TECHHUB, s.d.), Modificado

2.5 VRF

O *Virtual Routing and Forwarding* (VRF) é um tipo de tecnologia presente no Protocolo de Internet (IP), que atua de forma a possibilitar a existência de várias tabelas de rotas que atuam de maneira simultânea e independente em um mesmo roteador (HANNA, 2021). Dessa maneira, esse tipo de funcionalidade ocasiona um aumento na conectividade ao permitir que haja essa segmentação de rotas e tabelas de rotas, sem que seja necessário a presença de novos dispositivos. Além do aumento de conectividade, é também aumentada a segurança, visto que somente redes específicas e definidas terão acesso a outras redes, ou seja, o tráfego entre diferentes clientes não será mesclado.

A ideia de segmentação na rede é muito parecido com o que ocorre na utilização de VLANs, porém enquanto a VLAN acontece na camada 2 do modelo OSI, o VRF ocorre na camada 3, permitindo assim a segmentação no nível de rede. Em outras palavras, a VLAN faz com que um único *switch* atue como se fosse vários *switches*, já a VRF permite que um único roteador atue de forma que pareça que há vários roteadores (BHARDWAJ, 2022). A Figura 2.5 abaixo ilustra como se dá o funcionamento da VRF, onde diferentes IPs de origem têm seus tráfegos encaminhados para partições lógicas, também chamados de roteadores virtuais, diferentes que estão em um único roteador físico.

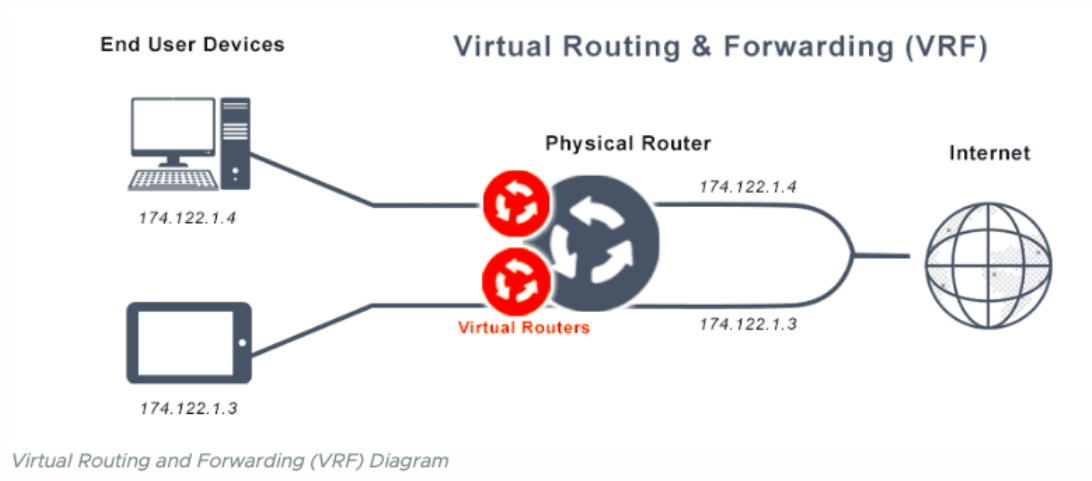


Figura 2.5: Funcionamento do VRF. Fonte: (LABS, 2022)

2.6 BGP

Este projeto utilizará o protocolo de roteamento dinâmico BGP (*Border Gateway Protocol*) para interligar os sistemas autônomos (AS, do inglês *Autonomous System*) presentes na topologia. Dessa forma, o protocolo BGP determina as melhores rotas de rede para transmissão de dados na Internet, sendo sua configuração fundamental, pois a Internet é feita de centenas de milhares de sistemas autônomos (AWS, s.d.). A Figura 2.6 ilustra como grandes redes de Internet são interconectadas.

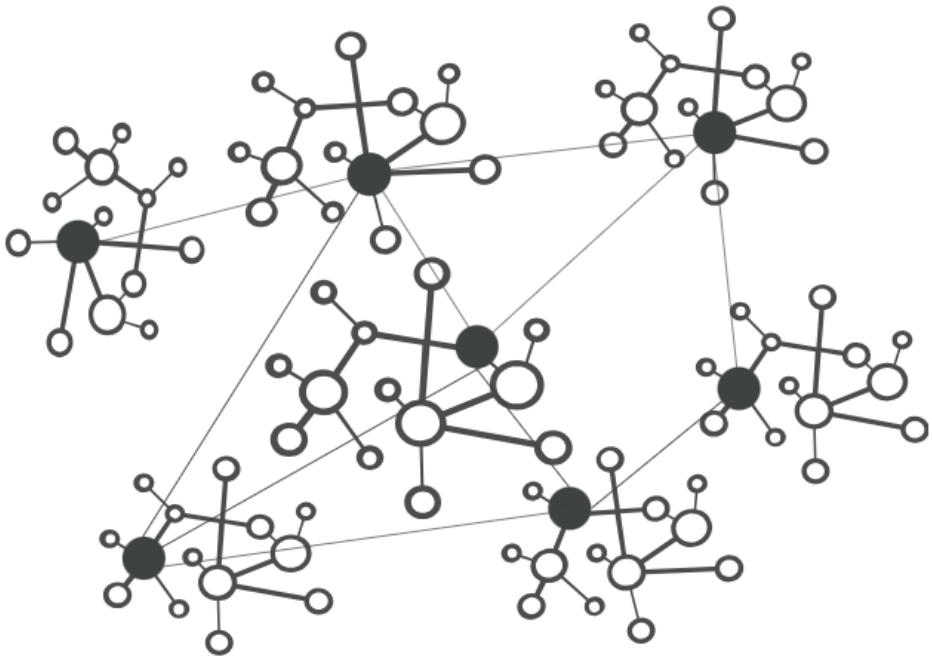


Figura 2.6: Grandes redes da Internet interconectadas. Fonte: (CLOUDFLARE, s.d.)

Com isso, os sistemas autônomos são as grandes redes que compõem a Internet, e assim os pacotes de dados cruzam diferentes ASs até chegarem ao seu destino correspondente. Cada AS possui sua identidade única e um conjunto de políticas de roteamento distintas, além disso, elas são administradas e operadas por uma única organização (ERICK, 2023).

A partir disso, a função do BGP é permitir que cada sistema autônomo compartilhe informações de roteamento atualizadas com outros sistemas autônomos, isso porque a estrutura da Internet está em constante mudança, permitindo, portanto, que o tráfego seja encaminhado de forma eficiente e confiável pela Internet.

Para estabelecer conexões ponto a ponto entre ASs diferentes (eBGP, *Exterior Border Gateway Protocol*) e manter a atualização das rotas é necessário configurar sessões BGP, também conhecidas como sessões de *peering*, em cada interface de um *link* ponto a ponto. Esses *peers*, ou seja, vizinhos BGP são estabelecidos para criar uma sessão TCP na porta 179. Dessa maneira, a conexão TCP é formada pela junção de dois roteadores de borda presentes na fronteira de cada AS, também conhecidos como PEs (*Provider edges*), permitindo que os pares eBGP troquem informações de roteamento.

Sendo assim, os *peers* BGP executam algumas funções principais, como: descoberta de rotas, a partir da troca de informações de acessibilidade da camada de rede e atributos de caminho, como latência, contagem de saltos e custo de transmissão; armazenamento de rotas, na forma de tabelas de roteamento; e seleção de caminho, a fim de obter direcionamento de tráfego otimizado a partir das informações armazenadas nas tabelas de rotas (AWS, s.d.).

2.7 OSPF

Este projeto utilizará o protocolo de roteamento dinâmico OSPF (*Open Shortest Path First*) para obter comunicação entre os roteadores da provedora presentes no *backbone*. Este protocolo utiliza o algoritmo de estado de enlace, também chamado de Dijkstra ou SPF (*Shortest Path First* - menor rota primeiro), no qual envia avisos de estado de conexão (LSAs - *Link-State Advertisements*) a todos os outros roteadores, a fim de acumular informações sobre o estado do *link*. Assim, no OSPF cada roteador constrói um mapa topológico completo de todo o sistema autônomo, contendo os dados sobre todos os *links* da rede, e utiliza o SPF para calcular a menor rota para cada nó. Além disso, o OSPF permite a divisão da rede em áreas, ou seja, a implementação de hierarquias na rede, no qual facilita no planejamento, agregação e sumarização de rotas (GONÇALVES, s.d.). Em relação às métricas, este protocolo utiliza custos dos enlaces individuais (de saída da interface), no qual cada enlace possui um "peso" que está relacionado inversamente com a largura de banda, ou seja, quanto maior a largura de banda, menor vai ser o peso daquele enlace. Ainda, o OSPF envia informações (anúncios) de mudança apenas quando estas ocorrem. Sendo assim, a partir destas características citadas, o protocolo de estado de enlace possui um maior processamento e rápida convergência.

Um dos princípios do OSPF mencionado acima é o conceito de áreas, no qual realiza uma divisão hierárquica com objetivo de diminuir a complexidade da rede e minimizar a comunicação

entre os roteadores, ou seja, as áreas limitam o espaço da distribuição da informação de rota. Necessariamente no OSPF, deve existir uma área central, chamada "*Backbone*" ou área 0 que vai servir como elo de ligação e comunicação entre as outras áreas.

No caso deste projeto, haverá somente uma área OSPF, que identificará a área do *backbone*, que é composta por dois dispositivos de borda da provedora (PEs) e dois dispositivos provedores (definidos pela sigla P). Detalhes acerca de como se dará a interconexão entre esses roteadores, bem como os demais ativos da rede poderão ser visualizados posteriormente no corpo deste projeto.

2.8 VLAN

Na camada 2 do modelo TCP/IP, conhecida como camada de enlace, é possível configurar redes virtuais, chamadas de VLANs (*Virtual Local Network*), no qual tem por objetivo dividir uma rede local (física) em várias redes virtuais, como visto na Figura 2.7, criando domínios de *broadcast* separados provendo um melhor desempenho, gerenciamento, segurança e escalabilidade.

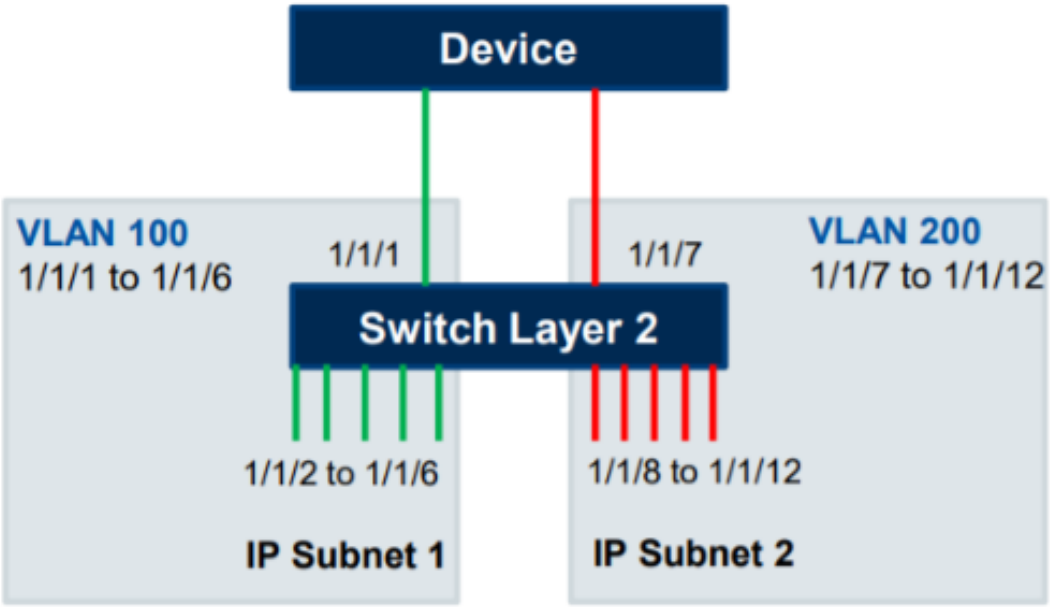


Figura 2.7: VLANs - Virtual Local Interfaces. Fonte própria.

As VLANs podem ser classificadas em dois tipos: VLANs com *tag* (dot1Q) ou sem *tag*, (MONTEIRO, s.d). As VLANs com *tag*, representados pelo protocolo IEEE 802.1Q, adicionam um campo de identificação (*tag*) nos quadros *Ethernet* a fim de encaminhar os pacotes em portas *trunk* para manter as VLANs separadas, como mostra a Figura 2.8. Ou seja, neste caso várias VLANs podem ser configuradas em uma única porta, no qual cada quadro enviado será marcado pela VLAN ID. Já as VLANs sem *tag*, representam aquela porta do *switch* associada a uma única VLAN e o *host* neste caso não tem conhecimento de sua associação pela mesma.

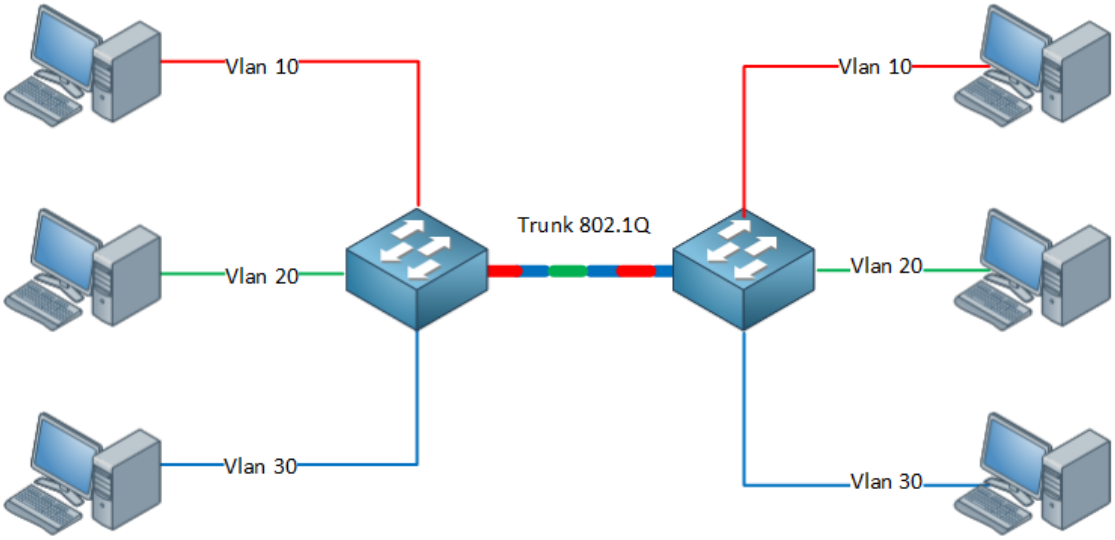


Figura 2.8: Modo *trunk* para permitir o trafégo de pacotes de diferentes VLANs

2.9 Protocolo HSRP

A redundância de rede é um item essencial para a implementação de uma infraestrutura, seja ela para LAN ou WAN, e se refere no processo de adição de dispositivos de rede, equipamentos ou linhas de comunicação extra para manter a conectividade caso o caminho principal fique inativo. Sendo assim, o *failover* é imprescindível para permitir que os sistemas continuem operacionais mesmo após falhas de componentes ou *links*.

Entretanto, mesmo com *links* ou equipamentos duplicados, a falha no dispositivo ou interface de comunicação principal causa interrupções na transmissão de pacotes, até que o dispositivo ou *link* secundário seja utilizado. Dessa forma, o protocolo proprietário da Cisco, HSRP, do inglês *Hot Standby Router Protocol*, foi desenvolvimento para fornecer redundância de *gateway*, ou seja, esse protocolo promove a alta disponibilidade em roteadores, de forma que, mesmo durante falhas, a rede sempre terá um equipamento em funcionamento atuando como *gateway* padrão (REDES, 2023).

O HSRP utiliza o endereço MAC e IP virtuais compartilhados entre os membros do grupo de roteadores que executam o protocolo. Este grupo deve conter um *Active Router* (Roteador Ativo), responsável pelo encaminhamento de pacotes, ou seja, o roteador ativo que irá receber os quadros destinados ao MAC/IP virtual do grupo, e um ou mais *Standby Routers*, responsável por assumir como ativo, em caso de falha (RIBEIRO, 2017). Dessa forma, o protocolo HSRP detecta quando o roteador ativo falha, e a partir desse momento, um roteador de *backup* assume o controle dos endereços do grupo. O dispositivo que realiza o controle é determinado por um valor de prioridade, sendo assim, para se tornar ativo, a prioridade de um roteador deve ser maior que a dos outros roteadores membros do grupo (REDES, 2023).

A partir disso, caso haja falhas, como por exemplo, queda de um *link* físico ou até mesmo perda de rota na tabela de roteamento, o protocolo detecta a falha a partir da troca de mensagens do tipo *Hello*, entre os equipamentos, destinados ao endereço IP *multicast* 224.0.0.2 sob o protocolo

de transporte UDP na porta 1985.

A Figura 2.9 exemplifica um caso de uso, no qual dois roteadores (R1 e R2) possuem acesso à Internet, com isso, para que a rede interna obtenha acesso à rede externa e ainda tenha redundância em caso de falhas, um roteador é declarado Ativo, sendo o outro *Standby*, e assim, os membros do grupo HSRP utilizam o *Virtual IP* (VIP), no qual receberá os pacotes destinados à rede externa. Caso o roteador ativo falhe, o outro dispositivo assumirá o tráfego de dados, garantindo, portanto, alta disponibilidade e resiliência.

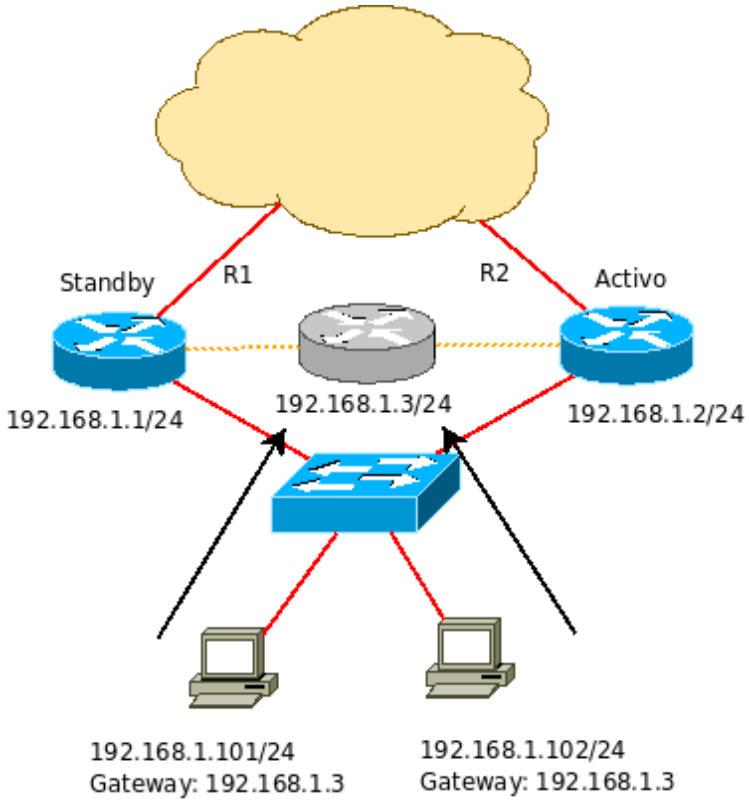


Figura 2.9: Caso de uso do protocolo HSRP. Fonte: (WEHER, 2009)

2.10 IP SLA *Tracking*

Como mencionado anteriormente, a redundância é um dos aspectos mais importantes ao se planejar uma infraestrutura de redes. Com isso, é necessário obter rotas de *backup* confiáveis.

Ao se configurar roteamento estático nos roteadores, é possível que haja uma situação em que uma rota estática está ativa, mas a rede de destino não é acessível por meio do próximo salto especificado por essa rota. A partir disso, para se obter uma redundância funcional, o modo mais confiável e simples é realizando a configuração de rotas estáticas de *backup* com IP SLA *tracking*.

O recurso de rastreamento de objetos do acordo de nível de serviço do protocolo da Internet (IP SLA) para rotas estáticas, incluído nos sistemas operacionais da Cisco, fornece um mecanismo de rastreio da conectividade com a rede de destino a partir do endereço de próximo salto especificado

na rota estática. Dessa maneira, se a conectividade com a rede de destino for perdida por algum motivo, o estado da rota será definido como inativo, e outra rota estática ativa poderá ser selecionada para rotear o tráfego (CISCO, 2020). Sendo assim, os IPs SLAs fornecem uma tecnologia de monitoramento de tráfego ativo a fim de analisar o tráfego na rede a partir de medições contínuas, garantindo melhor desempenho e redundância.

Essa funcionalidade é configurada para enviar pacotes do tipo ICMP, do inglês *Internet Control Message Protocol*, para um endereço de destino definido pelo usuário a fim de monitorar o sucesso ou a falha da comunicação para o destino especificado.A partir disso, é definido um *status* para a operação, sendo ativo, caso o rastreamento tenha ocorrido com sucesso, fazendo assim com que o estado da rota estática permaneça como ativo. Caso contrário, a rota estática assumirá o *status* inativo, e outra rota será anunciada, caso esteja disponível (CISCO, 2020). Dessa maneira, o recurso *IP SLA Tracking* oferece um mecanismo de *backup* confiável, garantindo maior redundância no caso de falhas de dispositivo ou de *link*.

2.11 *Performance* SLA

Acordos de nível de serviço (SLAs), do inglês *Service-level Agreement*, podem ser utilizados para verificar a performance de um determinado serviço. Sendo assim, os SLAs de desempenho presentes na configuração da tecnologia SD-WAN do *firewall* Fortigate, são utilizados para mensurar e avaliar a integridade dos *links* membros do SD-WAN, ao enviar sinais de sondagem através de cada *link* para um servidor e medir a qualidade desse *links* com base em três parâmetros: latência, *jitter* e perda de pacotes (FORTINET, S., s.d.).

Nesse caso, a latência se refere ao atraso, medida em milissegundos (ms), ou seja, a quantidade de atraso que os dados levam para serem transferidos de um ponto a outro na rede. É importante observar, que a largura de banda impactará diretamente no valor da latência, sendo que para uma largura de banda mais estreita, os dados levarão mais tempo para chegar até o servidor (G., 2023).

O *jitter* também é medido em milissegundos e indica a variação da latência ao longo do tempo, ou seja, a variação do atraso na entrega de dados em uma rede. Isso significa que há uma interrupção no envio normal dos pacotes de dados, ocasionando em uma flutuação. No caso normal, os pacotes para um determinado destino, levam aproximadamente o mesmo tempo para chegar, com pequenas variações. Entretanto, se há grandes variações do atraso no envio desses pacotes, como por exemplo: 20ms, 10ms, 40ms, e assim por diante, isso quer dizer que o *jitter* está alto, ou seja, a latência está sofrendo grande variação e isso indica instabilidade na conexão (REDE, 2021).

Já a perda de pacotes, também conhecido por seu termo em inglês, *Packet Loss*, significa que os pacotes se perderam no caminho entre a origem e o destino final. Isso pode ocorrer por diversos motivos, como por exemplo, sobrecarga da rede ou até mesmo baixa qualidade da conexão, seja por problemas na infraestrutura da organização ou por interferências externas (PONTES, 2023).

Sendo assim, se um dos *links* membros do SD-WAN falhar em todas as verificações de integridade, as rotas para esse *link* serão removidas do balanceamento de carga e o tráfego será roteado

por meio de outros *links* que estiverem disponíveis, evitando, portanto, que o tráfego de dados seja enviado para um *link* indisponível (FORTINET, S., s.d.), permitindo maior gerenciamento e desempenho nas comunicações.

Dessa maneira, ao se analisar questões de performance para o tráfego de dados em uma rede, é necessário seguir a recomendação dada pela I.350 do ITU-T, no qual define a Qualidade de Serviço (QoS) como sendo um conjunto de características necessárias para atingir a qualidade de uma certa funcionalidade/serviço. Com isso, certos parâmetros devem ser estabelecidos para que seja assegurado que todos os componentes da rede possam atingir um nível aceitável de QoS (PINHEIRO, J. M. S., 2008). E nesse projeto, a fim de verificar a performance da comunicação entre os túneis SD-WAN que interligam os campus da UnB, três parâmetros serão verificados: latência, *jitter* e perda de pacotes a partir do protocolo ICMP.

2.12 Gerenciamento de Redes e Sistemas

A gerência de uma rede tem como objetivo controlar uma rede de dados visando maximizar sua eficiência e produtividade, o que também inclui o monitoramento e controle dos elementos da rede, sendo eles físicos ou lógicos, de forma que seja assegurado um nível de qualidade de serviço ideal. Portanto, a obtenção de informações da rede, o tratamento dessas informações e a entrega de diagnósticos e soluções são tarefas de gerenciamento.

Não é novidade o fato de que as redes de Internet são indispensáveis nos dias atuais. Seja para o uso no ambiente doméstico, em hospitais ou em grandes corporações, é na Internet que estão diversos recursos importantes para o bom funcionamento da sociedade. Assim, para que haja a garantia de que se tenha um bom funcionamento de cada rede de Internet, faz-se necessário haver o gerenciamento dessas redes, que estão cada vez mais heterogêneas e complexas.

Um gerente de rede é responsável então por monitorar o comportamento da rede e, caso necessário, atuar na resolução de possíveis problemas. Por exemplo, caso seja verificado uma incidência de erro de entrega de pacotes ou o aumento repentino da latência em algum dos *links*, é atribuição do gerente da rede verificar e tomar atitudes de forma a garantir a qualidade do ambiente sendo monitorado.

Dessa maneira, a partir do tema foco deste projeto, com a interligação das redes LANs dos campus da UnB, é também de grande importância o gerenciamento das redes WAN. Dessa maneira, a tecnologia SD-WAN oferecida pela Fortinet possui alguns benefícios, como:

- Painel de gerenciamento único e centralizado, para configuração e gerenciamento de WAN, *cloud* e segurança;
- Provisionamento automatizado e baseado em modelo em todos os locais: filial, campus e nuvem;
- Relatório detalhado de aplicações e desempenho de WAN para análise de negócios e antecipação da largura de banda necessária.

Com isso, a tecnologia SD-WAN, além de possuir os melhores recursos de segurança, roteamento avançado e otimização de WAN, também oferece um gerenciamento simplificado de forma a obter as informações necessárias de desempenho do negócio.

2.13 Segurança

Se por um lado é boa a notícia de que a Internet está sendo cada vez mais utilizada e tornando-se uma das principais ferramentas de comunicação, também é de se preocupar o fato de que pessoas maliciosas podem se aproveitar desse espaço, que é público, para prejudicar outras pessoas, tornando assim o ambiente vulnerável. Dessa forma, atualmente nenhuma rede é projetada sem levar em consideração medidas de segurança para impedir a ocorrência de acessos não autorizados na rede.

O *firewall* é um ativo de rede amplamente conhecido e que é utilizado visando implementar medidas de segurança visto que nele é possível criar regras de acesso (PINHEIRO, J., 2004) que irão definir quem pode ou não ter a permissão de trafegar entre a rede interna e externa de uma organização, estabelecendo assim uma espécie de barreira entre uma rede interna conhecida e uma rede externa totalmente desconhecida, como ilustrado na Figura 2.10. Além de ser possível controlar o tráfego entre a rede interna e externa, também é possível realizar controles de acesso entre os próprios ativos da rede, administrando quem tem ou não autorização para acessar certos dispositivos ou endereços de internet.

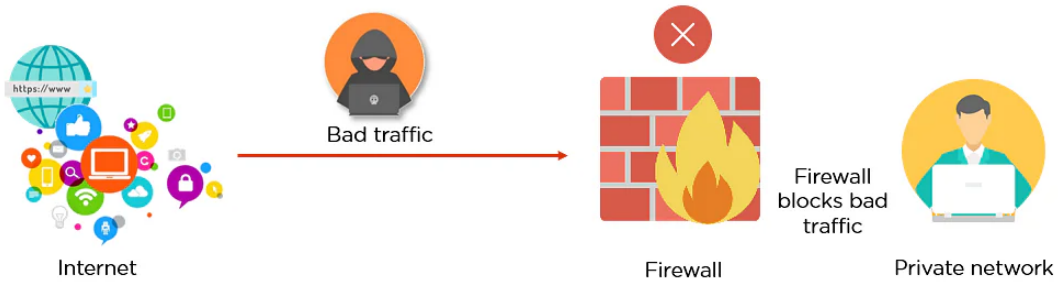


Figura 2.10: *Firewall* e sua relação com a rede interna e externa.

Dessa maneira, é imprescindível analisar todas as medidas de segurança necessárias na implementação de uma rede, tanto na comunicação entre diferentes usuários, conhecido como tráfego leste-oeste, como também na comunicação da rede interna e rede externa, conhecido como tráfego norte-sul. Assim, em um arquitetura de universidade composta por diversos campus, além da tecnologia SD-WAN utilizada é importante analisar as questões de segurança, e o *firewall* da FortiGate a ser utilizado neste projeto possui uma integração de *Next Generation Firewall* com SD-WAN (DANRESA, s.d.), como pode ser visto na Figura 2.11.

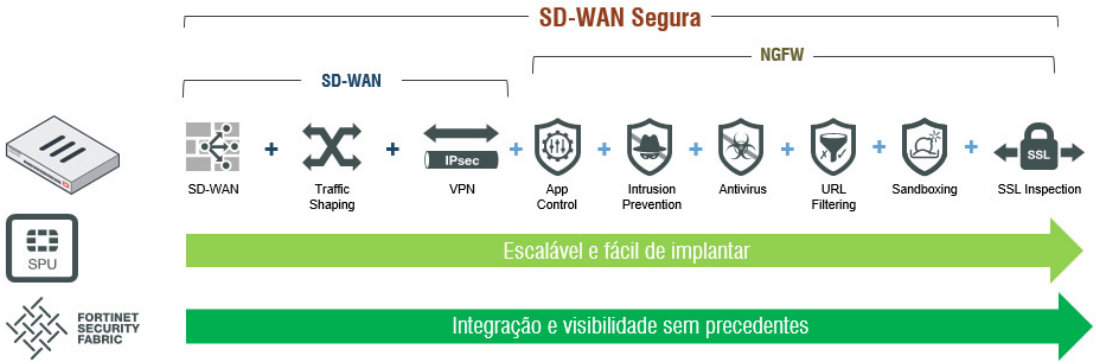


Figura 2.11: FortiGate *Next Generation Firewall* com SD-WAN integrada. Fonte: (DANRESA, s.d.)

.

Capítulo 3

Ferramentas Utilizadas

3.1 Graphical Network Simulator 3

O GNS3, do inglês *Graphical Network Simulator*, é um *software* de simulação de redes utilizado neste projeto, que permite a implementação de uma infraestrutura de rede completa, que está de acordo com o que seria implementado em um ambiente real. Dessa maneira, o GNS3 torna possível a realização de estudos, análises e conclusões acerca do funcionamento de uma rede, sem que com isso esteja atrelado custos monetários ou ainda o transtorno que a implementação dessa infraestrutura somente para testes ocasionaria. Por se tratar de um *software* de código aberto, torna-se somente necessário realizar a sua instalação, sem precisar levar em consideração questões que dizem respeito ao direito de uso.

Com o GNS3 é possível ter uma integração com dispositivos de redes disponíveis no mercado, emulando o próprio processador do dispositivo ao utilizar imagens fornecidas pelas próprias fabricantes, permitindo assim uma virtualização completa de um sistema dentro de outro. Assim sendo, é possível reafirmar que na infraestrutura de rede implementada, serão utilizadas as mesmas ferramentas e dispositivos que seriam utilizados no ambiente real. Para a realização deste projeto, foi possível realizar a inserção dos seguintes ativos externos no GNS3: *firewalls* da Fortigate, *switches* Extreme, roteadores da Cisco e também o sistema operacional Ubuntu. Os ativos externos mencionados serão detalhados nos tópicos seguintes.

Assim como dito acima, o GNS3 permite trabalhar com QEMUs (*Quick Emulators*), no qual implementa um emulador de processador, permitindo uma virtualização completa de um sistema dentro de outro. No caso deste projeto foi criado uma QEMU para a utilização do *switch* EXOS da Extreme *Networks*, a fim de utilizá-lo como *switch* de acesso *Layer* 2/ *Layer* 3 da rede. Também foi criado para a utilização dos roteadores CISCO 7200 como roteadores da provedora presentes no *backbone*. Além disso, foi ainda criada uma QEMU para o Fortigate, o *firewall* da Fortinet. Mais detalhes com relação a esses dois recursos serão posteriormente mencionados.

Por fim, é importante mencionar que, apesar de ser possível simular uma infraestrutura de redes no GNS3 em um computador pessoal, para o caso deste projeto foi utilizado somente o Servidor de Emulação de Redes para Emulação de Redes de Forma Remota, que está localizado no LabRedes,

da Faculdade de Tecnologia da Universidade de Brasília. Este servidor conta com uma capacidade de memória RAM de 512 GB, o que torna qualquer tipo de simulação livre de possíveis sobrecargas na capacidade operacional da máquina.

3.2 FORTIGATE

O FortiGate é um *firewall* de proteção de rede desenvolvido pela Fortinet, uma empresa multinacional que oferece soluções de segurança cibernética, no que diz respeito à convergência de rede e segurança. Inclusive, no que tange um dos escopos deste projeto, de implementação de SD-WAN, é pertinente a menção de que a fabricante Fortinet, foi nomeada líder por quatro anos consecutivos e a mais alta em capacidade de execução por dois anos consecutivos para a solução SD-WAN, conforme pode ser visto na Figura 3.1 (FORTINET, 2023).

Figura 3.1: Fortinet nomeada líder no Gartner® Magic Quadrant™ 2022 para SD-WAN. Fonte: (FORTINET, 2023)

Sendo assim, a solução FortiGate *Secure* SD-WAN da Fortinet que será utilizada no Projeto Final de Graduação inclui os melhores recursos para a adoção de uma rede SD-WAN em qualquer tipo de negócio, no qual pode ser aplicado por empresas globais sensíveis à segurança e que priorizam a nuvem. As seguintes características são aplicadas nesta solução: Segurança de *Next-Generation Firewall* (NGFW); Consolidação da rede SD-WAN; Roteamento avançado; Otimização de WAN, fornecendo uma transformação de borda WAN baseada em segurança em uma oferta uni-

ficada; Controlador de caminho de WAN com remediação; Identificação e direção de aplicativo mais rápidas e, melhor preço/desempenho de Borda WAN.

Ao acessar o *marketplace* do GNS3 foi possível realizar o *download* da *Appliance* do Fortigate na versão FortiOS 7.0.10. Para a realização do *download* da imagem nesta versão foi necessário realizar cadastro no FortiCloud, que trata-se de uma plataforma oficial da Fortinet, e em seguida selecionar a opção de imagem desejada. Sendo assim, neste projeto foi utilizado uma versão do *firewall* Fortinet disponibilizada pela própria fabricante, garantindo a conformidade com os direitos de uso concedidos pela empresa.

3.3 *SWITCH* EXTREME

A Extreme N*etworks* é uma empresa líder em infraestrutura de redes em nuvem (*cloud networking*) e tem como foco a entrega de serviços para conectar dispositivos, aplicações e pessoas. Ela trabalha desenvolvendo, projetando e fabricando equipamentos utilizados na composição de uma infraestutura de rede, seja ela com ou sem fio. Além disso, a Extreme *Networks* também atua de forma a desenvolver o seu próprio *software*, utilizado em seus equipamentos, para o gerenciamento da rede, políticas, controle de acesso, dentre outros.

Tendo em vista que na implementação deste projeto final é priorizada a utilização de dispositivos de última geração e que cumpram com as demandas de segurança e boas práticas atuais, foi realizada a escolha de um equipamento da Extreme, o *Switc*h EXOS em sua versão 31.7.1.4 para compor os *switches* de Acesso, Core e Distribuíção de cada uma das quatro LANs geograficamente separadas.

Um *switch* trata-se de um dispositivo que conecta usuários, dispositivos e recursos que compõem uma rede. A utilização do *switch* Extreme apresenta a vantagem de que ele consegue integrar qualquer infraestrutura de rede, independentemente da presença de dispositivos de outros fabricantes, por ser um "*Switch Universal*", onde ele pode rodar dois tipos de sistemas operacionais: a *Switch Engine* (EXOS) ou o *Fabric Engine* (VOSS).

A realização da instalação da imagem do EXOS não se fez necessária, pois o Servidor de Emulação de Redes para Emulação de Redes de Forma Remota, utilizado como Servidor GNS3 deste projeto, já continha o QEMU deste *switch*. É importante reafirmar que esse QEMU está presente no Servidor de maneira legal, ou seja, cumprindo com os conformes legais de direitos de propriedade que a *Network* Extreme possui.

3.4 CISCO

Mundialmente conhecida no mercado de rede, a Cisco é uma empresa líder mundial no fornecimento de equipamentos de rede para Internet (EXAME, 2018). A qualidade dos *hardwares* e *softwares* criados e vendidos pela Cisco é a razão que justifica a sua consolidação no mercado.

Os roteadores que compõem o *backbone* da infraestrutura de rede implementada neste projeto

são da Cisco, no modelo 7200 v. 124-24.T5. Uma das razões pela qual foi priorizada a escolha de roteadores Cisco, foi o fato deles oferecerem a funcionalidade de implementação de MPLS (*Multiprotocol Label Switching*), um protocolo de roteamento que concede uma tecnologia de tráfego de dados baseado em rótulos/etiquetas pré-determinados para cada pacote na comunicação, no qual proporciona encaminhamento e comutação eficiente de forma mais rápida, como já mencionado anteriormente.

Assim como no caso do FortiGate, foi necessário realizar a instalação da imagem do roteador da Cisco para posteriormente adicioná-lo ao GNS3. Primeiramente foi efetuado a instalação da *Appliance* do Cisco 7200 no *MarketPlace* oficial do GNS3 e em seguida realizado a instalação da imagem correspondente ao roteador da Cisco 7200 124-24.T5. A instalação dessa imagem ocorreu em um repositório que disponibiliza imagens IOS para *Dynamips*, que é um tipo de emulador dedicado para emular alguns tipos de *hardwares* da Cisco, principalmente quando se trata de imagens mais antigas. É válido pontuar que essas instalações ocorreram dentro dos parâmetros legais, ou seja, cumprindo com os conformes legais de direitos de propriedade que a Cisco *Systems*, Inc. possui.

3.5 UBUNTU

O Ubuntu é um sistema operacional configurável, estável e de fácil uso, com uma interface gráfica bem construída e intuitiva, sendo uma das distribuições mais populares do Linux. Neste projeto foi utilizado o Ubuntu 18.04 LTS, que trata-se da primeira versão LTS com 5 anos de suporte, que contém um *Gnome Shell* como interface gráfica. Essa versão apresenta uma maior estabilidade e com um melhor *Apport*, quando comparado com versões anteriores.

Especificamente neste projeto, o Ubuntu foi escolhido e implementado para ser possível efetuar o acesso à interface gráfica (GUI) do *firewall* FortiGate, onde será possível controlar, editar, implementar e monitorar as diversas configurações dentro do *firewall*, como regras de *firewall*, implementação de regras SD-WAN, dentre outras funcionalidades. Utilizando a interface gráfica do FortiGate à partir do Ubuntu é inclusive possível ter acesso à CLI do *firewall*. Outra utilização do Ubuntu será na rede interna de cada campus, mais detalhes do seu uso serão expostos nas seções subsequentes.

A imagem do Ubuntu utilizado já estava localizada no Servidor de Emulação de Redes para Emulação de Redes de Forma Remota, utilizado como Servidor GNS3 deste projeto. Sendo assim, não foi necessário realizar a sua instalação.

3.6 WIRESHARK

É possível analisar cada um dos pacotes e protocolos das camadas do modelo TCP/IP utilizando um analisador de pacotes, ou como também chamado de "*sniffer*", muito utilizado por especialistas de TI e engenheiros, que tem por objetivo interceptar cada pacote e registrar o tráfego que passa

sobre uma rede, permitindo analisar de forma aprofundada os diferentes valores do cabeçalho dos pacotes, seus conteúdos ou especificações, como também auxiliar na detecção de problemas, durante o monitoramento do fluxo de redes. No entanto, o farejador de pacote pode ser utilizado para propósitos maliciosos, no qual invasores (*hackers*) o utilizam para capturar o tráfego da rede, roubando e coletando dados de usuários, como por exemplo, senhas e arquivos importantes.

Os *sniffers* podem ser classificados em dois tipos. Sendo o *sniffer* passivo, aquele que todo o tráfego capturado não pode ser alterado de nenhuma maneira, sendo apenas possível analisá-lo. Já o *sniffer* ativo, além de poder monitorar e analisar o tráfego, é possível alterá-lo de alguma forma (MACÊDO, 2017). Este tipo é muito praticado por atacantes de rede e pode ser evitado instalando um antivírus potente, não visitando sites sem criptografia, não utilizando redes Wi-Fi públicas, entre outras medidas (BELCIC, 2020).

Existem diversos analisadores de pacotes que podem ser utilizados hoje em dia de forma gratuita, como por exemplo, Microsoft Network Monitor, Capsa Packet Sniffer, InnoNWSniffer, SniffPass e o WireShark que é o mais utilizado. É importante entender que a placa de interface de rede deve estar atuando em modo promíscuo para que o *sniffer* seja eficaz (MACÊDO, 2017). Dessa forma, este projeto apresentará a utilização do *sniffer* WireShark a fim realizar coletas de estatísticas da rede, análise de protocolos e compreensão a respeito do encapsulamento de dados na arquitetura em camadas do TCP/IP.

Capítulo 4

Metodologia

Este capítulo visa descrever toda a arquitetura proposta bem como a metodologia utilizada para a condução dos testes de conectividade realizados. Além disso, é descrito todas as configurações realizadas para o perfeito funcionamento da topologia de redes. Sendo assim, espera-se que a partir do conteúdo apresentado por este, seja possível o entendimento de como as tecnologias envolvidas na solução proposta podem ser utilizadas de forma híbrida em ambientes reais, objetivando obter um gerenciamento simplificado de toda a rede WAN, bem como maior performance, segurança e custo-benefício.

4.1 Arquitetura Proposta

Com o alto desenvolvimento tecnológico, adoção da nuvem de forma integral ou híbrida, busca por eficiência, desempenho, baixa latência, segurança, gerenciamento simplificado e custo benefício, as empresas no geral encontram desafios para absorver o crescente tráfego da WAN. Dessa maneira, é essencial a implementação de um modelo ideal que esteja de acordo com as tendências atuais e futuras do ponto de vista de redes, como também de mercado.

Além disso, as redes de campus estão em crescente evolução e compreendem uma variedade de dispositivos IP, e por isso, os usuários destas localidades exigem conectividade constante e experiência de qualidade. Dessa maneira, é necessário que esse tipo de infraestrutura obtenha flexibilidade, escalabilidade e alta qualidade de serviço, ao mesmo tempo que os dados críticos são protegidos contra acessos não autorizados (JUNIPER, 2020).

Com isso, o projeto, como citado anteriormente, tem como finalidade estudar, identificar, projetar e analisar a arquitetura de redes de campus com o emprego da tecnologia SD-WAN e com a combinação de um serviço de transporte MPLS em seu *backbone* provido por uma operadora de Internet. É ainda possível dizer que essa arquitetura contará com um modelo híbrido, ou seja, integração com o ambiente de simulação e a *cloud*, isso porque a infraestrutura criada no *software* de simulação GNS3 funciona utilizando o Servidor de Emulação de Redes para Emulação de Redes de Forma Remota do Lab Redes, que está remotamente localizado e, além disso, essa infraestrutura só terá acesso a Internet ao passar pela rede do Lab Redes, utilizando esse mesmo servidor.

4.1.1 Arquitetura Hipotética de Redes - UnB

Dessa forma, a infraestrutura hipotética escolhida para esta implantação refere-se a rede campus da Universidade de Brasília, no qual conta com quatro campus: Darcy Ribeiro localizado no Plano Piloto, Faculdade de Ceilândia (FCE), Faculdade do Gama (FGA) e Faculdade de Planaltina (FUP). Sendo assim, é necessário realizar a interconexão de todos estes segmentos, formando uma grande malha, conhecida como Rede WAN. A Figura 4.1 abaixo ilustra esta infraestrutura de maneira simplificada.

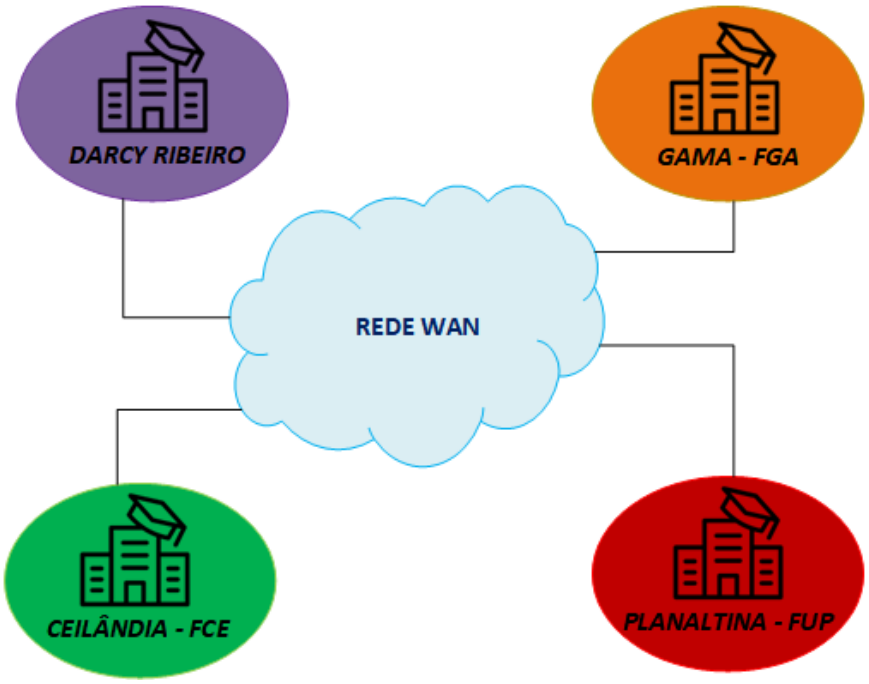


Figura 4.1: Infraestrutura de campus da Universidade de Brasília - UnB. Fonte própria

Sabe-se que podem ser utilizados diferentes tipos de tecnologias para estabelecer a comunicação entre as LANs, neste caso, conforme mencionado anteriormente, será utilizado a tecnologia SD-WAN com a combinação do serviço de transporte MPLS no *backbone* a fim de garantir transmissão de dados entre diferentes tipos de usuários com segurança, garantia de desempenho, resiliência consistente, suporte para nuvem e tolerância a falhas a partir da automatização do direcionamento de tráfego de maneira orientada por parâmetros de qualidade de serviço entregue pela solução SD-WAN.

4.1.2 Infraestrutura Geral de Implementação

4.1.2.1 Rede Local - *Intranet*

Primeiramente, é importante compreender a composição e funcionalidade da *Intranet*, antes de se pensar na infraestrutura WAN que interliga os campus da Universidade. A *Intranet* é uma rede de ativos privada de uma organização, ou seja, de uso exclusivo por utilizadores e colaboradores internos da empresa. Os usuários desta área devem ser capazes de realizar comunicação interna

instantânea, ter acesso à rede local, compartilhamento de dados e acesso à Internet.

Normalmente, em uma rede de campus, é adotado um *design* em camadas, dimensionado de acordo com as necessidades de cada campus, no qual é composto por uma camada *Core*, Agregação/Distribuição e uma camada de Acesso, no qual compreende a borda da rede interna. Essa arquitetura pode ser visualizada na Figura 4.2. Conforme as práticas recomendadas para a implementação de uma rede Campus pela Cisco, este modelo é utilizado continuamente, pois é comprovadamente escalável a fim de se adequar a todos os casos de uso (CISCO, 2022).

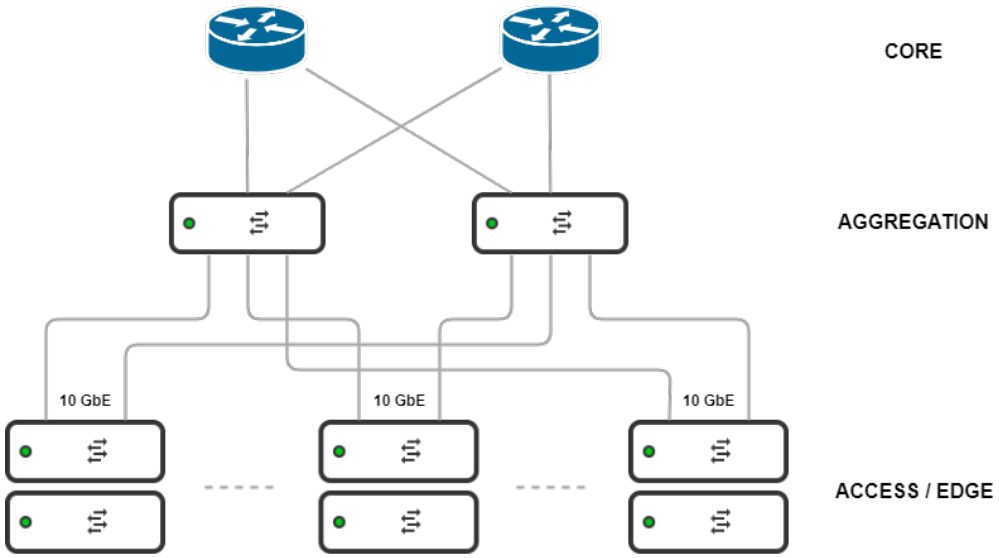


Figura 4.2: Modelo escalável para implementação interna de uma rede Campus. Fonte: (CISCO, 2022)

Sendo assim, a partir da infraestrutura de redes proposta para a Universidade de Brasília (UnB) composta por quatro campus, cada pólo universitário, contará com os seguintes dispositivos:

- ***Switches* de Acesso:** Localizado na borda da rede e possui como objetivo interligar os diversos dispositivos finais à rede interna da organização, como computadores, impressoras e *access points*. Cada departamento dentro da universidade pode possuir seu próprio CPD contendo a quantidade necessária de *switches* de acesso a fim de atender a quantidade de usuários naquela localidade;
- ***Switches* de Distribuição/Agregação:** Localizado na camada intermediária da rede, no qual se conecta ao *switch* Core no lado da transmissão e ao *switch* de acesso no lado da recepção. Sua principal função é agregar os dados da borda, ou seja, limitar a quantidade de conexões dos *switches* de acesso ao núcleo da rede, como também obter maior redundância;
- ***Switch* Core:** Comumente caracterizado como sendo o *switch* central da rede, ou seja, o equipamento concentrador. Dessa forma, este equipamento interliga os equipamentos de rede, como, por exemplo, *switches* de acesso/agregação, *firewall*, servidores, entre outros.

Com isso, a fim de simular a proposta de redes de maneira ideal, foram implementados dois de cada um dos equipamentos, pois é fundamental garantir a redundância da infraestrutura de redes,

obtendo uma adição de caminhos alternativos, gerando continuidade de serviços em caso de algum tipo de crise ou inatividade de algum dispositivo de rede.

Além disso, os usuários presentes na rede interna do campus, serão subdivididos em VLANs, para que sejam criados domínios de *broadcast* separados provendo um melhor desempenho, gerenciamento, segurança e escalabilidade. Para isso, é necessário que a arquitetura das VLANs seja troncalizada apenas para determinados pontos do campus, a fim de transmitir comunicação apenas para os usuários realmente presentes em cada localidade.

A segurança de redes também é imprescindível em uma organização, com objetivo de garantir proteção de qualquer rede contra ataques internos/externos, instabilidades de dados e acesso não autorizado. Um *firewall* é uma solução que executa uma barreira entre redes internas e externas, que trabalha de forma a evitar que perigos vindos da rede externa ultrapassem para dentro da rede interna. Dessa maneira, este dispositivo controla, separa, analisa e bloqueia os tráfegos indesejados dentro da organização e está presente na camada de borda externa de cada campus.

Neste caso, o *firewall* FortiGate além das funcionalidades de segurança de próxima geração com roteamento avançado, também oferece a solução de implantação e gerenciamento SD-WAN em seu dispositivo. Dessa maneira, a arquitetura utilizada neste projeto foi indicada pelo Gartner, como pode ser visto na Figura 4.3, e se refere ao *firewall* FortiGate com SD-WAN incorporado, no qual além dessas funcionalidades, ele será considerado como o dispositivo cliente de borda para a rede externa.

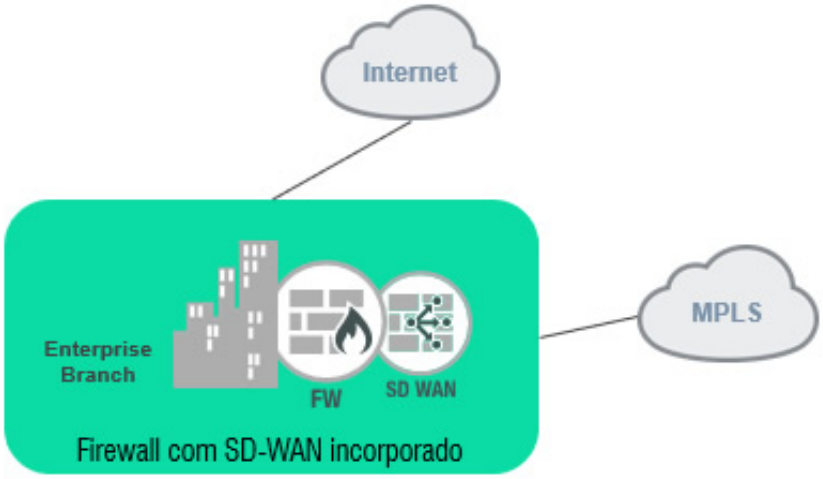


Figura 4.3: Arquitetura indicada pelo Gartner - Firewall com SD-WAN incorporado. Fonte: (DANRESA, s.d.)

Sendo assim, a solução SD-WAN aproveita os pontos de conectividade para decidir qual dos caminhos é o mais apropriado para direcionar o tráfego a partir do monitoramento de três parâmetros: latência, *jitter* e perda de pacotes. Dessa maneira, é garantido o desempenho e maximização da disponibilidade dos serviços.

4.1.2.2 Rede WAN - *Backbone* Externo

Sabe-se que a rede WAN interliga um conjunto de redes locais (LANs) ou outras redes privadas que se comunicam entre si e possuem acesso à Internet. Neste caso, o *firewall* da FortiGate realizará conexão direta com ativos que provêm acesso à Internet. Estes ativos são conhecidos como o *Backbone* da provedora, no qual tem como objetivo ser um esquema de ligações centrais de alto desempenho por onde os dados dos clientes da Internet trafegam. Dessa maneira, foi configurado um *backbone* em formato "malha", para que os ativos de um campus possam obter acesso à Internet e acesso aos outros campus de maneira redundante, a partir da combinação da tecnologia SD-WAN e o serviço de transporte MPLS L3VPN, composta por quatro roteadores, sendo dois deles dispositivos de borda da provedora, e outro dois denominados como roteadores da operadora, no qual estão conectados diretamente à *cloud*, a fim de obter acesso externo à Internet e à rede do Laboratório de Redes presente no campus Darcy Ribeiro.

4.1.2.3 Infraestrutura Física

A partir das informações citadas anteriormente, a topologia de implementação física proposta para as redes internas dos campus da UnB, como também a rede externa conhecida como *Backbone* da provedora, pode ser visualizada na Figura 4.4 a seguir:

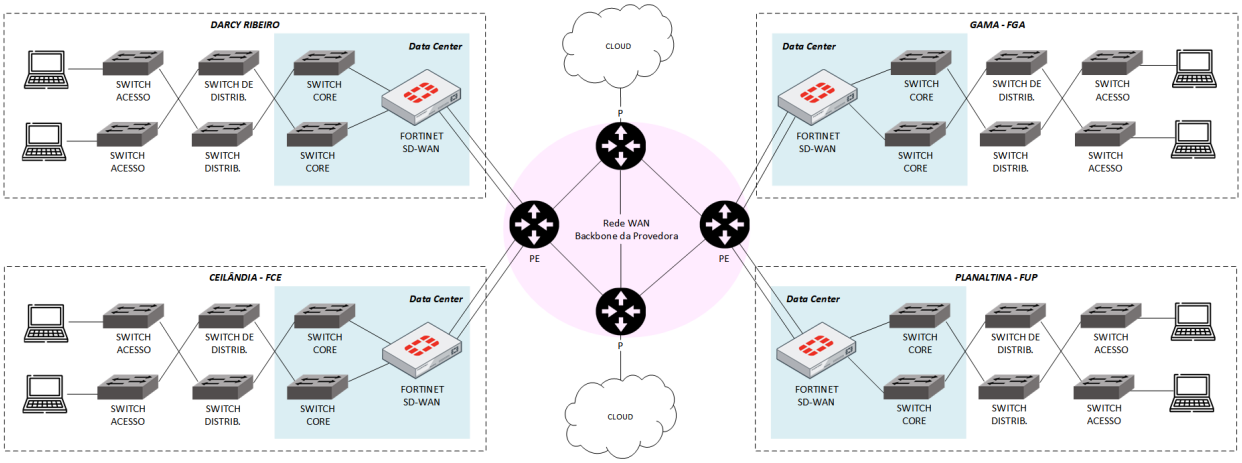


Figura 4.4: Infraestrutura física proposta. Fonte própria

4.1.2.4 Infraestrutura SD-WAN ADVPN

Com a infraestrutura física é fundamental compreender a estrutura lógica da implementação da topologia SD-WAN, no qual todos os campus, além da conexão com a Internet através do *backbone* que possui o MPLS L3VPN implantado, deverão se comunicar entre si a partir da tecnologia de tunelamento dinâmico - *Auto-Discovery VPN* (ADVPN), no qual é criado túneis IPsec automaticamente entre os sites que desejam se comunicar. Esses túneis tornam-se imediatamente parte da topologia de *overlay* da solução SD-WAN.

Dessa maneira, a infraestrutura lógica SD-WAN ADVPN entre os campus da Universidade pode ser observada a partir da Figura 4.5 abaixo:

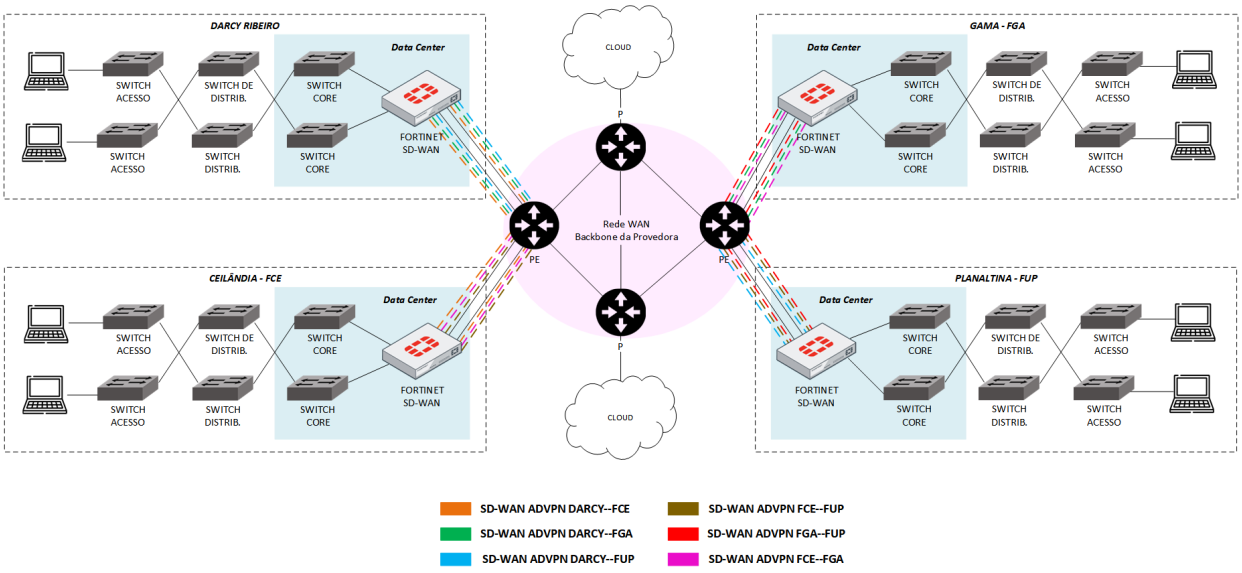


Figura 4.5: Infraestrutura SD-WAN ADVPN proposta. Fonte própria

4.2 Etapas para implementação do projeto

A partir da infraestrutura descrita acima, a implementação e execução do projeto foi confeccionada de forma a permitir um entendimento passo-a-passo da arquitetura proposta, como demonstrado a seguir:

- **PASSO 1 → Instalação da aplicação GNS-3 e conexão com o Servidor de Emulação de Redes para Emulação de Redes de Forma Remota:** O GNS-3 é o sistema emulador e simulador utilizado para este projeto, e para isso foi utilizado o servidor de forma remota para emular a arquitetura proposta;
- **PASSO 2 → Instalação dos *appliances* e configuração das QEMUs para os dispositivos de redes necessários:** Os QEMUs permitirão uma virtualização completa de um sistema dentro de outro, com isso, será possível obter os dispositivos de redes necessários para as funcionalidades que devem ser implementadas no projeto;
- **PASSO 3 → Implementação das Redes Internas de cada campus da UnB:** Implementação da Intranet composta por *switches* Core, de distribuição e acesso, juntamente com o *firewall* FortiGate exercendo função de *gateway* das redes;
- **PASSO 4 → Implementação dos perfis de segurança para cada tipo de usuário:** Implementação de perfis de segurança a fim de controlar o tráfego de dados entre os diferentes usuários dentro da infraestrutura;

- **PASSO 5 → Implementação do *Backbone* externo e interligação com as redes dos campus:** Implementação da rede WAN composta por roteadores de alto desempenho, através da tecnologia MPLS L3VPN;
- **PASSO 6 → Implementação da tecnologia SD-WAN ADVPN:** Implementação conjunta da tecnologia SD-WAN ADVPN a fim de obter automatização e maior desempenho entre a conectividade dos campus;
- **PASSO 7 → Testes e análises de resultados:** Após todo o cenário configurado e entendido, é necessário realizar testes de conectividade de toda a infraestrutura. Estes testes e resultados serão melhor detalhados no capítulo 5.

4.3 Configuração e Desenho da Arquitetura

4.3.1 Instalação e Utilização da Aplicação GNS-3

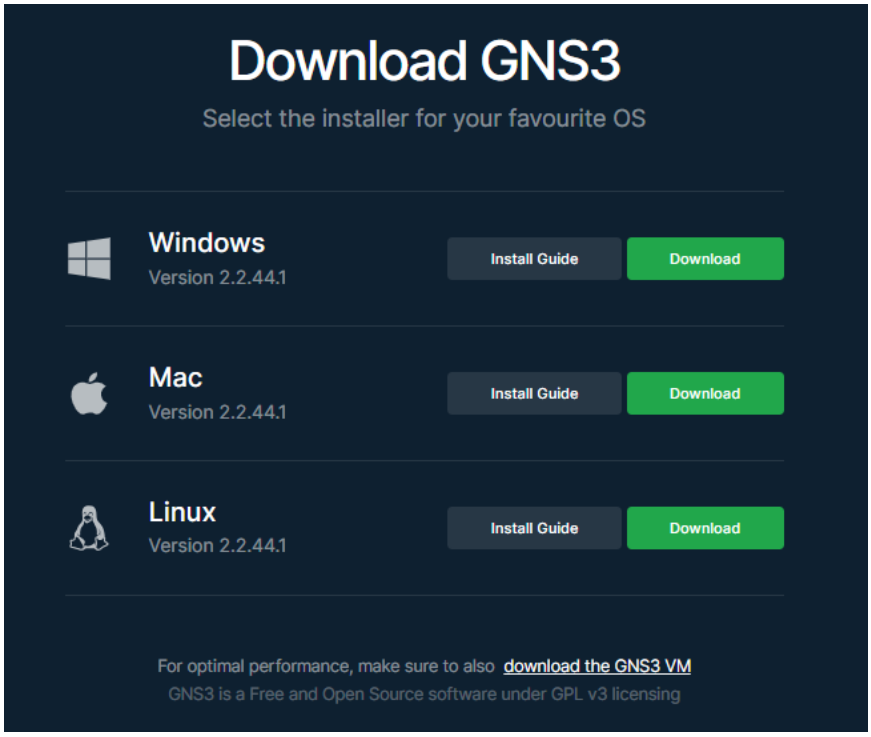


Figura 4.6: Página de *Download* GNS3. Fonte Própria.

