MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE COMPARATIVA DE TECNOLOGIAS SDWAN OPEN SOURCE VS PROPRIETÁRIAS

João Vítor Fonseca de Lima

Curso Superior de Engenharia de Redes de Comunicação

DEPARTAMENTO DE ENGENHARIA ELÉTRICA
FACULDADE DE TECNOLOGIA
UNIVERSIDADE DE BRASÍLIA

UNIVERSIDADE DE BRASÍLIA
Faculdade de Tecnologia

MONOGRAFIA DE PROJETO FINAL DE GRADUAÇÃO

ANÁLISE COMPARATIVA DE TECNOLOGIAS SDWAN OPEN SOURCE VS PROPRIETÁRIAS

João Vítor Fonseca de Lima

Monografia de Projeto Final de Graduação submetida ao Departamento de Engenharia Elétrica como requisito parcial para obtenção do grau de Bacharel em Engenharia de Redes de Comunicação

Banca Examinadora

Dr. Georges Daniel Amvame Nze, EnE/UnB _____
Orientador

Dr. Fábio Lúcio Lopes de Mendonça, EnE/UnB _____
Examinador Interno

Esp. Welber Santos de Oliveira, Estácio/Brasília _____
Examinador Externo

FICHA CATALOGRÁFICA

LIMA, J.V.F.
ANÁLISE COMPARATIVA DE TECNOLOGIAS SDWANOPEN SOURCE VS PROPRIETÁRIAS [Distrito Federal] 2023.
xvi, 85 p., 210 x 297 mm (ENE/FT/UnB, Bacharel, Engenharia de Redes de Comunicação, 2023).
Monografia de Projeto Final de Graduação - Universidade de Brasília, Faculdade de Tecnologia.
Departamento de Engenharia Elétrica

1. Software Defined Network
2. Software Defined Wide Area Network
3. Cloud Computing
4. Open Source

I. ENE/FT/UnB
II. Título (série)

REFERÊNCIA BIBLIOGRÁFICA

LIMA, J.V.F. (2023). *ANÁLISE COMPARATIVA DE TECNOLOGIAS SDWANOPEN SOURCE VS PROPRIETÁRIAS* . Monografia de Projeto Final de Graduação, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 85 p.

CESSÃO DE DIREITOS

AUTOR: João Vítor Fonseca de Lima
TÍTULO: ANÁLISE COMPARATIVA DE TECNOLOGIAS SDWANOPEN SOURCE VS PROPRIETÁRIAS .
GRAU: Bacharel em Engenharia de Redes de Comunicação ANO: 2023

João Vítor Fonseca de Lima
Depto. de Engenharia Elétrica (ENE) - FT
Universidade de Brasília (UnB)
Campus Darcy Ribeiro
CEP: 70919-970 - Brasília-DF - Brasil

Dedico esse trabalho comunidade acadêmica e aos meus pais, ambos sempre me incentivaram a buscar conhecimento e excelência.

AGRADECIMENTOS

Agradeço primeiramente aos meus pais, Wanderson G. de Lima e Elane C. F. de Lima, por sempre terem acreditado em mim, me apoiado em todos os momentos da minha vida e por me incentivarem constantemente a buscar conhecimento. Sem a orientação deles, eu jamais estaria onde estou hoje.

Agradeço aos meus amigos e colegas de vida e de curso, que, de alguma maneira, sempre me ajudaram nessa trajetória. Sou moldado pela contribuição de cada um deles. Gostaria de agradecer especialmente à minha amiga Cíntia G. Lucena, que me indicou a seguir meus estudos em Engenharia de Redes de Comunicação.

Agradeço a todos os meus professores da graduação e meu orientador. O papel de lecionar, sem dúvidas, é um dos mais genuínos. Vocês fizeram com que minha paixão e interesse pelo curso fossem amplificados ao máximo, e no decorrer das disciplinas, me vi cada vez mais imerso no mundo de redes de comunicação.

Agradeço também aos meus colegas e amigos de trabalho da Teltec Solutions onde pude por em pratica todo o conhecimento adquirido no curso de Engenharia de Redes de Comunicação, em especial ao meu líder Thiago Manente que sempre foi solidário com minhas demandas universitárias, além de conhecimento me disponibilizou os recursos necessários dos quais pude implementar este trabalho.

Por fim meu ultimo agradecimento vai a Flexiwan por ter disponibilizado gratuitamente sua solução de SDWAN, a Flexiwan.

Hoje, me desconecto da Universidade para amanha conectar o mundo.

RESUMO

O avanço constante da tecnologia em diferentes setores, principalmente a grande onda de migração para serviços em nuvem, como SaaS e IaaS, faz com que surjam demandas cada vez mais desafiadoras para redes de computadores. É um ciclo orgânico onde a evolução constante de uma série de tecnologias faz com que outras novas tecnologias surjam para suprir as novas demandas. Desta vez não é diferente, a grande demanda por sistemas mais eficientes de redes trouxe a SDWAN como uma tecnologia que provê a solução para muitas demandas do mercado. Este projeto tem o foco em explorar a tecnologia SDWAN, descrevendo suas principais funcionalidades, aspectos e serviços. Além disso, o foco está também na análise comparativa de desempenho de duas tecnologias SDWAN, uma que utilize soluções open source e outra que utilize soluções proprietárias.

Palavras-chave: SDWAN, Automação de Redes, WAN, SDN, Redes de Computadores, Open Source, Analise Comparativa.

ABSTRACT

The continuous advancement of technology across various sectors, particularly the significant wave of migration to cloud services such as SaaS and IaaS, has led to increasingly challenging demands for computer networks. It is an organic cycle where the constant evolution of various technologies gives rise to new technologies that can address emerging demands. In this context, the high demand for more efficient network systems has brought SDWAN as a technology that provides a solution to many market demands. This project aims to explore SDWAN technology by describing its key functionalities, aspects, and services. Additionally, the focus will be on conducting a comparative performance analysis of two SDWAN technologies: one utilizing open-source solutions and the other employing proprietary solutions.

Keywords: SDWAN, Network Automation, WAN, SDN, Computer Networks, Open Source, Comparative Analysis.

SUMÁRIO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SÍMBOLOS

Siglas

AP	*Access Point*
API	*Application Programming Interface*
CE	*Customer Equipment*
CPE	*Customer Premise Equipment*
DTL	*Data Transaction Language*
ESP	*Encapsulating Security Payload*
IaaS	*Infraestructure as a Service*
IEEE	*Instituto de Engenheiros Eletricistas e Eletrônicos*
IPSec	*Internet Protocol Security*
LAN	*Local Area Network*
MPLS	*Multiprotocol Label Switching*
NFV	*Network Functions Virtualization*
NOS	*Network Operating System*
ONF	*Open Networking Foundation*
QoS	*Quality of Service*
SASE	*Secure Access Service Edge*
SaaS	*Software as a Service*
SDN	*Software Defined Network*
SD-WAN	*Software Defined Wide Area Network*
TLS	*Transport Layer Security*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*
ZTP	*Zero touch Providing*

1 INTRODUÇÃO

O avanço constante do setor de tecnologia e da digitalização trouxe desafios às redes já existentes. A migração de várias tecnologias para a nuvem é um exemplo disso, assim como a necessidade de conexão eficiente entre os sites. Nos dias atuais, surge um novo conceito descrito como "Cloud Based Everything", onde há um grande foco na utilização de recursos em nuvem, como SaaS (Software as a Service) e IaaS (Infrastructure as a Service). As soluções tradicionais existentes não conseguem lidar com essa nova demanda, que requer alta disponibilidade de largura de banda, gerenciamento dinâmico e alta performance acessível de qualquer lugar. O maior impacto dessas mudanças ocorre nas topologias de redes WAN, pois elas não conseguem atender aos requisitos necessários abordados, [Red Hat].

As redes WAN atuais contam com diversos problemas, muitos deles ligados a complexidades operacionais e gerenciamento. A variação de largura de banda provida de múltiplos links de acesso e múltiplos provedores em diferentes sites podem gerar complexidade de roteamento, impossibilitando o roteamento eficiente e ainda acarretando problemas de gerenciamento, implementação e segurança.

A falta de simetria de trafego e má utilização da largura de banda também podem ser bastantes danosos a redes WAN, onde muitas vezes alguns sites preferem manter dois links para assegurar um certo nível de redundância, onde geralmente segundo link estará disponível apenas em caso de falha do link primário. Há uma complexidade na configuração que utilizam meios de redistribuição de tráfego, deve haver politicas para evitar loops e afins, além disso há uma clara má utilização da largura de banda total disponível quando esse tipo de implementação é feita.

Essa nova demanda não saciada trouxe como resposta a SDWAN (Software Defined Wide Aarea Network). Umas das características principais da SDWAN é o conceito de “Aplication Driven Network” (Rede Dirigida por Aplicação) isso significa que a tecnologia foca em QoS (Qualitty Of Service – Qualidade de Serviço). A SDWAN tem como principio tornar a WAN totalmente programável, flexível e completamente gerenciável. A tecnologia se adapta de acordo com as necessidades de redes particulares de cada organização/corporação, totalmente diferente do conceito de WAN em que as decisões são tomadas localmente pelos elementos que compõe a rede o que gera dificuldade de implementar mudanças globais na rede. Além disso a SDWAN toma vantagem dos vários meios de acesso à internet como MPLS, 4G/5G e banda larga, a utilização de qualquer forma de acesso traz mais redundância de links além de proporcionar um melhor balanceamento de carga e uma alta disponibilidade de serviço provendo vários meios de acesso a internet.

Com isso o conceito de como gerenciar e monitorar WANs antigas está mudando e aos poucos a adoção da SDWAN vem tomando espaço no mercado como uma solução que entrega impactos significativos. A SDWAN além de criar políticas e aplica-las a rede de maneira programável e automatizada traz consigo um gerenciamento centralizado da WAN e uma redução dos custos de implementação.

Nota-se um grande potencial dessa tecnologia principalmente para o meio corporativo e educacional, a SDWAN supre as demandas do Cloud Computing além de ser de fácil implementação e baixo custo, isso acaba gerando um retorno de médio prazo as organizações que acabam migrando suas WANs. Além

de ajudar com aplicações cloud, algumas soluções de SDWAN já contam com gerenciamento 100% em nuvem como as soluções Cisco Meraki. [What is SD-WAN].

1.1 OBJETIVOS

Emular, em ambiente controlado e conhecido, uma mesma topologia WAN campus simples para duas tecnologias SDWAN diferentes, uma que use tecnologias de open source e outra que use tecnologia proprietária com fim de mapear tecnologias que possam ser exploradas e medir desempenho de ambas as tecnologias.

1.1.1 Objetivos Específicos

Os objetivos específicos consistem no derivação do objetivo geral, ou seja, nos passos que devem ser feitos para que o objetivo do trabalho seja concluído:

- Implementar uma topoalgia Campus de camada 2 com Switches da Extreme Swtiches.
  - Criação de VLANs (Virtual Local Area Network) com o intuito de criar diferentes domínios de broadcast;
  - Implementação do MSTP (Multiple Spanning Three Protocol);
  - Configuração adequada do DHCP.
- Configuração do roteamento inter-Vlan feito pelo SW-CORE.
- Implementar e coletar métricas da SDWAN Open Souce;
- Implementar e coletar métricas da SDWAN proprietária;
- Analise das métricas e resultados obtidos;

1.2 JUSTIFICATIVA

Com o avanço do setor de Tecnologia da Informação o setor de redes organicamente tende a evoluir junto, um acompanha o outro. A tecnologia SDWAN teve sua grande estreia na pandemia e apesar de ser uma tecnologia recente seu avanço já é muito significativo principalmente no que se diz respeito dentro do meio privado. O meio acadêmico, apesar de explorar a tecnologia, não se aprofunda muito, apenas com algumas literaturas. O mapeamento de recursos irá fornecer ao meio acadêmico caminhos para melhor exploração da tecnologia abrindo assim novas possibilidades de implementação de recursos que muitas vezes não são citados em artigos.

1.3 METODOLOGIA

De maneira geral será utilizado um ambiente controlado para a emulação de uma rede WAN simples, composta por dois sites. Para isso serão utilizados softwares de emulação de redes como o *GNS3* e algumas ferramentas de emulação de tráfego como o *iperf3*.

Será escolhida uma topologia base para a rede e em seguida serão alocados os recursos necessários para a confecção das soluções SDWAN que utilizam soluções de código aberto e depois para a que utilizam de soluções proprietárias.

Para a solução de código aberto foi escolhido as soluções da FLexiWan e a proprietária Fortinet. Após a devida configuração de ambas as soluções serão feitas analises das tecnologias e testes de performance em ambas as redes a fim de medir A performance de uma mesma rede para diferentes tecnologias. Os testes irão medir as principais funções da SDWAN descritas em 2, como QoS, segurança, tunelamento e afins.

1.4 CONTRIBUIÇÕES

Esse projeto é uma contribuição ao projeto [Garcia 2023], onde nesse projeto pretende-se explorar mais os benefícios e vantagens da SDWAN, assim como mapear os principais pontos que precisam ser aperfeiçoados/implementados em tecnologias open source. Além disso esse projeto visa contemplar uma análise comparativa de tecnologias SDWAN open source versus proprietária.

2 FUNDAMENTAÇÃO TEÓRICA

Este capitulo tem como foco abordar as tecnologias, protocolos e fundamentos utilizados em todo o projeto proposto.

2.1 SWITCHES

Switches são equipamentos de redes que geralmente operam na camada 2 tendo como referencia o modelo TCP/IP descrito em [Odom 2020]. Sua principal função é encaminhar pacotes para usuários finais em uma LAN (Local Area Network). No entanto, switches não se limitam apenas a conexões de usuários finais, eles também podem conectar servidores, outros switches e dispositivos similares. Além disso, switches costumam ter uma alta densidade de portas, o que permite múltiplas conexões para um mesmo equipamento, tornando-os úteis em diversas aplicações. Switches modernos não se limitam a funções de camada 2, os chamados *Multi Layer Switches* podem implementar funções de camadas de 3 e 2, o que os tornam mais flexíveis.

Uma das funções mais interessantes dos switches é a segmentação de domínios de broadcast através de VLANs (Virtual Local Area Network), os switches segmentam a rede em diferentes setores, isso facilita o gerenciamento de redes, essa segmentação é feita na camada 2 e a interconexão dessas VLANs deve ser feita por um equipamento de camada 3 como um roteador ou um switch multi camada.

2.2 LANS E VLANS

Uma LAN (Local Area Network) é um grupo de aparelhos que pertencem a uma mesma rede e geralmente estão concentrados no mesmo espaço georográfico ou operacional. A rede, geralmente é composta por uma série de equipamentos como switches, roteadores, servidores, pontos de acesso etc. Uma definição de LAN muito interessante está em [Odom 2020] onde uma LAN é descrita da seguinte forma, "Uma LAN inclui todos os dispositivos em um mesmo domínio de broadcast ".

Atualmente, a implementação das redes locais (LANs) está passando por mudanças significativas, com uma abordagem hierárquica na sua implementação. Dentro de uma mesma organização, é comum a existência de várias LANs, conforme mencionado em [F.Kurose 2014]. Essa configuração implica que cada departamento ou setor da organização está inserido em um domínio de broadcast separado, o que traz benefícios em termos de segurança, eficiência e gerenciamento da rede.

Pensando em LANs de maneira mais conservadora, ou seja, não separadas hierarquicamente, como mostrado na figura 2.1, existem algumas desvantagens no que diz ao seu uso:

- *Falta de Isolamento de Tráfego*: O não isolamento de tráfego pode causar danos sérios ao desem-

penho de redes, principalmente na camada 2. Além disso quesitos de segurança e gerenciamento são prejudicados ao extremo, mensagens de broadcast podem trazer grandes problemas quando são difundidas para um alto número de equipamentos finais.

- *Alta Densidade de Switches*: Em uma rede separada hierarquicamente sem nenhum tipo de tecnologia facilitadora toda a divisão de departamentos/grupos de trabalho deverá ser feita por um switch (ou um comutador de pacotes, [F.Kurose 2014]). Além de aumentar os custos do projeto esse tipo de solução não escalona bem, visto que podem haver desperdícios no que se referente ao numero de portas em cada switch e uma complexidade e exaustão de configuração de cada equipamento.

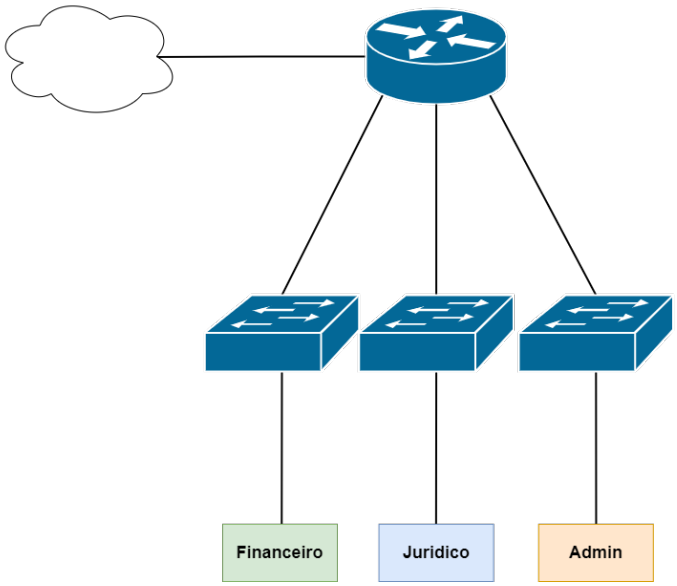


Figura 2.1: Arquitetura LAN Tradicional. Fonte: autor

Tais problemas mencionados acima podem ser resolvidos com a utilização de VLAN (Virtual Area Local Network), esse protocolo tem como intuito segmentar domínios de broadcast, ou seja, criar diferentes LANs utilizando apenas um aparelho físico. O Conceito é simples, dentro de um switch serão criadas diferentes VLANs que recebem um nome e uma *TAG*, então cada porta do switch pode ser relacionada a uma VLAN especifica, fazendo assim uma separação logica por software. Quando existem mais de dois switches que comportam uma ou mais VLANs iguais os mesmos devem ser ligados através de um link de trocamento (*"trunk"*) onde os pacotes que passarão por dentro desse link receberão uma inclusão no frame Ethernet, definido no padrão 802.Q, [Odom 2020]. A figura 2.2 ilustra como o exemplo da figura 2.1 ficaria ao introduzir o conceito de VLAN.

A utilização de VLANs traz uma serie de benefícios, não só para a estrutura de redes:

- *Usuários Finais*: Reduz as mensagens de broadcast com a segmentação, isso implica que os usuários finais terão de processar menos mensagens de broascast reduzindo o seu uso de CPU;
- *Redução dos Riscos de Segurança*: Com a segmentação consegue-se ter um controle maior de áreas/grupos, podendo assim aplicar diferentes politicas de segurança para cada VLAN.

- *Resolução de Problemas*: A resolução de problemas com a utilização de VLANs se torna mais rápida e eficiente pois desde o principio do problema é possível separar a qual rede o mesmo pertence.

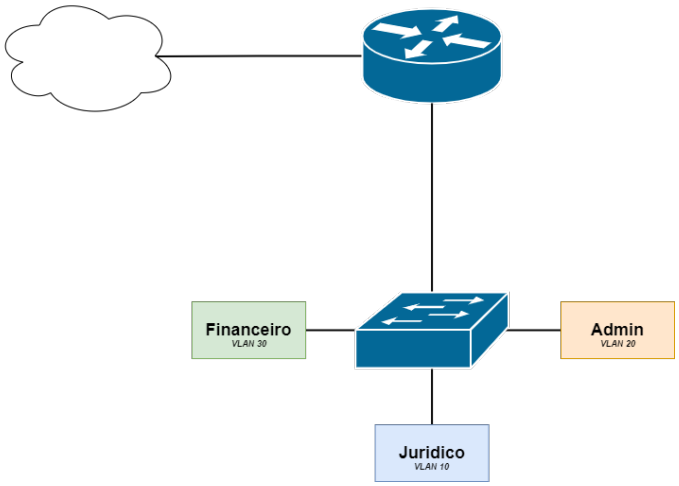


Figura 2.2: Arquitetura VLAN. Fonte: autor

2.3 STP

O STP (Spanning Tree Protocol) é um protocolo definido pelo padrão IEEE 802.1D. Foi idealizado para impedir inundações de mensagens de broadcast em uma LAN. Como se sabe, algumas mensagens dentro de uma LAN são propagadas em forma de broadcast (quando uma mensagem deve ser enviada a todos os dispositivos de uma LAN; roteadores não propagam mensagens de broadcast). No entanto, quando existem dois ou mais switches dentro de uma LAN, pode ocorrer o que chamamos de loop infinito de broadcast, ou seja, quando uma mensagem fica sendo propagada indefinidamente dentro de uma LAN.

Isso acontece porque os switches propagam as mensagens em todas as portas, exceto a porta pela qual a mensagem foi recebida. Por exemplo, se um switch envia uma mensagem de broadcast e possui dois caminhos para outro switch, pode ocorrer um loop. A função básica do STP é prevenir a ocorrência de tais loops, bloqueando uma ou mais portas dentro de uma mesma LAN. Vale lembrar que o STP é um protocolo de camada 2 e não é utilizado em roteadores. O protocolo IP possui seu próprio mecanismo de prevenção de inundações/loops, [Odom 2020].

Existem variações do STP, tanto proprietárias, como o RSTP (Cisco), quanto abertas como o MSTP (Multiple Spanning Tree Protocol - 802.1s). Ambas as variações do STP têm como objetivo aumentar o tempo de convergência da topologia e criar uma árvore do STP para cada VLAN.

2.4 ROTEADORES

Roteadores são equipamentos de redes que lidam com uma alta demanda de roteamento de pacotes, geralmente esses equipamentos estão dispostos nas bordas de LANs e fazem a função de interligar um site

a internet, mas não estão restritos a isso, roteadores mais modernos já implementam funções de firewall, politicas de QoS e afins.

Roteadores processam pacotes de camada 3 como o IPv4 ou IPv6 e são responsáveis por montar grandes tabelas de roteamento que ajudam na decisão de roteamento. Cada roteador pode rodar diferentes protocolos de roteamento para conseguir diferentes rotas com diferentes custos, mas no final de cada execução apenas as melhores rotas são selecionadas para entrar na tabela de roteamento.

2.5 ROTEAMENTO

O roteamento é um processo no qual ocorre a decisão de para onde encaminhar um pacote. Para que o roteamento seja eficiente, existem diversos protocolos que dão suporte a esse processo. Por exemplo, o IPv4 e IPv6 são responsáveis pela identificação de redes e dispositivos, enquanto protocolos como BGP, OSPF, RIPv2 e EIGRP são responsáveis por criar rotas para outras redes, sendo conhecidos como protocolos de roteamento.

Existem diversos tipos de protocolos de roteamento, e o que os diferencia é a métrica que utilizam. Entre os protocolos de roteamento mais conhecidos, destacam-se:

- **Vetor de Distância**: Esses protocolos utilizam a métrica de saltos, ou seja, quantos saltos (enlaces) devem ser feitos para que o pacote chegue na rede desejada, um protocolo que utiliza dessa métrica é o RIPv1 e RIPv2;
- **Estado de Enlace**: Como o nome sugere, esse protocolo leva em consideração o estado dos enlaces que formam um caminho, esse tipo de métrica é mais aberta e pode levar em consideração diferentes informações a respeito do enlace como largura de banda e delay para que seja definido um custo ao enlance, o caminho que tiver a menor somatória dos enlaces que os compõem será selecionado como o melhor caminho, um protocolo que utiliza dessa métrica é o OSPF que utiliza a largura de banda do link disponível e atribui um valor a ela.

2.5.1 OSPF

O OSPF (Open Shortest Path Firist) é um protocolo de estado de enlace que utiliza a largura de banda do enlace como métrica. O protocolo é considerado um protocolo dinâmico.

O OSPF é um protocolo de roteamento interno (IGP - Interior Gateway Protocol), o que significa que o mesmo é comumente usado par roteamento em redes internas, como redes LAN. O funcionamento desse protocolo é definido no documento [Force 1198], no qual são propagadas mensagens "Hello"no endereço de broadcast **224.0.0.5** para descobrir outros roteadores que suportam OSPF [Odom 2020]. Uma vez que outros roteadores OSPF são encontrados, são trocadas mensagens LSA (link State Advertisement). Dependendo do tipo de enlace entre os roteadores, pode ocorrer uma eleição para selecionar um DR (Designated Router) e um BDR (Backup Designated Router). O OSPF é amplamente utilizado em redes LAN de pequeno e grande porte. Seu funcionamento permite a criação de várias áreas que podem ser interconectadas

por ABRs (Area Border Routers). Além disso, a nova versão do OSPF, o OSPFv3, oferece suporte ao roteamento de pacotes IPv6.

2.6 TCP

O *Transmission Control Protocol* é um protocolo que opera abaixo da camada de rede, ou seja, na camada de transporte e ele se destaca por ser um protocolo orientado a conexão. O TCP conta com muitos mecanismos que servem para "guiar"uma conexão mais segura e eficaz.

Antes de uma conexão TCP começar a trocar os dados há uma etapa conhecida como *Three Way HandShake*, nesta primeira parte, antes da conexão ser devidamente formada, há uma apresentação, entre as duas entidades finais que irão formar a conexão para a troca de dados, onde serão estabelecidos parâmetros como o ISN (Initial Sequence Number), ACK Number, Receive Window e as opções de Flag de Controle, [Postel 1981]. Um dos recursos mais interessantes do TCP é a segmentação e identificação de pacotes, permitindo que cada conexão TCP tenha controle sobre o fluxo de dados. Isso possibilita a retransmissão de pacotes perdidos durante o processo de roteamento. Além disso, o TCP oferece uma conexão *Full Duplex*, em que o fluxo de dados de $A \rightarrow B$ ocorre simultaneamente ao fluxo de $B \rightarrow A$, [F.Kurose 2014].

Outra função bastante importante implementada pelo TCP é o controle de congestionamento através do janelamento, [Odom 2020], que tem como objetivo reduzir a carga de dados enviada dentro de uma rede uma vez que a mesma começa apresentar sobrecarga no que se refere ao trhoughput disponível. O controle de congestionamento aplicado é o fim a fim, ou seja, os responsáveis por fazer o controle são os sistemas finais. O TCP utiliza de uma janela de congestionamento fixada em seu cabeçalho, **cwnd**, essa janela estabelece um limite máximo na quantidade de dados não reconhecidos que podem ser enviados, essa janela não é fixa e é ajustada de acordo com o congestionamento que está sendo percebido pela rede.

Para a percepção de congestionamento o TCP utiliza dos **ACKs** enviados e recebidos pelo remetente/-destinatário, o TCP monitora o tempo de envio do pacote até o recebimento do ACK, caso um ACK não seja recebido dentro de um determinado intervalo de tempo o TCP, reconhece como uma possível perda de pacote, que por fim pode significar um congestionamento em algum link do caminho. Sendo assim a partir do congestionamento identificado o TCP toma medidas de controle, reduzindo sua taxa de envio de dados em ambos os lados da conexão utilizando algoritmos como o *Slow Start* e *Congestion Avoidance*.

2.7 DHCP

O DHCP (Dynamic Host Configuration Protocol) é um protocolo dinâmico definido em [Group 1197], o protocolo tem como foco criar regras de atribuição de endereços a usuários de uma LAN. Esse protocolo pode rodar em grandes servidores ou até mesmo em roteadores e swtiches cores (switches de camada 3).

Para a abordagem do projeto apenas o básico do DHCP é necessário, ou seja, seu processo de funcionamento conhecido como **DORA**, que é descrito em quatro etapas:

1. **D**escoberta do Servidor DHCP: Quando um usuário final se conecta a qualquer rede, caso o DHCP esteja configurado é iniciado o processo de *Discovery* ou descoberta, onde o usuário final manda uma mensagem de descoberta DHCP para o endereço de broadcast 255.255.255.255 utilizando o protocolo UDP na porta 67. Como é de se esperar a mensagem é transmitida por todos os enlaces dentro da LAN.

2. **O**ferta(s) do(s) Servidor(es): Nesta etapa os servidores, após escutarem a mensagem de descoberta, enviam uma serie de ofertas, chamadas de ofertas DHCP que também é transmitida por broadcast no endereço 255.255.255.255. Nesta mensagem costumam ter os endereços disponíveis para o usuário final que solicitou .

3. **R**equisição: Após analise das ofertas o usuário seleciona um IP dentro das ofertas recebidas.

4. **A**CK DHCP: Resposta do servidor confirmando a requisição e o alocamento do endereço IP.

2.8 VXLAN

O protocolo VXLAN (Virtual Extensible LAN) é utilizado para o encapsulamento de tráfego de camada 2 em uma rede completamente baseada em camada 3, onde esse "encapsulamento"é chamado de segmento VXLAN que é feito através da inclusão dos frames de camada 2 no datagrama UDP usando a porta 4789 (porta separada pela IANA para o protocolo UDP VXLAN), [Nadeem e Karamat 2016], isso permite que dentro de um segmento VXLAN apenas maquinas que pertencem a ele consigam se comunicar entre si. O identificador do VXLAN se difere muito do identificador de VLANs, o identificador tem um espaço separado de 24 bits, isso dá ao total mais de 16 milhões de segmentos, contra 4096 do identificador usado em VLANs. [Mahalingam et al. 2014].

2.9 IPSEC

o IPSec (Internet Protocol Security) é um conjunto de de protocolos e algoritmos de seguranças que dão suporte na proteção de redes de computadores. Esses protocolos quando combinados oferecem diversas funções de segurança para os dados que trafegam na internet, como autenticação, confiabilidade e integridade.

Além das funções de segurança o IPSec pode ser amplamente utilizado para conexão de sites, ou seja, quando duas redes precisam se comunicar mas estão diretamente ligadas a internet. O chamados **túneis** oferecem segurança reforçada para que dois sites consigam trocar informações dentre de uma rede aberta sem que haja nenhum problema de segurança envolvido, [Frankel Karen Kent 2005].

2.10 ESP

O ESP (Encapsulating Security Payload) é um protocolo de segurança, definido nos RFC's [4301], [4303] e [4305], é utilizado para fornecer confidencialidade, integridade e autenticação dos dados transmitidos em redes de comunicação [Force 2005]. Ele faz parte do conjunto de protocolos IPSec (Internet Protocol Security). O protocolo é responsável por encapsular os dados originais em um novo pacote protegido.

O algoritmos utilizados pelo protocolo muitas vezes são de criptografia simétrica, como AES (Advanced Encryption Standard), para proteger os dados contra acesso não autorizado. Ele também pode usar funções hash, como HMAC (Hash-based Message Authentication Code), para verificar a integridade dos dados e garantir que eles não tenham sido modificados durante a transmissão.

Além disso, o ESP suporta a autenticação do remetente através do uso de certificados digitais ou pré-compartilhamento de chaves. Isso garante que os dados sejam originados de uma fonte confiável e não tenham sido adulterados por intermediários maliciosos.

2.11 IKEV2

O IKEv2 (Internet Key Exchange version 2) é um protocolo amplamente utilizado para o estabelecimento e gerenciamento de túneis IPSec. Esta versão melhorada do protocolo originário IKE é projetada para melhorar a segurança, eficiência e capacidade dos tuneis, o mesmo e definido no RFC [5996].

O IKEv2 suporta EAP (Extensible Authentication Protocol), que permite aos tuneis a utilização de servidores externo de autenticação usando protocolos como Kerberos e o RADIUS, [Frankel Karen Kent 2005].

2.12 WIDE AREA NETWORK

A Wide Area Network (WAN) é um tipo de rede de computadores que abrange uma grande área geográfica, como cidades, estados, países e até mesmo continentes. Ela é utilizada para conectar redes locais (LANs) em diferentes locais, permitindo a comunicação entre dispositivos em diferentes pontos geográficos. A Figura 2.3 ilustra de maneira clara o conceito de uma WAN tradicional.

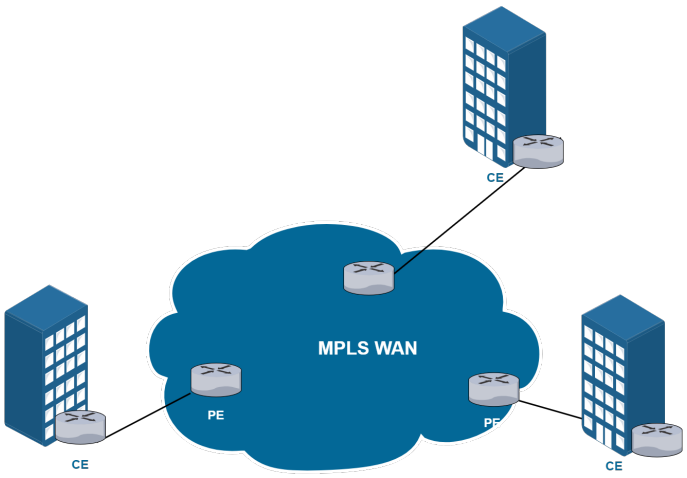


Figura 2.3: Arquitetura WAN Tradicional. Fonte: autor

As WANs geralmente são compostas por uma combinação de tecnologias de rede, como roteadores, switches, gateways e modens. Elas podem ser criadas e gerenciadas por empresas de telecomunicações, provedores de serviços de internet ou empresas privadas. As principais tecnologias usadas em WANs incluem o Frame Relay, ATM, MPLS e VPNs. Cada uma dessas tecnologias apresenta diferentes características em termos de velocidade, segurança, disponibilidade e custo, [Conrad Menezes et al. 2014].

2.13 SOFTWARE DEFINED NETWORK

Definida pela Open Networking Foundation (ONF), Software Defined Network (SDN) é uma arquitetura de redes que implementa o desacoplamento do plano controle da rede (control plane) do plano de dados da rede (data plane). Contudo esse conceito já estava sendo abordado por outras tecnologias entretanto a SDN se torna única pelo fato que a mesma prove programabilidade de todos os elementos ativos de redes, esse desacoplamento traz um gerenciamento centralizado, a nova arquitetura permite que o controle da rede seja executado de maneira separada sem interferir no fluxo de dados.

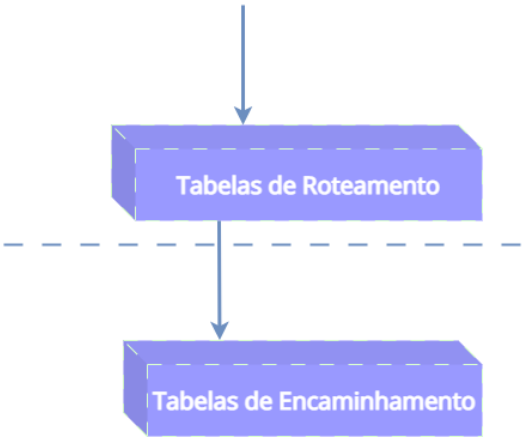


Figura 2.4: Desacoplamento de Planos. Fonte: autor

Um dos princípios da rede definida por software é o desacoplamento do plano de dados do plano de roteamento. Antigamente um elemento de rede, como um roteador ou um Switch de camada 3 tomava suas decisões de roteamento de maneira local, independente, com o desacoplamento ocorre uma centralização e uma "divisão" das camadas de rede, a rede pode ser descrita em 3 planos principais, o plano de roteamento (forwarding plane) onde se encontram todos os ativos de redes como Switches, roteadores, AP's e etc. O Plano de controle é onde o gerenciamento é feito, geralmente controlado por uma entidade de software, combina o controle e o gerenciamento da rede via API (Application Programming Interface) prove uma abstração das funções de rede e serviços do plano de dados. Por fim Plano de Aplicação (Application Plane) o mesmo utiliza as funções e serviços providos do plano de controle para criar a logica da rede SDN que por fim é "traduzida" em configurações para os ativos de rede, [Xia et al. 2015].

Um dos pontos chave do desacoplamento é focado no roteamento, onde a criação e manutenção das tabelas de roteamento está no plano de controle e as tabelas de encaminhamento são o processo final contidas no plano de dados, assim a lógica de criação e atualização de rotas pode ser feita de maneira separada sendo assim fornecida apenas a tabela de encaminhamento com isso os elementos que cuidam do plano de dados podem focar apenas no encaminhamento de pacotes gerando assim a otimização do encaminhamento de pacotes.

2.14 SOFTWARE DEFINED WIDE AREA NETWORK

A SDWAN (Software-Defined Wide Area Network) é uma extensão da arquitetura SDN (Software-Defined Network) para a infraestrutura de rede WAN, que é geralmente mais complexa do que as redes locais. Alguns dos principais objetivos da SDWAN são melhorar o desempenho da rede, simplificar sua gestão e reduzir os custos de infraestrutura [Yalda, Hamad e Ţăpuş 2022].

Na SDWAN, a fragmentação dos planos é semelhante à SDN, no entanto o plano de aplicação agora se chama plano de orquestração, que é responsável por coordenar e gerenciar a política de rede global. Esse plano coordena os planos de controle e de dados, estabelecendo políticas de tráfego que priorizam a transmissão de dados mais críticos e aplicativos essenciais, como voz e vídeo, garantindo a melhor qualidade do serviço.

Além disso, a arquitetura SDWAN permite que as organizações possam escolher entre diferentes formas de transporte para conectar suas filiais, como MPLS, 4G, 5G e banda larga. Isso traz mais flexibilidade e eficiência ao balanceamento de carga, bem como uma maior redundância nas conexões de acesso à internet.

Portanto, a SDWAN oferece uma abordagem mais flexível e econômica para gerenciar redes de área ampla, permitindo a simplificação e o gerenciamento centralizado da rede, além de oferecer mais opções de conectividade e aumentar a eficiência na transmissão de dados. A figura 2.5 ilustra a arquitetura da SDWAN.

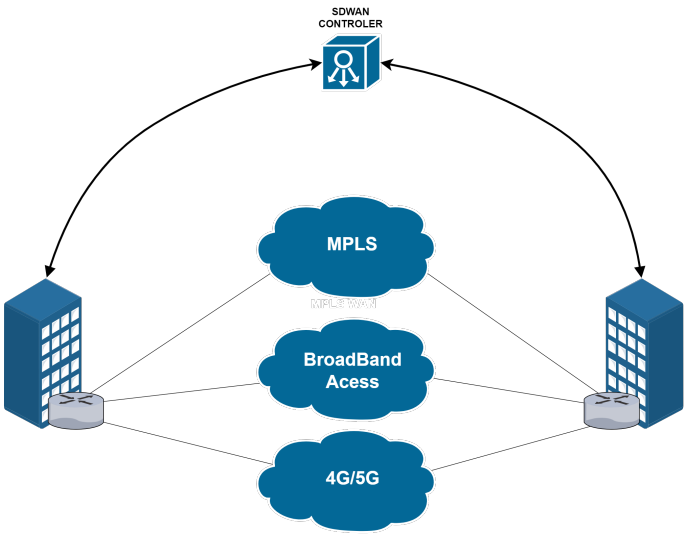


Figura 2.5: Arquitetura SDWAN com diferentes acessos e uma controladora. Fonte: autor

Existem duas formas de design de uma SDWAN:

- **Software Orientation**: Se baseia na arquitetura que pode ser compatível com diferentes tipos de hardwares (VMWARE - VeloCloud) conduto é reproduzida em sofwares;
- **Hardware Orientation**: Utilizam apenas soluções em hardware, geralmente proprietários (Cisco Meraki e Cisco Viptela).