O GNS3 trata-se de um *software* de simulação de redes de código aberto, assim como descrito na seção 3.1, que dá ao usuário a possibilidade de emular redes reais, permitindo assim análises completas, eficazes e com alto custo-benefício, visto que é possível verificar o resultado da arquitetura de rede proposta sem que com isso seja necessária a implementação de toda essa infraestrutura em um ambiente real, poupando tempo e custos associados.

Para a realizar a instalação do GNS3 é necessário ir até o site oficial do GNS3 e instalar a versão relacionada ao sistema operacional utilizado e em seguida instalar também um GNS3 VM,

podendo ser importado, por exemplo, para o *VMware Workstation*. A opção para instalar o GNS3 VM aparecerá na própria página de *download* do GNS3, como visto na Figura 4.6.

O GNS3 é um tipo de aplicação cliente-servidor, onde a interface gráfica apresentada se refere ao lado cliente e o GNS3 VM instalado é a parte que corresponde ao servidor, que atuará como um servidor virtual para viabilizar a comunicação com a Internet e também na comunicação entre cliente-servidor.

Para a realização desse Projeto não foi necessário realizar o *download* do GNS3 VM, isso porque foi utilizado o Servidor de Emulação de Redes para Emulação de Redes de Forma Remota do Lab Redes, que está remotamente localizado na Faculdade de Tecnologia - UnB. Portanto, bastou efetuar o *download* do GNS3 e configurar o servidor informando endereço IP correspondente ao servidor remoto utilizado.

4.3.2 Instalação dos *Appliances* dos dispositivos de redes

4.3.2.1 *Firewall* FortiGate

Com a instalação do FortiGate no GNS3 será possível ter acesso não somente a CLI, mas também à interface gráfica deste *firewall*, trazendo assim uma experiência completa e próxima ao real.

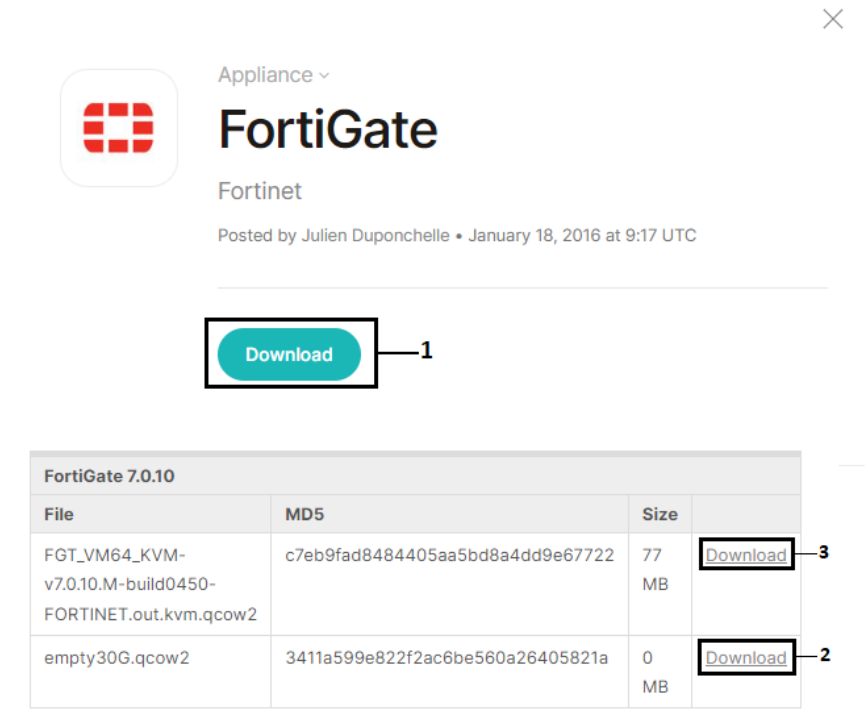


Figura 4.7: Ordem de *download* de *Applicance* do Fortigate no *MarketPlace* do GNS3. Fonte Própria.

Em um primeiro momento foi necessário acessar o *marketplace* do GNS3 (https://gns3.com/

marketplace/featured), no site oficial do GNS3, onde é possível realizar o *download* das *Appliances* disponíveis. Nesse caso, o *Appliance* escolhido foi do FortiGate em sua versão 7.0.10, após a instalação da *Applicance* (item 1 da Figura 4.7) e do arquivo explicitado no item 2 da Figura 4.7 é necessário manter esses arquivos localmente no computador, pois serão utilizados posteriormente no GNS3.

O próximo passo é realizar o *download* da imagem do FortiGate e para isso é necessário selecionar o botão "*Download*" (item 3 da Figura 4.7), que redireciona para a página oficial da FortiGate, o FortiCloud. Nesse momento é preciso se cadastrar na FortiCloud, utilizando e-mail e senha e, após logado, ir até a aba *Download* > *VM Images*; selecionar "FortiGate" como produto; "KVM" como plataforma; e a versão utilizada para só então finalmente realizar o *download* da Imagem ao clicar em "*Download*" no arquivo que contém a extensão ".out.kvm".

Por fim, é necessário adicionar essa *Appliance* no GNS3 ao selecionar *File* > *Import Appliance* e importar a *Applicance* anteriormente instalada. Em seguida, na própria janela já aberta, basta se certificar que todos os arquivos que o GNS3 requer sejam importados corretamente. O procedimento de importar *appliance* trata-se de algo simples e intuitivo dentro do GNS3.

4.3.2.2 Cisco

Figura 4.8: Ordem de *download* de *Applicance* da Cisco no MarketPlace do GNS3. Fonte Própria.

Neste projeto foi possível emular o roteador da Cisco, em sua versão 7200 124-24.T5, no GNS3, permitindo a implementação de configurações e obtênção de análises idênticas às que seriam realizadas em um ambiente de infraestrutura de rede *on-premises*.

Em um primeiro momento foi necessário acessar o *marketplace* do GNS3 (https://gns3.com/marketplace/featured), no site oficial do GNS3, onde é possível verificar todas as *Appliances* que

podem ser utilizadas no GNS3. Nesse caso, o Appliance escolhido foi o da Cisco e a realização do *download* trata-se de um procedimento simples e intuitivo. No site do *marketplace* do GNS3, basta clicar em "*Download*" no item 1 destacado na Figura 4.8.

O próximo passo é realizar o *download* da imagem do roteador Cisco na versão 7200 124-24.T5 e para isso é necessário selecionar "*Download*" (item 2 da Figura 4.8), que iniciará o *download* automaticamente. Após ter sido efetuado a instalação da *Appliance* e da Imagem, basta se certificar que os arquivos foram salvos corretamente no computador para depois serem utilizados no GNS3.

Finalmente, como último passo é necessário adicionar essa *Appliance* no GNS3 ao selecionar *File* > *Import Appliance* e importar a *Applicance* anteriormente instalada. Em seguida, na própria janela já aberta, basta se certificar que o arquivo referente à imagem do roteador, que o GNS3 requer, seja importado corretamente. Conforme mencionado anteriormente, o procedimento de importar *appliance* trata-se de algo simples e intuitivo dentro do GNS3.

4.3.3 Implementação *Intranet* dos Campus

Com os recursos instalados, é possível iniciar a implementação da infraestrutura proposta conforme ilustrado na Figura 4.4. Assim, inicia-se com a configuração da topologia de redes interna de cada campus. A Figura 4.9 abaixo, exemplifica a arquitetura da *Intranet* no campus Darcy Ribeiro. Essa arquitetura deve ser seguida para os outros pólos universitários.

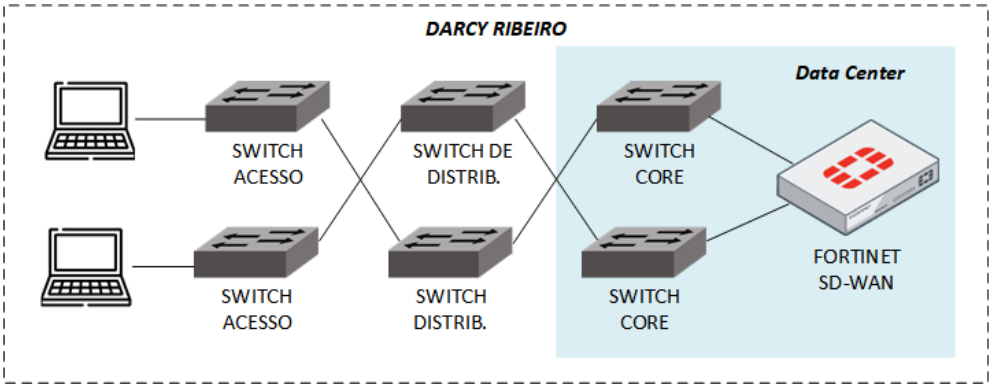


Figura 4.9: Arquitetura da Intranet no campus Darcy Ribeiro. Fonte própria.

Conforme a infraestrutura de redes proposta para cada campus da Universidade de Brasília, os ativos expostos na Tabela 4.1 foram utilizados.

Tabela 4.1: Ativos de Redes utilizados na Intranet de cada campus

Dispositivo	**Modelo**	**Localização**	**Serviços**
Switches Core	Extreme EXOS 31.7.1.4	*Data Center*	*Layer* 2 *Layer* 3
Switches de Distribuição	Extreme EXOS 31.7.1.4	CPD do departamento	
Switches de Acesso	Extreme EXOS 31.7.1.4	CPD do departamento	
Dispositivos Finais	VPC e Ubuntu Linux	Campus	ICMP, FTP, VOIP, SSH, SCP
Firewall	FortiGate v.7.0.12	*Data Center*	NGFW Roteamento avançado SD-WAN

Além disso, para cada campus foi realizada a fragmentação de cinco tipos de usuários presentes nesta topologia em diferentes VLANs, sendo eles: Graduação, Pós-Graduação, Professores, Diretoria e Suporte. Estes usuários devem poder enviar e receber dados diretamente, entretanto, alguns colaboradores finais terão acessos bloqueados a serviços específicos dentro da rede, para uma maior segurança da organização. As informações dos tipos de usuário, para cada pólo universitário podem ser observadas na Tabela 4.2.

É importante mencionar que a escolha das máscaras de rede para cada perfil de usuário foi implementada ao pensar na quantidade aproximada de dispositivos finais para determinado departamento.

Tabela 4.2: Separação dos perfis de usuários em VLANs

VLAN	Nome	Campus	Sub-rede	Gateway
10	GRADUAÇÃO	DARCY	172.24.8.0/21	172.24.15.254 (Firewall FortiGate)
		FCE	172.25.8.0/21	172.25.15.254 (Firewall FortiGate)
		FGA	172.26.8.0/21	172.26.15.254 (Firewall FortiGate)
		FUP	172.27.8.0/21	172.27.15.254 (Firewall FortiGate)
20	PÓS-GRADUAÇÃO	DARCY	172.24.16.0/22	172.24.19.254 (Firewall FortiGate)
		FCE	172.25.16.0/22	172.25.19.254 (Firewall FortiGate)
		FGA	172.26.16.0/22	172.26.19.254 (Firewall FortiGate)
		FUP	172.27.16.0/22	172.27.19.254 (Firewall FortiGate)
30	PROFESSORES	DARCY	172.24.30.0/24	172.24.30.254 (Firewall FortiGate)
		FCE	172.25.30.0/24	172.25.30.254 (Firewall FortiGate)
		FGA	172.26.30.0/24	172.26.30.254 (Firewall FortiGate)
		FUP	172.27.30.0/24	172.27.30.254 (Firewall FortiGate)
40	DIRETORIA	DARCY	172.24.40.0/24	172.24.40.254 (Firewall FortiGate)
		FCE	172.25.40.0/24	172.25.40.254 (Firewall FortiGate)
		FGA	172.26.40.0/24	172.26.40.254 (Firewall FortiGate)
		FUP	172.27.40.0/24	172.27.40.254 (Firewall FortiGate)
50	SUPORTE	DARCY	172.24.50.0/24	172.24.50.254 (Firewall FortiGate)
		FCE	172.25.50.0/24	172.25.50.254 (Firewall FortiGate)
		FGA	172.26.50.0/24	172.26.50.254 (Firewall FortiGate)
		FUP	172.27.50.0/24	172.27.50.254 (Firewall FortiGate)

A partir das informações mencionadas, a *Intranet* realiza a divisão dos usuários em diferentes tipos de VLANs. Com isso, a tabela 4.3 indica os parâmetros de configuração de endereçamento IP em interfaces VLANs em cada um dos *switches* Extreme EXOS presentes em cada campus. Sendo que o valor de "x" presente nos endereços IP de cada ativo, indicará um campus específico. Sendo x=*4* para o campus Darcy; x=*5* para o campus FCE; x=*6* para o campus FGA e por fim, x=*7* para o campus FUP.

Tabela 4.3: Parâmetros utilizados na configuração de endereçamento IP dos ativos presentes na Intranet dos campus UnB

Dispositivo	**VLAN**	**Endereço IP**
CORE-1	10 tagged	172.2x.8.200/21
	20 tagged	172.2x.16.200/22
	30 tagged	172.2x.30.200/24
	40 tagged	172.2x.40.200/24
	50 tagged	172.2x.50.200/24
CORE-2	10 tagged	172.2x.8.100/21
	20 tagged	172.2x.16.100/22
	30 tagged	172.2x.30.100/24
	40 tagged	172.2x.40.100/24
	50 tagged	172.2x.50.100/24
DISTRIBUIÇÃO-1	10 tagged	172.2x.8.20/21
	20 tagged	172.2x.16.20/22
	30 tagged	172.2x.30.20/24
	40 tagged	172.2x.40.20/24
	50 tagged	172.2x.50.20/24
DISTRIBUIÇÃO-2	10 tagged	172.2x.8.10/21
	20 tagged	172.2x.16.10/22
	30 tagged	172.2x.30.10/24
	40 tagged	172.2x.40.10/24
	50 tagged	172.2x.50.10/24
ACESSO-1	10 tagged	172.2x.8.2/21
	20 tagged	172.2x.16.2/22
	30 tagged	172.2x.30.2/24
	40 tagged	172.2x.40.2/24
	50 tagged	172.2x.50.2/24
ACESSO-2	10 tagged	172.2x.8.1/21
	20 tagged	172.2x.16.1/22
	30 tagged	172.2x.30.1/24
	40 tagged	172.2x.40.1/24
	50 tagged	172.2x.50.1/24

Com estas informações, para realizar as configurações de VLAN dos *switches* Extreme foram utilizados os comandos expostos na Tabela 4.4:

Tabela 4.4: Comandos para configuração de VLAN nos *switches* Extreme

Comando	Descrição
#create vlan "NOME" tag "X"	Cria a VLAN com certo nome e *tag*
#configure vlan "NOME" add ports "X" tagged/untageed	Adiciona a VLAN na porta específica em modo *tagged* ou *untagged*
#configure vlan "NOME" ipaddress "x.x.x.x/x"	Adiciona um endereço IP a VLAN
#enable ipforwarding vlan "NOME"	Habilita o roteamento inter-VLAN

A partir disso, é importante verificar quando deve-se utilizar uma VLAN em *trunk*, ou seja, em modo *tagged*, e quando deve-se utilizar uma VLAN em modo *access*, ou também conhecida como *untagged*. Conforme mencionado anteriormente, as VLANs com *tag*, representados pelo protocolo IEEE 802.1Q adicionam uma identificação ao quadro Ethernet, a fim de enviar diferentes pacotes em uma mesma interface mantendo as VLANs separadas. Já as VLANs *untagged* (sem *tag*), representam as portas do *switch* associadas apenas a uma única VLAN, ou seja, trata-se de uma porta que realiza a conexão direta com um dispositivo final. Dessa maneira, apenas os *switches* de acesso obterão configuração de VLANs *untagged*, já que a conexão de dispositivos finais é realizada nele, diferentemente dos *switches* de agregação e core, no qual possuem, neste caso, apenas portas em modo *trunk*.

Além disso, devido as redundâncias presentes na topologia da Intranet, é necessário habilitar o protocolo STP, do inglês *Spanning Tree Protocol*, para que resolva os problemas de *looping* gerados pelos anéis de ligação que a topologia possui, auxiliando portanto, para uma melhor performance da rede. Sendo assim, a Tabela 4.5 explicita o comando necessário para configurar o STP nos *switches* Extreme-EXOS.

Tabela 4.5: Comando para configuração do protocolo STP nos *switches* Extreme

Comando	Descrição
#configure stpd s0 add "NOME DA VLAN" ports "X"	Habilita STP em uma porta individual de acordo com a VLAN configurada

Por fim, para que as redes configuradas nos *switches* sejam capazes de chegar ao *gateway* correto, neste caso, o *firewall* FortiGate, é necessário realizar a configuração de roteamento estático, de acordo com o comando exposto na Tabela 4.6:

Tabela 4.6: Comando para configuração do roteamento estático nos *switches* Extreme

Comando	Descrição
#configure iproute add default "gateway"	Configura uma rota *default* (0.0.0.0/0) para o *gateway* correto

Com a configuração dos *switches* realizada, é necessário configurar o *firewall* FortiGate. A partir da implementação necessária para este projeto, o *firewall* é tratado no modo "*NAT/Router mode*", onde o FortiGate atuará como *gateway* das redes internas, e será o meio de campo entre a rede LAN dos campus e a rede WAN. É possível verificar esse modo a partir da *dashboard* do *firewall* exposta na Figura 4.10.

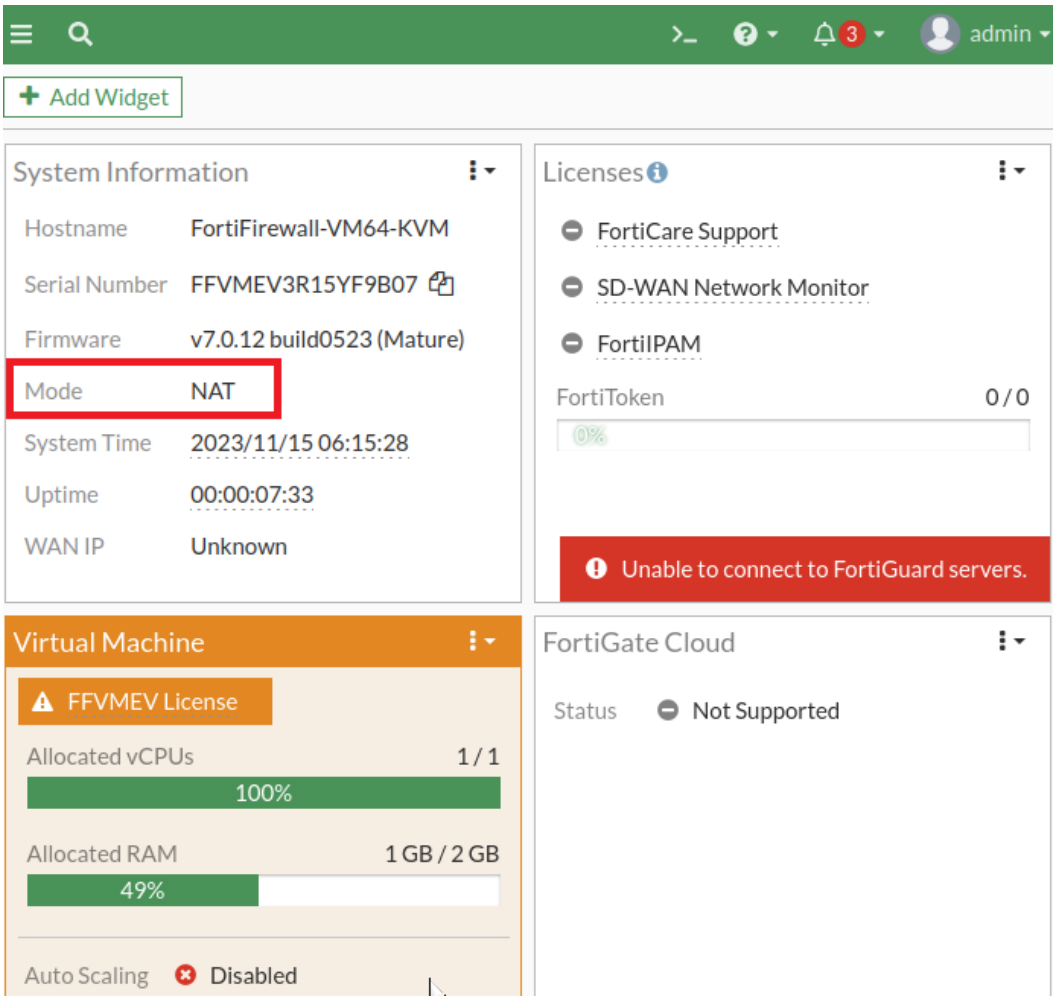


Figura 4.10: Modo NAT no *firewall* FortiGate. Fonte própria.

Além disso, todas as interfaces físicas do FortiGate são tratadas de forma individual, ou seja, cada interface pode possuir seu próprio endereçamento IP ou podem ainda ser combinadas logicamente ou virtualmente. Sendo assim, é necessário realizar a combinação entre duas interfaces do *firewall*, já que existem duas conexões LAN, conforme pode ser observado na Figura 4.9, sendo uma a partir do *switch* Core-1 e outra a partir do *switch* Core-2.

Para isso, é necessário utilizar o modo *Software Switch* da FortiGate a fim de agrupar duas interfaces físicas como se fossem uma só. Além disso, é necessário atrelar cinco interfaces VLANs ao *Software switch*, já que o *firewall* será *gateway* da rede interna de cada campus, e a *intranet*, conforme mencionado anteriormente, é composta por cinco redes, sendo elas: Graduação (VLAN 10), Pós-Graduação (VLAN 20), Professores (VLAN 30), Diretoria (VLAN 40) e Suporte (VLAN 50).

Dessa maneira, cada *firewall* FortiGate deverá obedecer a seguinte configuração: Primeiramente é realizada a configuração do *Software Switch* a fim de agrupar as interfaces físicas vindas dos *switches* Core. Para isso, deve-se selecionar a opção *Network->Interfaces* no menu principal. Assim, a Figura 4.11 demonstra em etapas a criação de uma nova interface do tipo *Software Switch*, onde é necessário inserir um nome, conforme indicado no item 1, no qual foi definido para esse caso como "UPLINK-INTERNO". Em seguida, deve-se selecionar o tipo da interface. Já o item 3 da Figura 4.11 indica que devem ser selecionadas as interfaces membro desse *link*, que nesse caso são as interfaces vindas dos *switches* Core. Deve-se então apontar um endereçamento IP, conforme indicado pelo item 4 da Figura 4.11. E, por fim, é possível realizar acessos administrativos para esse tipo de interface. O item 4.3.4 desta seção irá expor de forma mais detalhada sobre perfis de segurança para cada usuário.

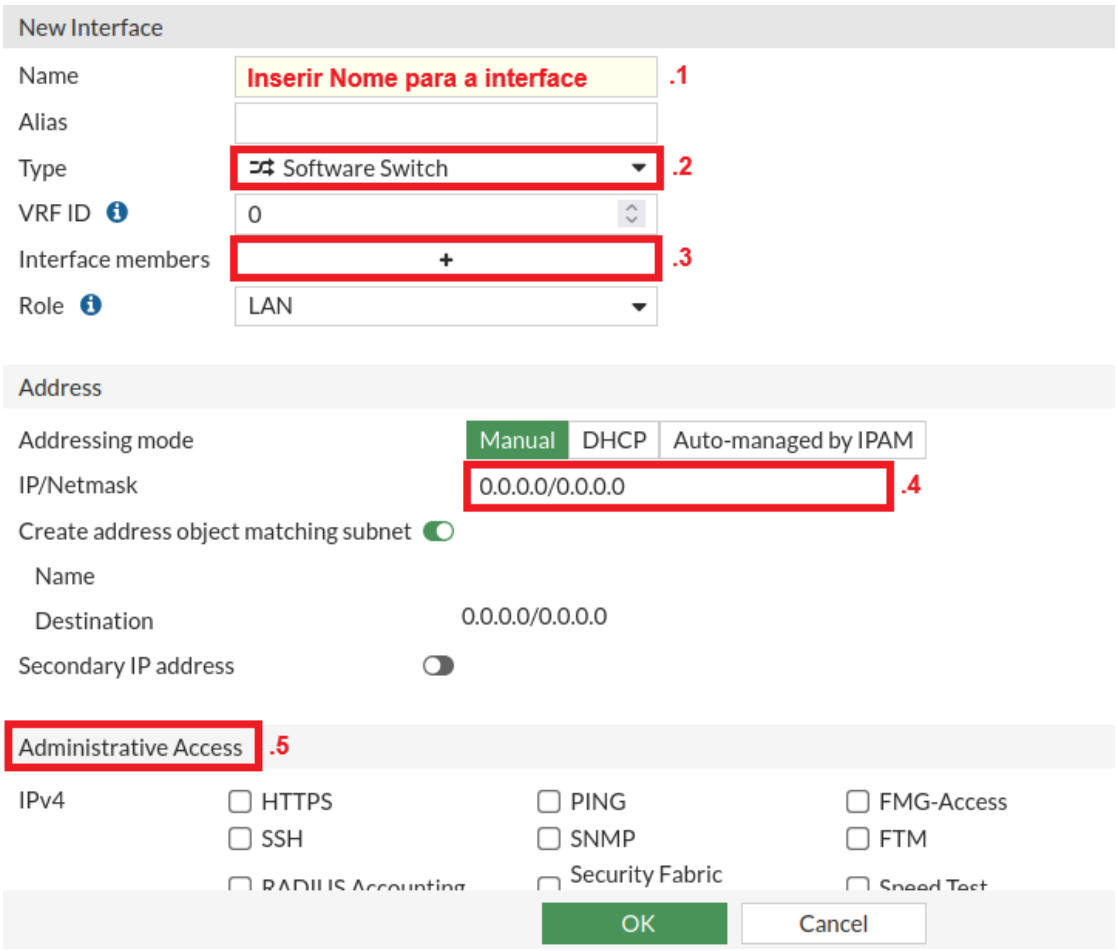


Figura 4.11: Etapas de configuração da interface do tipo *Software Switch*. Fonte própria.

Ao criar a interface "UPLINK-INTERNO" do tipo *Software Switch*, é necessário atrelar interfaces VLAN a esse *link*. Para isso, deve-se criar novas interfaces, cada uma correspondente a uma VLAN da rede interna. Sendo assim, a Figura 4.12 expõe as etapas para a criação desse tipo de interface, onde primeiramente deve-se designar um nome, nesse caso, "VLAN-X", indicando a VLAN correspondente presente na rede interna de cada campus. Em seguida, conforme ilustrado no item 2 desta Figura, deve-se selecionar o tipo "VLAN"para a interface. A partir disso, deve-se

apontar a interface do tipo *Software switch* criada anteriormente, como membro. Por fim, deve-se apontar um endereçamento IP para esse *link*, conforme ilustrado no item 5. Nesse caso, o endereço IP será o *gateway* da VLAN correspondente, conforme indicado na Tabela 4.2.

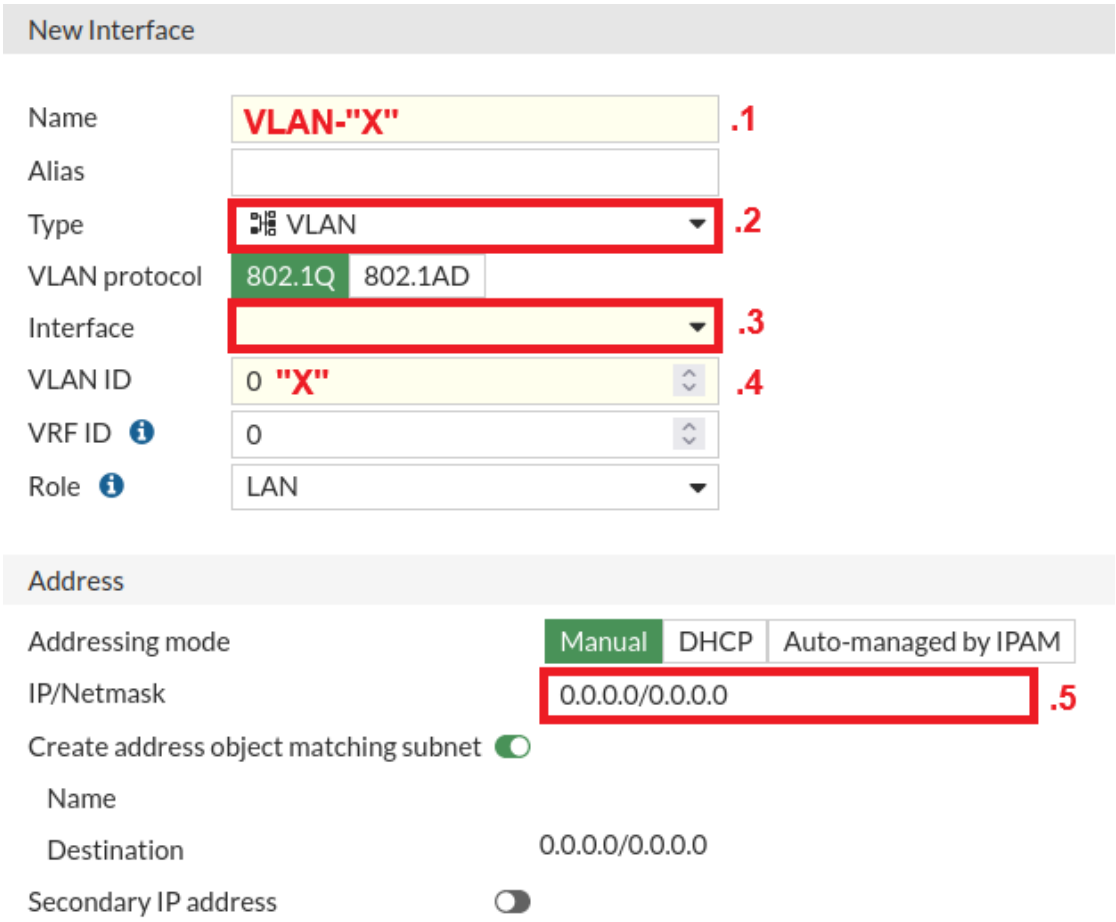


Figura 4.12: Etapas de configuração para as interfaces VLAN correspondentes aos tipos de usuários da rede interna. Fonte própria.

Feita as devidas configurações, a Figura 4.13 exemplifica o resultado dos *links* de *uplink* das redes internas do Campus Darcy Ribeiro. Nesse momento, os usuários presentes na rede interna possuem comunicação com o seu *gateway* correspondente.

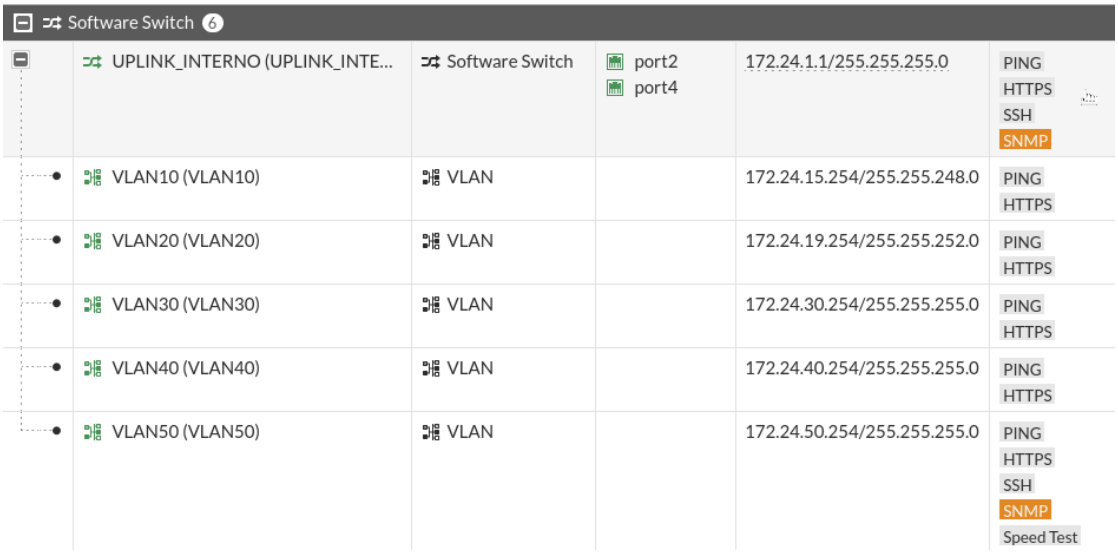


Figura 4.13: Interfaces de *uplink* referente as redes internas do Campus Darcy Ribeiro. Fonte própria.

4.3.4 Implementação dos perfis de segurança

Conforme mencionado anteriormente, o *firewall* é amplamente utilizado visando implementar medidas de segurança visto que nele é possível criar regras de acesso (PINHEIRO, J., 2004) que irão definir quem pode ou não ter a permissão de trafegar entre a rede interna e externa de uma organização. Dessa maneira, é imprescindível analisar todas as medidas de segurança necessárias na implementação de uma infraestrutura de redes de uma organização. Sendo assim, foram analisados e estudados nesse projeto perfis de segurança para cada tipo de usuário presente no Campus da UnB, a fim de que eles tenham acesso apenas a recursos necessários, estabelecendo, portanto, uma espécie de barreira entre serviços permitidos e serviços não autorizados.

Foi considerada a presença de cinco grupos distintos que utilizam a rede da UnB: alunos da graduação, professores, alunos da pós-graduação, diretoria e suporte. Para cada um desses grupos é necessário atribuir regras de segurança no *firewall* de forma a limitar o acesso a serviços, a depender da necessidade, para contribuir assim com a segurança. O *firewall* FortiGate foi configurado com regras de forma a criar uma "*Whitelist*", onde foi especificado uma lista de serviços e aplicações que estão liberados para uso, tudo o que não estiver contido nessa lista será bloqueado, pois cairá na última política de "*Deny All*", que está presente para todos os usuários da rede.

Antes de expor as tabelas que detalham quais serviços/portas foram liberadas para cada um dos grupos de usuários, é pertinente realizar uma explicação pontual de cada um desses serviços.

O DHCP (*Dynamic Host Configuration Protocol*) é um protocolo de rede utilizado para assinalar, de maneira dinâmica, endereços IPs para cada *host* que compõem a rede de uma organização (FORTINET, DHCP, s.d.). Esse protocolo atribui de maneira automática endereços IPs, bem como máscaras de sub-redes, endereços DNS e também outros dados essenciais, que caso fossem atribuídas de maneira manual, iria demandar muito tempo e trabalho, visto que há organizações que irão possuir milhares de dispositivos operantes.

Um protocolo do tipo DHCP possui três componentes: servidor, cliente e *relay*. Um servidor DHCP é o responsável por atribuir endereços IPs, juntamente com outros parâmetros que os dispositivos precisam ter para compor a rede; ele consegue atribuir endereços IPs dinâmicos, retirando-os de um *pool* de endereços disponíveis. Um cliente DHCP trata-se de qualquer dispositivo que se conecta com uma rede em questão, que irá receber as informações enviadas pelo servidor DHCP para que consiga interagir dentro da rede. Já o DHCP *relay* diz respeito às mensagens DHCP que são enviadas entre servidores e clientes, ele atua de forma a permitir que um mesmo servidor DHCP consiga se comunicar de maneira eficaz com todos os dispositivos, estando eles em uma rede primária ou em sub-redes.

Já o protocolo ICMP (*Internet Control Message Protocol*) é um protocolo auxiliar da camada de rede, definido pelo RFC 792, utilizado para transportar mensagens de controle e mensagens de teste entre os equipamentos, além de transmitir relatórios de erros (de nível IP) à origem, mas sem a responsabilidade sobre a correção dos mesmos, conforme (SANTOS, 2016). Estas mensagens ICMP são encapsuladas e transportadas através do datagrama IP, correspondente a camada de rede, como visto na Figura 4.14.

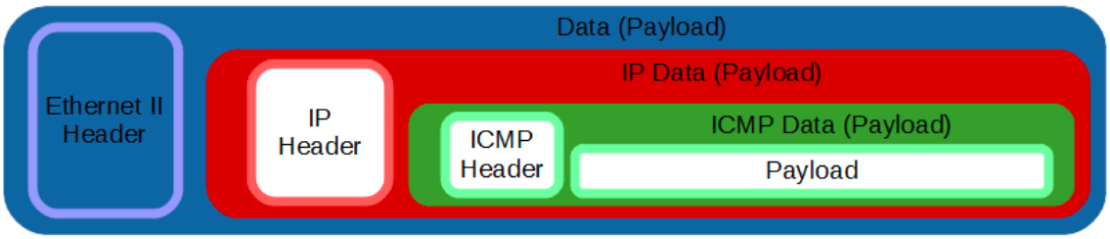


Figura 4.14: Encapsulamento do datagrama IP. Fonte: (BUENO, 2015)

Para realizar um teste de conectividade entre equipamentos (computadores, servidores, *switches*, entre outros dispositivos), o protocolo ICMP possui um utilitário chamado "*ping*", no qual utiliza mensagens do tipo 8 "*echo request*" e tipo 0 "*echo reply*" para verificar a comunicação entre as máquinas, ou seja, a origem envia pacotes do tipo ICMP e "escuta" respostas do destino. Dessa forma, é possível verificar este protocolo com o comando "*ping [endereço IP]*" no *prompt* de comando do Windows, como mostrado na Figura 4.15. Além disso, quando o *sniffer* WireShark estiver habilitado no *link*, será possível fazer uma análise detalhada do pacote partindo da origem ao destino.

O protocolo FTP (*File Transfer Protocol*), do português "Protocolo de Transferência de Arquivo", define as regras que permitem que um usuário em um *host* acesse e transfira arquivos de/para outro *host* em uma rede (DEPTAL, s.d.). E ele funciona com uma arquitetura cliente-servidor, ou seja, possui dois tipos de conexão: a do cliente (computador que realiza o pedido de conexão) e a do servidor (computador que recebe o pedido e fornece o arquivo solicitado). Sendo assim, o servidor FTP permite realizar a transferência de arquivos, possuem um endereço FTP fixo e são dedicados a receber conexões FTP. Eles executam duas tarefas básicas: baixar e enviar (DROPBOX, s.d.). Com isso, quando um usuário envia arquivos para um destino, eles serão transferidos do dispositivo daquele usuário para o servidor FTP. No caso do usuário baixar por determinados arquivos, eles então serão transferidos do servidor para a máquina do usuário.

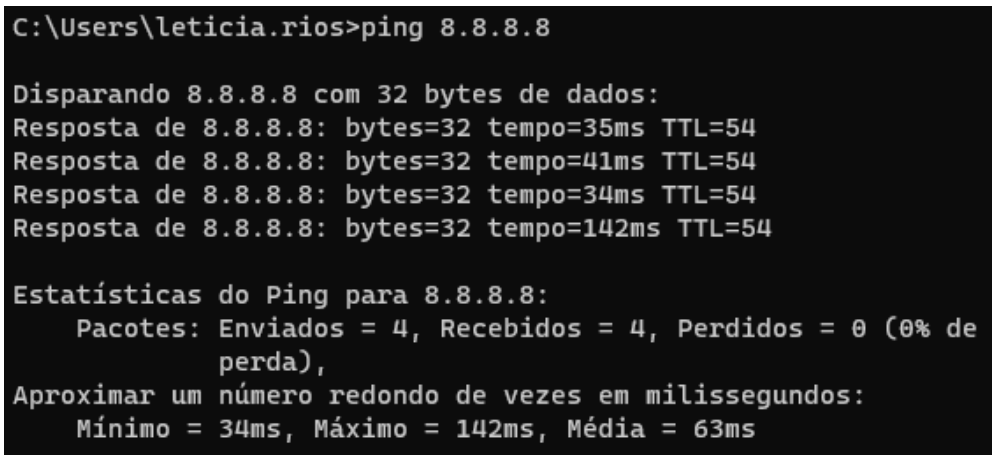


Figura 4.15: Comando *ping* sendo executado no *prompt* de comando do Windows. Fonte própria.

Além disso, o protocolo FTP possui uma entrega de arquivos confiável, por utilizar o TCP para a transmissão dos dados no qual é orientado a conexão, realiza confirmação de recebimentos de pacotes, como também controle de congestionamento e de fluxo.

Já o protocolo DNS (*Domain Name System*), do português "Sistema de Nomes de Domínio", resolve/converte nomes de Internet (www.nome.com) em endereços IP, controlando qual servidor o usuário alcançará quando digitar um nome de domínio no navegador *web*, ou seja, o DNS funciona como uma agenda de telefone, no qual mapeia nomes e números (AWS, s.d.). Além disso, este protocolo utiliza o UDP (melhor esforço) para a transmissão dos dados, na porta padrão 53, no qual, diferentemente do TCP, este protocolo não é confiável, não oferece controle de congestionamento e fluxo, como também não é orientado a conexão.

Sabe-se que a camada de aplicação gera os dados e os prepara para a transmissão, no qual são encaminhados para as camadas mais baixas (encapsulamento), até serem efetivamente enviados pela camada física como sinais (*bits*). Com isso, os protocolos da camada de aplicação atuam juntamente com os protocolos da camada de transporte (camada 4 do modelo TCP/IP) e assim definem como os processos de uma aplicação trocam mensagens entre si.

Desse modo, a camada de transporte é responsável pela transferência de dados fim-a-fim entre dois *hosts*, independentemente da aplicação usada e do tipo, topologia ou configuração das redes físicas existentes entre elas. Sendo assim, os processos de aplicação usam a comunicação lógica fornecida pela camada de transporte para enviar mensagens entre si. O lado remetente da transmissão quebra as mensagens da camada de aplicação em segmentos adicionando um cabeçalho da camada de transporte e os envia para o destino, já o lado destinatário remonta os segmentos em mensagens para a aplicação do usuário (processo de encapsulamento e desmultiplexação). Conforme já mencionado, existem dois tipos de serviços de transporte, sendo orientado a conexão, chamado de TCP ou não orientado a conexão, denominado UDP.

O protocolo UDP (*User Datagram Protocol*) oferece à aplicação solicitante um serviço não confiável, não orientado à conexão, no qual os segmentos UDP podem ser entregues fora de ordem ou perdidos. Sendo assim, a aplicação estará quase "falando" diretamente com o IP, ou seja, não há

nenhum tipo de apresentação (*handshake*) entre as entidades remetente e destinatária da camada de transporte antes de enviar algum segmento. Dessa forma, cada segmento é tratado de forma independente. O UDP, portanto, fornece a função de multiplexação e demultiplexação para passar os dados da camada de rede ao processo em nível de aplicação correto. Além disso, ele oferece uma verificação de erros simples, entretanto, nada é utilizado para recuperar os erros possíveis e nada é adicionado ao IP. Assim, o UDP é muito utilizado em aplicações de multimídia contínua, por ser tolerante a perda e sensível a taxa. No caso da infraestrutura implementada, o UDP será usado para o estabelecimento de comunicações VoIP entre os usuários dos quatro campus.

Dessa maneira, o VoIP, do inglês *Voice over Internet Protocol*, trata-se de um serviço que faz a conversão da voz em sinais digitais, que são transmitidos pela Internet. É uma tecnologia que permite que os usuários façam ligações telefônicas utilizando-se da Internet ao invés de uma linha convencional telefônica (JOHNSON, 2023). Um cenário típico de implementação envolve um roteador no qual possui telefones conectados a ele, e que utilizam a Internet do serviço provedor para transmitir sinais. A Figura 4.16 traz um esquemático do seu funcionamento. Grandes empresas ou instituições que possuem filiais geograficamente separadas preferem o uso dessa tecnologia para o estabelecimento de comunicação de voz entre seus funcionários.

Figura 4.16: Funcionamento do VoIP. Fonte: (JOHNSON, 2023). Traduzida

O "*Email Access*"trata-se de um serviço padrão do *firewall* FortiGate que, quando ativado, permite o acesso a serviços de e-mail pelos usuários. Este serviço oferece o acesso aos seguintes protocolos: DNS, IMAP, IMAPS, POP3, SMTP e SMTPS. É importante mencionar que o sistema de e-mail consiste no trabalho de dois servidores distintos. No qual, um deles será responsável pelo envio do e-mail, já o outro deverá ser responsável pelo recebimento deste e-mail, ou seja, ele baixará as mensagens enviadas pelo servidor de saída para a sua máquina, *smartphone* ou *tablet*.

Primeiramente, o SMTP (*Simple Mail Transfer Protocol*) se refere ao protocolo de envio, ou seja, ele será o servidor de saída, no qual enviará as mensagens ao cliente. Dessa maneira, este padrão é utilizado na transferência de emails pela Internet. Além disso, ele é compatível com as grandes plataformas, como o Gmail, Hotmail e Outlook. Já o SMTPS (*Simples Mail Transfer*

Protocol Secure) é um método utilizado para proteger o SMTP a partir do fornecimento de autenticação SSL (*Secure Sockets Layer*) ou TLS (*Transport Layer Security*) para o estabelecimento de uma conexão segura, garantindo, portanto integridade e confidencialidade dos dados.

Além do protocolo de envio, é necessário outro protocolo, como por exemplo o POP3 (*Post Office Protocol*) e IMAP (*Internet Message Access Protocol*), no qual atuará como servidor de entrada, ou seja, o padrão utilizado receberá as mensagens do servidor de saída, completando assim, a transferência da mensagem eletrônica.

A diferenciação entre os protocolos POP3 e IMAP se refere na capacidade de sincronização de informações com o servidor de saída. O IMAP permite que o usuário sempre consiga ter acesso aos seus e-mails, independente de onde está realizando a requisição para visualizá-los (GASPAR, 2022). Sendo assim, caso o usuário marque uma mensagem como lida em algum dispositivo, automaticamente outros dispositivos que utilizam o IMAP, também serão sincronizados com essa informação. Já o POP3, apenas baixa as mensagens e as remove do servidor, não possuindo a capacidade de sincronização de informações.

Outro serviço importante é referente ao protocolo HTTP (*Hypertext Transfer Protocol*) que faz parte da camada de aplicação da arquitetura TCP/IP definido no RFC 1945 e RFC 2616 e permite a obtenção de recursos, como por exemplo, o documento HTML do site visitado. É modelado como um protocolo cliente-servidor, no qual o cliente solicita uma requisição, utilizando o endereço URL, o navegador portanto envia as solicitações utilizando mensagens HTTP. Dessa forma, o servidor recebe a solicitação e envia os arquivos associados (SOUZA, 2019). Além disso, este protocolo é definido como “sem estado”, onde o servidor não mantém informações sobre as requisições dos clientes. O protocolo HTTP não oferece nenhum tipo de segurança por ser capaz de enviar qualquer tipo de informação de aplicações *Web* sem criptografia, sendo preferível e recomendável a utilização do HTTPS.

O HTTPS trata-se do próprio protocolo HTTP quando há a utilização de criptografia TLS/SSL, onde faz-se o uso de uma "infraestrutura assimétrica de chaves públicas"(*asymmetric public key infrastructure*) onde há a presença de uma chave privada (controlada pelo servidor) e uma chave pública (disponível para usuários), que irá assegurar que haja um tipo de autenticação antes de se iniciar uma transferência de dados (AWATI, 2022). Dessa maneira, o HTTPS garante que toda a comunicação estabelecida entre o lado cliente e o lado servidor ocorra de maneira criptografada e segura.

Já o *traceroute* trata-se de uma ferramenta de linha de comando que, ao ser utilizada, oferece dados específicos de qual o caminho percorrido por um pacote IP dentro de uma rede ou entre redes diferentes, quando uma requisição percorre o caminho entre o dispositivo de origem e o dispositivo de destino. Essa ferramenta é primariamente utilizada para diagnosticar a saúde de uma infraestrutura de redes, verificando como o tráfego está sendo direcionado para que, caso seja necessário, alterações nas configurações sejam realizadas para que a rede esteja funcionando dentro do esperado.

O serviço "*Tracert*"foi ativado temporariamente nos perfis de usuários para que fosse possível realizar os testes de conectividade, na infraestrutura de redes criada, que serão expostos no capítulo

5 desse projeto. Sendo assim, trata-se de um serviço que não estará contido na lista de serviços liberados para os usuários. Em um primeiro momento o usuário pode executar o comando "*traceroute [ip de destino]*"ou ainda "*traceroute [nome de domínio de destino]*", caso o usuário informe um nome de domínio, o próprio *traceroute* irá encontrar e encaminhar dados para o endereço IP correspondente.

Para exemplificar o funcionamento do *Traceroute*, tomemos como exemplo a infraestrutura explicitada na Figura 4.17 abaixo, onde o dispositivo de origem, de endereço IP 1.1.1.1 está em uma sub-rede diferente do dispositivo de destino, de endereço IP 2.2.2.2, por 4 roteadores diferentes. A ferramenta *traceroute* exibirá ao usuário qual o caminho que os pacotes estão percorrendo.

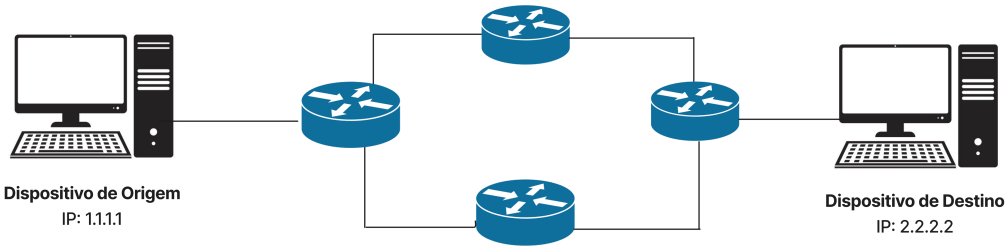


Figura 4.17: Infraestrutura para exemplificação do comando "*traceroute*". Fonte própria.

Após a execução do comando do *traceroute* no dispositivo de origem, ele irá enviar pacotes de dados em direção ao destino com um TTL setado em "1". Porém, após chegar ao primeiro ativo de rede, esse TTL é setado para "0", fazendo com que um pacote de "*TTL exceeded*"seja retornado ao dispositivo de origem, de forma que ele registre então o endereço IP do primeiro dispositivo que o pacote alcançou. A Figura 4.18 mostra uma versão simplificada de um pacote IP, somente com informações de endereço de origem, endereço de destino e valor do TTL. É possível observar que, após ter seu valor setado para "0", o pacote retorna ao dispositivo de origem.

Em seguida, tendo as informações do 1º *Hop*, o *traceroute* irá enviar um novo pacote com destino ao dispositivo final, porém agora com um TTL setado para "2". Após passar pelo primeiro dispositivo, o TTL é setado para "1"e, somente após passar pelo segundo dispositivo, o TTL é setado para "0", fazendo assim com que um pacote de "*TTL exceeded*"seja enviado de volta para o dispositivo de origem, sendo possível registrar qual o endereço desse ativo da rede em que o TTL foi setado para "0". A Figura 4.19 exibe qual o caminho percorrido por esse pacote, no caso da infraestrutura de rede utilizada como exemplo.

Novamente, tendo as informações do 2º *Hop*, o *traceroute* irá enviar um novo pacote com destino ao dispositivo final, porém agora com um TTL setado para "3". Após passar pelo primeiro dispositivo, o TTL é setado para "2"e, após passar pelo segundo dispositivo, o TTL é setado para "1"e somente após passar pelo terceiro dispositivo que o TTL é setado para "0", fazendo assim com que um pacote de "*TTL exceeded*"seja enviado de volta para o dispositivo de origem, sendo

possível registrar qual o endereço desse ativo da rede em que o TTL foi setado para "0". A Figura 4.20 mostra qual o caminho percorrido por esse pacote.

Por fim, tendo as informações do 3º *Hop*, o *traceroute* irá enviar um novo pacote com destino ao dispositivo final, porém agora com um TTL setado para "4". Após passar pelo primeiro dispositivo, o TTL é setado para "3", após passar pelo segundo dispositivo, o TTL é setado para "2", , após passar pelo terceiro dispositivo o TTL é setado para "1"e somente após passar pelo quarto dispositivo que o TTL é setado para "0", fazendo assim com que um pacote de "*TTL exceeded*"seja enviado de volta para o dispositivo de origem, sendo possível registrar qual o endereço desse ativo da rede em que o TTL foi setado para "0". Coincidentemente, no caso da infraestrutura de exemplo, o quarto dispositivo em que o pacote percorre se trata do dispositivo de destino, por essa razão o *traceroute* irá armazenar essa mensagem com todas as outras mensagens geradas nos "*Hops*"anteriores, juntamente com a quantidade de tempo que demorou para que o pacote chegasse e retornasse do dispositivo (valor que será armazenado na variável "*Round Trip Time*"). E então, irá exibir para o usuário um resumo com todos os saltos que o pacote percorreu para alcançar o destino final. A Figura 4.21 expõe qual foi o caminho percorrido por esse pacote.

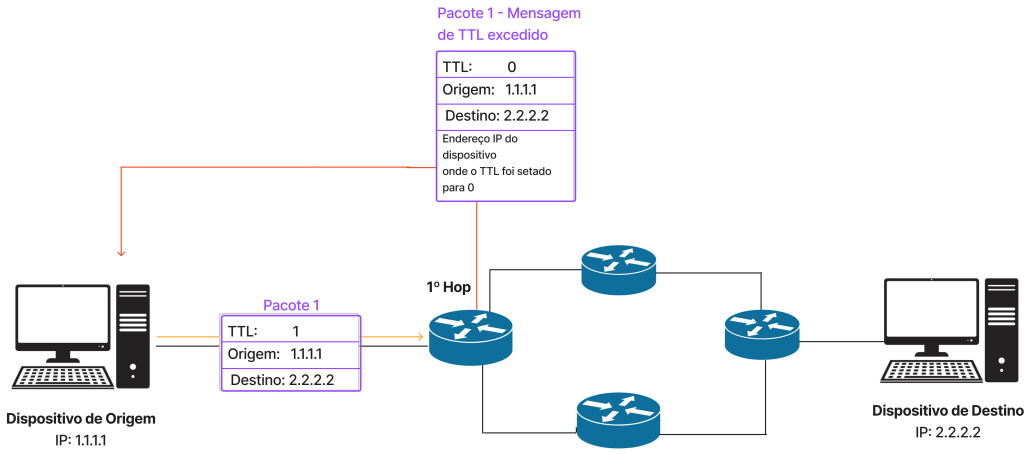


Figura 4.18: Exemplificação do funcionamento do comando "*traceroute*"(Parte 1). Fonte própria.

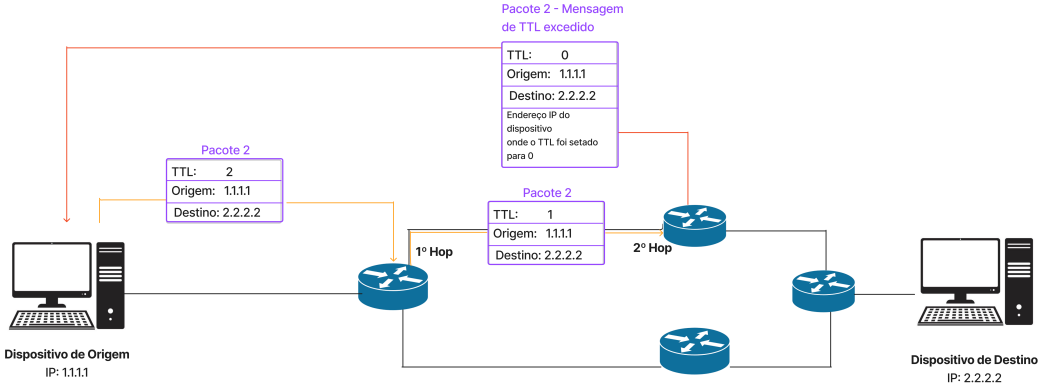


Figura 4.19: Exemplificação do funcionamento do comando "*traceroute*"(Parte 2). Fonte própria.

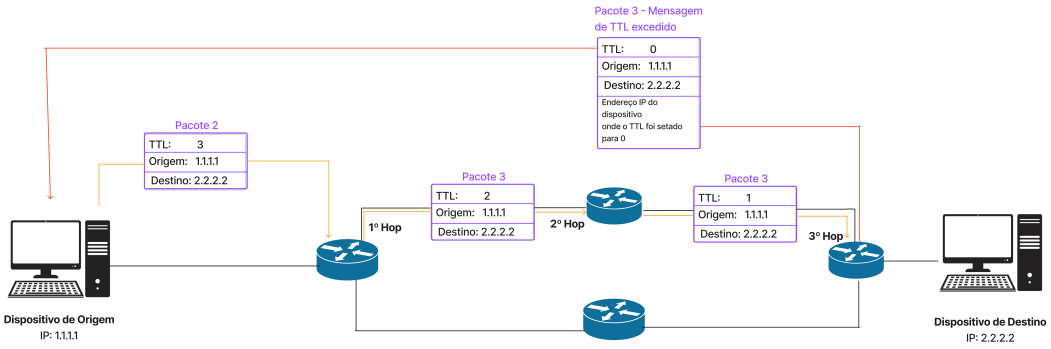


Figura 4.20: Exemplificação do funcionamento do comando "*traceroute*"(Parte 3). Fonte própria.

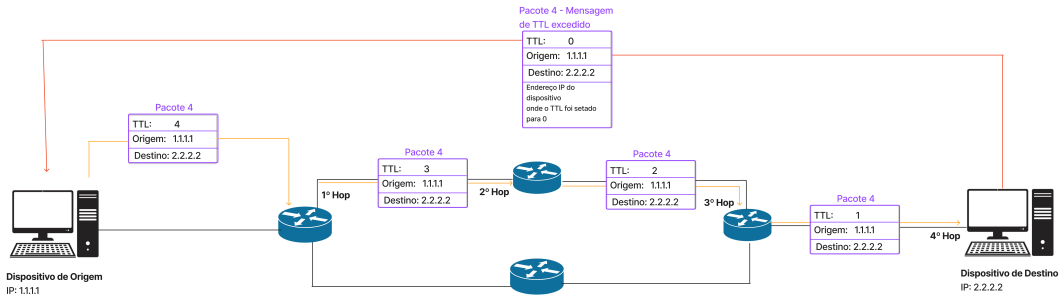


Figura 4.21: Exemplificação do funcionamento do comando "*traceroute*"(Parte 4). Fonte própria.

A partir da compreensão do funcionamento deste serviço, a Figura 4.22 mostra um exemplo realizado pelo terminal de comando onde, após a execução do *traceroute*, é printado todos os endereços IPs em que o pacote IP percorreu até chegar ao destino final, juntamente com o tempo em milissegundos que foi necessário para alcançar cada salto. É importante ainda mencionar que o *traceroute* consegue rastrear endereços que não excedam 30 *Hops* de distância.

```
C:\Users>tracert -d www.google.com

Tracing route to www.google.com [216.58.222.4]
over a maximum of 30 hops:

  1     1 ms     4 ms     1 ms  10.0.0.1
  2     4 ms     5 ms     3 ms  192.168.0.1
  3    10 ms    10 ms    10 ms  10.36.0.1
  4    13 ms    11 ms    10 ms  191.183.237.1
  5    13 ms    12 ms    16 ms  191.183.233.13
  6    31 ms    41 ms    56 ms  74.125.119.46
  7    16 ms    26 ms    15 ms  108.170.226.233
  8    15 ms    16 ms    11 ms  142.251.76.113
  9    25 ms    12 ms    27 ms  216.58.222.4

Trace complete.
```

Figura 4.22: Exemplo da execução do comando "*traceroute*"para o endereço www.google.com. Fonte própria.

Sendo assim, tendo como base o conhecimento de todos os serviços e protocolos acima citados, as tabelas abaixo (4.7, 4.8, 4.9, 4.10 e 4.11) apresentadas mostrarão quais serviços foram habilitados para cada grupo de usuário, tanto quando há uma requisição realizada com destino à rede externa, mas também quando essa requisição é direcionada para alguém que compõe os outros quatro grupos de usuários.

Tabela 4.7: Serviços e Portas liberadas para usuários da Graduação.

Origem	Destino	Serviço	Porta
GRADUAÇÃO	PROFESSORES	ICMP (UDP/TCP)	–
GRADUAÇÃO	PÓS-GRADUAÇÃO	ICMP (UDP/TCP)	–
GRADUAÇÃO	DIRETORIA	ICMP (UDP/TCP)	–
GRADUAÇÃO	PROFESSORES	FTP/VOIP	5001
GRADUAÇÃO	PÓS-GRADUAÇÃO	FTP/VOIP	5001
GRADUAÇÃO	DIRETORIA	FTP/VOIP	5001
GRADUAÇÃO	PROFESSORES	*Tracert*	–
GRADUAÇÃO	PÓS-GRADUAÇÃO	*Tracert*	–
GRADUAÇÃO	DIRETORIA	*Tracert*	–
GRADUAÇÃO	all	DNS	53
GRADUAÇÃO	all	HTTP	80
GRADUAÇÃO	all	HTTPS	443
GRADUAÇÃO	all	DHCP	67-68
GRADUAÇÃO	all	*Email Access*	–

Tabela 4.8: Serviços e Portas liberadas para os usuários que compõem o grupo de Professores.

Origem	Destino	Serviço	Porta
PROFESSORES	GRADUAÇÃO	ICMP (UDP/TCP)	–
PROFESSORES	PÓS-GRADUAÇÃO	ICMP (UDP/TCP)	–
PROFESSORES	DIRETORIA	ICMP (UDP/TCP)	–
PROFESSORES	GRADUAÇÃO	FTP/VOIP	5001
PROFESSORES	PÓS-GRADUAÇÃO	FTP/VOIP	5001
PROFESSORES	DIRETORIA	FTP/VOIP	5001
PROFESSORES	GRADUAÇÃO	*Tracert*	–
PROFESSORES	PÓS-GRADUAÇÃO	*Tracert*	–
PROFESSORES	DIRETORIA	*Tracert*	–
PROFESSORES	all	DNS	53
PROFESSORES	all	HTTP	80
PROFESSORES	all	HTTPS	443
PROFESSORES	all	DHCP	67-68
PROFESSORES	all	*Email Access*	–

Tabela 4.9: Serviços e Portas liberadas para usuários da Pós-Graduação.

Origem	Destino	Serviço	Porta
PÓS-GRADUAÇÃO	PROFESSORES	ICMP (UDP/TCP)	–
PÓS-GRADUAÇÃO	GRADUAÇÃO	ICMP (UDP/TCP)	–
PÓS-GRADUAÇÃO	DIRETORIA	ICMP (UDP/TCP)	–
PÓS-GRADUAÇÃO	GRADUAÇÃO	FTP/VOIP	5001
PÓS-GRADUAÇÃO	PROFESSORES	FTP/VOIP	5001
PÓS-GRADUAÇÃO	DIRETORIA	FTP/VOIP	5001
PÓS-GRADUAÇÃO	PROFESSORES	*Tracert*	–
PÓS-GRADUAÇÃO	GRADUAÇÃO	*Tracert*	–
PÓS-GRADUAÇÃO	DIRETORIA	*Tracert*	–
PÓS-GRADUAÇÃO	all	DNS	53
PÓS-GRADUAÇÃO	all	HTTP	80
PÓS-GRADUAÇÃO	all	HTTPS	443
PÓS-GRADUAÇÃO	all	DHCP	67-68
PÓS-GRADUAÇÃO	all	*Email Access*	–

Tabela 4.10: Serviços e Portas liberadas para usuários da Diretoria.

Origem	Destino	Serviço	Porta
DIRETORIA	PROFESSORES	ICMP (UDP/TCP)	–
DIRETORIA	GRADUAÇÃO	ICMP (UDP/TCP)	–
DIRETORIA	PÓS-GRADUAÇÃO	ICMP (UDP/TCP)	–
DIRETORIA	GRADUAÇÃO	FTP/VOIP	5001
DIRETORIA	PROFESSORES	FTP/VOIP	5001
DIRETORIA	PÓS-GRADUAÇÃO	FTP/VOIP	5001
DIRETORIA	PROFESSORES	*Tracert*	–
DIRETORIA	GRADUAÇÃO	*Tracert*	–
DIRETORIA	PÓS-GRADUAÇÃO	*Tracert*	–
DIRETORIA	all	DNS	53
DIRETORIA	all	HTTP	80
DIRETORIA	all	HTTPS	443
DIRETORIA	all	DHCP	67-68
DIRETORIA	all	*Email Access*	–

Por fim, o grupo de usuários pertencente ao Suporte terá acesso a todos os serviços, usuários e portas, conforme identificado na Tabela 4.11. Isso porque trata-se de um grupo de usuários que atuarão na administração e gerenciamento da rede da Universidade, onde terão acesso aos equipamentos, podendo realizar implementações de novas configurações, manutenção da rede, entre outros serviços. Por serem gerentes da rede, poderão ter acesso em tempo real à saúde da infra-

estrutura, por meio de relatórios e *softwares* de monitoramento, podendo realizar intervenções ao detectarem anomalias na rede, como possível queda de *link*, tentativa de invasão, dentre outros.

Tabela 4.11: Serviços e Portas liberadas para usuários do Suporte.

Origem	Destino	Serviço	Porta
SUPORTE	all	all	all

4.3.5 Implementação *Backbone* Externo

O *Backbone* externo, conforme pode ser observado na Figura 4.23, é composto por quatro roteadores Cisco 7200 e 2 *clouds* que dão acesso à Internet e ao ambiente remoto do Laboratório de Redes da UnB, sendo que os roteadores R1 e R4 são definidos como sendo dispositivos de borda da provedora, do inglês *Provider Edges* (PE). Já os roteadores R2 e R3 são os dispositivos da provedora, do inglês *Provider Router* (P). Além disso, interligados aos PEs estão os *firewalls* FortiGate de cada campus da UnB, também definidos, do ponto de vista do *backbone*, como dispositivos de borda do cliente, do inglês *Customer Edge* (CE).

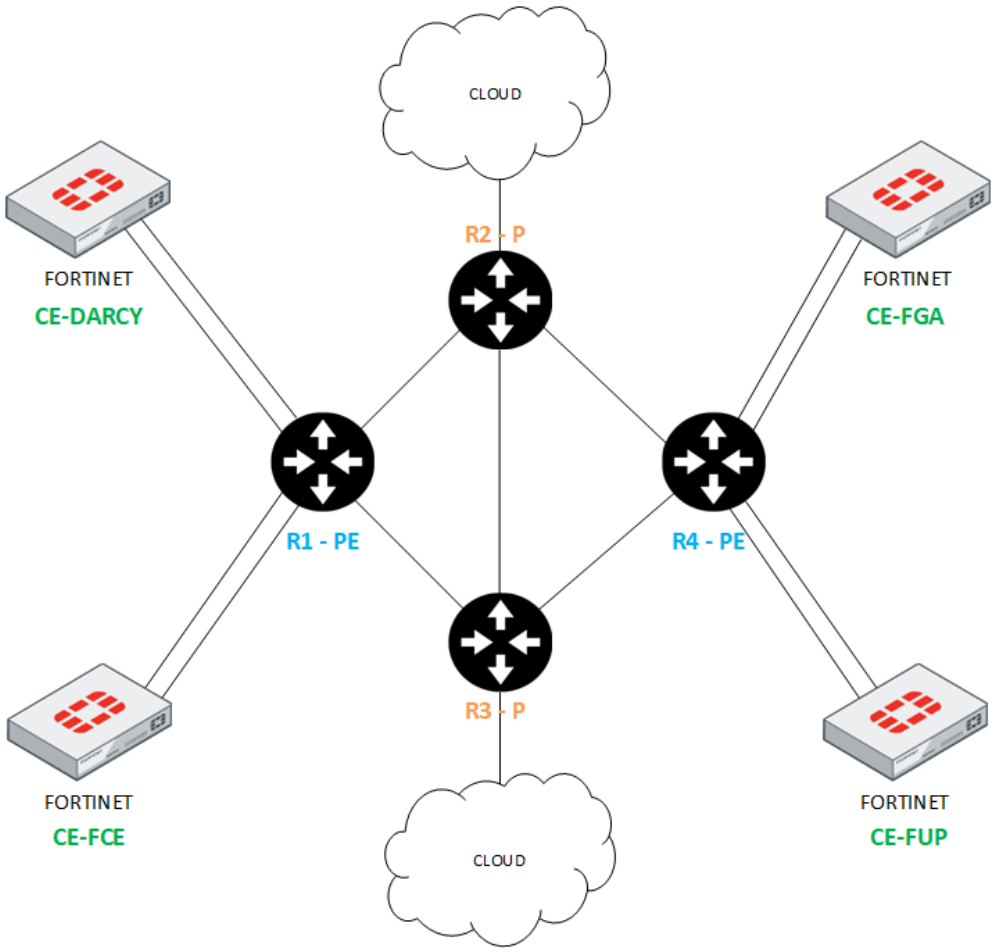


Figura 4.23: Infraestrutura do *Backbone* da provedora. Fonte própria.

A partir disso, o *Backbone* foi configurado para obter maior disponibilidade e redundância dos

links. Assim, a Tabela 4.12 a seguir descreve os parâmetros de configuração de endereçamento IP dos roteadores nesta topologia.

Tabela 4.12: Parâmetros de configuração IP dos roteadores do Backbone.

Dispositivo	**Interface**	**Endereço IP**	**Máscara de sub-rede**
R1	Gig 1/0	10.0.0.2	/30
	Gig 2/0	10.0.0.9	/30
	Gig 3/0	10.0.0.13	/30
	Gig 4/0	10.0.0.6	/30
	Gig 5/0	10.0.0.38	/30
	Gig 6/0	10.0.0.41	/30
R2	Gig 1/0	10.0.0.10	/30
	Gig 2/0	10.0.0.21	/30
	Gig 3/0	10.0.0.17	/30
	Gig 4/0	dhcp	dhcp
R3	Gig 1/0	10.0.0.14	/30
	Gig 2/0	10.0.0.25	/30
	Gig 3/0	10.0.0.18	/30
	Gig 4/0	dhcp	dhcp
R4	Gig 1/0	10.0.0.22	/30
	Gig 2/0	10.0.0.26	/30
	Gig 3/0	10.0.0.29	/30
	Gig 4/0	10.0.0.33	/30
	Gig 5/0	10.0.0.45	/30
	Gig 6/0	10.0.0.49	/30

A partir dessas informações, o *Backbone* desse projeto foi configurado utilizando a tecnologia L3VPN, no qual uma VPN aplica o protocolo BGP para enviar e receber pacotes VPN, esse funcionamento se dá através do *peering* entre o cliente (CE) e o roteador de borda da provedora (PE). Além disso, utiliza técnicas de roteamento e encaminhamento virtual (VRF) para realizar e segregar a comunicação do cliente dentro do *backbone* de maneira transparente. A tecnologia L3VPN funciona sobre uma rede MPLS a fim de obter alta disponibilidade e resiliência, garantindo a comunicação do cliente entre diversos pontos da malha MPLS (PEDRO, 2021).

Dessa maneira, a Figura 4.24 abaixo exemplifica o diagrama de rede esquemático desse projeto para a utilização da tecnologia MPLS L3VPN.

A partir dos dados descritos e do diagrama exposto, a configuração do *backbone* é iniciada pela definição dos endereçamentos IPs das interfaces dos roteadores. Sendo assim, a Tabela 4.13 aponta os comandos necessários para essa configuração.

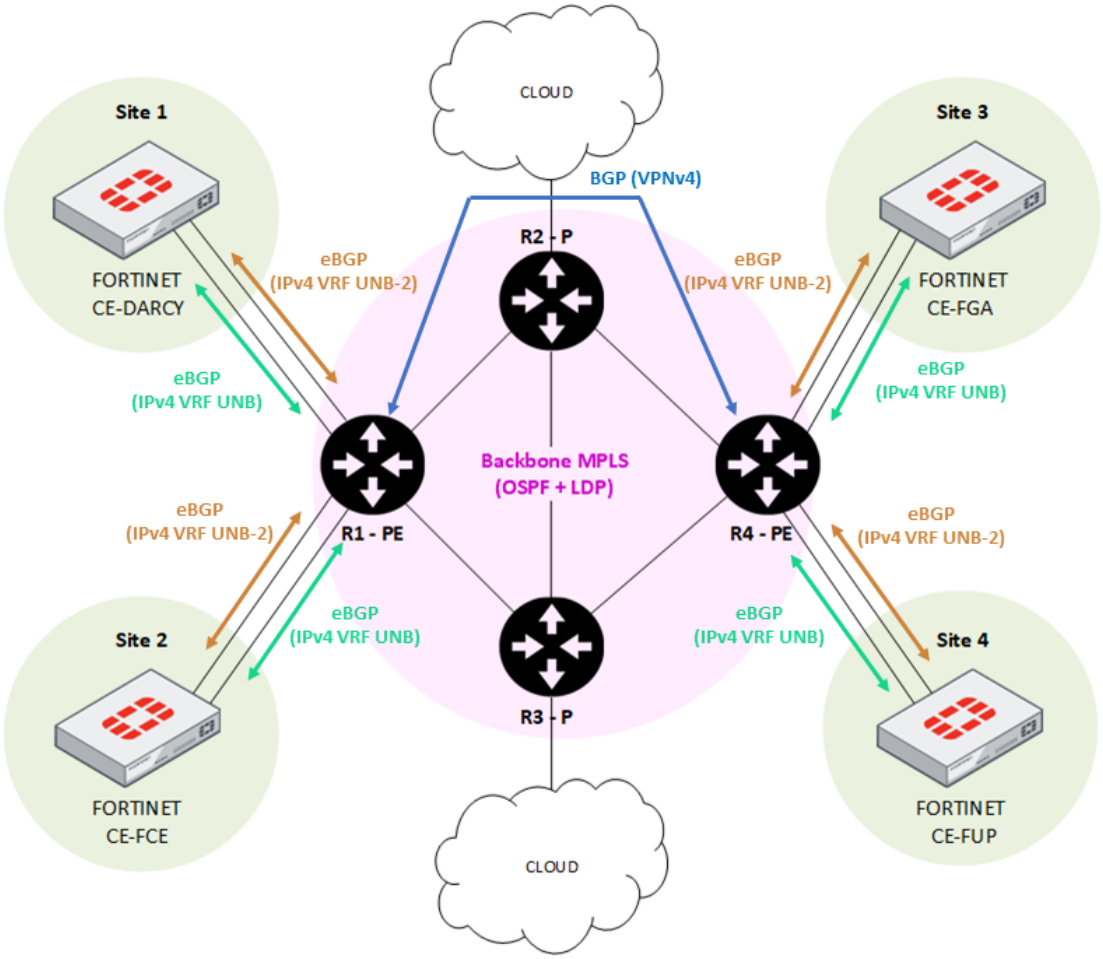


Figura 4.24: Diagrama de redes para a utilização da tecnologia MPLS L3VPN. Fonte própria.

Tabela 4.13: Comandos para configuração das interfaces dos roteadores Cisco.

Comando	Descrição
#interface GigabitEthernet X/0 *ou* *#interface Loopback0*	Entra no modo de configuração da interface Gigabit Ethernet ou Loopback
#ip address "x.x.x.x" "x.x.x.x"	Insere um endereço IP com uma máscara de sub-rede específica para aquela interface
#no shutdown	Liga a interface

Após a configuração das interfaces dos roteadores, deve-se configurar a rede MPLS. Para isso, é necessário que os roteadores do *backbone* sejam capazes de realizar roteamento entre eles, nesse caso, será utilizado o protocolo de roteamento dinâmico OSPF. Além disso, juntamente com o OSPF, o protocolo LDP será o responsável por gerar e distribuir *labels* entre os roteadores. Os comandos de configuração dessa etapa podem ser visualizados na Tabela 4.14.

Tabela 4.14: Comandos para configuração de OSPF e MPLS no *backbone*.

Comando	Descrição
#router ospf "id process"	Entra no modo de configuração OSPF do processo "x"
#router-id "interface loopback"	Define o identificador do roteador como sendo o endereço de *loopback*
#mpls ldp autoconfig	Habilita o LDP automaticamente nas interfaces que possuem configuração OSPF
#network "x.x.x.x" "x.x.x.x" area "x"	Anuncia o endereço de rede diretamente conectado ao roteador de acordo com a área pertencente

Neste momento, obtém-se uma rede MPLS funcional no *backbone* (MPLS - OSPF - LDP). Em seguida, deve-se configurar duas VRFs para os clientes nos roteadores de borda da provedora (PEs), chamadas de UNB e UNB-2, uma para cada *link* diretamente conectado aos *firewalls*, a fim de obter redundância entre um campus e outro da UnB, além de segregar a comunicação do cliente dentro do *backbone* de maneira transparente. Os comandos de configuração dessa etapa podem ser visualizados na Tabela 4.15.

Tabela 4.15: Comando para configuração das VRFs nos roteadores PEs

Comando	Descrição
#vrf definition "NOME"	Cria uma VRF com um "NOME"
#rd "x:x"	Identificação da VRF (*Route Distinguisher*) a fim de distinguir as rotas entre VRFs diferentes
#address-family ipv4	Recurso para especificar a VRF
#route-target both "x:x"	Define o que será importado e exportado da/para VRF
#interface GigabitEthernet "X/0"	Entra no modo de configuração da interface GigabitEthernet "X/0"
#vrf forwarding "NOME"	Associar à interface física sua respectiva VRF
#ip address "x.x.x.x" "x.x.x.x"	Após o comando anterior, o IP configurado é descartado, assim é necessário configurar novamente o IP da interface

Em seguida, é necessário configurar os dispositivos clientes (CE) conectados aos PEs, que nesse caso são os *firewalls* FortiGate presentes em cada campus. É importante mencionar que os clientes não possuem ciência da existência das VRFs e do MPLS.

Para isso, basta acessar a interface *Web* de cada *firewall* e selecionar a opção *Network->Interfaces* no menu principal. Nesse momento, deve-se selecionar a interface WAN que está diretamente conectada aos dispositivos de borda da provedora, e assim selecionar a opção "*Edit*". Dessa maneira, a Figura 4.25 ilustra as etapas de configuração da interface no *firewall* FortiGate, no qual primeiramente deve-se nomear a interface, nesse caso, foi chamada de MPLS-1 como sendo o primeiro

link conectado ao *backbone*, dessa forma, o segundo *link* que irá prover redundância será chamado de MPLS-2. Em seguida, conforme enumerado na Figura 4.25, deve-se definir a interface como do tipo WAN, já que ela está conectada aos dispositivos provedores de Internet. Por fim, na etapa 3, o endereçamento IP é configurado, sendo que deve obedecer a sub-rede presente no roteador da provedora, conforme especificado na Tabela 4.12.

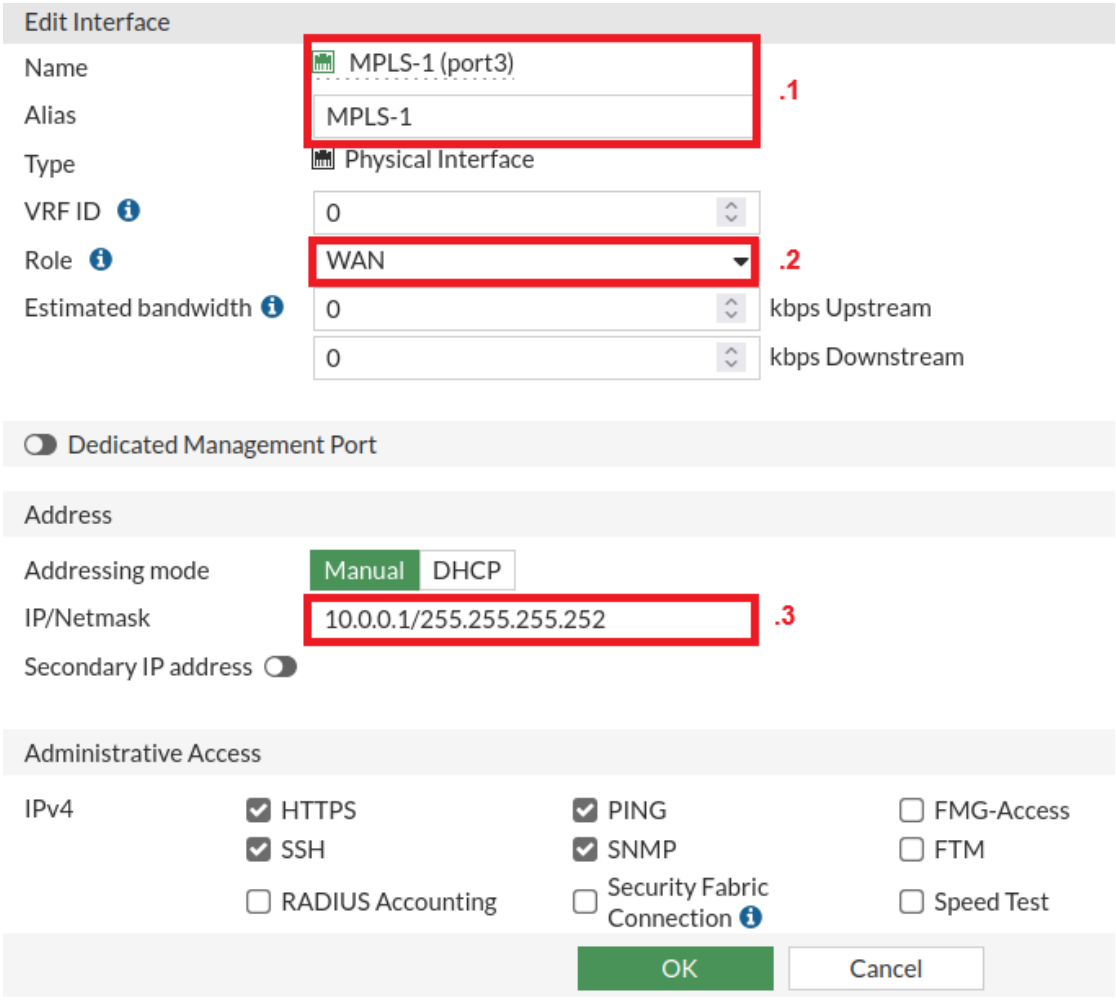


Figura 4.25: Configuração das interfaces físicas conectados ao backbone, no *firewall* FortiGate. Fonte própria.

Feita as devidas configurações em cada campus da UnB, o próximo passo é a configuração do roteamento entre os clientes CEs e os roteadores PEs. Nesse projeto, conforme mencionado anteriormente, o protocolo de roteamento dinâmico eBGP foi utilizado para obter a conectividade entre os roteadores de borda da operadora e os dispositivos clientes, sendo assim, o eBGP é utilizado para anunciar as rotas VPNs.

Dessa maneira, antes de iniciar a configuração do protocolo de roteamento, deve-se tomar conhecimento sobre os sistemas autônomos presentes na topologia. Os ASs se referem a uma grande rede ou grupo de redes que possuem uma política unificada de roteamento. Com isso, a arquitetura desse projeto contém 5 sistemas autônomos, sendo 4 deles presentes em cada campus da UnB, sendo o pólo Darcy Ribeiro com a AS 65011; FCE com a AS 65012; FGA com a AS

65013, e por fim, a FUP com a AS 65014. Além disso, o *backbone*, que interliga os campus e os conecta com a Internet, possui o AS com ID 100. A Figura 4.26 apresenta de maneira ilustrativa os ASs presentes na topologia em questão.

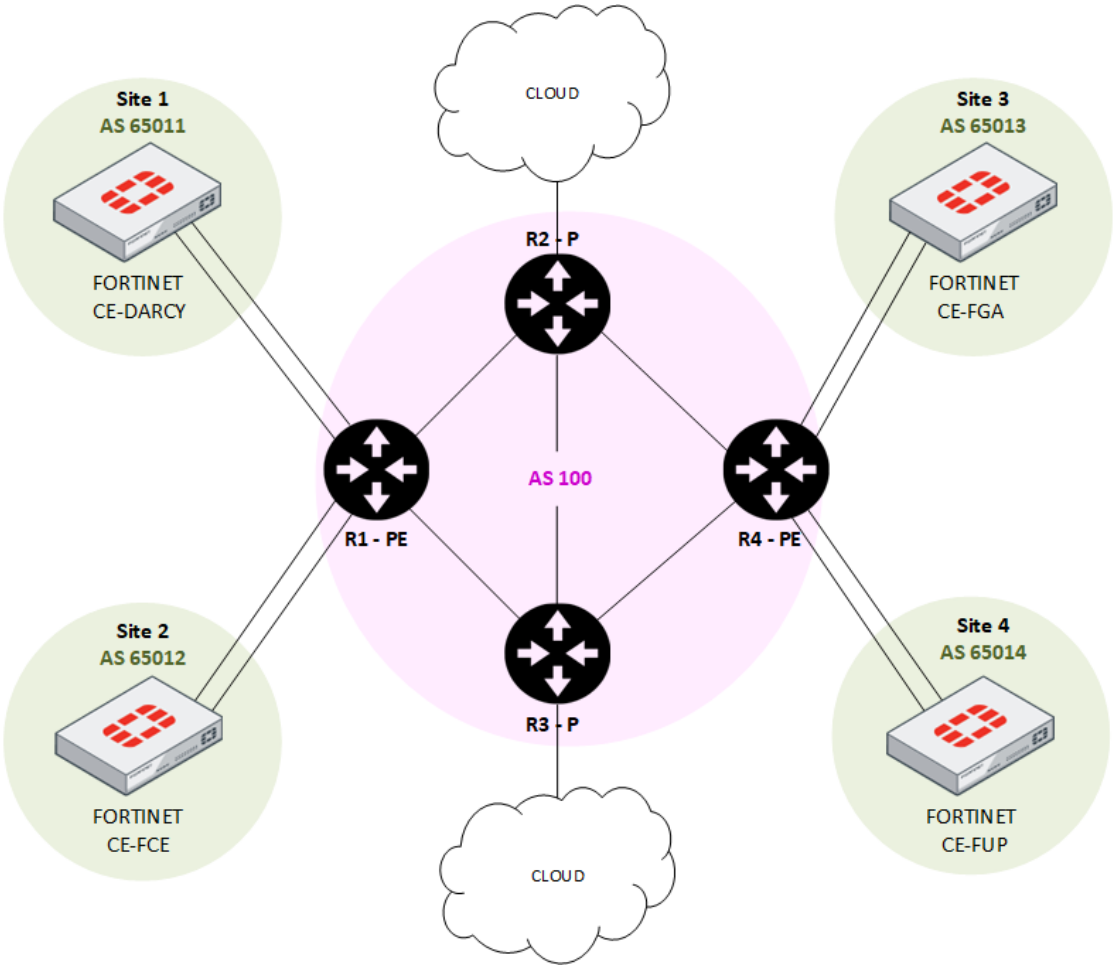


Figura 4.26: Sistemas autônomos presentes na topologia hipotética da Universidade de Brasília. Fonte própria.

A partir disso, a Tabela 4.16 descreve os comandos necessários para a configuração do protocolo BGP do lado da operadora (*backbone*) com AS 100, no qual deve-se utilizar as VRFs (UNB e UNB-2) configuradas previamente, a fim de separar corretamente as redes divulgadas por cada VRF.

Tabela 4.16: Comando para configuração do BGP do lado da operadora

Comando	Descrição
#router bgp 100	Entra no modo de configuração BGP com ID referente ao número do processo BGP local
#address-family ipv4 vrf "NOME"	Especifica a VRF onde irá divulgar a rede vizinha
#neighbor "x.x.x.x" remote-as "X"	Cria uma adjacência BGP (*peer*) com o endereço IP remoto "x.x.x.x" no AS "X"
#neighbor "x.x.x.x" activate	Permite a troca de informações de uma família de endereços especificada com o vizinho BGP

Em seguida, deve-se configurar a sessão BGP do lado do cliente. Para isso, basta acessar a interface *Web* de cada *firewall* e selecionar a opção "*Network->BGP*"no menu principal. Primeiramente, conforme especificado na Figura 4.27, item 1, deve-se inserir o número do AS Local corretamente para cada campus. Posteriormente, configura-se o *Router ID*, esta identificação se refere ao endereço de *Loopback* de cada *firewall*, sendo que o pólo Darcy Ribeiro recebeu o endereço 24.24.24.24/32; FCE recebeu *Loopback* 25.25.25.25/32; FGA recebeu 26.26.26.26/32, e por fim, FUP recebeu o endereço 27.27.27.27/32. Logo após essa configuração, deve-se clicar em "*Create New*" conforme indicado pelo item 3 na Figura 4.27, a fim de criar os *neighbors* que realizarão adjacências com os roteadores da provedora.

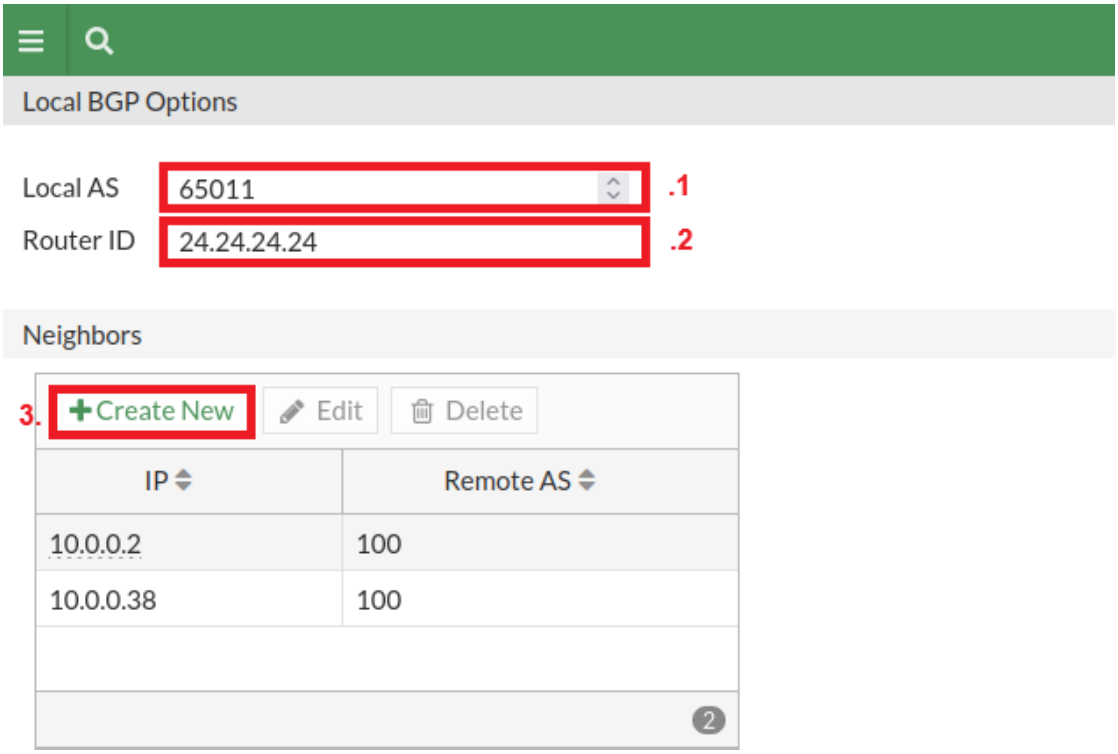


Figura 4.27: Etapas para a configuração da sessão BGP do lado cliente. Fonte própria.

A partir disso, uma nova aba será aberta, conforme indicado pela Figura 4.28. Neste campo

deve-se preencher o endereço IP do *neighbor*, como indicado no item 1, em seguida, é necessário indicar o número do AS remoto, neste caso igual a 100, referente ao sistema autônomo presente no *backbone* da provedora. Deve-se também selecionar a interface que participará dessa adjacência. Para isso, deve-se habilitar o campo indicado no item 3 e definir a interface participante da sessão BGP. Em seguida, habilita-se o campo "*Allow AS in*"para permitir que o BGP informe das atualizações da sessão. Por fim, deve-se selecionar o *checkbox* referente à configuração "*Soft Reconfiguration*", para armazenar as atualizações do protocolo BGP, como também selecionar o *checkbox* referente à configuração "*Next hop self*", com o objetivo de forçar o dispositivo a realizar uma pesquisa recursiva para determinar qual interface de saída deve ser utilizada para o encaminhamento dos pacotes. Com as configurações realizadas, clica-se em OK para finalizar a edição do *neighbor* BGP.

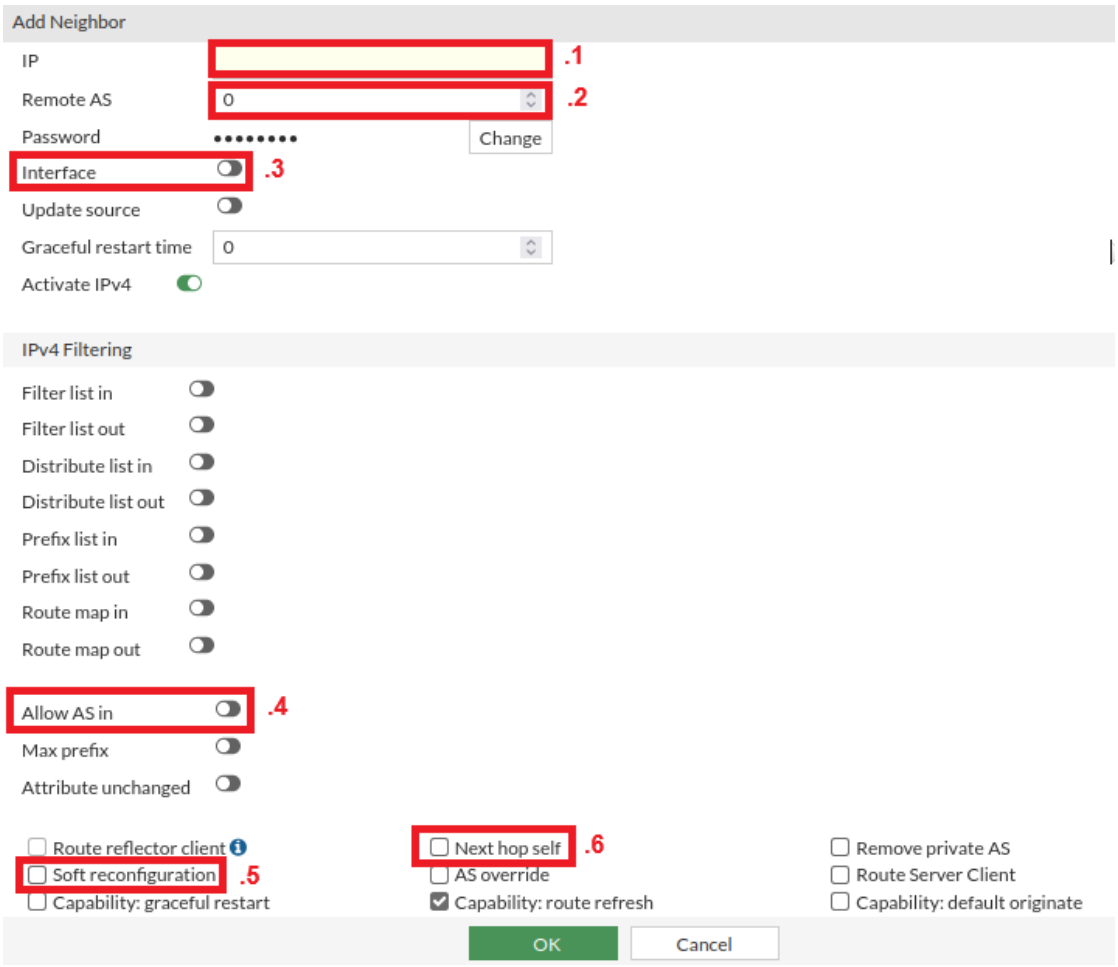


Figura 4.28: Etapas para a configuração dos *neighbors* BGP. Fonte própria.

Após realizar a criação de *neighbors*, é necessário indicar as redes que devem ser redistribuidas via protocolo BGP, conforme indicado na Figura 4.29. Além disso, para que essa redistribuição ocorra é preciso configurar a opção "*Redistribute*". Dessa maneira, habilita-se a opção "*Connected*", "*Static*" e "*OSPF*"para divulgar as rotas às adjacências BGP.

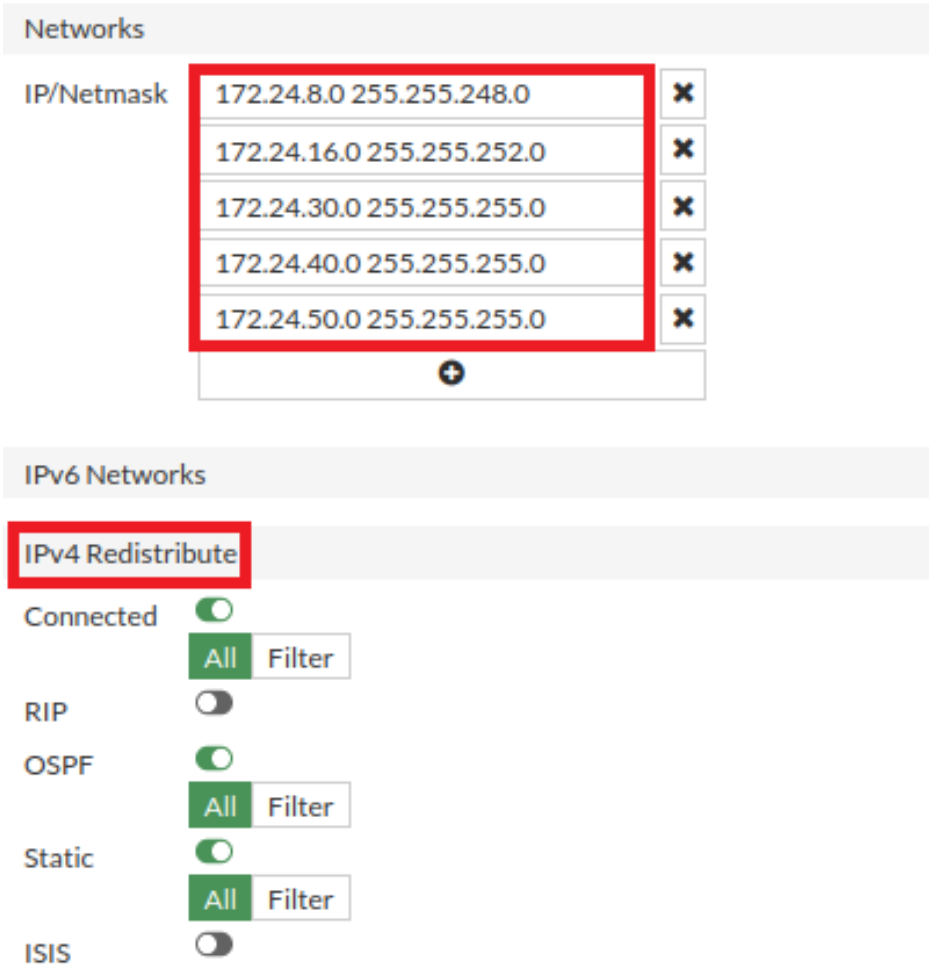


Figura 4.29: Últimas etapas para a configuração da sessão BGP do lado cliente Fonte própria.

Neste momento, com as configurações de roteamento dinâmico realizadas do lado da operadora e do lado dos clientes, têm-se a comunicação dos sites com o *backbone*, entretanto, os campus ainda não se comunicam entre si. Sendo assim, é necessário configurar o MP-BGP no roteador de borda da provedora (PE-R1) para importar as rotas das VRFs e divulgar via iBGP (OSPF+LDP) as redes para o outro roteador de borda (PE-R4).

O MP-BGP, do inglês *Multiprotocol BGP*, se refere à uma extensão do BGP que permite que o protocolo carregue informações de roteamento para várias camadas de rede. Neste caso, ele é utilizado na tecnologia MPLS L3VPN para trocar rótulos (*labels*) VPNv4 dentro do *backbone*.

Dessa maneira, para que os campus da UnB troquem pacotes de dados entre si, é necessário realizar a configuração do MP-BGP. A Tabela 4.17 descreve os comandos necessários para essa etapa.

Tabela 4.17: Comando para configuração do MP-BGP nos roteadores de borda (PEs)

Comando	Descrição
#router bgp 100	Entra no modo de configuração BGP com ID referente ao número do processo BGP local
# neighbor "endereço de loopback" remote-as 100	Cria uma adjacência BGP (*peer*) com o endereço IP de *loopback* remoto presente no outro roteador de borda no AS local 100
#neighbor "endereço de loopback" update-source Loopback"X"	Especifica o endereço de origem (Loopback"X") para alcançar o vizinho especificado
#address-family vpnv4	Especifica a família de endereços VPNv4
#neighbor "endereço de loopback" activate	Permite a troca de informações de uma família de endereços especificada com o vizinho BGP
#neighbor "endereço de loopback" send-community extended	Permite que os valores da comunidade (informações como alvos de rota para MPLS VPN) sejam enviados para o vizinho especificado.

Com as configurações realizadas corretamente, neste momento, é possível realizar a comunicação entre os campus, desde que o *firewall* permita que a rede interna de cada pólo universitário tenha conexão com a rede externa. As devidas análises deste cenário serão detalhadas no capítulo 5.

Em seguida, com as conexões do *backbone* em perfeito funcionamento, é necessário realizar as configurações de conectividade com a *Cloud*, conforme observado na Figura 4.26.

Na maioria das redes, apenas um equipamento é apontado como *gateway* padrão e os *hosts* internos deste segmento encaminham suas solicitações externas para este endereço (REDES, 2023). Entretanto, é de grande importância a redundância numa topologia de redes, a fim de obter *failover* em caso de falhas em um *link* ou até mesmo falhas em um dispositivo. Dessa forma, veio a motivação para a escolha de conexão com a *Cloud* a partir de dois roteadores do *backbone*. Mas, para que a arquitetura tenha sempre um *gateway* padrão em funcionamento mesmo que haja interrupções na comunicação com a saída principal, deve-se configurar o protocolo HSRP, proprietário da Cisco, com o objetivo de prover a alta disponibilidade nos roteadores conectados a *Cloud*.

Conforme mencionado no capítulo 2, o protocolo HSRP foi desenvolvido para fornecer redundância de *gateway* com a utilização de um endereço MAC e IP virtuais compartilhados entre os membros do grupo de roteadores que executam o protocolo, no qual este grupo deve conter um *Active Router*, responsável pelo encaminhamento de pacotes, e um ou mais *Standby Routers*, responsável por assumir como ativo, em caso de falhas.

Dessa maneira, conforme pode ser observado na Figura 4.30, o roteador R2 será definido como o *Active Router*, e o roteador R3 como *Standby Router*. A alta disponibilidade é obtida através do VIP (*Virtual IP*) compartilhado entre os roteadores, e é definido como o *gateway* padrão da rede.

E no caso de falha no equipamento ou *link* principal, o outro componente do grupo assumirá o papel utilizando o endereço virtual. Dessa forma, os clientes não são afetados já que a comunicação permanece ininterrupta (REDES, 2023).

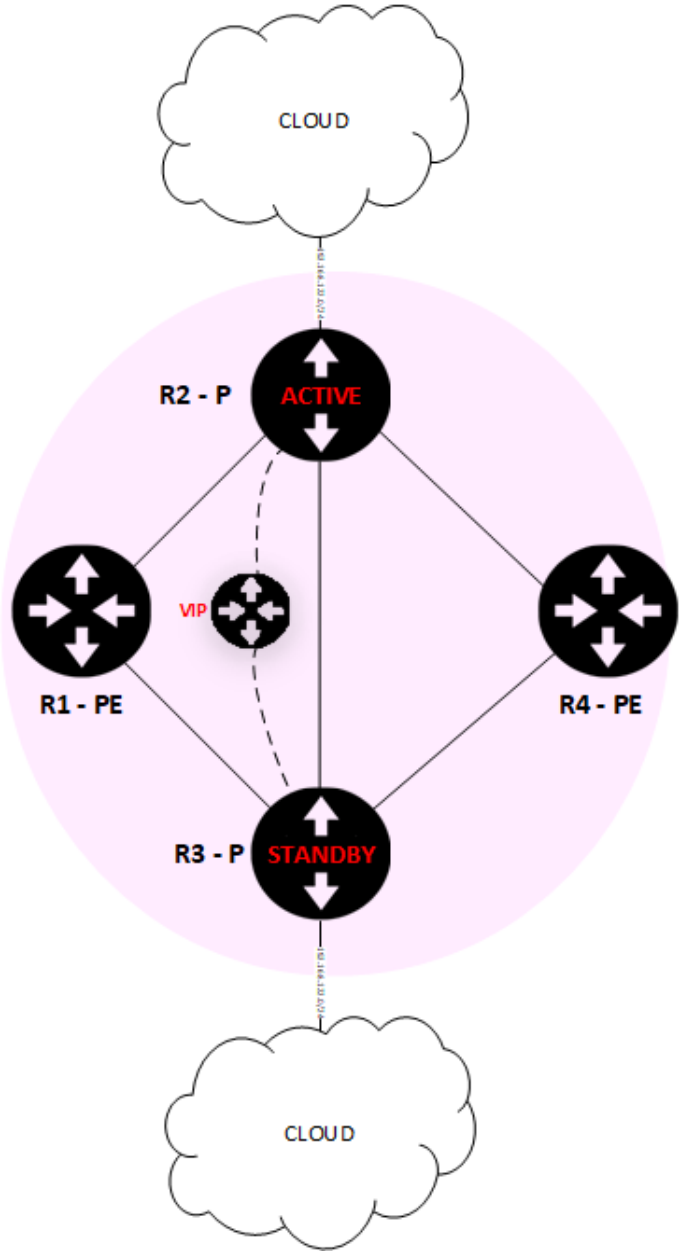


Figura 4.30: Topologia HSRP no *backbone* da provedora. Fonte própria.

A Tabela 4.18 exibe os comandos necessários para a configuração do protocolo HSRP nos roteadores.

Tabela 4.18: Comando para configuração do HSRP nos roteadores conectados à *Cloud*

Comando	Descrição
#interface GigabitEthernet X/0	Acessa o modo de configuração da interface que está diretamente conectada à *Cloud*
#ip address dhcp	Define que o endereçamento IP será entregue através de DHCP
#standby 1 ip "x.x.x.x"	Ativa o HSRP na interface no grupo 1 com IP virtual "*x.x.x.x*"
#standby 1 priority "0-255"	Configura o valor da prioridade do roteador. Sendo que o roteador com o maior número de prioridade no grupo, será definido como *Active Router*

A partir desses comandos, o protocolo HSRP está configurado e os roteadores já assumiram como *Active* e *Standby* conforme definido a partir da prioridade. Entretanto, para que os vizinhos obtenham conectividade com a *Cloud*, é preciso anunciar o *gateway* padrão como sendo estes dois roteadores. Para isso, é necessário configurar rotas estáticas de *backup* com IP SLA *Tracking*, a fim de obter redundância e rotas estáticas de *backup* confiáveis a partir do mecanismo de rastreio da conectividade com a rede de destino com o endereço de próximo salto especificado na rota estática. Dessa maneira, conforme mencionado no capítulo 2, se a conectividade com a rede de destino for perdida por algum motivo, o estado da rota será definido como inativo, e outra rota estática ativa poderá ser selecionada para rotear o tráfego.

O IP SLA é configurado para executar *ping* em um alvo, ou seja, um endereço IP de destino. Dessa maneira, a Tabela 4.19 exibe os comandos para a configuração da tecnologia IP SLA que devem ser configurados nos roteadores R1 e R4.

A última etapa da configuração de rotas estáticas de *backup* com IP SLA *Tracking*, é adicionar a instrução *track* às rotas *default* apontando para os roteadores conectados às *Cloud*s. A Tabela 4.20 exibe os comandos que devem ser configurados.

Com as configurações de IP SLA *Tracking* nos roteadores de borda da provedora (R1 e R4), será possível obter conectividade com a *Cloud* através da rota estática primária somente se o estado do *track* estiver ativo. Caso contrário, a rota secundária será usada para encaminhar todo o tráfego.

A partir disso, o *backbone* possui as configurações de MPLS L3VPN juntamente com a conectividade de alta disponibilidade para a *Cloud* em perfeito funcionamento. O capítulo 5 deste projeto apresentará os resultados e análises de cada uma das tecnologias utilizadas, como também será verificado a redundância presente nessa arquitetura.

Tabela 4.19: Comando para configuração do IP SLA nos roteadores de borda R1 e R4

Comando	Descrição
#ip sla 1	Acessa o modo de configuração IP SLA 1
# icmp-echo "x.x.x.x" source-interface GigabitEthernet"X/0"	Inicia um IP SLA *tracking* e define um alvo "*x.x.x.x*" a partir da interface de origem do roteador, sendo GigabitEthernet"X/0". O alvo deve corresponder a um endereço do *Active Router* definido pelo protocolo HSRP.
#timeout 5000	Define um valor para *timeout*, ou seja, o tempo em que a operação do IP SLA aguardará uma resposta de seu pacote de solicitação ICMP
#threshold 2	Define um valor para *threshold*, ou seja, um limite que gera um evento de reação e armazena informações para a operação do IP SLA
#ip sla schedule 1 life forever start-time now	Define a operação do IP SLA
#track 1 ip sla 1 reachability	Permite o rastreamento do estado de operação do IP SLA

Tabela 4.20: Comando para configuração de rotas *default* com a instrução *track* nos roteadores R1 e R4

Comando	Descrição
#ip route 0.0.0.0 0.0.0.0 "x.x.x.x" track 1	Define a rota *default* principal (para o *Active router* como alvo) com a instrução *track* 1
#ip route 0.0.0.0 0.0.0.0 "x.x.x.x" 10	Define a rota *default* secundária (para o S*tandby router* como alvo) com prioridade 10

4.3.6 Implementação da tecnologia SD-WAN ADVPN

Conforme mencionado anteriormente, a solução SD-WAN aproveita os pontos de conectividade para decidir qual dos caminhos é o mais apropriado para direcionar o tráfego a partir do monitoramento de três parâmetros: latência, *jitter* e perda de pacotes. No caso da infraestrutura desse projeto, há a junção de duas tecnologias, sendo: MPLS L3VPN para conexão com a Internet através do *backbone*, no qual já foi descrito anteriormente, e a solução SD-WAN que será implementado em todos os campus a fim de obter maior desempenho e maximização da disponibilidade dos serviços entre os pólos universitários. Com isso, a comunicação entre os campus ocorrerá a partir da configuração da tecnologia de SD-WAN com tunelamento dinâmico – *Auto-Discovery* VPN (ADVPN), onde túneis IPsec são implementados entre os sites.

Sendo assim, ao projetar uma solução SD-WAN segura,é recomendado pela própria fabricante

Fortinet, utilizar uma abordagem de 5 pilares, conforme é ilustrado na Figura 4.31.

Figura 4.31: Pilares da solução SD-WAN. Fonte: (FORTINET, DESIGN, s.d.). Modificada

O objetivo dos primeiros quatro pilares se refere apenas em definir e proteger os caminhos disponíveis para os destinos desejados. Sendo assim, o primeiro pilar "*Underlay*" se refere a definição de quais *links* WAN serão usados e que tipo de tecnologia será empregada. No caso deste projeto, cada *firewall* presente no campus possui dois *links* WAN no qual se interligam a um *backbone* que possui acesso para a Internet através da solução MPLS L3VPN e além disso, será implementado a solução SD-WAN para interconectar os pólos universitários.

O segundo pilar "*Overlay*" define qual a topologia que irá interligar os sites de forma que os caminhos e destinos disponíveis possam mudar de maneira dinâmica em caso de falhas na rede, migrações planejadas ou até mesmo mudanças nos padrões de tráfego. Nesse caso, a topologia de interconexão entre os sites que será utilizada é a tecnologia de tunelamento dinâmico - *Auto-Discovery* VPN (ADVPN), no qual túneis IPsec diretos entre os sites serão criados a fim de obter uma comunicação de natureza *Zero-Touch*, ou seja, sem intervenção adicional do operador de redes, onde em caso de adição ou remoção de sites, a configuração de todos os outros dispositivos permanecerá inalterada. Além disso, essa tecnologia fornece confidencialidade, integridade e vantagens devido a comunicação direta entre os campus, sem gargalos de rede.

O terceiro pilar "Roteamento" garante que todos os dispositivos de borda do cliente, ou seja, os *firewalls* FortiGate, obtenham informações de roteamento corretas e necessárias para usar nos diversos caminhos disponíveis. No caso das rotas para os caminhos de *overlay*, rotas estáticas serão utilizadas a fim de obter conectividade entre os destinos desejados.

O quarto pilar "Segurança" define como será realizada a proteção de cada um dos caminhos

disponíveis, ou seja, quais serão os tipos de acesso permissivos para cada um dos pólos universitários.

Por fim, o quinto pilar "SD-WAN" se refere à inteligência que será aplicada a cada sessão de saída para decidir qual caminho será selecionado como ideal em um determinado momento e para uma determinada aplicação. Para isso, a tecnologia irá considerar todos os caminhos disponíveis para um destino desejado e irá realizar uma comparação de integridades em tempo real para assim, aplicar uma estratégia de negócios para uma aplicação específica. Se as condições mudarem, um novo caminho será selecionado de maneira rápida.

A partir dos cinco pilares apresentados, a configuração do Fortinet SD-WAN inclui as seguintes etapas:

1. **Criar uma Zona SD-WAN**

   A tecnologia SD-WAN permite realizar diferentes agrupamentos lógicos para as interfaces membro, seja interfaces de *underlay* ou *overlay*. Dessa maneira, as interfaces membros SD-WAN são atribuídas a zonas, e essas zonas são utilizadas em políticas de *firewall*. Neste projeto, apenas uma zona é criada, a fim de agrupar as interfaces VPNs que interconectam os campus. Para isso, basta acessar a aba *Network->SD-WAN* no menu principal, clicar em "*Create New*" e selecionar a opção "*SD-WAN Zone*". A Figura 4.32 mostra a aba de configuração que será aberta, basta adicionar um nome para a zona, que neste caso é "SDW-VPN" e clicar em OK. As interfaces membro desta zona serão criadas na próxima etapa de configuração.

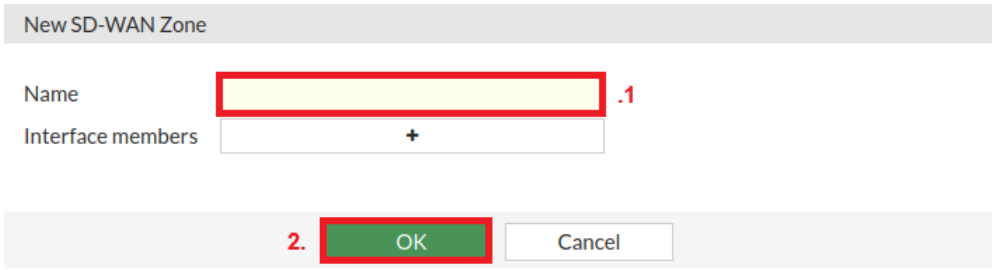


Figura 4.32: Criação da Zona SD-WAN. Fonte própria.

2. **Criar os membros SD-WAN**

   Os membros SD-WAN são as interfaces, sejam elas portas físicas, interfaces VLAN, VPNs ou LAGs, que serão controladas pela tecnologia SD-WAN e por onde o tráfego de dados poderá potencialmente fluir.

   Conforme mencionado neste tópico, a tecnologia de *overlay* utilizada neste projeto é o tunelamento dinâmico - *Auto-Discovery* VPN (ADVPN), no qual túneis IPsec são criados para a interconexão dos campus da UnB.

   Dessa maneira, para se criar os membros participantes da zona "SDW-VPN" criada anteriormente, basta clicar em "*Create New*" na página de configuração de redes "SD-WAN"

e selecionar a opção "*SD-WAN Member*". A Figura 4.33 mostra a aba de configuração que será aberta.

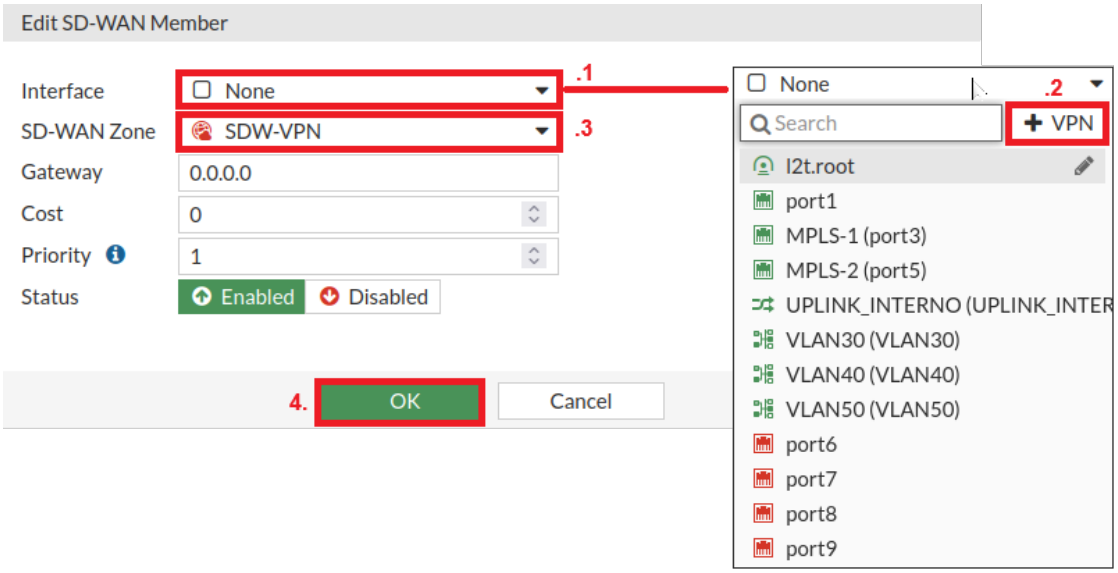


Figura 4.33: Criação dos membros SD-WAN. Fonte própria.

Neste momento, conforme indicado pelo item 1 desta Figura, deve-se clicar na opção "*Interface*". Uma barra de rolagem será exibida. No canto superior direito, conforme indicado pelo item 2, deve-se selecionar o botão "VPN", para criar os túneis IPsec que irão conectar os sites.

A Figura 4.34 exibe a página de configuração do IPsec VPN como membro SD-WAN. Primeiramente, deve-se selecionar o nome da VPN que está sendo criada. Em seguida, conforme indicado pelo item 2 desta figura, deve-se indicar o endereço IP remoto, ou seja, o endereço IP presente no *firewall* FortiGate de outro campus. Na etapa 3, deve-se selecionar a interface de saída do *firewall* local, onde o tráfego irá sair até chegar ao destino. Em seguida, é necessário criar uma chave para a autenticação, nesse caso, para todos os membros a serem criados, será definido como "VPN@VPN". A Tabela 4.21 informa os parâmetros de configuração dos túneis IPsec para cada campus da universidade.

Tabela 4.21: Parâmetros de configuração dos túneis IPsec VPN

Campus	Nome	IP Remoto	Interface de saída
DARCY	VPN-FCE	10.0.0.5	MPLS-1
	VPN-FGA	10.0.0.30	MPLS-1
	VPN-FUP	10.0.0.34	MPLS-1
	VPN-FCE-2	10.0.0.42	MPLS-2
	VPN-FGA-2	10.0.0.46	MPLS-2
	VPN-FUP-2	10.0.0.50	MPLS-2
FCE	VPN-DARCY	10.0.0.1	MPLS-1
	VPN-FGA	10.0.0.30	MPLS-1
	VPN-FUP	10.0.0.34	MPLS-1
	VPN-DARCY-2	10.0.0.37	MPLS-2
	VPN-FGA-2	10.0.0.46	MPLS-2
	VPN-FUP-2	10.0.0.50	MPLS-2
FGA	VPN-DARCY	10.0.0.1	MPLS-1
	VPN-FCE	10.0.0.5	MPLS-1
	VPN-FUP	10.0.0.34	MPLS-1
	VPN-DARCY-2	10.0.0.37	MPLS-2
	VPN-FCE-2	10.0.0.42	MPLS-2
	VPN-FUP-2	10.0.0.50	MPLS-2
FUP	VPN-DARCY	10.0.0.1	MPLS-1
	VPN-FCE	10.0.0.5	MPLS-1
	VPN-FGA	10.0.0.30	MPLS-1
	VPN-DARCY-2	10.0.0.37	MPLS-2
	VPN-FCE-2	10.0.0.42	MPLS-2
	VPN-FGA-2	10.0.0.46	MPLS-2

Ao criar a VPN, deve-se selecioná-la na barra de rolagem indicada por “Interface”, conforme destacado pelo item 1 da Figura 4.33. Em seguida, é necessário indicar a zona criada anteriormente, conforme o item 2 desta Figura. Por fim, clica-se em OK.

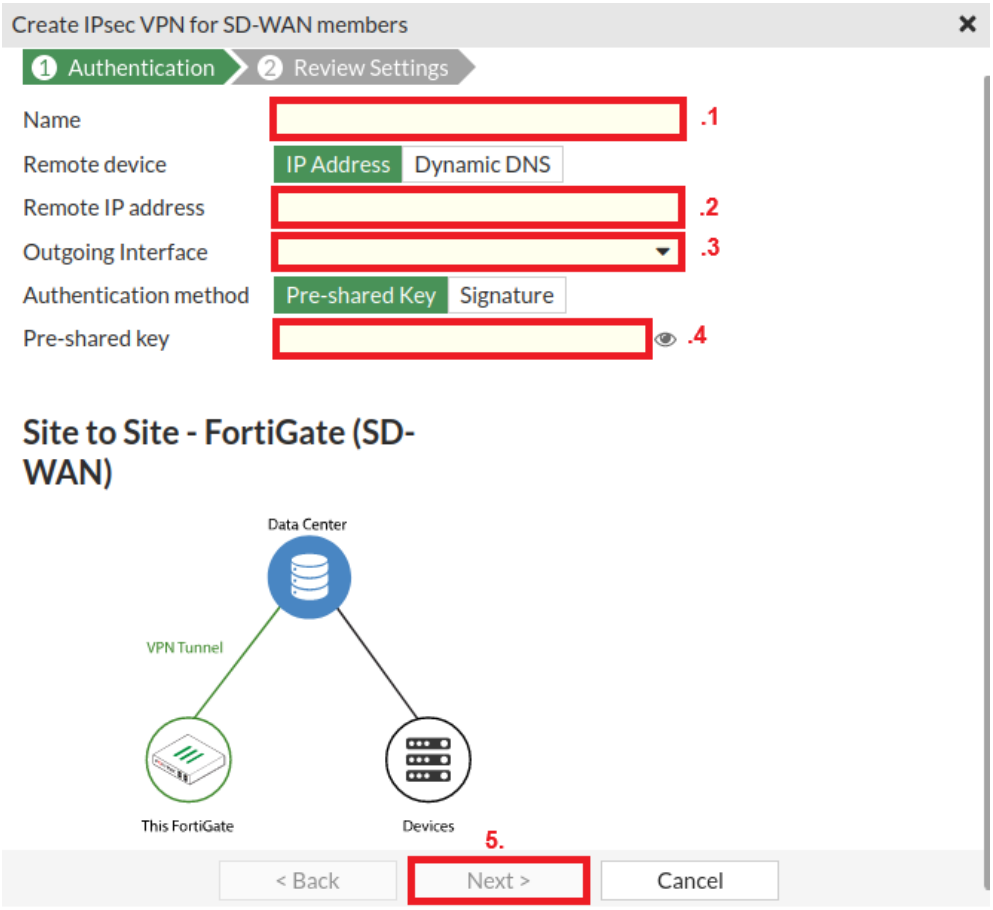


Figura 4.34: Configuração do IPsec VPN como membro SD-WAN. Fonte própria.

3. **Configurar rotas estáticas**

Neste momento, os pilares *Underlay* e *Overlay* foram definidos. Em seguida, deve-se configurar o roteamento. Nesse caso foi utilizado rotas estáticas. Para isso, basta acessar a aba *Network->Static Route* no menu principal, e clicar no botão "*Create New*". Uma nova janela de configuração será aberta, conforme indicado na Figura 4.35. Dessa maneira, é necessário indicar a rede de destino, conforme destacado no item 1 desta Figura, a partir dos parâmetros definidos na Tabela 4.22, para cada campus da universidade. Em seguida, após definir a rede de destino, deve-se selecionar a interface que irá participar do roteamento, conforme destacado no item 2 da Figura, sendo que para todos os casos, deve-se indicar a Zona SD-WAN chamada de "SDW-VPN" configurada anteriormente, no qual possui todas as interfaces membro VPN IPsec agrupadas. Por fim, clica-se em OK, para finalizar a configuração da rota.

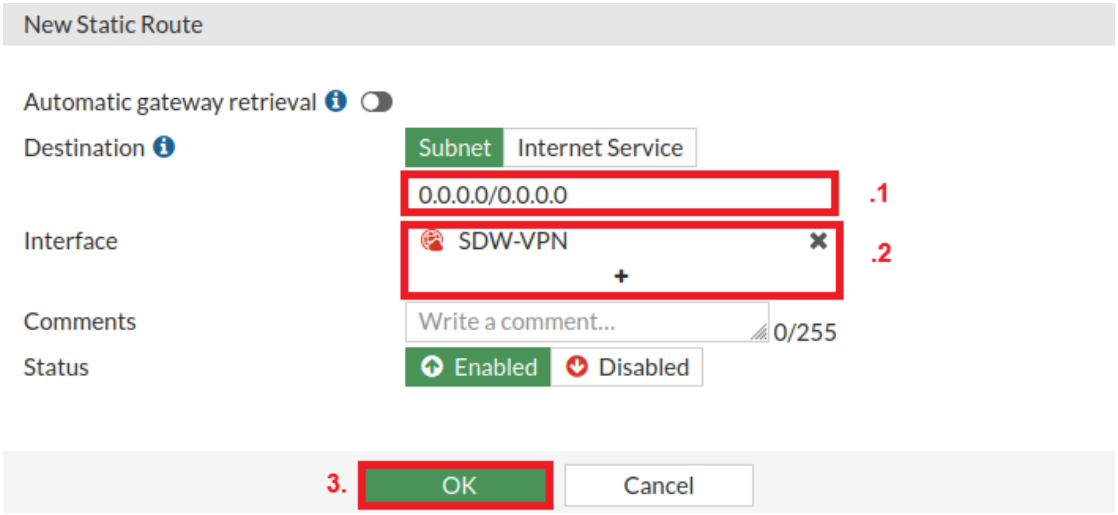


Figura 4.35: Configuração das rotas estáticas para funcionamento da solução SD-WAN. Fonte própria.

Tabela 4.22: Parâmetros de configuração das rotas estáticas

Origem	Destino	Rede de Destino
DARCY	FCE	172.25.0.0/16
	FGA	172.26.0.0/16
	FUP	172.27.0.0/16
FCE	DARCY	172.24.0.0/16
	FGA	172.26.0.0/16
	FUP	172.27.0.0/16
FGA	DARCY	172.24.0.0/16
	FCE	172.25.0.0/16
	FUP	172.27.0.0/16
FUP	DARCY	172.24.0.0/16
	FCE	172.25.0.0/16
	FGA	172.26.0.0/16

4. **Definir regras de segurança**

Com os caminhos aprendidos para todos os destinos possíveis, é necessário definir regras de permissão para que o tráfego de entrada e saída para as interfaces agrupadas na zona "SDW-VPN" possam fluir de forma correta, caso um caminho em específico seja escolhido a partir da estratégia de SD-WAN que será definida posteriormente.

Dessa maneira, as políticas são instruções que controlam o fluxo de tráfego que passa pelo *firewall*. Essas instruções controlam para onde o tráfego deve fluir, como é processado, se é processado e se é permitido ou não passar pelo dispositivo (FIREWALL, 2020).

Para isso, deve-se acessar a aba "*Policy & Objects->Firewall Policy*" e clicar no botão "*Create New*". Uma nova janela de configuração será aberta, conforme ilustrado na

Figura 4.36. Assim, primeiramente, deve-se inserir um Nome para a política, por padrão será utilizado "*Inbound-Nome do Campus REMOTO-Nome do Campus LOCAL*" para definir a política para o tráfego de entrada, e "*Outbound-Nome do Campus REMOTO-Nome do Campus LOCAL*" para definir a política para o tráfego de saída. Isso é necessário para que a comunicação bidirecional ocorra. Em seguida, conforme especificado no item 2 e 3 da Figura, é necessário definir qual a interface de entrada, ou seja, por onde o tráfego irá se originar, como também a interface de saída, que se refere por onde os dados devem sair para alcançar um determinado destino. Deve-se também selecionar uma origem e destino. Para facilitar essa configuração, é possível definir objetos chamados "*Addresses*" inserindo o endereço de sub-rede desejado. E assim, seleciona-se como origem e destino o *Addresses* configurado. Em seguida, conforme destacado no item 6, é necessário inserir o tipo de serviço, neste caso, será definido como "*ALL*". Além disso, deve-se desativar a opção NAT, conforme o item 7 da Figura. Por fim, seleciona-se o botão OK para finalizar a configuração.