A SDWAN é uma das soluções que se aproximam do conceito de redes IBN (Intent-Based Network), que é uma rede que opera com base nas intenções dos usuários, permitindo que as políticas sejam criadas de forma abstrata e a rede traduza automaticamente essas intenções em ações de rede executáveis. Para entender melhor como a SDWAN consegue explorar o conceito de Driven Application Network, é necessário conhecer seus planos e como eles operam, se comunicam e trocam informações.

A infraestrutura ou plano de dados consiste nos ativos de rede disponibilizados na infraestrutura da rede. Para fazer o controle desses ativos, a SDWAN cria um software de gerenciamento que vai operar em cima da infraestrutura existente. Esse tipo de arquitetura recebe o nome de overlay, enquanto a infraestrutura que está abaixo é chamada de underlay [Segeč et al. 2020]. O underlay costuma ser uniforme e consistente, enquanto o overlay é mais dinâmico e consegue criar diversos tipos de links que interligam os elementos.

O plano de controle é responsável por receber informações do plano de orquestração e fazer a programação dos dispositivos do plano de dados, garantindo assim o desempenho desejado da rede, além disso o plano de orquestração é responsável pelas politicas dinâmicas e intensões corporativas, sua principal função é monitorar toda a infraestrutura da SDWAN medir parâmetros de qualidade de serviço (QoS), a camada de orquestração prove também o ZTP (Zero Touch Providing) onde a configuração de qualquer ativo de rede é automaticamente baixada pelo mesmo no momento em que é conectado na rede.

E ssa fragmentação da SDWAN procura fornecer a priorização do tráfego de rede baseada em políticas dinâmicas, ao mesmo tempo que remove as decisões locais dos dispositivos de rede. Anteriormente, essas

decisões dificultavam a implementação de mudanças globais ou regionais na rede.

Deve haver uma comunicação entre os planos descritos acima, logo a comunicação entre cada plano é feita de diferentes formas, utilizando diferentes meios, temos que entre entre o plano de dados e o plano de controle é utilizado o *Southbound API*, a comunicação das aplicações e o plano de controle é chamada de *Northbound API* e a comunicação entre controladores, orquestradores ou até mesmo entre dois elementos de rede é chamada de *Esat-West API*, sendo assim ambas são descrita a seguir com suas respectivas funções [Segeč et al. 2020]:

- *Southbound API*: Responsável por promover a comunicação entre os ativos de redes, e a controladora, existem diferentes formas de comunicação muitas proprietárias, como a Cisco que utiliza (OMP sobre DTL/TLS) e alguma soluções abertas que utilizam do OpenFlow ou REST API.
- *Northbound API*: Responsável pela comunicação da controladora com aplicações externa, essas aplicações podem enviar informações de controle ou solicitar informações, assim como a Southbound API, existem soluções proprietárias e de código aberto para essa comunicação.
- *East-West API*: Responsável pela comunicação entre dispositivos iguais, como duas controladores ou duas entidades de redes.

A figura 2.6 explicita bem os conceitos que descrevem a arquitetura de uma SDWAN, onde pode-se ter uma ideia mais clara dos planos e suas funções e como ambos de comunicam.

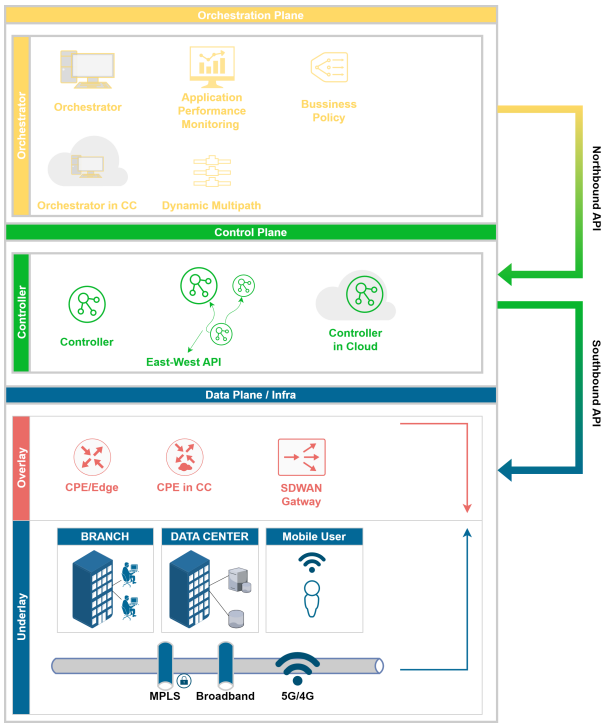


Figura 2.6: Arquitetura SDWAN. Fonte: Autor

É notória uma grande evolução da tecnologia SDWAN principalmente dentro do mercado de soluções proprietárias, algumas soluções já citadas como cisco Viptela, Cisco Meraki, VmWare, Fortinet e afins,

contudo nota-se que a tecnologia está sendo pouca explorada no meio acadêmico, ate o presente momento foram encontradas apenas duas tecnologias open source SDWAN, EveryWAN e flexiwan, que serão melhor exploradas a seguir.

2.15 FLEXIWAN

Entrando nas soluções OpenSource conhecidas até então sobre a SDWAN, temos um destaque a **FlexiWan** [Fleiwan] uma solução open source, onde o principal foco é reduzir os custos e aumentar a confiabilidade da rede. De acordo com a documentação fornecida pela própria organização, disponível em [Flexiwan 2019], a tecnologia conta com um esquema de arquitetura aberta (open architecture) *open source SDWAN infrastructure*, onde a mesma inclui um vRouter (Flexiedge), gerenciamento, orquestração e automação e funcionalidades essenciais da SDWAN. A visão de SDWAN abordada pela Flexiwan é mais clássica, onde as funções de controle ainda rodam no roteadores virtuais (Flexiedges).

O software de código aberto da flexiWAN permite a integração com terceiros para agregação de serviços e performance, como descrito na figura 2.7.

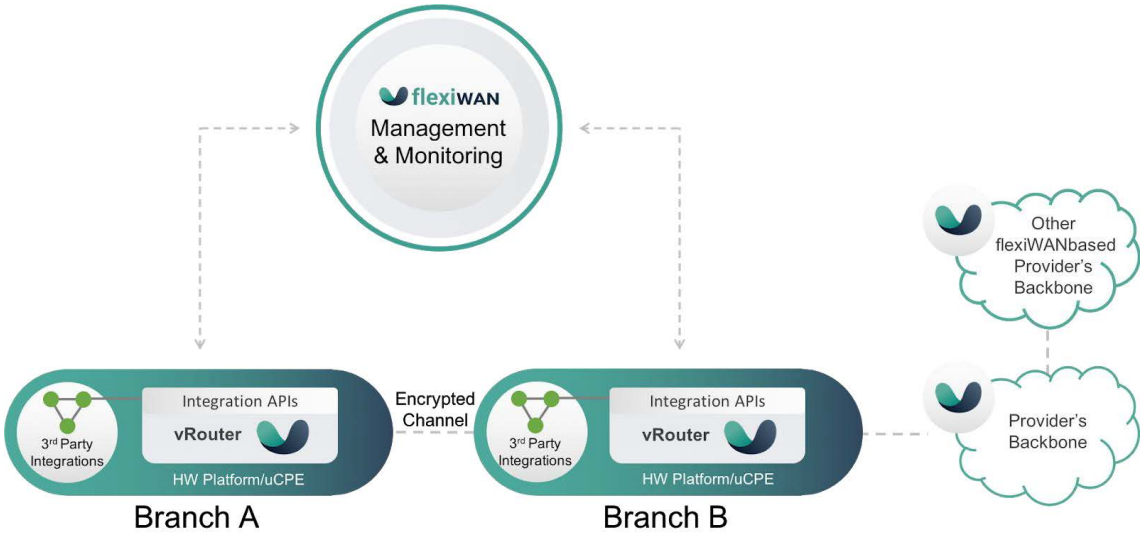


Figura 2.7: FlexiWAN Architecture. Fonte: [Flexiwan 2019]

Dentro da arquitetura proposta a integração com terceiros ou *3rd party integrations* pode acrescentar serviços aos domínios/sites, descritos em 3 tipos pela Flexiwan:

- *"Domain Experts"*: Integrações que são fornecidas por empresas que adicionam funcionalidades como segurança e otimização de VoIP.
- *"Application/Service Providers*: Integração com SaaS, MSPs, IaaS onde podem ser oferecidas integrações para gerenciamento proprietário dos serviços fornecidos.
- *"Enterprises/users"*: Gerenciamento especifico com adição de logica para como o trafego gerado

sera manejado.

2.16 EVERYWAN

A EveryWAN é uma SDWAN open source, descrita em [Scarpitta et al. 2021], totalmente modelada com tecnologias open source e conta com robustas funcionalidades e esta totalmente aberta e disponível em EveryWAN Download.

A arquitetura utilizada é totalmente baseada em sofware, utilizando conceitos de SDN e NFV, que por meio de vCEs são construídos os *EveryEdge routers* que por fim são implementando com VNF e são totalmente controlados pelo *EveryEdgeOS*. Tal controlador vai além das funções de gerenciamento e programabilidade, há uma implementação de ZTP fazendo o registro dos devices na topologia e além disso iniciando suas configurações. Há também a possibilidades da NOS e do orquestrador estarem inclusos dentro da topologia física em alguma site ou em uma solução em nuvem, como google cloud, AWS e afins.

A implementação das funções e de arquiteturas mais robustas contam com flexibilidade e podem ser moduladas de acordo com as necessidades de cada usuário da EveryWAN. Instancia logicas podem ser criadas utilizando a camada de overlay, onde permite que diferentes aplicações rodem em diferentes "pedaços"da rede, oque permite a alocação de recursos de acordo com a aplicação.

Um dos principais serviços abordado na pesquisa da EveryWAN é o mecanismo de tunelamento proposto, utilizando o conceito de *"Network Slicing"* que garante a alocação de recursos de uma infraestrutura de rede física para um serviço, permitindo assim a separação logica e física dos recursos de rede. onde instancias de redes virtuais são criadas sobre a mesma conexão WAN, esse tipo de pratica é justamente o conceito de "redes dirigidas por aplicação"onde os serviços podem modular a rede, neste caso criando instancias para redirecionar o trafego de um aplicativo especifico, assim diferentes aplicativos podem executar de maneira separada contudo utilizando a mesma conectividade.

2.17 SOLUÇÕES SDWAN PROPRIETÁRIAS

O mercado de SDWAN teve um salto muito grande no que se refere a tecnologia em si cada fabricante implementa a SDWAN de maneira diferente, contudo existem alguns requisitos mínimos nos quais devem ser satisfeitos para que a s implementações sejam consideras verdadeiras SDWANs. Existem algumas soluções no mercado que se destacam dado ao alto numero de clientes e sua performance, as soluções, como descrito, podem ter diferentes arquiteturas, mesclando software e hardware. De acordo com [Sturt 2023] as melhores soluções disponíveis no mercado atualmente podem ser rankeadas de acordo com alguns parâmetros levados em conta como:

- **ZTP**;
- **Traffic Steering Circuit (Direcionamento de trafego)**;
- **Gerenciamento**;

- **Reporting**;
- **Acesso Nativo na Nuvem**;
- **SASE Security**;
- **Next generaton Firewall**;
- **Network POPs**;

Assim de acordo com [Best SDWAN SOFTWARES] temos que os melhores softwares SDWAN (Maio - 2023) são: (Top 5 avaliado pela G2 co base na comunidade em quesitos de satisfação, analise de dados e documentação de cada tecnologia):

1. *Cisco Meraki SDWAN*;
2. *Bigleaf Networks*;
3. *Cradlepoint*;
4. *Cisco SDWAN*;
5. *VPN Gateway virtual appliance*;

No que diz respeito ao mercado de soluções proprietárias é difícil comparar as soluções, uma vez que cada fabricante implementa a mesma de maneira única, com diferentes focos e diferentes integrações, até mesmo quando a proposta é a mesma as soluções podem variar. Em [Segeč et al. 2020] é explorado algumas das principais funções que ajudam a ter um parâmetro de comparabilidade entre as diferentes soluções:

- **Active/Active**: Diz respeito a operação em modo hibrido de um site utilizando links WAN privados e públicos a fim de utilizar a capacidade total dos recursos.
- **CPE**: Facilidade na implementação dos dispositivos que compõe a SDWAN como os roteadores de borda ou outros elementos, virtual ou físico.
- **Segurança e Politicas Corporativas**: Prover suporte para politicas de segurança em arquiteturas WAN, além de criação de politicas de rotas baseada nas intenções corporativas.
- **Visibilidade, priorização e gerenciamento de aplicação**: Este tópico esta relacionado a politicas de QoS e gerenciamento avançando, geralmente providos por politicas de aplicativos criticos.
- **Resiliência e alta disponibilidade**: Esta função esta ligada com a função *"Active/Active"*, onde há uma relação a interrupções, como falhas nos dispositivos CPE (Customer Premises Equipment) ou nos links WAN. É necessário manter uma experiência ideal para o usuário final ou para as aplicações em execução na rede, ou seja, garantir que, mesmo em caso de falhas ou interrupções em determinados componentes da infraestrutura, a SDWAN seja capaz de redirecionar o tráfego de forma inteligente e eficiente para evitar interrupções na conectividade e proporcionar uma experiência contínua e otimizada para os usuários.

- **Interoperabilidade nas camadas 2 e 3**: Dispositivos da SDWAN precisam ser capazes de interagir e cooperar com os dispositivos adjacentes na rede local (LAN), que podem ser switches ou roteadores. Essa colaboração é necessária para estabelecer conexões, trocar informações de roteamento, realizar segmentação de rede etc.
- **Gerenciamento**: Para facilitar o gerenciamento é de suma importância que a SDWAN conte com portais onde seja de fácil visualização e acesso a métricas, gráficos e índices de performance da rede, assim como reportes de incidentes.
- **Suporte de API para a controladora**: Além da capacidade de comunicação com os dispositivos a SDWAN deve ser integrada com outras APIs como o SIEM (*Security Information and Event Management*) e leitura e escrita de eventos de logs.
- **ZTP**: A capacidade de prover a função de ZTP é essencial em uma WAN pois eleva o nível de implementação e reduz a complexidade de instalação.
- **Certificado FIPS 140-2**: Certificado base da FIPS (*Fedaral Information Processing Standard*).

3 FERRAMENTAS UTILIZADAS

Neste capítulo será abordado de maneira detalhada cada ferramenta utilizada para o desenvolvimento do projeto, como como o hardware e softwares que foram utilizados para a confecção da rede controlada.

3.1 SERVIDOR

O servidor utilizado foi disponibilizado pela empresa Teltec Solutions, o servidor conta com clusterização de 4 hosts. O software de gerenciamento dos servidores é o VMware Vcenter (A versão fica restrita devida a politicas da empresa). A maquina virtual que será responsável pela execução do GNS3 server conta as seguintes especificações:

- **vCPUs**: 20;
- **Armazenamento**: 350GB;
- **RAM**: 32GB;
- **Sistema Operacional**: Linux Server 22.04.2 .

3.2 GNS3

O GNS-3 (*Graphical Network Simulator 3*) é uma plataforma de emulação de redes de código aberto que permite a criação de topologias de redes simples a complexas em ambiente virtual, [GNS3 Documentation].

Uma das grandes vantagens sobre o uso do GNS3 é que o mesmo possui suporte para diversos equipamentos de redes, como switches, roteadores, firewalls, controladores etc. No GNS3 é também possível a integração com outros softwares como *Virtual Box*, *VMWare* e ate mesmo dispositivos de redes físicos. A flexibilidade na implementação de diversas topologias de redes faz desse software uma poderosa ferramenta para explorar diversas topologias e soluções.

Foi utilizada a versão "**GNS3 Server (2.2.40)**"do GNS3.

3.3 SWITCHES EXOS

A Extreme networks é uma empresa de redes focada na areá de routing/swtiching, há uma solução de Open Switches disponível no "Market Place"do GNS3, que será utilizada na topologia e irão fazer o pepel como switches de distribuição (camada 2) e switches Core (camada 3).

O switch EXOS é um software de código aberto [Switching Wired Access].

3.4 IPERF

O *iperf*, especialmente sua ultima versão *iperf3* é uma ferramenta muito utilizada para a geração de trafego, conta com diversas funcionalidades para medição de diversos parâmetros de analise e desempenho de redes como medição de largura de banda, jittler e delay, [iperf3 Documentation]

O *iperf3* pode ser facilmente instalado nos sistemas dispostos no site <https://iperf.fr/> assim como sua documentação e exemplos de uso também estão dispostos no site citado. O principal papel da ferramenta é a medição da largura de banda disponível entre dois links, podem ser criados servidores que clientes usam para se conectar ou é possível se conectar com um dos servidores disponibilizados pelo próprio **iperf**.

Além da medição de largura de banda pode ser fornecido também a quantidade de Bytes/Bits transferidos, jittler e atraso, essa ferramenta conta com um poderoso leque de possibilidades, as opções contam com sincronização de tráfego, utilização de IPv4 ou IPv6, utilização de TCP ou UDP, duração do teste, intervalo de atualização e afins. Com tais ferramentas pode-se simular trafego de voz, videlcall e derivados.

Além disso, em sistemas Linux, é possível executar dois ou mais processos do **iperf3**, permitindo que o sistema tenha certa flexibilidade para executar várias sessões com diferentes protocolos.

3.5 WIRESHARK

O wireshark é um software de captura de dados, muito utilizado em redes. O mesmo permite uma visualização clara de todos os protocolos que compõe um determinado pacote. Além da captura dos pacotes, o software prove ferramentas adicionais que simplificam, separam e geram gráficos de um determinado fluxo de acordo com um filtro aplicado, [Foundation 2023].

No que diz respeito ao tipos de filtros aplicados no wireshark pode-se utilizar diversos exemplos, podemos por exemplo filtrar pacotes com um endereço de destino $a.b.c.d$ com protocolo da camada de transporte UDP na porta 80. Isso permite uma analise criteriosa e mais detalhada dos fluxos que estão acontecendo na rede nessa porta e endereço.

Além disso o GNS3 possui uma ferramente de captura de pacores integrada diretamente com o wireshark, essa ferramente permite o wireshark analisar qualquer link (enlance) dentro da topologia, o que permite que seja feita uma analise detalhada de qualquer ponto da rede.

3.6 MÉTRICAS DE PERFORMANCE

Existem algumas métricas amplamente utilizadas em redes de comunicação que guiam no entendimento e analise de dados como o throughput, delay e jitter. De acordo com [Yuniarto e Sari 2021], temos que o throughput é definido como o numero de bits recebido por segundo em um determinado fluxo, essa métrica é considerada a taxa de entrega. O delay por sua vez corresponde ao tempo de viagem de um determinado pacote, normalmente o tempo de viagem entre os comunicadores da conexão como cliente e

servidor. Apesar do delay ter um valor fixo ele inclui uma serie de atrasos que o pacote sofre em todo caminho percorrido, como atrasos de processamento, fila, transmissão e propagação, [F.Kurose 2014], sendo assim o atraso total pode ser dado por:

$$D_{total} = d_{proc} + d_{fila} + d_{trans} + d_{prop} \tag{3.1}$$

Por fim o jitter que diz respeito a variação de delay entre o pacote atual e o pacote anterior dentro de um mesmo fluxo, [Yuniarto e Sari 2021]. Considerando t um instante de tempo qualquer em que $t \neq 0$, temos que o jitter em um determinado instante de tempo é dado por:

$$J_t = D_t - D_{t-1} \tag{3.2}$$

3.7 FLEXIWAN

Dentre as tecnologias citadas que utilizam código aberto foi optada pela escolha da Flexiwan, onde a mesma disponibiliza os softwares para download. Os códigos fontes de todos os componentes da Flexiwan estão dispostas em [FlexiWan Components]. Vale notar que apesar de ser uma solução que utiliza de código aberto é uma solução paga, contudo conta com o período de teste de um mês, foi solicitado a equipe da Flexiwan a extensão do período de testes para a melhor coleta e analise dos resultado com intuito de pesquisa, que corinhosamente cedida pela equipe.

3.7.1 FlexiEdge

O FlexiEdge é o roteador que utiliza a integração com o vManager, ele baixa todas as suas configurações da nuvem da Flexiwan, desde politicas de QoS até rotas estáticas, tabelas OSPF, BGP, politicas de firewall e varias outras funções, sua estrutura de código aberta esta disponibilizada em [Flexiwan 2019].

A versão utilizada para trabalho foi a **FlexiEdge 6.1.22**, toda a documentação está disposta em [Flexiwan 2019].

3.7.2 FlexiManager

O FLexiManager é a plataforma de gerenciamento da SDWAN que está localizado em nuvem, nesta plataforma pode-se adicionar os FlexiEdge, criar tuneis entre os roteadores, criar politicas, gerenciamento, analise de trafego, criação de politicas de firewall, criação de caminhos, diversas funcionalidades estão dispostas.

A versão utilizada para trabalho foi a **FlexiManager 6.2.19**, toda a documentação está disposta em [Flexiwan 2019].

3.8 FORTINET

A tecnologia proprietária escolhida foi a SDWAN da Fortinet, onde o foco da solução se concentra principalmente no ZTP e segurança, [Laliberte 2023], a solução promete entregar visibilidade, análises e segurança dentro de sua solução. Ainda de acordo com [Laliberte 2023], a empresa foca no reconhecimento e separação de aplicações para prover uma nível de segurança maior por meios de politicas de rede.

Existem diferentes níveis de implementação da SDWAN da Fortinet, esses níveis variam de acordo com a demanda da organização e podem aumentar o custo total da implementação. Para este trabalho visando apenas a coleta de dados e implementação dos principais recursos da SDWAN foi optado pela implementação simples, feita apenas pelo Fortigate e FortiManager, descritos a seguir. Contudo a solução mais completa da Fortinet inclui uma séria de recursos como o FortiManager e o Fortianalyzer, [Laliberte 2023].

3.8.1 Fortigate

o Fortigate, descrito pela Fortinet é um NGFW (Next Generation Firewall) contudo ele não está restrito apenas as funções de firewall oferecendo também funções de roteador, [Fortinet 2023]. Com isso o Fortigate conta com recursos de SDWAN, sendo assim o mesmo escolhido para ser o roteador de borda da topologia. A SDWAN da Fortinet conta uma avaliação gratuita de 15 dias desde a primeira execução dos compenentes, para realizar os downloads dos equipamentos deve ser criada uma conta no site da empresa, FortiCloud

A versão utilizada para este trabalho foi o **Fortigate 7.0.9**, toda a documentação está disposta em [Fortinet 2023].

4 ARQUITETURA PROPOSTA

Este capitulo tem como foco especificar a arquitetura base dos testes, assim como a metodologia de análise. Neste capitulo teremos uma visão clara da topologia desenvolvida em ambiente controlado.

4.1 TOPOLOGIA

A topologia de um sistema dita como o fluxo de dados do mesmo funciona, a escolha da topologia deve ser pensada de modo a facilitar o fluxo de dados para uma determinada demanda. Existem diferentes tipos de topologias de redes, como a topologia em estrela, em barramento, em anel, em malha, entre outras, [Odom 2020]. Cada topologia possui características distintas em termos de escalabilidade, facilidade de implantação, confiabilidade e custo. A seleção da topologia adequada depende dos requisitos da rede, como o número de dispositivos, a distância entre eles, a capacidade de expansão e a tolerância a falhas.

Para o projeto a topologia estrela foi selecionada para os switches de acesso, e uma topologia árvore para toda a LAN a fim de criar uma hierarquia de campus design.

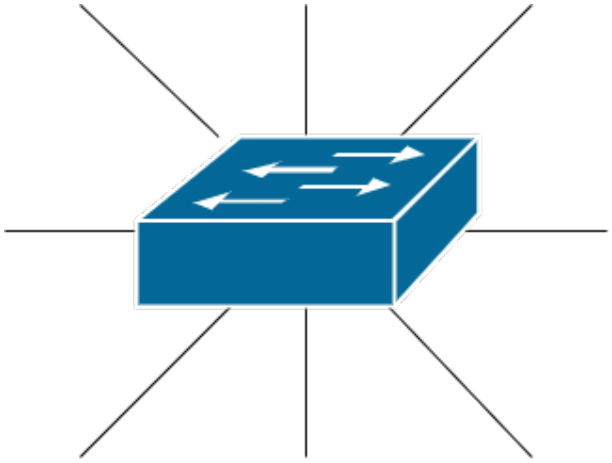


Figura 4.1: Topologia Estrela. Fonte: Autor

4.2 ARQUITETURA

A topologia dita como o fluxo de dados deve seguir, contudo a arquitetura nos orienta a como dispor nossos recursos de maneira mais eficiente a fim de alocar, de maneira lógica e organizada, a distribuição dos equipamentos de rede. Para esta pesquisa foi escolhida a arquitetura *Campus Tier 3*, essa arquitetura é muito utilizada para redes de grande porte, [Odom 2020].

Esse tipo de topologia conta com três camadas separadas por suas finalidades:

- **Camada de Acesso**: A camada de acesso é responsável pela ligação de usuários finais ao resto da rede, nesta camada a densidade do switch escolhido deve ser alta, ou seja, um grade numero de portas para suprir a demanda de usuários finais. Vale notar que usuários finais podem ser tanto pontos de acesso para areá de trabalho assim como servidores de distruibição de dados. Nesta camada os switches operam em camada 2.

- **Camada de Distribuição**: A camada de distribuição prove um ponto de agregação dos Switches de acesso, esses switches tendem a ser menos densos em portas mas possuem um alto throughput pois muitas vezes são pontos de agregação de varios swtiches de acesso switches de distruibção não conectados diretamente aos dispositivos finais. Nesta camada os switches operam em camada 2.

- **Camada Core**: Responsável por interligar todos os switches de distribuição e também pode ser responsável por funções de roteamento de pacotes, tanto entre as VLANs que compõem a LAN tanto quanto para roteamento para fora da LAN. Switches core devem ser switches que operam em camada 3 e é altamente recomendável que tenham um alto throughput para aguentar o tráfego de toda a rede que está abaixo do mesmo.

Para melhor entendimento a figura 4.2 exemplifica melhor a arquitetura. Em seguida temos nas figuras 4.3 e 4.4 das LANs que serão projetadas no GNS3.

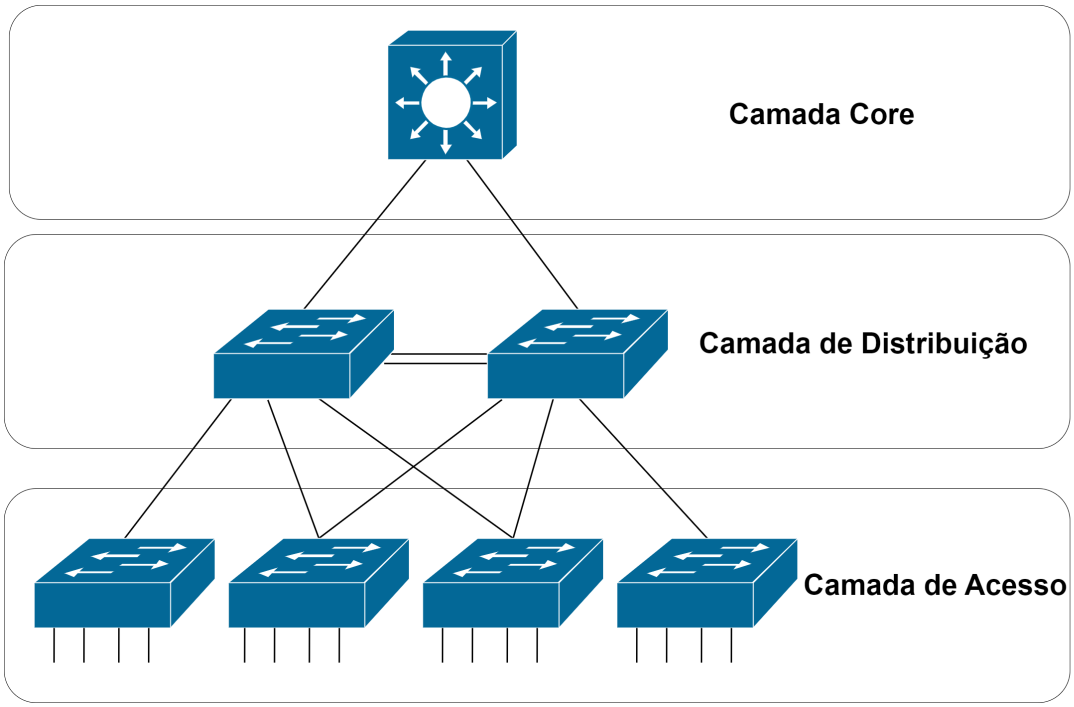


Figura 4.2: Campus Tier 3 Architecture. Fonte: Autor

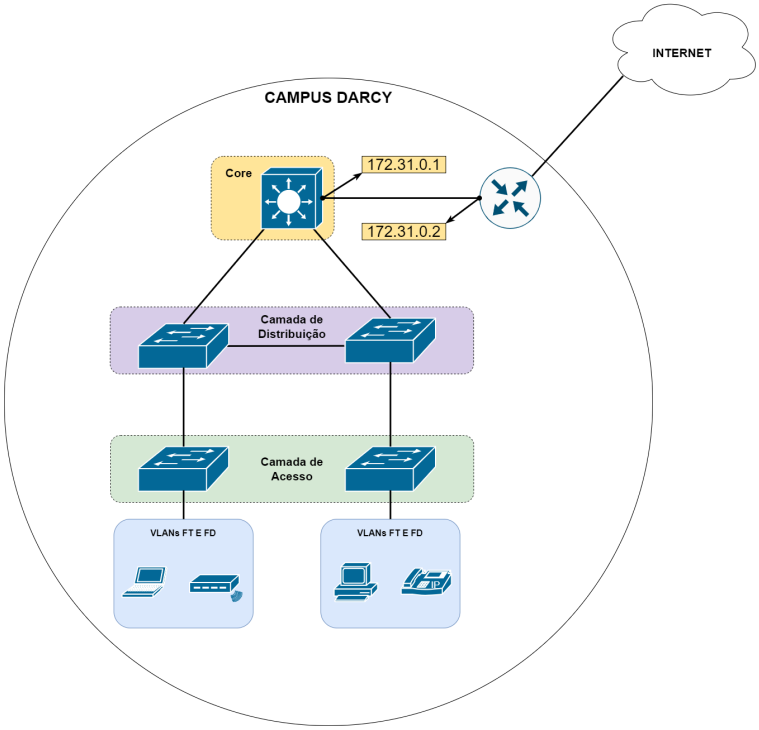


Figura 4.3: Arquitetura do Campus Darcy. Fonte: Autor

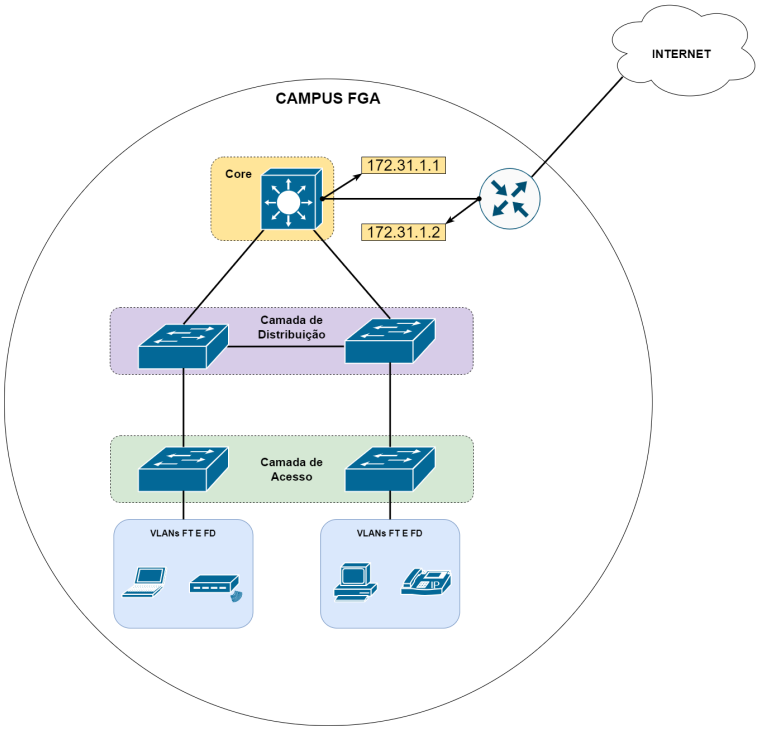


Figura 4.4: Arquitetura do Campus FGA. Fonte: Autor

4.3 REDE

Após a descrição de como a topologia física será implementada, há de se pensar no endereçamento da rede como criação de VLANs, MSTP, roteamento e afins.

Para melhor divisão foram criadas 4 VLANs em cada LAN, começando com o Campus Darcy:

- *MGMT*: VLAN de gerenciamento, essa vlan nos dará acesso as funções de gerenciamento remoto nos SW;
- *FT*: VLAN fictícia simbolizando uma unidade do Campus Darcy, neste casso a Faculdade de Tecnologia;
- *FD*: VLAN fictícia simbolizando uma unidade do Campus Darcy, neste casso a Faculdade de Direito;
- *Default*: VLAN utilizada para o enlace entre o SWCORE e o Router Edge.

Para cada VLAN deve ter separado, por demanda, um determinado numero de IP's, para que sejam distribuídos via **DHCP**. A distribuição é feita pelo Switch Core de cada topologia. Além disso é importante notar que o MSTP (Multi Spanning Three) é de suma importância visto que em ambas as topologias 4.3 e 4.4 há um loop de camada 2 entre os switches.

Tabela 4.1: Distribuição de sub redes Entre as VLANs no Campus Darcy

Campus Darcy			
VLAN/TAG	**ID da Rede**	**Broadcast**	**IP/Mascara**
MGMT/4096	**-**	**-**	**-**
FT/10	**192.168.10.0**	**192.168.10.254**	**192.168.10.0/24**
FD/20	**192.168.20.0**	**192.168.20.254**	**192.168.20.0/24**
Default/1	**172.31.0.0**	**172.31.0.3**	**172.31.0.0/30**

EM seguida as mesmas configurações se aplicam ao campus FGA, contudo os endereços devem ser diferentes:

- *MGMT*: VLAN de gerenciamento, essa vlan nos dará acesso as funções de gerenciamento remoto nos SW;
- *ENG*: VLAN fictícia simbolizando uma unidade do Campus FGA, neste caso a redes para estudos de Engenharia;
- *ADM*: VLAN fictícia simbolizando uma unidade do Campus FGA, neste caso para a parte administrativa do Campus;
- *Default*: VLAN utilizada para o enlace entre o SWCORE e o Router Edge.

Dado esses detalhes de projeto é possível então replicar as topologias no GNS3.

Tabela 4.2: Distribuição de sub redes Entre as VLANs no Campus FGA

Campus FGA			
VLAN/TAG	**ID da Rede**	**Broadcast**	**IP/Mascara**
MGMT/4096	**-**	**-**	**-**
ENG/30	**172.16.30.0**	**172.16.30.254**	**172.16.30.0/24**
ADM/40	**172.16.40.0**	**172.16.40.254**	**172.16.40.0/24**
Default/1	**172.31.1.0**	**172.31.1.3**	**172.31.1.0/30**

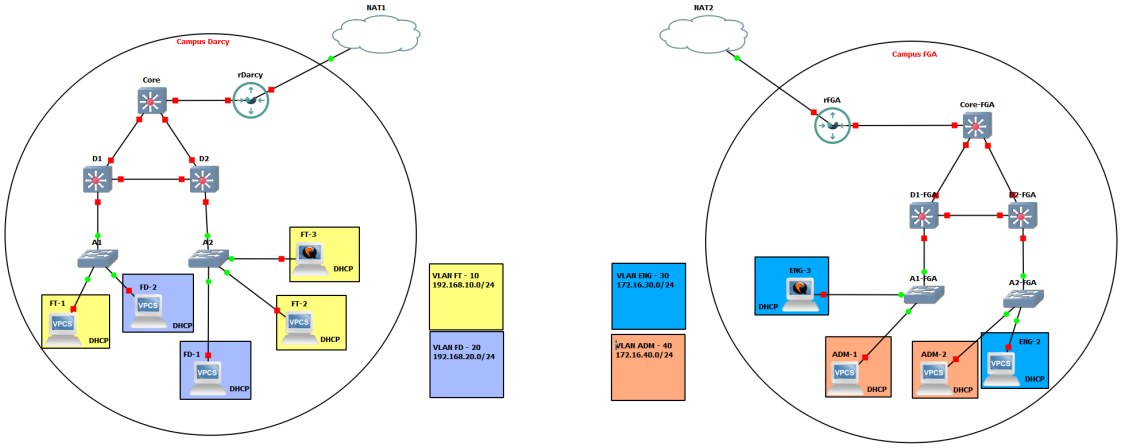


Figura 4.5: Arquitetura Completa da WAN. Fonte: Autor

4.4 DETALHES DE IMPLEMENTAÇÃO

4.4.1 CONEXÃO DAS LANs

Em uma WAN, como comentado anteriormente, um dos maiores focos e fazer com que todos os sites (LANs) se comuniquem entre si, muitos meios de acesso podem ser utilizados para tal feito, contudo alguns deles como acesso banda larga, 4G/5G são meios de acesso que trafegam direto pela internet, sendo assim todo o tráfego entre os sites estará exposto a internet publica. Para prover segurança, autenticação e integridade da mensagem é necessário a utilização de técnicas que provem níveis de segurança.

4.4.2 POLITICAS DE SEGURANÇA

Dentro de qualquer rede nos dias atuais é indispensável a aplicação de politicas de segurança, de maneira a proteger os vários tipos de dados que existem dentro de uma corporação, instituição ou até mesmo dentro de uma residencia.

Politicas de segurança podem ser aplicadas de diferentes formas, politicas de segurança podem privar o uso de aplicativos/sites indevidos, ou podem ser usados para não autorizar acesso a redes especificas dentro da corporação, o que, em muitos casos, é uma boa pratica.

4.4.3 TIPO DE SDWAN

4.4.3.1 Flexiwan

Como comentado a Flexiwan utiliza do gerenciamento em cloud, ou seja, não há necessidade de alocar recursos para o orquestrador/controlador em algum site ou até mesmo em um nuvem publica como AWS ou Azure. Esse serviço é oferecido dentro do pacote da SDWAN da FlexiWan e pode ser acessado no site Management Flexiwan.

4.4.3.2 Fortinet

Existem várias formas de se implementar a SDWAN da Fortinet, as diferenças estão na quantidade de soluções utilizadas, existem três principais equipamentos que provem a SDWAN na Fortinet: Fortigate, Fortimanager e o Fortianalyzer. Além disso é possivel a implementação em cloud.

Para este projeto optou-se pela utilização apenas do Fortigate dada a sua simplicidade de implementação, o fortimanager e fortianalyzer além de possuírem requisitos complexos de instalação (como RAM, CPU e memória) são de alta complexidade de configuração e além disso a solução em cloud não está disponível para a licença grátis de 15 dias disponibilizada pela empresa para o Fortigate/manager e analyzer.

5 ANÁLISE E RESULTADOS

Este capítulo será dividido em três partes. A primeira parte tem como objetivo analisar a tecnologia de código aberto da Flexiwan, enquanto a segunda parte se concentra na análise da tecnologia proprietária da Fortinet. Em seguida, será realizada uma análise comparativa entre as duas tecnologias.

5.1 FUNCIONALIDADES BÁSICAS

5.1.1 DHCP

Dentro das funcionalidades básicas de uma rede são as conexões primordiais entre equipamentos dentro de uma mesma LAN, saída para a internet e a conexão plena entra as LANs o que caracterizará a WAN.

Antes dos teste de conectividade serem efetuados é necessário testar se o serviço DHCP está em pleno funcionamento, nenhum dispositivo final foi configurado com IP estático em vez disso foi configurado que utilizassem o servidor DHCP para obterem um endereço IP. Como mencionado anteriormente em 4 os responsáveis pela distribuição dos IPs são os switches core de cada LAN. A seguir, na figura 5.1 temos um print do vPC (**FT-1**) fazendo o processo de solicitação de um endereço que compete a sua VLAN "FT". Na figura pode-se observar o processo de solicitação DHCP, **DORA**, mencionado no capitulo 2 foi realizado e a maquina está configurada com um endereço IP.

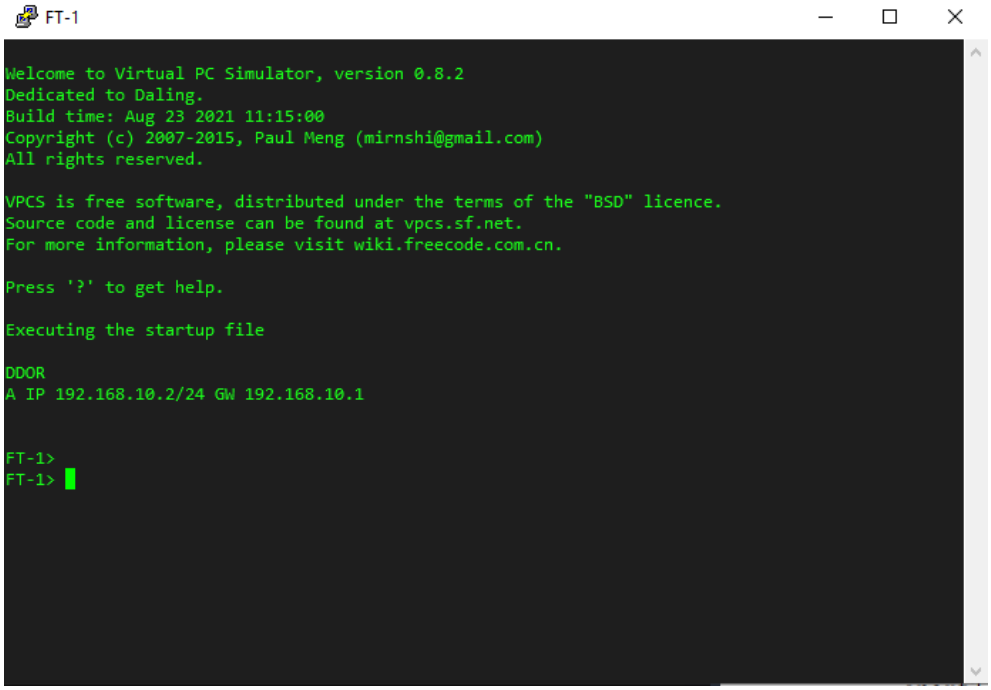


Figura 5.1: Protocolo DHCP em Operação. Fonte: Autor

Com o serviço de DHCP funcionando assegura-se que todos os usuários finais que utilizarem de DHCP terão um endereço IP não duplicado e válido dentro de suas LANs pertencentes.

5.2 ANÁLISE FLEXIWAN

5.2.0.1 Tunelamento e Conexões Essenciais

Para a conexão dentro de uma mesma VLAN foram utilizadas os vPCs *FT-1* e *FT-2*, foi utilizado o comando *ping*, segue resultados:

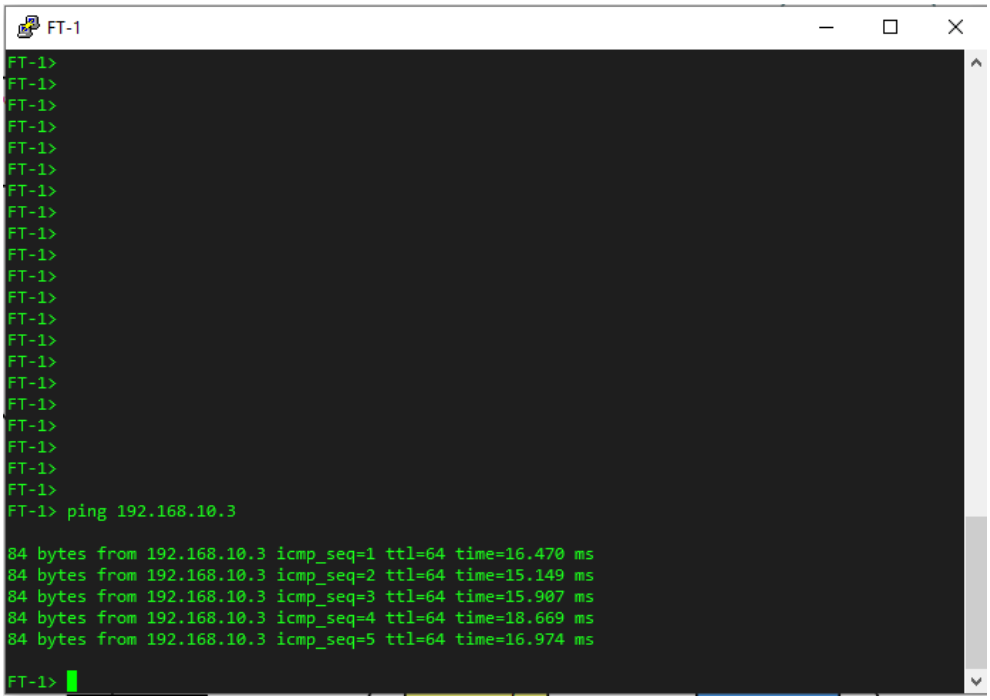


Figura 5.2: Ping entre FT-1 → FT-2. Fonte: Autor

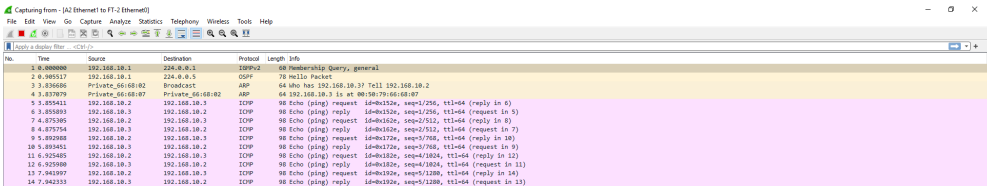


Figura 5.3: Ping entre FT-1 → FT-2 (WireShark). Fonte: Autor

Com a comunicação de camada 2 em funcionamento deve-se testar a comunicação de camada 3 dentro da LAN, neste caso, a comunicação ente as VLANs, o roteamento é feito pelo SWCORE através do OSPF e de rotas diretamente conectadas. Para esse teste utilizamos a LAN da FGA. Para este processo vamos utilizar dos vPCs *ENG-1* e *ADM-2*, seguem resultados:

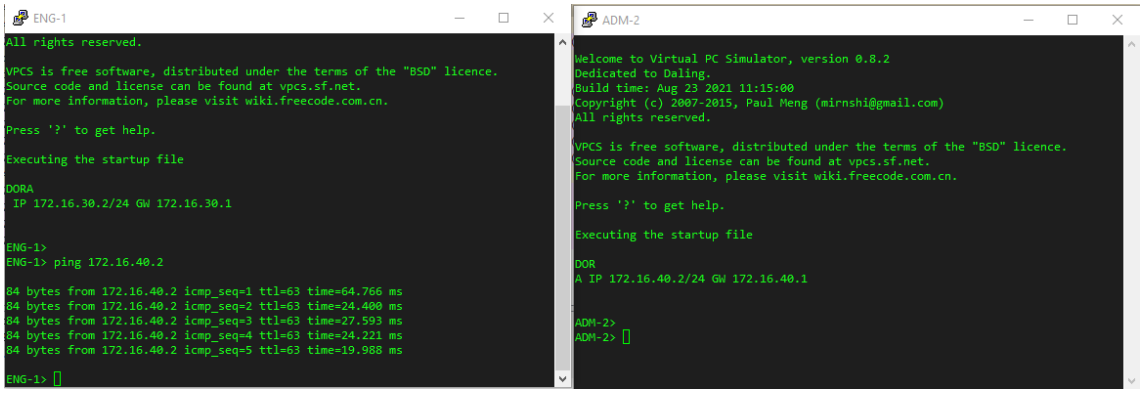


Figura 5.4: Ping entre ENG-1 → ADM-2. Fonte: Autor

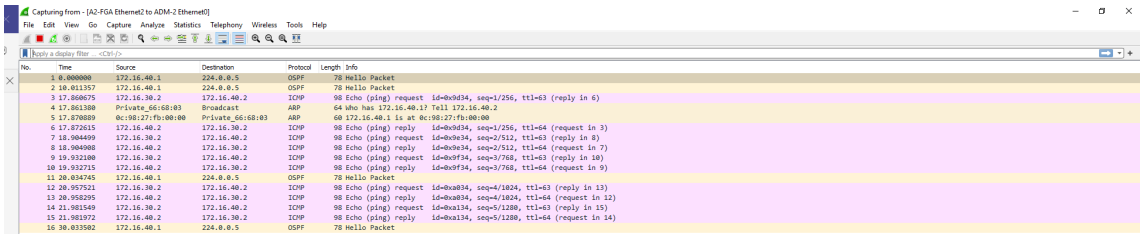


Figura 5.5: Ping entre ENG-1 → ADM-2 (WireShark). Fonte: Autor

Para a conexão com a internet, em ambos os sites a saída é o Flexiedge, como ilustrado em 4.5, nos switches cores foi configurada uma rota default (0.0.0.0/0) pelo FlexiEdge. Seguem resultados:

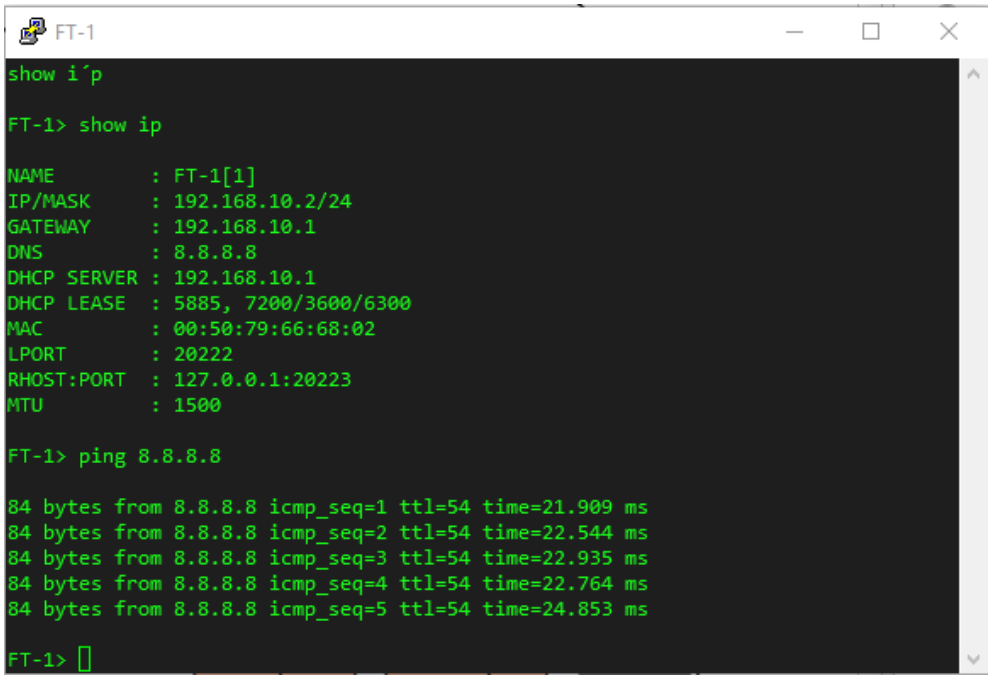


Figura 5.6: Ping entre ENG-1 → 8.8.8.8. Fonte: Autor

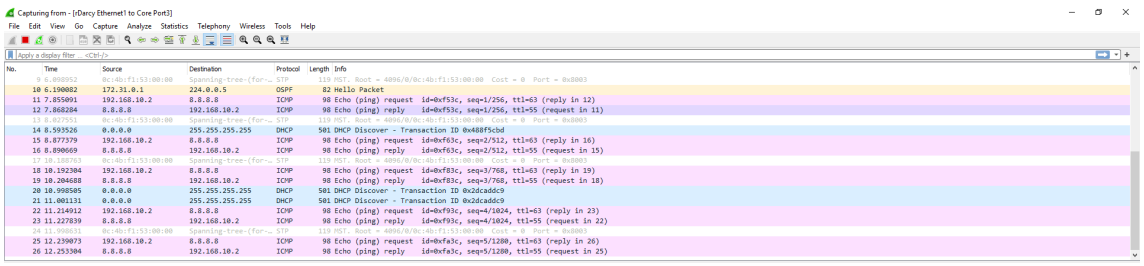


Figura 5.7: Ping entre ENG-1 → 8.8.8.8 (WireShark). Fonte: Autor

Um dos principais diferenciais da SDWAN é a capacidade de criar túneis de forma automática ou simples. Esses túneis são úteis de várias maneiras, fornecendo segurança na Internet e conectividade entre sites (LANs). Na plataforma Flexiwan, mais especificamente no Fleximanager, é possível criar túneis e definir o método de troca de chaves a ser utilizado, juntamente com a porta UDP para o protocolo VxLAN. Neste caso, foi aplicado o método IKEv2. O FlexiManager oferece um método de túnel seguro chamado IPSec over VxLAN, cujo cabeçalho do túnel está representado na Figura 5.9. Esse tipo de túnel proporciona flexibilidade na implementação de vários tipos de topologias, o que pode ser interessante dependendo do projeto em execução.

Figura 5.8: Método escolhido para troca de chaves. Fonte: Autor

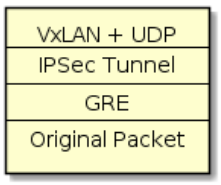


Figura 5.9: Cabeçalho do Túnel. Fonte: Flexiwan Documentation - Tunnels

A criação do túnel dentro do FlexiManager é bem simples, basta criar um *"Path"* (Caminho), e depois selecionar os roteadores que deseja criar o túnel, [Flexiwan 2019]. Como no projeto há apenas dois roteadores de borda, optou-se pelo método *Full-Mesh*.

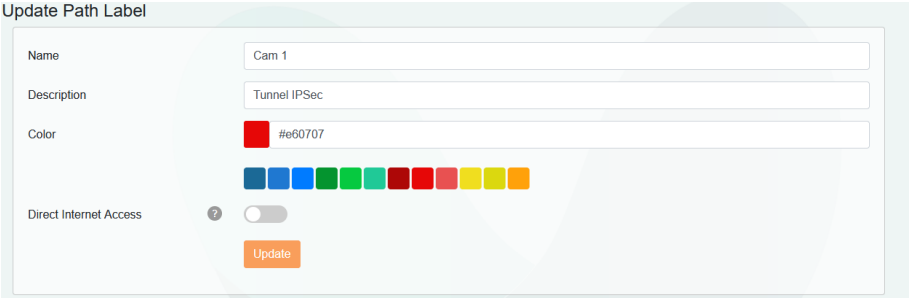


Figura 5.10: Path utilizado para o túnel. Fonte: Autor

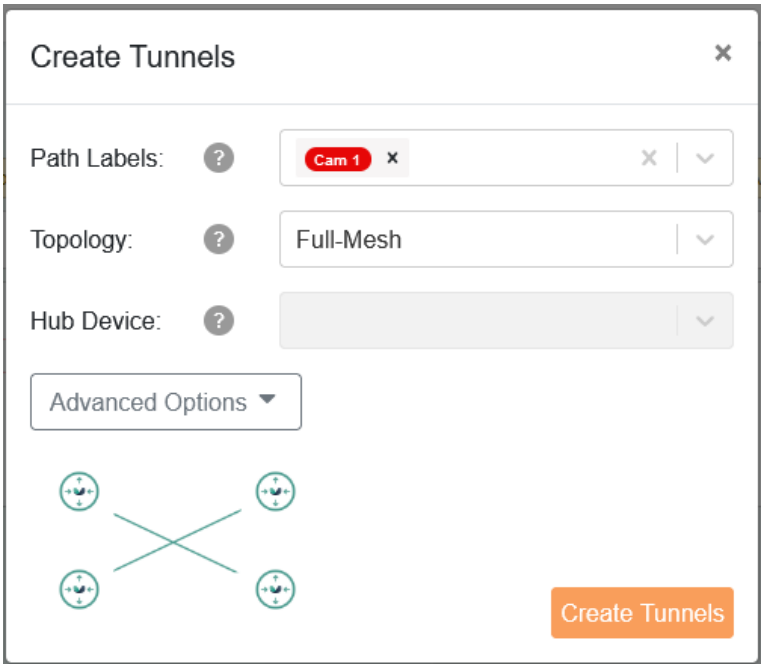


Figura 5.11: Túnel Criado . Fonte: Autor

Após isso todos os túneis criados utilizarão esse método que é um do mais seguros, como discutido em 2. Os túneis serão o ponto chave para fazer a testagem de conexão entre os sites, assim como medir a largura de banda da mesma, utilizando a ferramenta *iperf3*. Para esse primeiro teste foi escolhida a maquina *FT-3* como servidor escutando na porta 5050, com o seguinte comando:

```
iperf-3 -s -p 49152
```

Na parte do cliente, vai ser gerado um fluxo TCP, com tempo de 60 segundos, com intervalos de atualização que ocorrem a cada meio de segundo, o formato de saída em bits em Mb/s com o seguinte comando:

```
iperf3 -c 192.168.10.4 -p 49152 -i 0.5 -t 60 -f m
```

Assim o resultado obtido foi uma largura de banda de $4,04 Mbps$, como mostrado abaixo.

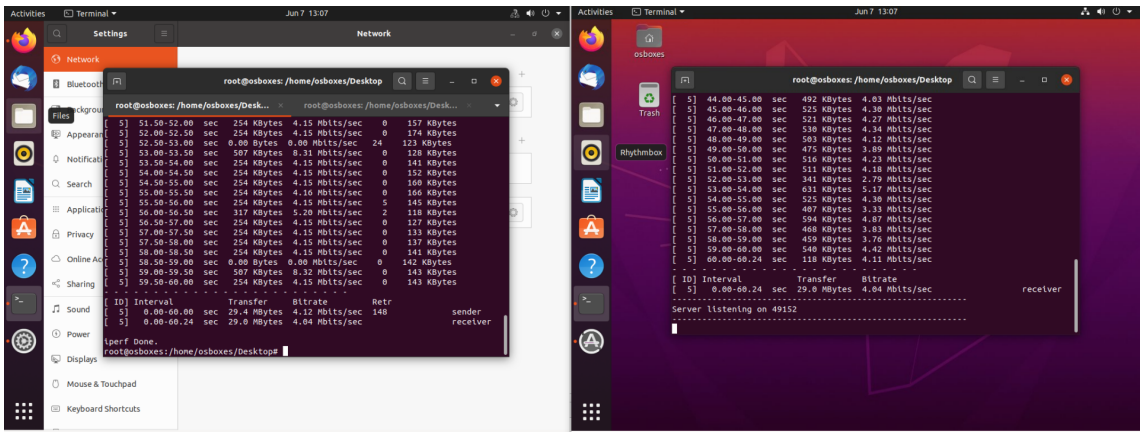


Figura 5.12: Utilização do iperf3 para medir largura de banda entre o link WAN. Fonte: Autor

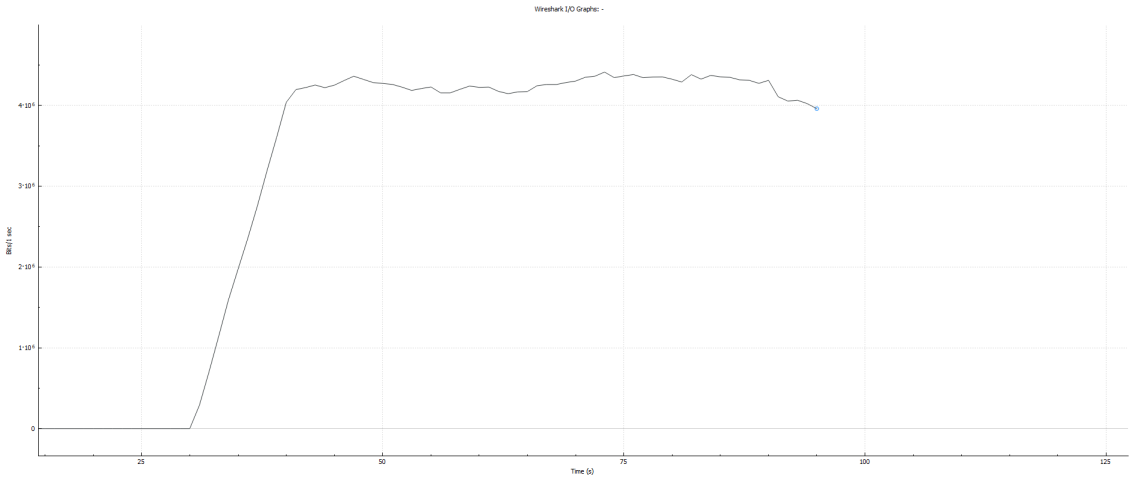


Figura 5.13: Gráfico Gerado pelo Wireshark a respeito do fluxo de dados para teste de velocidade. Fonte: Autor

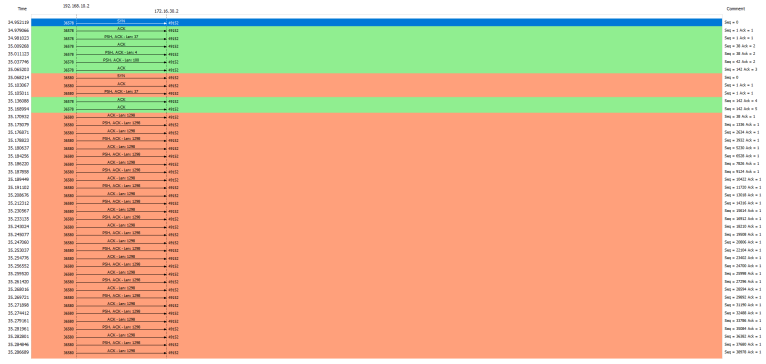


Figura 5.14: FlowGraph mostrando as estapas do TCP. Fonte: Autor

Todos os pacotes transmitidos pelo túnel utilizam do protocolo ESP que são criptografados. A figura abaixo contem um print do fluxo transmitido acima, neste print podemos ver a pilha de protocolos utilizada pelo ESP, além disso u tunelamento também conta com a utilização de VxLAN. Podemos notar que a porta UDP utilizada é a mesma estabelecida na configuração dos túneis, como mostrado na Figura 5.8.

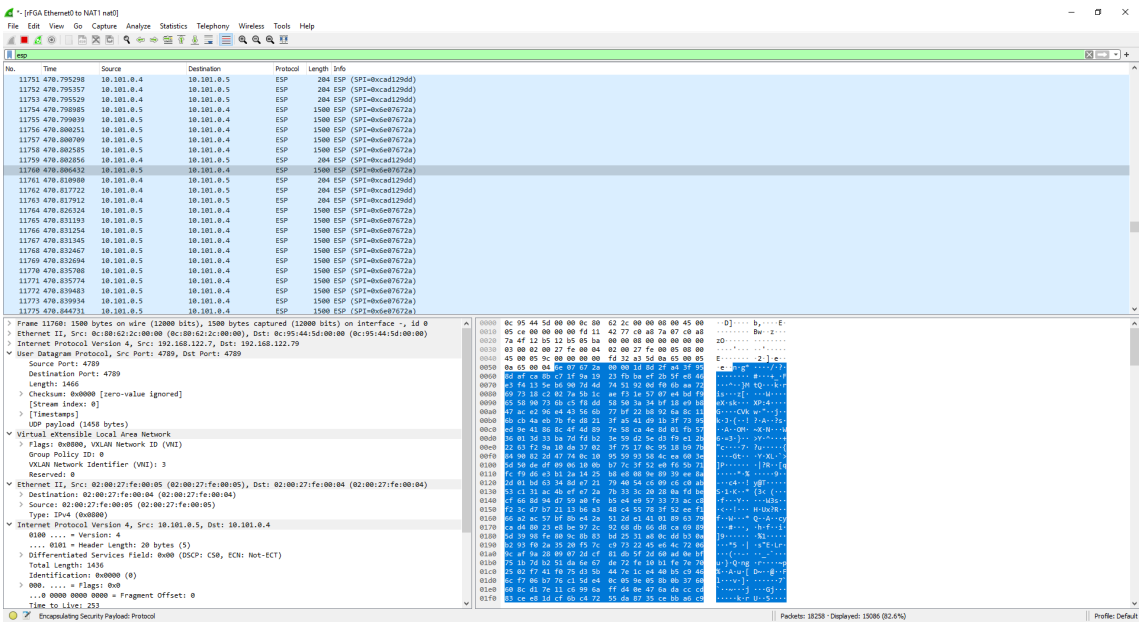


Figura 5.15: Captura do tráfego entre o túnel WAN. Fonte: Autor

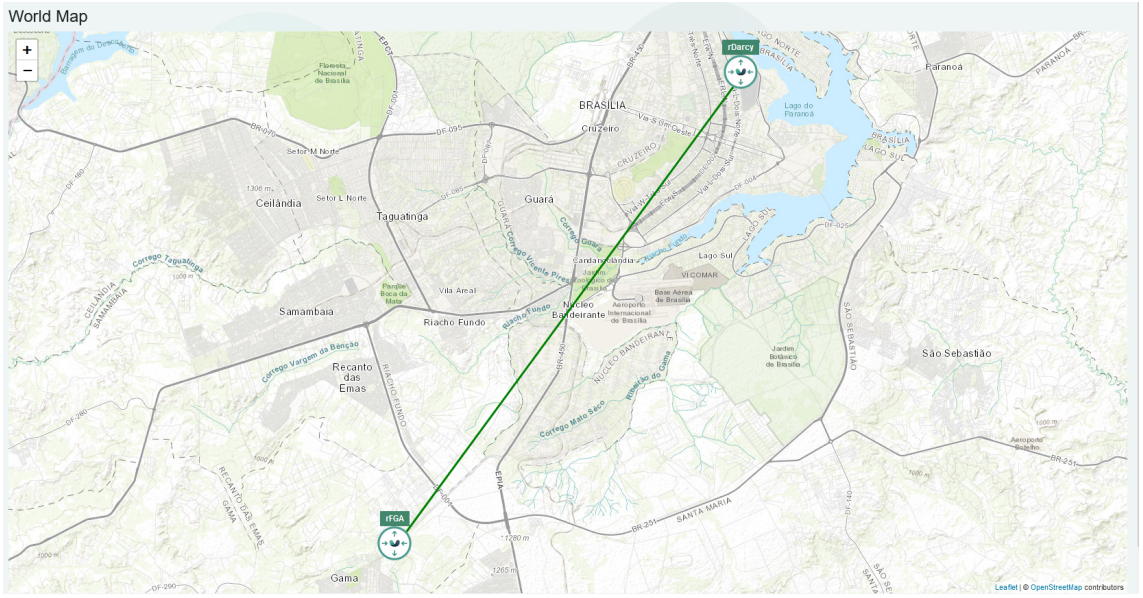


Figura 5.16: Visão do Túnel pelo FlexiManager. Fonte: Autor

5.2.1 QoS

Para a testagem do QoS, foi selecionado um método de análise quantitativa, foi criada uma instância dentro das opções de *APP Identification* do FlexiManager, identificando um novo aplicativo, neste identificador, foi alocado o endereço **0.0.0./0** para identificar todo o range de IP's, contudo o que importa neste novo aplicativo será seu protocolo, neste caso o **TCP** na porta **3030**.

5.2.1.1 QoS Desativado

Para a primeira parte do teste nenhuma política de QoS será aplicada em nenhum roteador de borda, FlexiEdge, assim sendo, será realizado um fluxo de dados utilizando o iperf3 em duas portas, a **3030** e outra na porta **5050**. Esses fluxos serão gerados de um cliente para um servidor e terão duração de **90 segundos**.

Para o servidor escolhemos a maquina que roda o próprio GNS3, a VM se encontra no LAB da Teltec Solutions e seu endereço é o **192.168.255.27** e os clientes serão as maquina FT-3 e ENG-3. Os Links utilizados para análise serão os links de saída para a internet de cada router. A seguir encontram-se os endereços do servidor e cliente:

- Servidor: 192.168.254.27;
- FT-3: 192.168.10.2;
- ENG-3: 172.16.30.2.

A seguir estão as análises feitas referentes aos fluxos:

Duas conexões TCP, 3030 e 5050, entre FT-3 → Servidor, a análise desse fluxo será feita com a saída do iperf3 e wireshark. O resultado observado na saída do iperf3, como mostra a figura 5.17, é notório que ambos os fluxos TCP compartilharam da banda total disponível, como mostrado em 5.12.

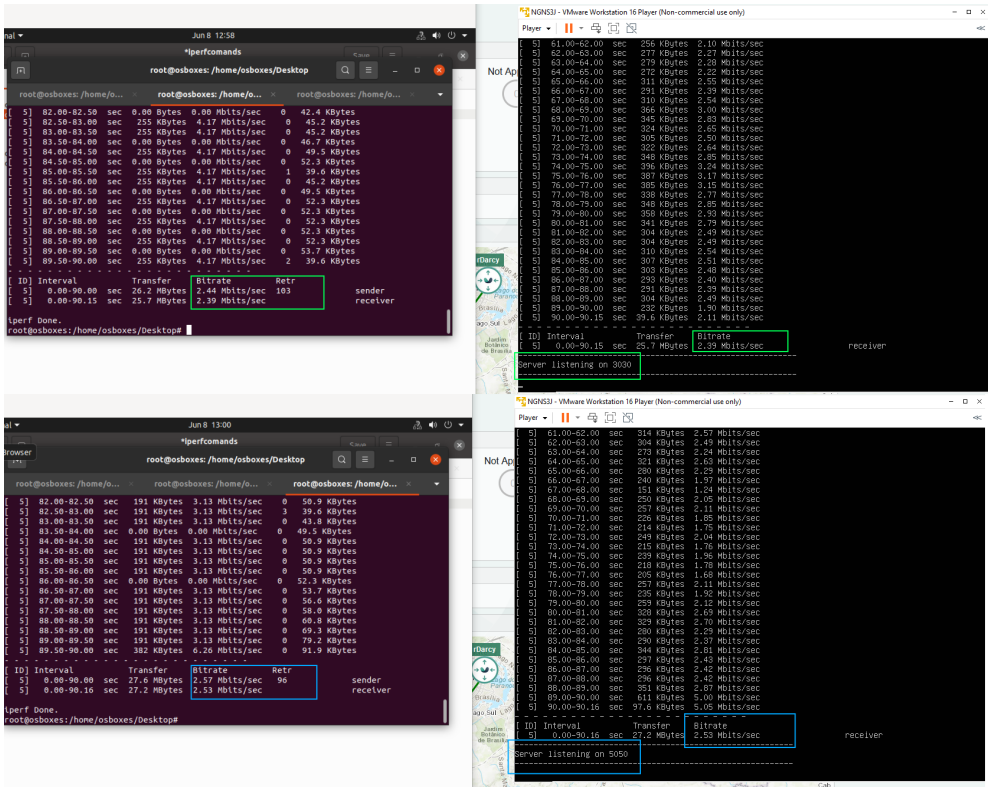


Figura 5.17: Saídas do iperf3. Fonte: Autor

A seguir estão os dados coletados pelo Wireshark, que serão utilizados para fornecer análises mais robustas. Na Figura 5.18, é possível observar uma leve diferença, no entanto, é notável a repartição de banda nos fluxos TCP. A Figura 5.19 mostra os gráficos de ambas as transmissões (com a média "10 interval SMA"aplicada, disponível nas opções de gráfico do Wireshark), que evidenciam as variações de banda, mas também mostram claramente a divisão da largura de banda total. Por fim, as Figuras 5.20 e 5.21 demonstram que não há nenhuma identificação específica no campo DSCP, como era de se esperar, uma vez que o QoS está inativo.

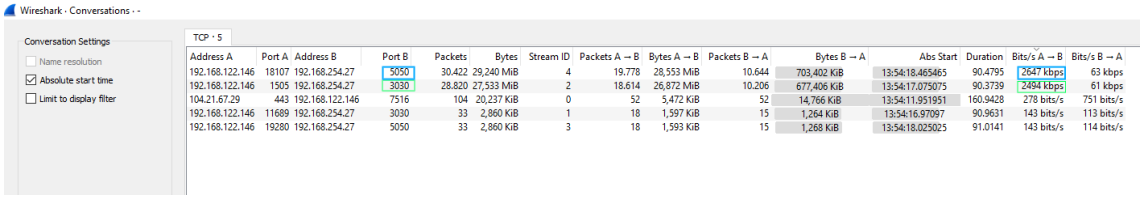


Figura 5.18: Estatísticas do Wireshark sobre os Fluxos para as portas TCP 3030 e 5050. Fonte: Autor

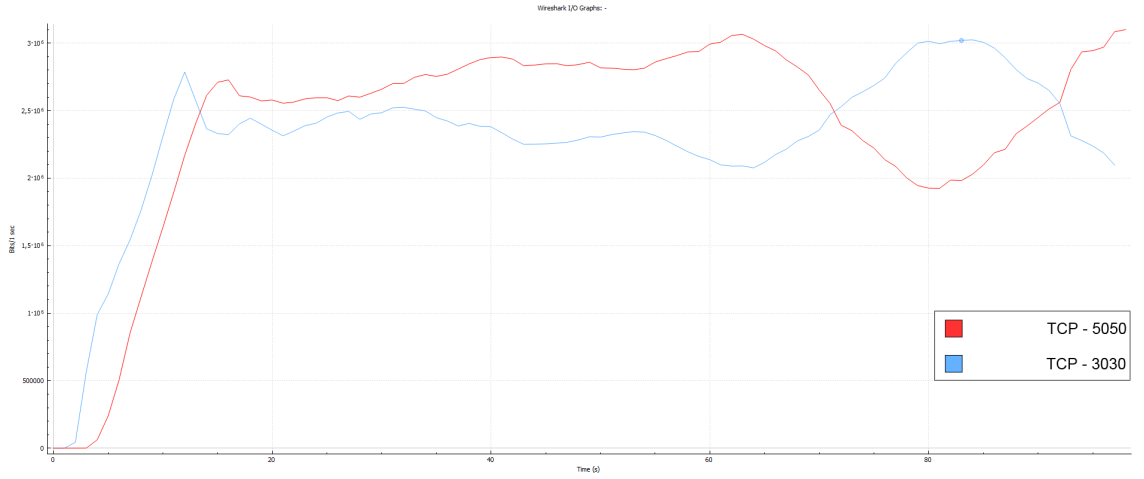


Figura 5.19: Gráfico dos Fluxos TCP. Fonte: Autor

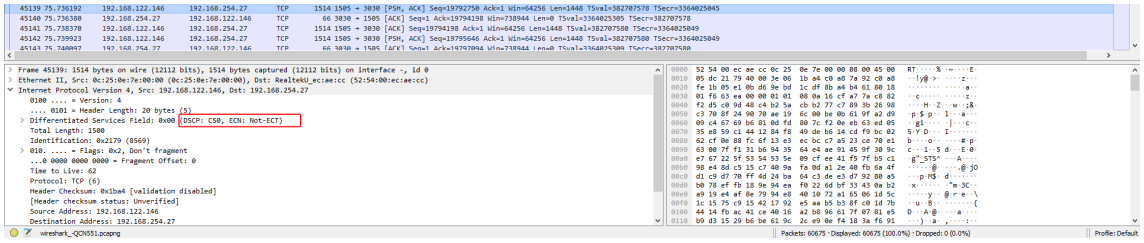


Figura 5.20: Cabeçalho de um pacote aleatório do Fluxo TCP 3030. Fonte: Autor

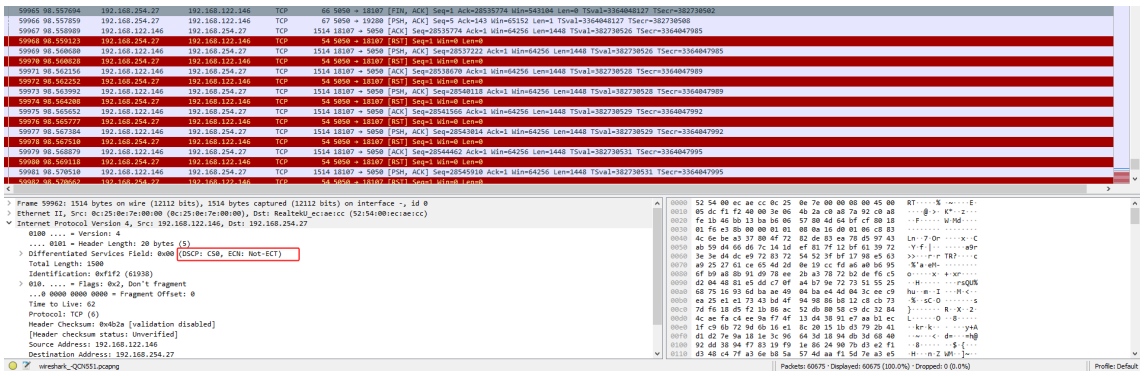


Figura 5.21: Cabeçalho de um pacote aleatório do Fluxo TCP 5050. Fonte: Autor

5.2.1.2 QoS Ativo

Para o próximo teste o QoS será aplicado em ambos os roteadores, para isso é necessário criar a politica de QoS dentro do Fleximanager e em seguida verificar o seu devido funcionamento.

Dentro da plataforma Flexiwan, existe a opção de identificação de aplicativos, na qual podemos selecionar o tipo de serviço, bem como os campos de identificação, como endereço IP, protocolo e porta. Após a criação do identificador de aplicativos, é possível aplicar políticas de segurança ou políticas de QoS a esses aplicativos. Para os testes futuros, optou-se por criar um "aplicativo"que opera na porta 3030 de qualquer endereço IP, conforme mostrado na Figura 5.22.