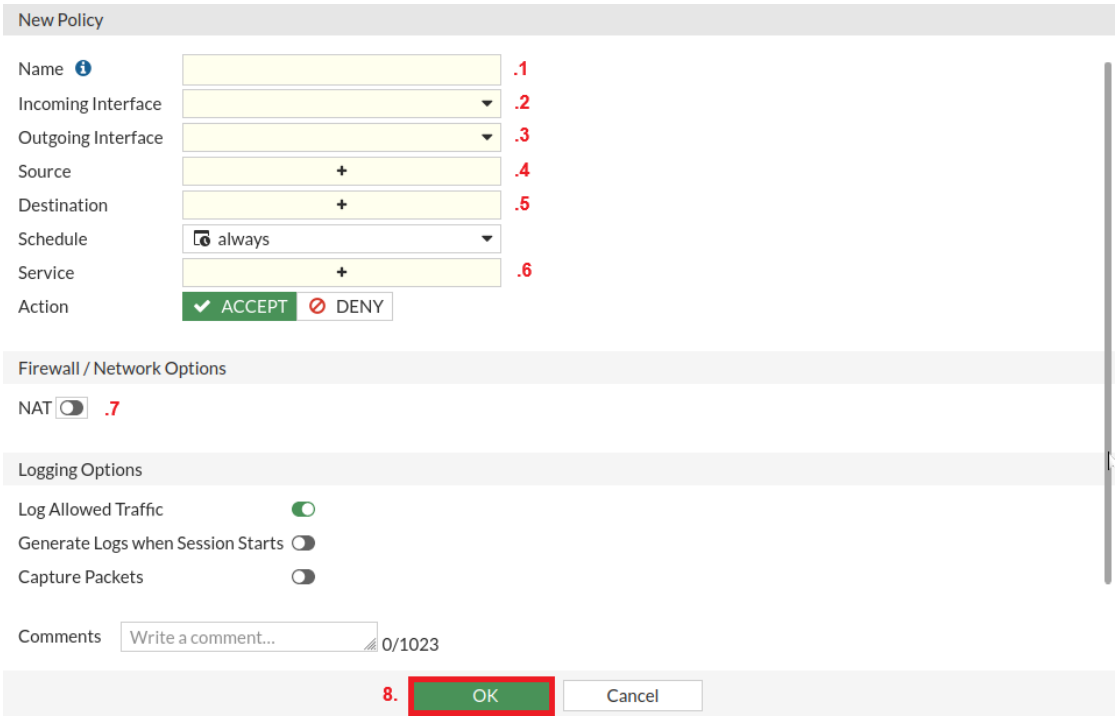


Figura 4.36: Configuração das políticas de segurança para o funcionamento da solução SD-WAN. Fonte própria.

A Tabela 4.23 a seguir descreve os parâmetros utilizados na criação das políticas de *firewall* para o Darcy Ribeiro. Esse modelo deve ser seguido para os outros campus da universidade.

Tabela 4.23: Parâmetros de configuração das políticas de *firewall* para o SD-WAN no campus Darcy Ribeiro

Nome da Regra	Interface de Entrada	Interface de Saída	Origem	Destino
Inbound-FCE-DARCY	SDW-VPN	VLAN"X"	Sub-rede VLAN"X" REMOTO	Sub-rede VLAN"X" LOCAL
Inbound-FGA-DARCY	SDW-VPN	VLAN"X"	Sub-rede VLAN"X" REMOTO	Sub-rede VLAN"X" LOCAL
Inbound-FUP-DARCY	SDW-VPN	VLAN"X"	Sub-rede VLAN"X" REMOTO	Sub-rede VLAN"X" LOCAL
Outbound-FCE-DARCY	VLAN"X"	SDW-VPN	Sub-rede VLAN"X" LOCAL	Sub-rede VLAN"X" REMOTO
Outbound-FGA-DARCY	VLAN"X"	SDW-VPN	Sub-rede VLAN"X" LOCAL	Sub-rede VLAN"X" REMOTO
Outbound-FUP-DARCY	VLAN"X"	SDW-VPN	Sub-rede VLAN"X" LOCAL"	Sub-rede VLAN"X" REMOTO

A Figura 4.37, ilustra o resultado das configurações no campus Darcy Ribeiro a partir dos parâmetros utilizados na Tabela 4.23.

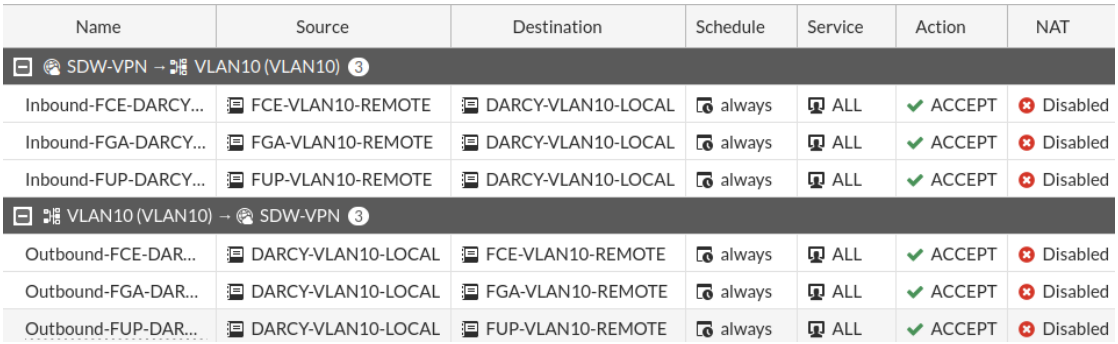


Figura 4.37: Resultado das configuração de políticas de segurança no campus Darcy Ribeiro. Fonte própria.

5. **Configurar estratégia SD-WAN**

Após a configuração das regras de segurança, é necessário definir qual será a inteligência que deve ser aplicada a cada sessão de saída para decidir qual caminho será selecionado como ideal. Para isso, o SD-WAN utilizará SLAs de desempenho, que se referem a sondagens de

verificação de integridade usadas pelos dispositivos de borda para mensurar e avaliar em tempo real, a integridade de cada caminho disponível. Para isso, o *firewall* FortiGate envia sinais de sondagem através de cada *link* SD-WAN para um servidor de destino a partir de um determinado protocolo, seja ele *Ping*, HTTP, TCP/UDP ou DNS, e mede a qualidade desse caminho com base em três parâmetros: latência, *jitter* e porcentagem de perda de pacotes. A partir destas métricas, o SD-WAN poderá definir qual o melhor *link* para o envio dos pacotes de dados.

Para configurar SLAs de desempenho, deve-se acessar a aba "*Network->SD-WAN*" e selecionar a opção "*Performance SLA*" presente no canto superior da tela. Uma nova aba será aberta, conforme ilustrado na Figura 4.38.

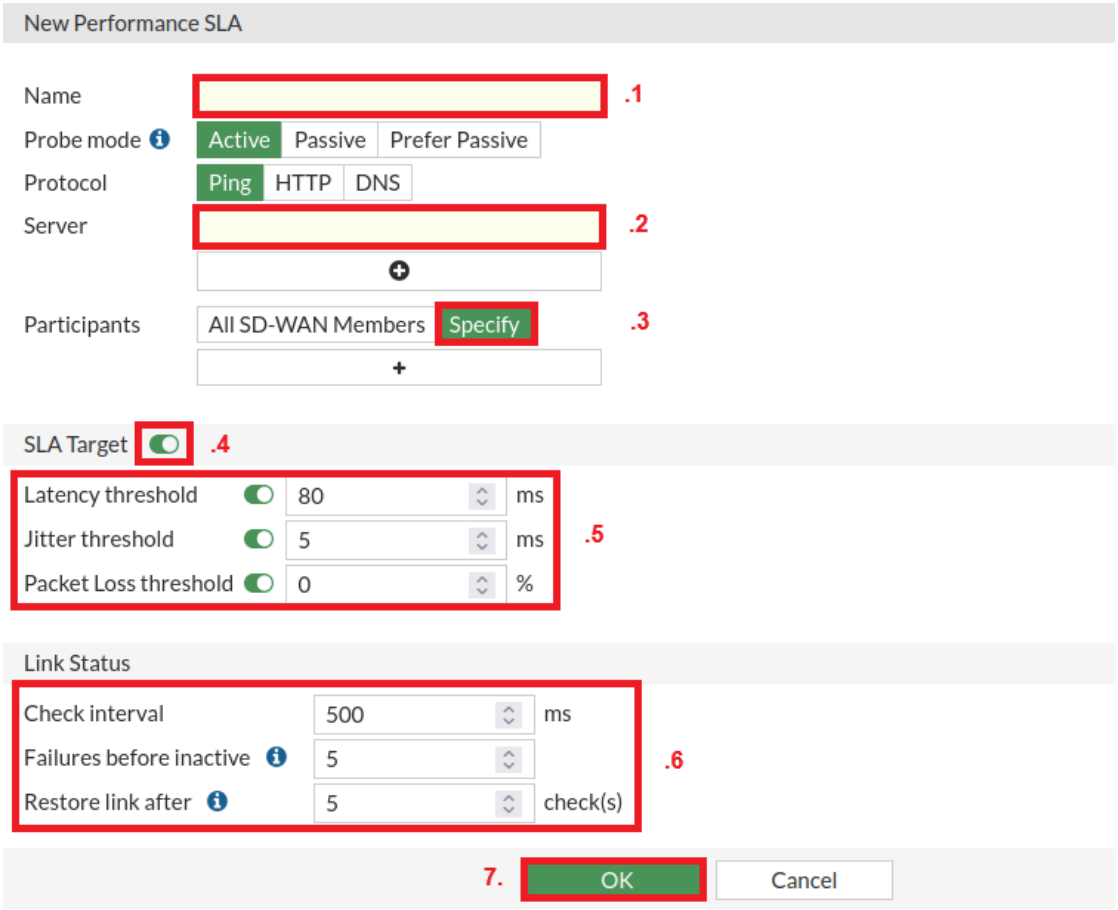


Figura 4.38: Etapas para configuração das SLAs de desempenho. Fonte própria.

Primeiramente, deve-se definir um Nome para o SLA, neste caso cada campus conterá 3 SLAs de desempenho, uma para cada campus remoto, conforme indicado pela Tabela 4.24.

Em seguida, conforme destacado no item 2, deve-se inserir um servidor que irá investigar a integridade a partir do protocolo *Ping*, com isso, para cada campus é necessário inserir um IP referente ao *gateway* da rede interna do campus remoto em questão, como por exemplo, no Darcy Ribeiro, devem-se ser criados 3 SLAs, sendo elas: ICMP-FCE, ICMP-FGA e ICMP-FUP. No caso, do ICMP-FCE, por exemplo, deve-se inserir um IP para o servidor que corresponda ao *gateway* da rede interna deste campus, como por exemplo, o IP 172.25.16.254.

Sendo assim, essa configuração deve ser seguida para os outros SLAs em todos os pólos universitários.

Tabela 4.24: Parâmetros de configuração dos nomes dos SLAs de desempenho em cada campus da UnB

Campus Local	**Campus Remoto**	**Nome do SLA**
DARCY	FCE	ICMP-FCE
	FGA	ICMP-FGA
	FUP	ICMP-FUP
FCE	DARCY	ICMP-DARCY
	FGA	ICMP-FGA
	FUP	ICMP-FUP
FGA	DARCY	ICMP-DARCY
	FCE	ICMP-FCE
	FUP	ICMP-FUP
FUP	DARCY	ICMP-DARCY
	FCE	ICMP-FCE
	FGA	ICMP-FGA

Já na etapa 3, é preciso selecionar a opção "*Specify*" a fim de especificar os membros SD-WAN participantes deste SLA. No caso exemplificado no campus Darcy Ribeiro, os participantes do SLA chamado ICMP-FCE, devem ser as VPNs que conectam o campus FCE, neste caso, VPN-FCE e VPN-FCE-2.

Em seguida, é necessário habilitar a opção "*SLA Target*", que definirá o conjunto de restrições usadas para controlar os caminhos que o tráfego de dados irá fluir, e assim será possível definir qual o melhor *link* para o encaminhamento dos pacotes. Conforme mencionado anteriormente, as restrições disponíveis para a configuração de metas SLA, são: *Latency threshold* (Limite de latência), que se refere ao limite de quantidade de atraso que os dados poderão levar para serem transferidos de um ponto a outro na rede, em milissegundos; *Jitter threshold* (Limite de Jitter), que indica o limite da variação do atraso na entrega de dados em uma rede, também em milissegundos e, por último *Packet Loss threshold* (Limite de Perda de pacotes) que se refere ao limite percentual de perdas de pacotes no caminho entre a origem e o destino final.

Conforme o Guia de Implementação de uma rede Campus de médio e grande porte da Huawei (HUAWEI, s.d.), é definido diversos indicadores de qualidade de serviço, e no caso do protocolo ICMP, o requisito é obter baixa tolerância à perda de pacotes e baixa tolerância à latência. Dessa maneira, deve-se configurar as metas SLA no *firewall* conforme os seguintes requisitos:

- ***Latency threshold*** (Limite de latência): A partir das metas de banda larga da Anatel, foi definido o valor de 80 milissegundos nesta configuração (VENTURA, 2014), a fim de obter um serviço sem interrupções;

- ***Jitter threshold*** (Limite de Jitter): Foi definido o valor de 5 milissegundos na variação do atraso, a fim de obter melhor experiência de qualidade para o usuário;
- ***Packet Loss threshold*** (Limite de Perda de pacotes): Foi definido 0% de limite de perda de pacotes, já que os parâmetros de qualidade de serviço são altos e conforme mencionado pelo Guia de Implementação de uma rede Campus da Huawei, é necessário obter baixa tolerância nesse quesito.

Com isso, após a configuração de metas SLA que definirá os limites utilizados para controlar os caminhos por onde o tráfego irá fluir, é ainda necessário configurar, conforme destacado no item 6 da Figura 4.38, o "*Link Status*", que consiste em três configurações, no qual a partir delas o SLA determinará a frequência com o que o *link* é avaliado e os requisitos para que esse *link* seja considerado válido ou inválido. São elas:

- ***Check Interval*** (Intervalo de verificação): Intervalo em que o *firewall* irá verificar a interface. Neste caso foi configurado um tempo de 500 milissegundos;
- ***Failures before inactive*** (Falhas antes do estado inativo): Número de verificações de *status* com falha antes do *link* ser exposto como inativo. Isso ajudará a evitar oscilações, ou seja, permitirá que o sistema transfira o tráfego entre os *links* sem interrupções. Neste caso, foi configurado um valor de 5 verificações;
- ***Restore link after*** (Verificações de restauração): Número de verificações de *status* de sucesso do *link*, antes que a interface seja exibida como ativa. Neste caso, também foi configurado um valor de 5 verificações.

É importante mencionar, que quando um caminho fica inativo, o SLA de desempenho faz com que o *firewall* retire todas as rotas estáticas associadas a esse *link*.

Feita as devidas configurações, basta clicar em OK para finalizar.

Neste momento, para que o SD-WAN utilize os parâmetros de qualidade de serviço configurados a fim de obter o melhor caminho para encaminhar os dados, é necessário configurar regras de SD-WAN. Dessa maneira, estas regras são usadas para direcionar o tráfego para um membro SD-WAN específico, considerando sua integridade atual e o *status* de SLA.

Sendo assim, deve-se acessar a aba "*Network->SD-WAN*" e selecionar a opção "*SD-WAN Rules*", presente também no canto superior da tela. A Figura 4.39 exibe os passos necessários para a configuração. Cada campus será composto por 3 regras SD-WAN, uma para cada pólo universitário remoto, como por exemplo, no campus Darcy Ribeiro, deverão ser configuradas 3 regras referentes aos campus FCE, FUP e FGA. Dessa maneira, conforme observado na Figura 4.39, deve-se primeiramente, inserir um Nome para a regra. Neste caso o seguinte modelo foi utilizado: "*SDW-Nome do Campus REMOTO-ICMP*". A Tabela 4.25 exemplifica todos os parâmetros de configuração do campus Darcy Ribeiro, no qual todos os outros sites devem seguir a mesma lógica.

Tabela 4.25: Parâmetros de configuração das Regras SD-WAN do campus Darcy Ribeiro

Nome da Regra	Origem	Destino	Membros SD-WAN	SLA
SDW-FCE-ICMP	Sub-rede VLAN"X" DARCY	Sub-rede VLAN"X" FCE	VPN-FCE VPN-FCE-2	ICMP-FCE
SDW-FGA-ICMP	Sub-rede VLAN"X" DARCY	Sub-rede VLAN"X" FGA	VPN-FGA VPN-FGA-2	ICMP-FGA
SDW-FUP-ICMP	Sub-rede VLAN"X" DARCY	Sub-rede VLAN"X" FUP	VPN-FUP VPN-FUP-2	ICMP-FUP

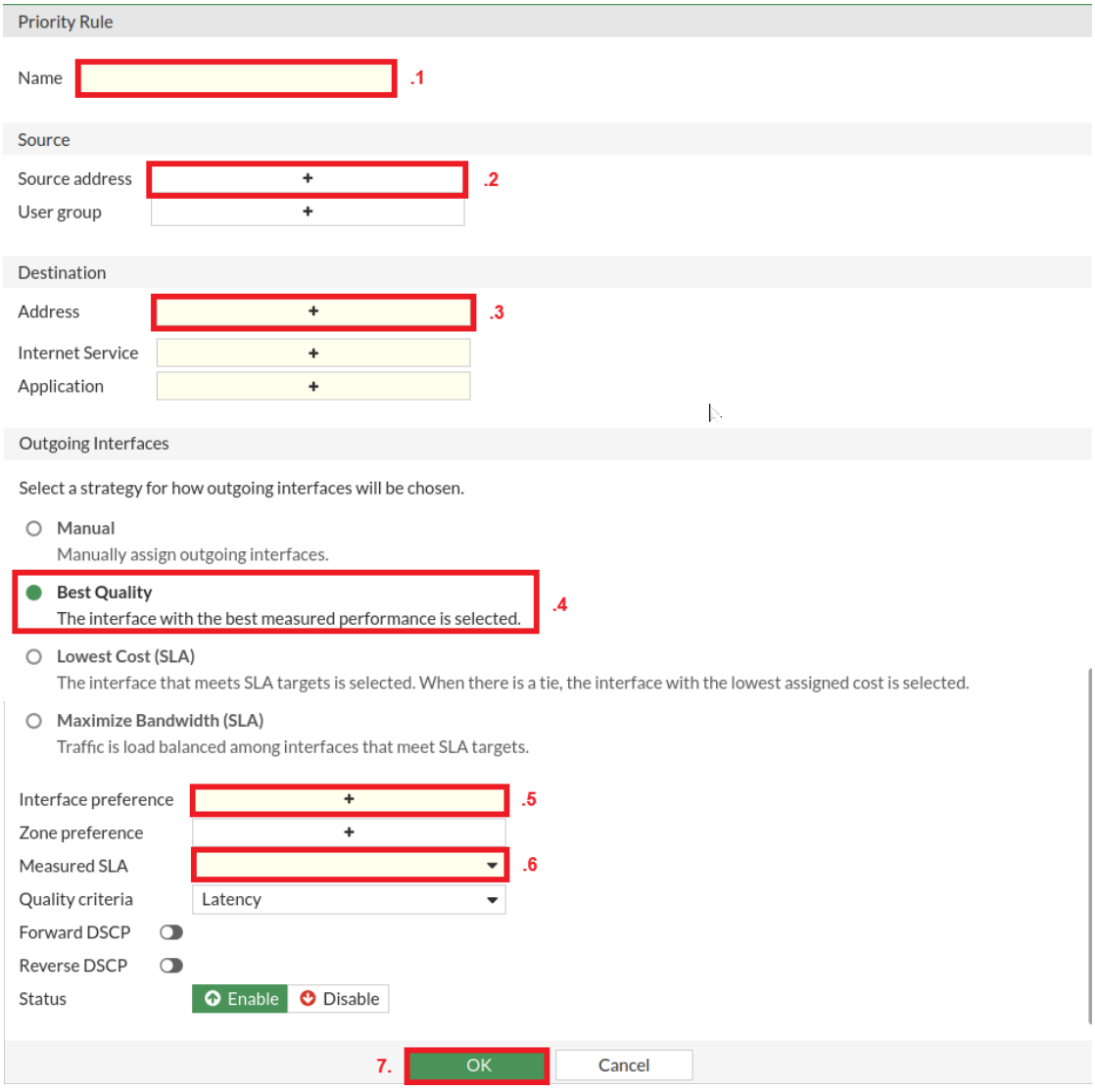


Figura 4.39: Etapas para configuração das Regras de SD-WAN a partir dos SLAs configurados. Fonte própria.

Em seguida, conforme destacado no item 2 e 3 da Figura 4.39, deve-se indicar qual a origem e destino do tráfego. Neste caso, a origem será indicada sempre pela sub-rede das VLANs internas do próprio campus. Já o destino, será indicado pela sub-rede das VLANs internas dos campus remotos. Por exemplo, conforme pode ser observado na Tabela 4.25, a regra SDW-FCE-ICMP presente no campus Darcy Ribeiro, possui como origem a própria rede interna do campus, e como destino a rede interna do campus FCE.

Após definir as redes de origem e destino, é necessário designar uma estratégia SD-WAN. Esta estratégia irá definir a lógica aplicada para selecionar um dos membros SD-WAN para direcionar o tráfego de dados. Neste caso, a estratégia escolhida foi a "*Best Quality*", no qual selecionará o membro SD-WAN com a melhor qualidade medida, com base no SLA configurado anteriormente. Dessa maneira, deve-se selecionar as interfaces membro que participarão desta regra, conforme indicado pelo item 5. Sendo assim, caso a regra seja destinada para o campus FCE, apenas os membros VPN-FCE e VPN-FCE-2 devem ser selecionados. Além disso, o item 6 se refere à seleção do SLA, o qual a regra utilizará para medir e validar o melhor caminho de transmissão. Após essas configurações, basta clicar no botão OK para finalizar.

Após as configurações dos pilares que compõem o SD-WAN em cada um dos campus da UnB, será possível observar os seus membros online, conforme pode ser visto na Figura 4.40. Análises e resultados detalhados dessa tecnologia serão exibidos no próximo capítulo.

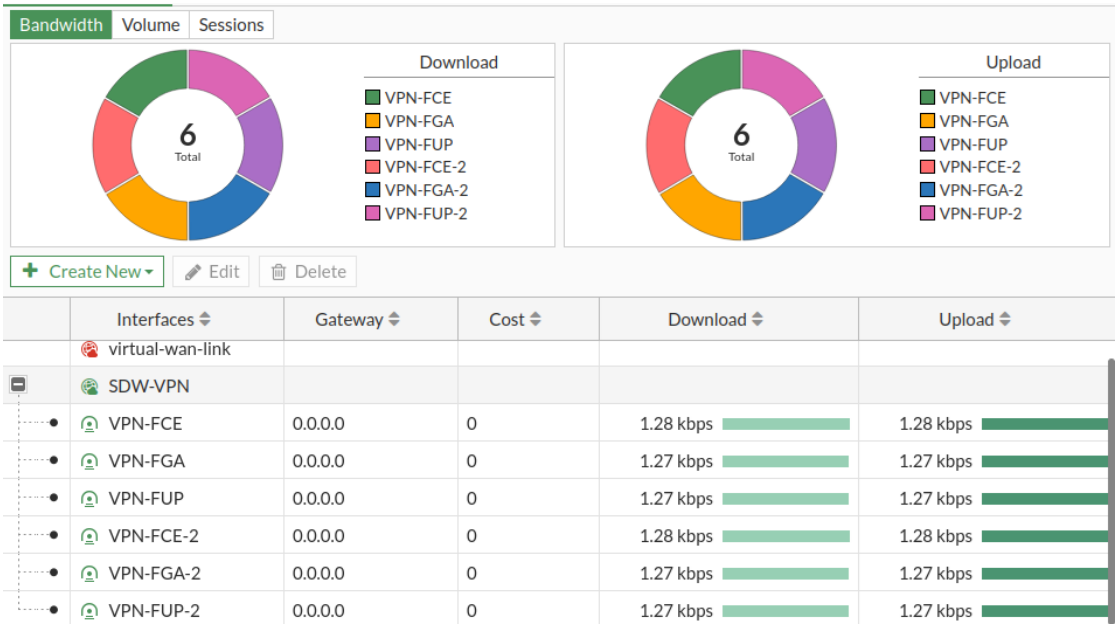


Figura 4.40: Membros SD-WAN Online referente ao campus Darcy Ribeiro. Fonte própria.

Capítulo 5

Testes e Resultados

Este capítulo irá expor uma série de testes realizados na infraestrutura de redes criada, de forma a comprovar e garantir que as escolhas de ativos, protocolos, tecnologias e configurações, foram efetuadas com êxito. Dentre as verificações, foram feitos testes de redundância de *link* entre os ativos do *backbone* e também dos ativos da *intranet* dos campus, além disso para analisar o caminho que o tráfego estava percorrendo, utilizou-se do *sniffer* Wireshark para explorar os pacotes e seus conteúdos sendo encaminhados pela rede.

Sendo assim, tendo como base o conhecimento de como os comandos "*ping*"e "*traceroute*"funcionam e contribuem para a realização de análises em uma infraestrutura de redes, juntamente com a análise de pacotes capturados utilizando-se do Wireshark, as seções abaixo apresentadas mostrarão os testes que foram realizados, bem como os resultados obtidos, que verificarão se a infraestrutura implementada está funcionando corretamente, de acordo com o esperado.

5.1 Rede Interna dos Campus

5.1.1 Comunicação entre os *switches*

Assim como especificado na seção 4.3.3, a rede interna de cada campus possui *switches* Core, de Distribuição e de Acesso. Cada *switch* foi configurado de forma a aceitar e suportar o tráfego de rede gerado por usuários pertencentes a VLANs diferentes, tornando possível que usuários de diferentes campus conseguissem se comunicar entre eles e também com usuários externos. Além disso, a razão pela qual cada rede interna possui 2 *switches* Core, de Distribuição e de Acesso está no fato de que essa rede oferece redundância de *link* para que no caso de uma eventual falha de *link* ou ativo de rede, a comunicação não seja perdida.

Os testes realizados a seguir serão efetuados nos *switches* que compõem a rede interna do campus Darcy Ribeiro, como pode ser visto na Figura 5.1, porém é preciso ressaltar que os resultados obtidos valem para qualquer um dos campus, isso porque foram efetuadas as mesmas configurações em cada um deles.

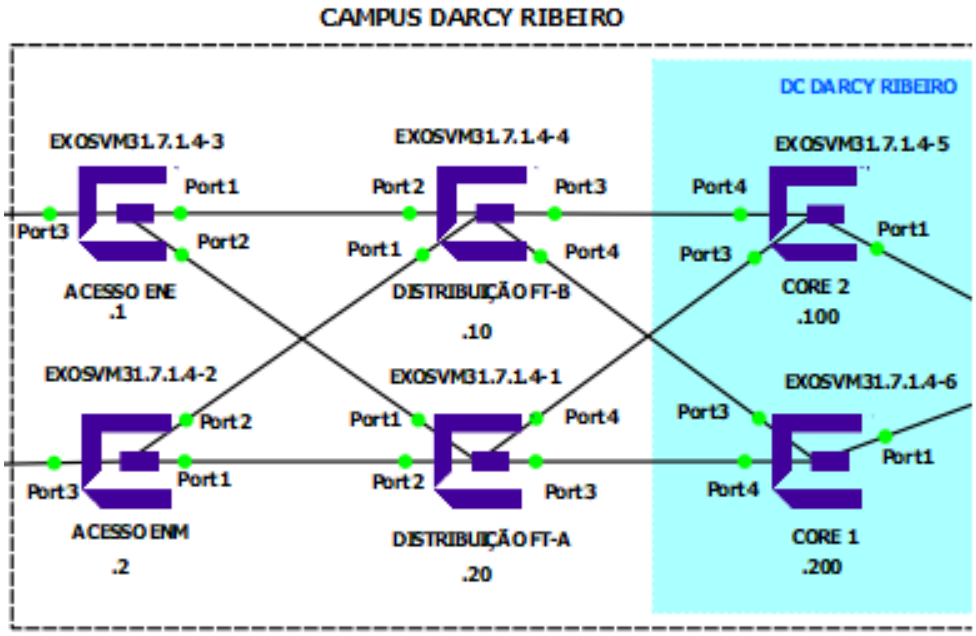


Figura 5.1: *Intranet* do Campus Darcy Ribeiro. Fonte Própria

Assim sendo, foi feita a execução do comando "*ping 172.24.8.1*"no terminal do *Switch* CORE 2, esse endereço IP diz respeito ao *Switch* denominado "ACCESSO ENE". Assim como pode ser visto na Figura 5.2, o *ping* ocorreu de maneira bem sucedida, indicando assim que o *Switch* Core possui comunicação com o *Switch* de Acesso.

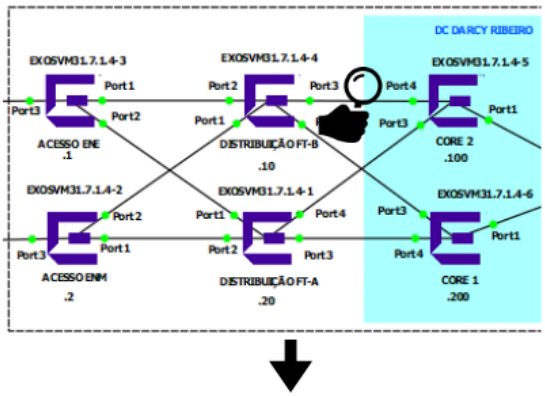
Switch Core -> Switch de Acesso

```
CORE-2-DC.3 # ping 172.24.8.1
Ping(ICMP) 172.24.8.1: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.8.1: icmp_seq=0 ttl=64 time=7.589 ms
16 bytes from 172.24.8.1: icmp_seq=1 ttl=64 time=1.944 ms
16 bytes from 172.24.8.1: icmp_seq=2 ttl=64 time=2.089 ms
16 bytes from 172.24.8.1: icmp_seq=3 ttl=64 time=2.098 ms
```

Figura 5.2: Teste de conectividade entre os ativos da *intranet* no campus Darcy Ribeiro. Fonte Própria

Para entender qual foi o caminho percorrido pelo pacote ICMP gerado por esse comando *ping*, foi utilizado o *sniffer* Wireshark na porta 4 e 3 do *Switch* Core 2 e, assim como exposto na Figura 5.3, a comunicação entre o *Switch* Core e o *Switch* de Acesso foi bem sucedida, onde o pacote foi direcionado pelo *link* que conecta o *Switch* Core 2 ao *Switch* de Distrbuição FT-B.

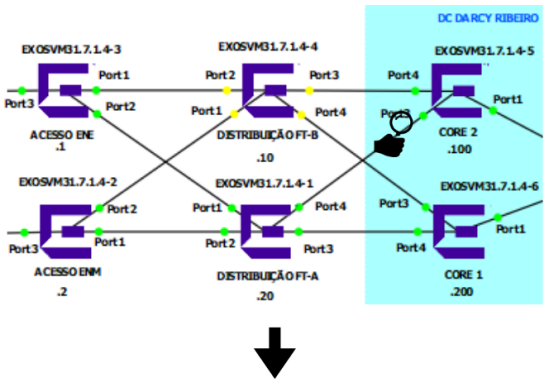
Apesar do resultado acima exposto ser satisfatório, considerando que a comunicação entre os *Switches* está ocorrendo de maneira bem sucedida, é ainda necessário verificar qual o comportamento da rede no caso desse *Switch* de Distrubuição FT-B falhe. Por isso, o mesmo comando *ping* foi executado, só que agora com o *Switch* de Distribuição FT-B desativado. Foi também feita a utilização do *sniffer* Wireshark para analisar se o pacote iria percorrer um novo caminho para alcançar o destino.




```
93979 37.025480   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0008, seq=0/0, ttl=64 (reply in 93980)
93980 37.026868   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0008, seq=0/0, ttl=64 (request in 93979)
93982 37.336709   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0008, seq=1/256, ttl=64 (reply in 93983)
93983 37.338042   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0008, seq=1/256, ttl=64 (request in 93982)
93986 38.394398   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0008, seq=2/512, ttl=64 (reply in 93987)
93987 38.395748   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0008, seq=2/512, ttl=64 (request in 93986)
93989 39.501176   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0008, seq=3/768, ttl=64 (reply in 93990)
93990 39.502661   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0008, seq=3/768, ttl=64 (request in 93989)
```

Figura 5.3: Pacotes capturados entre o *Switch* Core e o *Switch* de Distribuição. Fonte Própria

Na Figura 5.4 é possível verificar que o pacote ICMP partindo do *Switch* Core 2 passou a ser encaminhado para o *Switch* de Distribuição FT-A e chegou de maneira bem sucedida ao destino final.




```
25 12.871949   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0009, seq=0/0, ttl=64 (reply in 26)
26 12.873183   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0009, seq=0/0, ttl=64 (request in 25)
38 13.542748   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0009, seq=1/256, ttl=64 (reply in 39)
39 13.544079   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0009, seq=1/256, ttl=64 (request in 38)
53 14.600751   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0009, seq=2/512, ttl=64 (reply in 54)
54 14.602309   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0009, seq=2/512, ttl=64 (request in 53)
66 15.708117   172.24.8.100   172.24.8.1     ICMP   64 Echo (ping) request  id=0x0009, seq=3/768, ttl=64 (reply in 69)
69 15.711887   172.24.8.1     172.24.8.100   ICMP   64 Echo (ping) reply    id=0x0009, seq=3/768, ttl=64 (request in 66)
```

Figura 5.4: Pacotes capturados detectando nova rota de passagem de pacotes, quando um *Switch* de Distribuição se torna inacessível. Fonte Própria

Sendo assim, após o comportamento acima exposto é possível concluir que a comunicação entre os *Switches* que compõem a infraestrutura de rede interna do campus Darcy Ribeiro está funcionando de maneira correta, de forma que mesmo em uma eventual queda de *link* ou falha de dispositivo, os dispositos conseguem se comunicar.

5.1.2 Comunicação entre a *intranet* e *Gateways*

Na seção acima foi possível comprovar que os *switches* possuem conectividade entre si. Nesta seção serão realizados testes e análises de forma a comprovar que os *switches* possuem comunicação bem sucedida com os *gateways* existentes no *firewall*.

Switch de Distribuição -> Gateway da VLAN 10

```
* DISTRIBUICAO-FT-B.3 # ping 172.24.15.254
Ping(ICMP) 172.24.15.254: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.15.254: icmp_seq=0 ttl=255 time=2.056 ms
16 bytes from 172.24.15.254: icmp_seq=1 ttl=255 time=1.791 ms
16 bytes from 172.24.15.254: icmp_seq=2 ttl=255 time=1.960 ms
16 bytes from 172.24.15.254: icmp_seq=3 ttl=255 time=1.844 ms

--- 172.24.15.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/1/2 ms
```

Switch de Distribuição -> Gateway da VLAN 20

```
* DISTRIBUICAO-FT-B.3 # ping 172.24.19.254
Ping(ICMP) 172.24.19.254: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.19.254: icmp_seq=0 ttl=255 time=4.499 ms
16 bytes from 172.24.19.254: icmp_seq=1 ttl=255 time=1.868 ms
16 bytes from 172.24.19.254: icmp_seq=2 ttl=255 time=1.794 ms
16 bytes from 172.24.19.254: icmp_seq=3 ttl=255 time=1.908 ms

--- 172.24.19.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
```

Switch de Distribuição -> Gateway da VLAN 30

```
* DISTRIBUICAO-FT-B.4 # ping 172.24.30.254
Ping(ICMP) 172.24.30.254: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.30.254: icmp_seq=0 ttl=255 time=7.709 ms
16 bytes from 172.24.30.254: icmp_seq=1 ttl=255 time=1.912 ms
16 bytes from 172.24.30.254: icmp_seq=2 ttl=255 time=1.758 ms
16 bytes from 172.24.30.254: icmp_seq=3 ttl=255 time=1.916 ms

--- 172.24.30.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/3/7 ms
```

Switch de Distribuição -> Gateway da VLAN 40

```
* DISTRIBUICAO-FT-B.5 # ping 172.24.40.254
Ping(ICMP) 172.24.40.254: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.40.254: icmp_seq=0 ttl=255 time=9.122 ms
16 bytes from 172.24.40.254: icmp_seq=1 ttl=255 time=1.700 ms
16 bytes from 172.24.40.254: icmp_seq=2 ttl=255 time=1.671 ms
16 bytes from 172.24.40.254: icmp_seq=3 ttl=255 time=1.877 ms

--- 172.24.40.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/3/9 ms
```

Switch de Distribuição -> Gateway da VLAN 50

```
* DISTRIBUICAO-FT-B.6 # ping 172.24.50.254
Ping(ICMP) 172.24.50.254: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.24.50.254: icmp_seq=0 ttl=255 time=4.732 ms
16 bytes from 172.24.50.254: icmp_seq=1 ttl=255 time=1.609 ms
16 bytes from 172.24.50.254: icmp_seq=2 ttl=255 time=1.890 ms
16 bytes from 172.24.50.254: icmp_seq=3 ttl=255 time=1.755 ms

--- 172.24.50.254 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
round-trip min/avg/max = 1/2/4 ms
```

Figura 5.5: *Switches* da intranet possuem conexão com o *gateway*, no *Firewall*. Fonte própria.

Comprovar e se certificar se a comunicação entre os *switches* e seus respectivos *gateways* está funcionando corretamente trata-se de um pré-requisito fundamental, que vai garantir que os ativos da *intranet* do campus conseguirão se comunicar com ativos externos. Sendo assim, a partir do *Switch* de Distribuição FT-B foi feita a execução do comando *ping* tendo como endereço IP de destino os *gateways* de cada VLAN, como pode ser visto na Figura 5.5.

A Figura 5.5 apresentada atesta que os *switches* da *intranet* possuem uma comunicação bem sucedida com cada um dos *gateways* presentes no *firewall* FortiGate. É ainda imprescíndivel realizar testes de conectividade entre ativos de redes pertencentes às diferentes VLANs que compõem a *intranet*. Pensando nisso, foi feito o teste de conectividade entre um dispositivo Ubuntu pertencente à VLAN 10, de endereço IP 172.24.8.15, e o *gateway* da VLAN 10, com endereço IP 172.24.15.254, localizado no FortiGate. De acordo com o visto na Figura 5.6, a conexão é estabelecida com sucesso. Para saber com precisão a localização desses Ubuntus na topologia do Campus Darcy Ribeiro, basta verificar a Figura 5.18 presente na seção 5.1.5.

Ubuntu VLAN 10 -> Gateway da VLAN 10

```
osboxes@osboxes:~$ ping 172.24.15.254
PING 172.24.15.254 (172.24.15.254) 56(84) bytes of data.
64 bytes from 172.24.15.254: icmp_seq=1 ttl=255 time=3.41 ms
64 bytes from 172.24.15.254: icmp_seq=2 ttl=255 time=3.07 ms
64 bytes from 172.24.15.254: icmp_seq=3 ttl=255 time=3.45 ms
64 bytes from 172.24.15.254: icmp_seq=4 ttl=255 time=3.22 ms
^C
--- 172.24.15.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.078/3.293/3.456/0.161 ms
osboxes@osboxes:~$
```

Figura 5.6: Dispositivo da VLAN 10 possui comunicação com o *gateway* da VLAN 10, localizado no *Firewall* FortiGate. Fonte própria.

A Figura 5.7 mostra o tráfego de pacotes detectado entre o endereço IP de origem, do Ubuntu pertencente à VLAN 10, e o endereço IP de destino, correspondente ao *gateway* da VLAN 10 localizado no *firewall* FortiGate, capturado utilizando o *sniffer* Wireshark.

Pacotes encaminhados entre o Ubuntu VLAN 10 e o Gateway da VLAN 10

icmp

No.	Time	Source	Destination	Protocol	Length	Info
16	6.103167	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x08cc, seq=1/256, ttl=64 (reply in 17)
17	6.103634	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x08cc, seq=1/256, ttl=255 (request in 16)
19	7.104750	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x08cc, seq=2/512, ttl=64 (reply in 20)
20	7.105103	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x08cc, seq=2/512, ttl=255 (request in 19)
22	8.106541	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x08cc, seq=3/768, ttl=64 (reply in 23)
23	8.106874	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x08cc, seq=3/768, ttl=255 (request in 22)
25	9.107098	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x08cc, seq=4/1024, ttl=64 (reply in 26)
26	9.107449	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x08cc, seq=4/1024, ttl=255 (request in 25)

Figura 5.7: Pacotes capturados entre dispositivo da VLAN 10 e o *gateway* da VLAN 10, localizado no *firewall* FortiGate. Fonte própria.

Da mesma maneira, foi feito o teste de conectividade entre um dispositivo Ubuntu pertencente à VLAN 20, de endereço IP 172.24.16.4, e o *gateway* da VLAN 20, de endereço IP 172.24.19.254, localizado no FortiGate. De acordo com o visto na Figura 5.8, a conexão é estabelecida com sucesso.

Ubuntu VLAN 20 -> Gateway da VLAN 20

```
osboxes@osboxes:~$ ping 172.24.19.254
PING 172.24.19.254 (172.24.19.254) 56(84) bytes of data.
64 bytes from 172.24.19.254: icmp_seq=1 ttl=255 time=7.23 ms
64 bytes from 172.24.19.254: icmp_seq=2 ttl=255 time=3.15 ms
64 bytes from 172.24.19.254: icmp_seq=3 ttl=255 time=3.40 ms
64 bytes from 172.24.19.254: icmp_seq=4 ttl=255 time=3.32 ms
^C
--- 172.24.19.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 3.151/4.280/7.238/1.711 ms
```

Figura 5.8: Dispositivo da VLAN 20 possui comunicação com o *gateway* da VLAN 20, localizado no *firewall* FortiGate. Fonte própria.

A Figura 5.9 mostra o tráfego de pacotes detectado entre o endereço IP de origem, correspondente ao Ubuntu da VLAN 20, e o endereço IP de destino, correspondente ao *gateway* da VLAN 20 localizado no *firewall* FortiGate, capturado utilizando o *sniffer* Wireshark.

Pacotes encaminhados entre o Ubuntu VLAN 20 e o Gateway da VLAN 20

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
3408	28.283439	172.24.16.4	172.24.19.254	ICMP	98	Echo (ping) request id=0x078e, seq=13/3328, ttl=64 (reply in 3409)
3409	28.321479	172.24.19.254	172.24.16.4	ICMP	98	Echo (ping) reply id=0x078e, seq=13/3328, ttl=255 (request in 3408)
3410	29.284832	172.24.16.4	172.24.19.254	ICMP	98	Echo (ping) request id=0x078e, seq=14/3584, ttl=64 (reply in 3411)
3411	29.321263	172.24.19.254	172.24.16.4	ICMP	98	Echo (ping) reply id=0x078e, seq=14/3584, ttl=255 (request in 3410)
3412	30.286532	172.24.16.4	172.24.19.254	ICMP	98	Echo (ping) request id=0x078e, seq=15/3840, ttl=64 (reply in 3413)
3413	30.321492	172.24.19.254	172.24.16.4	ICMP	98	Echo (ping) reply id=0x078e, seq=15/3840, ttl=255 (request in 3412)
3414	31.287769	172.24.16.4	172.24.19.254	ICMP	98	Echo (ping) request id=0x078e, seq=16/4096, ttl=64 (reply in 3415)
3415	31.333172	172.24.19.254	172.24.16.4	ICMP	98	Echo (ping) reply id=0x078e, seq=16/4096, ttl=255 (request in 3414)
3416	32.289510	172.24.16.4	172.24.19.254	ICMP	98	Echo (ping) request id=0x078e, seq=17/4352, ttl=64 (reply in 3417)
3417	32.328409	172.24.19.254	172.24.16.4	ICMP	98	Echo (ping) reply id=0x078e, seq=17/4352, ttl=255 (request in 3416)

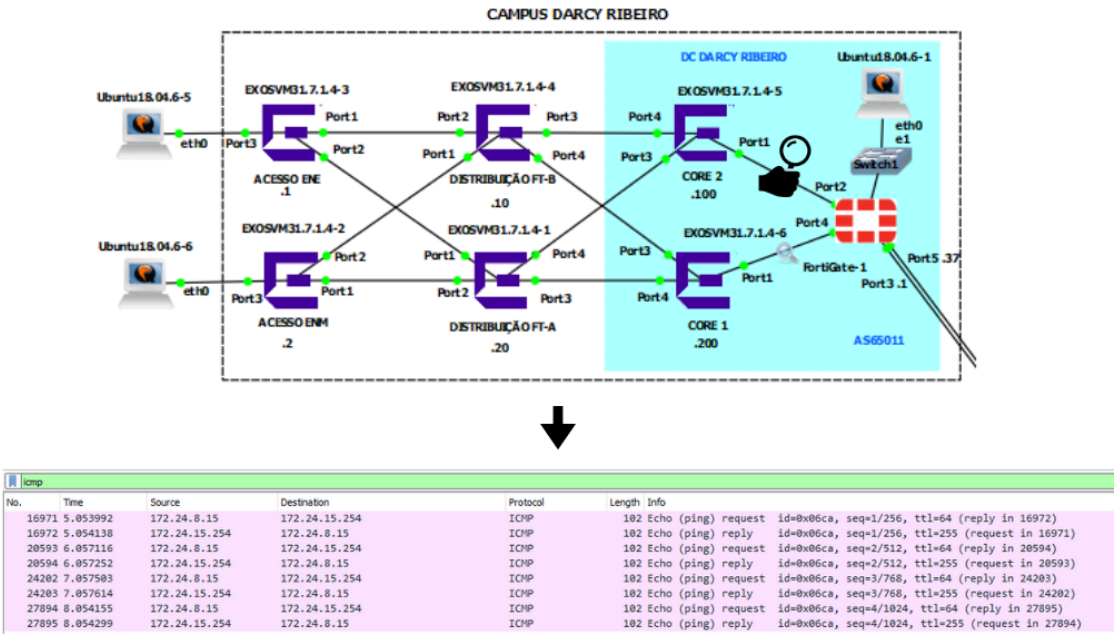
Figura 5.9: Pacotes capturados entre dispositivo da VLAN 20 e o *gateway* da VLAN 20, localizado no *firewall* FortiGate. Fonte própria.

É ainda importante ressaltar que, para fins de simplificação, a exposição dos testes juntamente com seus resultados estão contemplando os dispositivos pertencentes às VLAN 10 e 20, mas as mesmas conclusões se aplicam para os demais usuários que compõem as outras VLANs.

5.1.3 Teste de queda de *link* de redundância para o *firewall* utilizando o *sniffer* Wireshark

Na Figura 5.6 da seção 5.1.2, é possível verificar que a comunicação entre um dispositvo pertencente às VLANs internas consegue estabelecer uma conexão bem sucedida com o seu *gateway* correspondente, localizado no *firewall* FortiGate. Ao fazer a captura de pacotes, utilizando o *sniffer* Wireshark, nos *links* que interligam os *switches* Cores ao *firewall*, foi possível descobrir qual o *link* em que os pacotes ICMP, gerados pelo comando *ping* executado, estavam trafegando. A Figura 5.10 explicita qual o *link* que estava sendo analisado pelo *sniffer*, juntamente com os pacotes que foram capturados, indicando que o *link* entre a porta 2 do *switch* Core 2 e a porta 2 do *firewall* que estava sendo utilizado.

Porém, é imprescindível atestar que a conexão continuará ativa mesmo com a presença de uma eventual queda de *link*. Nas seções anteriores, foi apresentado a topologia e configurações realizadas na *intranet* de cada campus, de forma a oferecer redundância e alta disponibilidade



icmp

No.	Time	Source	Destination	Protocol	Length	Info
16971	5.053992	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x06ca, seq=1/256, ttl=64 (reply in 16972)
16972	5.054138	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x06ca, seq=1/256, ttl=255 (request in 16971)
20593	6.057116	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x06ca, seq=2/512, ttl=64 (reply in 20594)
20594	6.057252	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x06ca, seq=2/512, ttl=255 (request in 20593)
24202	7.057503	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x06ca, seq=3/768, ttl=64 (reply in 24203)
24203	7.057614	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x06ca, seq=3/768, ttl=255 (request in 24202)
27894	8.054155	172.24.8.15	172.24.15.254	ICMP	102	Echo (ping) request id=0x06ca, seq=4/1024, ttl=64 (reply in 27895)
27895	8.054299	172.24.15.254	172.24.8.15	ICMP	102	Echo (ping) reply id=0x06ca, seq=4/1024, ttl=255 (request in 27894)

Figura 5.10: *Link* de conexão com o *firewall*, no qual os pacotes originados na VLAN 10 foram encaminhados até o destino. Fonte própria.

para os ativos da rede. Sendo assim, para confirmar o funcionamento do ambiente configurado e sua confiabilidade, foi realizado a queda do *link* entre o *switch* Core 2 e o *firewall* FortiGate, assim como pode ser verificado na Figura 5.11.

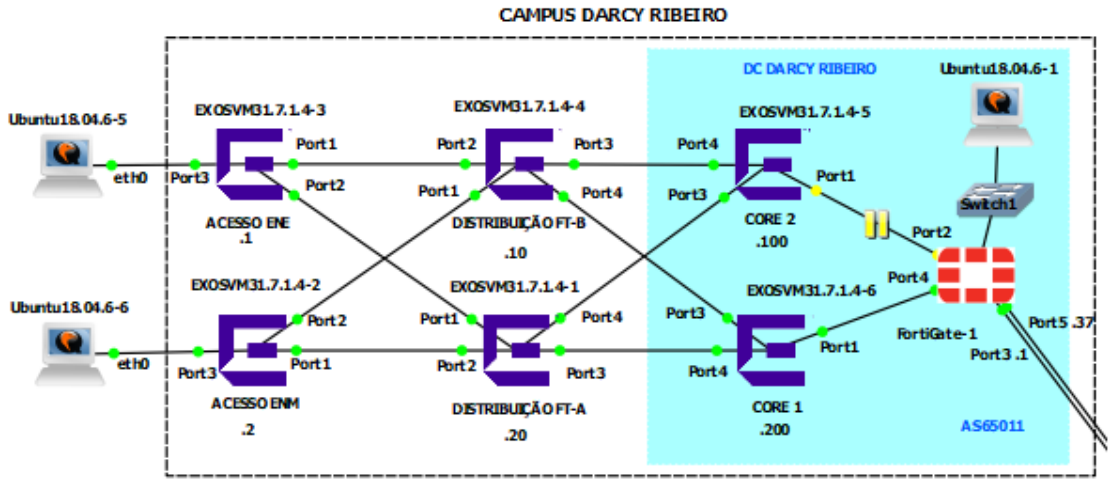


Figura 5.11: *Link*, onde os pacotes trafegavam, suspenso. Fonte própria.

Em seguida, após forçar a queda desse *link*, o comando *ping* com destino ao *gateway* da VLAN 10 foi executado no Ubuntu da VLAN 10 localizado na *intranet* do campus. Verificou-se, assim como mostra a Figura 5.12, que a conexão continuou ocorrendo normalmente.

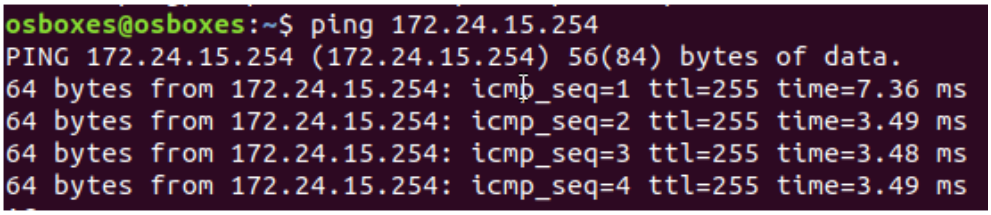


Figura 5.12: Conexão bem sucedida entre VLAN 10 e *gateway*, mesmo após queda do *link*. Fonte própria.

A realização deste teste, juntamente com a análise dos resultados, ajudou a comprovar que as configurações foram realizadas corretamente e tiveram um resultado satisfatório. Isso porque, mesmo em uma eventual queda de *link*, a infraestrutura de rede continuará operacional, provendo conexão entre seus ativos.

5.1.4 Comunicação entre os usuários da *intranet* - Regras de *Firewall*

A rede *intranet* de um campus deve garantir que os seus usuários internos consigam estabelecer comunicação entre si e isso é alcançado a partir de regras configuradas no *firewall*, que irão definir quais ativos possuem ou não autorização para se comunicar com outros ativos. Além de identificar os usuários finais baseado no endereço IP, ou range de endereços IPs, as regras de *firewall* possuem a capacidade de limitar os serviços que um usuário, ou grupo de usuário consegue, ter acesso. Mais informações referente aos serviços de rede que foram autorizados para cada grupo de usuários foram expostas na seção 4.3.4.

Nesta seção será verificado o estabelecimento da comunicação entre usuários da *intranet* e quais regras no *firewall* foram criadas de forma a permitir que essa comunicação ocorresse. Assim, a Figura 5.13 mostra que foi bem sucedido o comando *ping* executado no Ubuntu pertencente a VLAN 20, de endereço IP 172.24.16.4, com destino ao Ubuntu da VLAN 10, com endereço IP 172.24.8.15.

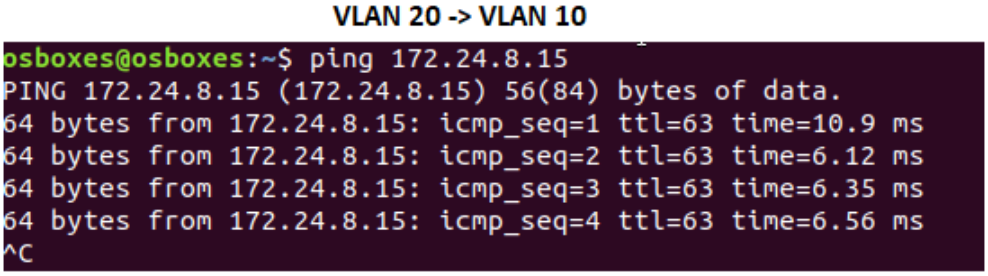


Figura 5.13: Conexão bem sucedida entre dispositivo da VLAN 20 e dispositivo da VLAN 10. Fonte própria.

Na interface gráfica do *firewall* FortiGate presente na *intranet* do campus Darcy Ribeiro é possível verificar as políticas de *firewall* que foram criadas para garantir que os usuários da intranet se comunicassem efetivamente entre si. A razão pela qual o comando *ping*, exposto na Figura 5.13, foi bem sucedido é que foi-se criada uma política no *firewall* de nome "VLAN20-VLAN10", de forma

a permitir o acesso de todo o tráfego originado na VLAN 20, com destino à VLAN 10, quando houver utilização dos serviços de “ALL_ICMP”, “DNS”, “HTTP”, “HTTPS” “UDP-TCP-VOIP e FTP”, como pode ser visualizado na Figura 5.14.

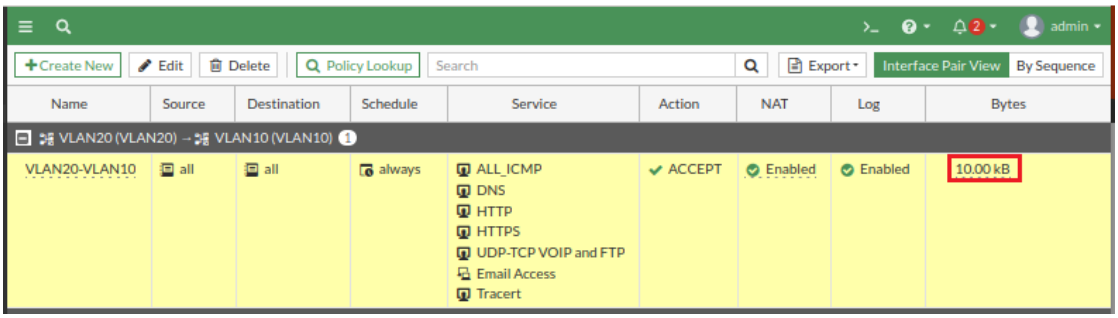


Figura 5.14: *Policy* criada para permitir comunicação entre dispositivos da VLAN 20 e VLAN 10. Fonte própria.

Portanto, como o comando *ping* executado utiliza pacotes do tipo ICMP, o *firewall* autorizou que houvesse esse fluxo de dados entre a origem e o destino. A Figura 5.14 ainda mostra em destaque a quantidade de dados que passou por essa política de *firewall* em específico, mostrando que o *firewall* além de permitir, armazena e detecta todo o tráfego que foi gerado referente a uma política em específico.

Da mesma maneira, foi bem sucedido o comando *ping* executado no Ubuntu pertencente a VLAN 10, de endereço IP 172.24.8.15, com destino ao Ubuntu da VLAN 20, com endereço IP 172.24.16.4, como pode ser visto na Figura 5.15. Nessa mesma Figura é exposto a política de *firewall* que foi criada de forma a permitir que a comunicação entre esses dois dispositivos ocorrese de maneira bem sucedida.

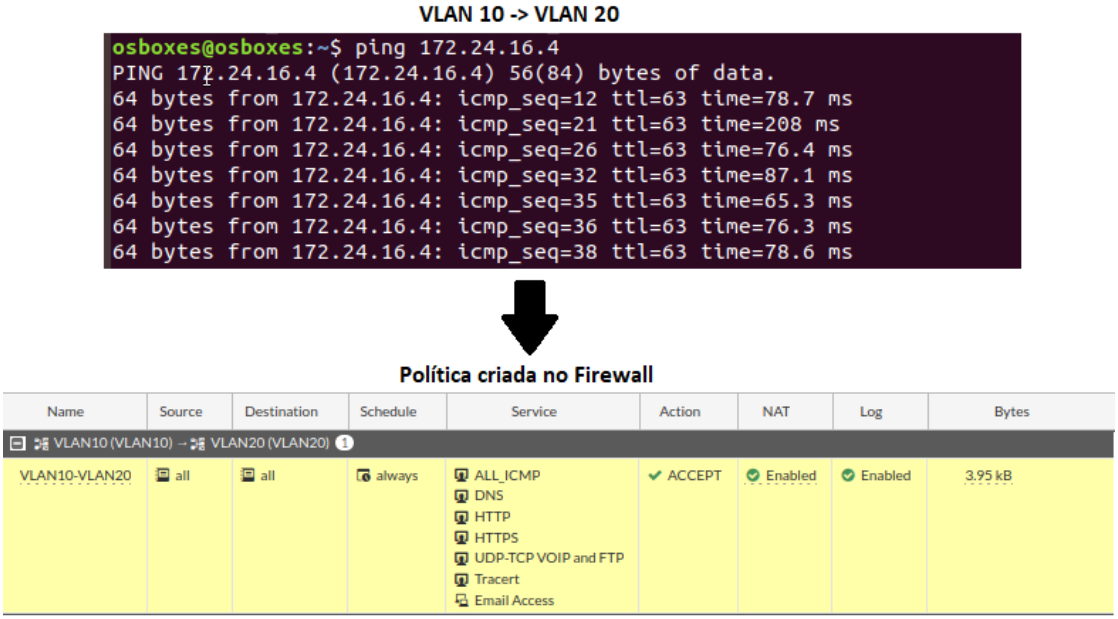


Figura 5.15: Conexão bem sucedida entre dispositivo da VLAN 10 e VLAN 20, juntamente com a *policy* criada para permitir essa comunicação. Fonte própria.

Observa-se que as duas políticas “VLAN20-VLAN-10” e “VLAN10-VLAN20” autorizam a utilização do serviço “*Tracert*” entre os usuários da *intranet*. Esse serviço foi inserido nas regras apenas para fins de teste, para que fosse possível realizar a verificação das rotas criadas entre os ativos da rede. A Figura 5.16 apresenta os detalhes desse serviço.

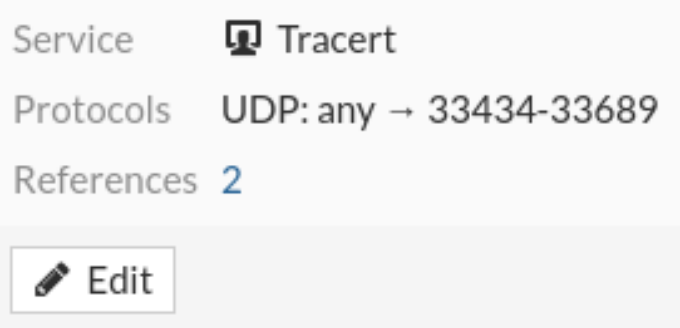


Figura 5.16: Serviço *traceroute* inserido nas regras para fins de teste. Fonte própria.

Na Figura 5.17 é exposto um exemplo de como esse comando pode ser utilizado, onde foi possível verificar qual foi o caminho percorrido no estabelecimento de comunicação entre o Ubuntu da VLAN 20 e o Ubuntu da VLAN 10. Percebe-se que primeiro o tráfego foi direcionado para o *gateway* da VLAN 20 para somente aí chegar no endereço IP do dispositivo pertecente à outra VLAN, neste caso, o endereço IP do Ubuntu presente na VLAN 10.

```
osboxes@osboxes:~$ traceroute 172.24.8.15
traceroute to 172.24.8.15 (172.24.8.15), 30 hops max, 60 byte packets
 1  _gateway (172.24.19.254)  10.527 ms  10.659 ms  11.124 ms
 2  172.24.8.15 (172.24.8.15)  19.127 ms  19.281 ms  19.534 ms
```

Figura 5.17: Serviço *traceroute* permite verificar o caminho percorrido pelo pacote ICMP dentro da *intranet*. Fonte própria.

Sendo assim, diante do exposto nas figuras e explicações acima, foi possível verificar e atestar a importância da criação e configuração das regras de políticas no *firewall*, de forma a garantir que a comunicação entre os ativos da rede ocorra dentro do esperado.

5.1.5 Iperf - Simulação de comunicação entre usuários da rede via FTP e VoIP

O iPerf, é um programa de linha de comando de plataforma cruzada de código aberto gratuito para realizar medições de taxa de transferência de rede em tempo real. Sendo assim é uma ferramenta que é comumente utilizada para criar fluxos de dados TCP e UDP, como também para a medição do *troughput* (taxa de transferência) de uma rede, métrica essa que permite avaliar a disponibilidade e capacidade da largura de banda em um *link*. Para observar o seu funcionamento na prática, esta seção traz como objetivo realizar a medição e análise da transmissão de dados que ocorrerão entre dois dispositivos presentes na topologia, nas comunicações FTP e VoIP. À seguir serão detalhados os passos dados para obter os resultados.

5.1.5.1 Configuração de rede dos computadores

No processo de transferência e recebimento de arquivos e também no caso da comunicação VoIP, funcionam dois protagonistas: o cliente e o servidor. Neste caso o papel do servidor é cumprido pelo Ubuntu destacado no item 1 da Figura 5.18, com IP 172.24.8.15/21 pertencente à VLAN 10 (GRADUAÇÃO), e o papel do cliente é o do Ubuntu destacado no item 2 da Figura 5.18, com IP 172.24.16.4/22 pertencente à VLAN 20 (PÓS GRADUAÇÃO).

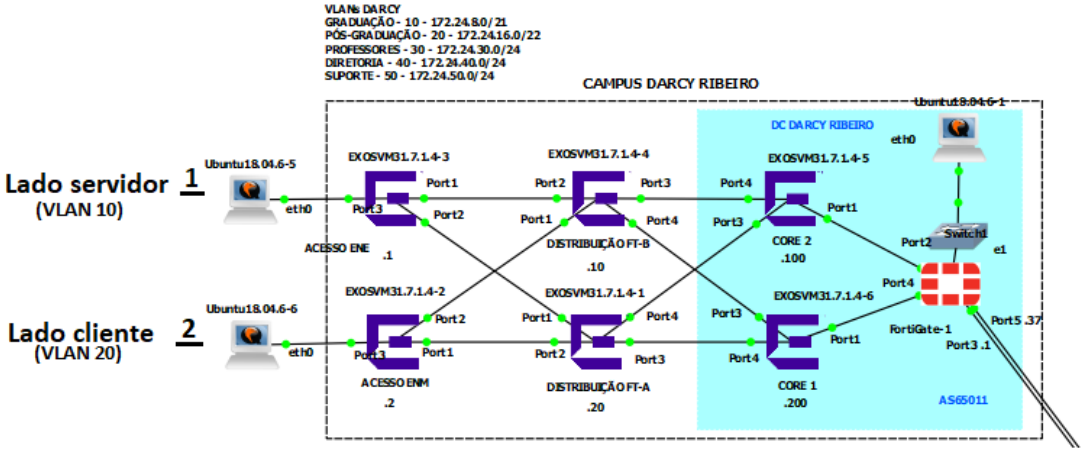


Figura 5.18: *Hosts* de diferentes VLANs escolhidos para estabelecer comunicação do tipo FTP e VOIP. Fonte própria.