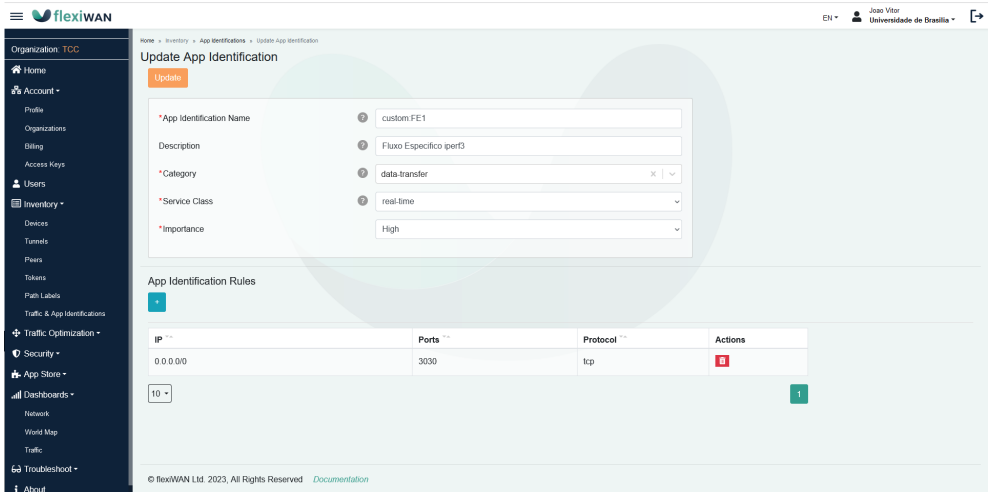


Figura 5.22: Identificação do Aplicativo (FlexiManager). Fonte: Autor

Na aba de QoS do fleximanager podemos configurar diversas politicas de QoS e aplicar essas diferentes politicas a diferentes roteadores, cada FlexiEdge pode rodar uma politica de QoS diferente. Sendo assim para essa parte dos testes escolhemos a que a politica será como mostrado na figura 5.23. Pode-se notar a escolha de separação da banda feita, alocou-se 70% para aplicações de "real-time", uma vez que o aplicativo criado recebe o valor de flag: *Service Class : real-time*. A escolha da porcentagem de banda pode levar em consideração vários fatores, como politicas corporativas, priorização de tráfego critico etc, nesse caso particular foram feitos testes e como podemos reparar, o tráfego TCP já faz um controle de con-

gestionamento que consegue, sem utilização de QoS, separar a banda total da rede de maneira eficiente, em torno de 50%/50% assim para melhor entendimento e visualização do QoS foi alocado uma banda de 70% para que fosse claro que o controle estivesse sendo feito pelo Flexiedge e não pelo TCP. Pode-se notar também a alocação do campo *DSCP : 4*, que irá guiar as capturas do Wireshark.

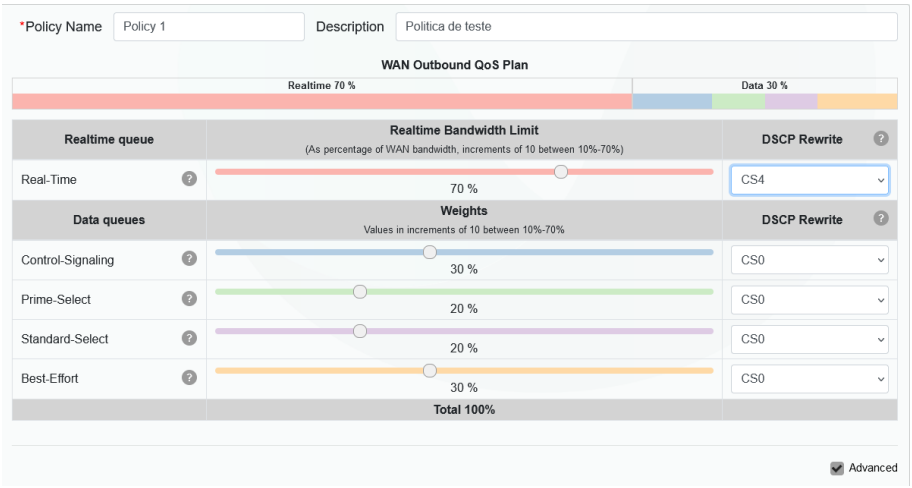


Figura 5.23: Parâmetros da Politica de QoS (FlexiManager). Fonte: Autor

Ambos os roteadores rodando as politicas de QoS, vamos repetir as análises feitas acima, duas conexões TCP, 3030 e 5050, entre FT-3 (Cliente) → ENG-3 (Servidor), a análise desse fluxo será feita com a saída do iperf3 e Wireshark.

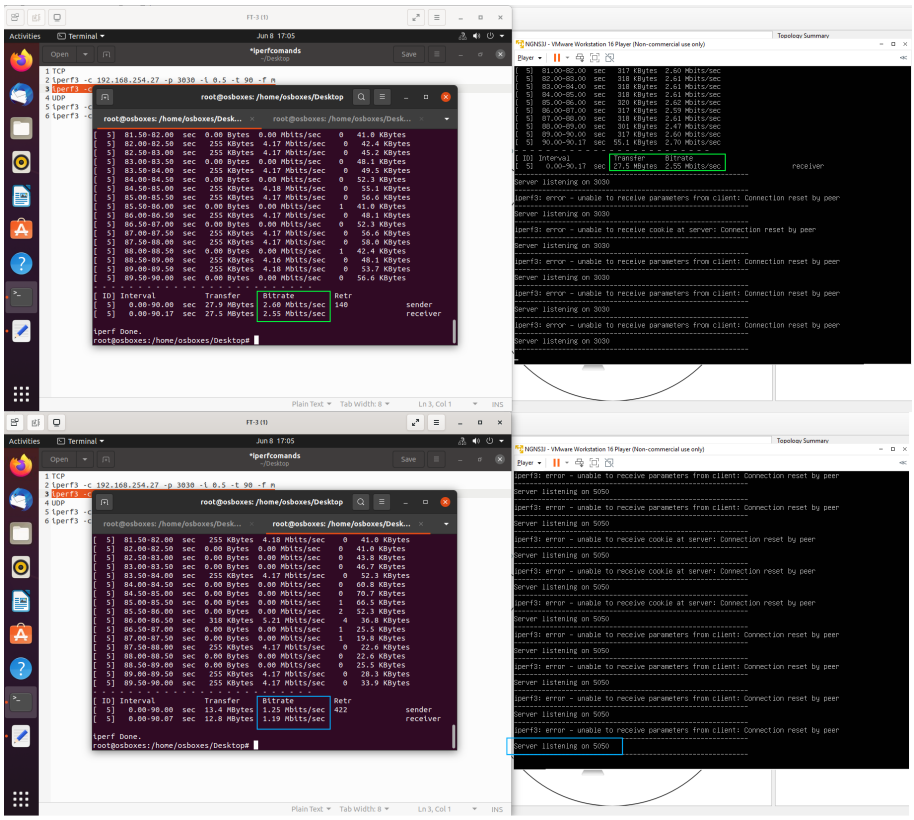


Figura 5.24: Saídas iperf3 (QoS Ativado). Fonte: Autor

Na figura acima é possível reparar na mensagem *"unable to recieve ..."* este erro está ligado a politica de fila, uma vez que o QoS aloca diferentes pacotes em diferentes filas tais pacotes ficam esperando para envio, contudo o nosso tempo de simulação esta restrito a 90 segundos, sendo assim quando a simulação acaba o iperf3 não recebe mais pacotes, entranto alguns pacotes que estavam dentro da fila restritos serão enviados.

A seguir estão os dados do wireshark, que serão utilizados para deixar mais claro alguns detalhes dos fluxos, além de servir como reforço complementar à saída do iperf3.

Comecemos com o gráfico de I/O do wireshark, disposto na figura 5.25 nota-se que a implementação da politica está sendo feita, uma vez que o o segmento Vermelho representa o fluxo de dados para a porta 5050 do TCP, nota-se um claro controle comparado com a figura 5.19.

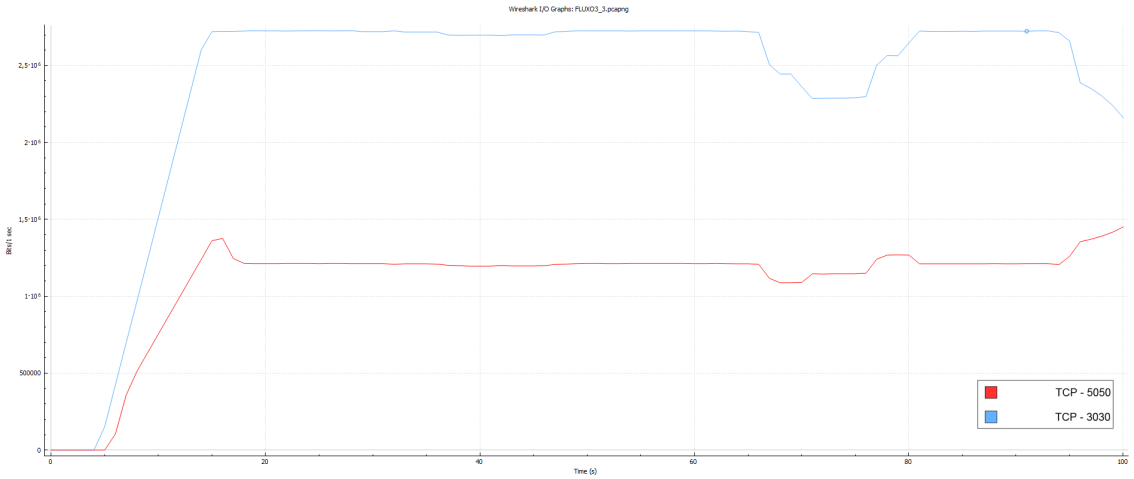


Figura 5.25: Gráfico dos Fluxos TCP gerados no Wireshark, (QoS Ativo). Fonte: Autor

A seguir, na figura 5.26 temos as conversas TCPs, mostrando algumas informações uteis, como por exemplo a taxa da conversa entre o cliente e servidor, pode-se observar que o fluxo para a porta 3030 teve uma taxa de $2,6Mbps$ enquanto a taxa do fluxo 5050 foi de $1,2Mbps$, dado nossa largura de banda disponível ser de $4Mbps$, podemos perceber que o QoS aplicado teve um alto índice de acerto, dado que 70% de $4Mbps$ é $2,8Mbps$ e os outros 30% são justamente $1.2Mbps$. Sendo assim para teste teve-se uma taxa de acerto de $92,86\%$ para o fluxo 3030 e 100% para o 5050.

IPv4 · 6 | TCP · 5 | UDP · 8

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.122.146	60746	192.168.254.27	3030	30.740	29,472 MiB	2	19.929	28,769 MiB	10.811	719,908 KiB	9.438688	90.3716	2670 kbps	65 kbps
192.168.122.146	49812	192.168.254.27	5050	14.988	13,792 MiB	4	9.281	13,396 MiB	5.707	405,311 KiB	10.381529	90.1650	1246 kbps	36 kbps
104.21.67.29	443	192.168.122.146	57504	80	15,260 KiB	0	40	4,226 KiB	40	11,034 KiB	0.349182	120.4967	287 bits/s	750 bits/s
192.168.122.146	49810	192.168.254.27	5050	33	2,869 KiB	3	18	1,597 KiB	15	1,272 KiB	10.238432	90.4182	144 bits/s	115 bits/s
192.168.122.146	60744	192.168.254.27	3030	33	2,867 KiB	1	18	1,597 KiB	15	1,271 KiB	9.337704	90.6641	144 bits/s	114 bits/s

Figura 5.26: Estatísticas do Wireshark sobre os Fluxos para as portas TCP 3030 e 5050 (QoS Ativo). Fonte: Autor

Por fim, um ponto "negativo"no processo de QoS, na figura 5.23 foi definido que a marcação de pacotes *"real-time"* tivesse sua flag com a bandeira **CS4**, contudo como mostram a figura 5.27 abaixo o mesmo foi marcado como **CS1**. Contudo a marcação do fluxo TCP 5050 está corrento com a marcação estipulada **CS0**, como mostra na figura 5.28.

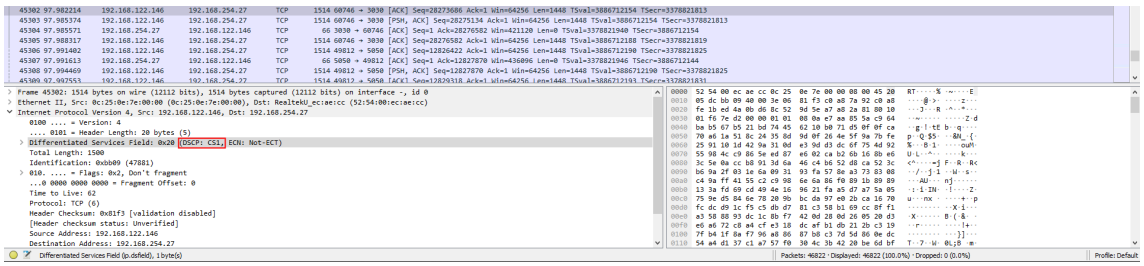


Figura 5.27: Cabeçalho de um pacote aleatório do Fluxo TCP 3030, com marcação errada. Fonte: Autor

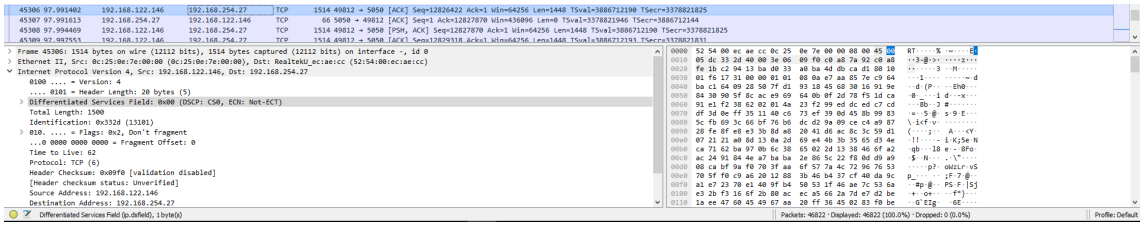


Figura 5.28: Cabeçalho de um pacote aleatório do Fluxo TCP 5050, com marcação certa. Fonte: Autor

Dadas tais análises, pode-se concluir que a politica de QoS foi devidamente aplicada, trazendo resultados satisfatórios, a parte no que diz respeito a marcação do campo DSCP pode influenciar caso hajam mais roteadores envolvidos no processo ou até mesmo na LAN, como não foi em nosso caso será feita uma sugestão de adaptação para a Fleiwan.

5.2.2 Segurança

Nesta parte a análise será focada em quesitos de segurança fornecidos pela Flexiwan. Como citado no tópico de QoS, a identificação de aplicativos é de suma importância pois é possível a aplicação de politicas para esses aplicativos. Dentro do FlexiManager pode-se aplicar as politicas de segurança para esses aplicativos e além disso criar politicas para outros fluxos de dados específicos.

Para esta análise vamos testar o bloqueio da pagina web **www.facebook.com** e além disso o bloqueio de pings entre as LAN's **ADM** e **FT**.

Dentro do catalogo existente de aplicativos da Flexiwan já existe o facebook cadastrado, como mostrado a seguir:

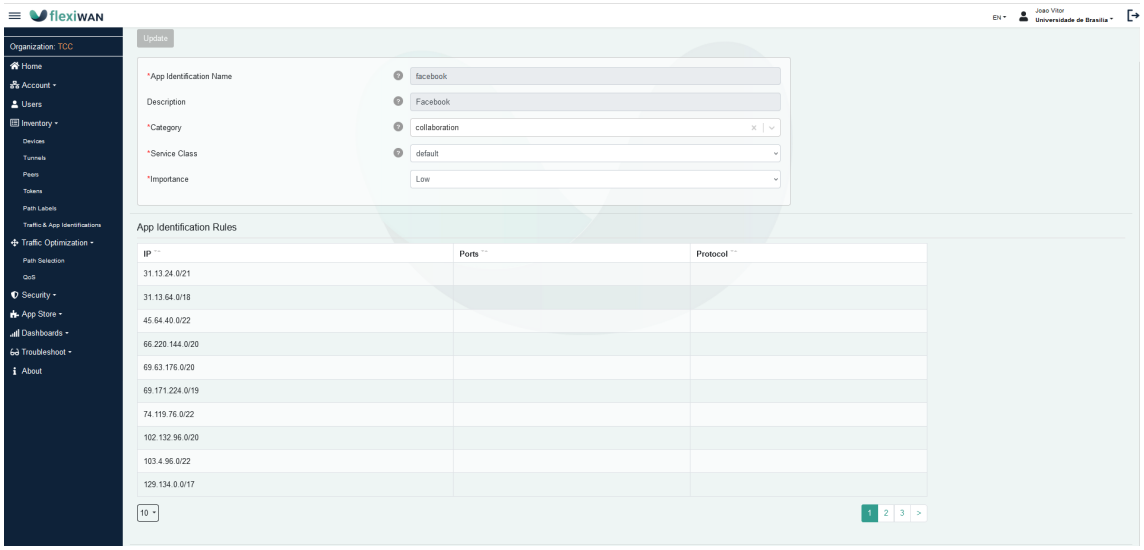


Figura 5.29: *App Identification Facebook*. Fonte: Autor

A seguir, deve-se ser criada uma regra de firewall para bloquear pings entre as LAN's **ADM** e **FT**. A regra foi criada de acordo com a figura abaixo:

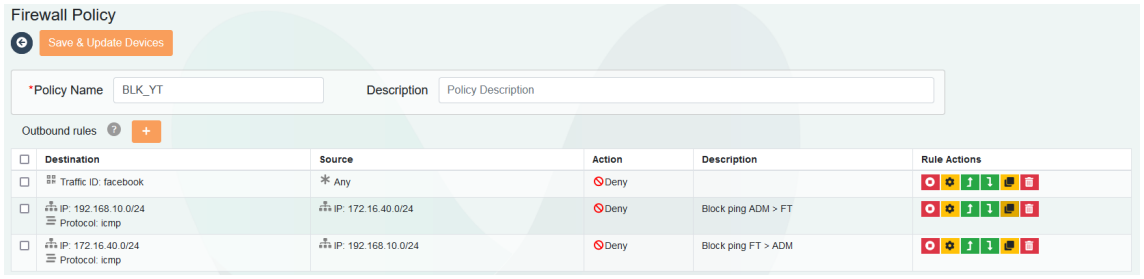


Figura 5.30: *Regras de Firewall. Fonte: Autor*

Após a devida criação da regras é necessário sincronizar os roteadores e em seguida testa-las, assim o primeiro teste vamos testar a regra de PING, que poderia ser facilmente trocada por uma regra de acesso externo, a seguir na figura 5.31.

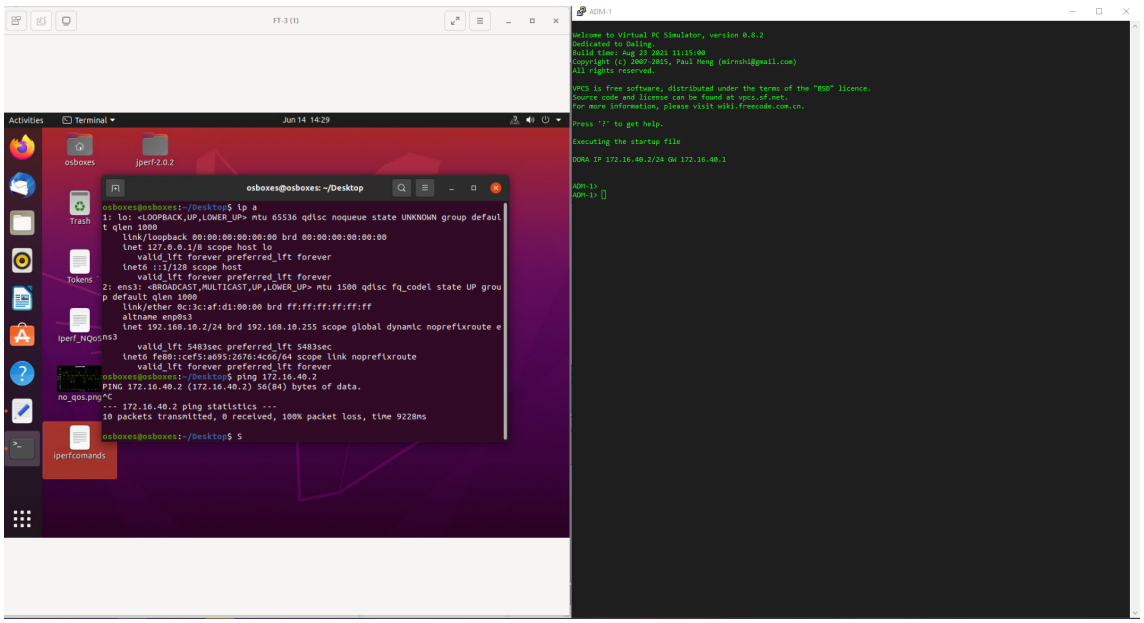


Figura 5.31: Ping entre as redes FT → ADM Fonte: Autor

A seguir, foi iniciada uma captura nos links entre **SWCORE** → **rDarcy** (lado direito) e entre **rFGA** → **SWCORE-FGA** (lado esquerdo), onde além do print acima onde temos que **10** pacotes foram transmitidos e nenhum recebido, podemos ver de maneira mais clara na figura 5.3 as solicitações ICMP saindo do SWCORE para o roteador de borda, contudo nenhuma solicitação passa pelo link que ligado o roteador de borda da FGA a LAN ADM.

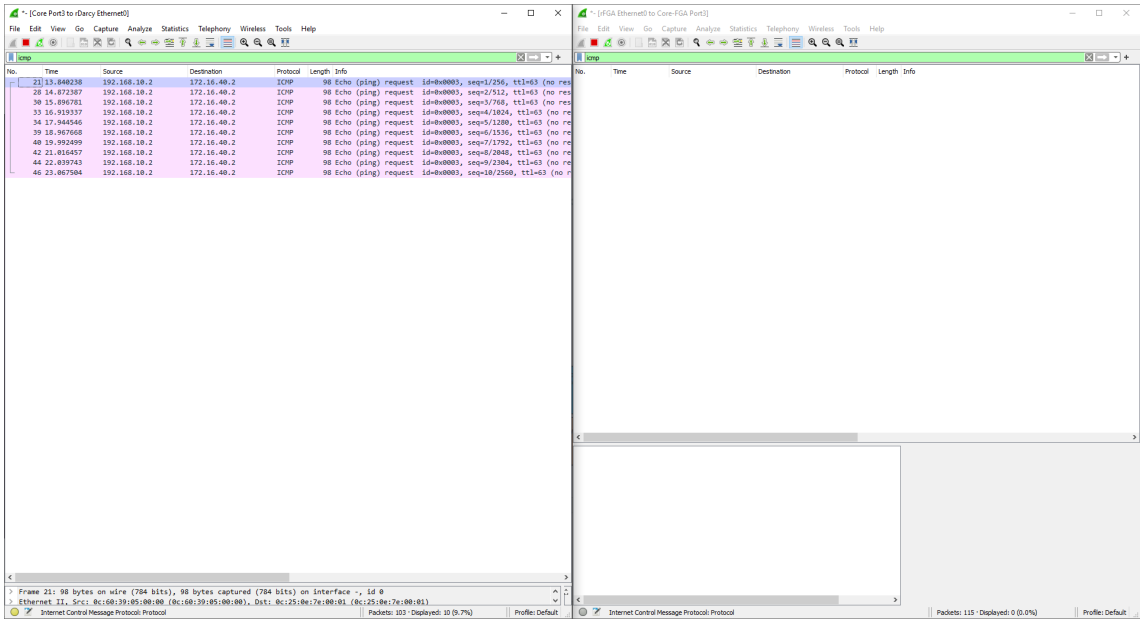


Figura 5.32: Ping entre as redes FT → ADM, Wireshark. Fonte: Autor

Como a comunicação ICMP foi bloqueada em ambos os lados da conversa, seguem pirnts do outro lado do bloqueio:

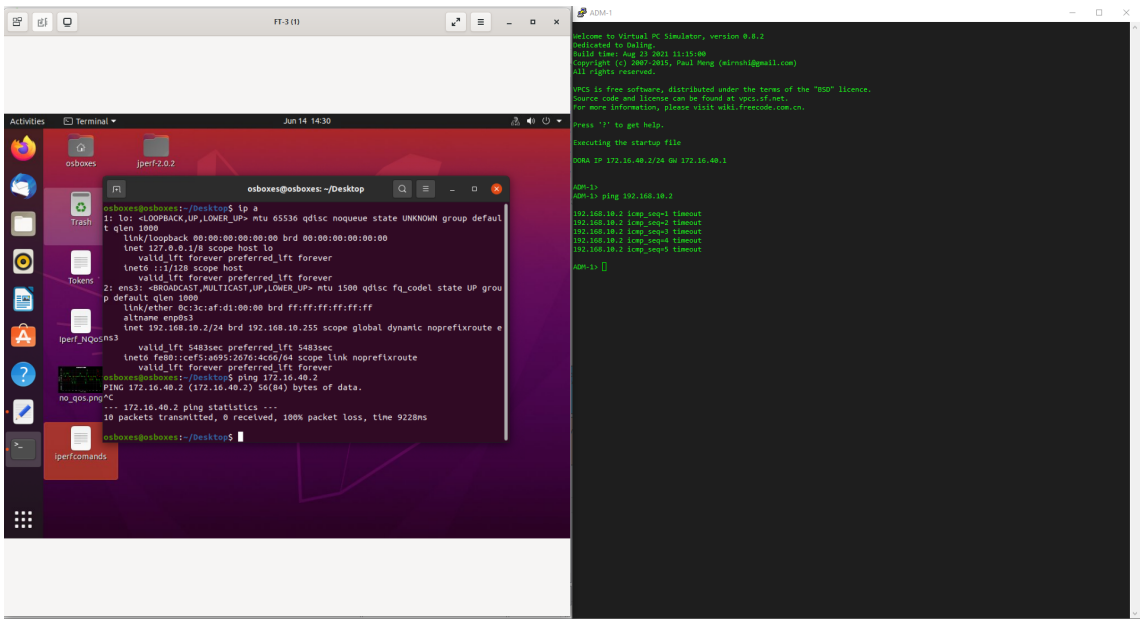


Figura 5.33: Ping entre as redes ADM → FT Fonte: Autor

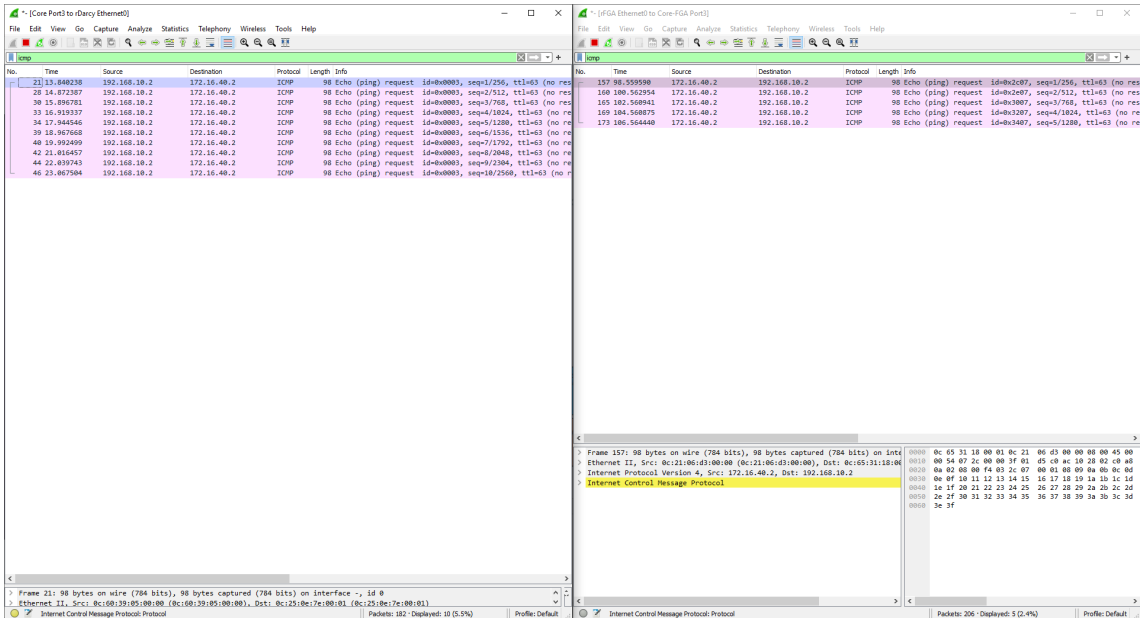


Figura 5.34: Ping entre as redes ADM → FT, Wireshark. Fonte: Autor

Como mostrados nas figuras acima, o mesmo processo ocorre, contudo podemos ver as requisições ICMP sendo enviadas e nao sendo recebidas, mostrando assim o seu devido bloqueio. Nota-se também que na figura 5.5 Podemos observar os 10 pacotes enviados na tentativa descrita anteriormente.

Por fim o bloqueio do facebook, vamos utilizar a rede FT e o computador FT-3 para tentar fazer o acesso. Os processo que envolvem a conexão entre o usuário final e o site propriamente dito consiste na coleta de um endereço através de uma requisição de DNS e em seguida a solicitação dos dados. Na figura 5.35 é possível notar que o computador solicita ao servidor DNS 8.8.8.8 o endereço da aplicação.

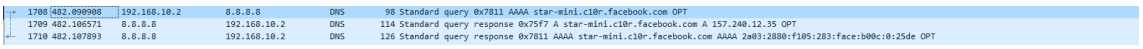


Figura 5.35: Solicitação do Endereço do site www.facebook.com, Wireshark. Fonte: Autor

Após isso é feita uma tentativa de conexão na porta 80 do **TCP** (figura 5.36 contudo a mesma diversas falhas mostrando que o endereço fornecido pelo DNS não é alcançável e de fato, ele se encontra bloqueado uma vez que o endereço fornecido esta no conjunto de endereços no identificador de aplicativo fornecido, como mostrado na figura 5.37.

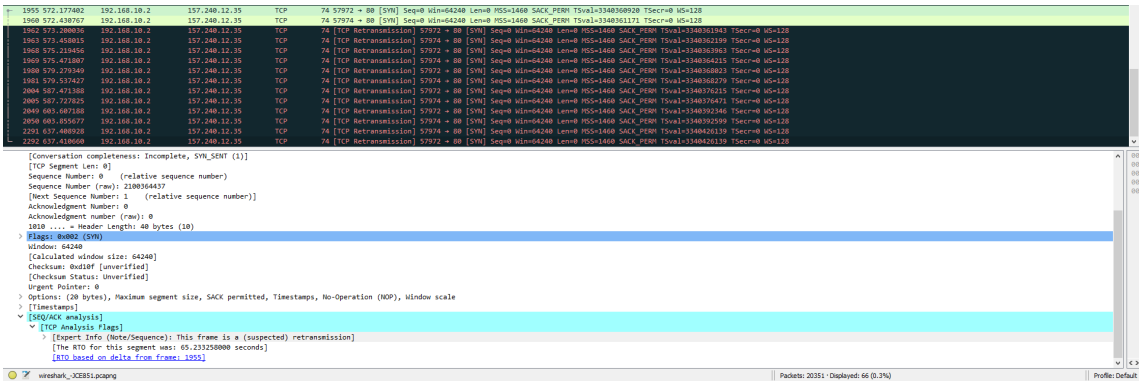


Figura 5.36: Retransmissões TCP, Wireshark. Fonte: Autor

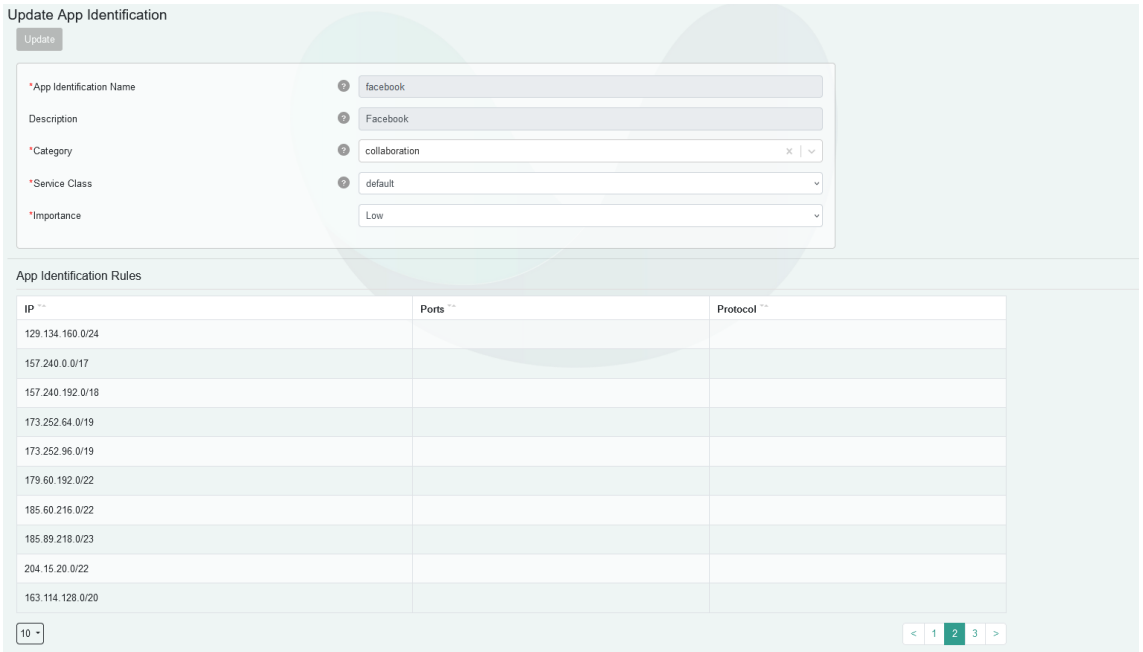


Figura 5.37: Endereço fornecido pelo DNS na lista de identificação. Fonte: Autor

5.2.3 Delay dos Túneis

É de suma importância que a conexões entre as LANs sejam completamente estabelecidas e tenham um desempenho apropriado, diversas topologias podem ser aplicadas mudando a maneira como o fluxo de dados trafego pela rede e pelo túneis, dado isso é muito importante que além de segurança o tunelamento

tenha um desempenho e rapidez necessários. Nesta parte serão medidos os tempos de resposta entre uma rede e outra através dos túneis criados na Flexiwan.

Para isso serão utilizados os computadores **FT-3** e **ENG-2**, para a realização dos testes vamos utilizar o comando *'traceroute'*. Esse comando pode ser modificado de maneira que possamos passar alguns parametros como por exemplo numero de solicitações ou pacotes, em nosso caso foram utilizados 4 pacotes, como mostra na figura 5.38.

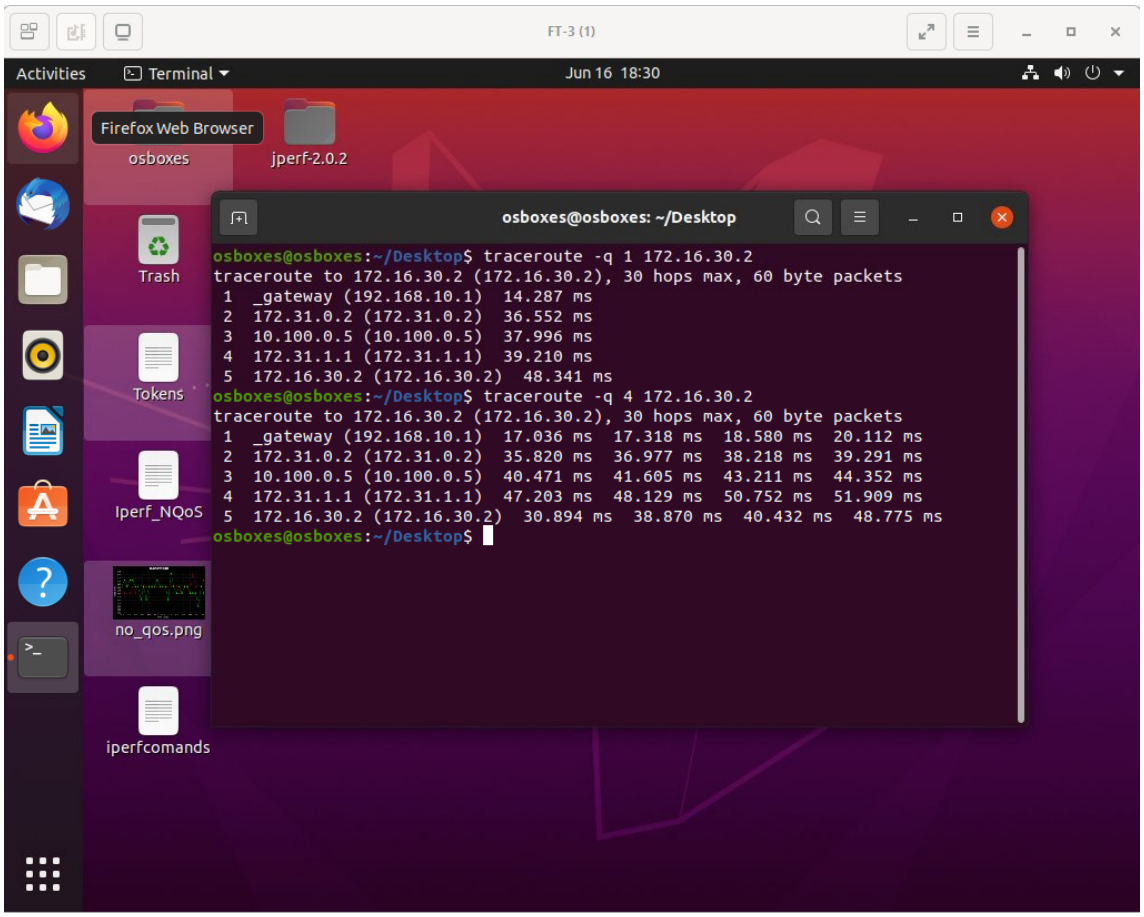


Figura 5.38: Rota entre FT-3 e ENG-2. Fonte: Autor

Assim, conhecendo a rota, podemos pingar todas as interfaces descritas para obter um resultado mais fiel, foi realizado um comando que envia 10 solicitações de ping e na tabela 5.1 podemos ver as médias para os destinos

Tabela 5.1: Delay Médio dos Pings

Destino	Média
192.168.10.1	**7,678 ms**
172.31.0.2	**10,437 ms**
10.100.0.5	**11,231 ms**
172.31.1.1	**13,609 ms**
172.16.30.2	**23,747 ms**

Nosso foco está nos endereços **172.31.0.2**, **10.100.0.5** e **172.31.1.1**. O tempo necessário do pacote

sair do PC FT-3 e chegar até a interface do roteador é de $10,437ms$. Contudo temos que dentro de nossa rota observa-se que o FlexiEdge, encaminha o pacote a interface de loopback 10.100.0.5 que pertence ao roteador **rFGA**, vale notar que a partir desse ponto o pacote já está rodando com o protocolo VXLAN sobre ESP, como mostrado em 5.15, ou seja, o tempo que nos interessa no processo é o processo de criptografia do túnel. Sendo assim entre os tempos de 172.31.0.2 para 10.100.0.5 onde é feito o encapsulamento e envio e o tempos entre 10.100.0.5 e 172.31.1.1 onde são realizados a descritografia e envio para a interface do roteador. Fazendo as contas temos que o processo de encapsulamento e envio do pacotes pelo túnel é de: $0,794ms$ e de desencapsulamento é de $2,378ms$ dando um total de $3.172ms$ para o encapsulamento, envio e desencapsulamento dos pacotes.

5.2.4 Seleção de Caminho Dinâmico

Para esta parte da análise serão necessárias algumas mudanças na topologia, a adição de mais duas saídas para a internet, em ambos os roteadores. Assim nossa topologia ficara com a seguinte forma:

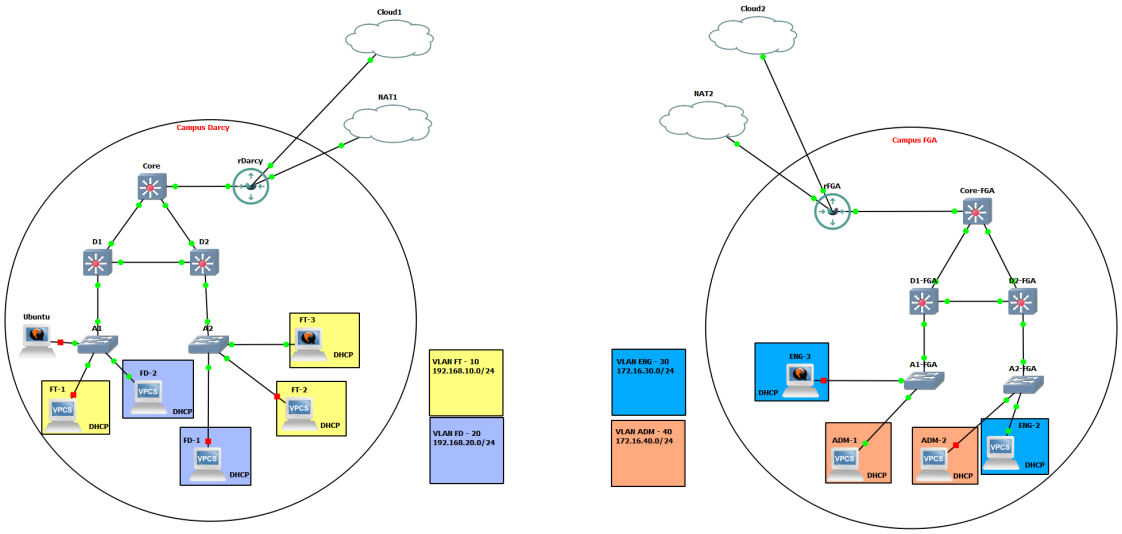


Figura 5.39: Nova Topologia. Fonte: Autor

Adicionando novos links de acesso conectados, temos mais de um caminho, podemos usar isso para que diferentes tráfegos possam seguir por diferentes caminhos,esse será o objetivo da análise. Um dos pontos chaves de uma SDWAN é a flexibilidade de integração de diferentes links de internet por diferentes tecnologias, como MPLS, 4G/5G etc. Neste caso existirão dois cenários, contudo antes da criação desses cenários é importante que sejam aplicadas mais configurações.

A primeira é a criação de outro *"Path Label"* e a configuração do segundo link WAN, que por fim irá originar outro Túnel IPSec. Como mostrado respectivamente nas figuras abaixo:

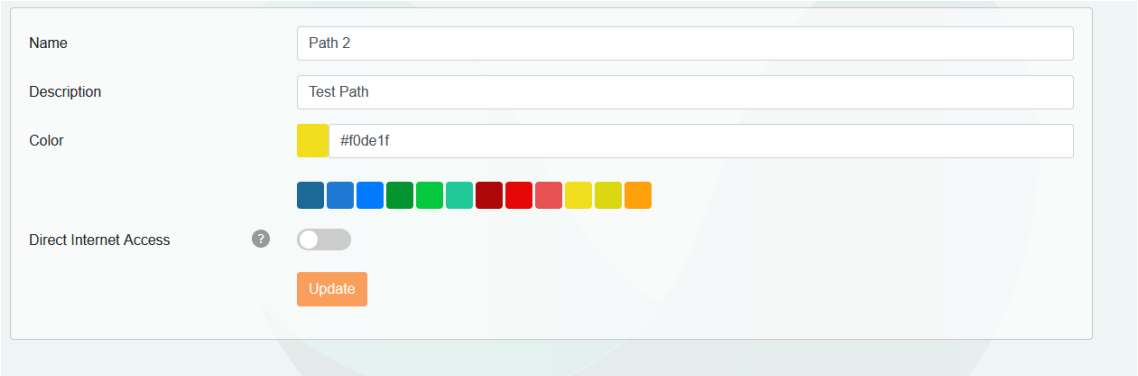


Figura 5.40: Novo Caminho Criado. Fonte: Autor

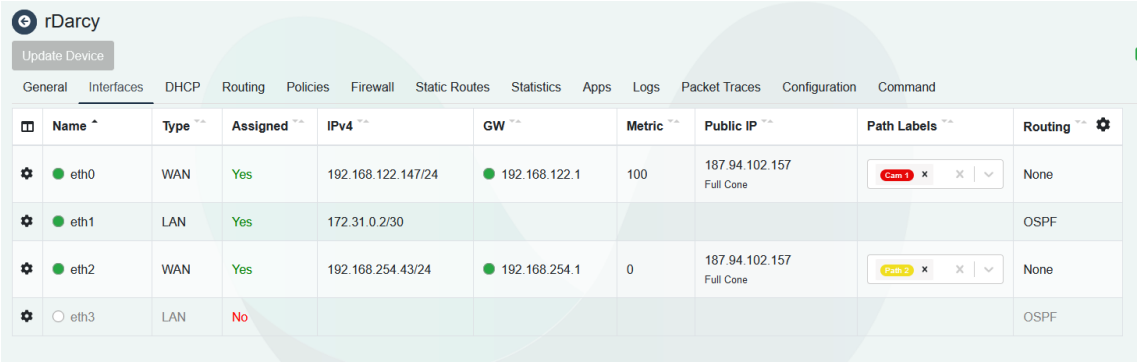


Figura 5.41: 2º Link WAN em rDarcy. Fonte: Autor

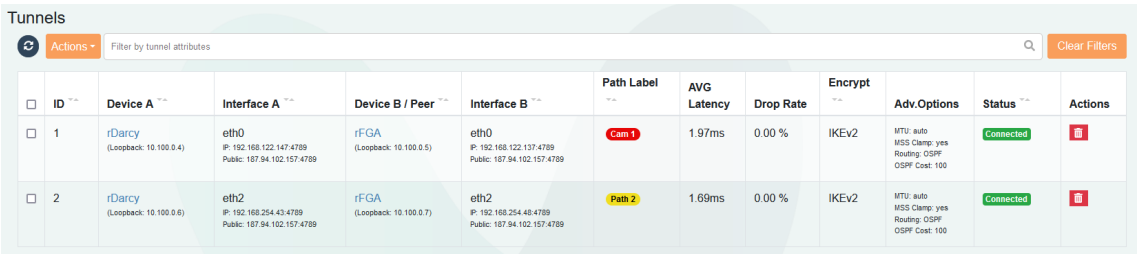


Figura 5.42: Novo Túnel. Fonte: Autor

5.2.4.1 Primeiro Cenário

Neste Primeiro cenário foram definidas duas regras principais, a primeira, chamada *ADM* diz respeito ao trafego que flui para a rede **172.16.40.0/24** e regra utiliza o caminho *Path 2*, ou seja, o caminho recém criado, como mostrado na figura abaixo (importante ressaltar que em 5.2.2 há uma regra de bloqueio de tráfego, a mesma foi desabilitada):

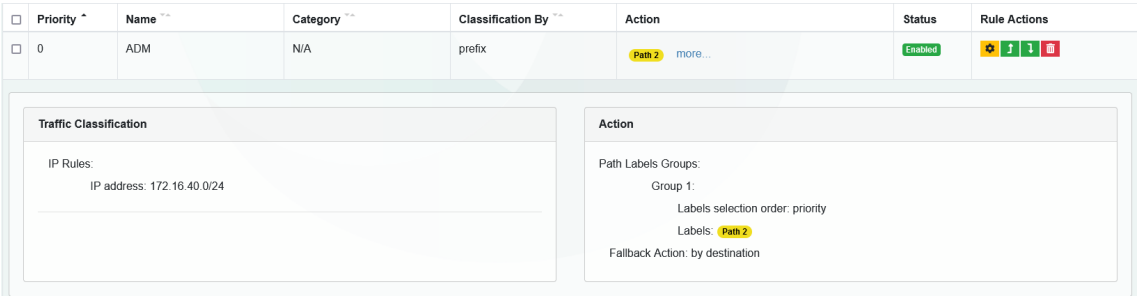


Figura 5.43: 1ª Regra do Path Selection. Fonte: Autor

A segunda regra segue a mesma logica, com o nome *ENG* é definido que todo o tráfego que for for para a **172.16.30.0/24** será redirecionado pelo caminho *"Cam 1"*.

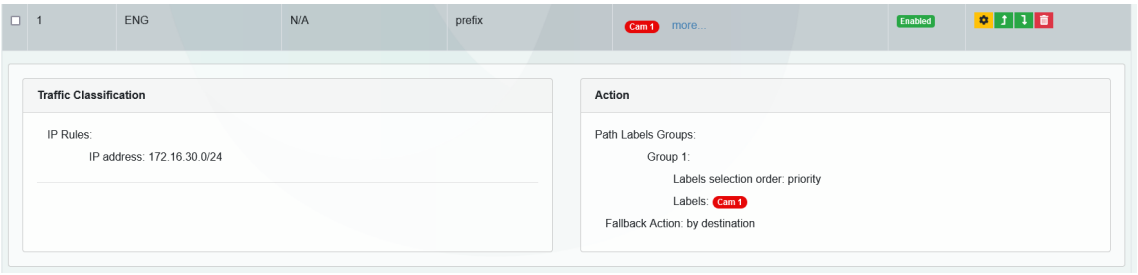


Figura 5.44: 2ª Regra do Path Selection. Fonte: Autor

Com isso pode-se iniciar nossos testes, para esta parte utilizaremos o comando *traceroute* nele conseguimos ver claramente por onde o pacote está seguindo, utilizaremos o device FT-3 como suporte, seguem resultados:

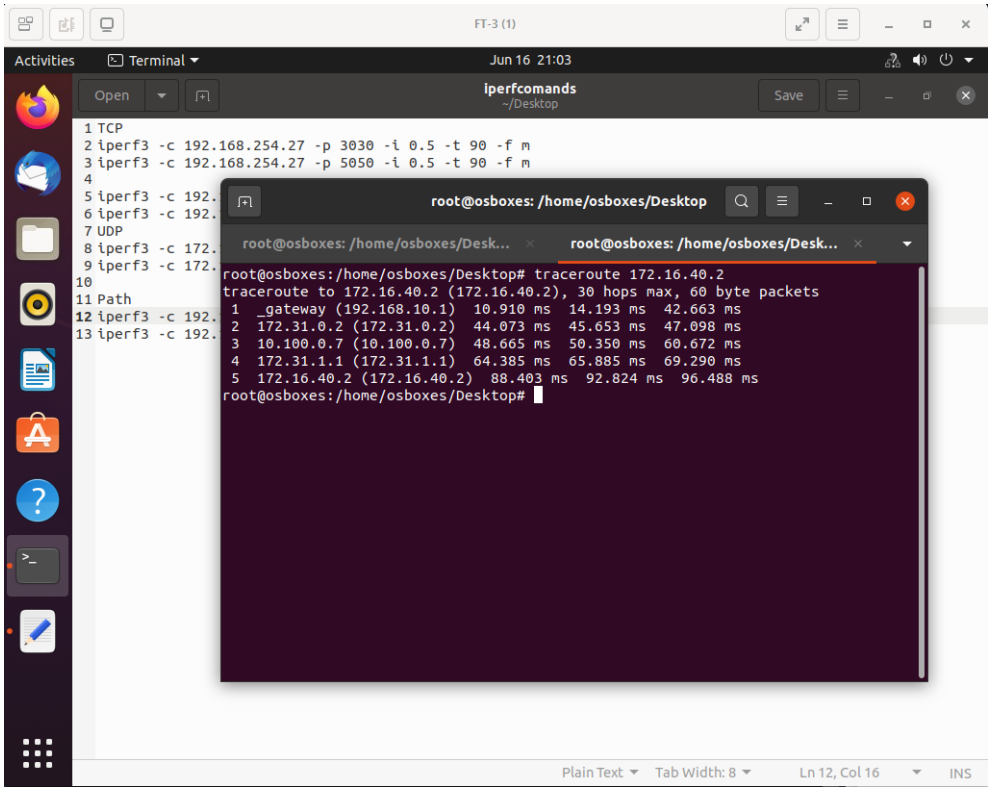


Figura 5.45: Traceroute para ADM. Fonte: Autor

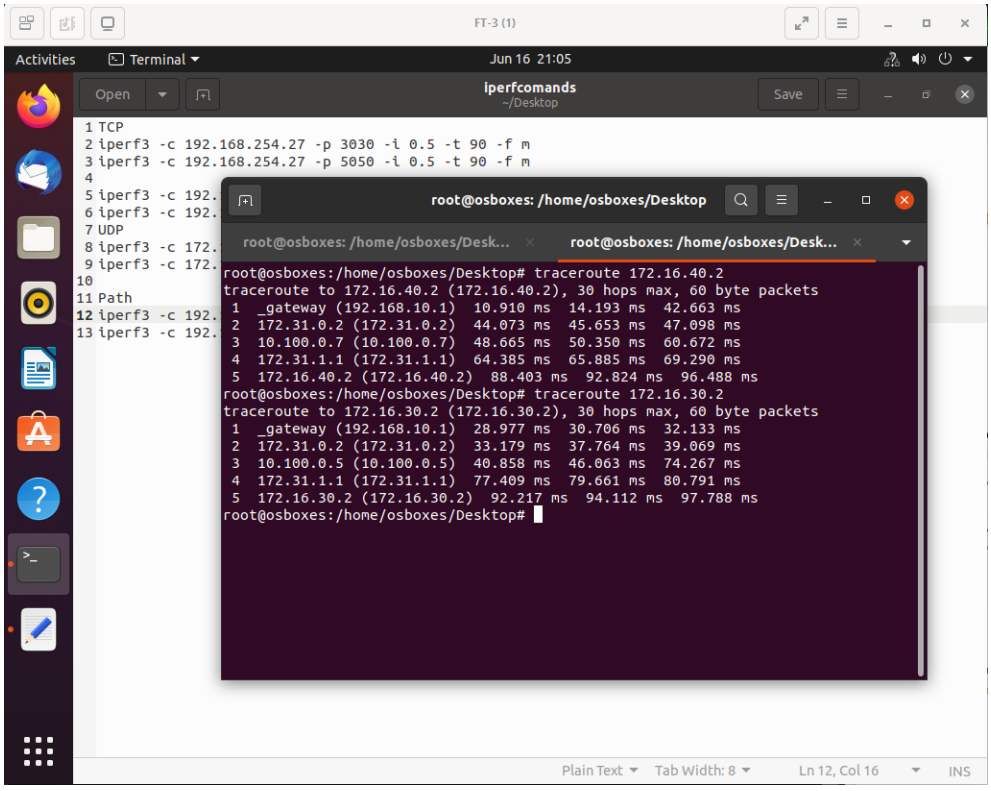


Figura 5.46: Traceroute para ENG. Fonte: Autor

Utilizando a figura 5.42, nota-se os endereços dos túneis e por fim as seguintes conclusões:

- Na figura 5.45, era esperado que todo trafego passasse pelo Túnel "Path 2", que tem endereços de loopback marcados como 10.100.0.6 e 10.100.0.7, o retorno do comando mostra claramente que o resultado obtido foi o esperado.
- Da mesma forma da análise acima, temos que o trafego destinado a rede **172.16.30.2** foi alocado no caminho escolhido em suas configuração, pelo *"Cam 1"* com endereço de loppkback 10.100.0.5.

5.2.4.2 Segundo Cenário

Para estes cenário os caminhos serão invertidos, assim os caminhos devem ser invertidos nas regras, como mostrado na figura 5.47.

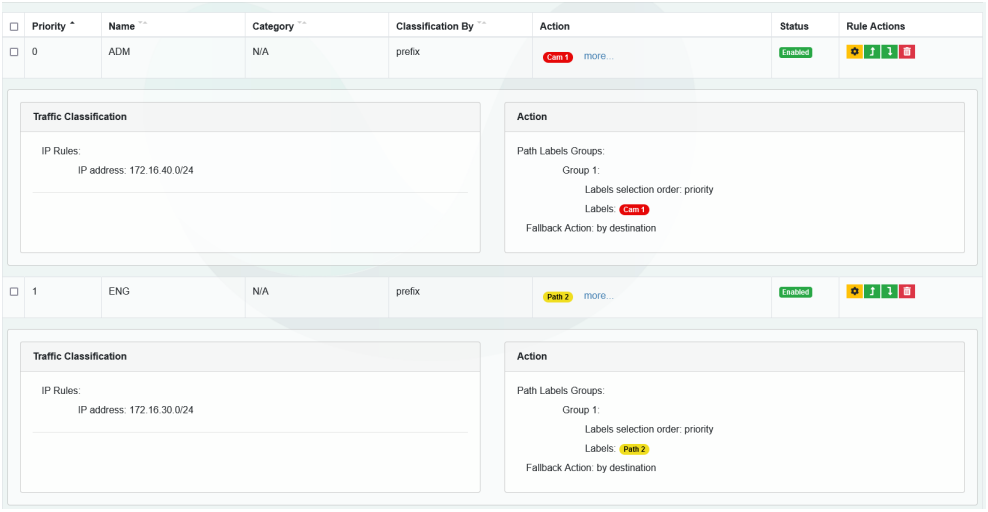


Figura 5.47: Regras invertidas para o cenário 2 do Path Selection. Fonte: Autor

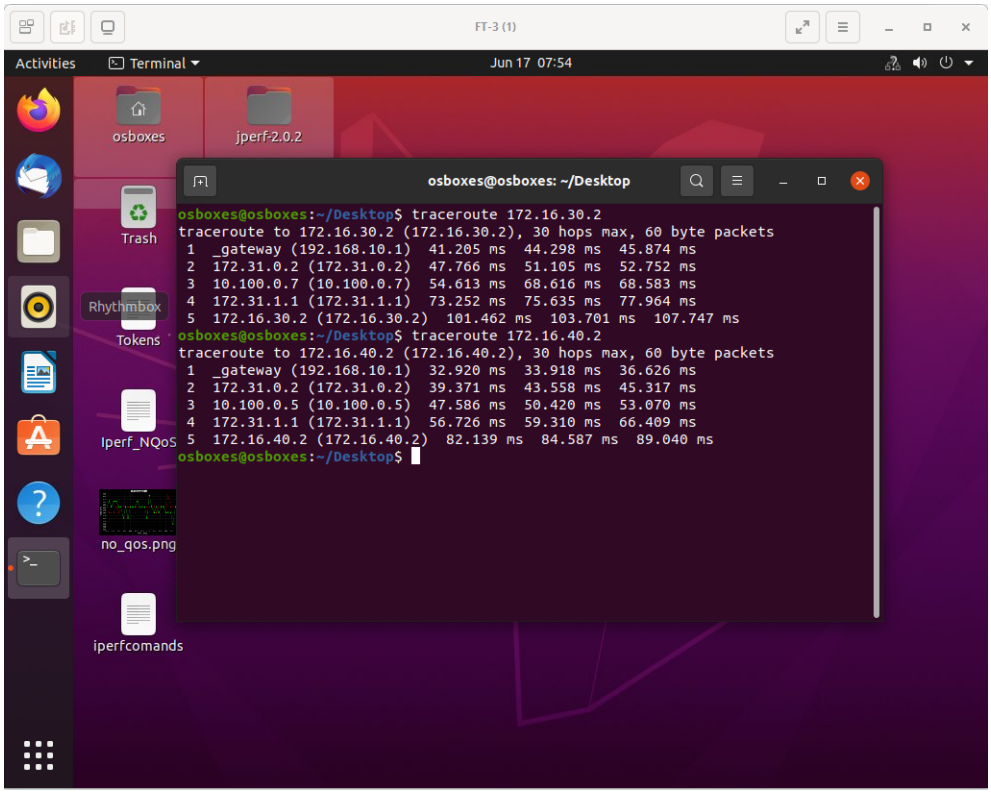


Figura 5.48: Traceroute para ADM com caminho invertido. Fonte: Autor

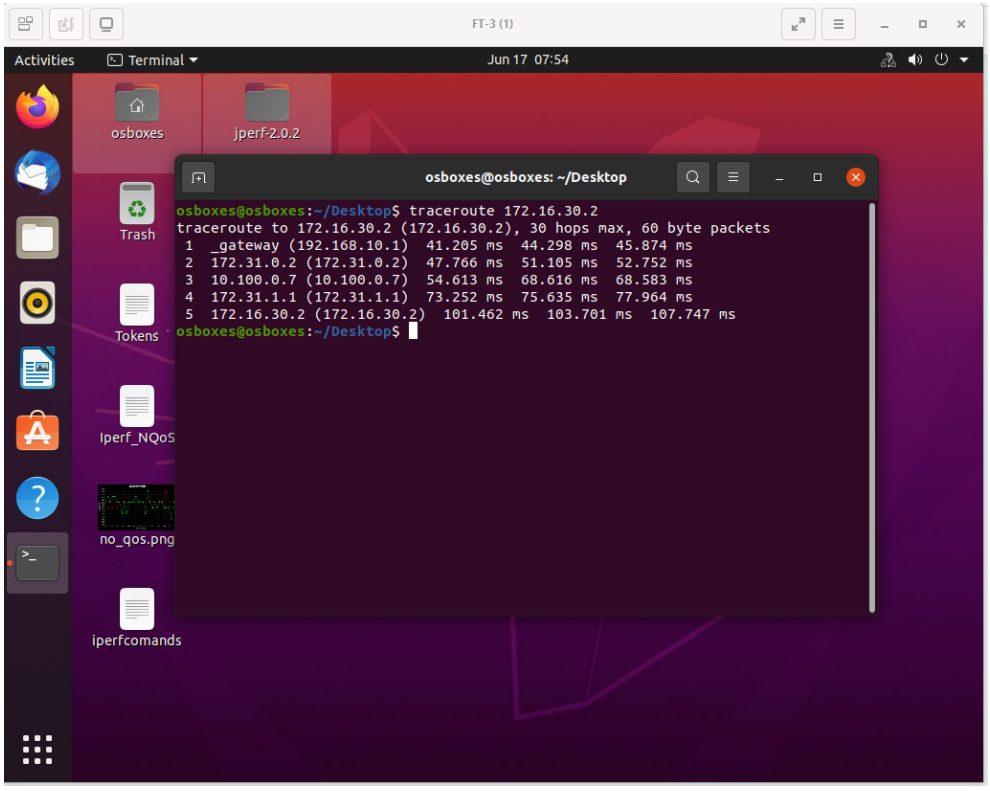


Figura 5.49: Traceroute para ENG com caminho invertido. Fonte: Autor

- Em 5.48 era esperado que todo trafego passasse pelo Túnel "Cam 1", uma vez que a regra foi inver-

tida, e de fato nota-se que o endereço 10.100.0.5 mostra que isso foi feito.

- Temos que o trafego destinado a rede **172.16.30.2** foi alocado no caminho escolhido em suas configuração, pelo *"Path 2"* com endereço de loppkback 10.100.0.7.

5.2.5 Análise Geral - Flexiwan

A partir dos resultados coletados nas sessões anteriores pode-se fazer uma análise geral das ferramentas que compõe a tecnologia SDWAN da Flexiwan. O primeiro ponto a se destacar é uma certa facilidade na implementação do recurso, apesar de ter sido implementada em ambiente virtualizado o que pode gerar alguns problemas externos ao software da fabricante, nota-se uma grande facilidade no cadastro e acesso.

O cadastro do Flexiedge é feito por um token, gerado dentro do Fleximanager, que é alocado no dispositivo na primeira integração, assim que cadastrado o código e o Flexiedge tem acesso a internet o mesmo se conecta automaticamente com o Fleximanager e é cadastrado dentro do inventario da conta que gerou o token, esse meio de integração dispositivo/orquestrador. Essa facilitação de acesso é abordada em 2.17, em **CPE**. Esse ponto é de suma importância dentro de uma solução SDWAN, pois como já abordado, leva uma facilitação na configuração do dispositivo.

O Flexiedge conta com distribuição de DHCP que pode ser configurada no FlexiManager, contudo a mesma não foi necessária. No que se refere ao QoS do dispositivo, consegui-se mostrar nesta sessão que a porcentagem de aproximou do previsto, e melhor ainda, na análise feita não foi considerado a taxa de ocupação dos outros fluxos que estavam acontecendo além dos dois fluxos TCP, ou seja, fluxos de controle como mensagens OSPF e a comunicação ativa do Flexiedge com o orquestrador que, por padrão, existem algumas regras de QoS que não podem ser excluídas, esse ponto foi observado nos teste de QoS feitos, proponho aqui uma revisão das politicas de aplicativos que por fim impactam no QoS que não podem ser excluídos ou desabilitadas, isso pode impactar em politicas mais criticas dentro de grandes corporações.

No que diz respeito as funcionalidades do dashboard a uma clara restrição no que se diz a análise de tráfego, como mostrado na figura 5.50, nota-se que pode-se se selecionar a interface contudo não é possível ter análises mais completas e densas, como por exemplo sobre aplicações, usuários, diapositivos e afins. Para fins de comparação a figura 5.51 exemplifica um dashborad mais completo da Cisco Meraki (de outra SDWAN), onde existem vários níveis de informação (nem todas as informações estão disponíveis dado a politicas internas da empresa que cedeu o acesso), além disso é possível escolher as datas das análises e afins.

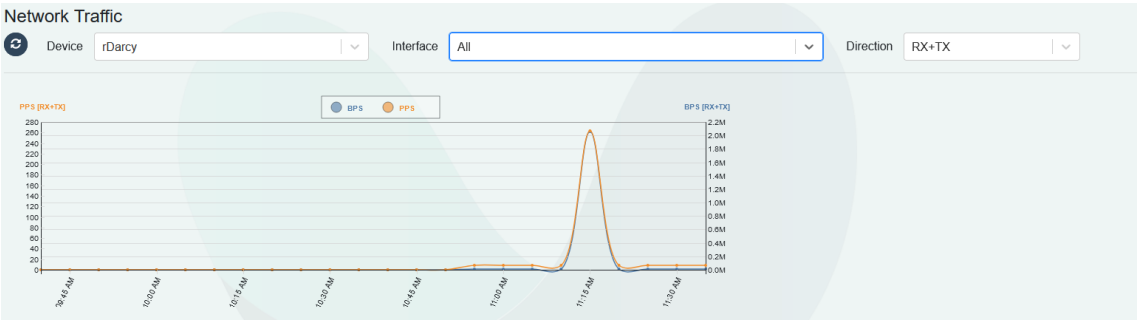


Figura 5.50: DashBoard de Rede, Flexiwan. Fonte: Autor

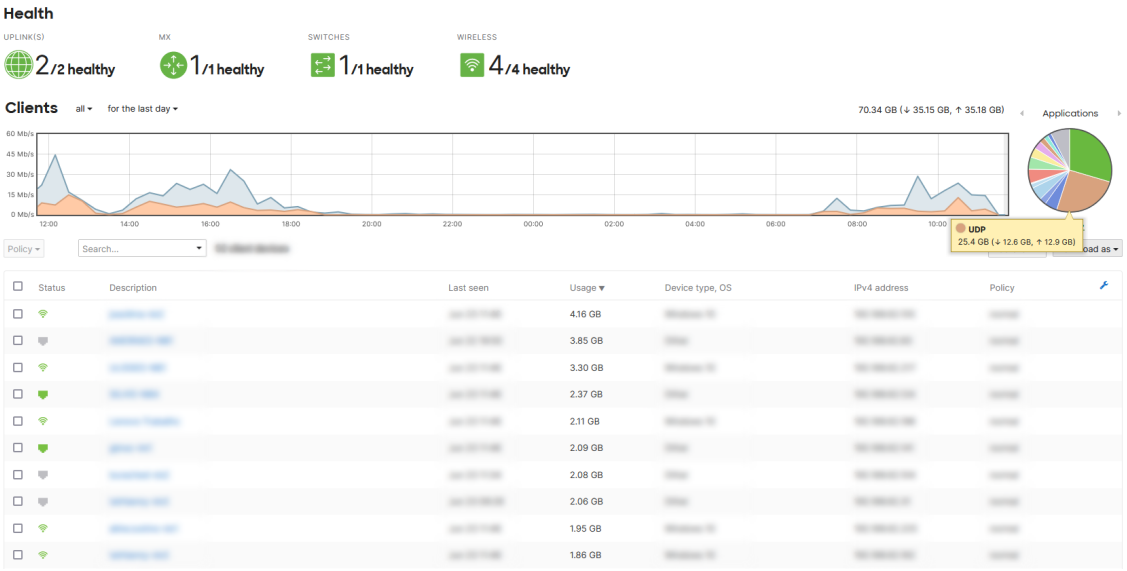


Figura 5.51: DashBoard de Rede, Meraki. Fonte: Autor

As funções de segurança providas pela SDWAN da Flexiwan conseguem ser bastante interessantes contudo ainda são de certa forma básicas, apenas aplicando ACLs de inbound e outbound, contudo a atualização dos dispositivos e a implementação tanto na ativação como desativação de novas regras é rápida o que garante a atualização dos dispositivos sem gerar impactos ao funcionamento da rede.

A seleção de caminho dinâmico se mostrou efetiva e funcional, além da análise do tunelamento trazer boas respostas no que se refere ao tempo de criptografia e descriptografia dos pacotes mostrando que os túneis são rápidos e seguros, componentes essenciais dependendo do acesso internet utilizado pelos clientes, neste caso a internet.

Existem muitas outras funcionalidades SDWAN dentro da solução da Flexiwan, o que a torna viável e implementável, a utilização de softwares open source não compromete a solução, pode-se também concluir que é possível implementar uma SDWAN completamente funciona e de alta qualidade apenas com códigos abertos. De maneira geral os resultados obtidos foram excelentes com apenas alguns pontos a se melhorar.

5.3 ANÁLISE FORTINET

5.3.1 Tunelamento e Conexões Essenciais

Dado que a realização da distribuição dos endereços DHCP já foi analisada em 5.1.1 e são utilizados os mesmos SWCORE em ambas as topologias esse teste será ignorado pois ja foi mostrado seu devido funcionamento, contudo a criação dos túneis e comunicação entre os sites muda dado a mudança de tecnologias, utilizando os novos dispositivos na rede serão realizados os testes de conectividade em uma mesma VLAN e em VLANs diferentes, em seguida os testes serão feitos com a conexão para internet seguindo do throughput disponível. Para mais robustez, escolheu-se o dispositivo **ENG-3**, a captura de pacotes foi realizada na saída do mesmo.

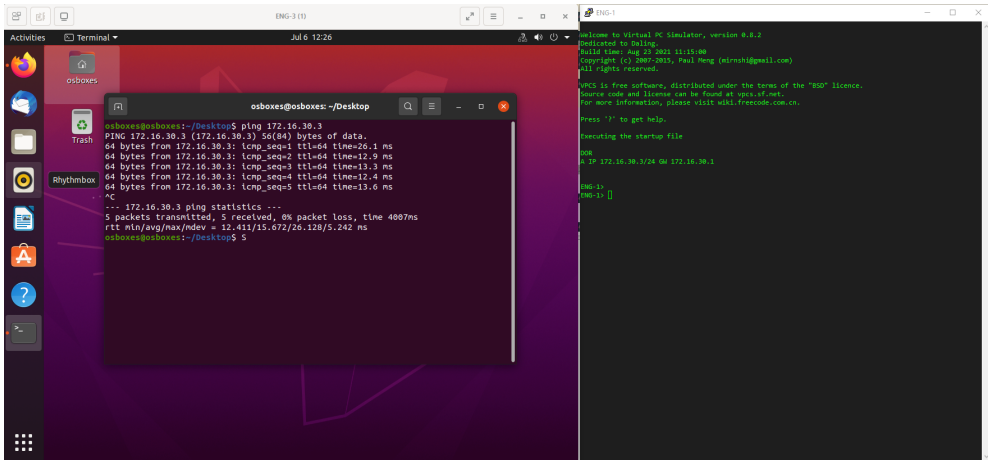


Figura 5.52: Ping Intra VLAN, ENG-3 → ENG-1. Fonte: Autor

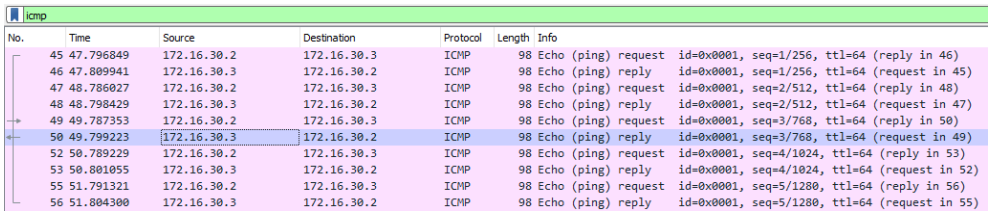


Figura 5.53: Ping Intra VLAN, ENG-3 → ENG-1 (WireShark). Fonte: Autor

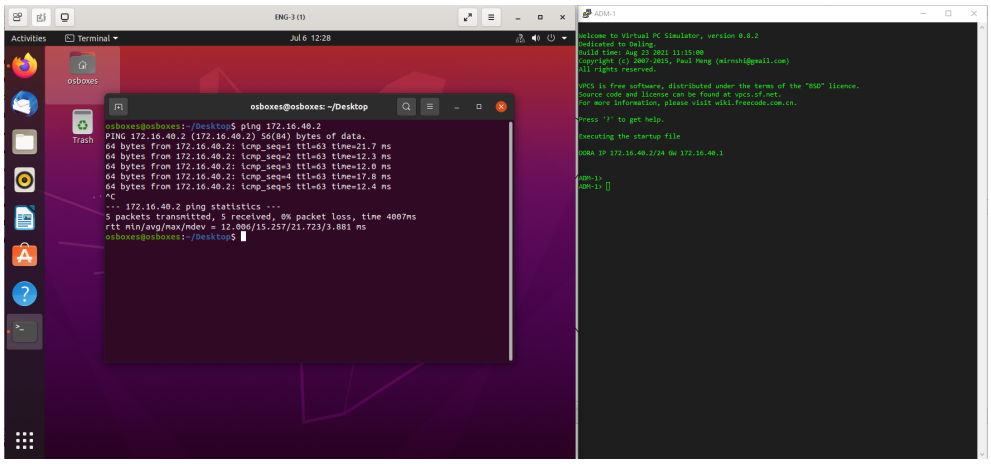


Figura 5.54: Ping Inter VLANs, ENG-3 → ADM-1. Fonte: Autor

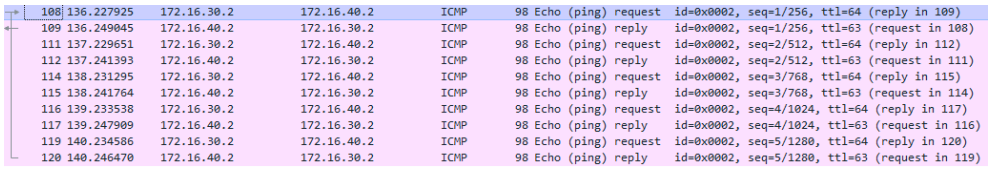


Figura 5.55: Ping Inter VLANs, ENG-3 → ADM-1 (Wireshark). Fonte: Autor

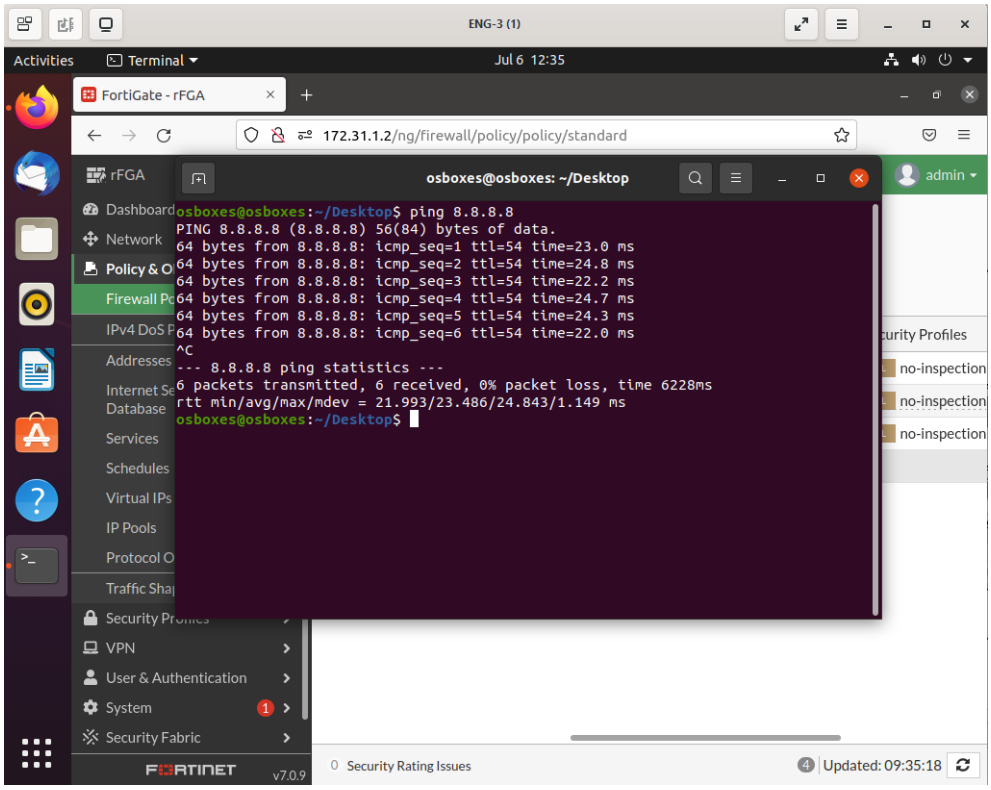


Figura 5.56: Ping externo, ENG-3 → 8.8.8.8 . Fonte: Autor

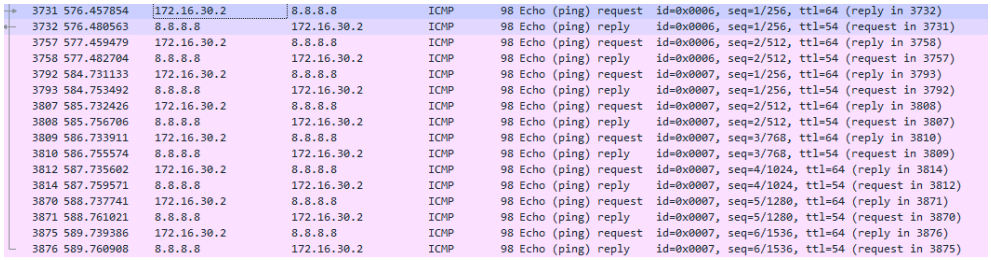


Figura 5.57: Ping externo ENG-3 → 8.8.8.8 (Wireshark). Fonte: Autor

As criações de túneis dentro da plataforma do Fortigate são mais complexas e dificultosas, contudo essa complexidade reflete na alta variedade de recursos e configurações, desde de a escolha do tipo de troca de chaves até algoritmos de criptografia e autenticação. Neste cenário optou-se por usar o algoritmo de troca de chaves IKEv2 e o algoritmo de autenticação o SHA-256, dado as suas altas taxas de segurança, assim ambos os túneis devem ser configurados com uma chave de acesso compartilhada, essa configuração é feita dentro de cada Fortigate separadamente, assim as configurações finais dos túneis em ambos os dispositivos estão dispostas abaixo na figura 5.58.