A configuração de rede dos dois Ubuntus, foi realizado levando em consideração as VLANs, bem como *gateways* apropriados, de acordo com o que é mostrado nas Tabela 5.1.

Tabela 5.1: Endereços IPs utilizados para configurar os Ubuntus.

UBUNTU VLAN 10 (servidor)	
Endereço IP da interface de rede	**Endereço IP do Gateway**
172.24.8.15/21	172.24.15.254
UBUNTU VLAN 20 (cliente)	
Endereço IP da interface de rede	**Endereço IP do Gateway**
172.24.16.4/22	172.24.19.254

5.1.5.2 Simulação de Transferência de arquivo via FTP utilizando o Iperf

O Protocolo de Transferência de Arquivos (FTP - *File Transfer Protocol*), permite a troca de arquivos entre dois ativos conectados à Internet. Para ocorrer a troca de arquivo, considerando as informações expostas no tópico acima, foi realizado o seguinte comando no terminal do Ubuntu utilizado como cliente:

iperf -c 172.24.8.15 -P 1 -i 10 -m -p 5001 -w 8.0K -f K -t 60

A tabela 5.2 apresenta um detalhamento de todos os parâmetros que compõem esse comando

executado para a realização da troca do arquivo FTP, no lado do cliente PC-2:

Tabela 5.2: Tabela de detalhamento dos parâmetros utilizados no comando do Iperf no lado cliente.

Parâmetro	Descrição
-c	Indica que o iPerf está sendo rodado do lado do cliente.
172.24.8.15	IP do Ubuntu servidor
-P 1	Corresponde ao número de conexões simultâneas a serem feitas para o servidor. No caso foi 1 conexão.
-i 10	Indica o intervalo, em segundos, entre os anúncios de atualização, que nesse caso é de 10 segundos.
-m	Imprima o tamanho de TCP MSS relatado e os tamanhos de leitura observados que geralmente se correlacionam com o MSS. O MSS geralmente é o MTU - 40 bytes para o cabeçalho TCP/IP.
-p 5001	Indica a porta do servidor que escutará o cliente para se conectar. Por padrão é o 5001.
-w 8.0K	Define os tamanhos da janela do FTP, neste caso 8.0 Kbytes/s
-f K	Diz respeito ao formato a ser expresso a medida da largura de banda, que nesse caso é KBytes/segundo.
-t 60	O tempo em segundos para transmitir.

No lado do servidor, o seguinte comando de escuta foi realizado no terminal do Ubuntu configurado como sendo pertencente a VLAN 10:

iperf -s

Neste caso temos um único parâmetro, que é descrito na tabela 5.3:

Tabela 5.3: Tabela de detalhamento do parâmetros utilizados no comando do Iperf no lado servidor

Parâmetro	Descrição
-s	Indica que o iPerf está sendo rodado do lado do servidor.

Conforme é possível visualizar na Figura 5.19, após a execução do comando, o Ubuntu cliente (VLAN 20) passa a estar conectado com o servidor 172.24.8.15 pela porta 5001, como é possível ver no item 1 desta mesma imagem. Também é possível ver que o tamanho do *buffer* disponível para realizar a transferência que corresponde a 131 Kbit. A linha destacada pelo item 2 informa que o dispositivo local (Ubuntu cliente, VLAN 20) de endereço IP 172.24.16.4 estabeleceu uma conexão pela porta 55956 com a porta 5001 do dispositivo de endereço IP 172.24.8.15, ou seja, com o servidor.

Ao se iniciar o recebimento dos dados, é imprimido na tela uma série de informações a respeito do *status* da comunicação, de acordo com alguns parâmetros, como é visto no item 3. O parâmetro

"*Interval*", diz respeito ao intervalo de tempo, em segundos, que se passou desde o último anúncio de atualização. Na coluna "*Transfer*" é imprimido em cada linha a quantidade de dados que foi enviado naquele intervalo de tempo. "*Bandwitch*" diz respeito à largura de banda que foi utilizada naquele intervalo.

Por exemplo, na linha destacada no item 4, o intervalo de tempo em que aquela atualização foi imprimida foi entre "0-62 segundos", onde foram enviados o total de 180 Mbits de dados nesse período. A largura de banda foi de 2.90 Mbits/segundo, resultado esse já esperado pois resulta da divisão entre os parâmetros "*Transfer*" e "*Interval*".

Por fim, é possível visualizar na linha destacada pelo item 5, que o tamanho máximo do segmento (MSS) corresponde a 1448 *bytes*. O MSS corresponde geralmente ao tamanho do MTU - 40 *bytes*, devido ao tamanho do cabeçalho do TCP/IP. Essa informação foi imprimida como consequência do parâmetro "*-m*" digitado na linha de comando, que solicita que tal informação seja dada.

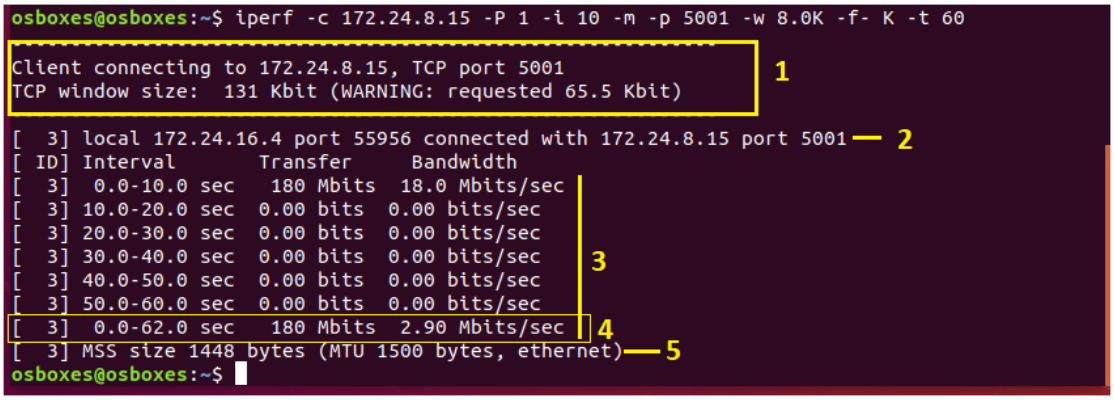


Figura 5.19: Resultado do comando executado do lado do cliente para iniciar comunicação FTP com o servidor. Fonte própria.

Já em se tratando do comportamento observado no terminal de comando do Ubuntu servidor (VLAN 10), como pode ser visto no item 1 da Figura 5.20, ele passa a estar disponível a receber os dados pela porta 5001, que é a porta padrão utilizada pelo servidor, ou seja, os dados enviados pelo cliente chegarão ao servidor pela porta 5001. O tamanho máximo suportado da janela TCP a ser enviada é de 128 Kbytes.

A linha destacada pelo item 2 informa que o dispositivo local (servidor, VLAN 10) de endereço IP 172.24.8.15 estabeleceu uma conexão pela porta 5001 com a porta 60394 do dispositivo de endereço IP 172.24.15.254, ou seja, com o *gateway* da VLAN 20, localizado no *firewall*. A partir desse momento, onde a conexão é estabelecida, o tráfego FTP será iniciado e, como visto na Figura 5.19, o cliente consegue receber todo o arquivo requisitado.

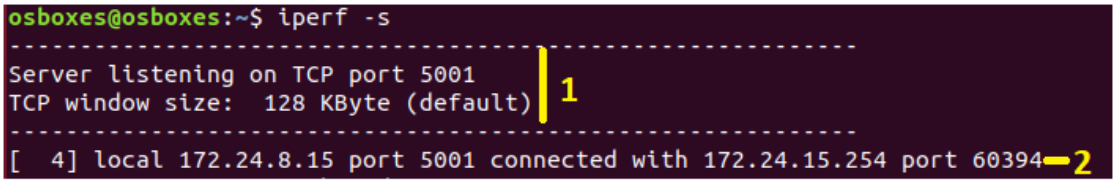


Figura 5.20: Resultado do comando executado do lado do cliente para iniciar comunicação FTP com o servidor. Fonte própria.

Ao acessar os *logs* gerados no *firewall* FortiGate, foi possível verificar que houve a detecção do *log* especificado na Figura 5.21, que indica que houve uma comunicação do tipo "UDP-TCP VOIP and FTP", partindo do servidor em direção ao cliente, entre a VLAN 20 e a VLAN 10. Ou seja, a comunicação ocorreu de maneira bem sucedida.

Date/Time		Source	Device	Destination	Application Name	Result	Policy ID
4 minutes ago		172.24.16.4	0c:ad:99:40:00:00	172.24.8.15	UDP-TCP VOIP and FTP	✔ 50.85 MB / 880.61 kB	VLAN20-VLAN10 (8)

Figura 5.21: Resultado do comando executado do lado do cliente para iniciar comunicação FTP com o servidor. Fonte própria.

5.1.5.3 Simulação de comunicação VOIP utilizando o Iperf

Para realização deste item do experimento, foi considerado as mesmas informações de Ubuntu servidor e Ubuntu cliente mostradas na Tabela 5.1. Estar ciente de qual é o lado servidor e qual é o lado cliente é muito importante para que a digitação dos comandos específicos, nos terminais de comando de cada dispositivo, seja realizada corretamente. Para iniciar, foi digitado no terminal de comando do Ubuntu cliente (VLAN 20) o comando apresentado na abaixo:

Iperf -c 172.24.8.15 -P 1 -i 10 -m -p 5001 -w 8.0K -f K -t 60

Observa-se que após "*iperf*" uma série de parâmetros são digitados, que especificarão as características da sessão que está sendo estabelecida. A Tabela 5.4 detalha do que se trata cada parâmetro digitado.

Tabela 5.4: Tabela de detalhamento dos parâmetros utilizados no comando do Iperf no lado cliente

Comando	Descrição
-c	Indica que o iPerf está sendo rodado do lado do cliente.
172.24.8.15	IP do Ubuntu servidor
-u	indica que será utilizado o UDP na sessão de transferência de dados
-b 64000	A largura de banda do pacote UDP a ser enviado, em bits/segundos.
-P 4	Corresponde ao número de conexões simultâneas a serem feitas para o servidor.
-f K	Diz respeito ao formato a ser expresso a medida da largura de banda, que nesse caso é KBytes/segundo.
-i 10	Indica o intervalo, em segundos, entre os anúncios de atualização, que nesse caso é de 10 segundos.
-t 60	Corresponde ao tempo total, em segundos, que a transmissão durará. Neste caso, 60 segundos.

No Ubuntu servidor (VLAN 10), o seguinte comando foi digitado e executado, para que fosse possível estabelecer a comunicação VoIP:

iperf -s -u -mss 160 -S 184 -P 4 -f K -i 10

Observa-se que após "*iperf*" uma série de parâmetros são digitados, que especificarão as características da sessão que está sendo estabelecida. A Tabela 5.5 detalha do que se trata cada parâmetro digitado.

Tabela 5.5: Tabela de detalhamento dos parâmetros utilizados no comando do Iperf no lado servidor

Comando	Descrição
-s	Indica que o iPerf está sendo rodado do lado do servidor.
-u	indica que será utilizado o UDP na sessão de transferência de dados
-mss 160	Corresponde ao tamanho máximo do segmento UDP em bytes, nesse caso 160 bytes
-S 184	O tipo de serviço utilizado nos pacotes.
-P 4	Corresponde ao número de conexões simultâneas a serem feitas para o servidor.
-f K	Diz respeito ao formato a ser expresso a medida da largura de banda, que nesse caso é KBytes/segundo.
-i 10	Indica o intervalo, em segundos, entre os anúncios de atualização , que nesse caso é de 10 segundos.

Após a execução desses comandos nos terminais do servidor e cliente, uma sessão de transferência de arquivo de voz se iniciou, ou seja, o lado do servidor e o lado do cliente passaram a imprimir periodicamente as atualizações referentes à transferência de dados que estava em andamento. Também foi possível monitorar os pacotes que começaram a transitar na rede após a execução de tais comandos.

O iPerf, em comunicações UDP, oferece uma série de recursos, como por exemplo, o cliente pode criar fluxos UDP especificando uma largura de banda. Também é possível fazer medições a respeito da perda de pacotes e dos atrasos na transmissão, dentre outras funcionalidades. Para iniciar, segue abaixo o que pôde ser observado nos *prompts* de comando dos dispositivos.

Conforme a Figura 5.22, após a execução do comando, o Ubuntu Servidor (VLAN 10) passa a estar disponível a receber os dados pela porta 5001, que é a porta padrão utilizada pelo servidor, ou seja, os dados enviados pelo cliente chegarão ao servidor pela porta 5001. Como é possível ver no item 1 desta mesma Figura, o servidor identifica que um pacote de 1470 *bytes* vai ser recebido. O "*UDP buffer size*", diz respeito ao tamanho do *buffer* de entrada, explicitando um limite máximo dos tamanhos de cada datagrama a ser recebido.

Enquanto a porta local do servidor "172.24.8.15" permanece sendo 5001 durante todo o período de duração da comunicação, as portas que foram utilizadas para que o cliente "172.24.16.4" envie os datagramas foram as 34821, 53072, 50130 e 4656 como pode ser visto no item 2 da Figura 5.22. Tais portas foram escolhidas à partir do parâmetro que foi especificado na linha de comando, ao ser definido que o cliente faria 4 conexões simultâneas para o servidor. Após ser informado a última porta, 50130, os dados começaram a ser recebidos, como é possível visualizar no item 3.

Ao iniciar o recebimento dos dados, é imprimido na tela uma série de informações a respeito do *status* da comunicação, de acordo com alguns parâmetros. O parâmetro "*Interval*", diz respeito ao intervalo de tempo, em segundos, que se passou desde o último anúncio de atualização. Na coluna "*Transfer*" é imprimido em cada linha a quantidade, em KBytes, de dados que foi recebido naquele intervalo de tempo. "*Bandwitch*" diz respeito à largura de banda que foi utilizada naquele momento.

Por exemplo, na linha em destaque no item 4 da Figura 5.22, o intervalo de tempo que decorreu desde a última atualização de anúncio corresponde à 10 segundos, sendo que foram recebidos 80.4 Kbytes de dados nesse período. A largura de banda foi a de 8.04 Kbytes/segundo, resultado esse já esperado pois resulta da divisão entre os parâmetros "*Transfer*" e "*Interval*".

Por fim, é possível visualizar, ao fim da linha destacada pelo item 3, que após os 60 segundos, que foi o tempo total definido para a transmissão de dados, foi recebido um total de 1414 Kbytes de dados.

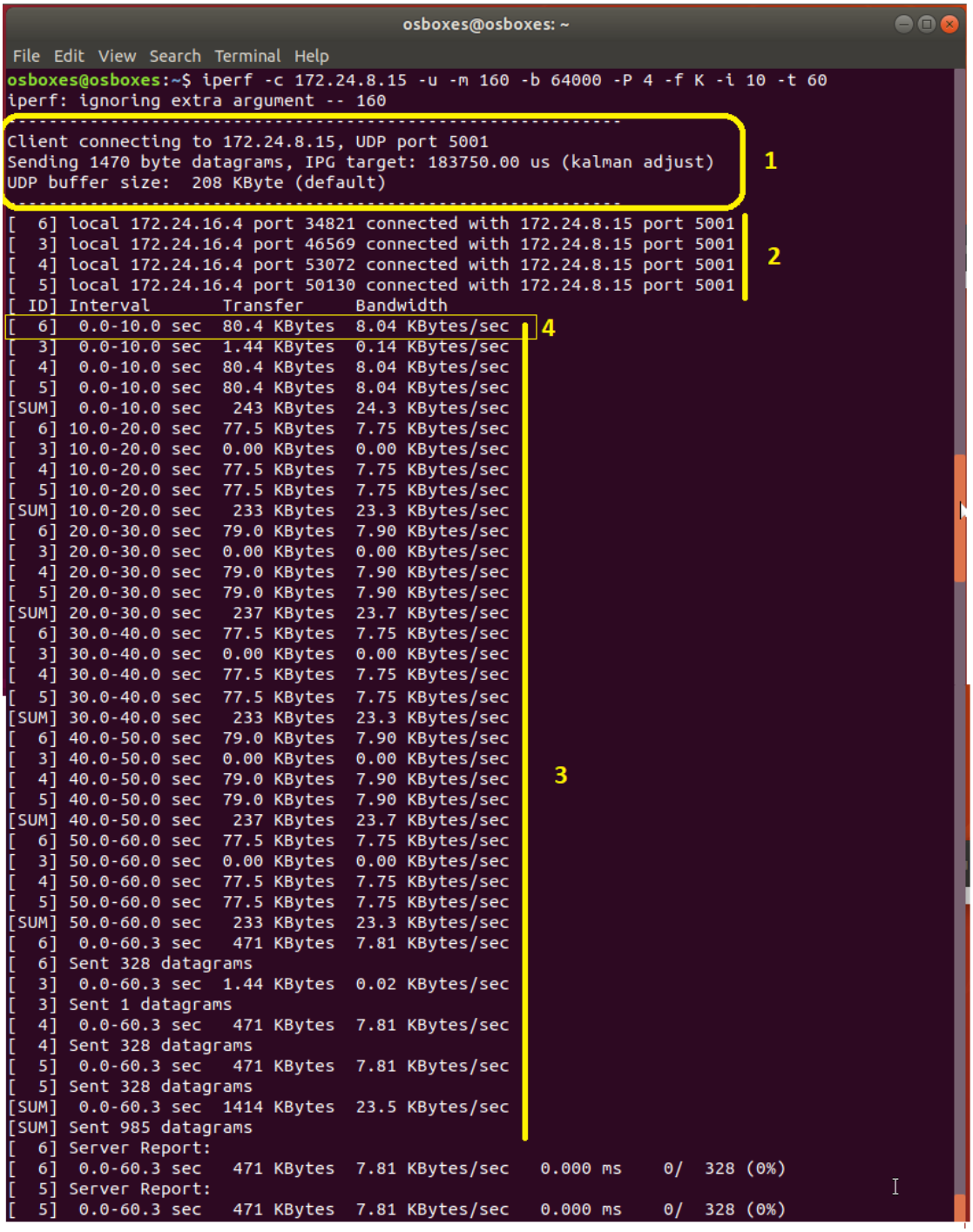


Figura 5.22: Comportamento observado no terminal onde foi executado o comando Iperf-VoIP do lado cliente. Fonte própria.

Na Figura 5.23 é possível visualizar qual foi o comportamento observado no terminal de comando do Ubuntu servidor (VLAN 10) após a execução do comando, onde o Ubuntu cliente (VLAN 20) passa a estar conectado com o servidor 172.24.8.15 pela porta 5001, como é possível ver no item 1 desta mesma Figura. Também é possível ver que o tamanho dos datagramas a serem enviados corresponde a 1470 *bytes*.

Enquanto a porta local do servidor "172.24.8.15" permanece sendo 5001 durante todo o período de tempo que durar a comunicação, as portas que foram utilizadas para que o cliente "172.24.16.4" envie os datagramas foram as 34821, 53072, 50130 e 46569, como pode ser visto no item 2 da Figura 5.23. Tais portas foram escolhidas à partir do parâmetro que foi especificado na linha de comando, ao ser definido que o cliente faria 4 conexões simultâneas para o servidor. Após ser informado a última porta, 46569, os dados começaram a ser enviados, como é possível visualizar no item 3.

Ao iniciar o envio dos dados, é impresso na tela uma série de informações a respeito do *status* da comunicação, de acordo com alguns parâmetros.Além dos parâmetros explicados anteriormente,tem também o parâmetro "*Jitter*", que vai informar o tempo de trânsito total relativo que aquele pacote demorou para se deslocar do cliente até o servidor, à partir do cálculo que subtrai a hora que o servidor recebeu da hora que o cliente enviou.

Por fim, o último parâmetro "*Lost/Total Datagrams*" vai informar se e quantos datagramas foram perdidos e qual a quantidade total de datagramas que foram enviados. O servidor vai detectar a perda de datagramas UDP a partir do ID dos datagramas. Como geralmente um único datagrama UDP se transforma em vários pacotes IP, a perda de um pacote IP vai ocasionar a perda de todo o datagrama UDP.

Por exemplo, na linha em destaque no item 4 da Figura 5.23, o intervalo de tempo que decorreu desde a última atualização de anúncio corresponde à 10 segundos, sendo que foram enviados 79.0 Kbytes de dados nesse período. A largura de banda foi a de 7.90 Kbytes/segundo, resultado esse já esperado pois resulta da divisão entre os parâmetros "*Transfer*" e "*Interval*". O Jitter, ou seja, o tempo total que esses dados foram recebidos correspondeu a 0.387ms. No parâmetro "Lost/Total Datagrams" é possível ver que nenhum pacote foi perdido dentre os 55 que foram recebidos com sucesso, tendo uma porcentagem de pacotes perdidos de 0%.

Por fim, é possível visualizar, na última linha do item 3, que após os 60 segundos, que foi o tempo total definido para a transmissão de dados, a quantidade de dados totais enviados foi a de 2196 Kbytes.

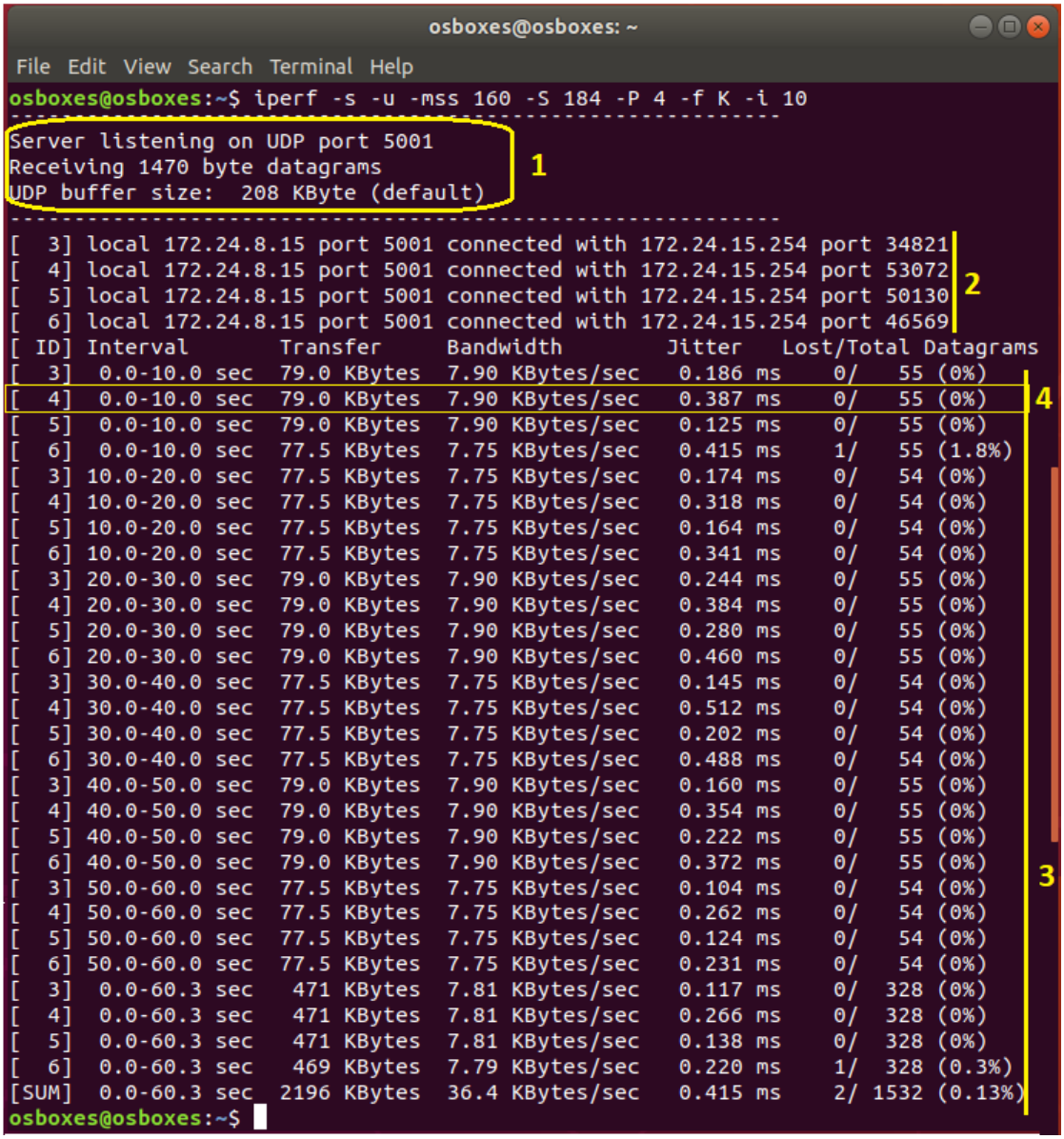


Figura 5.23: Comportamento observado no terminal onde foi executado o comando Iperf-VoIP do lado servidor. Fonte própria.

5.2 Rede *Backbone* da Provedora

Com a configuração do *Backbone* da provedora, conforme as etapas descritas no capítulo 4, é possível realizar algumas análises a fim de observar o funcionamento e conectividade da tecnologia MPLS L3VPN. Além disso, a redundância obtida através dos *links* físicos, bem como através dos roteadores da provedora, ao configurar o protocolo HSRP serão analisados a partir de testes de queda da conexão. Dessa maneira, os resultados desta etapa do projeto serão divididos em alguns subtópicos para obter melhor compreensão sobre o assunto.

5.2.1 Análises referentes à configuração da rede MPLS (OSPF + LDP)

Após a definição dos endereçamentos IPs das interfaces dos roteadores, a primeira etapa para a configuração da tecnologia MPLS L3VPN é configurar a rede MPLS de maneira funcional, no qual os roteadores do *backbone* são capazes de realizar roteamento entre eles a partir do protocolo de roteamento dinâmico OSPF, e para que os *labels* MPLS sejam gerados e distribuídos entre os roteadores, o protocolo LDP é configurado. Dessa maneira, a Figura 5.24 expõe as configurações desta etapa de implementação, para os quatro roteadores presentes na topologia.

Roteador de borda da provedora (R1)

```
router ospf 10
 mpls ldp autoconfig
 router-id 1.1.1.1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
```

Roteador de borda da provedora (R4)

```
router ospf 10
 mpls ldp autoconfig
 router-id 4.4.4.4
 log-adjacency-changes
 network 4.4.4.4 0.0.0.0 area 0
 network 10.0.0.20 0.0.0.3 area 0
 network 10.0.0.24 0.0.0.3 area 0
```

Roteador da provedora (R2)

```
router ospf 10
 mpls ldp autoconfig
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.16 0.0.0.3 area 0
 network 10.0.0.20 0.0.0.3 area 0
```

Roteador da provedora (R3)

```
router ospf 10
 mpls ldp autoconfig
 router-id 3.3.3.3
 log-adjacency-changes
 network 3.3.3.3 0.0.0.0 area 0
 network 10.0.0.12 0.0.0.3 area 0
 network 10.0.0.16 0.0.0.3 area 0
 network 10.0.0.24 0.0.0.3 area 0
```

Figura 5.24: Configurações realizadas no *backbone* da provedora referente à solução MPLS (OSPF + LDP). Fonte própria.

(a) **Análises do protocolo OSPF**

A partir disso, com a configuração do protocolo de roteamento OSPF, o roteador cria pacotes do tipo "*Hello*" que são então trocados periodicamente entre vizinhos diretamente conectados a fim de descobrir e manter relacionamento de adjacência, além disso são enviados informações como prioridades, estado dos roteadores, informações da área, entre outros dados. Dessa maneira, os roteadores adjacentes encaminham mensagens "*Hello*" para verificação da disponibilidade, mensagens LSAs (*Link-State Advertisements*) com avisos sobre o estado de conexão e atualizações da rede, e mensagens de *refresh* de cada LSA, a cada 30 minutos, para certificar que a tabela de dados OSPF esteja sincronizada. Após a sincronização de informações, os roteadores de uma mesma área terão a mesma visão da topologia de redes e então poderão obter o melhor caminho para um determinado destino a partir do algoritmo SPF (DIAS, 2013).

É possível verificar a estrutura de dados do vizinho OSPF a partir do comando "*show ip ospf neighbor*", conforme pode ser observado na Figura 5.25, para cada um dos roteadores.

Com este comando, é possível observar os vizinhos no qual os roteadores criaram adjacência, a prioridade, o estado de cada vizinho, *Dead Time*, o endereço dessa adjacência,

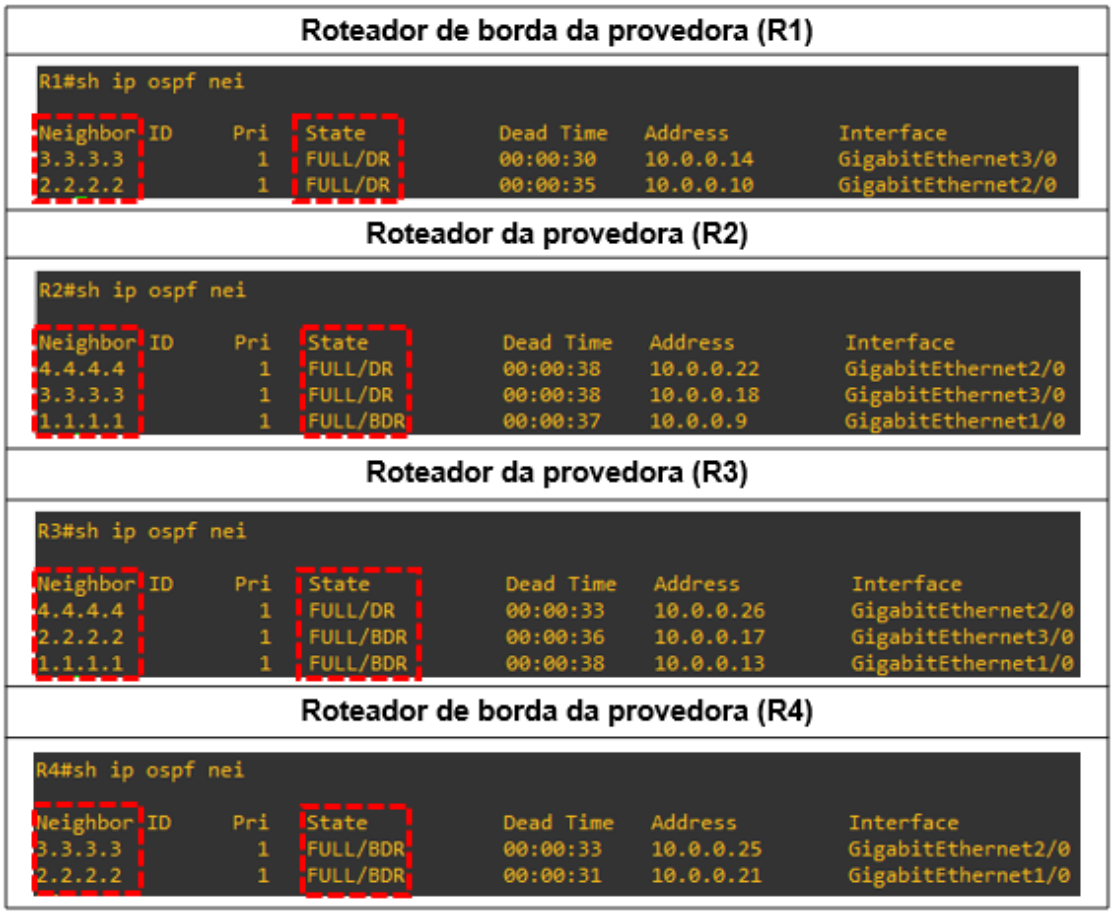


Figura 5.25: Estrutua de dados dos vizinhos OSPF de cada roteador do *backcbone*. Fonte própria.

como também a interface de saída para alcançá-lo.

Em redes de acesso múltiplo, ou seja, redes que suportam mais de dois roteadores, o OSPF elege dois tipos de estados para estes dispositivos: Um roteador designado, do inglês *Designated Router* (DR), que possui a função de gerar as mensagens LSAs para toda a rede multiacesso a fim de diminuir o tráfego e o tamanho da base de dados. E o roteador designado substituto, do inglês *Backup Designated Router* (BDR), que assumirá caso haja falha no roteador DR, falha no processo OSPF ou falha na interface multi-acesso no DR.

Sendo assim, para exemplificar, como pode ser observado na Figura 5.25, o roteador R1 forma adjacência com os roteadores R2 e R3 que possuem como *Router-ID* os endereços 2.2.2.2 e 3.3.3.3, respectivamente. O campo "*Pri*" se refere a prioridade do roteador vizinho. O roteador R2 (2.2.2.2) e R3 neste caso foram definidos como roteadores designados. O estado "*FULL*" significa que o roteador é totalmente adjacente com seus vizinhos e que o banco de dados do roteador está totalmente sincronizado. O campo "*Dead Time*" indica o período de tempo restante que o roteador aguarda para receber um pacote de saudação de OSPF do vizinho antes de declarar que este está inativo. Além disso, é possível observar os endereços IP e a interface correspondente a cada um dos vizinhos que formaram adjacências.

É possível ainda identificar as tabelas de roteamento de cada roteador, a partir do

comando "*show ip route*" que tem como objetivo exibir as atualizações dinâmicas da tabela de roteamento armazenada na memória RAM, apresentando as redes conhecidas, o código que indica como a informação foi obtida e a distância administrativa (preferência de rotas) deste roteador.

A Figura 5.26 abaixo, exibe a saída do comando "*show ip route*" do roteador R1 a fim de apresentar de maneira detalhada as informações presentes neste comando. Verifica-se que as redes diretamente conectadas a esse roteador e suas respectivas interfaces correspondentes, são representadas com o código "C". Já as redes aprendidas através do protocolo OSPF, são definidas com o código "O" e possuem distância administrativa igual a 110. Além disso, para redes que possuem mais de um caminho para um certo destino, como é o caso do IP 4.4.4.4 (roteador R4), a tabela, então, apresentará qual o endereço de próximo salto para os dois caminhos e suas respectivas interfaces de saída. O algoritmo SPF decidirá qual o caminho ideal para transmitir os pacotes enviados por este roteador.

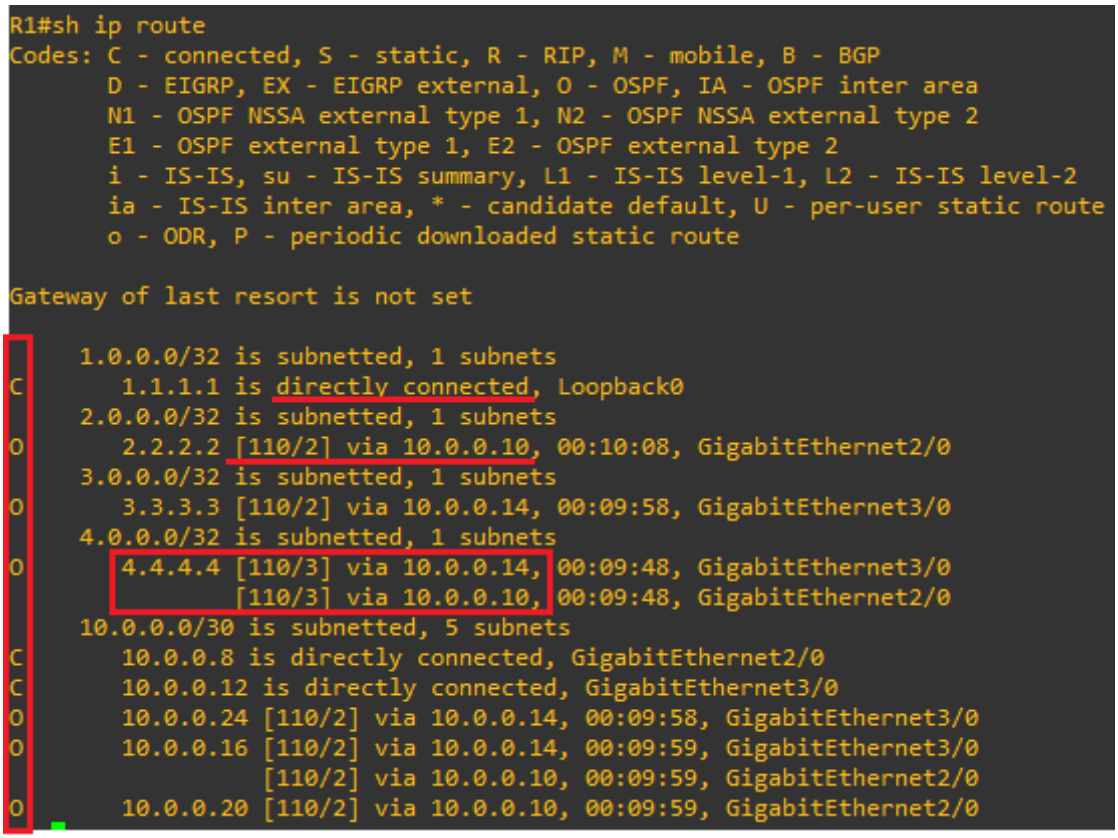


Figura 5.26: Identificação da tabela de roteamento do roteador R1. Fonte própria.

Dessa maneira, é validado que ao configurar o protocolo de roteamento OSPF de maneira correta, os roteadores do *backbone* possuem conectividade entre si. A Figura 5.27 exemplifica um *ping* partindo do roteador R1 para uma interface presente no roteador R4 com IP 10.0.0.22, para provar essa conexão.

```
R1#ping 10.0.0.22

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.22, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/32 ms
```

Figura 5.27: Verificação da comunicação entre os roteadores R1 e R4 através do comando "*ping*". Fonte própria.

(b) **Análises da tecnologia MPLS (LDP)**

Com a infraestrutura IP configurada e com todos os roteadores tendo conectividade com todas as redes da topologia devido à configuração do roteamento OSPF, é possível analisar a implementação do protocolo LDP de maneira dinâmica no qual foi utilizado o comando "*mpls ldp autoconfig*", conforme descrito no capítulo anterior.

O protocolo LDP é utilizado para estabelecer LSPs dinamicamente, no qual os LSRs da topologia MPLS poderão mapear as informações de roteamento da camada de rede para caminhos de comutação da camada de enlace. Sendo assim, o papel do LDP é focado em realizar a distribuição de rótulos, ou também chamados de *labels* MPLS, a depender de um *Interior Gateway Protocol* (IGP) para realizar as decisões de roteamento, no qual para este caso, o protocolo OSPF foi utilizado (FREITAS, 2013).

Este protocolo utiliza o mecanismo de codificação *Type-Length-Value* (TLV) para encaminhar as informações. A Figura 5.28 ilustra os componentes presentes neste mecanismo. O Tipo, do inglês *Type*, composto por 2 *bytes*, identifica qual informação está sendo trocada e informa como deve ser realizado o restante da decodificação da informação. O Valor, do inglês *Value*, se refere a informação que será decodificada. Por fim, o Comprimento, do inglês *Length*, é o delimitador da informação (FREITAS, 2013).

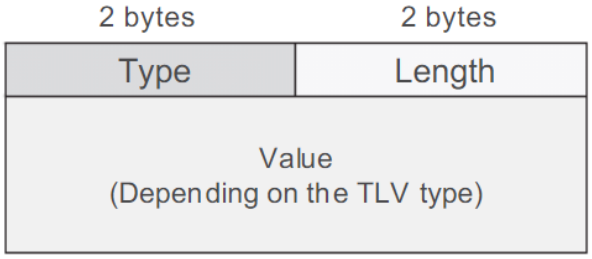


Figura 5.28: Estrutura do mecanismo TLV. Fonte: (ESTEBAN, 2023)

Para que seja possível trocar informações de *labels* MPLS para construir os LSPs, um roteador deve fazer a descoberta dos outros elementos na rede. Dessa maneira, o LDP realiza essa descoberta através do envio de pacotes "*Hello*" em todas as interfaces com o protocolo habilitado (FREITAS, 2013).

Sendo assim, é possível verificar as informações de sessões LDP formadas com seus vizinhos, através do comando "*show mpls ldp neighbor*". A saída desse comando para o roteador R1 pode ser observado na Figura 5.29.

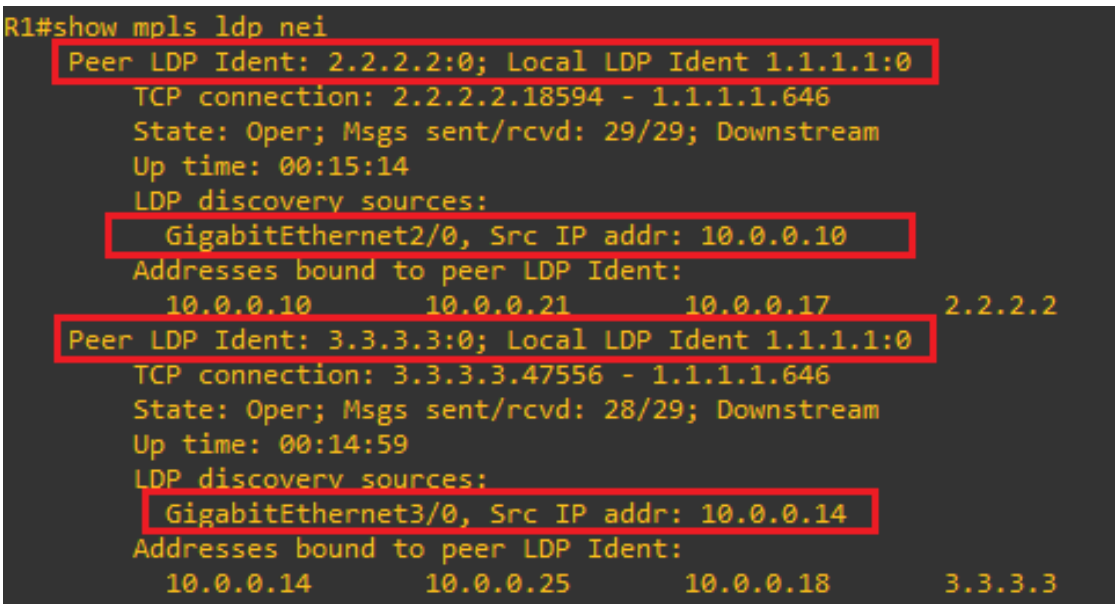


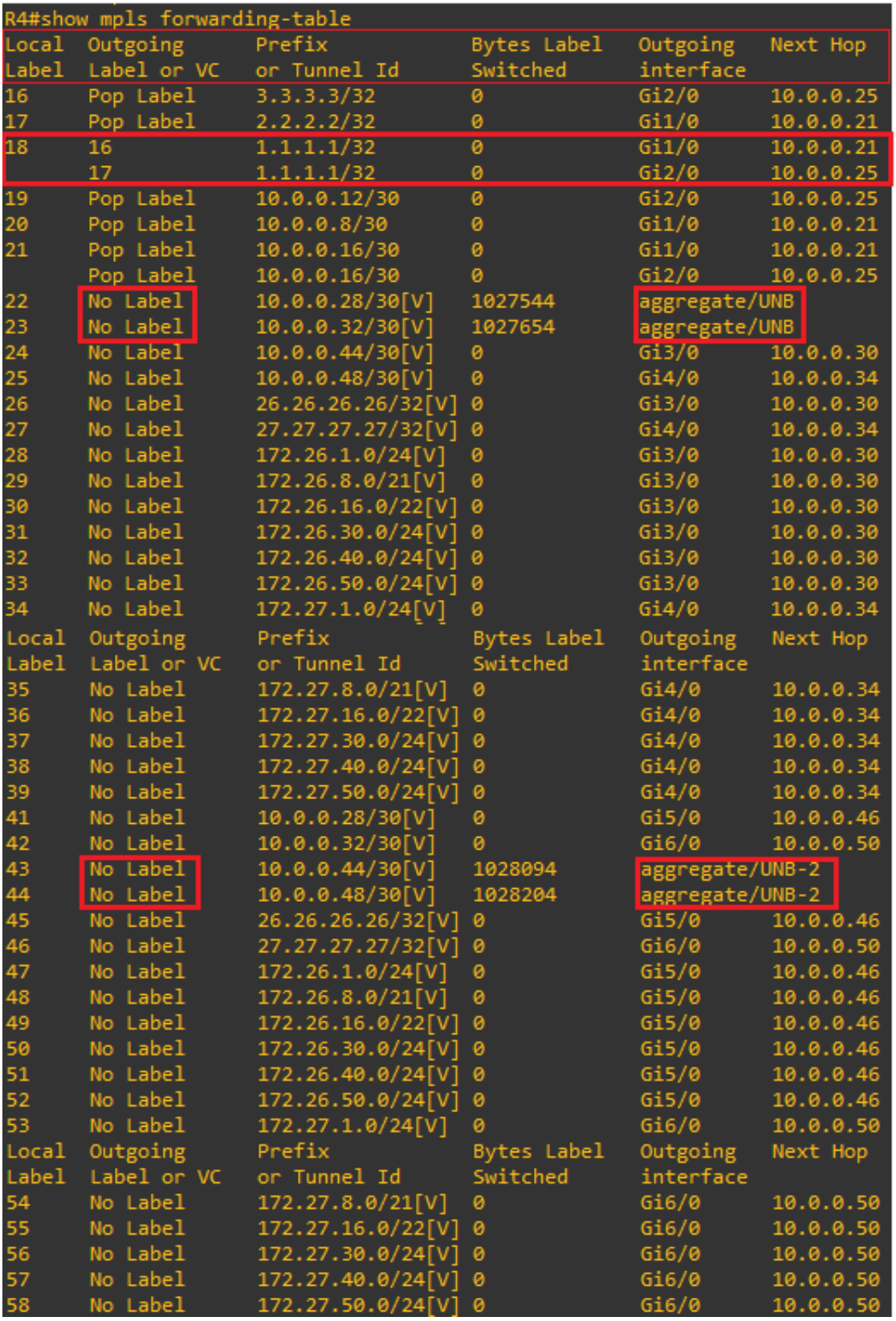
Figura 5.29: Saída do comando "*show mpls ldp neighbor*"no roteador R1. Fonte própria.

A partir desse comando é possível observar que o roteador R1 fez a descoberta dos dois roteadores adjacentes, sendo o R2 com *Loopback* 2.2.2.2 e R3 com *Loopback* 3.3.3.3. Além disso é também informado as origens para se alcançar cada vizinho, sendo que a interface *Gigabit Ethernet* 2/0 com endereço IP de origem 10.0.0.10 é utilizado para alcançar o roteador R2, e a interface *Gigabit Ethernet* 3/0 com endereço IP de origem 10.0.0.14 é utilizado para alcançar o roteador R3.

Com as sessões formadas, é possível verificar os LSPs formados a partir da base de informações de encaminhamento de rótulos MPLS (LFIB), através do comando "*show mpls forwarding-table*". É possível verificar um exemplo de saída deste comando na Figura 5.30, referente ao roteador R4.

Nesta Figura, a coluna "*Local Label*" se refere ao rótulo/*tag* que este LSR atribui e distribui aos outros LSRs. Sendo assim, o roteador R4 espera que pacotes rotulados cheguem até ele com estes *labels*. A coluna "*Outgoing Label*" se refere ao rótulo de saída que será atribuído ao pacote para alcançar um determinado destino. Ainda é possível verificar que as redes aprendidas através das VRFs UNB e UNB-2, não possuem *labels* de saída, já que o MPLS é configurado apenas no *backbone* da provedora, não alcançando os clientes.

Para compreender da melhor forma o funcionamento desta tabela de encaminhamento MPLS, o cenário presente na Figura 5.31 será utilizado como exemplo, no qual o roteador de borda R4, definido como origem neste caso, é conhecido por ser o "*Ingress LSR*", no qual recebe pacotes dos clientes que não possuem *label*, insere um rótulo na sua pilha e então o encaminha para o próximo salto. O próximo salto, neste caso, será o roteador R2 ou R3, no qual são chamados de "*Intermediate LSR*", que recebem um pacote com uma *label*, realizam a troca dos rótulos e então encaminham para o próximo salto, que será o roteador de borda R1, definido como o dispositivo de destino e é conhecido por ser o "*Egress LSR*", no qual recebe um pacote já com uma *label*, a remove e então envia para o cliente correto.



```
R4#show mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     3.3.3.3/32       0             Gi2/0       10.0.0.25
17     Pop Label     2.2.2.2/32       0             Gi1/0       10.0.0.21
18     16            1.1.1.1/32       0             Gi1/0       10.0.0.21
       17            1.1.1.1/32       0             Gi2/0       10.0.0.25
19     Pop Label     10.0.0.12/30     0             Gi2/0       10.0.0.25
20     Pop Label     10.0.0.8/30      0             Gi1/0       10.0.0.21
21     Pop Label     10.0.0.16/30     0             Gi1/0       10.0.0.21
       Pop Label     10.0.0.16/30     0             Gi2/0       10.0.0.25
22     No Label      10.0.0.28/30[V]  1027544       aggregate/UNB
23     No Label      10.0.0.32/30[V]  1027654       aggregate/UNB
24     No Label      10.0.0.44/30[V]  0             Gi3/0       10.0.0.30
25     No Label      10.0.0.48/30[V]  0             Gi4/0       10.0.0.34
26     No Label      26.26.26.26/32[V] 0            Gi3/0       10.0.0.30
27     No Label      27.27.27.27/32[V] 0            Gi4/0       10.0.0.34
28     No Label      172.26.1.0/24[V] 0             Gi3/0       10.0.0.30
29     No Label      172.26.8.0/21[V] 0             Gi3/0       10.0.0.30
30     No Label      172.26.16.0/22[V] 0            Gi3/0       10.0.0.30
31     No Label      172.26.30.0/24[V] 0            Gi3/0       10.0.0.30
32     No Label      172.26.40.0/24[V] 0            Gi3/0       10.0.0.30
33     No Label      172.26.50.0/24[V] 0            Gi3/0       10.0.0.30
34     No Label      172.27.1.0/24[V] 0             Gi4/0       10.0.0.34
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
35     No Label      172.27.8.0/21[V] 0             Gi4/0       10.0.0.34
36     No Label      172.27.16.0/22[V] 0            Gi4/0       10.0.0.34
37     No Label      172.27.30.0/24[V] 0            Gi4/0       10.0.0.34
38     No Label      172.27.40.0/24[V] 0            Gi4/0       10.0.0.34
39     No Label      172.27.50.0/24[V] 0            Gi4/0       10.0.0.34
41     No Label      10.0.0.28/30[V]  0             Gi5/0       10.0.0.46
42     No Label      10.0.0.32/30[V]  0             Gi6/0       10.0.0.50
43     No Label      10.0.0.44/30[V]  1028094       aggregate/UNB-2
44     No Label      10.0.0.48/30[V]  1028204       aggregate/UNB-2
45     No Label      26.26.26.26/32[V] 0            Gi5/0       10.0.0.46
46     No Label      27.27.27.27/32[V] 0            Gi6/0       10.0.0.50
47     No Label      172.26.1.0/24[V] 0             Gi5/0       10.0.0.46
48     No Label      172.26.8.0/21[V] 0             Gi5/0       10.0.0.46
49     No Label      172.26.16.0/22[V] 0            Gi5/0       10.0.0.46
50     No Label      172.26.30.0/24[V] 0            Gi5/0       10.0.0.46
51     No Label      172.26.40.0/24[V] 0            Gi5/0       10.0.0.46
52     No Label      172.26.50.0/24[V] 0            Gi5/0       10.0.0.46
53     No Label      172.27.1.0/24[V] 0             Gi6/0       10.0.0.50
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
54     No Label      172.27.8.0/21[V] 0             Gi6/0       10.0.0.50
55     No Label      172.27.16.0/22[V] 0            Gi6/0       10.0.0.50
56     No Label      172.27.30.0/24[V] 0            Gi6/0       10.0.0.50
57     No Label      172.27.40.0/24[V] 0            Gi6/0       10.0.0.50
58     No Label      172.27.50.0/24[V] 0            Gi6/0       10.0.0.50
```

Figura 5.30: Saída do comando "*show mpls forwarding-table*"no roteador R4. Fonte própria.

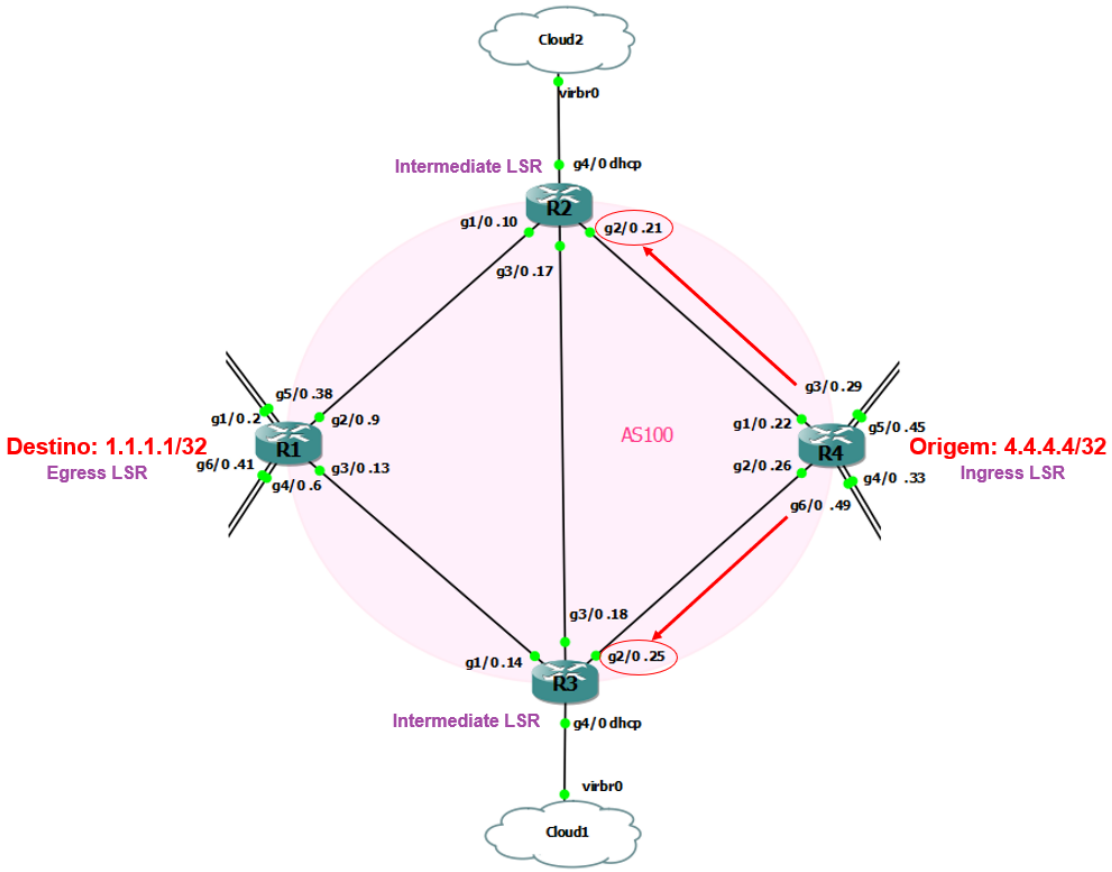


Figura 5.31: Cenário para compreensão da tabela de encaminhamento MPLS. Fonte própria.

Dessa maneira, o roteador R4 ao enviar um pacote para o roteador R1 que possui endereço de *Loopback* 1.1.1.1/32, dois caminhos (LSPs) serão possíveis, através da interface Gi1/0 ou Gi2/0, no qual o próximo salto são respectivamente, o IP 10.0.0.21 que corresponde ao roteador R2, ou o IP 10.0.0.25 que corresponde ao roteador R3. Neste caso, conforme a Figura 5.30, o "*Local Label*" que o LSR irá atribuir será o rótulo "18". Caso o encaminhamento seja definido como sendo por Gi1/0, o *label* de saída para este destino será o *label* "16". E caso o encaminhamento seja por Gi2/0, o *label* de saída será definido como "17".

Dessa maneira, para exemplificar, caso o pacote saia do roteador R4 com destino ao IP 10.0.0.21 com o label 16 para o roteador R2, verifica-se a saída do mesmo comando "*show mpls forwarding-table*" neste roteador, a partir da Figura 5.32.

Nota-se que o pacote que chega com o rótulo 16, com destino ao roteador R1 que possui o endereço *Loopback* 1.1.1.1, chegará ao destino a partir da interface Gi1/0 com IP de próximo salto 10.0.0.9. A coluna "*Outgoing Label*" apresenta o processo de *Pop Label*, isso significa que ao chegar o *label* 16 no roteador R2 ela irá remover o *label* visto que o próximo roteador será o "*Egress LSR*" na topologia MPLS. Sendo assim, o campo "*Local Label*" ao chegar no destino (R1) não possuirá nenhum valor. A remoção da *label* no penúltimo roteador é conhecida como PHP, do inglês *Penultimate Hop Popping*.

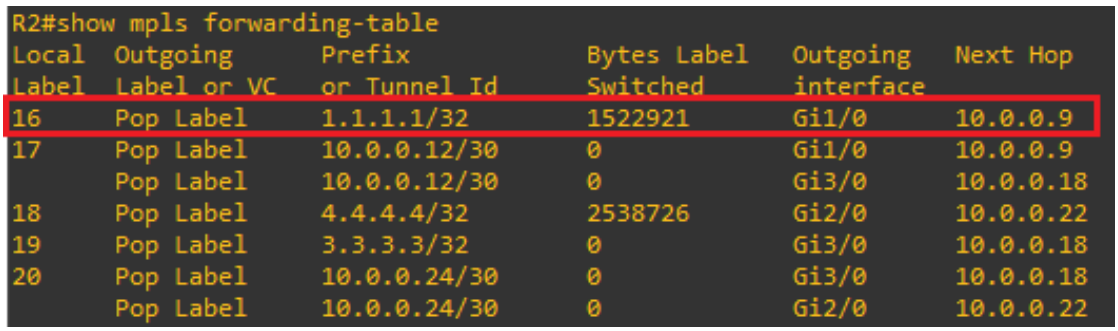


Figura 5.32: Saída do comando "*show mpls forwarding-table*"no roteador R2. Fonte própria.

É possível ainda verificar a rota pelos pacotes em uma rede MPLS através do comando "*traceroute mpls ipv4 x.x.x.x/x*", no qual o endereço inserido se refere ao destino que deseja alcançar, conforme ilustrado pela Figura 5.33.

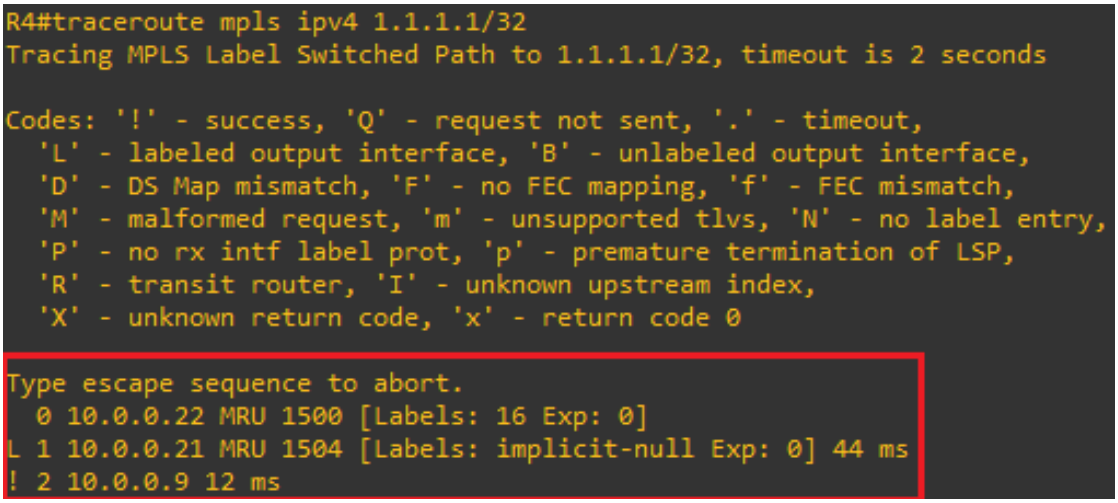


Figura 5.33: Resultado do comando "*traceroute mpls ipv4 1.1.1.1/32*"partindo do roteador R4 com destino ao roteador R1. Fonte própria.

Como já foi citado, o mecanismo básico de descoberta de vizinhos LSRs do LDP é a partir do envio de mensagens *Hello* através das interfaces habilitadas.

Para exemplificar o fluxo de mensagens *Hello*, utilizou-se o *sniffer* Wireshark para a captura de pacotes na interface que interconecta os roteadores R1 e R3, conforme pode ser observado na Figura 5.34.

Ao aplicar o filtro de pacotes LDP, verificou-se mensagens LDP do tipo *Hello* capturadas nesta interface, conforme pode ser observado na Figura 5.35.

Conforme pode ser observado, o pacote *Hello* é gerado com o IP de origem da interface, tanto do lado do roteador R1 com IP 10.0.0.13, quanto do lado do roteador R3 com IP 10.0.0.14, com destino ao endereço *multicast* 224.0.0.2 reservado pela IANA (*Internet Assigned Numbers Authority*) que tem como alvo todos os roteadores na sub-rede. Como o pacote é enviado para um endereço *multicast*, o cabeçalho do LDP tem de ser transportado via protocolo de transporte UDP, na porta 646 (FREITAS, 2013).

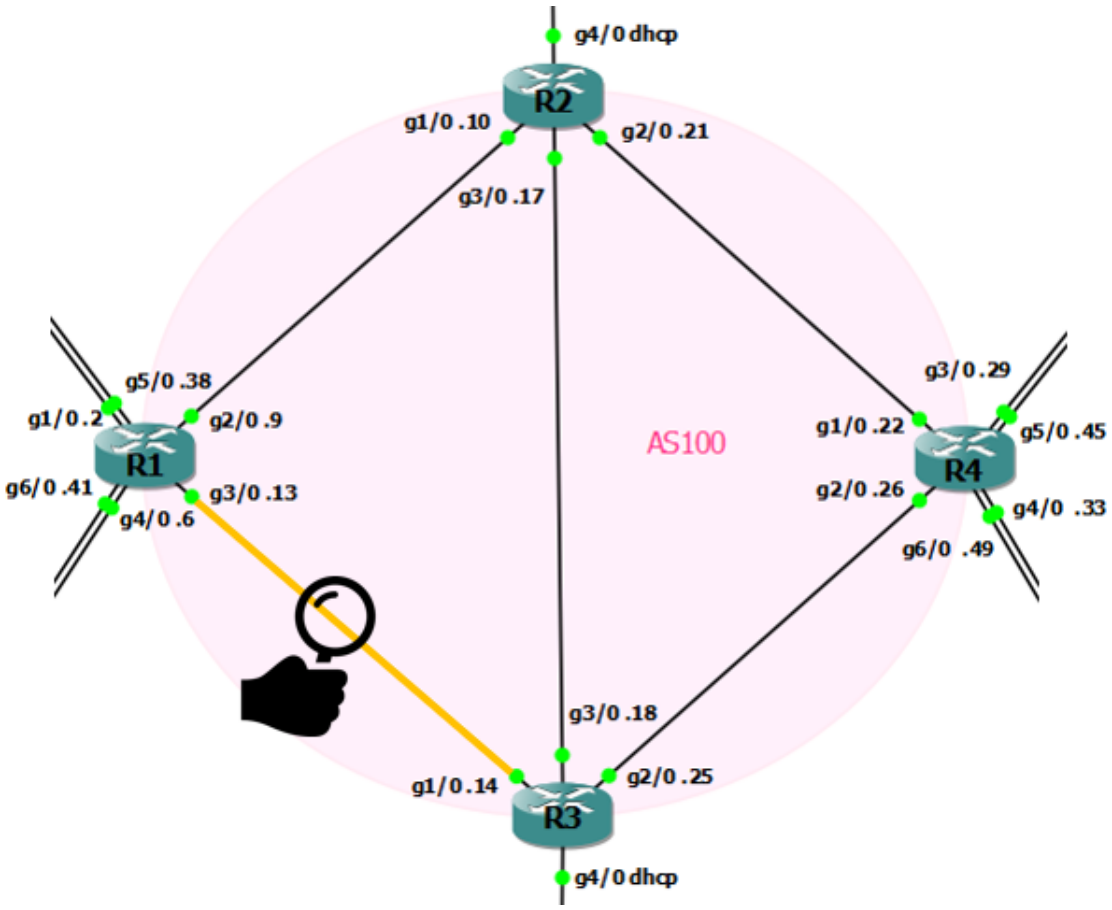


Figura 5.34: *Link* no qual o *sniffer* Wireshark será utilizado para a captura de pacotes. Fonte própria.