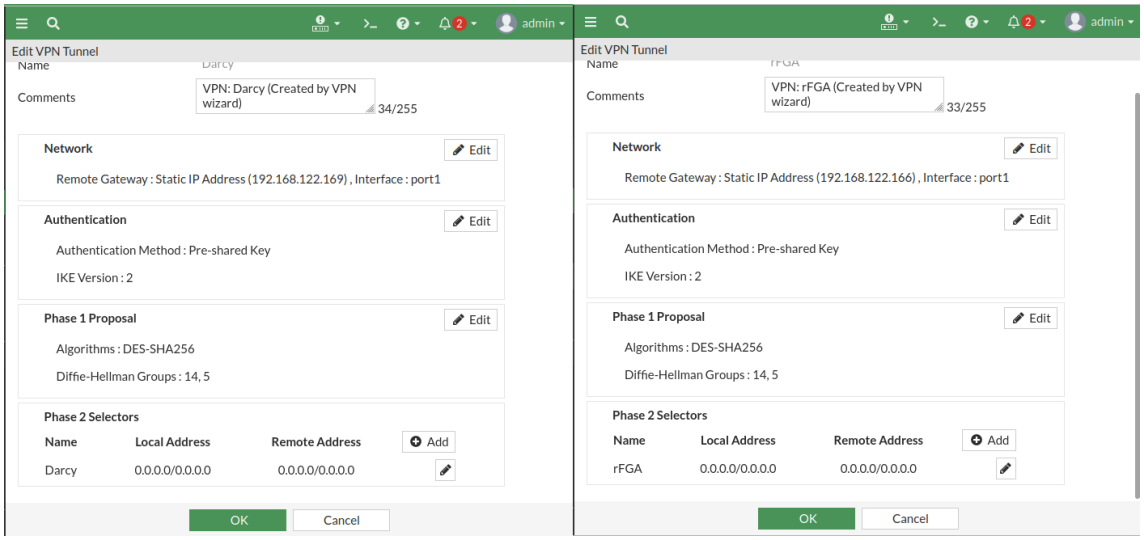


Figura 5.58: Configuração dos IPSec túneis em rDarcy e rFGA. Fonte: Autor

Para a comunicação entre LANs, ou entre sites foi realizado um ping entre as maquinas FT-3 e ENG-3, as capturas dos pacotes mostram que é utilizado o protocolo ESP, assim como na Flexiwan, contudo não são utilizadas VxLAN para o transporte dos mesmo.

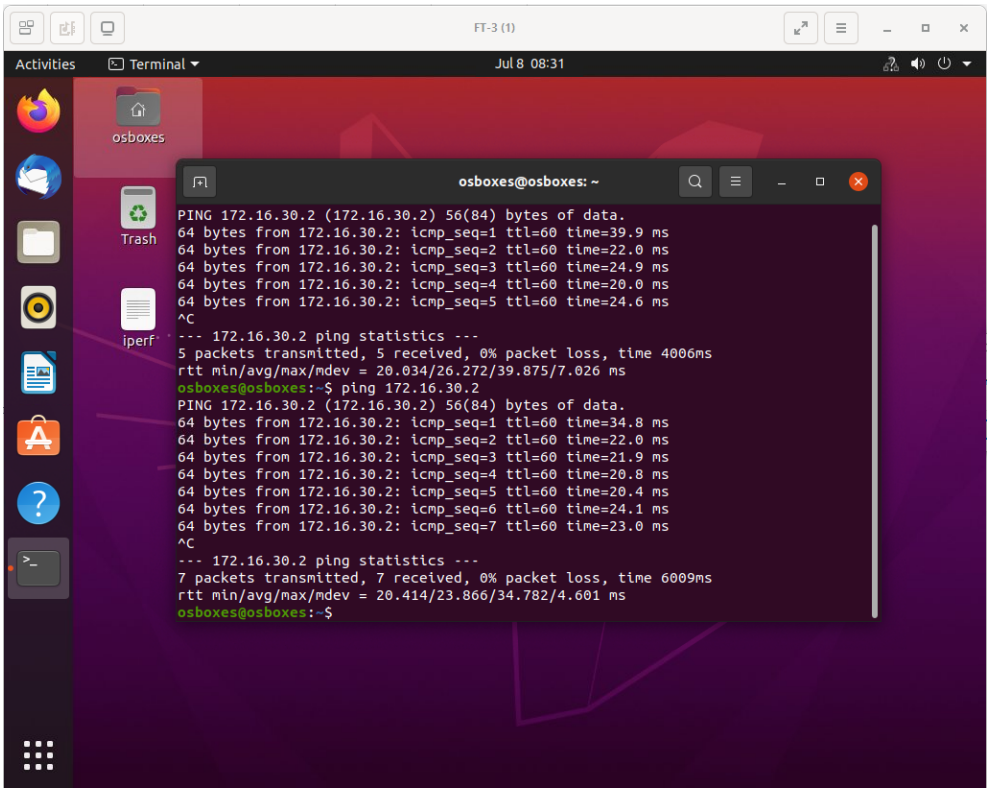


Figura 5.59: Ping entre FT-3 e ENG-3. Fonte: Autor

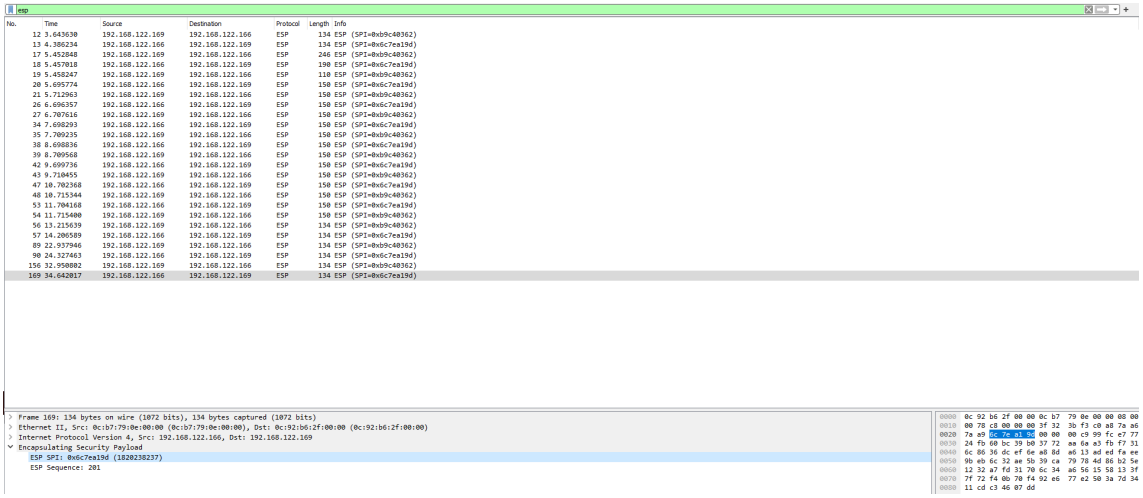


Figura 5.60: Ping entre FT-3 e ENG-3 (Wireshark). Fonte: Autor

Uma vez que a conexão entre os sites esta devidamente pode-se realizar o teste de largura de banda, teste essencial para utilização de recursos como QoS e seleção de caminho dinamico. Serão utilizados os mesmos comandos no teste da Flexiwan, utilizando os dispositivos FT-3 e ENG-3, como ENG-3 de servidor. A captura dos pacotes será feita na saída do roteador de borda, rFGA.

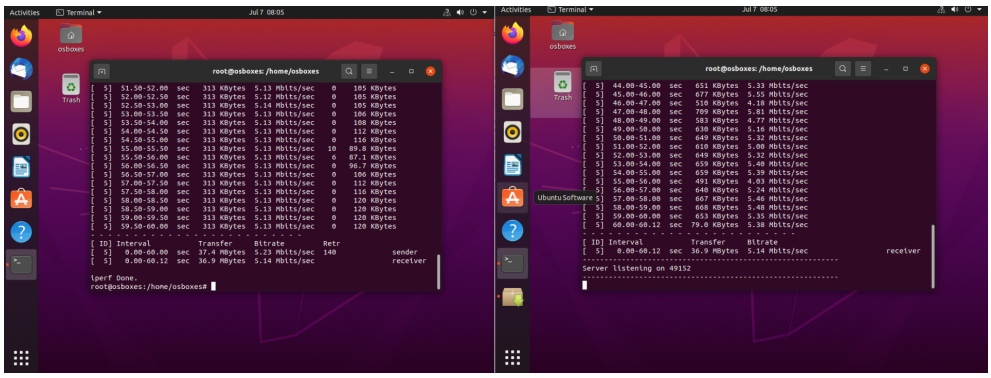


Figura 5.61: Largura de Banda da rede (iperf3). Fonte: Autor

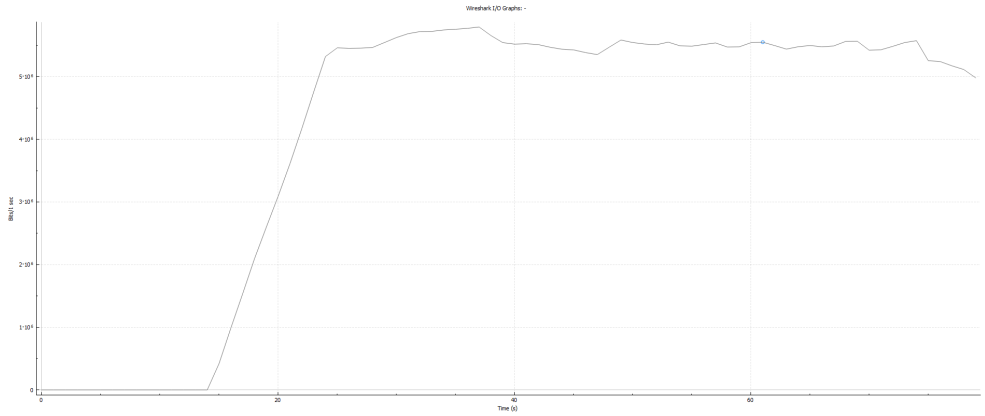


Figura 5.62: Largura de Banda da rede (Wiresahrk). Fonte: Autor

Ambas as figuras 5.61 e 5.62 mostram um throughput disponível de $5,14Mbps$ a figura 5.63 capturada das conversas pelo wireshark, mostra na verdade a largura de banda de $5,3Mbps$ se aproximando bastante da medição realizada pelo iperf3, para este caso vamos considerar nossa lagura de banda total disponível de $5,14Mbps$.

IPv4 · 11 TCP · 3

Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
91.189.91.39	80	172.16.30.2	50776	59.506	52,630 MiB	2	37.320	51,035 MiB	22.186	1,595 MiB	297.100952	83.1502	5148 kbps	160 kbps
172.31.1.2	42966	172.16.30.2	49152	34	2,936 KiB	0	18	1,606 KiB	16	1,329 KiB	19.027716	60.6003	217 bits/s	179 bits/s
172.31.1.2	42980	172.16.30.2	49152	42.615	39,695 MiB	1	27.825	38,737 MiB	14.790	980,475 KiB	19.132533	60.4106	5379 kbps	132 kbps

Figura 5.63: Largura de Banda da rede (Wiresahrk - "Conversations"). Fonte: Autor

5.3.2 QoS

Para a testagem do QoS, selecionamos um método de análise quantitativa que será idêntico ao utilizado para a flexiwan para termos resultados validos, as mesmas regras se aplicam aqui, entretanto, naturalmente, o processo de configuração da politica é diferente. Utilizaremos a mesma regra, trafego gerado po **0.0.0./0** para identificar todo o range de IP's, contudo o que importa neste novo será seu protocolo, neste caso o **TCP** na porta **3030**.

5.3.2.1 QoS Desativado

Para está parte as mesma configurações são aplicadas, utilizaremos a maquina do GNS3 com endereço **192.168.254.27** rodando dois servidores iperf um na porta 3030 e outro na porta 6060* (esse processo de mudança da segunda porta se faz necessário dado que o SW core FGA estava rodando na porta 5050 para acesso ao GNS3). Seguem resultados:

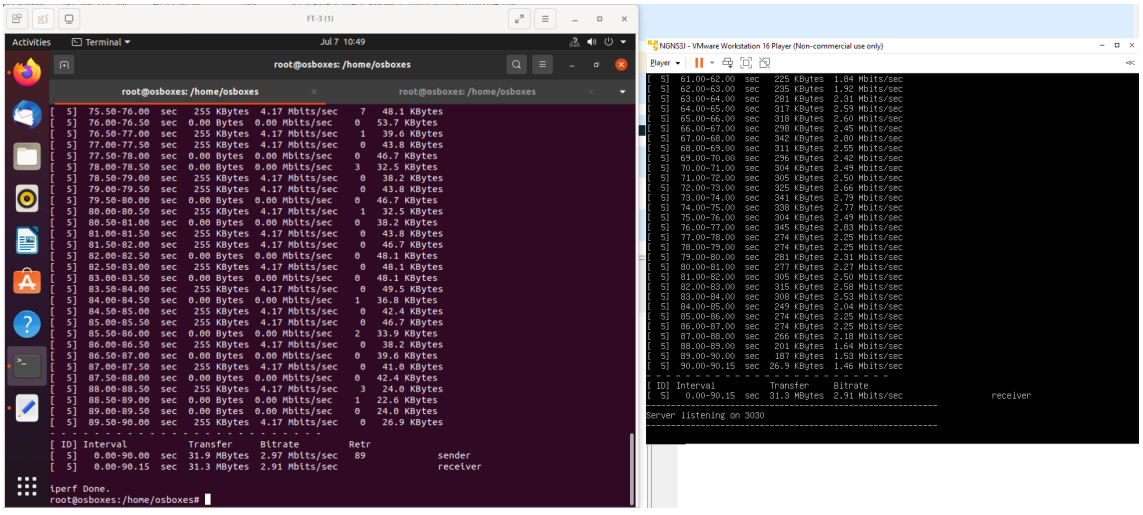


Figura 5.64: Saídas do iperf3 para os fluxos. Fonte: Autor

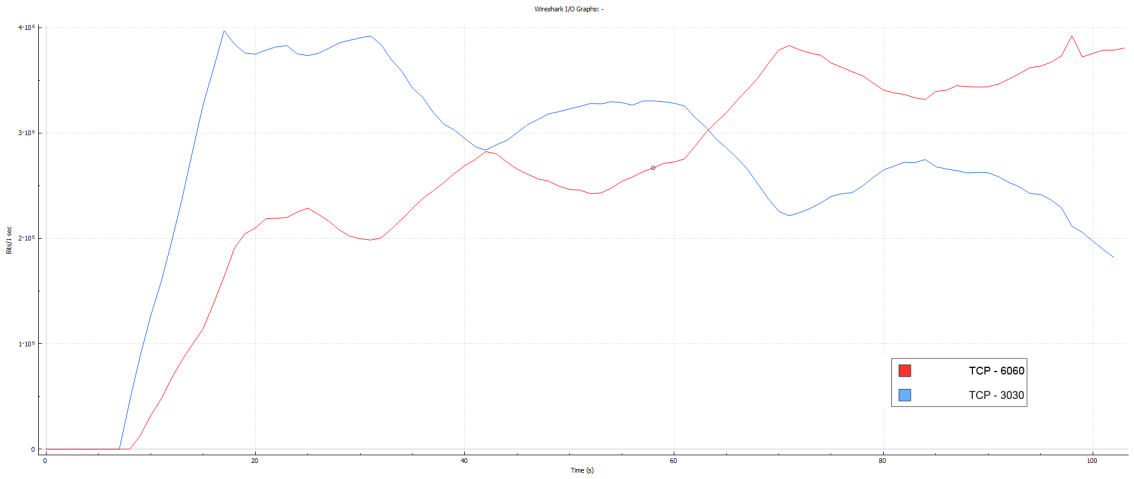
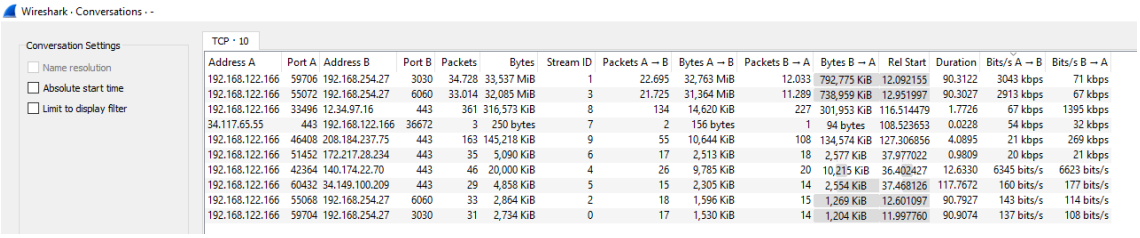


Figura 5.65: Gráfico dos Fluxos TCP para o QoS Desativado - FORTINET. Fonte: Autor



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.122.166	59706	192.168.254.27	3030	34,728	33,537 MiB	1	22,695	32,763 MiB	12,033	792,775 KiB	12.092155	90.3122	3043 kbps	71 kbps
192.168.122.166	55072	192.168.254.27	6060	33,014	32,085 MiB	3	21,725	31,364 MiB	11,289	738,959 KiB	12.951997	90.3027	2913 kbps	67 kbps
192.168.122.166	33496	12.34.97.16	443	361	316,573 KiB	8	134	14,620 KiB	227	301,953 KiB	116.514479	1.7726	67 kbps	1395 kbps
34.117.65.55	443	192.168.122.166	36672	3	250 bytes	7	2	156 bytes	1	94 bytes	108.523653	0.0228	54 kbps	32 kbps
192.168.122.166	46408	208.184.237.75	443	163	145,218 KiB	9	55	10,644 KiB	108	134,574 KiB	127.306856	4.0895	21 kbps	269 kbps
192.168.122.166	51452	172.217.28.234	443	35	5,090 KiB	6	17	2,513 KiB	18	2,577 KiB	37.977022	0.9809	20 kbps	21 kbps
192.168.122.166	42364	140.174.22.70	443	46	20,000 KiB	4	26	9,785 KiB	20	10,215 KiB	36.402427	12.6330	6345 bits/s	6623 bits/s
192.168.122.166	60432	34.149.100.209	443	29	4,858 KiB	5	15	2,305 KiB	14	2,554 KiB	37.468126	117.7672	160 bits/s	177 bits/s
192.168.122.166	55068	192.168.254.27	6060	33	2,864 KiB	2	18	1,596 KiB	15	1,269 KiB	12.601097	90.7927	143 bits/s	114 bits/s
192.168.122.166	59704	192.168.254.27	3030	31	2,734 KiB	0	17	1,530 KiB	14	1,204 KiB	11.997760	90.9074	137 bits/s	108 bits/s

Figura 5.66: Conversas TCP capturadas pelo Wireshark (QoS Desativado). Fonte: Autor

O comportamento do fluxo é semelhante ao capturado na sessão de análise do fleximanager, podemos ver que ambos os fluxos competem pela largura de banda total e neste caso a dividindo-a. Como reparado também o perf calculou um total de $2,91Mbps$ para o fluxo 3030 e $2,79Mbps$ para o fluxo 6060 já o wireshark, como mostra na figura 5.66 podemos notar que tivemos uma taxa de $3Mbps$ ára o fluxo 3030 e $2.91Mbps$ para o fluxo 6060, ambas as taxas ultrapassaram o valor base de largura de banda medido para esse cenário, o que é normal.

5.3.2.2 QoS Ativo

A criação de regras de QoS no Fortigate é bem maid dificil e complexa comprada à solução da flexliwan. Primeiro deve-se criar um perfil de "Traffic Shaping"que ira gerar um Class ID dentro do roteador, pode-se criar um tamplete no fortmanager, contudo o processo é mais complexo e envolve uma serie de etapas, foi optado por colocar o QoS apenas no roteador "rDarcy", neste perfil podemos alocar a banda que quisermos, dado que nos teste com o FlexiEdge alocamos a banda para 70% aqui será feito o mesmo, a seguir criou-se uma politica default que serve para todos os outros fluxos que utilizara os outros 30% da banda ou 100% caso não haja nenhuma fila. Como mostrado na figura abaixo.

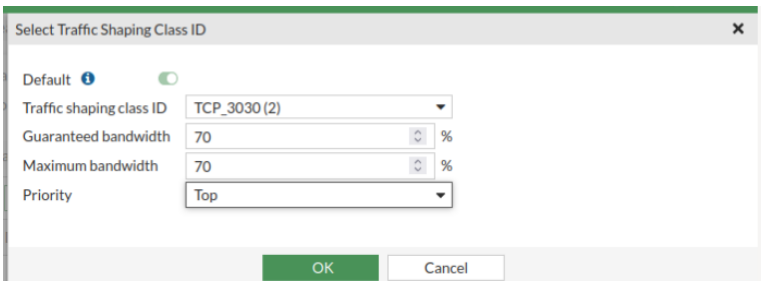


Figura 5.67: Traffic Shaping Fortigate. Fonte: Autor

Dado o perfil criado logo após precisamos criar o serviço, figura 5.68, neste ponto nos aproximamos do conceito de aplicativos da flexiwan o processo aqui é similar, foi criado um serviço de nome **PORT_3030** com protocol type TCP/UDP/SCTP. Com o serviço devidamente criado agora é necessário juntar tudo em uma politica de trafego, figura 5.69 e em seguida adiciona a interface de saída, em nosso caso a "WAN1", figura 5.70.

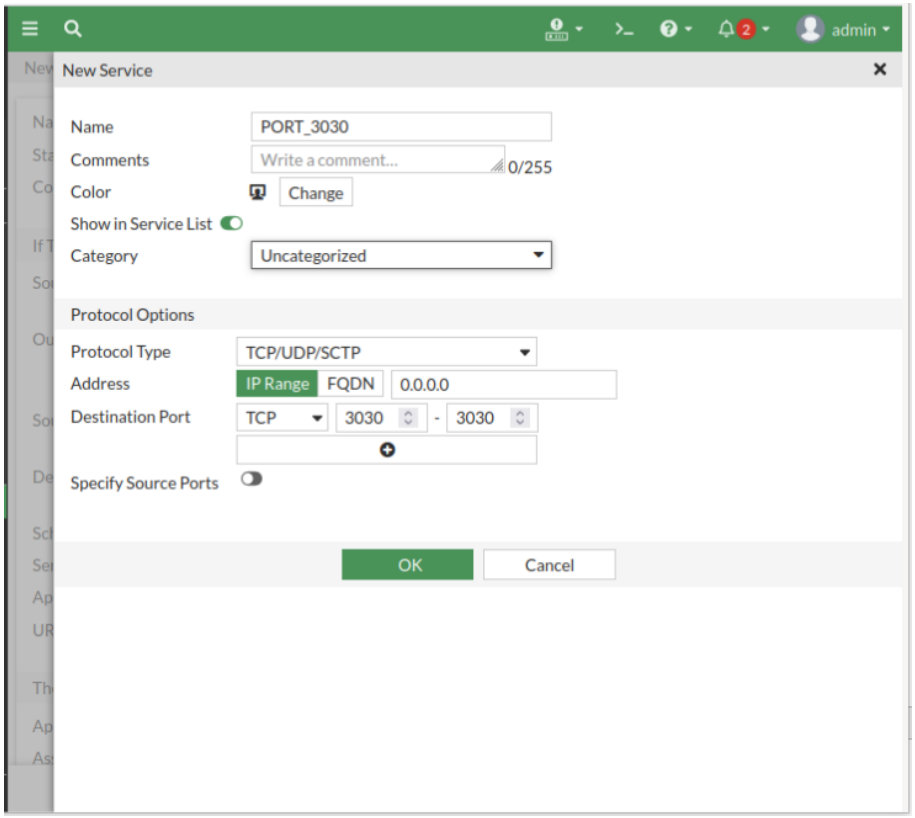


Figura 5.68: Serviço criado no Fortigate, porta 3030. Fonte: Autor

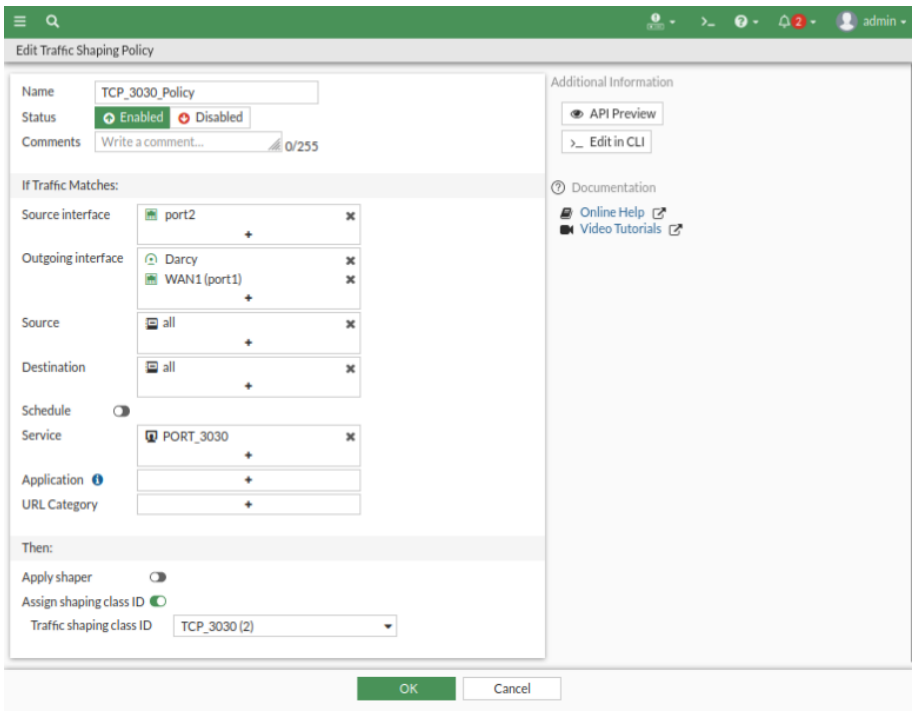


Figura 5.69: Traffic Policy Fortigate. Fonte: Autor

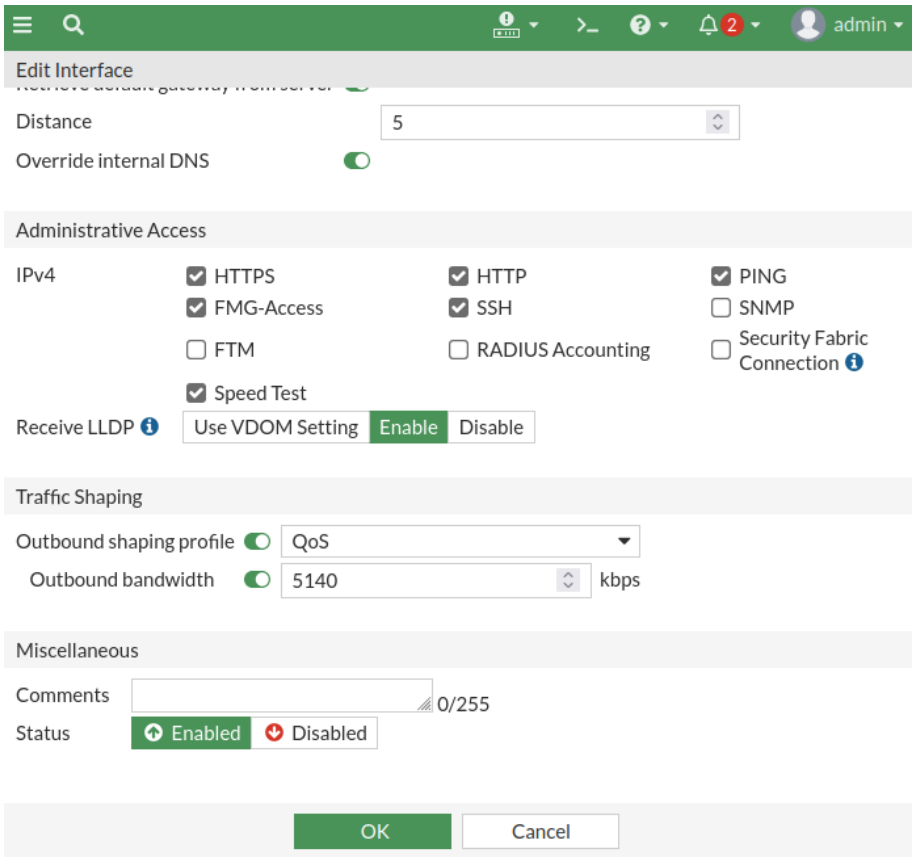


Figura 5.70: Traffic Policy Fortigate Aplicado a Interface. Fonte: Autor

Com o QoS devidamente configurado e ativado na interface de interesse foram realizados e os resulta-

dos estão dispostos abaixo:

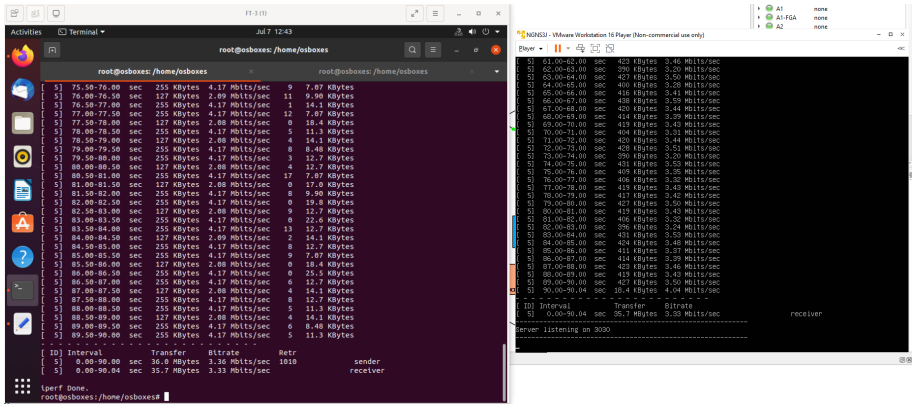


Figura 5.71: Saídas do iperf3 para os Fluxo, QoS Ativo. Fonte: Autor

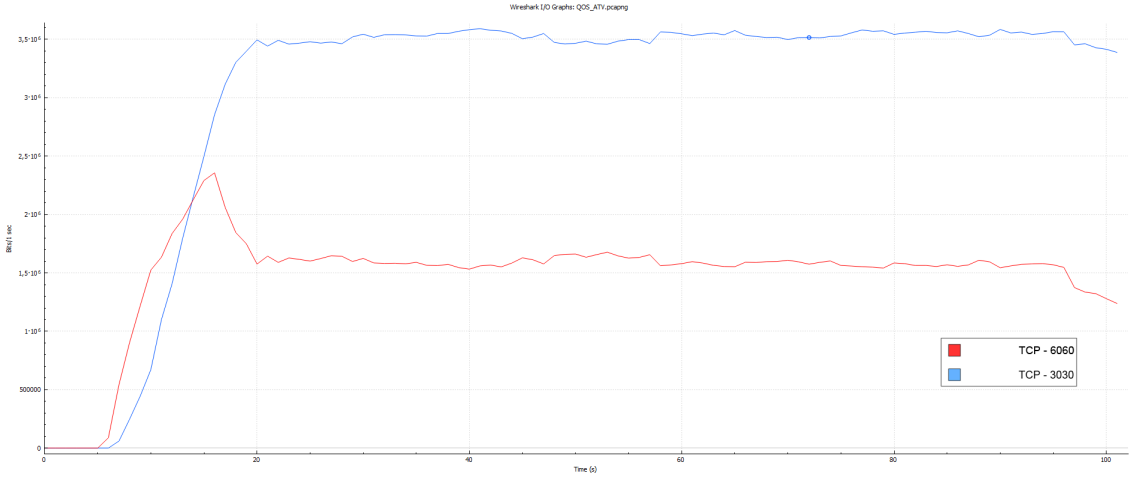
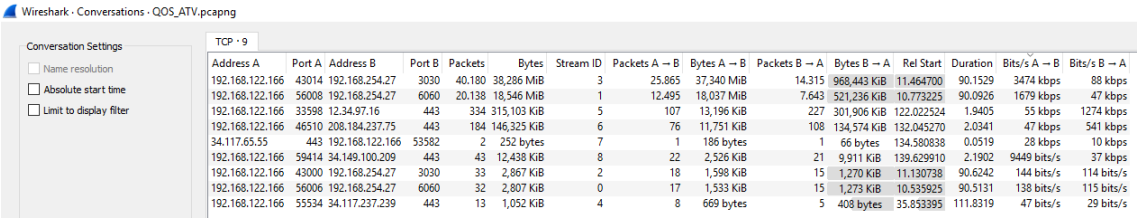


Figura 5.72: Gráfico dos Fluxos TCP para o QoS Ativado - FORTINET. Fonte: Autor



Address A	Port A	Address B	Port B	Packets	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.122.166	43014	192.168.254.27	3030	40.180	38,286 MiB	3	25.865	37,340 MiB	14.315	968,443 KiB	11.464700	90.1529	3474 kbps	88 kbps
192.168.122.166	56008	192.168.254.27	6060	20.138	18,546 MiB	1	12.495	18,037 MiB	7.643	521,236 KiB	10.773225	90.0926	1679 kbps	47 kbps
192.168.122.166	33598	12.34.97.16	443	334	315,103 KiB	5	107	13,196 KiB	227	301,906 KiB	122.022524	1.9405	55 kbps	1274 kbps
192.168.122.166	46510	208.184.237.75	443	184	146,325 KiB	6	76	11,751 KiB	108	134,574 KiB	132.045270	2.0341	47 kbps	541 kbps
34.117.65.55	443	192.168.122.166	53582	2	252 bytes	7	1	186 bytes	1	66 bytes	134.580838	0.0519	28 kbps	10 kbps
192.168.122.166	59414	34.149.100.209	443	43	12,438 KiB	8	22	2,526 KiB	21	9,911 KiB	139.629910	2.1902	9449 bits/s	37 kbps
192.168.122.166	43000	192.168.254.27	3030	33	2,867 KiB	2	18	1,598 KiB	15	1,270 KiB	11.130738	90.6242	144 bits/s	114 bits/s
192.168.122.166	56006	192.168.254.27	6060	32	2,807 KiB	0	17	1,533 KiB	15	1,273 KiB	10.535925	90.5131	138 bits/s	115 bits/s
192.168.122.166	55534	34.117.237.239	443	13	1,052 KiB	4	8	669 bytes	5	408 bytes	35.853395	111.8319	47 bits/s	29 bits/s

Figura 5.73: Conversas TCP capturadas pelo Wireshark, QoS Ativo. Fonte: Autor

Como era de se esperar houve a aplicação do QoS no fluxo 3030, como podemos reparar em 5.72, dado o throughput descrito de $5,14Mbps$ o esperado é que o fluxo 3030 ocupasse em torno de $3,6Mbps$ e o fluxo 6060 $1,5Mbps$, os resultados do iperf3 mostram de fato um resultado em torno do esperado com o fluxo 3030 ocupando $3,33Mbps$ e o fluxo 6060 ocupando $1,61Mbps$. Contudo o Wireshark coletou os dados e mostrou um total de $3,4Mbps$ para o fluxo 3030 e $1,6Mbps$, resultados próximos e que também se aproximam do esperado. Durante a criação das regras de QoS não foi identificado uma opção para a marcação do DSCP no cabeçalho IP, logo o tipo ficou como marcação padrão, como mostrado na figura

5.74.

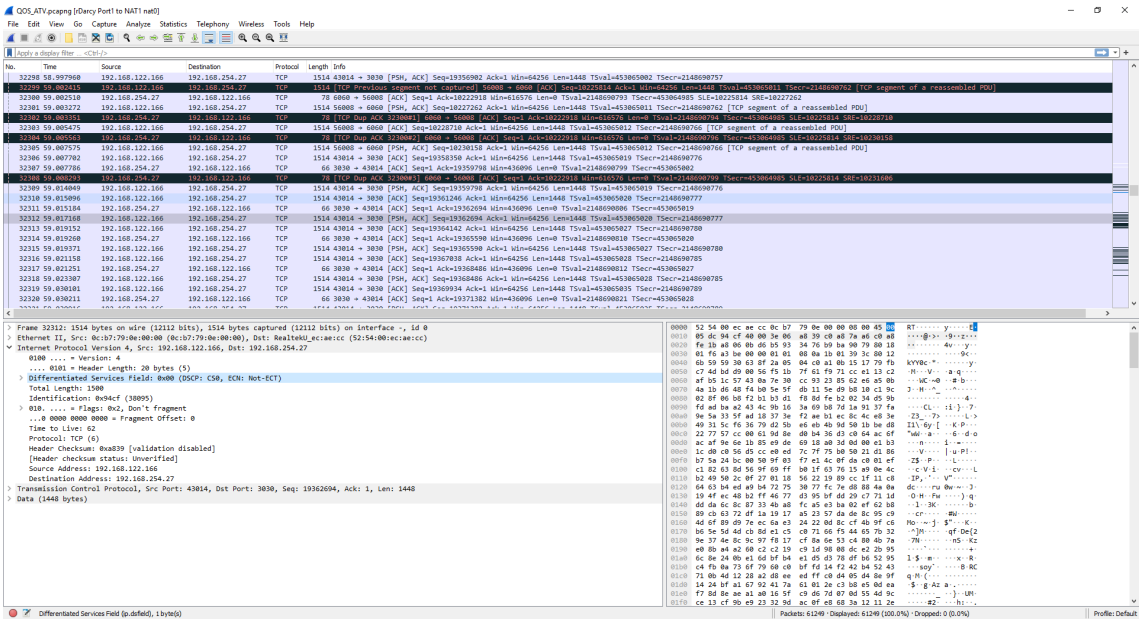


Figura 5.74: Campo DSCP em um cabeçalho IP aleatório do fluxo 3030 - Fortinet. Fonte: Autor

5.3.3 Segurança

Nesta parte a análise será focada em quesitos de segurança fornecidos pela Fortinet. Para esta análise vamos testar o bloqueio da pagina web **www.facebook.com** e além disso o bloqueio de pings entre as LAN's **ADM** e **FT**, como feito na flexiwan. O Fortigate conta com uma serie de serviços e aplicações já mapeados em um banco de dados, contudo o mesmo não está disponível na licença trial utilizada, com isso a criação da regra será feita pelo recurso WEB FILTER, onde é alocado um endereço web e o mesmo é bloqueado, como mostrado na figura 5.75, assim que criada a regra a mesma deve ser adiconado em uma police do firewall, como mostrado na figura 5.76. A seguir, deve-se ser criada uma regra de firewall para bloquear pings entre as LAN's **ADM** e **FT**. As regras foram criadas de acordo com as figuras abaixo:

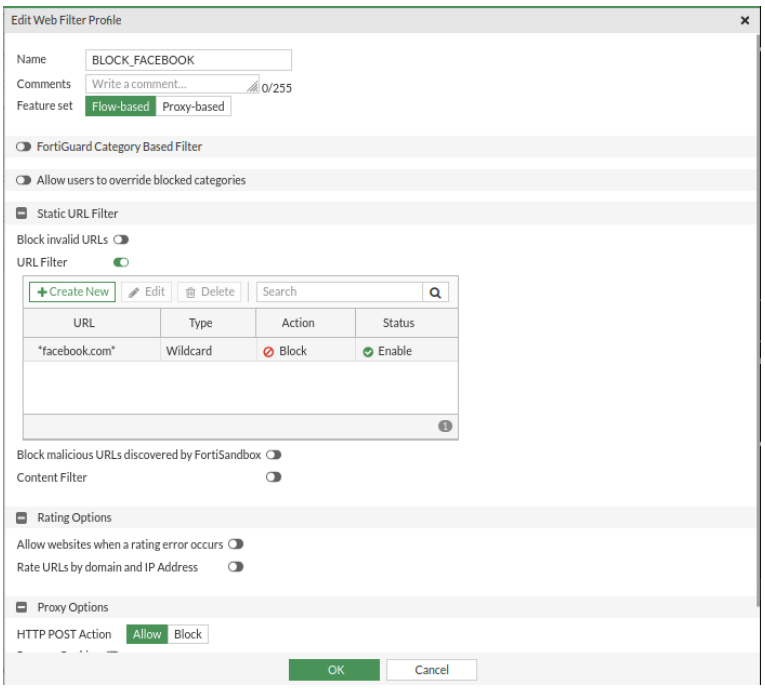


Figura 5.75: Web Filter para o facebook - Fortigate. Fonte: Autor

Figura 5.76: Regras de Firewall para o Facebook - Fortigate. Fonte: Autor

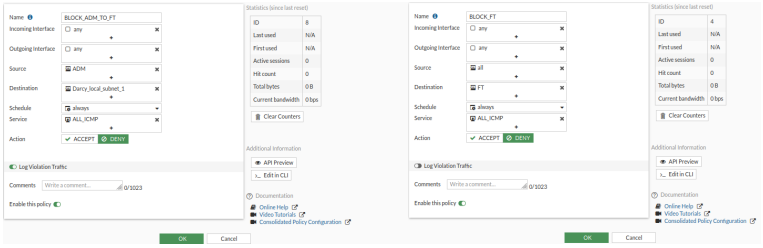


Figura 5.77: Regras de Firewall para as LANs - Fortigate. Fonte: Autor

Após a devida criação da regras é necessário sincronizar os roteadores e em seguida testa-las, assim o primeiro teste vamos testar a regra de PING, que poderia ser facilmente trocada por uma regra de acesso externo, a seguir na figura 5.78.

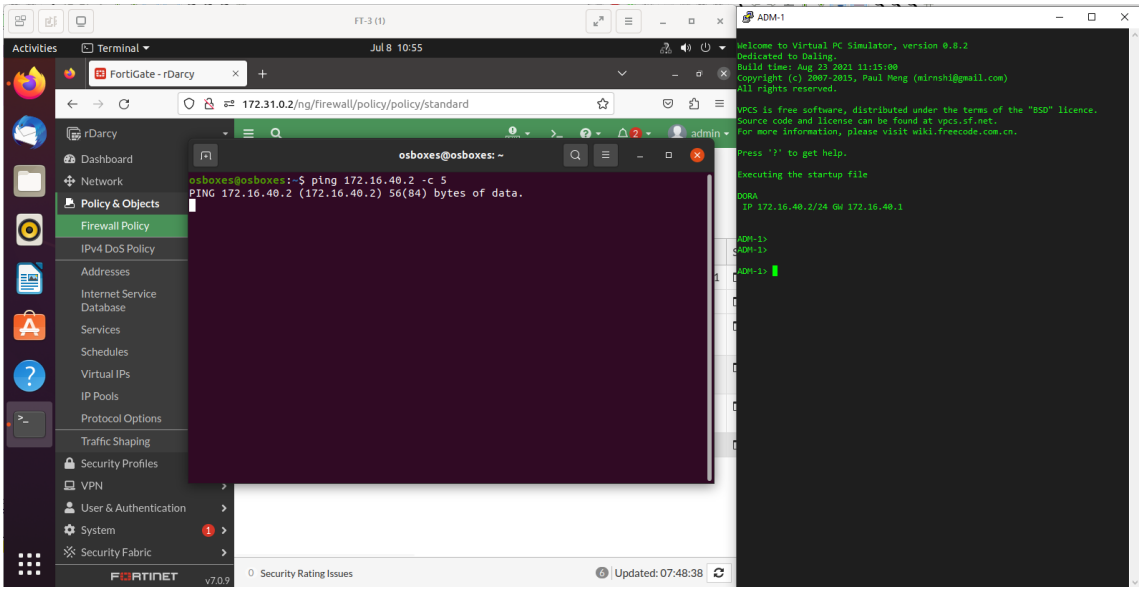


Figura 5.78: Ping entre as redes FT → ADM (Fortinet).Fonte: Autor

A seguir, foi iniciada uma captura nos links entre **SWCORE** → **rDarcy** (lado direito) e entre **rFGA** → **SWCORE-FGA** (lado esquerdo), onde além do print acima onde temos que **5** pacotes foram transmitidos e nenhum recebido, podemos ver de maneira mais clara na figura 5.79 as solicitações ICMP saindo do SWCORE para o roteador de borda, contudo nenhuma solicitação passa pelo link que ligado o roteador de borda da FGA a LAN ADM.

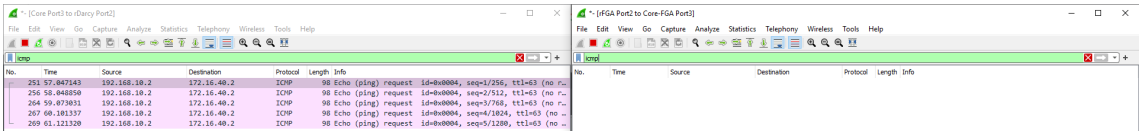


Figura 5.79: Ping entre as redes FT → ADM, Wireshark (Fortinet). Fonte: Autor

Como a comunicação ICMP foi bloqueada em ambos os lados da conversa, seguem prints do outro lado do bloqueio:

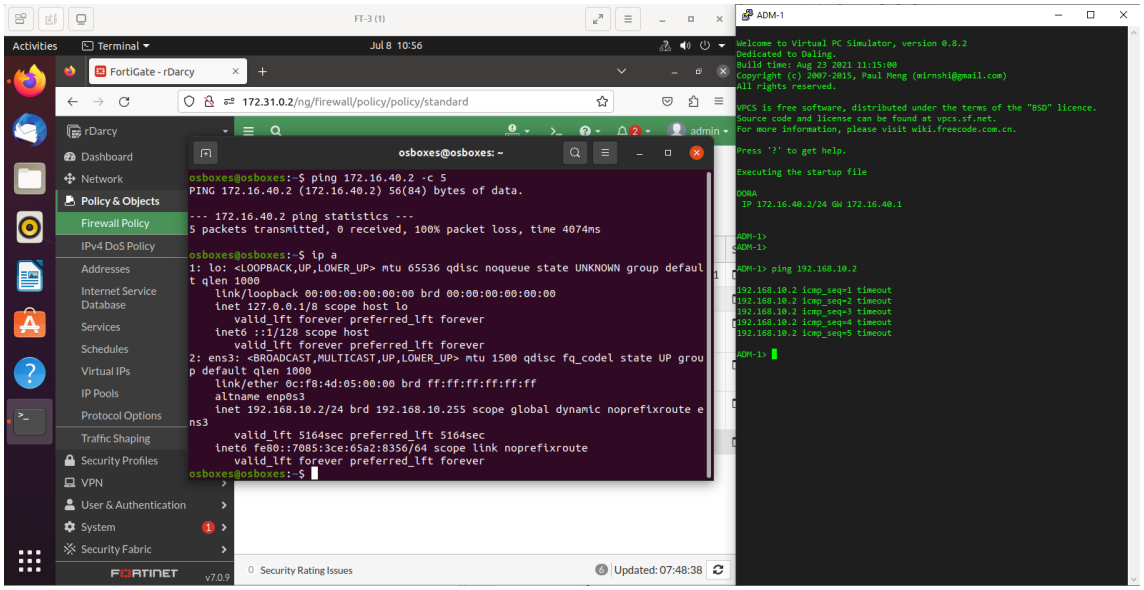


Figura 5.80: Ping entre as redes ADM → FT (Fortinet).Fonte: Autor

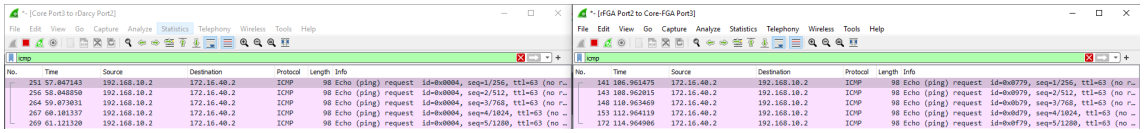


Figura 5.81: Ping entre as redes ADM → FT, Wireshark (Fortinet). Fonte: Autor

Como mostrados nas figuras acima, o mesmo processo ocorre, contudo podemos ver as requisições ICMP sendo enviadas e não sendo recebidas, mostrando assim o seu devido bloqueio. Nota-se também que na figura 5.81 Podemos observar os 5 pacotes enviados na tentativa descrita anteriormente.

Por fim o bloqueio do facebook, vamos utilizar a rede FT e o computador FT-3 para tentar fazer o acesso. Os processo que envolvem a conexão entre o usuário final e o site propriamente dito consiste na coleta de um endereço através de uma requisição de DNS e em seguida a solicitação dos dados. Na figura 5.82 é possível notar que o computador solicita ao servidor DNS 8.8.8.8 o endereço da aplicação.

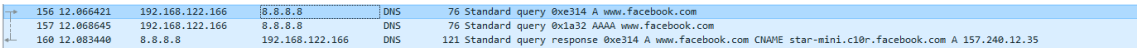


Figura 5.82: Solicitação do Endereço do site www.facebook.com, Wireshark. Fonte: Autor

Após isso é feita uma tentativa de conexão na porta 80 do **TCP** (figura 5.83 contudo a mesma diversas falhas mostrando que o endereço fornecido pelo DNS não é alcançável e de fato, ele se encontra bloqueado. Um diferencial do Fortigate é mensagem de firewall emitida no site, uma vez que o mesmo esta bloqueado, como mostrado na figura 5.84.

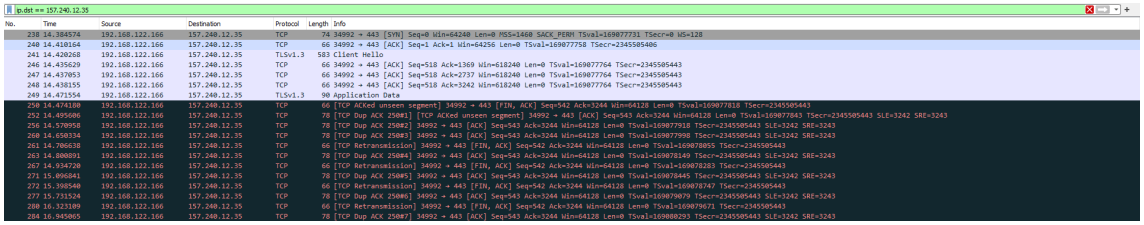


Figura 5.83: Retransmissões TCP, Fortinet (Wireshark). Fonte: Autor

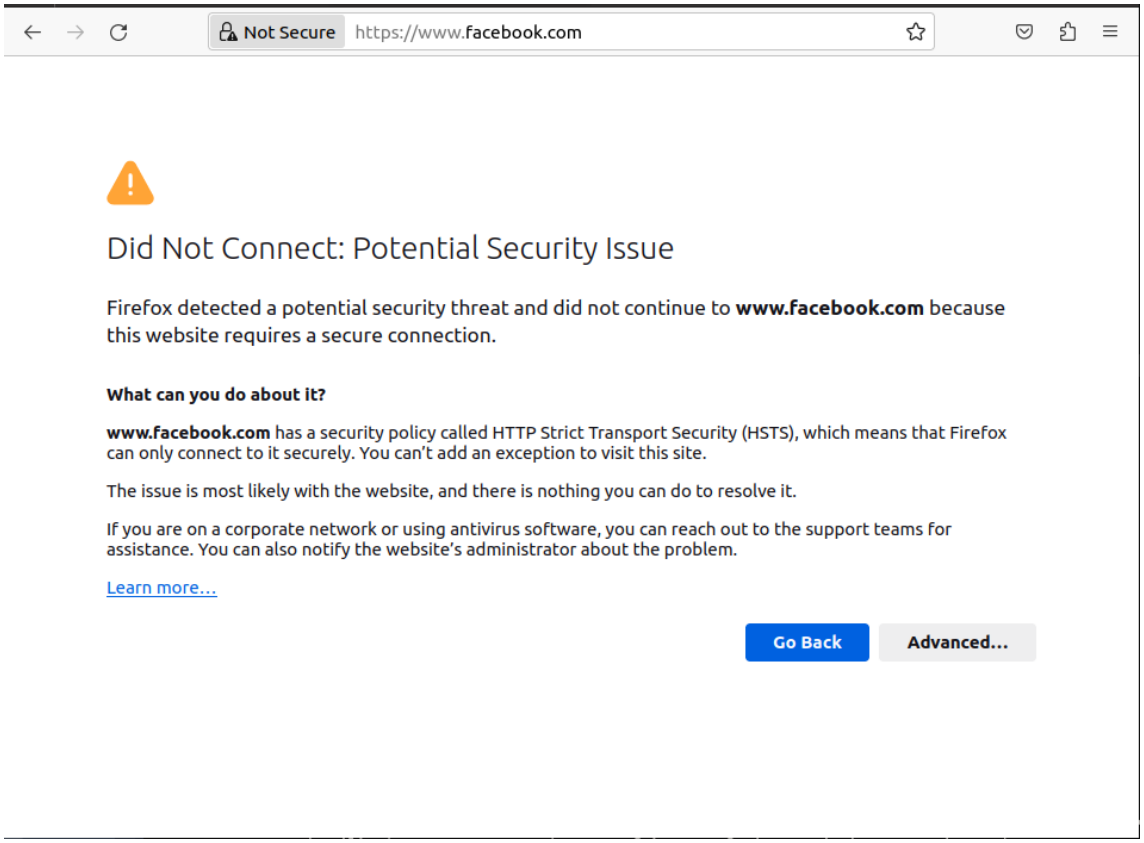


Figura 5.84: Erro no Navegador após a solicitação. Fonte: Autor

5.3.4 Delay dos Túneis

Nesta parte serão medidos os tempos de resposta entre uma rede e outra através dos túneis criados nos Fortigates. Para isso serão utilizados os computadores **FT-3** e **ENG-3**, para a realização dos testes será utilizado o mesmo esquema de testes feitos na Flexiwan. Primeiro se precisa conhecer a rota, como disposto na figura 5.85.

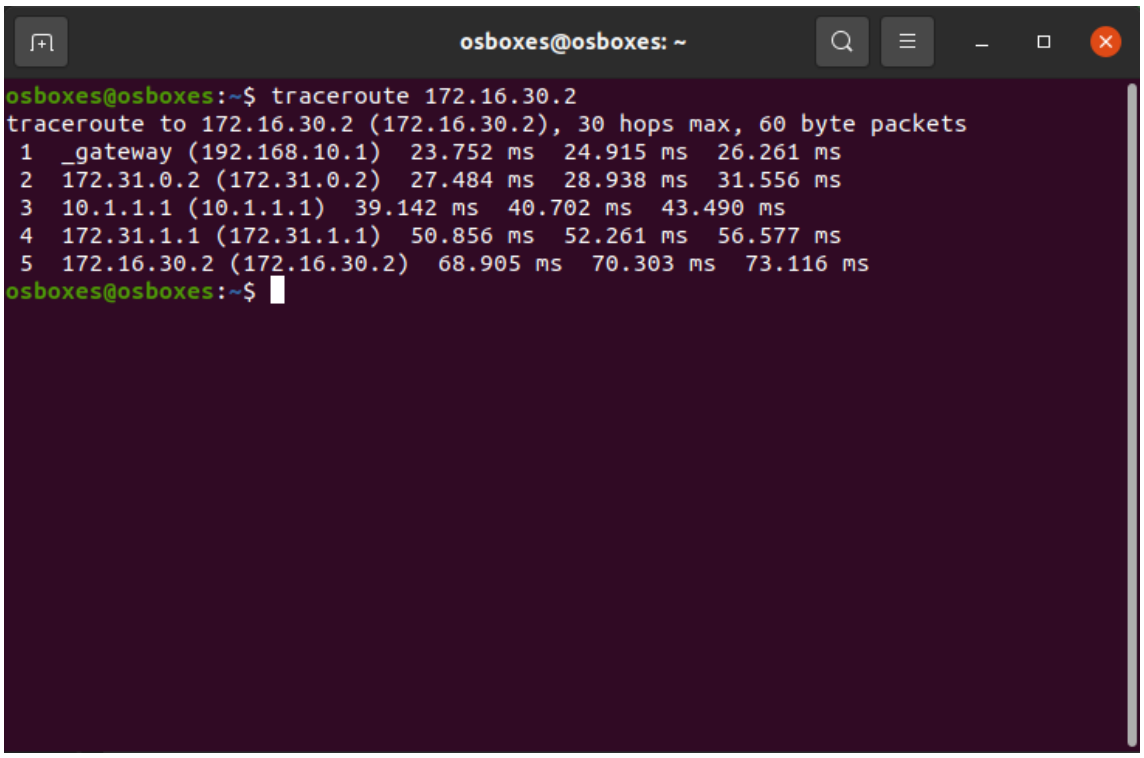


Figura 5.85: Rota entre FT-3 e ENG-3. Fonte: Autor

Assim, conhecendo a rota, podemos pingar todas as interfaces descritas para obter um resultado mais fiel, foi realizado um comando que envia 10 solicitações de ping e na tabela 5.2 podemos ver as médias para os destinos.

Tabela 5.2: Delay Médio dos Pings

Destino	Média
192.168.10.1	**5,906 ms**
172.31.0.2	**9,600 ms**
10.1.1.1	**11,717 ms**
172.31.1.1	**15,100 ms**
172.16.30.2	**22,682 ms**

Nosso foco está nos endereços **172.31.0.2**, **10.1.1.1** e **172.31.1.1**. O tempo necessário do pacote sair do PC FT-3 e chegar até a interface do roteador é de $9,6ms$. Contudo temos que dentro de nossa rota observa-se que o Fortigate, encaminha o pacote pela interface de virtual 10.1.1.1 que pertence ao roteador **rFGA**, vale notar que a partir desse ponto o pacote já está rodando com o protocolo ESP, como mostrado em 5.58, ou seja, o tempo que nos interessa no caminho é o processo de criptografia do túnel, sendo assim entre os tempos de 172.31.0.2 para 10.1.1.1 onde é feito o encapsulamento e envio e o tempos entre 10.1.1.1 e 172.31.1.1 onde são realizados a descriptografia e envio para a interface do roteador. Fazendo as contas temos que o processo de encapsulamento e envio do pacotes pelo túnel é de: $2,117ms$ e de desencapsulamento é de $3,3838ms$ dando um total de $5,5ms$ para o encapsulamento, envio e desencapsulamento dos pacotes.

5.3.5 Seleção de Caminho Dinâmico

Para esta parte da análise serão necessárias algumas mudanças na topologia, assim como na implementação da Flexiwan, a adição de mais duas saídas para a internet, em ambos os roteadores. Assim a topologia apresentada ficará com a seguinte forma:

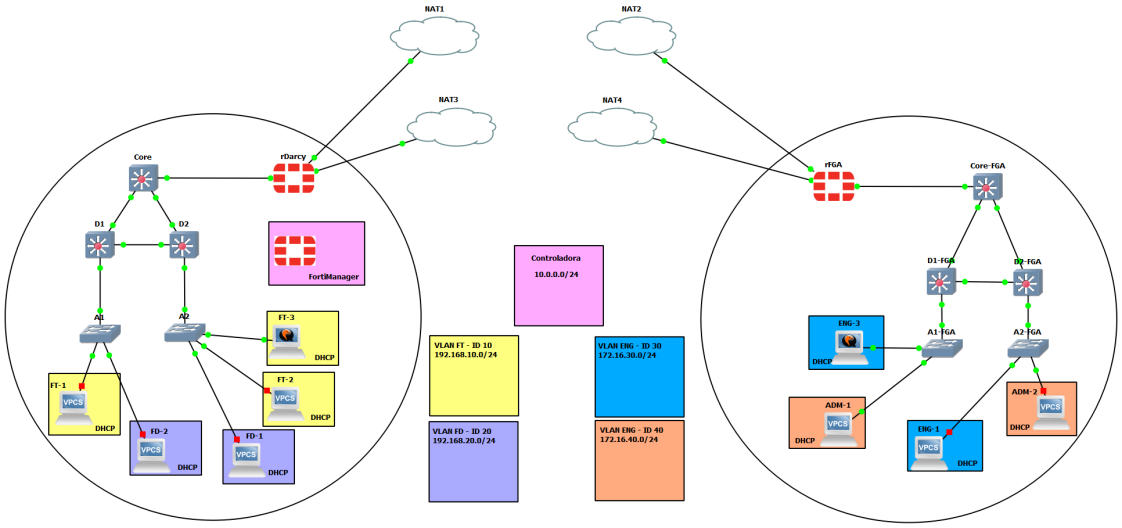


Figura 5.86: Nova Topologia. Fonte: Autor

Podemos, mais uma vez tirar proveito dos links e usar para que diferentes tráfegos possam seguir por diferentes caminhos. A configuração da Fortigate quando existem mais caminhos é diferente da flexiwan, antes precisamos estabelecer um novo túnel, em seguida propagar o OSPF pelos túneis criados e logo após aplicar uma politica SDWAN, identificada como *SDWAN RULES* que irá gerenciar os caminhos de acordo com a politica criada, neste caso uma demanda simples. Os passos estão descritos abaixo, a criação do túnel não será exposta.

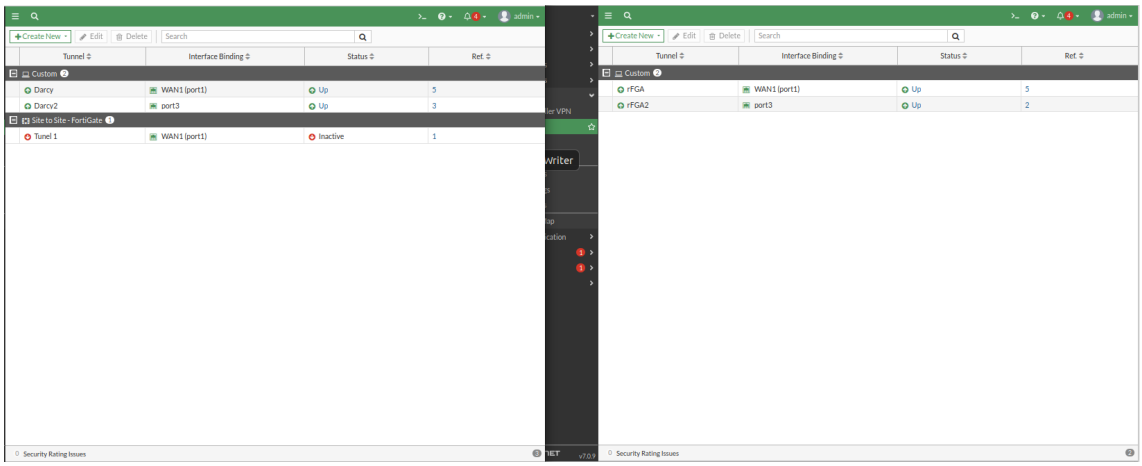


Figura 5.87: Novo túnel Criado. Fonte: Autor

5.3.5.1 Primeiro Cenário

Neste Primeiro cenário foram definidas duas regras principais, a primeira, chamada *ADM* diz respeito ao trafego que flui para a rede **172.16.40.0/24** e regra utilizará o túnel recém criado, *Darcy2* (importante ressaltar que há uma regra de bloqueio de tráfego, a mesma foi desabilitada):

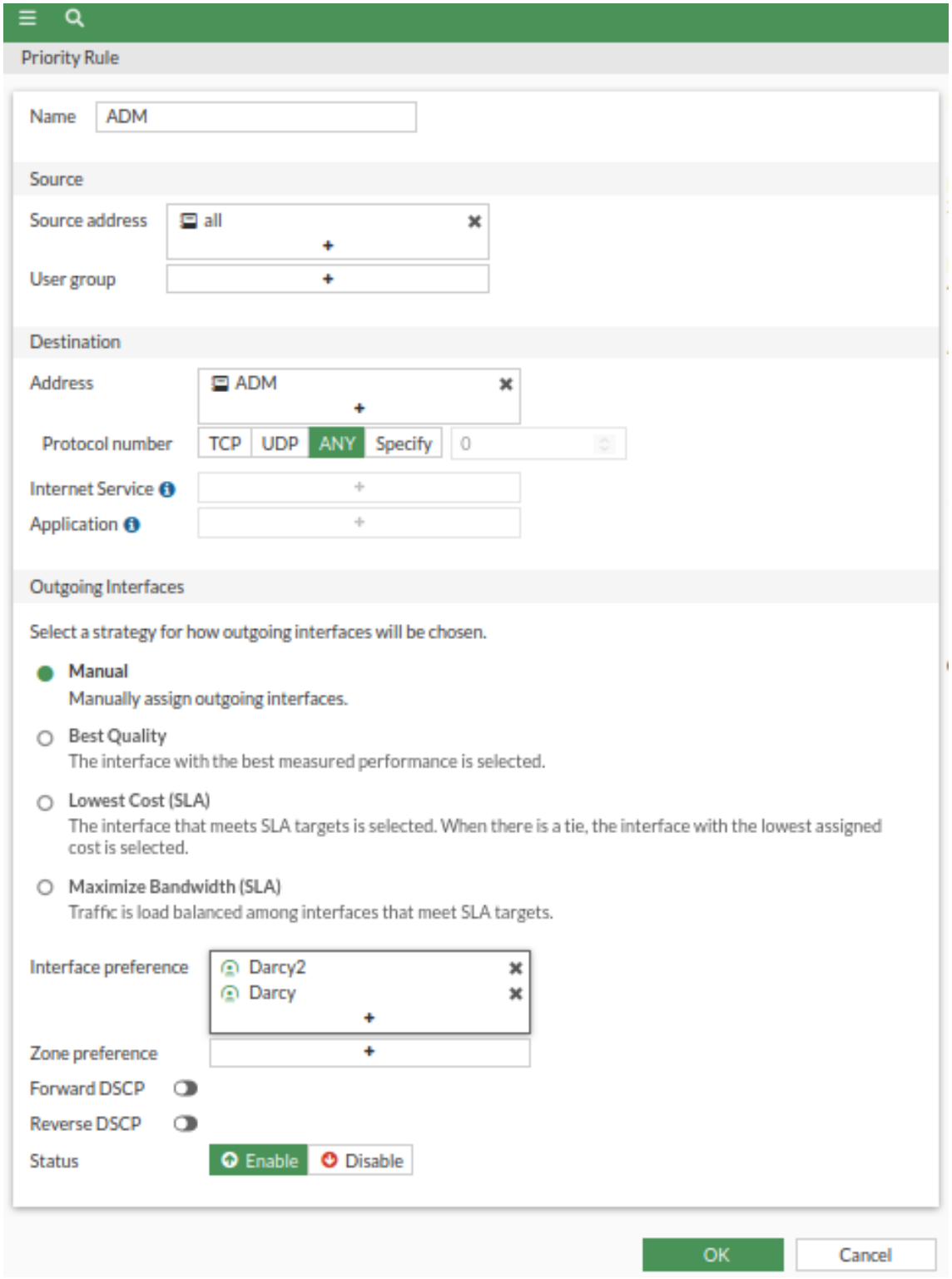


Figura 5.88: 1ª Regra do Path Selection, Fortigate. Fonte: Autor

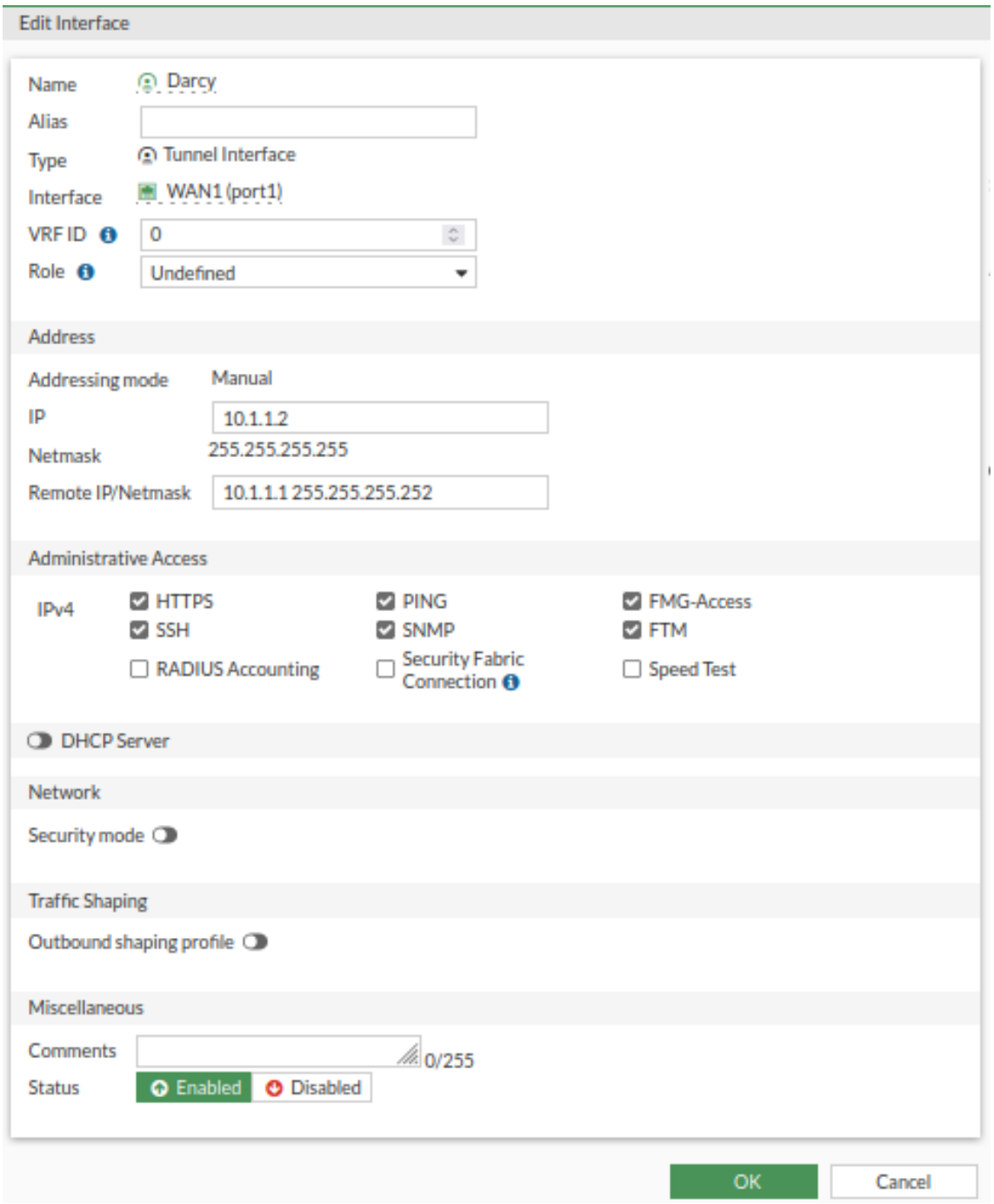


Figura 5.89: Endereços do Túnel Darcy. Fonte: Autor

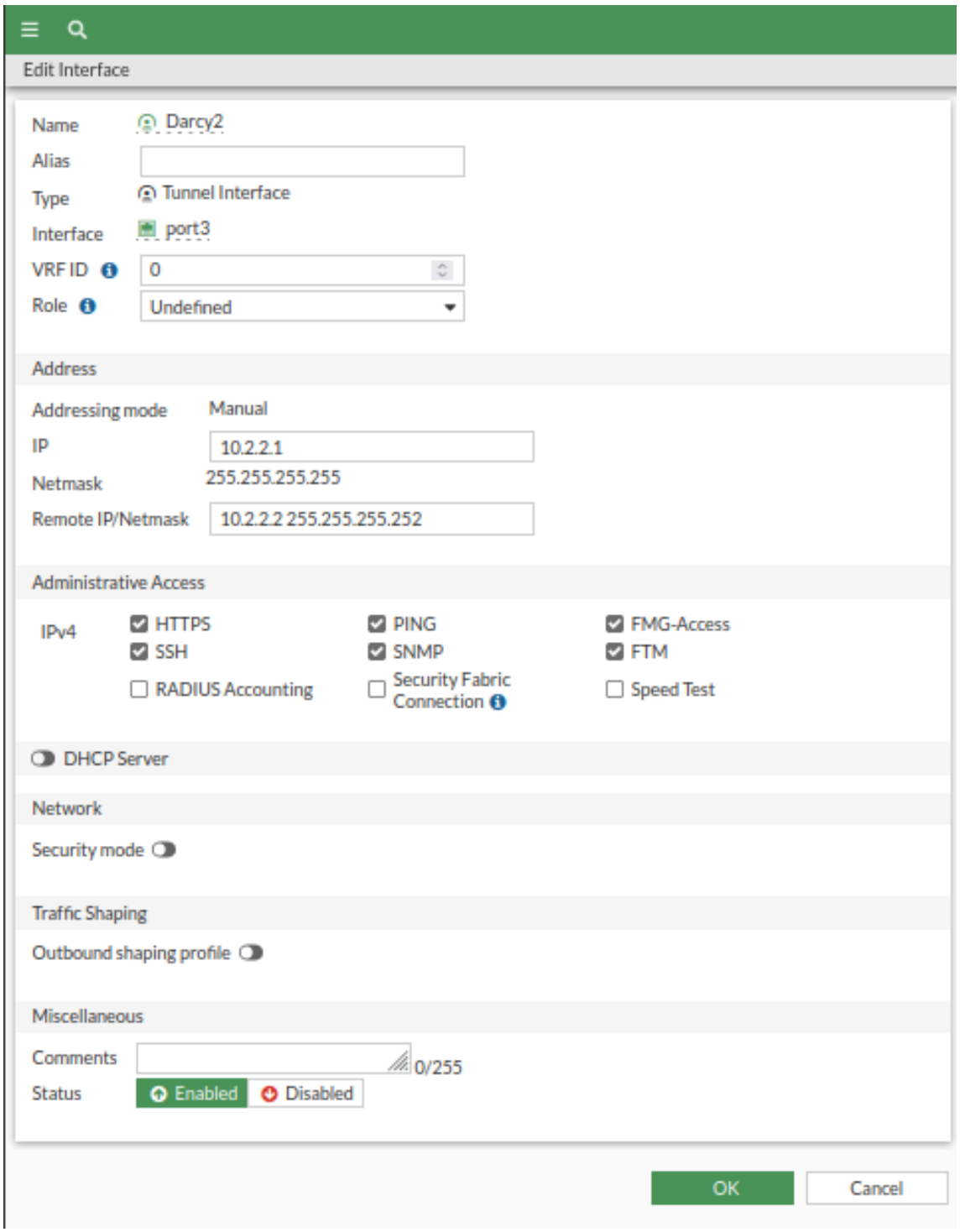


Figura 5.90: Endereços do Túnel Darcy2. Fonte: Autor

A segunda regra segue a mesma logica, com o nome *ENG* é definido que todo o tráfego que for for para a **172.16.30.0/24** será redirecionado pelo túnel *Darcy*.