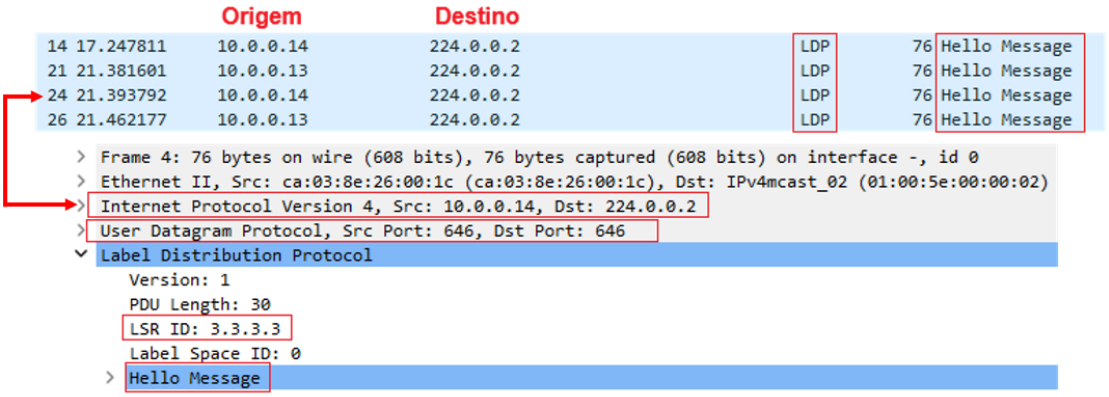


Figura 5.35: Mensagens do tipo *Hello* do protocolo LDP capturadas através do *sniffer* Wireshark. Fonte própria.

Quando um roteador que também possui o LDP habilitado detecta a mensagem de um outro roteador, estes passam a se comunicar por *unicast* através de uma sessão TCP entre eles, conforme indicado pela Figura 5.36.

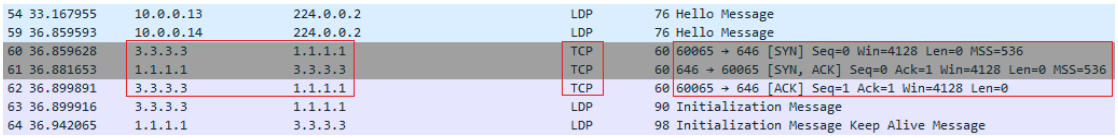


Figura 5.36: Iniciação da sessão TCP entre os roteadores R1 e R3. Fonte própria.

Essa troca de pacotes TCP são definidas como mensagens de sessão, no qual permite que os pares LDP estabeleçam, mantenham e encerrem sessões/conexões LDP. Dessa forma, no momento em que um roteador estabelece uma sessão com outro roteador através das mensagens *Hello*, ele inicia o estabelecimento de Conexão da Camada de Transporte a partir do processo de *Three Way Handshake* do protocolo TCP, a fim de garantir que a sessão LDP tenha conectividade bidirecional. Nota-se que após a descoberta, a comunicação entre os pacotes passa a utilizar o IP de *Loopback* dos roteadores, neste caso o R1 com IP 1.1.1.1 e R3 com IP 3.3.3.3.

Após o estabelecimento da sessão TCP para o transporte de PDUS (*Protocol Data Units*) LDP, um dos LSRs nessa comunicação envia uma mensagem do tipo *INITIALIZATION* contendo a negociação de parâmetros de sessão e as informações das características suportadas pelo LSR, como versão do protocolo, método de distribuição dos *labels*, tamanho máximo dos PDUs e intervalo de *KeepAlive*.

No momento em que esse procedimento é concluído, os dois roteadores são considerados *peers* LDP e se encontram na fase ativa e então podem realizar trocas de mensagens de anúncio, no qual permite que os LSRs troquem informações de *labels* para determinar os próximos saltos em um LSP específico. Dessa maneira, mensagens de anúncio criam, mudam e apagam mapeamentos de rótulos para o encaminhamento de FECs (FREITAS, 2013).

É importante recordar, que o funcionamento da tecnologia MPLS é baseada na identificação dos pacotes que são transportados por uma mesma rota, ou seja, que pertençam à mesma classe de encaminhamento (FEC), do inglês *Forward Equivalence Class* (MÜLLER, 2002).

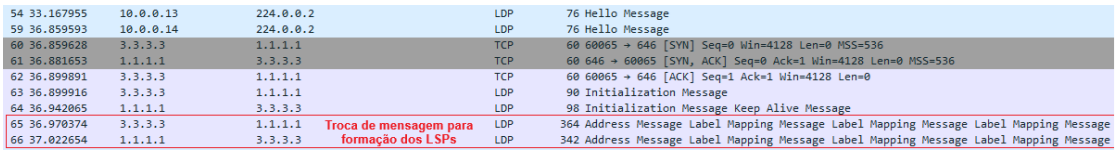


Figura 5.37: Mensagens de anúncio LDP capturadas através do *sniffer* Wireshark. Fonte própria.

Nota-se, a partir da Figura 5.37, que após o processo de inicialização, um LSR transmite informações sobre a topologia a partir de mensagens de anúncio a fim de criar, modificar e excluir associações de rótulos à FECs, ou seja, formar os LSPs. A colocação de um rótulo em um pacote significa atribuir este pacote a uma determinada FEC (MÜLLER, 2002).

O LDP consegue transmitir diversas informações de forma eficiente. Conforme pode ser observado na Figura 5.38, um único pacote carrega diversos TLVs. Além disso, para distribuir uma associação rótulo-FEC é necessário o envio da mensagem *Label Mapping*, no qual contém informações como FEC e o *label* atribuído, conforme destacado na figura 5.38, no qual o TLV em questão anuncia o prefixo 3.3.3.3 com o *Label* igual a 3.

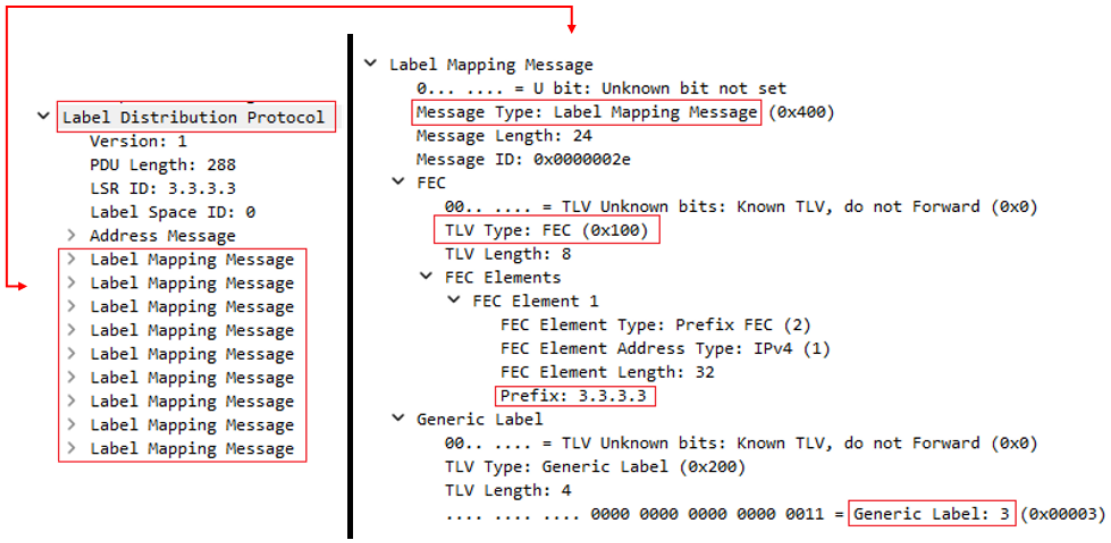


Figura 5.38: Detalhes do pacote de anúncio do protocolo LDP. Fonte própria.

Qualquer tipo de modificação ou possíveis falhas nos LSRs, notificações LDP são geradas que podem então encerrar uma sessão LDP ou gerar anúncios a fim de anunciar as alterações dos caminhos de encaminhamento (JUNIPER, L., 2023).

A partir do funcionamento do MPLS mencionado, o diagrama presente na Figura 5.39 aborda as etapas do protocolo LDP a fim de que roteadores LSRs criem *peers* LDP para anunciar os LSPs disponíveis.

É possível verificar a comunicação entre os LSRs através do comando "*ping mpls ipv4 x.x.x.x/x*". O MPLS LSP *ping* funciona de forma análoga ao ICMP para redes IP, no qual utiliza pacotes do tipo MPLS *Echo Request* e *Echo Reply* para validar um LSP.

A Figura 5.40 verifica o uso do comando "*ping mpls ipv4 x.x.x.x/x*" a partir do roteador R1 com destino ao roteador R4. Nota-se que foram enviados 5 pacotes de requisição para o destino, e a comunicação ocorreu com sucesso, no qual foram recebidos 5 pacotes de resposta.

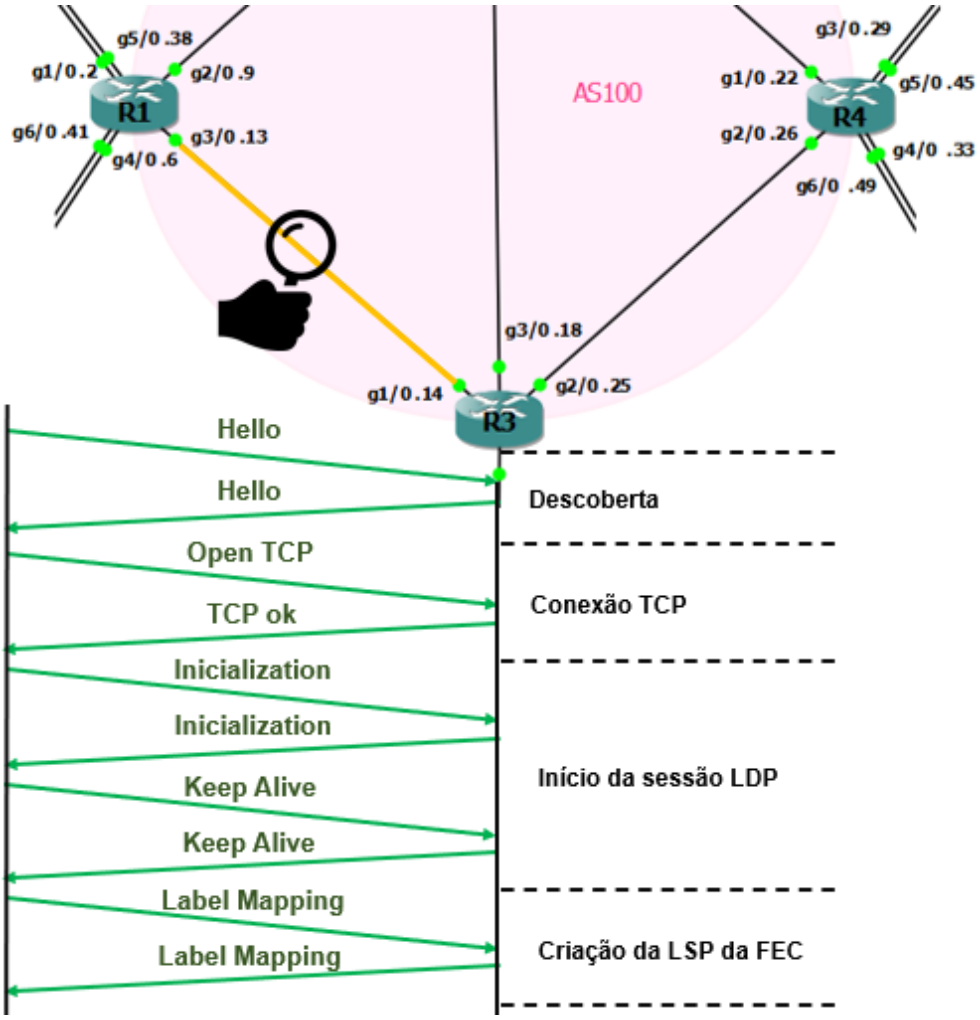


Figura 5.39: Troca de mensagens LDP. Fonte própria.

```
R1#ping mpls ipv4 4.4.4.4/32
Sending 5, 100-byte MPLS Echos to 4.4.4.4/32,
     timeout is 2 seconds, send interval is 0 msec:

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
  'L' - labeled output interface, 'B' - unlabeled output interface,
  'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
  'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
  'P' - no rx intf label prot, 'p' - premature termination of LSP,
  'R' - transit router, 'I' - unknown upstream index,
  'X' - unknown return code, 'x' - return code 0

Type escape sequence to abort.
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/13/16 ms
```

Figura 5.40: Teste de conectividade MPLS entre os roteadores R1 e R4. Fonte própria.

Para validar o caminho realizado partindo do roteador R1, foi iniciado a captura de pacotes entre os *links* que conectam R1→R2 e R1→R3, conforme pode ser observado na Figura 5.41.

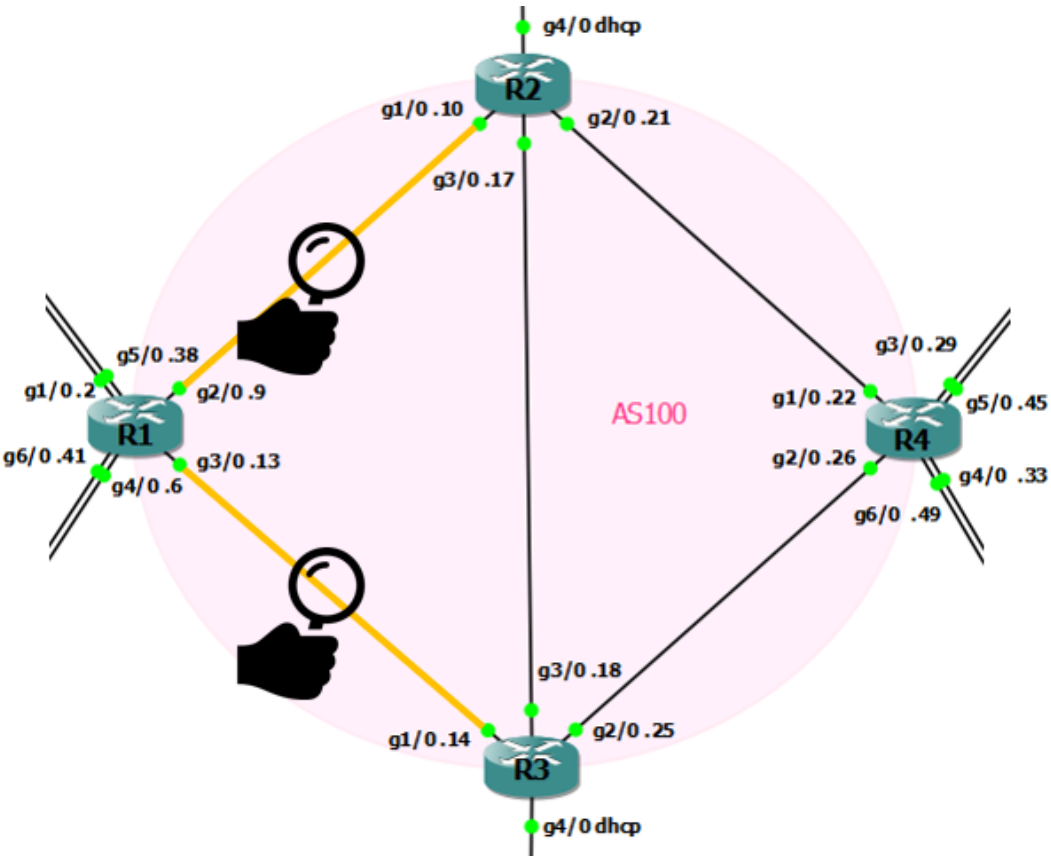


Figura 5.41: *Links* no qual o *sniffer* Wireshark será utilizado para verificar o encaminhamento dos pacotes. Fonte própria.

A partir disso, verificou-se que o envio de pacotes do R1 para o destino R4, partiram de R1 com destino ao roteador R3, conforme os seguintes pacotes capturados pelo *sniffer* Wireshark apresentados na Figura 5.42.

Verifica-se o envio de pacotes MPLS *Echo Request*, partindo da origem com IP 10.0.0.13, referente à interface Gi3/0 que interconecta o roteador R1 ao R3. Nota-se também que o conteúdo encapsulado possui como destino o endereço IP 127.0.0.1. Este endereço é utilizado como uma maneira de minimizar a possibilidade de um pacote ser entregue ao usuário final ou que este seja reenviado a algum outro destino, caso o LSP esteja com falha (FREITAS, 2013).

Ao chegar os pacotes MPLS *Echo Request*, o destino responde com pacotes MPLS *Echo Reply*. É importante mencionar que o pacote de resposta é feito de maneira *unicast* a partir da utilização da estrutura de roteamento IP, assim esse pacote não possui *labels* MPLS. Isso ocorre devido à natureza assimétrica dos LSPs. Se o pacote de resposta fosse comutado através do MPLS, o *ping* estaria na verdade testando mais de um caminho LSP simultaneamente (FREITAS, 2013). Dessa maneira, é válido verificar o sentido contrário.

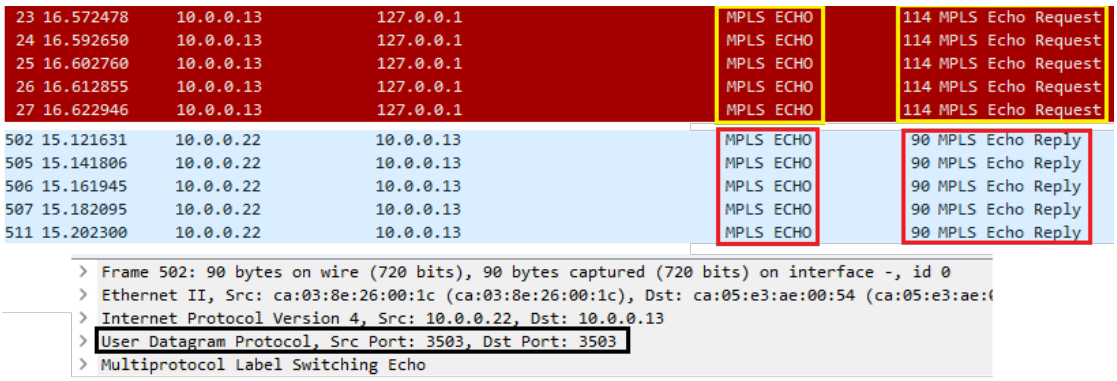


Figura 5.42: Verificação do envio de pacotes partindo de R1 para o destino em R4. Fonte própria.

Além disso, tanto pacotes de solicitação quanto pacotes de resposta são transferidos pela camada de transporte utilizando o protocolo UDP com porta de origem e destino definidas como 3503.

A partir deste teste de conectividade, realizou-se a suspensão da conexão entre R1 e R3 e iniciou-se a captura de pacotes no *link* que interconecta R1 ao roteador R2, a fim de verificar a redundância do *Backbone* MPLS, conforme a Figura 5.43 abaixo:

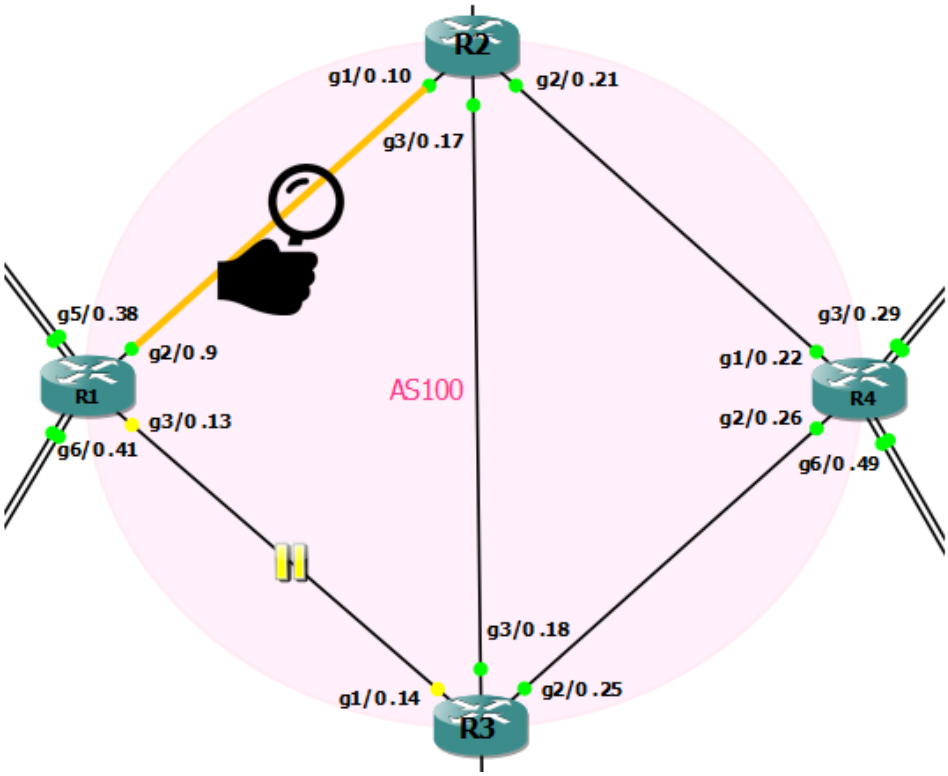


Figura 5.43: Suspensão do *link* de conexão R1→R3 e captura de pacotes no *link* de conexão R1→R2, para verificar a redundância no *backbone* MPLS. Fonte própria.

Ao suspender a comunicação direta entre R1 e R3 verificou-se o seguinte *log*, exibido na Figura 5.44, do roteador R1, no qual a vizinhança LDP com o IP 3.3.3.3 passa a estar com o *status* "*DOWN*", pois o LSR não recebeu pacotes *Hello* dentro do período padrão de

"*Hold Time*".

```
*Nov  6 23:16:22.199: %LDP-5-NBRCHG: LDP Neighbor 3.3.3.3:0 (2) is DOWN (Discove
ry Hello Hold Timer expired)
!
```

Figura 5.44: *Log* de vizinhança LDP com *status* "*down*". Fonte própria.

Verificou-se a partir da captura de pacotes feita pelo *sniffer* Wireshark que a comunicação ocorreu com sucesso através do *link* que interconecta os dispositivos R1 e R2, conforme pode ser observado pela Figura 5.45.

4276 71.587834	10.0.0.9	127.0.0.1	MPLS ECHO	114 MPLS Echo Request
4281 71.606694	10.0.0.22	10.0.0.9	MPLS ECHO	90 MPLS Echo Reply
4290 71.628560	10.0.0.9	127.0.0.1	MPLS ECHO	114 MPLS Echo Request
4299 71.647237	10.0.0.22	10.0.0.9	MPLS ECHO	90 MPLS Echo Reply
4304 71.659023	10.0.0.9	127.0.0.1	MPLS ECHO	114 MPLS Echo Request
4305 71.677481	10.0.0.22	10.0.0.9	MPLS ECHO	90 MPLS Echo Reply
4306 71.689247	10.0.0.9	127.0.0.1	MPLS ECHO	114 MPLS Echo Request
4307 71.707723	10.0.0.22	10.0.0.9	MPLS ECHO	90 MPLS Echo Reply
4308 71.719483	10.0.0.9	127.0.0.1	MPLS ECHO	114 MPLS Echo Request
4309 71.737948	10.0.0.22	10.0.0.9	MPLS ECHO	90 MPLS Echo Reply

Figura 5.45: Verificação dos pacotes após a suspensão do *link*. Fonte própria.

Dessa maneira, conclui-se que a tecnologia mínima para o MPLS funcionar nesta topologia, roteamento OSPF, além da redundância do *Backbone* está em completo funcionamento.

5.2.2 Análises da configuração do roteamento BGP nos roteadores de borda da provedora

Após a configuração do roteamento IGP utilizando OSPF e da tecnologia MPLS a partir do protocolo LDP, a segunda etapa para a configuração da topologia MPLS L3VPN é configurar as VRFs UNB e UNB-2 nos roteadores de borda da provedora a fim de separar o tráfego de redundância do cliente, como também realizar a configuração de roteamento BGP para interligar os sites ao *backbone* da provedora.

Dessa maneira, a Figura 5.46 expõe as configurações das VRFs nesta etapa de implementação, para os dois roteadores de borda da provedora presentes na topologia, onde o destaque em vermelho se refere à VRF UNB indicando as interfaces no qual essa VRF foi inserida. Da mesma forma, a cor amarela em destaque se refere à VRF UNB-2.

Além disso, ainda do lado da operadora, os roteadores foram configurados com o protocolo de roteamento BGP utilizando as VRFs previamente configuradas, conforme pode ser observado na Figura 5.47.

Roteador R1

```
vrf definition UNB
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
vrf definition UNB-2
 rd 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
```

```
interface GigabitEthernet1/0
 vrf forwarding UNB
 ip address 10.0.0.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 10.0.0.9 255.255.255.252
 negotiation auto
!
interface GigabitEthernet3/0
 ip address 10.0.0.13 255.255.255.252
 negotiation auto
!
interface GigabitEthernet4/0
 vrf forwarding UNB
 ip address 10.0.0.6 255.255.255.252
 negotiation auto
!
interface GigabitEthernet5/0
 vrf forwarding UNB-2
 ip address 10.0.0.38 255.255.255.252
 negotiation auto
!
interface GigabitEthernet6/0
 vrf forwarding UNB-2
 ip address 10.0.0.41 255.255.255.252
 negotiation auto
```

Roteador R4

```
interface GigabitEthernet1/0
 ip address 10.0.0.22 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 10.0.0.26 255.255.255.252
 negotiation auto
!
interface GigabitEthernet3/0
 vrf forwarding UNB
 ip address 10.0.0.29 255.255.255.252
 negotiation auto
!
interface GigabitEthernet4/0
 vrf forwarding UNB
 ip address 10.0.0.33 255.255.255.252
 negotiation auto
!
interface GigabitEthernet5/0
 vrf forwarding UNB-2
 ip address 10.0.0.45 255.255.255.252
 negotiation auto
!
interface GigabitEthernet6/0
 vrf forwarding UNB-2
 ip address 10.0.0.49 255.255.255.252
 negotiation auto
```

Figura 5.46: Configurações das VRFs realizadas nos roteadores de borda da provedora. Fonte própria.

Roteador R1

```
router bgp 100
 address-family ipv4 vrf UNB-2
  neighbor 10.0.0.37 remote-as 65011
  neighbor 10.0.0.37 ebgp-multihop 255
  neighbor 10.0.0.37 activate
  neighbor 10.0.0.37 allowas-in
  neighbor 10.0.0.42 remote-as 65012
  neighbor 10.0.0.42 ebgp-multihop 255
  neighbor 10.0.0.42 activate
  neighbor 10.0.0.42 allowas-in
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf UNB
  neighbor 10.0.0.1 remote-as 65011
  neighbor 10.0.0.1 ebgp-multihop 255
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 allowas-in
  neighbor 10.0.0.5 remote-as 65012
  neighbor 10.0.0.5 ebgp-multihop 255
  neighbor 10.0.0.5 activate
  neighbor 10.0.0.5 allowas-in
  no synchronization
 exit-address-family
```

Roteador R4

```
router bgp 100
 address-family ipv4 vrf UNB-2
  neighbor 10.0.0.46 remote-as 65013
  neighbor 10.0.0.46 ebgp-multihop 255
  neighbor 10.0.0.46 activate
  neighbor 10.0.0.46 allowas-in
  neighbor 10.0.0.50 remote-as 65014
  neighbor 10.0.0.50 ebgp-multihop 255
  neighbor 10.0.0.50 activate
  neighbor 10.0.0.50 allowas-in
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf UNB
  neighbor 10.0.0.30 remote-as 65013
  neighbor 10.0.0.30 ebgp-multihop 255
  neighbor 10.0.0.30 activate
  neighbor 10.0.0.30 allowas-in
  neighbor 10.0.0.34 remote-as 65014
  neighbor 10.0.0.34 ebgp-multihop 255
  neighbor 10.0.0.34 activate
  neighbor 10.0.0.34 allowas-in
  no synchronization
 exit-address-family
```

Figura 5.47: Configuração do protocolo BGP utilizando as VRFs configuradas. Fonte própria.

Cada VRF foi utilizada para separar o tráfego de redundância do cliente, assim caso um *link* caia, outra conectividade ainda estará disponível. Abaixo a Figura 5.48 ilustra a qual VRF foi configurada em cada um dos *links* que conectam aos campus da UnB. Assim, conforme observado anteriormente, o BGP do lado da operadora é configurado de forma a separar as adjacências de cada VRF implementada nas interfaces dos roteadores da operadora.

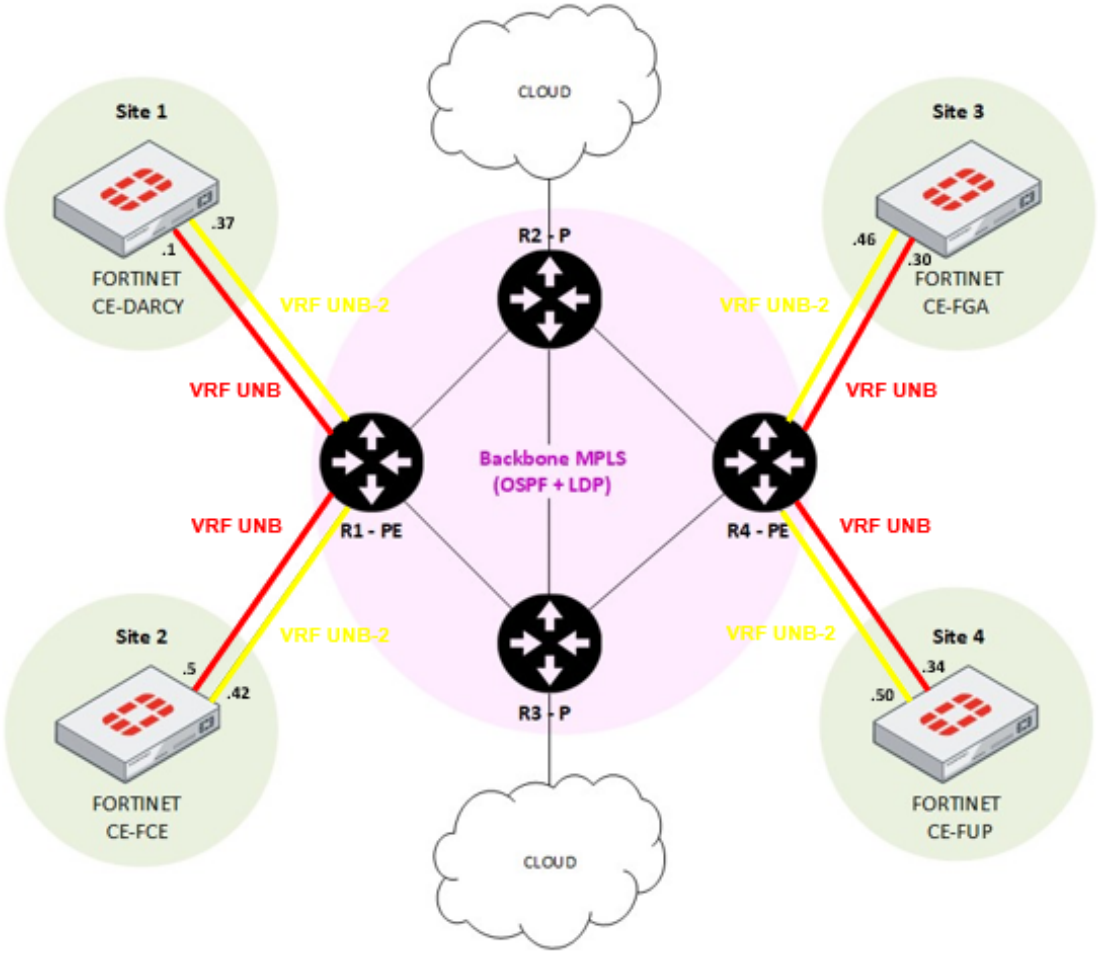


Figura 5.48: Separação do tráfego de redundância utilizando as VRFs. Fonte própria.

Com essa etapa configurada, os PEs são capazes de aprender as rotas presentes na rede interna dos clientes. Sendo assim, é possível, neste momento, verificar algumas informações acerca dessa configuração.

Como por exemplo, ao utilizar o comando "*show bgp vpnv4 unicast all summary*" nos roteadores de borda da provedora, será exibido um resumo do *status* do vizinho *unicast* do BGP VPNv4. A Figura 5.49, expõe a saída deste comando nos roteadores R1 e R4. Nele é possível verificar o identificador do roteador, neste caso, seu endereço de *Loopback*, juntamente com o número do AS local do *Backbone*, neste caso, 100. Em destaque na cor verde verifica-se os *neighbors* BGP referentes à VRF UNB juntamente com o número do AS remoto. Da mesma forma, verifica-se na cor azul os *neighbors* BGP, mas referentes à VRF UNB-2.

ROTEADOR R1

```
R1# show bgp vpnv4 unicast all summary
BGP router identifier 1.1.1.1, local AS number 100
BGP table version is 115, main routing table version 115
74 network entries using 11544 bytes of memory
132 path entries using 8976 bytes of memory
23/8 BGP path/bestpath attribute entries using 3864 bytes of memory
10 BGP AS-PATH entries using 240 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 4 (at peak 4) using 128 bytes of memory
BGP using 24800 total bytes of memory
BGP activity 74/0 prefixes, 132/0 paths, scan interval 15 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
4.4.4.4         4          100      39      39      115    0    0 00:33:54        38
10.0.0.1        4        65011      45      42      115    0    0 00:33:51        37
10.0.0.5        4        65012      44      48      115    0    0 00:33:27        37
10.0.0.37       4        65011      41      42      115    0    0 00:33:59        10
10.0.0.42       4        65012      41      40      115    0    0 00:34:06        10
```

ROTEADOR R4

```
R4#show bgp vpnv4 unicast all summary
BGP router identifier 4.4.4.4, local AS number 100
BGP table version is 259, main routing table version 259
74 network entries using 11544 bytes of memory
132 path entries using 8976 bytes of memory
23/8 BGP path/bestpath attribute entries using 3864 bytes of memory
10 BGP AS-PATH entries using 240 bytes of memory
2 BGP extended community entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
Bitfield cache entries: current 4 (at peak 5) using 128 bytes of memory
BGP using 24800 total bytes of memory
BGP activity 110/36 prefixes, 206/74 paths, scan interval 15 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
1.1.1.1         4          100      73      80      259    0    0 00:35:21        38
10.0.0.30       4        65013      81      73      259    0    0 01:03:25        37
10.0.0.34       4        65014      81      74      259    0    0 01:03:23        37
10.0.0.46       4        65013      74      69      259    0    0 01:03:26        10
10.0.0.50       4        65014      75      69      259    0    0 01:03:24        10
```

Figura 5.49: Saída do comando "*show bgp vpnv4 unicast all summary*" nos roteadores de borda da provedora. Fonte própria.

5.2.3 Análises da configuração da VPNv4 nos roteadores de borda da provedora

Após a configuração das VRFs e do protocolo BGP nos roteadores de borda da provedora, neste momento os sites conectados ao roteador R1 possuem comunicação entre si, como também os sites conectados ao roteador R4. Entretanto, os campus ao lado do R1 não se comunicam com os campus ao lado de R4. Para isso, foi necessário configurar o MP-BGP no PE a fim de importar as rotas das VRFs e divulgá-las via iBGP para o outro PE na topologia.

Neste caso, em R1 foi configurado o MP-BGP com *neighbor* para o roteador R4. Da mesma maneira, em R4 foi implementado o MP-BGP a fim de formar adjacência BGP com o roteador R1. A Figura 5.50 abaixo ilustra os comandos utilizados para essa etapa da configuração, conforme

detalhado no capítulo anterior.

Roteador R1

```
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 4.4.4.4 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit-address-family
```

Roteador R4

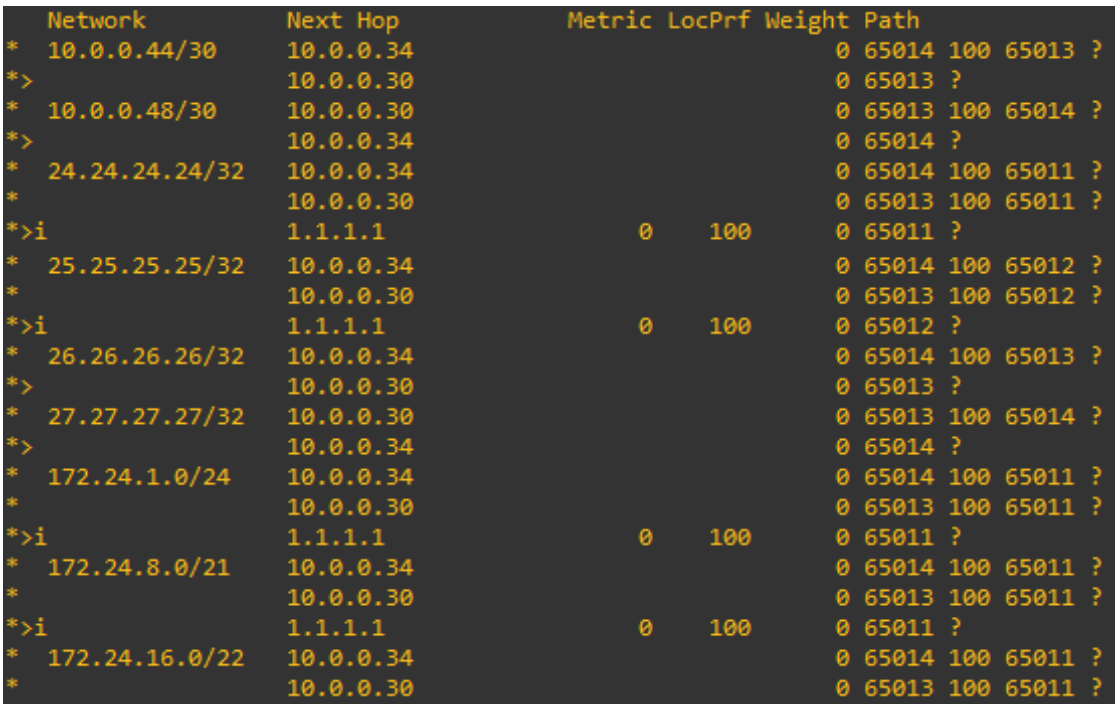
```
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 1.1.1.1 remote-as 100
 neighbor 1.1.1.1 update-source Loopback0
 !
 address-family ipv4
  neighbor 1.1.1.1 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 1.1.1.1 activate
  neighbor 1.1.1.1 send-community extended
 exit-address-family
```

Figura 5.50: Configuração do MP-BGP nos roteadores de borda da provedora. Fonte própria.

Para verificar se a comunicação entre os sites ao lado de R1 se comunicam com os sites ao lado de R4, basta utilizar o comando "*show bgp vpnv4 unicast all*". Este comando exibe todas as entradas VPNv4 na tabela de roteamento BGP. As Figuras 5.51 a 5.56 expõem a saída deste comando no roteador R4, no qual observa-se que o PE aprendeu todas as rotas internas dos clientes.

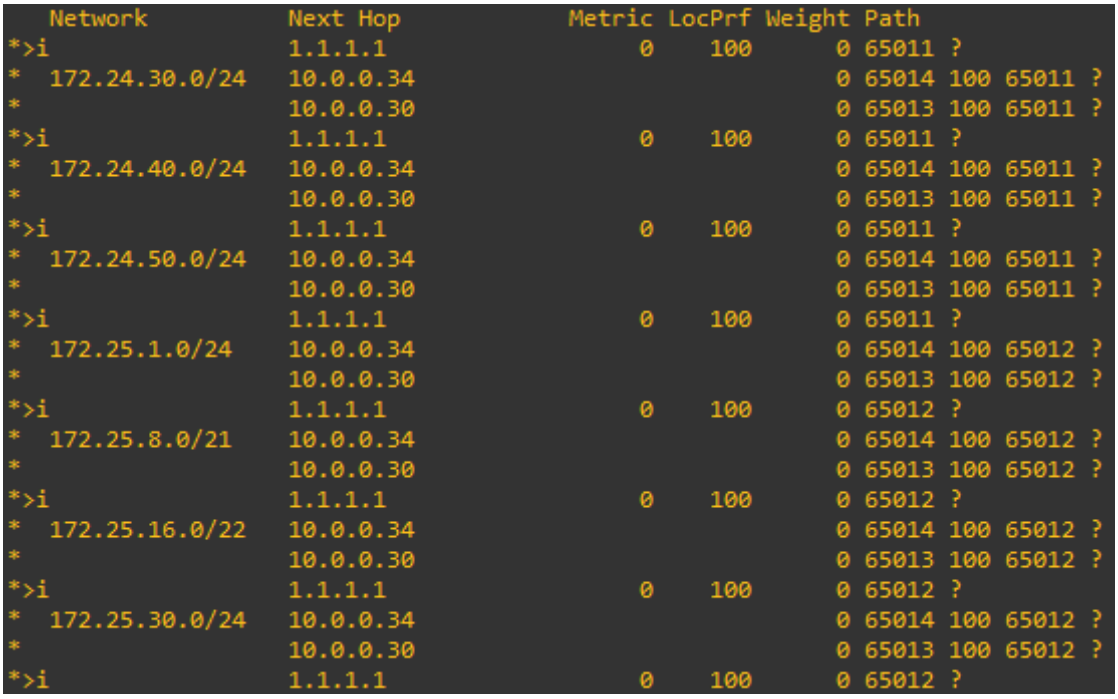
```
R4#show bgp vpnv4 unicast all
BGP table version is 259, local router ID is 4.4.4.4
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf UNB)
*  10.0.0.0/30      10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  10.0.0.4/30      10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
r  10.0.0.28/30     10.0.0.34                              0 65014 100 65013 ?
r>                  10.0.0.30                              0 65013 ?
r  10.0.0.32/30     10.0.0.30                              0 65013 100 65014 ?
r>                  10.0.0.34                              0 65014 ?
*  10.0.0.36/30     10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  10.0.0.40/30     10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
```

Figura 5.51: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 1). Fonte própria.



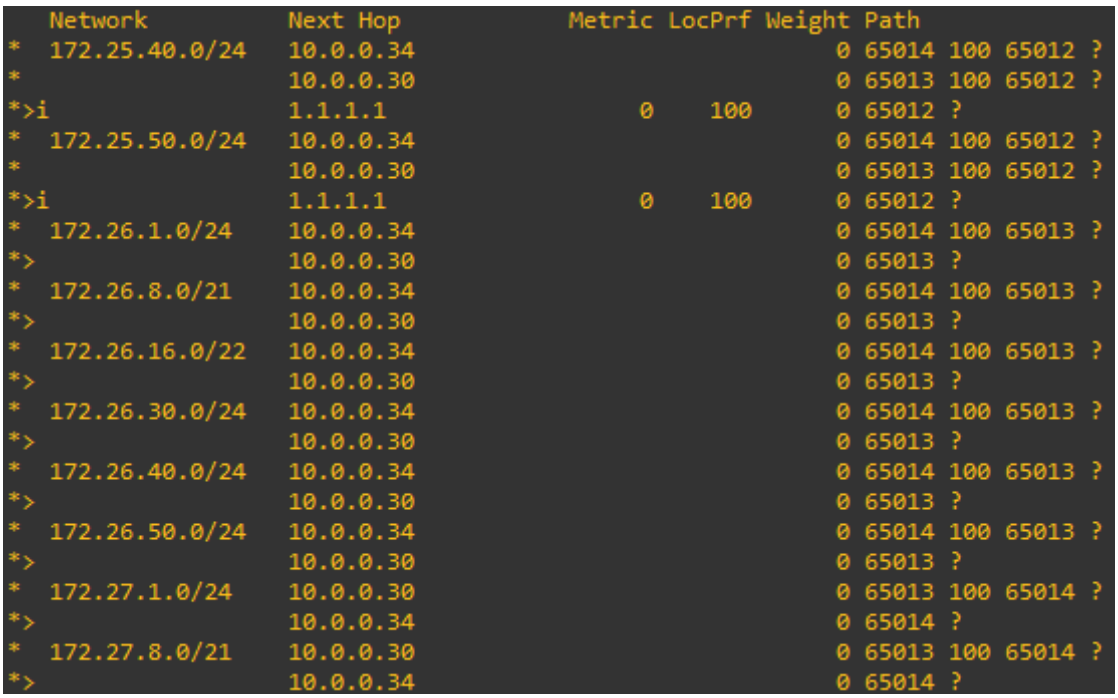
```
   Network          Next Hop            Metric LocPrf Weight Path
*  10.0.0.44/30     10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  10.0.0.48/30     10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  24.24.24.24/32   10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  25.25.25.25/32   10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  26.26.26.26/32   10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  27.27.27.27/32   10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  172.24.1.0/24    10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.24.8.0/21    10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.24.16.0/22   10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
```

Figura 5.52: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 2). Fonte própria.



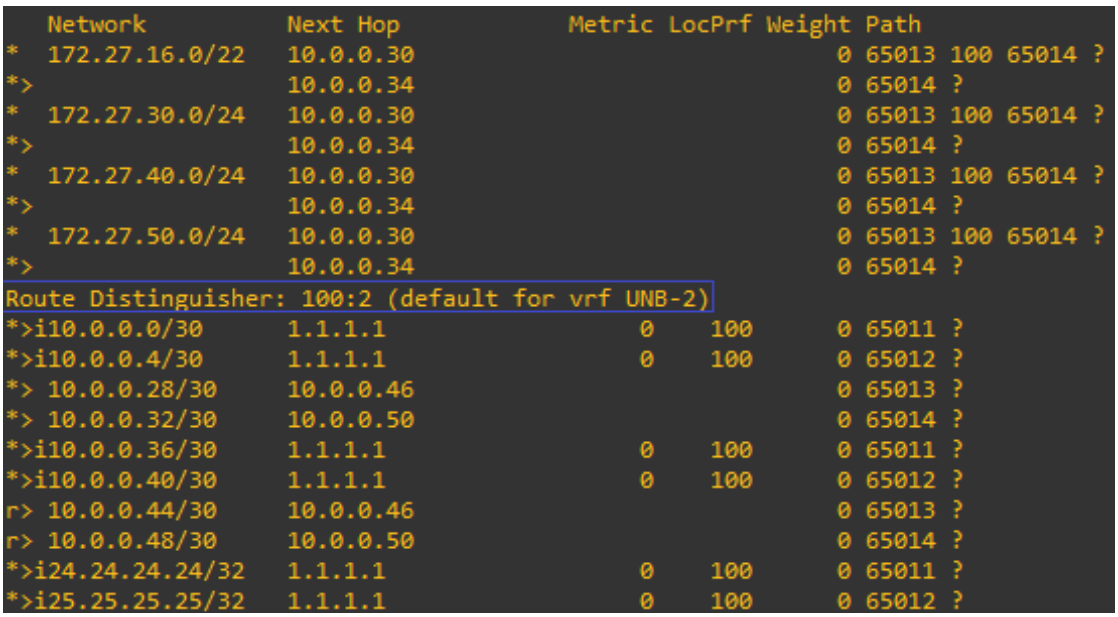
```
   Network          Next Hop            Metric LocPrf Weight Path
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.24.30.0/24   10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.24.40.0/24   10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.24.50.0/24   10.0.0.34                              0 65014 100 65011 ?
*                   10.0.0.30                              0 65013 100 65011 ?
*>i                 1.1.1.1                  0    100      0 65011 ?
*  172.25.1.0/24    10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  172.25.8.0/21    10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  172.25.16.0/22   10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  172.25.30.0/24   10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
```

Figura 5.53: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 3). Fonte própria.



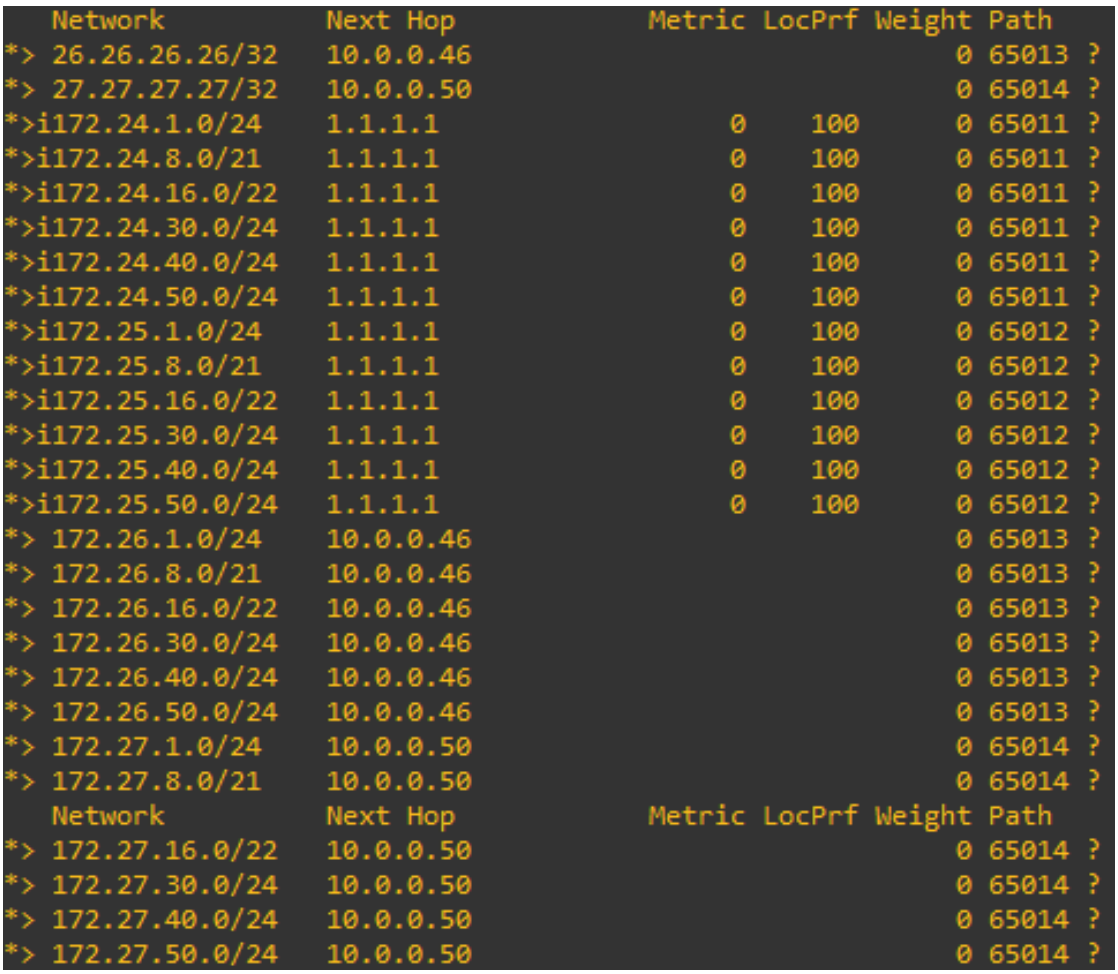
```
   Network          Next Hop            Metric LocPrf Weight Path
*  172.25.40.0/24   10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  172.25.50.0/24   10.0.0.34                              0 65014 100 65012 ?
*                   10.0.0.30                              0 65013 100 65012 ?
*>i                 1.1.1.1                  0    100      0 65012 ?
*  172.26.1.0/24    10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.26.8.0/21    10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.26.16.0/22   10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.26.30.0/24   10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.26.40.0/24   10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.26.50.0/24   10.0.0.34                              0 65014 100 65013 ?
*>                  10.0.0.30                              0 65013 ?
*  172.27.1.0/24    10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  172.27.8.0/21    10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
```

Figura 5.54: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 4). Fonte própria.



```
   Network          Next Hop            Metric LocPrf Weight Path
*  172.27.16.0/22   10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  172.27.30.0/24   10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  172.27.40.0/24   10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
*  172.27.50.0/24   10.0.0.30                              0 65013 100 65014 ?
*>                  10.0.0.34                              0 65014 ?
Route Distinguisher: 100:2 (default for vrf UNB-2)
*>i10.0.0.0/30      1.1.1.1                  0    100      0 65011 ?
*>i10.0.0.4/30      1.1.1.1                  0    100      0 65012 ?
*> 10.0.0.28/30     10.0.0.46                              0 65013 ?
*> 10.0.0.32/30     10.0.0.50                              0 65014 ?
*>i10.0.0.36/30     1.1.1.1                  0    100      0 65011 ?
*>i10.0.0.40/30     1.1.1.1                  0    100      0 65012 ?
r> 10.0.0.44/30     10.0.0.46                              0 65013 ?
r> 10.0.0.48/30     10.0.0.50                              0 65014 ?
*>i24.24.24.24/32   1.1.1.1                  0    100      0 65011 ?
*>i25.25.25.25/32   1.1.1.1                  0    100      0 65012 ?
```

Figura 5.55: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 5). Fonte própria.



	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	26.26.26.26/32	10.0.0.46			0	65013 ?
*>	27.27.27.27/32	10.0.0.50			0	65014 ?
*>i	172.24.1.0/24	1.1.1.1	0	100	0	65011 ?
*>i	172.24.8.0/21	1.1.1.1	0	100	0	65011 ?
*>i	172.24.16.0/22	1.1.1.1	0	100	0	65011 ?
*>i	172.24.30.0/24	1.1.1.1	0	100	0	65011 ?
*>i	172.24.40.0/24	1.1.1.1	0	100	0	65011 ?
*>i	172.24.50.0/24	1.1.1.1	0	100	0	65011 ?
*>i	172.25.1.0/24	1.1.1.1	0	100	0	65012 ?
*>i	172.25.8.0/21	1.1.1.1	0	100	0	65012 ?
*>i	172.25.16.0/22	1.1.1.1	0	100	0	65012 ?
*>i	172.25.30.0/24	1.1.1.1	0	100	0	65012 ?
*>i	172.25.40.0/24	1.1.1.1	0	100	0	65012 ?
*>i	172.25.50.0/24	1.1.1.1	0	100	0	65012 ?
*>	172.26.1.0/24	10.0.0.46			0	65013 ?
*>	172.26.8.0/21	10.0.0.46			0	65013 ?
*>	172.26.16.0/22	10.0.0.46			0	65013 ?
*>	172.26.30.0/24	10.0.0.46			0	65013 ?
*>	172.26.40.0/24	10.0.0.46			0	65013 ?
*>	172.26.50.0/24	10.0.0.46			0	65013 ?
*>	172.27.1.0/24	10.0.0.50			0	65014 ?
*>	172.27.8.0/21	10.0.0.50			0	65014 ?
	Network	Next Hop	Metric	LocPrf	Weight	Path
*>	172.27.16.0/22	10.0.0.50			0	65014 ?
*>	172.27.30.0/24	10.0.0.50			0	65014 ?
*>	172.27.40.0/24	10.0.0.50			0	65014 ?
*>	172.27.50.0/24	10.0.0.50			0	65014 ?

Figura 5.56: Saída do comando "*show bgp vpnv4 unicast all*" no roteador R4 (Parte 6). Fonte própria.

Para finalizar as análises referentes à configuração da tecnologia MPLS L3VPN, é possível ainda realizar testes de conectividade utilizando o *PING* e o *TRACEROUTE*.

A Figura 5.57 abaixo ilustra o teste de conectividade utilizando o comando "*ping vrf [NOME DA VRF] x.x.x.x*" partindo do roteador R4. Verifica-se, portanto, a comunicação com sucesso entre a origem e o destino descrito.

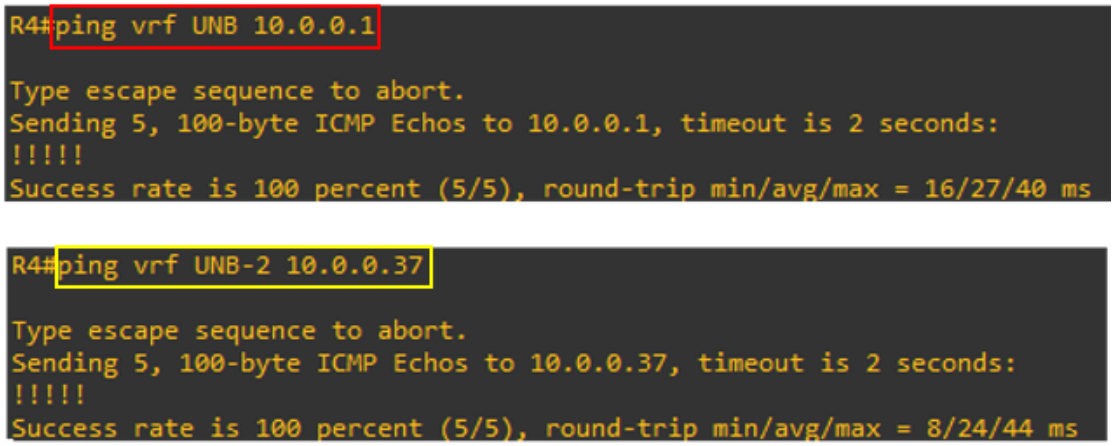


Figura 5.57: Teste de conectividade utilizando o comando "*ping vrf [NOME DA VRF] x.x.x.x*". Fonte própria.

É importante notar a especificação da VRF neste comando, pois a comunicação não ocorre entre VRFs diferentes. Sendo assim, caso insira o comando especificado mas com o endereço IP não acessível pela VRF inserida, haverá falha na entrega e recebimento dos pacotes ICMP, conforme exemplificado pela Figura 5.58.

Figura 5.58: Teste de conectividade utilizando o comando "*ping vrf [NOME DA VRF] x.x.x.x*", mas com o endereço IP não acessível pela VRF especificada. Fonte própria.

5.2.4 Análises de redundância para a *Cloud*

Em seguida, com as conexões do *backbone* em perfeito funcionamento, foram realizadas as configurações de conectividade com a *Cloud*, conforme observado na Figura 4.23, presente no capítulo anterior.

O protocolo HSRP foi utilizado para que a arquitetura tenha sempre um *gateway* padrão em funcionamento mesmo que haja interrupções na comunicação com a saída principal. Sendo assim, esse protocolo provê alta disponibilidade aos roteadores conectados à saída de Internet, neste caso os dispositivos da provedora R2 e R3.

A Figura 5.59 descreve os comandos utilizados para a configuração deste protocolo nos roteadores da provedora.

Roteador R2

```
interface GigabitEthernet4/0
 description CONEXAO_INTERNET
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 negotiation auto
 standby 1 ip 192.168.122.10
 standby 1 priority 150
ip route 0.0.0.0 0.0.0.0 192.168.122.1
```

Roteador R3

```
interface GigabitEthernet4/0
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 negotiation auto
 standby 1 ip 192.168.122.10
ip route 0.0.0.0 0.0.0.0 192.168.122.1
```

Figura 5.59: Configurações do protocolo HSRP nos roteadores da provedora. Fonte própria.

O roteador R2 foi definido como o *Active Router* devido à configuração de prioridade ser maior, igual a 150, e o roteador R3 como *Standby Router*. A alta disponibilidade é obtida através do VIP compartilhado entre os roteadores, e é definido como o *gateway* padrão da rede, neste caso o IP 192.168.122.10. E no caso de falha no equipamento ou *link* principal, o outro componente do grupo assumirá o papel utilizando o endereço virtual. Além disso, uma rota estática é configurada para definir que o acesso à Internet se dá através do IP de próximo salto 192.168.122.1 presente na *cloud*.

É possível verificar informações sobre a configuração realizada através do comando "*show standby*" nos roteadores R2 e R3, conforme ilustrado na Figura 5.60. A partir disso, observa-se os seguintes dados: "*State*", sendo *Active* ou *Standby*. Neste caso, o roteador R2 foi definido como *Active Router* devido sua maior prioridade (igual a 150). Sua função é encaminhar de forma ativa os pacotes vindos de outros dispositivos até a saída de Internet, além de enviar mensagens do tipo "*Hello*" do protocolo HSRP, no qual permite que os demais roteadores tenham conhecimento sobre seu valor de prioridade e informações de *status* HSRP. Já o roteador R3, definido como *Standby Router* devido sua menor prioridade (igual a 100), continuará o envio de mensagens "*Hello*". Caso o *Active Router* falhe, ele assumirá o controle, tomando o envio de pacotes dos clientes como função. Além disso, é possível observar outras informações como o endereço VIP sendo igual a 192.168.122.10; o endereço MAC virtual e temporizador do envio de pacotes *Hello* e temporizador *Hold Time*.

Além disso, antes que cada roteador pertencente ao grupo HSRP, se torne um *Active Router* ou *Standby Router*, eles passarão por vários estados, conforme exposto na Tabela 5.6.

ROTEADOR R2

```
R2#show standby
GigabitEthernet4/0 - Group 1
  State is Active
    2 state changes, last state change 00:01:33
  Virtual IP address is 192.168.122.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.656 secs
  Preemption disabled
  Active router is local
  Standby router is 192.168.122.84, priority 100 (expires in 10.528 sec)
  Priority 150 (configured 150)
  Group name is "hsrp-Gi4/0-1" (default)
```

ROTEADOR R3

```
R3#show standby
GigabitEthernet4/0 - Group 1
  State is Standby
    1 state change, last state change 00:00:33
  Virtual IP address is 192.168.122.10
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.232 secs
  Preemption disabled
  Active router is 192.168.122.222, priority 150 (expires in 11.920 sec)
  Standby router is local
  Priority 100 (default 100)
  Group name is "hsrp-Gi4/0-1" (default)
```

Figura 5.60: Saída do comando "*show standby*"nos roteadores da provedora. Fonte própria.

Tabela 5.6: Estados do protocolo HSRP

Estado	Explicação
Initial	Primeiro estado quando o HSRP é configurado, ou seja, quando uma interface está disponível pela primeira vez ou através de uma mudança de configuração
Listen	O roteador conhece o endereço VIP e escuta as mensagens Hello vindas de outros roteadores no grupo HSRP
Speak	O roteador envia mensagens Hello para os outros roteadores do grupo HSRP a fim de participar da seleção do Activer e Standby Router
Standby	Roteador não se tornou ativo, mas envia continuamente mensagens Hello, pois no caso de falha do Active Router, o Standby Router deve assumir a transferência de pacotes
Active	Roteador ativo encaminhará os pacotes destinados à Internet, além de enviar continuamente mensagens Hello

É possível observar a transição de estados dos roteadores R2 e R3 ao se tornarem *Active* e *Standby Router*, conforme destacado na Figura 5.61.

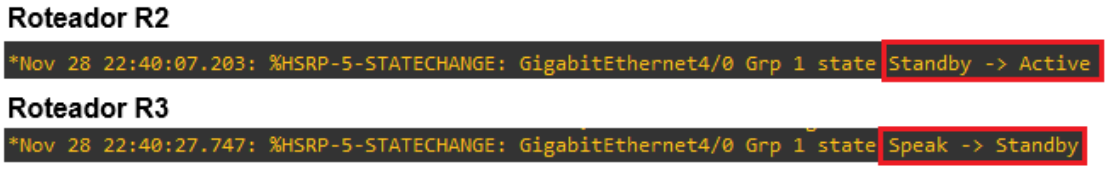


Figura 5.61: Transição de estado HSRP nos roteadores R2 e R3. Fonte própria.

Além disso, ao acionar o comando "*debug standby*" a fim de verificar os *logs* do protocolo HSRP nos roteadores da provedora, é possível verificar as mensagens do tipo *Hello*, conforme indicado na Figura 5.62 abaixo. No qual o roteador R2 envia um pacote *Hello* informando o endereço IP físico conectado à *Cloud*, juntamente com seu *status Active*, identificação de prioridade e o endereço VIP. Além disso, ele recebe um pacote *Hello* contendo as mesmas informações, mas referentes ao roteador *Standby*. Da mesma forma, esse processo ocorre no roteador R3.

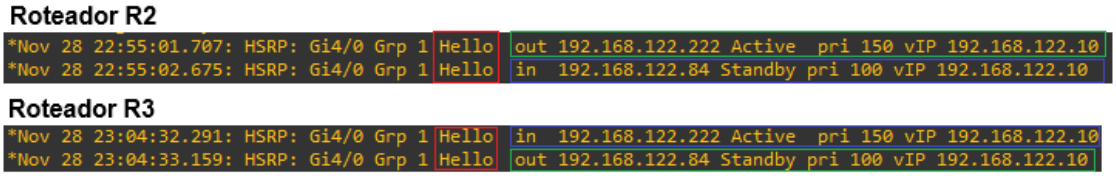


Figura 5.62: *Logs* referentes ao protocolo HSRP nos roteadores da provedora. Fonte própria.

Os pacotes *Hello* são utilizados para enviar informações pertinentes ao funcionamento do protocolo HSRP, como *timers*, prioridade dos roteadores pertencentes ao grupo, autenticação, versão, entre outras informações. Além disso, em caso de falhas ou alterações de prioridade, a troca de pacotes *Hello* permitirão que os roteadores identifiquem caso haja mudanças na rede. Esses pacotes são destinados ao endereço *multicast* 224.0.0.2, sob o protocolo de transporte UDP na porta 1985.

Após a eleição dos roteadores como *Active* e *Standby* para o funcionamento do HSRP, é possível verificar a comunicatividade a partir dos dois roteadores da provedora (R2 e R3) para o endereço IP do servidor do GNS3 (172.16.5.80) presente na infraestrutura do Laboratório de Redes da Universidade de Brasília, através das duas *Clouds* existentes na topologia. A Figura 5.63 expõe o teste realizado utilizando o comando *PING* nos roteadores.

Roteador R3 --> Servidor GNS3 (172.16.5.80)

```
R3#ping 172.16.5.80

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.80, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/24 ms
```

Roteador R2 --> Servidor GNS3 (172.16.5.80)

```
R2#ping 172.16.5.80

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.5.80, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/12 ms
```

Figura 5.63: Teste de comunicação para o endereço IP do servidor do GNS3 presente na infraestrutura do Laboratório de Redes da UnB. Fonte própria.

Dessa maneira, conclui-se que os roteadores R2 e R3 possuem conectividade com a *Cloud*, entretanto, foi necessário anunciar o *gateway* padrão como sendo estes dois dispositivos para que os vizinhos também obtenham essa comunicação. Conforme descrito no capítulo anterior, rotas estáticas com IP SLA *Tracking* foram configuradas nos roteadores de borda da provedora a fim de obter redundância e caminhos de *backup* confiáveis em caso de falhas do *link* principal. Dessa maneira, se a conectividade com a rede de destino primária for perdida por algum motivo, o estado da rota será definido como inativo, e outra rota estática ativa poderá ser selecionada para rotear o tráfego.

Sendo assim, a Figura 5.64 exibe os comandos utilizados para a configuração de rotas estáticas com a funcionalidade IP SLA *Tracking* nos roteadores de borda da provedora R1 e R4. Observa-se que o IP SLA é configurado para executar *ping* ao endereço IP de destino principal, ou seja, para o *link* no qual os roteadores de borda estão conectados ao *Active Router* do HSRP. Com isso, é configurado a rota *default* primária utilizando a instrução *track*. Em seguida, a rota *default* secundária é configurada com uma prioridade maior, com o objetivo de que ela assuma caso o IP SLA *Tracking* verifique que seu alvo não está mais acessível.

Roteador R1

```
ip sla 1
 icmp-echo 10.0.0.10 source-interface GigabitEthernet2/0
 threshold 2
ip sla schedule 1 life forever start-time now
```

```
ip route 0.0.0.0 0.0.0.0 10.0.0.10 track 1
ip route 0.0.0.0 0.0.0.0 10.0.0.14 10
```

Roteador R4

```
ip sla 2
 icmp-echo 10.0.0.21 source-interface GigabitEthernet1/0
 threshold 2
ip sla schedule 2 life forever start-time now
```

```
ip route 0.0.0.0 0.0.0.0 10.0.0.21 track 2
ip route 0.0.0.0 0.0.0.0 10.0.0.25 10
```

Figura 5.64: Exibição da configuração da solução IP SLA *Tracking*. Fonte própria.

Dessa forma, a Figura 5.65 exibe de maneira ilustrativa o funcionamento da solução IP SLA *Tracking* na topologia deste projeto.

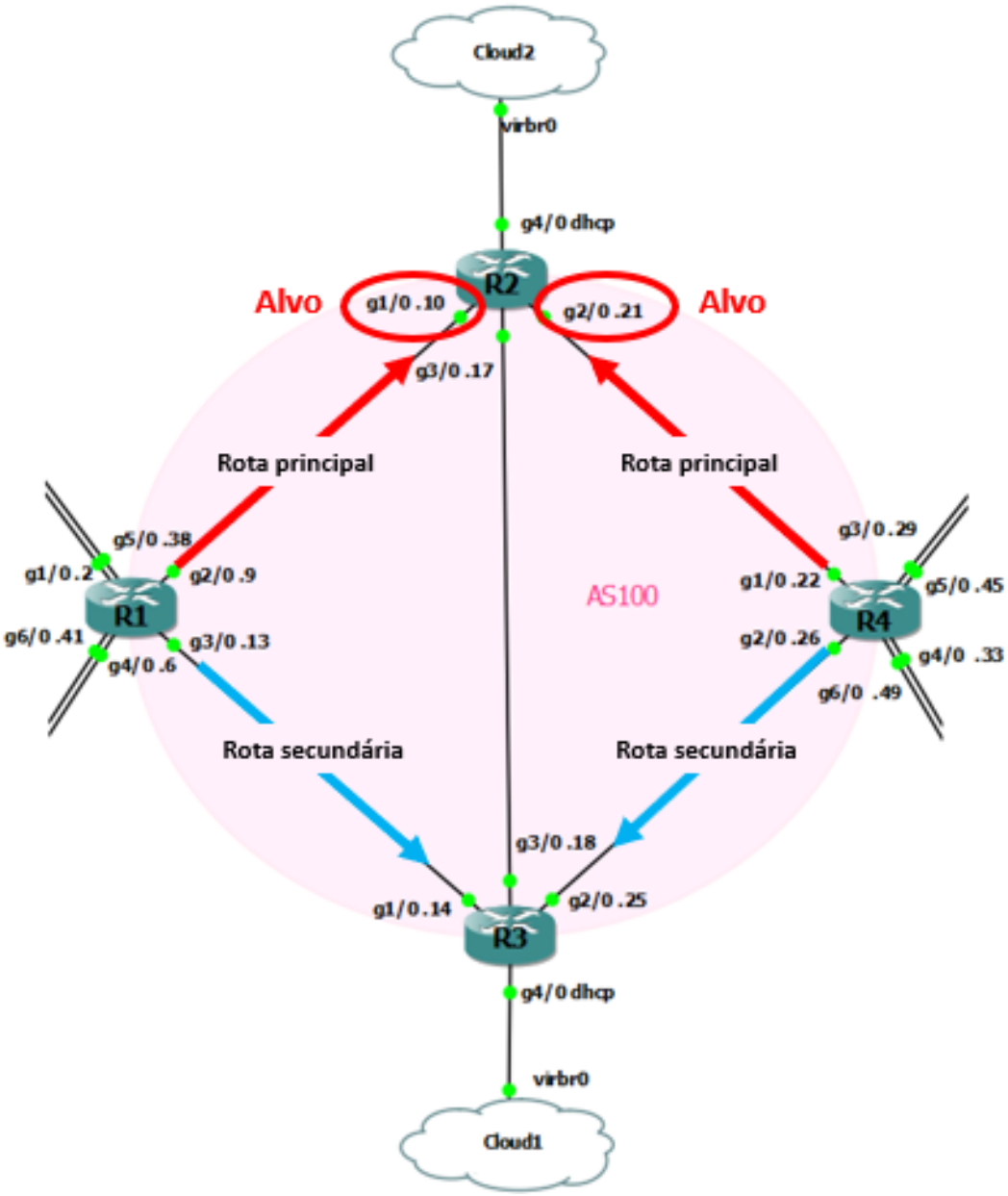


Figura 5.65: Exibição da solução IP SLA *Tracking* na topologia *backbone* do projeto. Fonte própria.

A partir disso, ao inserir o comando "*show ip route*" nos roteadores R1 e R4 será possível verificar qual rota *default* está sendo empregada. Conforme pode ser visto na Figura 5.66, verifica-se que a configuração foi realizada corretamente, já que neste primeiro caso, o roteador R2 considerado o *Active Router* está em perfeito funcionamento. Assim, caso os vizinhos precisem se comunicar com a rede externa presente no Laboratório de Redes da UnB através da *Cloud*, essa comunicação será realizada com destino ao roteador R2, já que ele contém a rota principal para a saída de Internet.

A fim de verificar a redundância disponibilizada pelo protocolo HSRP e o funcionamento da rota *default* de *backup*, os *links* referentes ao *Active Router* foram suspensos, conforme observado

na Figura 5.67.

Roteador R1

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.10 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.0.0.10, 00:00:35, GigabitEthernet2/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.0.0.14, 00:00:25, GigabitEthernet3/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/3] via 10.0.0.14, 00:00:25, GigabitEthernet3/0
                [110/3] via 10.0.0.10, 00:00:25, GigabitEthernet2/0
     10.0.0.0/30 is subnetted, 5 subnets
C       10.0.0.8 is directly connected, GigabitEthernet2/0
C       10.0.0.12 is directly connected, GigabitEthernet3/0
O       10.0.0.24 [110/2] via 10.0.0.14, 00:00:25, GigabitEthernet3/0
O       10.0.0.16 [110/2] via 10.0.0.14, 00:00:26, GigabitEthernet3/0
                  [110/2] via 10.0.0.10, 00:00:26, GigabitEthernet2/0
O       10.0.0.20 [110/2] via 10.0.0.10, 00:00:26, GigabitEthernet2/0
S*   0.0.0.0/0 [1/0] via 10.0.0.10
```

Rota estática principal

Roteador R4

```
R4#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.21 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/3] via 10.0.0.25, 00:00:56, GigabitEthernet2/0
                [110/3] via 10.0.0.21, 00:01:06, GigabitEthernet1/0
     2.0.0.0/32 is subnetted, 1 subnets
O       2.2.2.2 [110/2] via 10.0.0.21, 00:01:07, GigabitEthernet1/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.0.0.25, 00:00:57, GigabitEthernet2/0
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 5 subnets
O       10.0.0.8 [110/2] via 10.0.0.21, 00:01:07, GigabitEthernet1/0
O       10.0.0.12 [110/2] via 10.0.0.25, 00:00:57, GigabitEthernet2/0
C       10.0.0.24 is directly connected, GigabitEthernet2/0
O       10.0.0.16 [110/2] via 10.0.0.25, 00:00:57, GigabitEthernet2/0
                  [110/2] via 10.0.0.21, 00:00:57, GigabitEthernet1/0
C       10.0.0.20 is directly connected, GigabitEthernet1/0
S*   0.0.0.0/0 [1/0] via 10.0.0.21
```

Rota estática principal

Figura 5.66: Verificação da rota *default* nos roteadores de borda da provedora. Fonte própria.

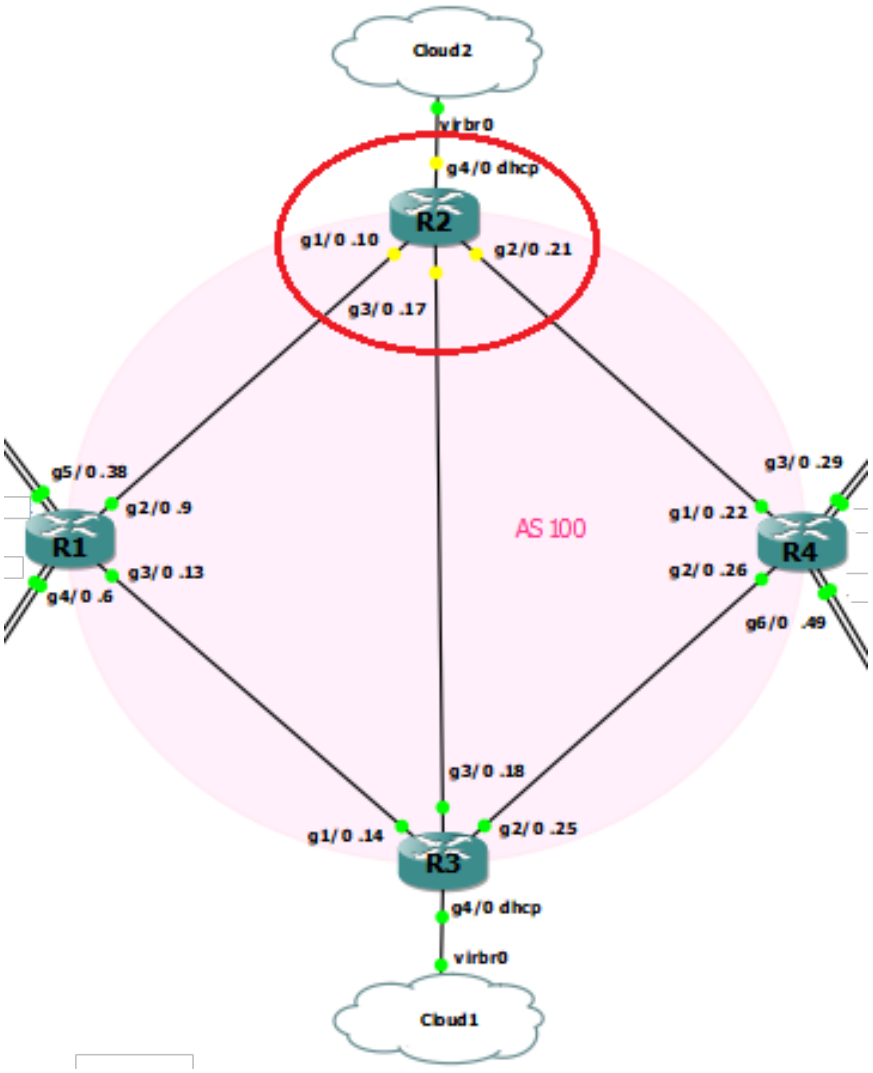


Figura 5.67: Suspensão de R2 a fim de verificar a redundância disponibilizada. Fonte própria.

A partir disso, observou-se nos roteadores de borda da provedora R1 e R4 que a acessibilidade ao alvo definido pelo IP SLA *Tracking* ficou inacessível a partir dos seguintes logs:

Roteador R1

```
*Nov 28 22:20:12.475: %TRACKING-5-STATE: 1 ip sla 1 reachability Up->Down
```

Roteador R4

```
*Nov 28 22:19:40.411: %TRACKING-5-STATE: 2 ip sla 2 reachability Up->Down
```

Figura 5.68: Alvo definido pelo IP SLA *Tracking* com *status* "*down*". Fonte própria.

Dessa maneira, a roda secundária deve ser utilizada para que a comunicação entre dispositivos vizinhos e dispositivos conectados à *Cloud* ocorra. É possível verificar a rota de *backup* sendo assumida através do comando "*show ip route*". A saída deste comando nos roteadores R1 e R4 está presente na Figura 5.69.

Roteador R1

```
R1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.14 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
C       1.1.1.1 is directly connected, Loopback0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.0.0.14, 00:05:53, GigabitEthernet3/0
     4.0.0.0/32 is subnetted, 1 subnets
O       4.4.4.4 [110/3] via 10.0.0.14, 00:05:43, GigabitEthernet3/0
     10.0.0.0/30 is subnetted, 5 subnets
C       10.0.0.8 is directly connected, GigabitEthernet2/0
C       10.0.0.12 is directly connected, GigabitEthernet3/0
O       10.0.0.24 [110/2] via 10.0.0.14, 00:05:43, GigabitEthernet3/0
O       10.0.0.16 [110/2] via 10.0.0.14, 00:05:53, GigabitEthernet3/0
O       10.0.0.20 [110/3] via 10.0.0.14, 00:01:23, GigabitEthernet3/0
S*   0.0.0.0/0 [10/0] via 10.0.0.14  Rota estática secundária assumiu
```

Roteador R4

```
R4# sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.0.0.25 to network 0.0.0.0

     1.0.0.0/32 is subnetted, 1 subnets
O       1.1.1.1 [110/3] via 10.0.0.25, 00:06:21, GigabitEthernet2/0
     3.0.0.0/32 is subnetted, 1 subnets
O       3.3.3.3 [110/2] via 10.0.0.25, 00:06:21, GigabitEthernet2/0
     4.0.0.0/32 is subnetted, 1 subnets
C       4.4.4.4 is directly connected, Loopback0
     10.0.0.0/30 is subnetted, 5 subnets
O       10.0.0.8 [110/3] via 10.0.0.25, 00:02:00, GigabitEthernet2/0
O       10.0.0.12 [110/2] via 10.0.0.25, 00:06:21, GigabitEthernet2/0
C       10.0.0.24 is directly connected, GigabitEthernet2/0
O       10.0.0.16 [110/2] via 10.0.0.25, 00:06:21, GigabitEthernet2/0
C       10.0.0.20 is directly connected, GigabitEthernet1/0
S*   0.0.0.0/0 [10/0] via 10.0.0.25  Rota estática secundária assumiu
```

Figura 5.69: Verificação da rota *default* secundária nos roteadores de borda da provedora. Fonte própria.

Além disso, para verificar a redundância do protocolo HSRP, no qual o roteador R3 deve assumir como *Active Router* para que a comunicação com a *Cloud* não seja perdida ao obter a falha no roteador R2, utilizou-se o comando "*debug standby*" a fim de observar os *logs* obtidos a partir da queda do roteador R2, que antes era considerado o *Active Router*.

A Figura 5.70 expõe alguns dos eventos obtidos após a suspensão dos *links* físicos do roteador R2. Primeiramente, observou-se que o temporizador do *Active Router* com IP 192.168.122.222, referente ao roteador R2, expirou. Em seguida, o HSRP informou que este dispositivo não está mais acessível para o grupo 1 configurado. Dessa maneira, verifica-se que o roteador R3 assume o papel de *Active Router*. Além disso, observa-se também que o roteador R3 envia pacotes do tipo *Hello* com informações de endereço IP físico, *status*, prioridade e endereço VIP.

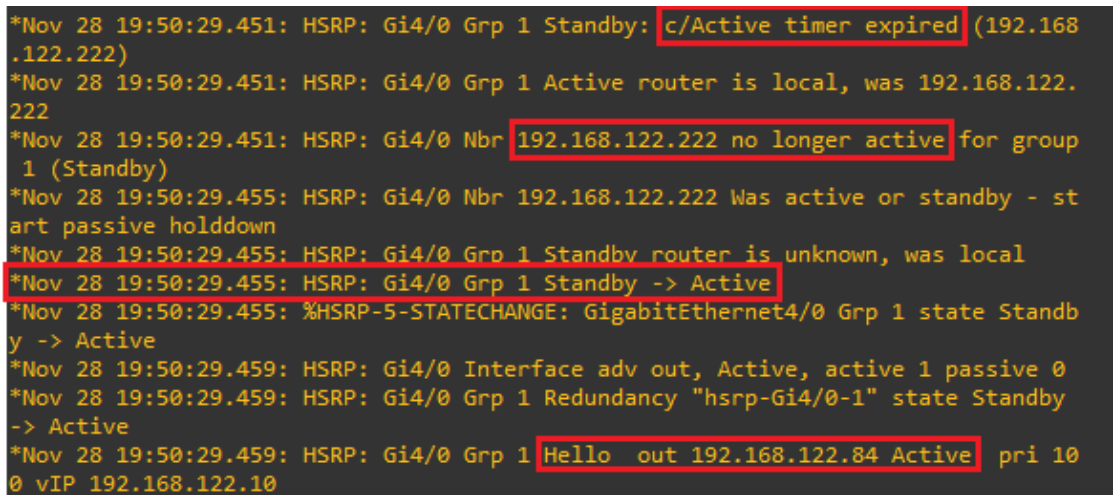


Figura 5.70: *Logs* do protocolo HSRP após a suspensão de R2. Fonte própria.

É possível também verificar estas informações na Figura 5.71, a partir do comando "*show standby*" já utilizado anteriormente.

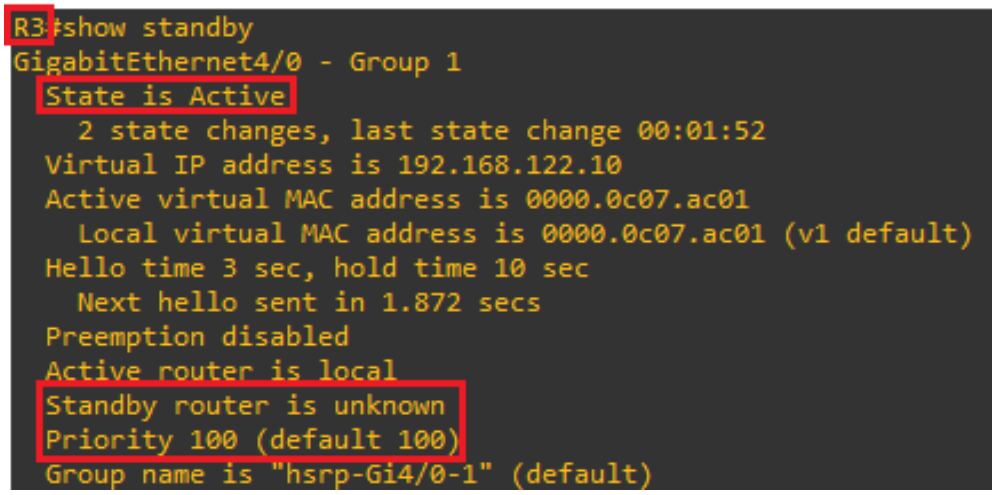


Figura 5.71: Informações de *status* HSRP de R3 após a suspensão de R2. Fonte própria.

Por fim, verifica-se na Figura 5.72 o sucesso da comunicação com a rede do servidor GNS3 presente no Laboratório de Redes através da *Cloud* conectada ao roteador R3, a partir do comando *PING*.

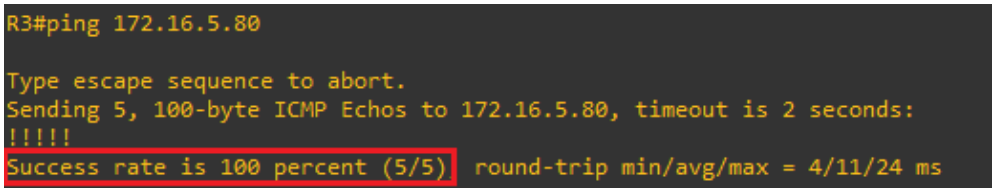


Figura 5.72: Teste de conectividade após suspensão de R2. Fonte própria.

A partir destas análises, conclui-se que a tecnologia MPLS L3VPN implementada neste projeto

atua de maneira correta e funcional resultando em diversos benefícios para a rede *Backbone* da provedora, como: controle granular sobre para onde os pacotes serão transmitidos; comutação eficiente dos fluxos de dados através da rede; redução de esforços operacionais; redução de riscos de indisponibilidade e escalabilidade *Layer* 2 e *Layer* 3. Além disso, o projeto obteve sucesso na configuração de alta disponibilidade nos roteadores com acesso à rede externa, referente ao ambiente do Laboratório de Redes do Departamento de Engenharia Elétrica, com a utilização do protocolo HSRP e rotas estáticas de *backup* com IP SLA *Tracking*.

5.3 SD-WAN ADVPN

Com a configuração da tecnologia SD-WAN ADVPN, conforme as etapas descritas no capítulo 4, é possível realizar algumas análises a fim de observar o funcionamento desta tecnologia e seus benefícios, como a automatização do tráfego com base em fatores determinados pelo SLA, gerenciamento simplificado, monitoramento centralizado e redundância de conexão entre os sites.

Conforme mencionado ao longo deste trabalho, a topologia em questão envolve a junção de duas tecnologias, sendo: MPLS L3VPN para conexão com a Internet através do *backbone* e a solução SD-WAN que foi implementada em todos os campus a fim de obter maior desempenho e maximização da disponibilidade dos serviços. Com isso, a comunicação entre os campus ocorre a partir da configuração da tecnologia de SD-WAN com tunelamento dinâmico – *Auto-Discovery* VPN (ADVPN), onde túneis IPsec são implementados entre os sites.

É importante mencionar a diferenciação entre SD-WAN e VPN. As duas tecnologias possuem como objetivo, a conexão de rede de maneira criptografada, no qual gera camadas de segurança a partir de certas regras preestabelecidas. A solução SD-WAN atua como um *gateway* para uma rede e otimiza o roteamento do tráfego de dados em múltiplas conexões, oferecendo escalabilidade, confiabilidade e alto desempenho. Já a VPN, fornece conectividade ponto a ponto entre um dispositivo e uma rede, ou entre duas redes, e encaminha o tráfego de dados através de uma única conexão (BROWN, 2023).

A solução SD-WAN da fabricante Fortinet implementada neste projeto segue o princípio de 5 pilares, conforme mencionado anteriormente. O segundo pilar "*Overlay*" define a topologia que interconexão entre os sites de forma que os caminhos e destinos disponíveis possam mudar de maneira dinâmica em caso de falhas na rede, migrações planejadas ou até mesmo mudanças nos padrões de tráfego. Nesse caso, a tecnologia de tunelamento dinâmico - *Auto-Discovery* VPN (ADVPN) foi utilizada, no qual túneis IPsec diretos entre os sites foram criados a fim de obter uma comunicação de natureza *Zero-Touch*, além de confidencialidade, integridade e sem gargalos na rede.

Já o quinto pilar "*SD-WAN*", se refere à inteligência aplicada a cada sessão de saída para decidir qual caminho será selecionado como ideal em um determinado momento e para uma determinada aplicação. Conforme o capítulo anterior, a tecnologia irá considerar todos os caminhos disponíveis para um destino desejado e irá realizar uma comparação de integridades em tempo real para assim, aplicar uma estratégia de negócios para uma aplicação específica. Se as condições mudarem, um

novo caminho será selecionado de maneira rápida.

Dessa maneira, a solução SD-WAN foi implementada com intuito de obter uma infraestrutura de conexão entre os campus da Universidade de Brasília de maneira redundante e eficiente a partir de SLAs de desempenho que verificarão em tempo real os seguintes parâmetros: latência, *jitter* e perda de pacotes.

Com isso, após as devidas configurações desta solução, conforme descrito no capítulo anterior, as conexões SD-WAN com ADVPN foram obtidas de forma que os campus possuam dois *links* de conectividade para cada campus remoto. A Figura 5.73 expõe os membros SD-WAN presentes na zona "SDW-VPN" do campus Darcy Ribeiro. Verifica-se que os dois túneis IPsec para cada site remoto estão em perfeito funcionamento, observa-se também a quantidade de tráfego de dados de *download* e *upload* para cada membro.

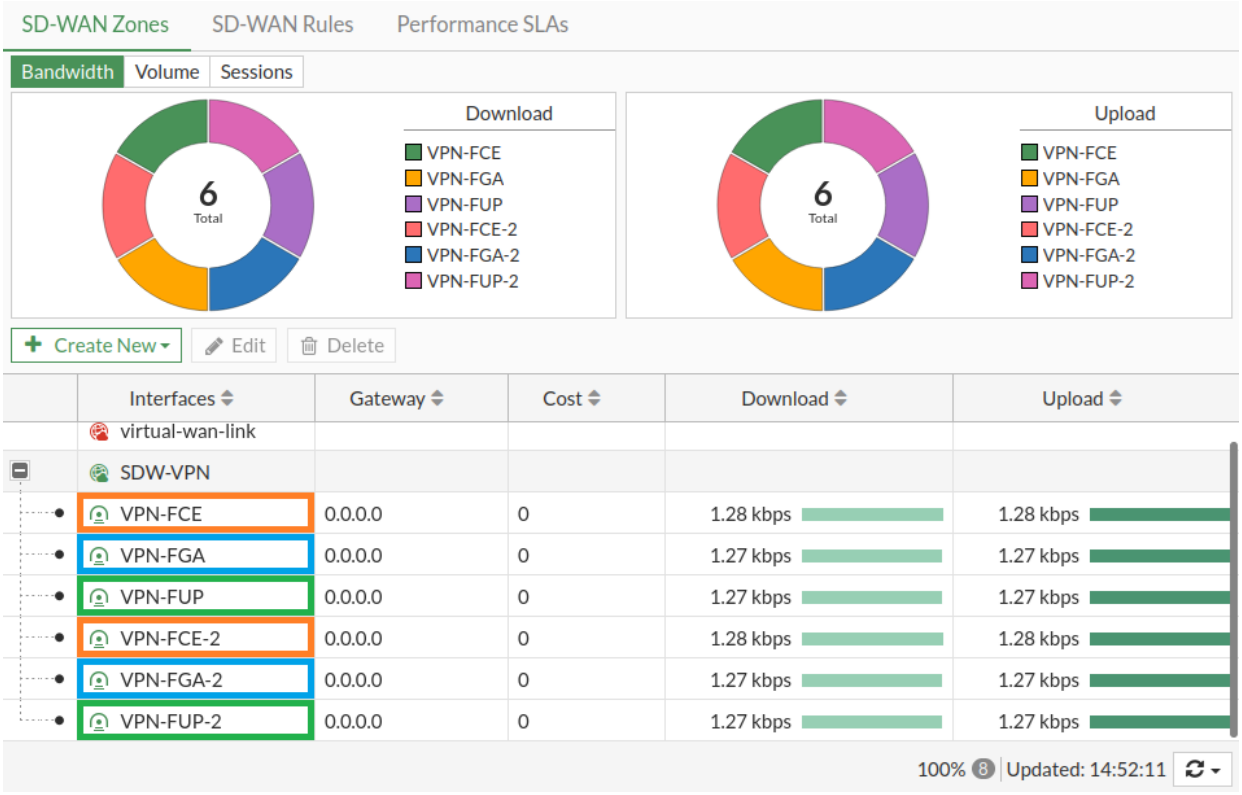


Figura 5.73: Membros SD-WAN *online* no campus Darcy Ribeiro. Fonte própria.

Além disso, regras SD-WAN foram configuradas para que a solução possa utilizar os parâmetros de qualidade de serviço a fim de obter o melhor caminho para encaminhar os dados entre os sites. Sendo assim, cada campus realiza verificações de integridade para mensurar e avaliar em tempo real, a integridade de cada caminho disponível para um determinado campus de destino, considerando o *status* do túnel IPsec e o *status* do SLA de desempenho.

Dessa maneira, a Figura 5.74 exibe as regras SD-WAN configuradas no campus Darcy Ribeiro, no qual utiliza os parâmetros de SLA definidos para cada pólo universitário remoto com o objetivo de definir qual o melhor caminho para transmissão de dados de um campus a outro. Verifica-

se que na coluna "*Members*" um ícone de *check* é exibido, isso indica por qual túnel IPsec a comunicação ocorre com melhor qualidade de serviço naquele momento, a partir da análise conjunta dos parâmetros de latência, *jitter* e perda de pacotes configurados. Além disso, observa-se também as verificações dos SLAs de desempenho para cada site remoto, no qual é possível observar as taxas de perda de pacote, valores de latência e *jitter* em milissegundos para cada um dos caminhos possíveis.

Regras SD-WAN

ID	Name	Source	Destination	Criteria	Members	Hit Count
IPv4 3						
1	SDW-FCE-ICMP	DARCY-VLAN10-LOCAL	FCE-VLAN10-REMOTE	Latency	VPN-FCE ✓ VPN-FCE-2	8
2	SDW-FGA-ICMP	DARCY-VLAN10-LOCAL	FGA-VLAN10-REMOTE	Latency	VPN-FGA ✓ VPN-FGA-2	4
3	SDW-FUP-ICMP	DARCY-VLAN10-LOCAL	FUP-VLAN10-REMOTE	Latency	VPN-FUP VPN-FUP-2 ✓	4

Verificação dos SLAs de Desempenho

Name	Detect Server	Packet Loss	Latency	Jitter	Failure Thresho
ICMP FCE	172.25.15.254	VPN-FCE: 0.00% VPN-FCE-2: 0.00%	VPN-FCE: 12.27ms VPN-FCE-2: 11.97ms	VPN-FCE: 0.44ms VPN-FCE-2: 0.45ms	5
ICMP FGA	172.26.15.254	VPN-FGA: 0.00% VPN-FGA-2: 0.00%	VPN-FGA: 34.68ms VPN-FGA-2: 34.10ms	VPN-FGA: 1.52ms VPN-FGA-2: 1.61ms	5
ICMP FUP	172.27.15.254	VPN-FUP: 0.00% VPN-FUP-2: 0.00%	VPN-FUP: 32.84ms VPN-FUP-2: 35.72ms	VPN-FUP: 3.09ms VPN-FUP-2: 3.17ms	5

Figura 5.74: Regras SD-WAN e Verificações dos SLAs de Desempenho no campus Darcy Ribeiro. Fonte própria.

A partir destas análises, é possível testar a comunicação entre um campus e outro. Dessa maneira, foi realizado um teste de conectividade através do comando "*ping*" partindo do *switch* Core no Darcy Ribeiro (com IP 172.24.8.100) com destino ao *switch* Core no campus FCE (com IP 172.25.8.100), a fim de observar que transferência de dados ocorre de maneira adequada. A Figura 5.75 exibe esse teste.

```
CORE-2-DC.22 # ping 172.25.8.100
Ping(ICMP) 172.25.8.100: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.25.8.100: icmp_seq=0 ttl=62 time=17 ms
16 bytes from 172.25.8.100: icmp_seq=1 ttl=62 time=26 ms
16 bytes from 172.25.8.100: icmp_seq=2 ttl=62 time=13 ms
16 bytes from 172.25.8.100: icmp_seq=3 ttl=62 time=51 ms

--- 172.25.8.100 ping statistics ---
```

Figura 5.75: Teste de conectividade do campus Darcy Ribeiro com destino ao campus FCE. Fonte própria.

Além disso, para verificar por qual caminho essa comunicação ocorre, a captura de pacotes foi habilitada entre os dois *links* redundantes que conectam o *firewall* FortiGate com o roteador R1, conforme pode ser observado na Figura 5.76.

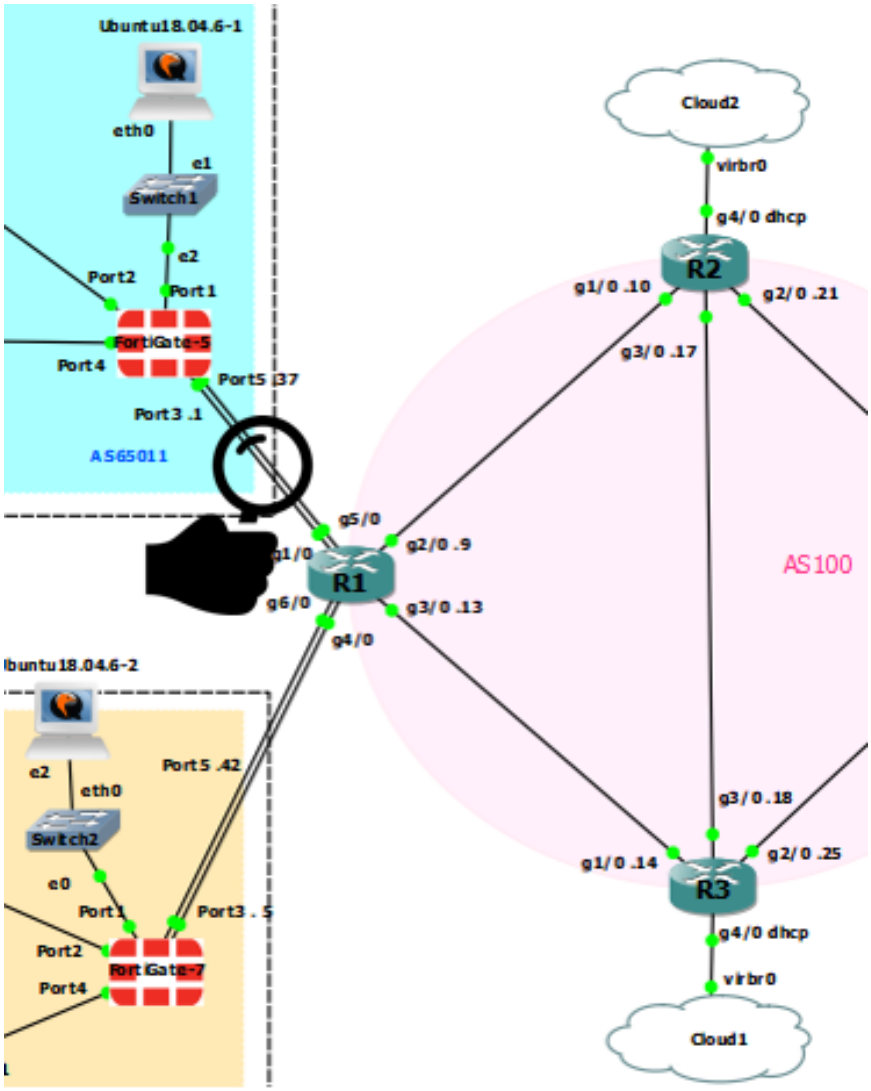


Figura 5.76: Utilização do Wireshark para verificar por qual *link* a comunicação entre Darcy e FCE ocorre. Fonte própria.

O teste de conectividade foi realizado novamente através do comando "*ping*" partindo do *switch* Core no Darcy Ribeiro (com IP 172.24.8.100) com destino ao *switch* Core no campus FCE (com IP 172.25.8.100) a fim de verificar se a comunicação ocorre através da porta WAN 3 (com IP 10.0.0.1) ou da porta WAN 5 (com IP 10.0.0.37) do *firewall*.

Verificou-se a partir da captura de pacotes nos dois *links*, utilizando o *sniffer* Wireshark, que a comunicação ocorreu através do *link underlay* referente a porta WAN 5 do *firewall*. Pacotes ICMP foram capturados nesta interface, conforme pode ser observado na Figura 5.77. Este *link* dá acesso ao túnel IPsec chamado "VPN-FCE-2".

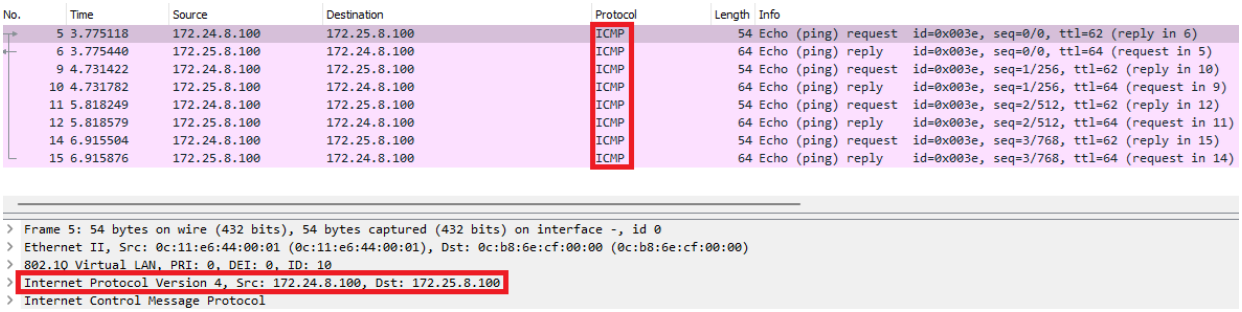


Figura 5.77: Verificação de pacotes ICMP através da interconexão de R1 com a porta WAN 5 do *firewall*. Fonte própria.

Dessa maneira, é de grande importância verificar a redundância e automatização na transferência de dados para o outro caminho disponível em caso de falhas ou perda da qualidade de serviço. Para isso, a conexão do *firewall* ao roteador R1 através da porta WAN 5 será suspensa. Neste momento, verificou-se que os membros SD-WAN referentes a esse tráfego *underlay* perderam conectividade, conforme observado na Figura 5.78.

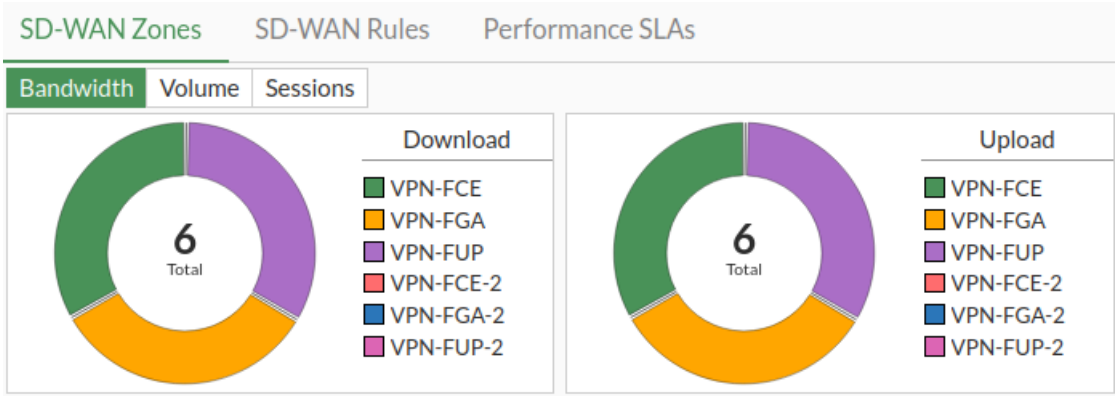


Figura 5.78: Verificação da perda de conectividade dos membros SD-WAN após a suspensão do *link*. Fonte própria.

Verifica-se também, conforme a Figura 5.79, que o melhor caminho definido neste momento para as localidades remotas se dá através dos túneis IPsec referentes ao tráfego *underlay* da porta WAN 3. Além disso, ao acessar a aba "*Performance SLAs*", observou-se que o *status* para os 3 SLAs configurados para os sites remotos, não apresenta valores definidos, devido à perda de comunicação.

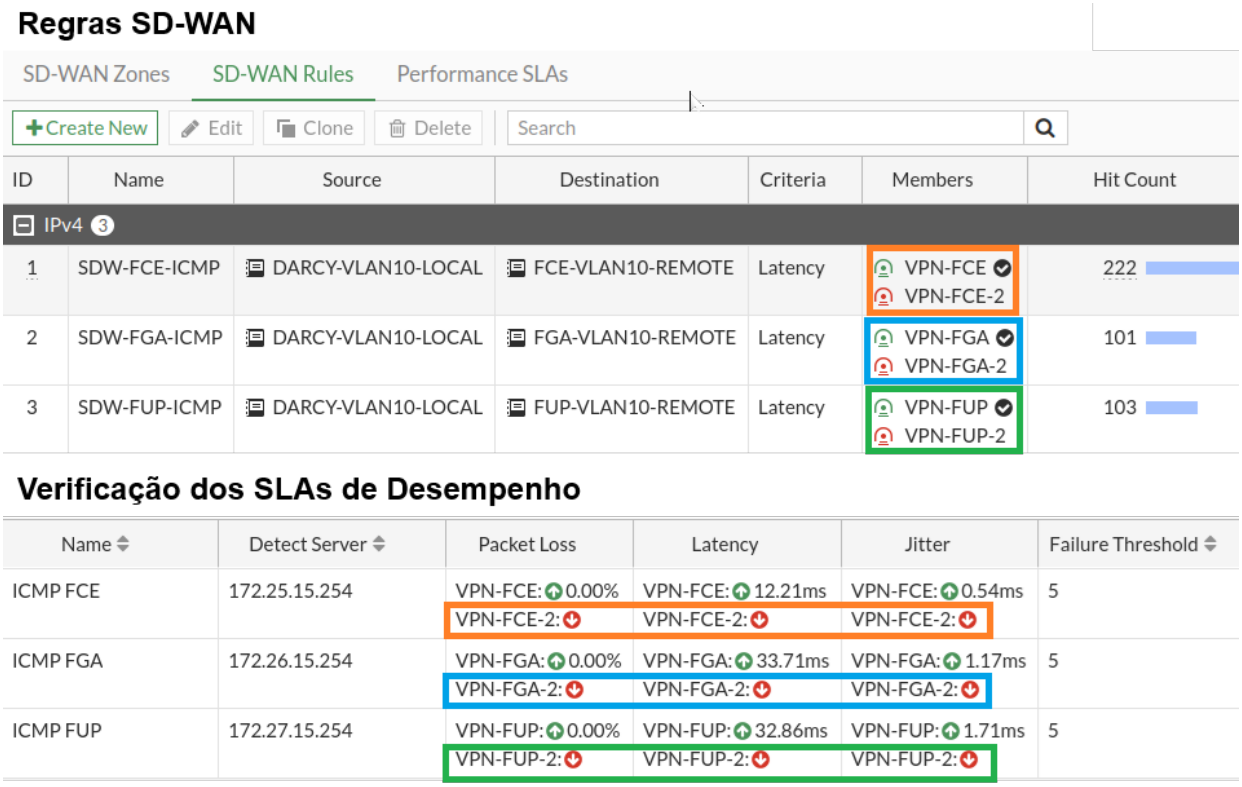


Figura 5.79: Regras SD-WAN e Verificações dos SLAs de Desempenho no campus Darcy Ribeiro após a suspensão do *link*. Fonte própria.

Entretanto, mesmo com a perda de conexão através de um dos caminhos disponíveis para os campus remotos, o outro caminho assumiu de maneira automatizada, sem nenhum tipo de intervenção adicional do operador de redes. Dessa maneira, ao realizar novamente o teste de conectividade através do comando "*ping*", a comunicação ocorre perfeitamente. Esse teste é exposto na Figura 5.80.

```
CORE-2-DC.2 # ping 172.25.8.100
Ping(ICMP) 172.25.8.100: 4 packets, 8 data bytes, interval 1 second(s).
16 bytes from 172.25.8.100: icmp_seq=0 ttl=62 time=24 ms
16 bytes from 172.25.8.100: icmp_seq=1 ttl=62 time=51 ms
16 bytes from 172.25.8.100: icmp_seq=2 ttl=62 time=50 ms
16 bytes from 172.25.8.100: icmp_seq=3 ttl=62 time=52 ms