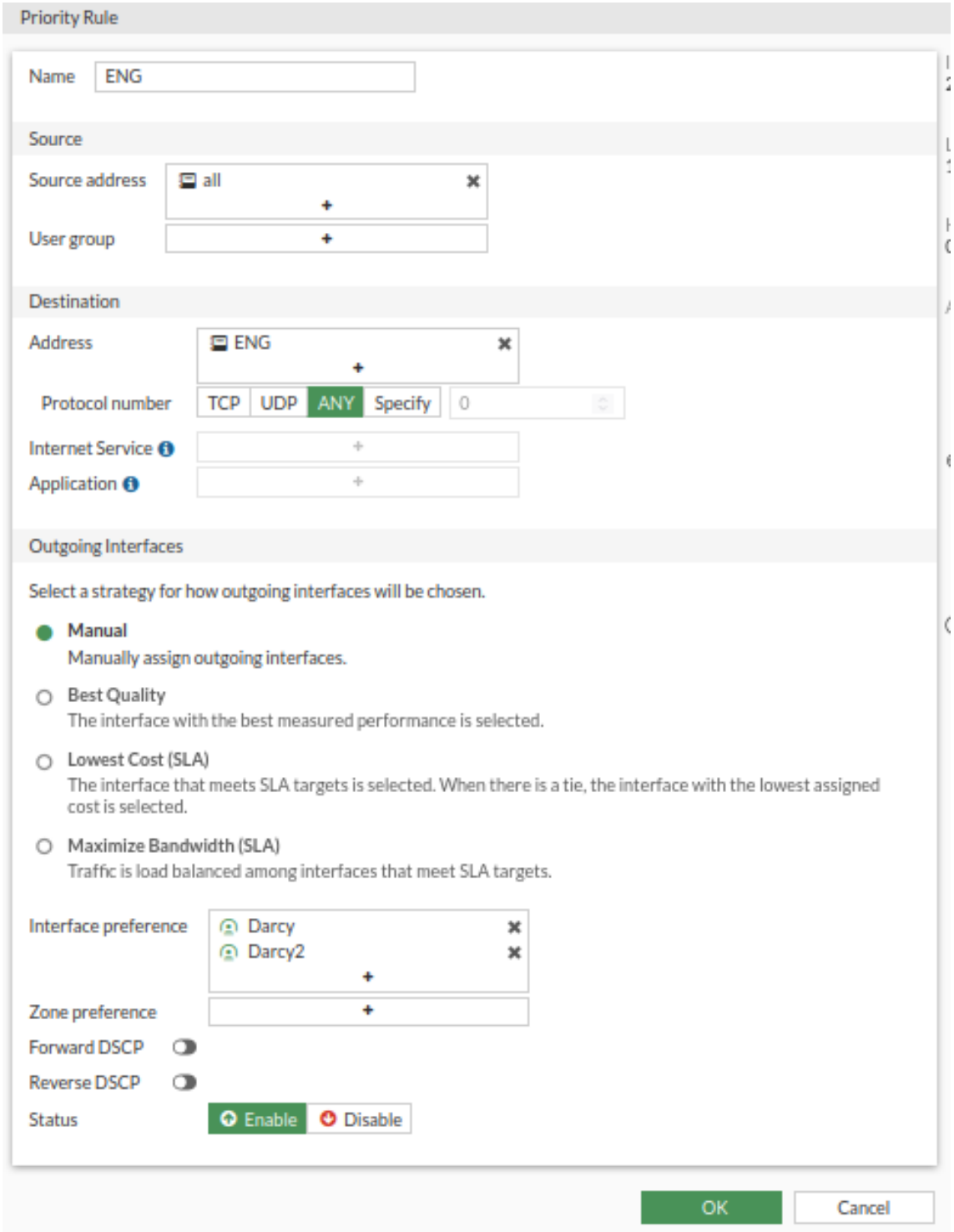


Figura 5.91: 2ª Regra do Path Selection, Fortinet. Fonte: Autor

Com isso pode-se iniciar nossos testes, para esta parte utilizaremos o comando *traceroute*, nele conseguimos ver claramente por onde o pacote está seguindo, utilizaremos o device FT-3 como suporte, seguem resultados:

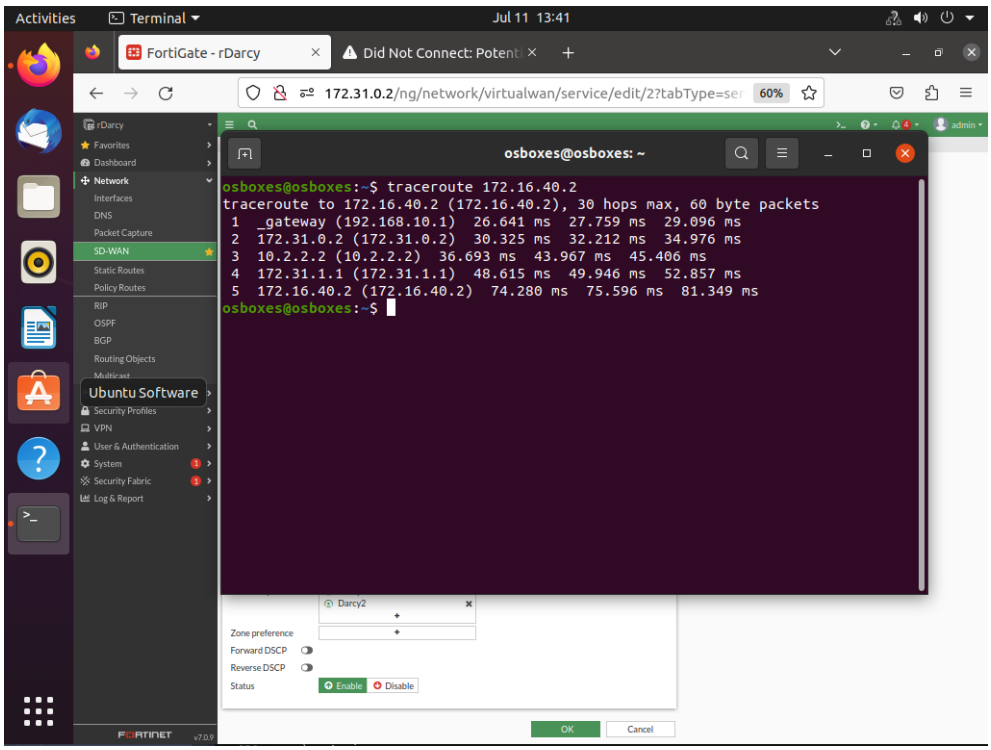


Figura 5.92: Traceroute para ADM, Fortinet. Fonte: Autor

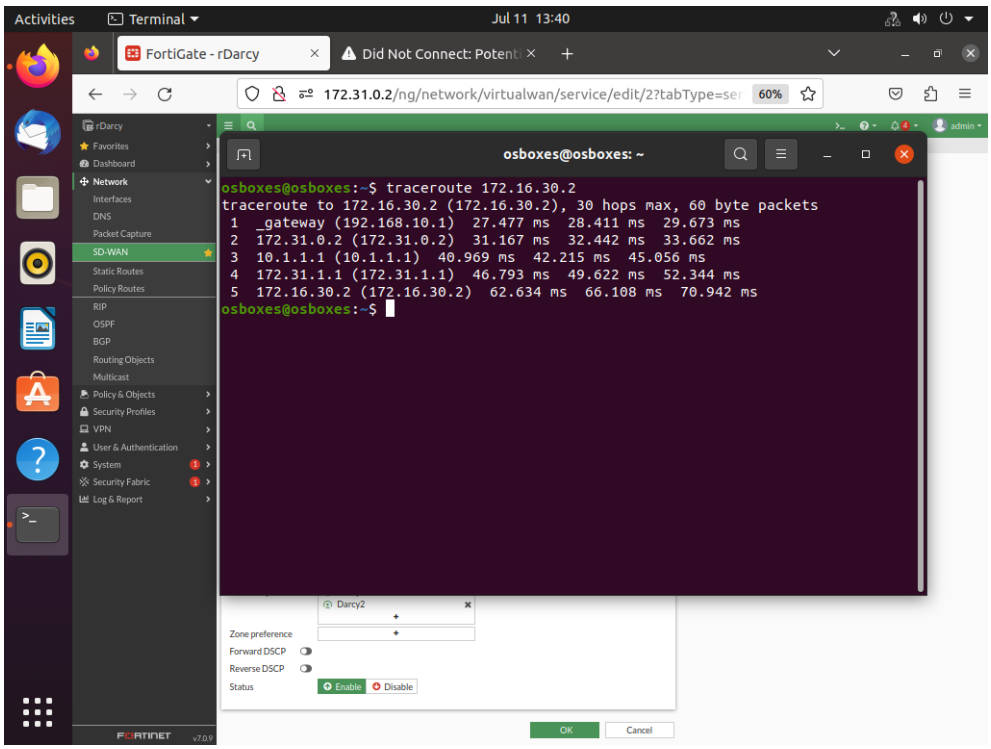


Figura 5.93: Traceroute para ENG, Fortinet. Fonte: Autor

Utilizando a figura 5.87, nota-se os endereços dos túneis e por fim as seguintes conclusões:

- Na figura 5.92, era esperado que todo trafego passasse pelo Túnel *"Darcy2"*, que tem endereço

de loopback final 10.2.2.2 , o retorno do comando mostra claramente que o resultado obtido foi o esperado.

- Da mesma forma da análise acima, temos que o trafego destinado a rede **172.16.30.2** foi alocado no caminho escolhido em suas configuração, pelo *"Darcy"* com endereço de loppkback 10.1.1.1.

5.3.5.2 Segundo Cenário

Para estes cenário os caminhos serão invertidos, assim os caminhos devem ser invertidos nas regras, como mostrado na figura 5.94. É importante notar que há dois túneis no caminho, contudo o prioritário é o primeiro e o segundo e para caso de falhas.

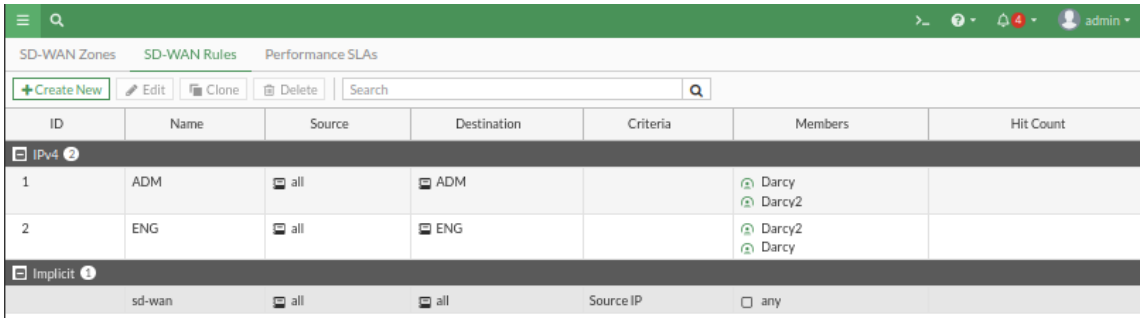


Figura 5.94: Regras invertidas para o cenário 2, Forinet Fonte: Autor

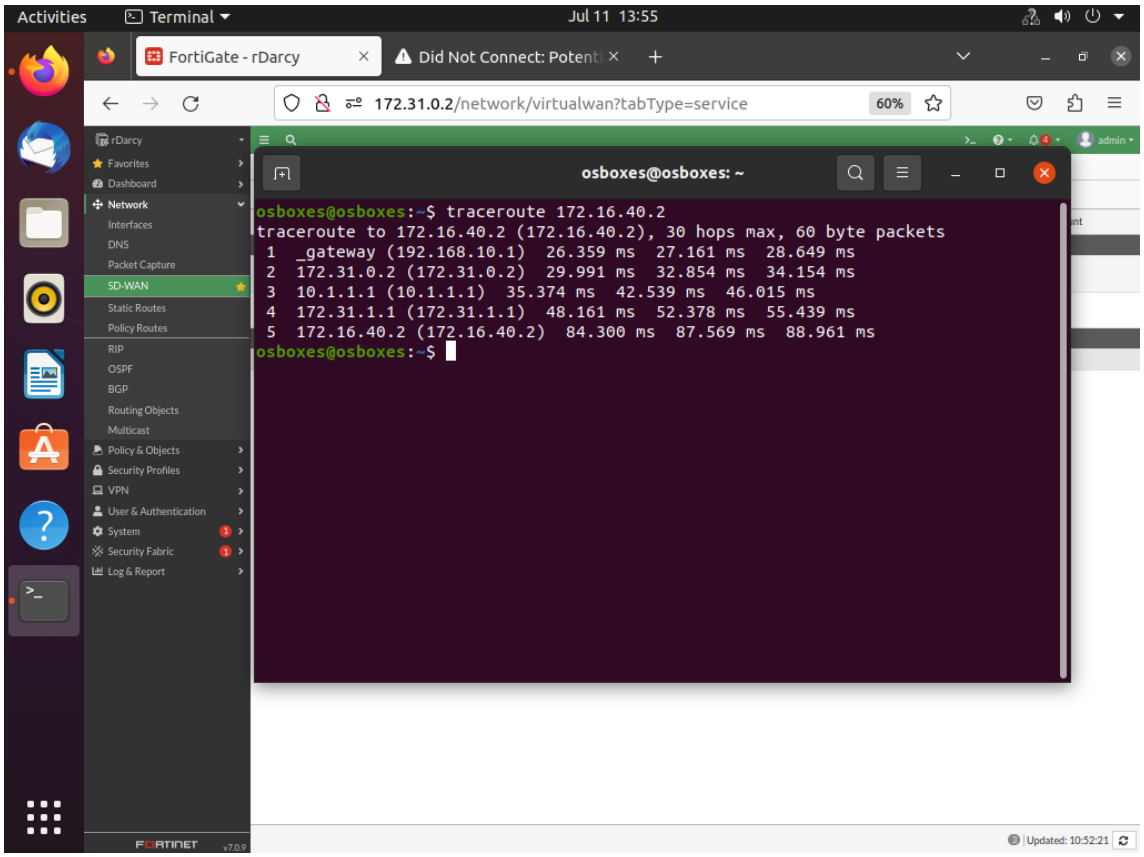


Figura 5.95: Traceroute para ADM com caminho invertido, Fortinet. Fonte: Autor

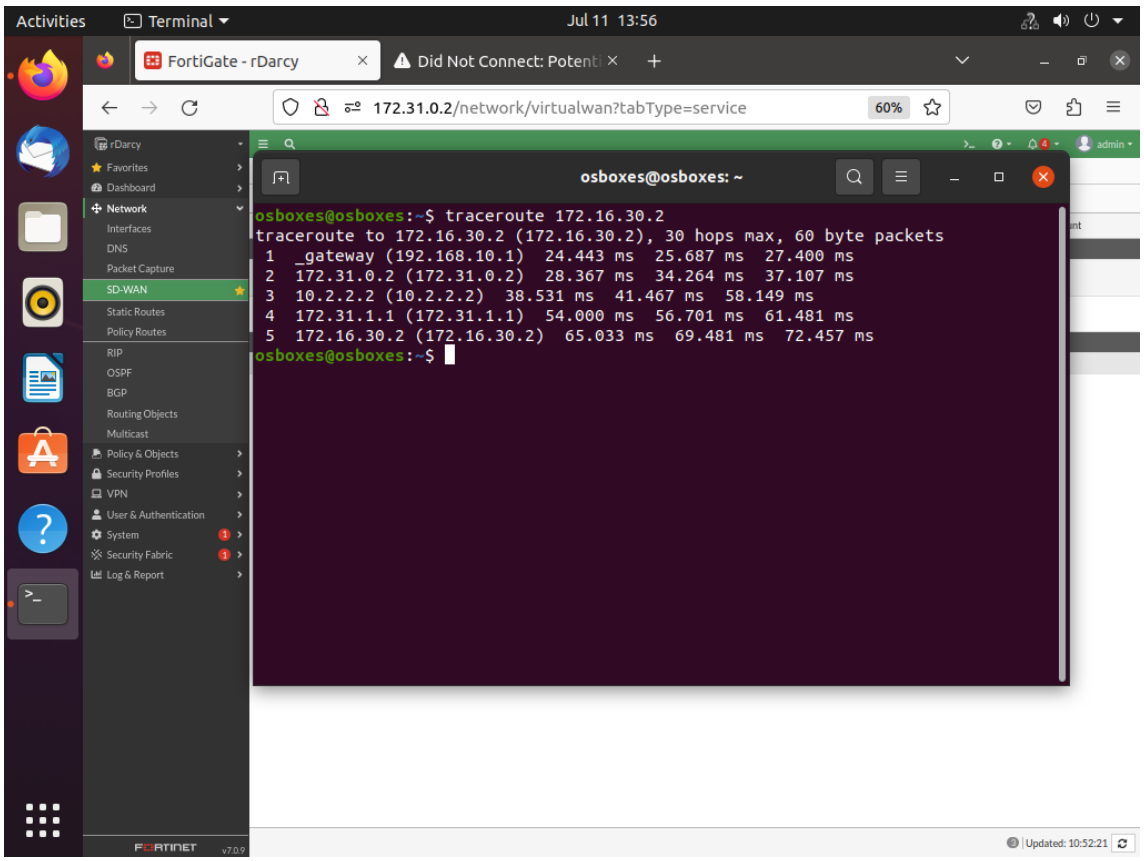


Figura 5.96: Traceroute para ENG com caminho invertido, Fortinet. Fonte: Autor

- Em 5.95 era esperado que todo trafego passasse pelo túnel *"Darcy"*, uma vez que a regra foi invertida, e de fato nota-se que o endereço 10.1.1.1 mostra que isso foi feito.
- Temos que o trafego destinado a rede **172.16.30.2** foi alocado no caminho escolhido em suas configuração, pelo túnel *"Darcy2"* com endereço de loppkback 10.2.2.2.

5.3.6 Análise Geral - Fortinet

Nota-se que há uma complexidade no que se refere a implementação da SDWAN da Fortinet, a mesma possui uma serie de recursos que interferem na simplicidade de implementação para todas os recursos testados o que pode gerar uma certa dificuldade na implementação de funcionalidades simples, como recursos de firewall, túneis IPSec, politicas de QoS etc. Contudo a grande gama de recursos podem ser uteis no que se refere a aplicabilidade, tais recursos podem trazer mais liberdade de escolha e robustez a redes gerenciadas pela SDWAN da Fortinet, quando aplicados de maneira correta.

Apesar de não ser necessário para a SDWAN, o cadastro dos equipamentos no Fortmanager é complexo e demanda do engenheiro um grande nível de conhecimento dos produtos da Fortinet, o que pode ser um problema, podem ser criados grupos e tais grupos podem conter uma serie de dispositivos. Não há muita facilidade de implementação dos equipamentos e seu gerenciamento pode ser um pouco mais complexo do que as propostas de SDWAN existentes no mercado.

O Fortigate conta com uma grande e vasta robustez de recursos para segurança de redes, alguns dele

como*Web Filter*, *Anti Virus* etc. Esses recursos não são do escopo deste trabalho mas é importante ressaltar que segurança de redes é um assunto que vem tomando conta do mercado e essas funções podem ser extremamente uteis e tornam a SDWAN da fortinet mais robusta em segurança.

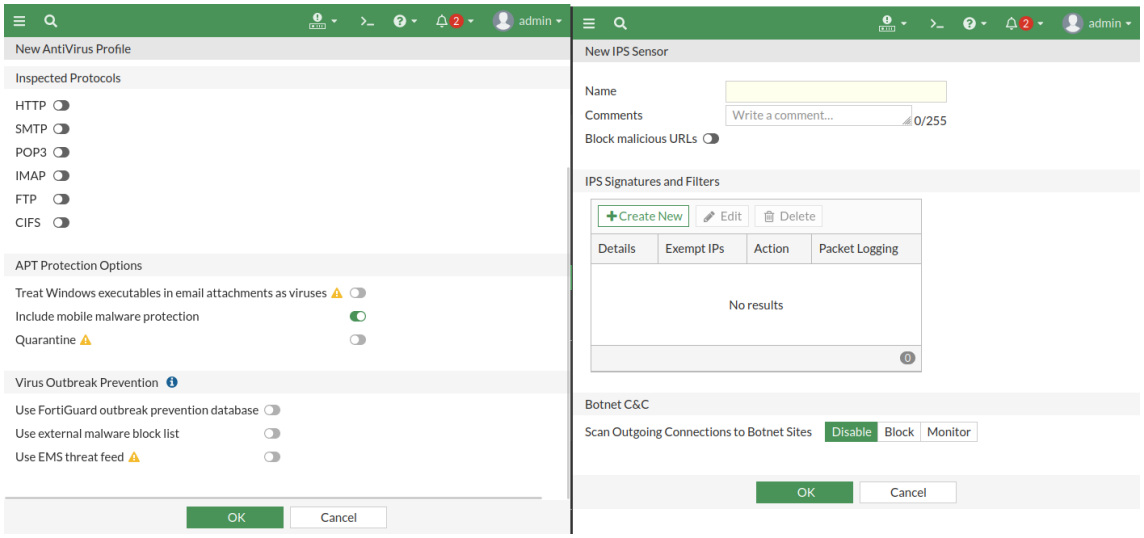


Figura 5.97: Funcionalidade de AntiVirus e Prevenção de Invasor Fortigate. Fonte: Autor

Não há uma nenhuma politica de QoS padrão o que dar uma liberdade na organização das politicas, contudo nota-se que há uma certa complicação no que se diz respeito a configuração das mesmas, podendo não ser muito intuitiva o que pode gerar certa confusão na criação das politicas.

Vale notar que existe uma ferramenta chamada de FortAnalyzer que concentra os dados de toda a rede SDWAN, a mesma não foi implementada dada ao grande numero de RAM necessário para executar toda a topologia, contudo as funcionalidades do dashboard do Fortigate são extensas, além disso os recursos não se limitam ao padrão de fabrica, podem ser adicionadas diversas instancias de análise, e dentro de cada instancia podem ser aplicados filtros de visibilidade que ajudam na identificação de fluxos de rede, os recursos contam com um painel de rotas, monitoramento de velocidade do Link, usuários dentro da rede LAN, uso de CPU e memoria etc. A figura 5.98 ilustra alguns dessas funções.

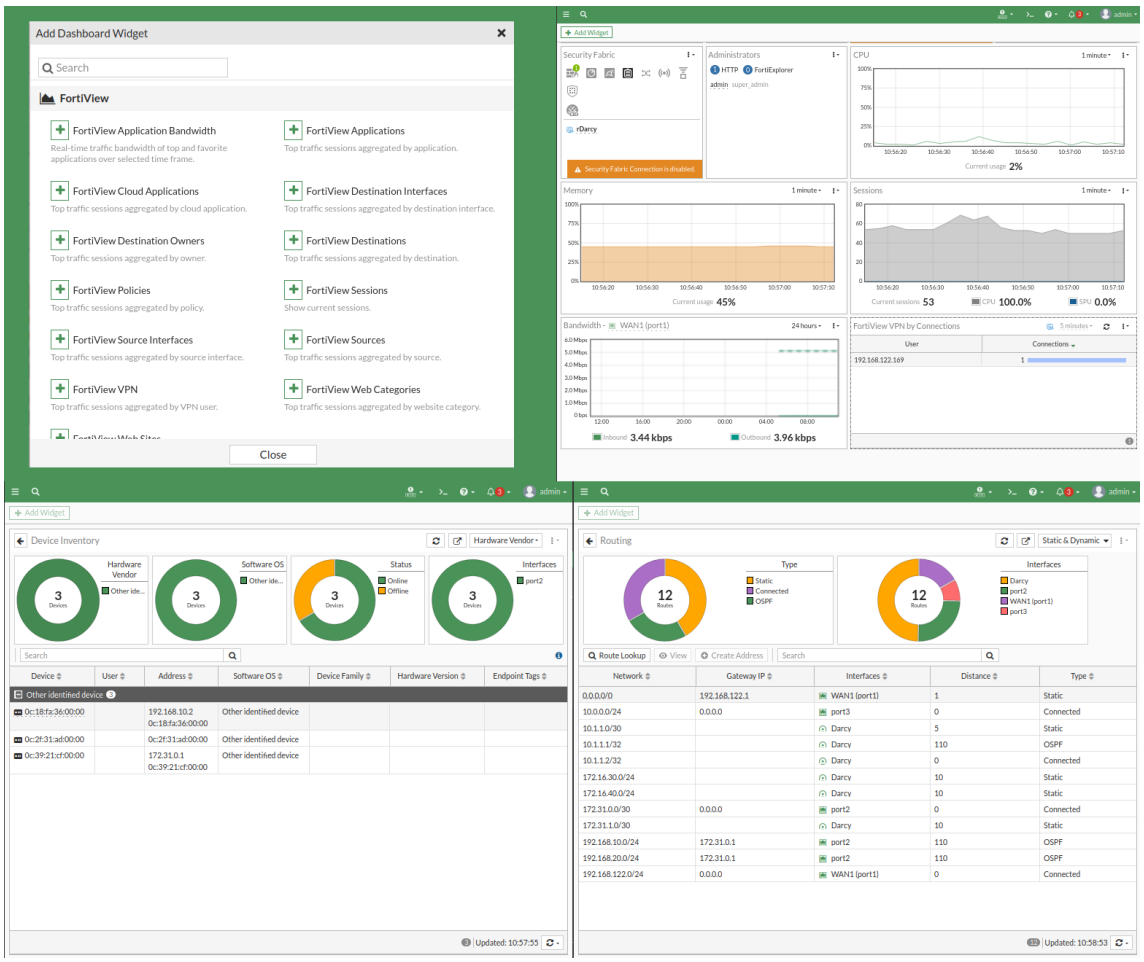


Figura 5.98: Algumas janelas de monitoramento do Fortigate. Fonte: Autor

5.4 ANÁLISE COMPARATIVA

Esta sessão tem como foco a análise comparativa através dos resultados coletados nas sessões acima, o foco será comparar as funcionalidades básicas e tunelamento, QoS, Segurança, Delay dos Túneis e Seleção de Caminho Dinâmico de ambas as soluções.

- **Funcionalidades Básicas e Tunelamento**: Nas seções que abordam as funcionalidades básicas e o tunelamento, foram testadas principalmente as conexões fundamentais da rede e, por fim, o tunelamento. O foco desta parte está na implementação dos dispositivos e na integração da SDWAN. Ambas as soluções exigem uma configuração prévia do dispositivo, seja para cadastrar um token que irá vincular o dispositivo à conta da organização, como na Flexiwan, ou para acessar o Fortigate e configurar a SDWAN, que pode ser feita tanto pelo Fortimanager quanto pelo próprio Fortigate, neste caso específico no Fortigate.

  Vale notar que a solução em nuvem da SDWAN da Fortinet utilizando a Forticloud não está disponível na licença gratuita de 15 dias aplicadas aos dispositivos utilizados na topologia, logo optou-se por fazer a SDWAN baseadas nos Fortigates, contudo existem diversas formas de implementar a

solução SDWAN da Fortinet.

A configuração das interfaces em ambas as soluções possuem os recursos básicos, como identificação de links (WAN/LAN), definição de throughput estimado da rede, configuração DHCP, IP estático e afins. A configuração do protocolo de roteamento abordado, o OSPF, em ambas as soluções é intuitivo e fácil de se entender e por fim de executar, contudo a Fortinet disponibiliza recursos mais robustos de configuração do protocolo, como tipo de ABR (Area Border Router), tipo de link, metric default etc.

A configuração dos túneis providos pela Flexiwan mostrou-se mais fácil e intuitiva. Com apenas alguns cliques e poucas configurações, é possível criar um túnel entre dois dispositivos FlexiEdge. Por outro lado, não conta com recursos mais robustos de escolha de algoritmos e vem habilitado por padrão um método pouco confiável de troca de chaves, o PSK. Já a Fortinet conta com uma ampla gama de opções de algoritmos de autenticação. No entanto, o processo de configuração dos túneis é mais complexo e demanda maior cuidado na criação dos mesmos. O processo realizado neste trabalho foi custoso e não envolveu o uso de uma controladora/orquestrador. Uma vez que a SDWAN pode ser feita dentro do próprio dispositivo, o sentido de ser dinâmica e fornecer uma configuração fácil pode não existir. Além disso, a configuração do FortiManager e a inclusão do mesmo na topologia são necessárias, o que pode alterar o cenário da solução. No entanto, vale notar que a Fortinet é uma empresa privada e oferece diversas soluções, cada uma delas com um nível diferente de funcionalidades disponíveis.

- **QoS**: O QoS de ambas as soluções funcionou como esperado, neste tópico será abordado as duas questões primordiais reparadas em ambas as soluções:
  - **Throughput Alocado**: Utilizando a tabela 5.3 podemos notar que as taxas de acerto são ótimas, contudo a Fortinet alocou mais fielmente os 70% do throughput estimados.

Tabela 5.3: Resultados do QoS para as Soluções Flexiwan e Fortinet

Solução	Throughput Medido	Fluxo 3030	Acerto	Fluxo 5050/6060	Acerto
Flexiwan	$4Mbps$	$2,6Mbps$	$92,86\%$	$1,2Mbps$	100%
Fortinet	$5,14Mbps$	$3,4Mbps$	$94,49\%$	$1,6Mbps$	100%

  - **Facilidade de Implementação**: Por outro lado, no que diz respeito à facilidade de implementação da política, como já citado, a Fortinet apresenta em sua solução processos mais custosos. Muitas vezes, é necessário criar várias regras para a aplicação de um simples QoS. No entanto, ela oferece flexibilidade na criação e exclusão de regras. Por outro lado, a Flexiwan, apesar de ter um processo simples e intuitivo, impõe restrições às regras pré-definidas no Fleximanager. Algumas dessas regras não podem ser excluídas, apenas alteradas. Isso pode limitar a criação de políticas de QoS.
- **Segurança**: No quesito de segurança ambas as soluções tem uma fácil implementação de regras básicas de firewall, que foi o quesito escolhido para análise. Contudo vale ressaltar que a Fortinet, como uma empresa focado para recursos de segurança oferece em sua solução uma grande variações de recursos, como citado, oferece uma proteção Anti-Vírus, recursos para bloquear invasores, bloqueio

por WebFilter. Além disso a Fortinet oferece uma visualização mais clara através do processamento visual de Logs pelo dashboards, informando quantas vezes uma regra foi ativada.

- **Delay dos Túneis**: A partir da tabela 5.4, podemos notar que os túneis criados pela Flexiwan se mostraram mais ágeis, vale notar que ambos os túneis utilizam o protocolo ESP e ainda que o túnel da Flexiwan encapsula os pacotes em uma cabeçalho VxLAN sendo assim um processo mais custoso pois dentro desse processo o protocolo é inserido em um novo cabeçalho VxLAN.

Tabela 5.4: Delay Médio dos Pings

Solução	Delay do Túnel
Flexiwan	$3,172ms$
Fortinet	$5,5ms$

- **Seleção de Caminho Dinâmico**: Os processos feitos em ambas as soluções são os mesmos: a criação de um novo túnel IPsec e em seguida a criação da regra de seleção de caminho, contudo o processo na Fortinet oferece mais opções, inclusive oferece um monitoramento dinâmico do link e além disso pode ser escolhida uma métrica como delay, largura de banda, jittler ou todas juntas, para selecionar o caminho por estado de enlace. A Flexiwan também conta com esse recurso, contudo é limitado e resume todas as métricas em uma única descrita como *"Link State"*, o que não gera flexibilidade na escolha de caminho. Além disso, na Fortinet é possível selecionar o caminho com base no tipo de protocolo da camada de transporte, o que pode oferecer mais flexibilidade para aplicações críticas ou específicas.

6 CONCLUSÃO

Após a analise feita entre as duas tecnologias pode-se concluir que ambas as soluções entregam todos os principais recursos de uma SDWAN, contendo algumas diferenças. A performance medida nos itens descritos para ambas as soluções foram excelentes com apenas algumas variações que dependendo da aplicação podem se tornar irrelevantes.

Durante o processo de construção das SDWAN pode-se reparar que a Fortinet oferece mais ferramentas de segurança voltada para a SDWAN, além de ferramentas de analise de rede mais robustas e completas. Em contraponto possui uma grande dificuldade de implementação e entendimento principalmente quando o Fotimanager está envolvido na topologia, os processos de configuração podem ser trabalhosos dependendo do recurso a ser implementado e as vezes pode não ser muito intuitivo, isso já era de se esperar dada que a solução é mais completa e mexe com software proprietário. Além disso a SDWAN da Fortinet conta com diferentes níveis de recursos, que variam de acordo com o pacote a ser adquirido, muitas vezes demanda mais de um equipamento (Fortigate, Fortianalyzer e Fortimanager), isso pode se tornar um limitador no que se refere aos custos e recursos disponíveis na implementação de uma SDWAN. Além disso temos que a solução usada pela Fortinet para este trabalho ainda utiliza grande parte das suas configurações locais, o que para uma rede pequena como a utilizada nesta pesquisa pode ser implementável, mas redes de larga escala com muitos sites é necessário a inclusão do Fortimanager e Fortianalyzer para facilitar a configuração.

O processo de construção da SDWAN da Flexiwan é bem mais simples, isso se da em parte pelo gerenciamento em nuvem e pela própria simplicidade da solução, essa simplicidade se refere no processo de criação de politicas de firewall, QoS e tuneis e nas configurações dos dispositivos. Os processo de configurações dentro da solução são mais direitos comparados ao processos da Fortinet.

De maneira geral ambas as soluções entregam performances parecidas para a rede analisada variando apenas na complexidade de configuração, contudo vale ressaltar que apesar de ambas as soluções possuírem a documentação de seus dispositivos aberta e de fácil acesso a Fortinet por ser mais complexa e conter mais recursos possui uma serie de certificações que progridem de acordo com o nível de conhecimento, essas certificações ajudam a entender melhor a dinâmica da solução oferecida pela empresa.

A utilização de código aberto em produtos pode expandir a pesquisa e além disso prove mais transparência ao usuário que esta utilizando, além disso a partir dos resultados coletado neste trabalho pode-se concluir que a utilização de soluções open source não é um fator limitador e não traz nenhum tipo de prejuízo no que se refere a performance da topologia, possui uma fácil implementação e excelentes resultados. Na topologias analisada ambas as soluções se encaixaram bem e trouxeram os benefícios e recursos de uma SDWAN, contudo vale ressaltar uma solução pode se adequar ou não a uma topologia, isso varia com o projeto.

6.1 TRABALHOS FUTUROS

Proponho para trabalhos futuros uma pesquisa mais aprofundada nos métodos utilizados por tecnologias open source para criação de uma SDWAN, como quais tuneis utilizar, tipo de criptografia, protocolos, APIs etc.

Proponho também uma analise de segurança aprofundada no nível de segurança das mensagens trocadas entre a controladora e elementos da rede, a fim de medir o nível de seguranças das mensagens quando as mesmas trafegam pela a internet aberta, seguindo da análise do tempo de resposta para o update das politicas atribuídas pelo orquestrador nos elementos de rede.

Até a presente data desta pesquisa apenas uma tecnologia SDWAN open source, totalmente aberta foi encontrada, a EveryWAN, proponho um tema de mestrado relacionado a criação de uma tecnologia SDWAN totalmente aberta e disponível para todos, seguindo todos os requisitos de uma SDWAN e utilizando códigos open source para que a mesma seja suscitável a constantes atualizações.

REFERÊNCIAS BIBLIOGRÁFICAS

Best SDWAN SOFTWARES BEST SDWAN SOFTWARES. <https://www.g2.com/categories/sd-wan>. (Acessado em 15/02/2023).

Conrad Menezes et al. 2014 Conrad Menezes et al. *Software-Defined WAN Use Case*. [S.l.], 2014. 10 p. Disponível em: <{https://www.onug.net/wp-content/uploads/2015/05/ONUG-SD-WAN-WG-Whitepaper_Final1.pd}.>

F.Kurose 2014 F.KUROSE, K. W. R. J. Redes de computadores e a internet. In: PEARSON. *Redes de Computadores e a Internet: uma abordagem top-down . 6 ª Edição*. [S.l.], 2014. p. 26–29,145–198, 357–359.

Fleiwan Fleiwan. *The World's First Open Source SD-WAN SASE*. <https://flexiwan.com/>. [Acessado em 02 de fevereiro de 2023].

Flexiwan 2019 FLEXIWAN. *FlexiWAN SD-WAN Open Surce Overview*. 2019. <https://flexiwan.com/wp-content/uploads/2019/08/flexiWAN-SD-WAN-Open-Source-Overview.pdf>. (Acessado em 02/02/2023).

FlexiWan Components FLEXIWAN Components. <https://gitlab.com/flexiwangroup>. (Acessado em 31/05/2023).

Force 1198 FORCE, I. E. T. *OSPF Version 2*. 1198. <https://www.ietf.org/rfc/rfc2328.txt>. (Acessado em 31/05/2023).

Force 2005 FORCE, I. E. T. *Security Architecture for the Internet Protocol*. 2005. <https://www.ietf.org/rfc/rfc4301.txt>. (Acessado em 31/05/2023).

Fortinet 2023 Fortinet. *Administration Guide, FortiOS 7.0.9*. 2023. <https://docs.fortinet.com/document/fortigate/7.0.9/administration-guide/954635/getting-started>. Acesso em: 11 de Julho de 2023.

Fortinet 2023 Fortinet. *Next Generation Firewall*. 2023. <https://www.fortinet.com/products/next-generation-firewall>. Acesso em: 17 Julho 2023.

Foundation 2023 FOUNDATION, W. *Wireshark Documentation*. 2023. <https://www.wireshark.org/docs/>. Acesso em: 26 de junho de 2023.

Frankel Karen Kent 2005 FRANKEL KAREN KENT, R. L. A. D. O. R. W. R. S. R. S. S. Guide to ipsec vpns. National Institute os Standards and Technology, 2005.

Garcia 2023 GARCIA, J. *ANÁLISE DE SOLUÇÃO OPEN SOURCE PARA A IMPLEMENTAÇÃO DE UMA REDE SD-WAN EM AMBIENTE CONTROLADO*. Monografia — Universidade de Brasília, DF, Fevereiro 2023.

GNS3 Documentation GNS3 Documentation. <https://docs.gns3.com/>. Acessado em: 15/05/2023.

Group 1197 GROUP, N. W. *Dynamic Host Configuration Protocol*. 1197. <https://datatracker.ietf.org/doc/html/rfc2131>. (Acessado em 31/05/2023).

iperf3 Documentation IPERF3 Documentation. <https://iperf.fr/iperf-doc.php>. (Acessado em 31/05/2023).

Laliberte 2023 LALIBERTE, B. *The Importance of Network Visibility and Analytics for Zero Trust Initiatives*. 2023. <https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/esg-importance-network-visibility.pdf>. Acesso em: 17 de Julho de 2023.

Mahalingam et al. 2014 MAHALINGAM, M.; DUTT, D.; DUDA, K.; AGARWAL, P.; KREEGER, L.; SRIDHAR, T.; BURSELL, M.; WRIGHT, C. *Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks*. 2014. IETF-RFC 7348.

Nadeem e Karamat 2016 NADEEM, M. A.; KARAMAT, T. A survey of cloud network overlay protocols. In: *2016 Sixth International Conference on Digital Information and Communication Technology and its Applications (DICTAP)*. [S.l.: s.n.], 2016. p. 177–182.

Odom 2020 ODOM, W. *CCNA Cisco Press 200-301 Volume 1*. 1. ed. Indianapolis: Cisco Press, 2020. 494-521 p.

Odom 2020 ODOM, W. *CCNA Cisco Press 200-301 Volume 2*. 1. ed. Indianapolis: Cisco Press, 2020. 52–62, 336 – 344 p.

Postel 1981 POSTEL, J. *Transmission Control Protocol*. [S.l.], 1981. Disponível em: <https://tools.ietf.org/html/rfc793>.

Red Hat Red Hat. *What is SD-WAN?* <https://www.redhat.com/pt-br/topics/edge-computing/what-is-sd-wan>. [Acessado em 25 de junho de 2023].

Scarpitta et al. 2021 SCARPITTA, C. et al. Everywan - an open source sd-wan solution. IEEE, 2021.

Segeč et al. 2020 SEGEč, P.; MORAVčIK, M.; URATMOVá, J.; PAPáN, J.; YEREMENKO, O. Sd-wan - architecture, functions and benefits. In: *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*. [S.l.: s.n.], 2020. p. 593–599.

Sturt 2023 STURT, R. *Who are the best SD WAN Providers? (Build your list)*. 2023. Disponível em: <https://www.netify.com/learning/who-are-the-best-sd-wan-providers>.

Switching Wired Access SWITCHING Wired Access. <https://www.extremenetworks.com/products/extremeswitching/>. (Acessado em 31/05/2023).

What is SD-WAN WHAT is SD-WAN. <https://www.arubanetworks.com/faq/what-is-sd-wan>. (Acessado em 31/01/2023).

Xia et al. 2015 XIA, W.; WEN, Y.; FOH, C. H.; NIYATO, D.; XIE, H. A survey on software-defined networking. *IEEE Communications Surveys Tutorials*, v. 17, n. 1, p. 27–51, 2015.

Yalda, Hamad e Ţăpuş 2022 YALDA, K. G.; HAMAD, D. J.; ŢăPUş, N. A survey on software-defined wide area network (sd- wan) architectures. In: *2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*. [S.l.: s.n.], 2022. p. 1–5.

Yuniarto e Sari 2021 YUNIARTO, R.; SARI, R. F. Performance analysis of multipath deployment in software-defined wide area network (sdwan). In: *2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST)*. [S.l.: s.n.], 2021. p. 124–128.