--- 172.25.8.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% loss
```

Figura 5.80: Teste de conectividade do campus Darcy Ribeiro com destino ao campus FCE, após a suspensão do *link*. Fonte própria.

Além desta análise, é possível observar a troca de pacotes realizados pelo protocolo BGP entre o campus Darcy Ribeiro presente no AS 65011 e o roteador de borda da provedora presente no AS 100.

Sabe-se que o protocolo de roteamento dinâmico BGP é utilizado para interligar sistemas

autônomos. Dessa maneira, o BGP está situado na borda dos ASs, permitindo que o protocolo trace um mapa de conectividade. Assim como outros protocolos já estudados, o BGP utiliza mensagens para realizar a sua convergência, sendo elas: *Open*, *Keepalive*, *Update* e *Notification*. Ele ainda usufrui do protocolo TCP em sua camada de transporte para obter confiabilidade e rapidez na troca de rotas entre os *peers* BGP. Após o estabelecimento da sessão TCP utilizando a porta 179, o BGP inicia o processo de convergência realizando a troca de mensagens BGP entre os *peers* envolvidos (JONATHAS, 2022), conforme pode ser observado na Figura 5.81.

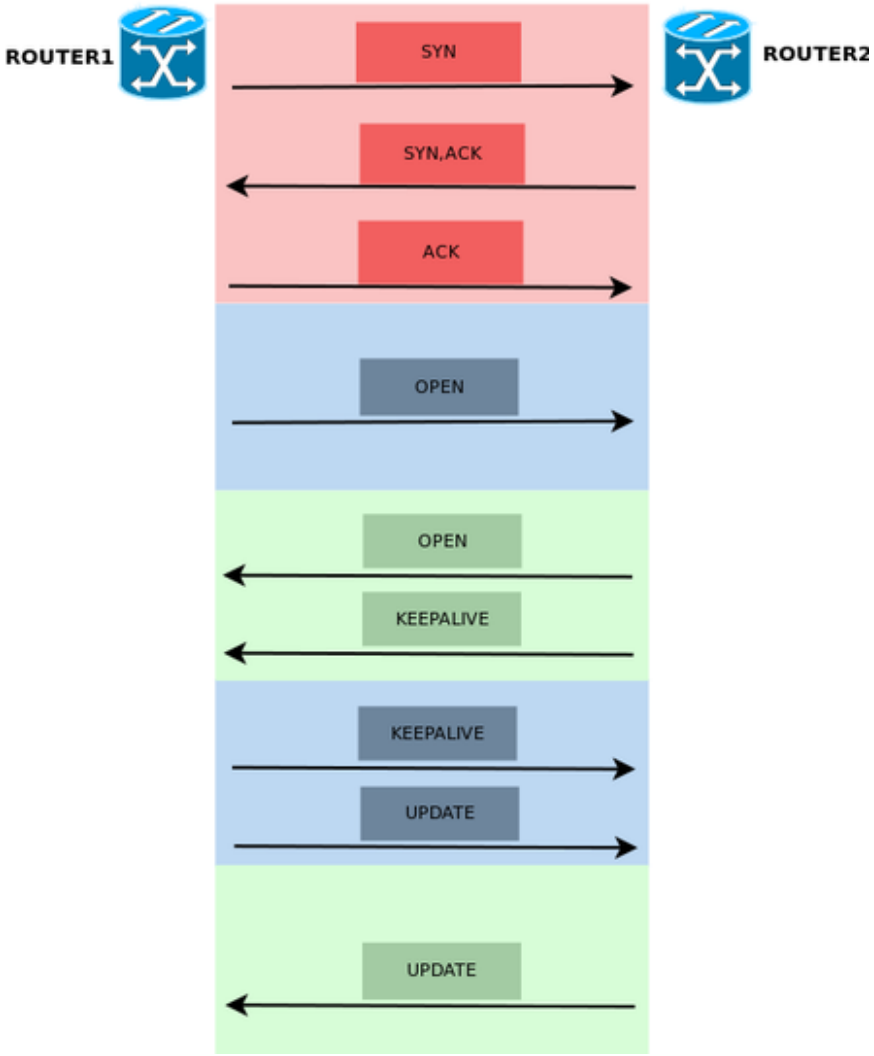


Figura 5.81: Troca de mensagens do protocolo BGP. Fonte: (JONATHAS, 2022)

Dessa maneira, ao realizar a suspensão da interface que conecta o *firewall* ao roteador R1 através da porta 5, verificou-se a partir da captura de pacotes entre a porta 3 do *firewall* e R1, mensagens de atualização (*Update Message*) do protocolo BGP, como também mensagens de *Keepalive*. A Figura 5.82 exibe esses pacotes.

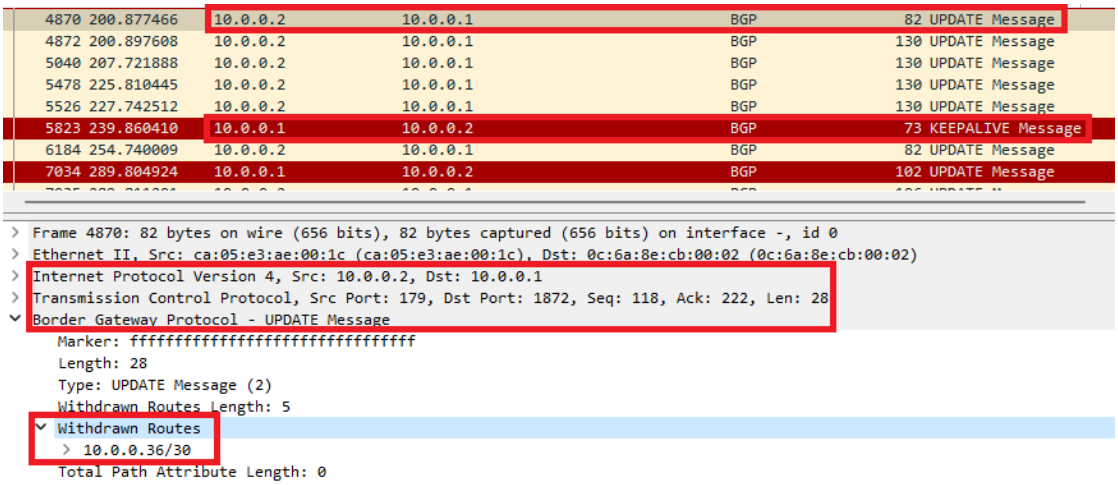


Figura 5.82: Troca de mensagens *Update* e *Keepalive* do protocolo BGP. Fonte própria.

A mensagem do tipo "*Update*" possui o objetivo de trocar informações de roteamento entre os *peers* BGP, ou seja, esse tipo de pacote propaga uma rota ou prefixo na tabela de roteamento juntamente com seus atributos. Observa-se na extremidade inferior da imagem o campo "*Withdrawn Routes*" com o valor "10.0.0.36/30", isso significa que esta sub-rede foi retirada da tabela de roteamento, devido à suspensão do *link* realizada entre o *firewall* e o roteador R1. Observa-se ainda a troca de mensagens *Keepalive* que são enviadas a cada 60 segundos, e que possui a função de manter a sessão TCP estabelecida entre os *peers*.

Além disso, ao realizar a queda de conexão do *link*, é possível observar alguns relatórios gráficos oferecidos na solução SD-WAN da Fortinet, referentes aos SLAs configurados. Como por exemplo, o SLA "ICMP-FCE" configurado no Darcy Ribeiro obtido com o objetivo de verificar o melhor caminho entre estes campus, utiliza para essa decisão os parâmetros de latência, *jitter* e perda de pacotes. Neste caso, as Figuras 5.83, 5.84 e 5.85 expõem os gráficos para estes 3 tipos de parâmetros, respectivamente.

Verifica-se que a partir de um determinado momento, a queda do túnel IPsec "VPN-FCE-2" se torna visível neste gráfico de gerenciamento, no qual apenas a latência e *jitter* referente ao caminho "VPN-FCE" é registrado, e a taxa de perda de pacotes aumenta gradativamente até atingir 100%.

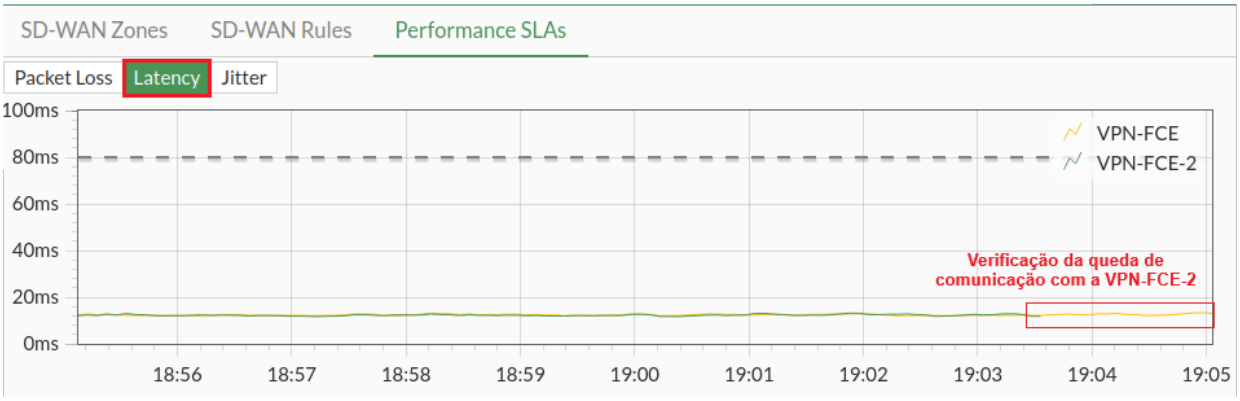


Figura 5.83: Gráfico de *Perfomance* referente a latência para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro. Fonte própria.

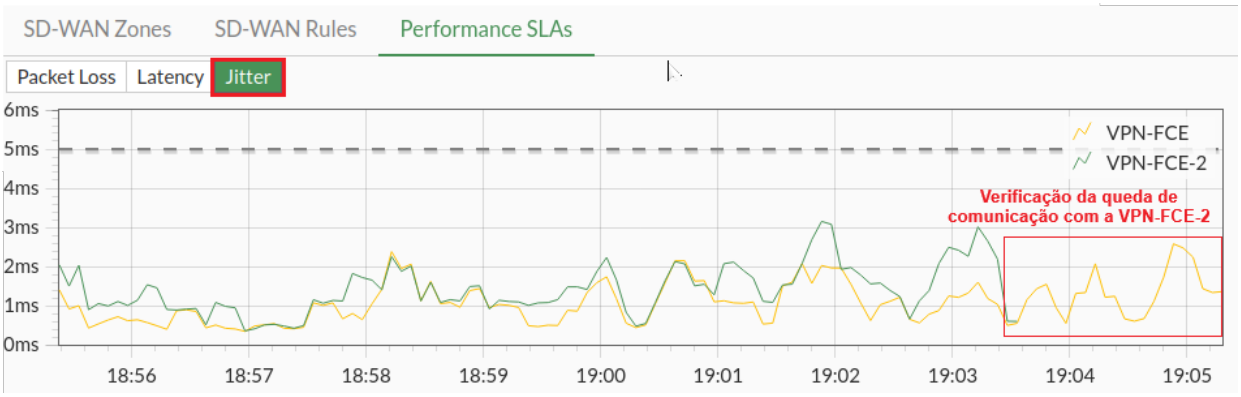


Figura 5.84: Gráfico de *Perfomance* referente a *jitter* para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro. Fonte própria.

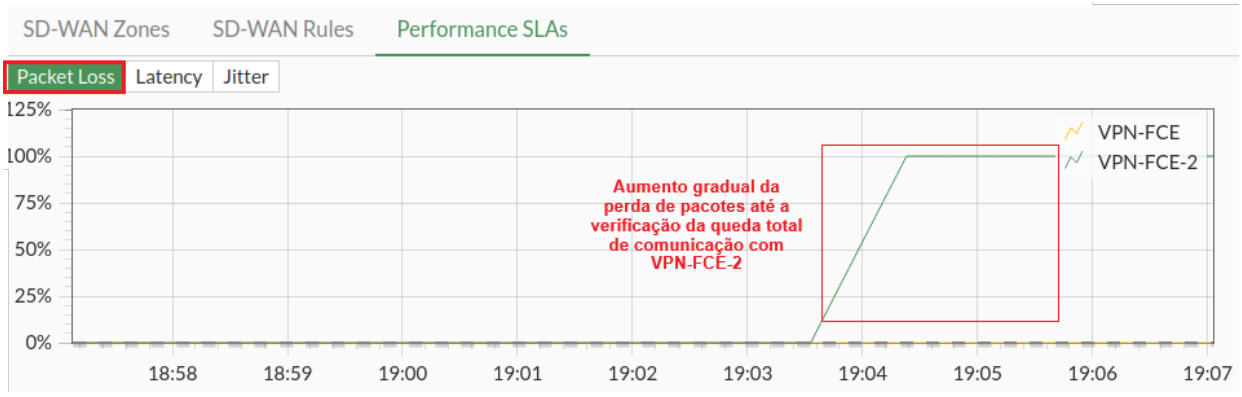


Figura 5.85: Gráfico de *Perfomance* referente a *packet loss* para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro. Fonte própria.

Após a validação de redundância dos caminhos configurados e a verificação da inteligência e automação da solução SD-WAN, o *link* suspenso voltou ao *status* "*up*", dessa maneira, a tecnologia proposta verifica o retorno do caminho referente ao túnel IPsec "VPN-FCE-2" e os parâmetros de

SLA são registrados novamente, conforme observado nas Figura 5.86, 5.87 e 5.88.

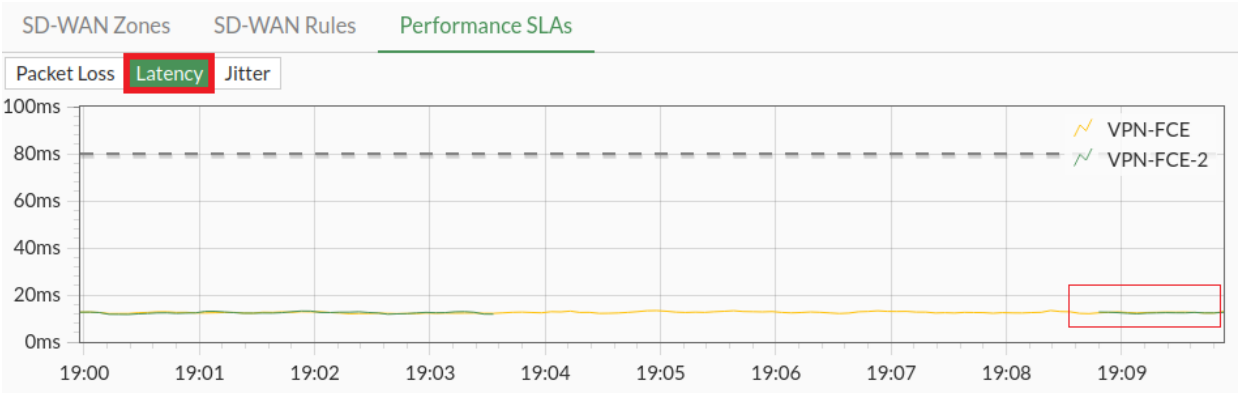


Figura 5.86: Gráfico de *Perfomance* referente a latência para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro, após o retorno do *link*. Fonte própria.

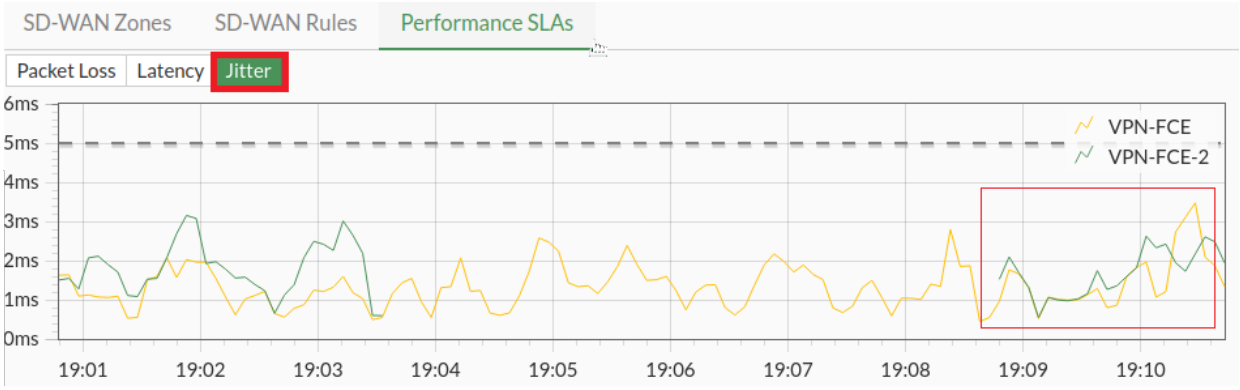


Figura 5.87: Gráfico de *Perfomance* referente a *jitter* para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro, após o retorno do *link*. Fonte própria.

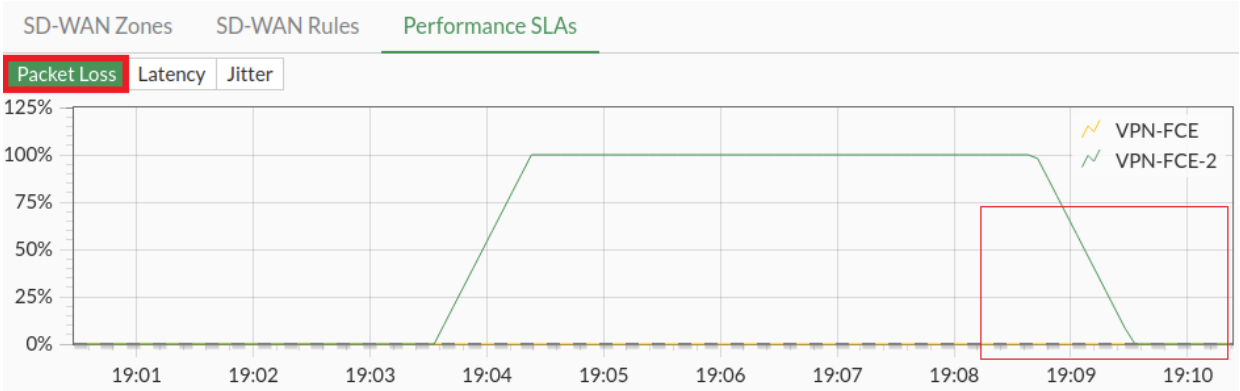


Figura 5.88: Gráfico de *Perfomance* referente a *packet loss* para o SLA "*ICMP-FCE*"do campus Darcy Ribeiro, após o retorno do *link*. Fonte própria.

Por fim, uma captura de pacotes foi realizada entre o *link* que conecta a porta 5 do *firewall* ao roteador R1 no momento em que essa conexão foi restabelecida, a fim de verificar a troca de

pacotes BGP. A Figura 5.89 exibe os pacotes capturados.

Figura 5.89: Troca de pacotes BGP no momento em que a conexão entre a porta WAN 5 do *firewall* e o roteador R1 foi restabelecida. Fonte própria.

A partir disso, verifica-se a troca de mensagens BGP entre os *peers*, neste caso, o *firewall* com IP 10.0.0.37 e o roteador R1 com IP 10.0.0.38. Primeiramente, o *Three-Way Handshake* do protocolo TCP é observado, com o objetivo de obter confiabilidade e rapidez na troca de rotas entre os *peers* BGP.

Em seguida, o roteador R1 envia uma mensagem do tipo "*Open*" para o *firewall*. Esta é a primeira mensagem a ser trocada após o estabelecimento da sessão TCP, neste pacote algumas informações são transmitidas, como: versão do protocolo, identificação do sistema autônomo, *Hold Time*, identificação do BGP e parâmetros adicionais. Se uma mensagem "*Open*" é aceitável, então uma mensagem "*Keepalive*" é enviada como resposta (JONATHAS, 2022).

Dessa forma, observa-se que o *firewall* retorna ao roteador R1 uma mensagem do tipo "*Open*" com as suas respectivas informações, juntamente com uma mensagem do tipo "*Keepalive*", enviada a cada 60 segundos, que atua como resposta da mensagem "*Open*", além também de manter a sessão TCP entre os *peers*.

Após a troca dessas mensagens, o roteador R1 envia uma mensagem "*Keepalive*" como resposta da mensagem "*Open*" enviada pelo *firewall*. Além disso, o roteador envia uma mensagem do tipo "*Update*" a fim de realizar a troca de informações de roteamento entre os *peerings* BGP juntamente com seus atributos. Por fim, o *firewall* também envia uma mensagem do tipo "*Update*" contendo os dados de roteamento e prefixo.

A partir destas análises, conclui-se que a tecnologia SD-WAN implementada neste projeto para garantir alta disponibilidade e eficiência de conexão entre os campus foi realizada com sucesso, no qual foi verificado a automatização do tráfego a partir do melhor canal de comunicação com base em fatores de qualidade de serviço estabelecidos previamente garantindo agilidade, otimização e segurança aos usuários da universidade. Além disso, verificou-se que essa tecnologia oferece simplicidade no gerenciamento ao desacoplar o *hardware* de rede de seu mecanismo de controle e monitoramento centralizado para direcionar o tráfego de forma segura e inteligente. Por fim, foi possível verificar a troca de pacotes BGP realizados entre os dispositivos clientes e os roteadores

de borda da provedora, o qual garante estabilidade na rede, convergência rápida e confiabilidade na comunicação.

Capítulo 6

Conclusão

É possível afirmar que há pelo menos uma característica que permanece constante mesmo com o passar dos séculos: a necessidade humana de estabelecer conexão. O estabelecimento de conexão entre usuários localizados em LANs diferentes, que compõem uma rede WAN foi discutido e implementado neste projeto final de graduação. É de muita valia e privilégio estudar e propor projetos de engenharia no século XXI, onde a tecnologia se encontra avançada ao ponto de atender nossas necessidades de maneira primorosa. Apesar de não termos abordado todo o *background* da história da Internet e das redes de comunicação que antecederam a data de publicação deste projeto, é preciso ficar claro que as tecnologias e descobertas do passado contribuíram para que o projeto aqui proposto se tornasse real.

Este projeto contribuiu de forma a promover o estudo de implementação de infraestrutura de redes WAN quando se há a utilização de SD-WAN em conjunto com tecnologias de última geração, que atuaram atendendo requisitos de alta disponibilidade, qualidade de serviço, segurança e confiabilidade. O cenário de implementação foi uma arquitetura de redes hipotética da Universidade de Brasília, englobando os seus quatro campus localizados em espaços geográficos diferentes, conectados com a utilização do MPLS como serviço de transporte legado presente no *backbone* da provedora a fim de oferecer acesso à Internet. Além disso, a implementação da solução SD-WAN nesta infraestrutura fornece conectividade entre os diferentes campus da UnB.

A idealização e implementação deste projeto só se tornou possível a partir de estudos extensos com relação a utilização da tecnologia SD-WAN nos dias atuais, olhando sob uma óptica de infraestrutura de redes WAN. A tecnologia SD-WAN oferecida pelo FortiGate foi escolhida, primeiro pelo fato da Fortinet oferecer gratuitamente uma versão de seus *firewalls*, como mostrado na seção 4.3.2.a, mas também por oferecer uma solução robusta, que está de acordo com as demandas de infraestrutura de redes WAN atuais. Além disso, o *firewall* FortiGate se mostrou mais do que o ideal a ser utilizado para grandes redes de campus universitários, que estão localizados em lugares geograficamente diferentes. Assim, foi possível realizar a criação de túneis SD-WAN para a interconexão dos quatro campus da Universidade, garantindo que houvesse redundância de comunicação entre eles.

Assim como mencionado no corpo deste projeto, a infraestrutura escolhida para esta implanta-

ção refere-se a rede campus da Universidade de Brasília, no qual conta com quatro campus. Além da tecnologia SD-WAN, utilizou-se da tecnologia MPLS L3VPN no *backbone* a fim de garantir transmissão de dados entre diferentes tipos de usuários com segurança, garantia de desempenho, resiliência e consistência. A infraestrutura hipotética de redes implementada foi composta pela *intranet*, que correspondeu ao ambiente interno de cada campus, onde foram criadas regras de segurança no *firewall*, definidos os perfis de usuário da rede e também configurado os *switches* Core, de distribuição e de acesso.

Também tomou-se o cuidado de apresentar como entregável neste projeto as devidas análises da infraestrutura de rede implementada. Ao assim fazer, foi possível expor não somente a implementação da infraestrutura proposta, mas também a verificação do funcionamento da rede tanto de forma interna, entre os ativos de um mesmo campus, quanto externa, entre os usuários dos diferentes pólos universitários. Dessa maneira, na *intranet* analisou-se a conectividade e regras de segurança entre os perfis de usuários, bem como testes de redundância entre os ativos. Já no ponto de vista da rede externa, no qual o *backbone* da provedora é utilizada para realizar a conexão entre os quatro campus da UnB, foi possível analisar e realizar testes no que diz respeito à tecnologia MPLS L3VPN; ao protocolo BGP; à redundância contida na infraestrutura da provedora para acesso à Internet através das *clouds*, como também, à própria tecnologia SD-WAN ADVPN no qual verificou-se as métricas de QoS no que diz respeito à conectividade entre os campus e entre os usuários externos e internos.

Sendo assim, é garantido que o leitor, ao final da leitura deste projeto poderá obter conhecimentos teóricos no que diz respeito aos conceitos de redes e tecnologias aqui utilizados, conhecimentos práticos de como implementar uma infraestrutura entre campus universitários e ainda, a compreensão da funcionalidade e viabilidade deste projeto. Ou seja, a implementação deste projeto em um ambiente real é possível e também recomendável, visto que foi-se escolhido um conjunto de equipamentos, tecnologias e configurações de última geração, que atenderão de maneira eficaz, de acordo com as melhores práticas, as demandas que uma rede entre pólos universitários possui.

6.0.1 Trabalhos Futuros

Em decorrência da pandemia do covid-19, houve a necessidade da adaptação aos métodos digitais, no qual o *home office* foi implementado na maioria das empresas privadas e públicas no Brasil e no Mundo, representando, portanto, um novo universo, tanto para os indivíduos quanto para a infraestrutura de redes da organização.

É certo que a produção deste projeto só se tornou possível porque foi tomado como base tecnologias e conceitos já pré existentes. Enquanto estudantes de engenharia sabemos que somos responsáveis por ajudar na criação do futuro e isso também implica criar tecnologias e estudos que atendam o futuro. Assim como dito anteriormente, o ano de 2020 trouxe consigo uma mudança drástica na utilização das redes WAN, em se tratando de grandes empresas e universidades, mas é certo que os próximos anos também exigirão que sejamos flexíveis e adeptas a mudanças.

Dessa maneira, sugere-se como trabalho futuro deste projeto a implementação da arquitetura

SASE, do inglês *Secure Access Service Edge*. Esta arquitetura se baseia na entrega de serviços de rede e segurança aos usuários, aplicações e dados através da nuvem. Pois, devido ao crescimento constante da migração do trabalho presencial para o trabalho remoto ou híbrido, é observado que os usuários e aplicativos não se encontram mais nas redes corporativas físicas, dessa maneira, as medidas de segurança na borda da rede não devem depender de *appliances* de *hardware* convencionais. Sendo assim, a tecnologia SASE, com seu modelo de acesso à segurança desde a borda da rede até os serviços na nuvem, juntamente com a tecnologia SD-WAN que fornece o direcionamento automatizado do tráfego para aplicações específicas, fornecerão à infraestrutura de redes da UnB maior otimização, gerenciamento, proteção e eficiência de rede para seus funcionários e alunos.

Referências

AUGUSTINE, Agne. **O que é MPLS e qual é o seu funcionamento?** 2022. Disponível em: <https://nordvpn.com/pt-br/blog/o-que-e-mpls/#:~:text=MPLS%20(Multiprotocol%20Label%20Switching%2C%20ou,3%20dentro%20de%20diferentes%20locat%C3%A1rios.>. (acessado em: 02.07.2023).

AWATI, Rahul. **Hypertext Transfer Protocol Secure (HTTPS)**. 2022. Disponível em: <https://www.techtarget.com/searchsoftwarequality/definition/HTTPS>. (acessado em: 03.12.2023).

AWS. **O que é BGP?** s.d. Disponível em: <https://aws.amazon.com/pt/what-is/border-gateway-protocol/>. (acessado em: 27.10.2023).

AWS, WAN. **O que é uma WAN? (rede remota)**. s.d. Disponível em: <https://aws.amazon.com/pt/what-is/wan/>. (acessado em: 02.07.2023).

BELCIC, Ivan. **O que é um sniffer e como se proteger contra ele?** 2020. Disponível em: <https://www.avast.com/pt-br/c-sniffer#gref>. (acessado em: 12.11.2023).

BHARDWAJ, Amit. **What is VRF? VRF Complete Guide 2022**. 2022. Disponível em: <https://ipwithease.com/vrf-basics/>. (acessado em: 28.10.2023).

BIANCA. **Entenda o que é MPLS e otimize seu tráfego de rede com o protocolo de roteamento**. 2017. Disponível em: <https://blog.algartelecom.com.br/tecnologia/entenda-o-protocolo-mpls-conceito-tecnologia-e-evolucao/>. (acessado em: 02.07.2023).

BROWN, Schuyler. **SD-WAN vs. VPN: All You Need to Know**. 2023. Disponível em: <https://www.strongdm.com/blog/sd-wan-vs-vpn>. (acessado em: 27.11.2023).

BUENO, Cleiton. **Linux – Conhecendo e usando tcpdump e wireshark**. 2015. Disponível em: <https://cleitonbueno.com/linux-conhecendo-e-usando-tcpdump-e-wireshark/>. (acessado em: 03.12.2023).

CISCO. **Configure IP SLA Tracking for IPv4 Static Routes on an SG550XG Switch through the CLI**. 2020. Disponível em:

<https://www.cisco.com/c/en/us/support/docs/smb/switches/cisco-550x-series-stackable-managed-switches/smb5797-configure-ip-sla-tracking-for-ipv4-static-routes-on-an-sg550.html#:~:text=The%20Internet%20Protocol%20Service%20Level,specified%20in%20the%20static%20route.>. (acessado em: 23.11.2023).

CISCO. **Large Campus Switching Best Practices**. 2022. Disponível em: <https://documentation.meraki.com/Architectures_and_Best_Practices/Cisco_Meraki_Best_Practice_Design/Best_Practice_Design_-_MS_Switching/Large_Campus_Switching_Best_Practices>. (acessado em: 20.11.2023).

CLOUDFLARE. **O que é BGP? | Entenda o roteamento BGP**. s.d. Disponível em: <https://www.cloudflare.com/pt-br/learning/security/glossary/what-is-bgp/>. (acessado em: 28.10.2023).

CLOUDFLARE, WAN. **O que é uma WAN? | WAN X LAN**. s.d. Disponível em: <https://www.cloudflare.com/pt-br/learning/network-layer/what-is-a-wan/>. (acessado em: 02.07.2023).

DANRESA. **Cenários de Implantação - Quatro arquiteturas de proteção ao SD-WAN indicadas pelo Gartner**. s.d. Disponível em: <https://www.danresa.com.br/fortinet/sd-wan-cenarios.aspx>. (acessado em: 09.11.2023).

DEPTAL. **Protocolos de camada de aplicação**. s.d. Disponível em: <http://deptal.estgp.pt:9090/cisco/ccna1/course/module10/10.1.1.4/10.1.1.4.html>. (acessado em: 25.03.2022).

DIAS, Diego. **OSPF – Roteador Designado (DR) e Roteador Designado de Backup (BDR)**. 2013. Disponível em: <https://www.comutadores.com.br/ospf-roteador-designado-dr-e-roteador-designado-de-backup-bdr/>. (acessado em: 22.11.2023).

DROPBOX. **O que significa FTP?** s.d. Disponível em: <https://experience.dropbox.com/pt-br/resources/what-is-ftp>. (acessado em: 25.03.2022).

DUARTE, Otto Carlos Muniz Bandeira. **Motivação MPLS**. s.d. Disponível em: <https://www.gta.ufrj.br/grad/09_1/versao-final/mpls/Motivao.html>. (acessado em: 14.11.2023).

ERICK. **O que é um sistema autônomo (ASN)?** 2023. Disponível em: <https://www.huge-networks.com/blog/noticias/asn-o-que-e-um-sistema-autonomo>. (acessado em: 28.10.2023).

ESTEBAN, Luis Velasco. **Operation Administration and Maintenance in MPLS based Ethernet Networks**. 2023. Disponível em:

<https://www.researchgate.net/publication/228899179_Operation_Administration_and_Maintenance_in_MPLS_based_Ethernet_Networks>. (acessado em: 23.11.2023).

EXAME, Revista. **Cisco**. 2018. Disponível em: <https://www.bh1.com.br/administracao-de-marketing/cisco/>. (acessado em: 12.11.2023).

FIREWALL, Forti. **Como Criar Policy no Firewall Fortinet Fortigate**. 2020. Disponível em: <https://fortifirewall.com.br/Blog/Como-Criar-Policy-No-Firewall-Fortinet-Fortigate/b/42/>. (acessado em: 16.11.2023).

FONSECA, Fernanda Veiga Gomes da. **Multi-Protocol Label Switching**. 2019. Disponível em: <https://www.gta.ufrj.br/ensino/eel879/vf/mpls/>. (acessado em: 14.11.2023).

FORTINET. **2023 Gartner® Magic Quadrant™ for SD-WAN**. 2023. Disponível em: <https://www.fortinet.com/br/solutions/gartner-wan-edge>. (acessado em: 16.09.2023).

FORTINET, DESIGN. **Design principles**. s.d. Disponível em: <hhttps://docs.fortinet.com/document/fortigate/7.2.0/sd-wan-architecture-for-enterprise/531289/design-principles>. (acessado em: 05.07.2023).

FORTINET, DHCP. **What is Dynamic Host Configuration Protocol (DHCP)?** s.d. Disponível em: <https://www.fortinet.com/br/resources/cyberglossary/dynamic-host-configuration-protocol-dhcp#:~:text=Dynamic%20Host%20Configuration%20Protocol%20(DHCP)%20is%20a%20networking%20protocol%20for,subnet%20masks%2C%20and%20default%20gateways.>. (acessado em: 03.12.2023).

FORTINET, SLA. **Performance SLA**. s.d. Disponível em: <https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/584396/performance-sla>. (acessado em: 30.10.2023).

FREITAS, MAURICIO DADA FONSECA DE. **PROJETO E SIMULAÇÃO DE REDE MPLS**. 2013. Disponível em: <https://repositorio.utfpr.edu.br/jspui/bitstream/1/17282/2/CT_GESER_IV_2014_06.pdf>. (acessado em: 08.11.2023).

G., Ariane. **O Que é Latência e Como Isso Afeta Sua Internet**. 2023. Disponível em: <https://www.hostinger.com.br/tutoriais/o-que-e-latencia>. (acessado em: 30.10.2023).

GASPAR, Larissa. **Para que serve o Protocolo IMAP?** 2022. Disponível em: <https://www.hostgator.com.br/blog/para-que-serve-o-protocolo-imap/>. (acessado em: 03.12.2023).

GONÇALVES, José. **O Protocolo OSPF**. s.d. Disponível em: <http://www.inf.ufes.br/~zegonc/material/S.O.%20II/Protocolo%20OSPF>. (acessado em: 27.10.2023).

HANNA, Katie Terrell. **Virtual Routing and Forwarding (VRF)**. 2021. Disponível em: <https://www.techtarget.com/searchnetworking/definition/virtual-routing-and-forwarding-VRF>. (acessado em: 02.11.2023).

HUAWEI. **Traffic Classification Design**. s.d. Disponível em: <https://support.huawei.com/enterprise/en/doc/EDOC1100141247/84d8d76c/traffic-classification-design>. (acessado em: 22.11.2023).

INFORCHANNEL. **As 10 previsões da IDC para o Futuro da Conectividade**. 2022. Disponível em: <https://inforchannel.com.br/2022/11/12/as-10-previsoes-da-idc-para-o-futuro-da-conectividade/>. (acessado em: 24.10.2023).

JOHNSON, CAMERON. **What Is VoIP? The Newbie's Guide to Voice over IP**. 2023. Disponível em: <https://www.nextiva.com/blog/what-is-voip.html>. (acessado em: 27.11.2023).

JONATHAS, Iago. **Fundamentos do BGP**. 2022. Disponível em: <https://wiki.brasilpeeringforum.org/w/Fundamentos-do-bgp#FUNCIONAMENTO_DO_BGP>. (acessado em: 27.11.2023).

JUNIPER. **Midsize Enterprise Campus Solution Configuration Example**. 2020. Disponível em: <https://www.juniper.net/documentation/en_US/release-independent/nce/information-products/pathway-pages/nce/nce-143-midsize-campus.pdf>. (acessado em: 20.11.2023).

JUNIPER, LDP. **Visão geral do LDP**. 2023. Disponível em: <https://www.juniper.net/documentation/br/pt/software/junos/mpls/topics/topic-map/ldp-overview.html>. (acessado em: 08.11.2023).

KOVACS, Leando. **O que é rede WAN? [Wide Area Network]**. 2023. Disponível em: <https://tecnoblog.net/responde/o-que-e-rede-wan-wide-area-network/>. (acessado em: 02.07.2023).

LABS, PyNet. **What is VRF? Its Advantages Show Commands!** 2022. Disponível em: <https://www.linkedin.com/pulse/what-vrf-its-advantages-show-commands-pynetlabs>. (acessado em: 16.11.2023).

MACÊDO, Diego. **Entendendo os Sniffers**. 2017. Disponível em: <https://www.diegomacedo.com.br/entendendo-os-sniffers/#:~:text=Sniffing%20pode%20ser%20ativo%20ou,sniffer%20%20passivo%20%20significa%20apenas%20ouvir.>. (acessado em: 12.11.2023).

MOBILIT. **O que é SD-WAN?** 2022. Disponível em: <https://www.mobilit.com.br/o-que-e-sd-wan/>. (acessado em: 02.07.2023).

MÜLLER, Morvan Daniel. **UMA SOLUÇÃO DE AUTENTICAÇÃO FIM A FIM PARA O LDP (LABEL DISTRIBUTION PROTOCOL)**. 2002. Disponível em: <https://core.ac.uk/download/pdf/30382149.pdf>. (acessado em: 08.11.2023).

NSB. **Mercado de SD-WAN aponta crescimento de 60% e ultrapassará a marca de US$ 30 bilhões até 2026**. s.d. Disponível em: <https://nsb.com.br/mercado-sd-wan-crescimento-de-60/>. (acessado em: 24.10.2023).

ORTEGA, ANDRÉ. **Configurando MPLS L3VPN (OSPF + LDP + VRF + BGP)**. 2017. Disponível em: <https://brainwork.com.br/2017/04/18/configurando-mpls-l3vpn-ospf-ldp-vrf-bgp/>. (acessado em: 15.09.2023).

PEDRO. **A utilização da L3VPN para comunicação entre sites**. 2021. Disponível em: <https://community.cisco.com/t5/blogues-de-routing-switching/a-utiliza%C3%A7%C3%A3o-da-l3vpn-para-comunica%C3%A7%C3%A3o-entre-sites/ba-p/4505694>. (acessado em: 17.11.2023).

PINHEIRO, José. **Redes de Perímetro**. 2004. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_redes_de_perimetro.php>. (acessado em: 27.10.2023).

PINHEIRO, José Mauricio Santos. **Métricas de Qualidade de Serviço em Redes de Computadores**. 2008. Disponível em: <https://www.projetoderedes.com.br/artigos/artigo_metricas_qos_em_redes.php>. (acessado em: 30.10.2023).

PONTES, Anderson. **O que é Packet Loss**. 2023. Disponível em: <https://geniodowifi.com/glossario/o-que-e-packet-loss/>. (acessado em: 30.10.2023).

REDE, Cidadão na. **JITTER**. 2021. Disponível em: <https://cidadaonarede.nic.br/pt/videos/jitter>. (acessado em: 30.10.2023).

REDES, ACADEMIA DE. **Tolerância a falhas**. 2023. Disponível em: <https://academiaderedes.com/conteudos/protocolos-de-roteamento/tolerancia-a-falhas/>. (acessado em: 23.11.2023).

RIBEIRO, ARTHUR GUILHERME LIMA. **Alta Disponibilidade com HSRP**. 2017. Disponível em: <https://brainwork.com.br/2017/01/03/hsrp-ha/>. (acessado em: 23.11.2023).

SANTA CATARINA, Instituto Federal de. **Redes MPLS**. 2023. Disponível em: <https://wiki.sj.ifsc.edu.br/index.php/Redes_MPLS/>. (acessado em: 02.07.2023).

SANTOS, ANDRE H O. **Arquitetura de Redes TCP/IP**. 2016. Disponível em: <https://www.uniaogeek.com.br/arquitetura-de-redes-tcpip/>. (acessado em: 13.11.2023).

SOUZA, Ivan de. **Entenda o que é HTTP e o quão importante esse protocolo é para o seu site**. 2019. Disponível em: <https://rockcontent.com/br/blog/http/>. (acessado em: 25.11.2023).

TECHHUB. **MPLS L3VPN overview**. s.d. Disponível em: <https://techhub.hpe.com/eginfolib/networking/docs/switches/3600v2/5998-7619r_l3-ip-rtng_cg/content/442284574.htm>. (acessado em: 28.10.2023).

TECNOLOGIA, Brayner. **Adaptabilidade da SD-WAN.** 2019. Disponível em: <http://www.brayner.com.br/post/adaptabilidade-da-sd-wan>. (acessado em: 02.07.2023).

TOSTES, Frederico. **Por que vale a pena migrar do modelo MPLS tradicional para SD-WAN?** 2020. Disponível em: <https://www.fortinet.com/br/blog/business-and-technology/por-que-vale-la-pena-migrar-modelo-mpls-tradicional-a-sd-wan>. (acessado em: 06.09.2023).

VENKO. **Conheça as 7 etapas de uma implementação de SD-WAN**. 2022. Disponível em: <https://venkonetworks.com/noticias/conheca-as-7-etapas-de-uma%20implementacao-de-sd-wan.php>. (acessado em: 08.09.2023).

VENTURA, Felipe. **Anatel obriga provedores de internet a fornecer, no mínimo, 40% da velocidade contratada**. 2014. Disponível em: <https://gizmodo.uol.com.br/regras-anatel-banda-larga-2/#:~:text=Estabilidade%2C%20lat%C3%AAncia%20e%20jitter&text=A%20lat%C3%AAncia%2C%20por%20sua%20vez,no%20m%C3%A1ximo%2C%20a%201%25.>. (acessado em: 22.11.2023).

WEHER, Ariel S. **HSRP segunda parte**. 2009. Disponível em: <http://blog.capaocho.net/2009/09/hsrp-segunda-parte.html>. (acessado em: 23.11.2023).

ANEXOS

1. **Configurações dos *Swtiches* EXOS**

- ***Switch* EXOS CORE**

  A Figura 1 abaixo exibe as principais partes da saída do comando "*show configuration*"no qual apresenta as configurações realizadas em um *switch* Core da *intranet*.

```
configure snmp sysName "CORE-2-DC"
configure sys-recovery-level switch reset

#
# Module vlan configuration.
#
configure vlan default delete ports all
```

```
create vlan "DIRETORIA"
configure vlan DIRETORIA tag 40
create vlan "GRADUACAO"
configure vlan GRADUACAO tag 10
create vlan "POS-GRADUACAO"
configure vlan POS-GRADUACAO tag 20
create vlan "PROFESSORES"
configure vlan PROFESSORES tag 30
create vlan "SUPORTE"
configure vlan SUPORTE tag 50
configure vlan Default add ports 1-12 untagged
configure vlan DIRETORIA add ports 1-4 tagged
configure vlan GRADUACAO add ports 1-4 tagged
configure vlan POS-GRADUACAO add ports 1-4 tagged
configure vlan PROFESSORES add ports 1-4 tagged
configure vlan SUPORTE add ports 1-4 tagged
configure vlan DIRETORIA ipaddress 172.24.40.100 255.255.255.0
configure vlan GRADUACAO ipaddress 172.24.8.100 255.255.248.0
configure vlan POS-GRADUACAO ipaddress 172.24.16.100 255.255.252.0
configure vlan PROFESSORES ipaddress 172.24.30.100 255.255.255.0
configure vlan SUPORTE ipaddress 172.24.50.100 255.255.255.0
```

```
#
configure iproute add default 172.24.15.254
configure iproute add default 172.24.19.254
configure iproute add default 172.24.30.254
configure iproute add default 172.24.40.254
configure iproute add default 172.24.50.254

#
```

```
#
# Module stp configuration.
#
configure stpd s0 add vlan DIRETORIA ports 1-4 dot1d
configure stpd s0 add vlan GRADUACAO ports 1-4 dot1d
configure stpd s0 add vlan POS-GRADUACAO ports 1-4 dot1d
configure stpd s0 add vlan PROFESSORES ports 1-4 dot1d
configure stpd s0 add vlan SUPORTE ports 1-4 dot1d
```

Figura 1: Principais fragmentos do comando "*show configuration*"no *switch* Core-2 do Darcy Ribeiro. Fonte própria.

- ***Switch* EXOS DISTRIBUIÇÃO**

  A Figura 2 abaixo exibe a saída do comando "*show configuration*"no qual apresenta as configurações realizadas em um *switch* de Distribuição da *intranet*.

```
configure snmp sysName "DISTRIBUICAO-FT-B"
configure sys-recovery-level switch reset

#
# Module vlan configuration.
#
configure vlan default delete ports all
create vlan "DIRETORIA"
configure vlan DIRETORIA tag 40
create vlan "GRADUACAO"
configure vlan GRADUACAO tag 10
create vlan "POS-GRADUACAO"
configure vlan POS-GRADUACAO tag 20
create vlan "PROFESSORES"
configure vlan PROFESSORES tag 30
create vlan "SUPORTE"
configure vlan SUPORTE tag 50
configure vlan Default add ports 1-12 untagged
configure vlan DIRETORIA add ports 1-4 tagged
configure vlan GRADUACAO add ports 1-4 tagged
configure vlan POS-GRADUACAO add ports 1-4 tagged
configure vlan PROFESSORES add ports 1-4 tagged
configure vlan SUPORTE add ports 1-4 tagged
configure vlan DIRETORIA ipaddress 172.24.40.10 255.255.255.0
enable ipforwarding vlan DIRETORIA
configure vlan GRADUACAO ipaddress 172.24.8.10 255.255.248.0
enable ipforwarding vlan GRADUACAO
configure vlan POS-GRADUACAO ipaddress 172.24.16.10 255.255.252.0
enable ipforwarding vlan POS-GRADUACAO
configure vlan PROFESSORES ipaddress 172.24.30.10 255.255.255.0
enable ipforwarding vlan PROFESSORES
configure vlan SUPORTE ipaddress 172.24.50.10 255.255.255.0
enable ipforwarding vlan SUPORTE
#
configure iproute add default 172.24.15.254
configure iproute add default 172.24.19.254
configure iproute add default 172.24.30.254
configure iproute add default 172.24.40.254
configure iproute add default 172.24.50.254

# Module stp configuration.
#
configure stpd s0 add vlan DIRETORIA ports 1-4 dot1d
configure stpd s0 add vlan GRADUACAO ports 1-4 dot1d
configure stpd s0 add vlan POS-GRADUACAO ports 1-4 dot1d
configure stpd s0 add vlan PROFESSORES ports 1-4 dot1d
configure stpd s0 add vlan SUPORTE ports 1-4 dot1d
```

Figura 2: Principais fragmentos do comando "*show configuration*"no *switch* Distribuição-2 do Darcy Ribeiro. Fonte própria.

- ***Switch* EXOS ACESSO**

  A Figura 3 abaixo exibe as principais partes da saída do comando "*show configuration*"no qual apresenta as configurações realizadas em um *switch* de Acesso da *intranet*.

```
configure snmp sysName "ACESSO-ENE"
configure sys-recovery-level switch reset

#
# Module vlan configuration.
#
configure vlan default delete ports all
```

```
create vlan "DIRETORIA"
configure vlan DIRETORIA tag 40
create vlan "GRADUACAO"
configure vlan GRADUACAO tag 10
create vlan "POS-GRADUACAO"
configure vlan POS-GRADUACAO tag 20
create vlan "PROFESSORES"
configure vlan PROFESSORES tag 30
create vlan "SUPORTE"
configure vlan SUPORTE tag 50
configure vlan Default add ports 1-2,4-12 untagged
configure vlan DIRETORIA add ports 1-2 tagged
configure vlan GRADUACAO add ports 1-2 tagged
configure vlan GRADUACAO add ports 3 untagged
configure vlan POS-GRADUACAO add ports 1-2 tagged
configure vlan PROFESSORES add ports 1-2 tagged
configure vlan SUPORTE add ports 1-2 tagged
configure vlan DIRETORIA ipaddress 172.24.40.1 255.255.255.0
enable ipforwarding vlan DIRETORIA
configure vlan GRADUACAO ipaddress 172.24.8.1 255.255.248.0
enable ipforwarding vlan GRADUACAO
configure vlan POS-GRADUACAO ipaddress 172.24.16.1 255.255.252.0
enable ipforwarding vlan POS-GRADUACAO
configure vlan PROFESSORES ipaddress 172.24.30.1 255.255.255.0
enable ipforwarding vlan PROFESSORES
configure vlan SUPORTE ipaddress 172.24.50.1 255.255.255.0
enable ipforwarding vlan SUPORTE
```

```
#
configure iproute add default 172.24.50.254
configure iproute add default 172.24.40.254
configure iproute add default 172.24.30.254
configure iproute add default 172.24.19.254
configure iproute add default 172.24.15.254
```

```
# Module stp configuration.
#
configure stpd s0 add vlan DIRETORIA ports 1-2 dot1d
configure stpd s0 add vlan GRADUACAO ports 1-2 dot1d
configure stpd s0 add vlan POS-GRADUACAO ports 1-2 dot1d
configure stpd s0 add vlan PROFESSORES ports 1-2 dot1d
configure stpd s0 add vlan SUPORTE ports 1-2 dot1d
```

Figura 3: Principais fragmentos do comando "*show configuration*"no *switch* Acesso-2 do Darcy Ribeiro. Fonte própria.

2. **Configurações dos Roteadores CISCO do *Backbone***

- **Roteador de Borda da Provedora**

  As Figuras 4, 5 e 6 abaixo exibem as principais partes da saída do comando "*show running config*"no qual apresenta as configurações realizadas em um roteador de borda da provedora, presente no *backbone*.

```
hostname R1
!
boot-start-marker
boot-end-marker
!
vrf definition UNB
 rd 100:1
 !
 address-family ipv4
 route-target export 100:1
 route-target import 100:1
 exit-address-family
!
vrf definition UNB-2
 rd 100:2
 !
 address-family ipv4
 route-target export 100:2
 route-target import 100:2
 exit-address-family
!
```

```
track 1 ip sla 1 reachability
!
!
!
!
interface Loopback0
 ip address 1.1.1.1 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 vrf forwarding UNB
 ip address 10.0.0.2 255.255.255.252
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 10.0.0.9 255.255.255.252
 negotiation auto
!
interface GigabitEthernet3/0
 ip address 10.0.0.13 255.255.255.252
 negotiation auto
!
interface GigabitEthernet4/0
 vrf forwarding UNB
 ip address 10.0.0.6 255.255.255.252
 negotiation auto
!
interface GigabitEthernet5/0
 vrf forwarding UNB-2
 ip address 10.0.0.38 255.255.255.252
 negotiation auto
!
interface GigabitEthernet6/0
 vrf forwarding UNB-2
 ip address 10.0.0.41 255.255.255.252
 negotiation auto
!
```

Figura 4: Principais fragmentos do comando "*show running config*"do Roteador de borda da provedora - R1. (Parte 1). Fonte própria.

```
router ospf 10
 mpls ldp autoconfig
 router-id 1.1.1.1
 log-adjacency-changes
 network 1.1.1.1 0.0.0.0 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.12 0.0.0.3 area 0
!
```

```
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.0.0.10 track 1
ip route 0.0.0.0 0.0.0.0 10.0.0.14 10
no ip http server
no ip http secure-server
!
!
!
ip sla 1
 icmp-echo 10.0.0.10 source-interface GigabitEthernet2/0
 threshold 2
ip sla schedule 1 life forever start-time now
no cdp log mismatch duplex
```

Figura 5: Principais fragmentos do comando "*show running config*"do Roteador de borda da provedora - R1. (Parte 2). Fonte própria.

```
router bgp 100
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 4.4.4.4 remote-as 100
 neighbor 4.4.4.4 update-source Loopback0
 !
 address-family ipv4
  neighbor 4.4.4.4 activate
  no auto-summary
  no synchronization
 exit-address-family
 !
 address-family vpnv4
  neighbor 4.4.4.4 activate
  neighbor 4.4.4.4 send-community extended
 exit-address-family
 !
 address-family ipv4 vrf UNB-2
  neighbor 10.0.0.37 remote-as 65011
  neighbor 10.0.0.37 ebgp-multihop 255
  neighbor 10.0.0.37 activate
  neighbor 10.0.0.37 allowas-in
  neighbor 10.0.0.37 soft-reconfiguration inbound
  neighbor 10.0.0.42 remote-as 65012
  neighbor 10.0.0.42 ebgp-multihop 255
  neighbor 10.0.0.42 activate
  neighbor 10.0.0.42 allowas-in
  neighbor 10.0.0.42 soft-reconfiguration inbound
  no synchronization
 exit-address-family
 !
 address-family ipv4 vrf UNB
  neighbor 10.0.0.1 remote-as 65011
  neighbor 10.0.0.1 ebgp-multihop 255
  neighbor 10.0.0.1 activate
  neighbor 10.0.0.1 allowas-in
  neighbor 10.0.0.1 soft-reconfiguration inbound
  neighbor 10.0.0.5 remote-as 65012
  neighbor 10.0.0.5 ebgp-multihop 255
  neighbor 10.0.0.5 activate
  neighbor 10.0.0.5 allowas-in
  neighbor 10.0.0.5 soft-reconfiguration inbound
  no synchronization
 exit-address-family
!
```

Figura 6: Principais fragmentos do comando "*show running config*"do Roteador de borda da provedora - R1. (Parte 3). Fonte própria.

- **Roteador da Provedora**

  As Figuras 7, 8 e 9 abaixo exibem as principais partes da saída do comando "*show running config*"no qual apresenta as configurações realizadas em um roteador da provedora, presente no *backbone*.

```
hostname R2
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
!
no aaa new-model
ip source-route
no ip icmp rate-limit unreachable
ip cef
!
!
!
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
mpls label protocol ldp
!
```

Figura 7: Principais fragmentos do comando "*show running config*"do Roteador da provedora - R2. (Parte 1). Fonte própria.

```
router ospf 10
 mpls ldp autoconfig
 router-id 2.2.2.2
 log-adjacency-changes
 network 2.2.2.2 0.0.0.0 area 0
 network 10.0.0.8 0.0.0.3 area 0
 network 10.0.0.16 0.0.0.3 area 0
 network 10.0.0.20 0.0.0.3 area 0
!
ip default-gateway 192.168.122.1
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.122.1
no ip http server
no ip http secure-server
!
!
ip nat pool nat-1 192.168.122.10 192.168.122.29 prefix-length 24
ip nat inside source list 7 pool nat-1
!
access-list 7 permit 10.0.0.0 0.0.0.255
no cdp log mismatch duplex
!
!
!
!
!
mpls ldp router-id Loopback0
```

Figura 8: Principais fragmentos do comando "*show running config*"do Roteador da provedora - R2. (Parte 2). Fonte própria.

```
interface Loopback0
 ip address 2.2.2.2 255.255.255.255
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
!
interface GigabitEthernet1/0
 ip address 10.0.0.10 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
!
interface GigabitEthernet2/0
 ip address 10.0.0.21 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
!
interface GigabitEthernet3/0
 ip address 10.0.0.17 255.255.255.252
 ip nat inside
 ip virtual-reassembly
 negotiation auto
!
interface GigabitEthernet4/0
 description CONEXAO_INTERNET
 ip address dhcp
 ip nat outside
 ip virtual-reassembly
 negotiation auto
 standby 1 ip 192.168.122.10
 standby 1 priority 150
!
interface GigabitEthernet5/0
 no ip address
 shutdown
 negotiation auto
```

Figura 9: Principais fragmentos do comando "*show running config*"do Roteador da provedora - R2. (Parte 3). Fonte própria.

3. **Configurações do *Firewall* FortiGate**

   Abaixo será exibido as configurações realizadas no *firewall* de cada campus da UnB utilizando a interface *web*.

   (a) Configuração da Interface do tipo *Software Switch*:

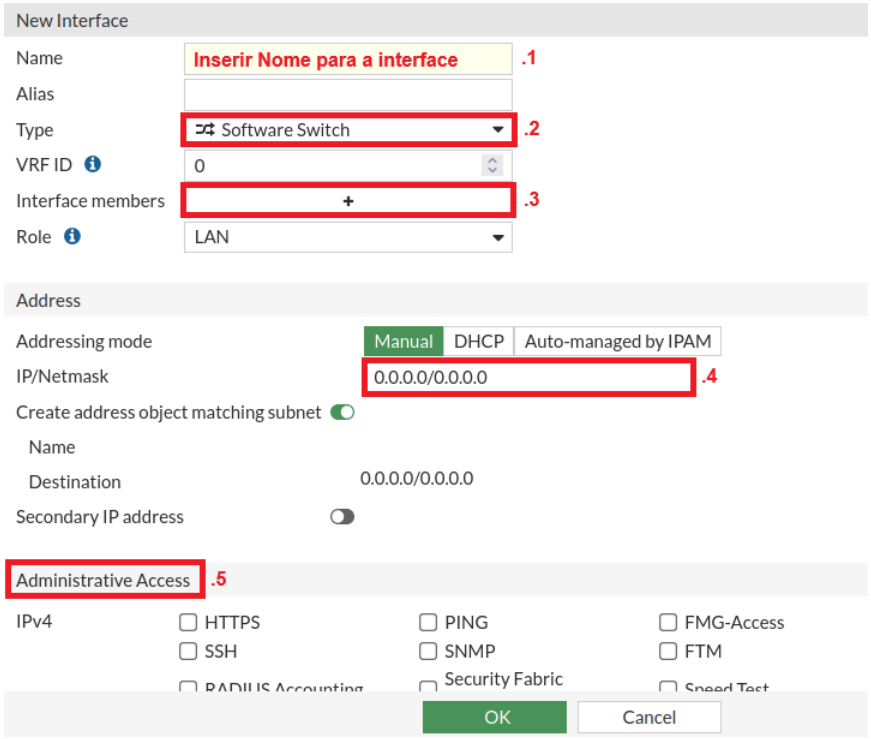


Figura 10: Etapas de configuração da interface do tipo *Software Switch*. Fonte própria.

(b) Configuração da Interface do tipo *VLAN*:

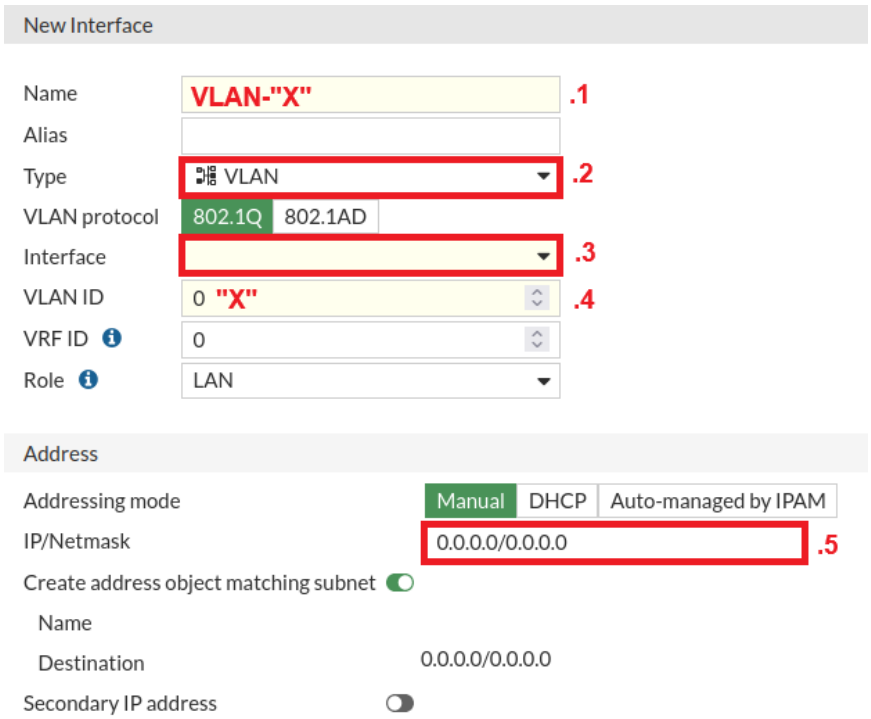


Figura 11: Etapas de configuração para as interfaces VLAN correspondentes aos tipos de usuários da rede interna. Fonte própria.

(c) Configuração da Interface física conectada ao *backbone*:

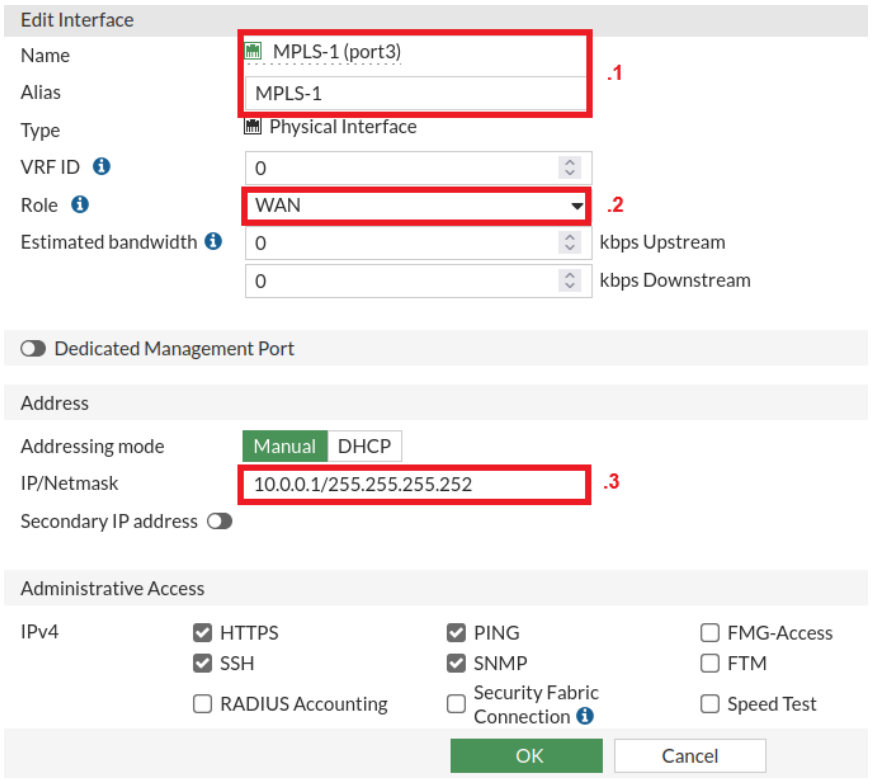


Figura 12: Configuração das interfaces físicas conectados ao backbone, no *firewall* FortiGate. Fonte própria.

(d) Configuração do protocolo de roteamento BGP:

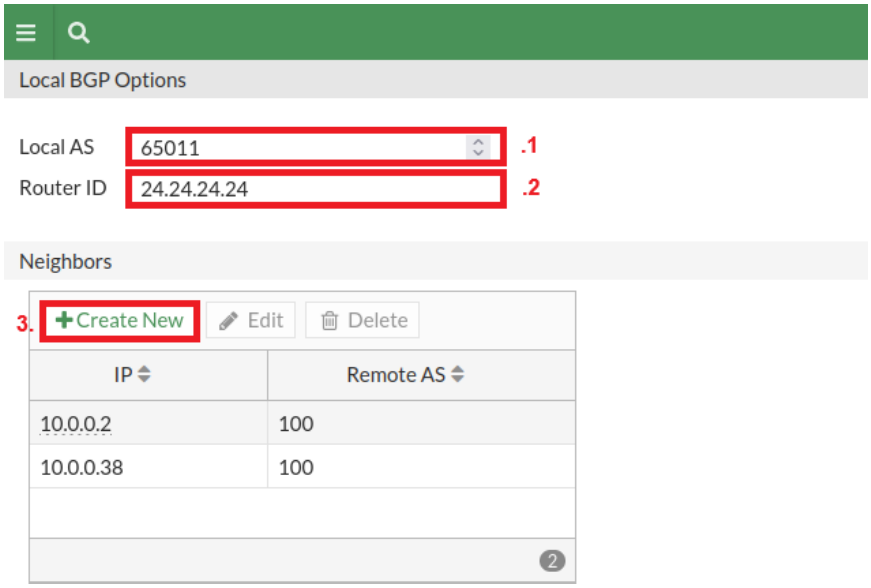


Figura 13: Etapas para a configuração da sessão BGP do lado cliente. Fonte própria.

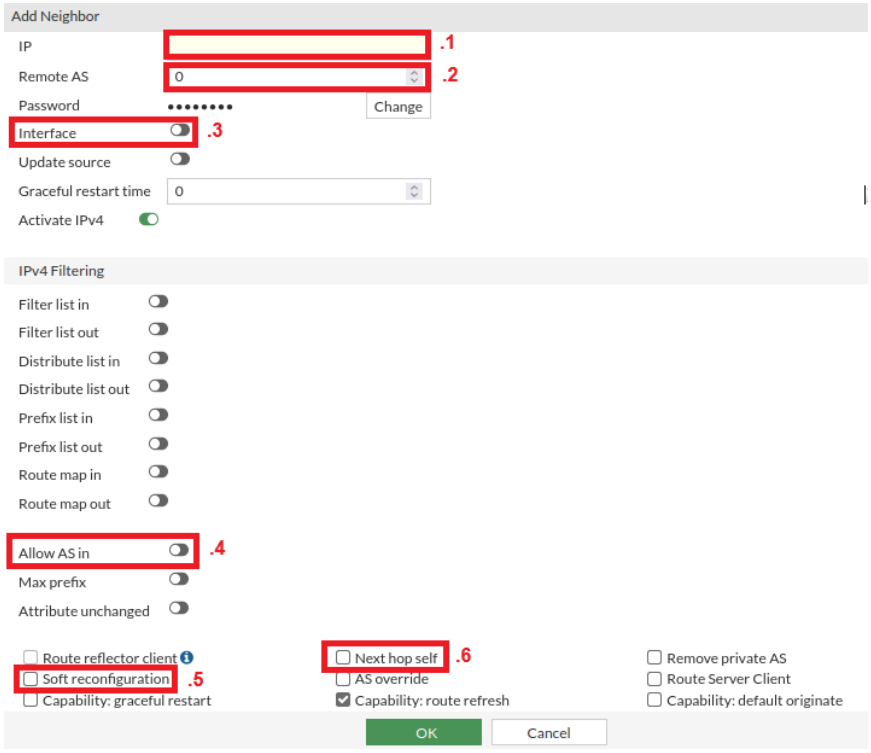


Figura 14: Etapas para a configuração dos *neighbors* BGP. Fonte própria.

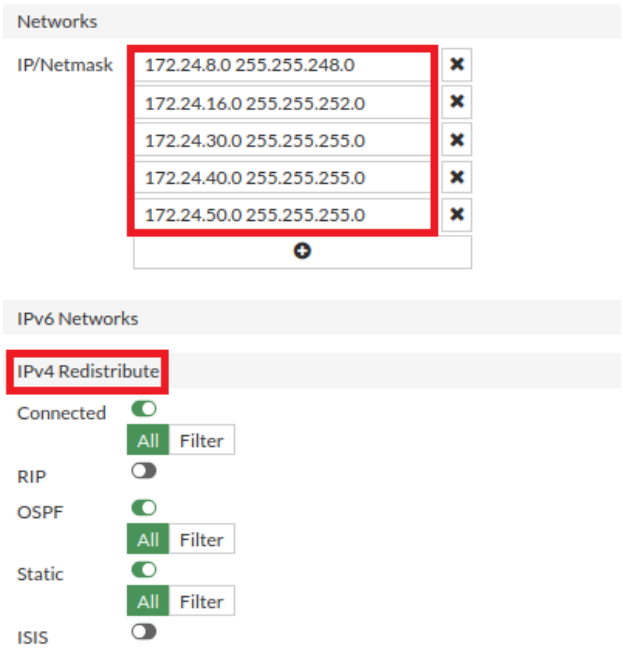


Figura 15: Últimas etapas para a configuração da sessão BGP do lado cliente Fonte própria.

(e) Configuração da Zona SD-WAN:

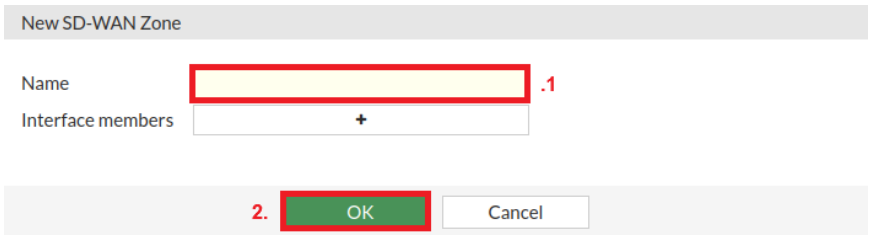


Figura 16: Criação da Zona SD-WAN. Fonte própria.

(f) Configuração dos membros SD-WAN:

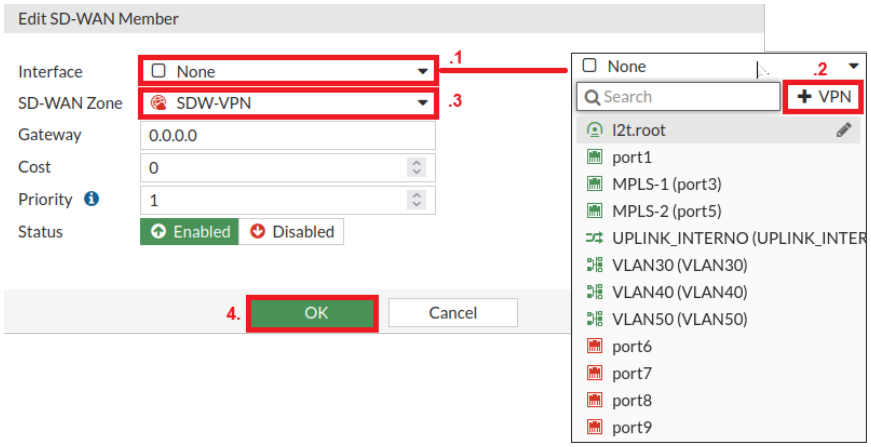


Figura 17: Criação dos membros SD-WAN. Fonte própria.

(g) Configuração de rotas estáticas:

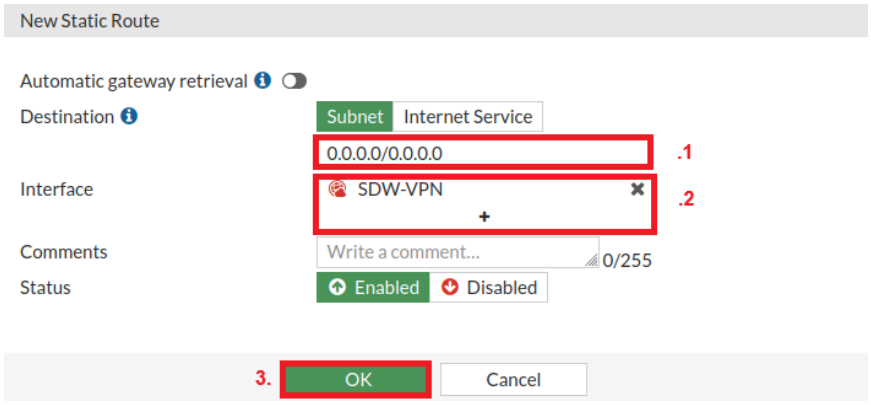


Figura 19: Configuração das rotas estáticas para funcionamento da solução SD-WAN. Fonte própria.

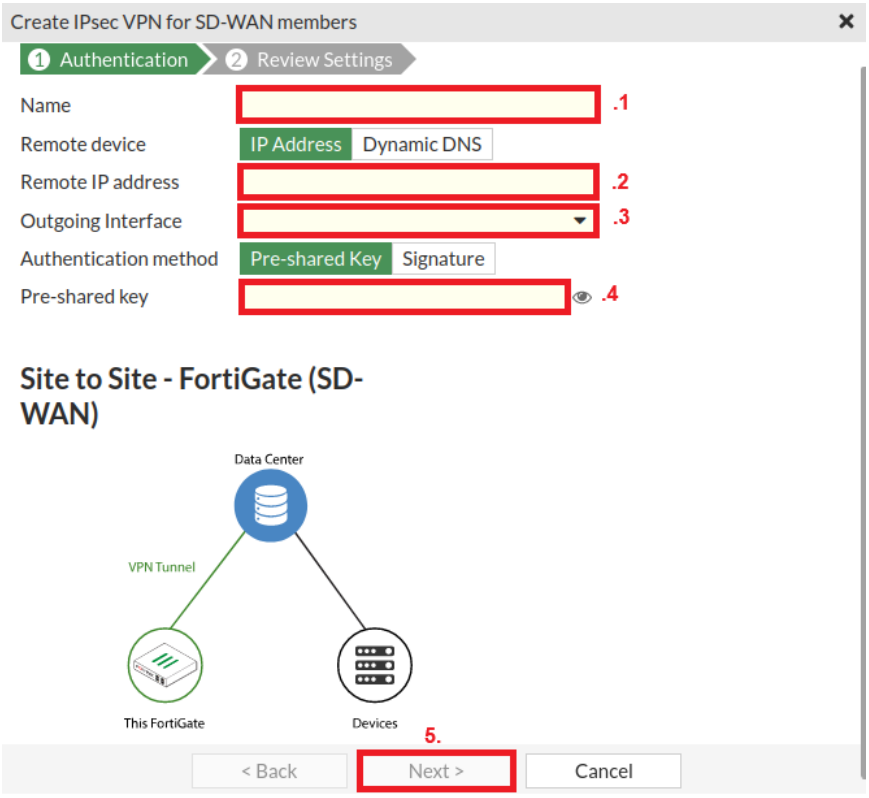


Figura 18: Configuração do IPsec VPN como membro SD-WAN. Fonte própria.

(h) Configurações de políticas de segurança:

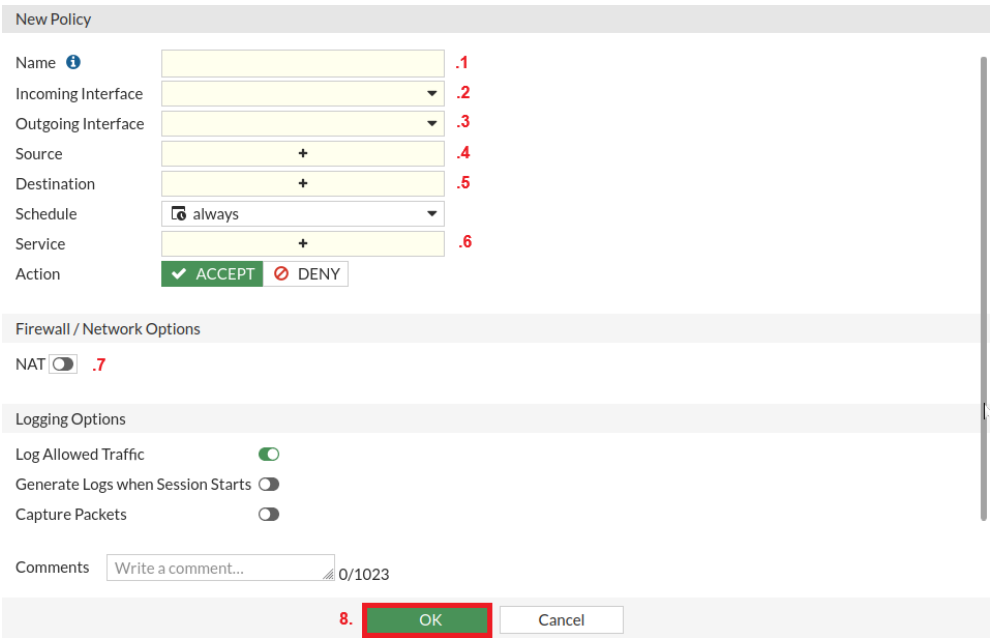


Figura 20: Configuração das políticas de segurança para o funcionamento da solução SD-WAN. Fonte própria.

(i) Configuração dos SLAs de Desempenho da solução SD-WAN:

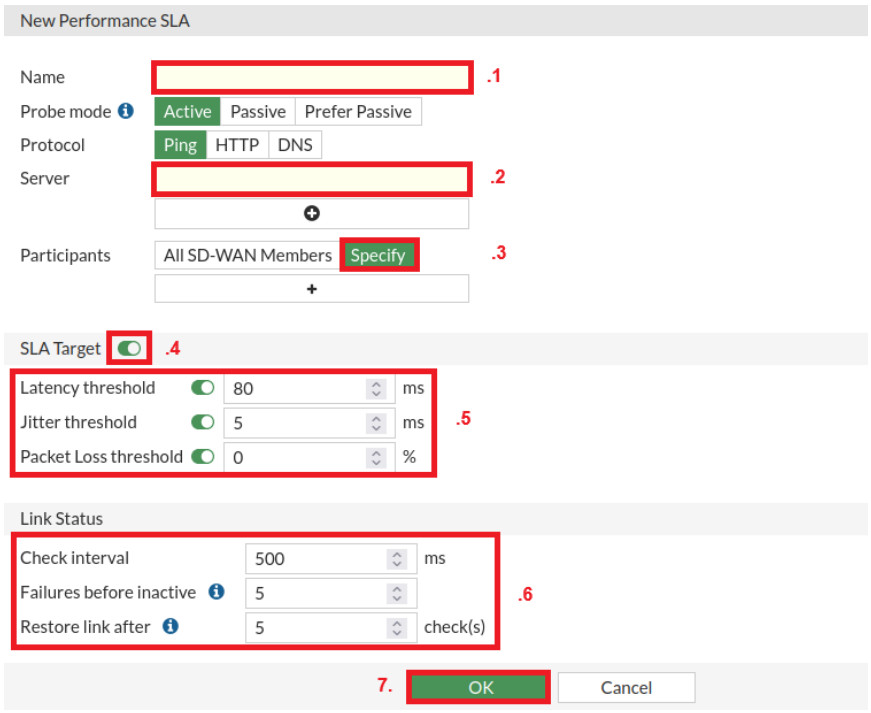


Figura 21: Etapas para configuração das SLAs de desempenho. Fonte própria.

(j) Configuração de Regras SD-WAN:

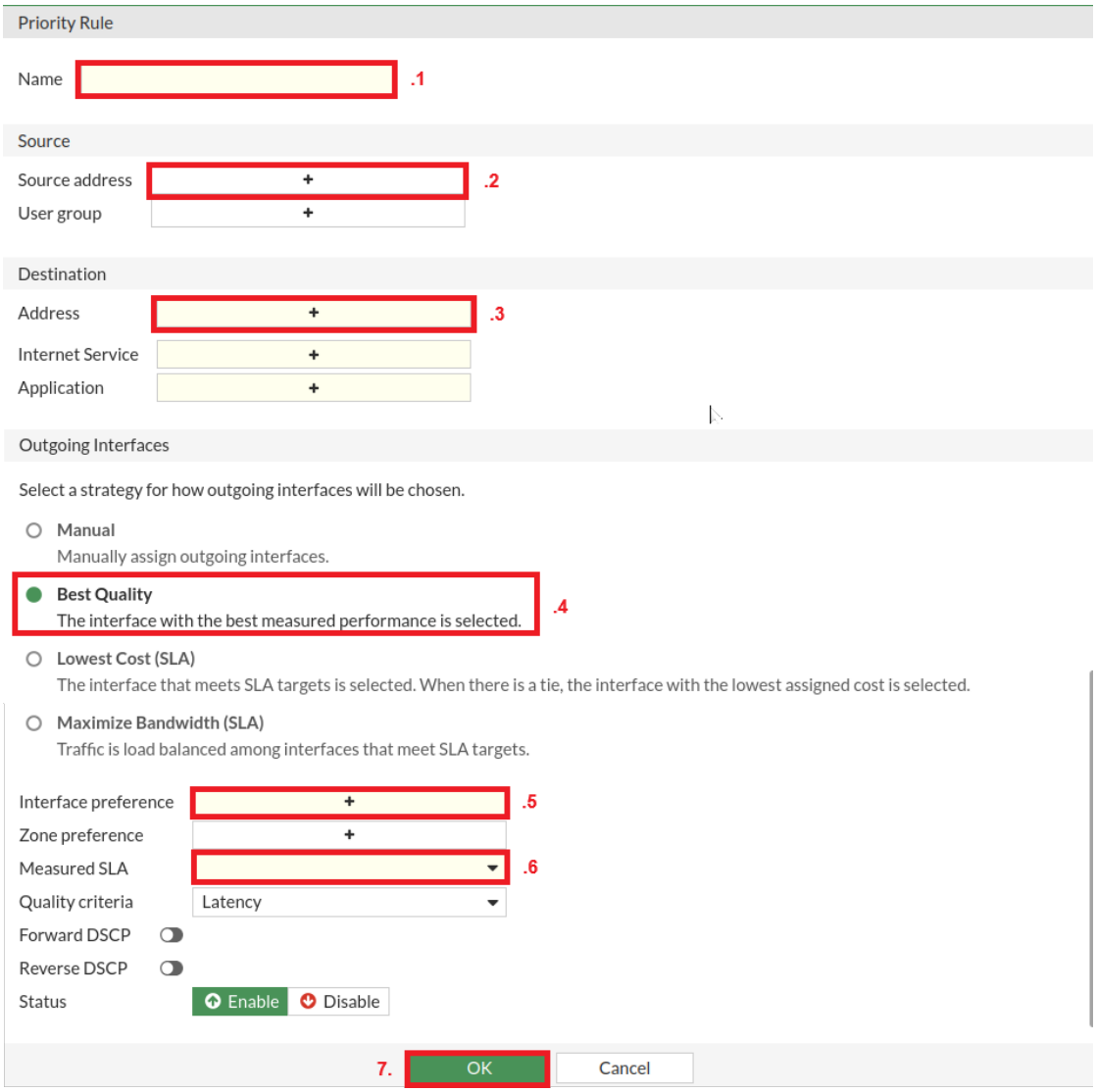


Figura 22: Etapas para configuração das Regras de SD-WAN a partir dos SLAs configurados. Fonte própria.