CENTRO UNIVERSITÁRIO UNIFECAF
GESTÃO TECNOLOGIA DA INFORMAÇÃO

Dannyelly Dayane Queiroz

Projeto de Expansão e Diagnóstico de Rede para Conexão Segura entre Unidades

Taboão da Serra, SP

2024

DANNYELLY DAYANE QUEIROZ

PROJETO DE EXPANSÃO E DIAGNÓSTICO DE REDE PARA CONEXÃO SEGURA ENTRE UNIDADES

Trabalho apresentado como requisito parcial de avaliação da disciplina **Computer Network** do Curso de Graduação em **Gestão Tecnologia da Informação** do Centro Universitário UniFECAF.

Tutor(a): **Marcel Teixeira**

Taboão da Serra, SP

Sumário

LISTA DE FIGURAS

LISTA DE ABREVIATURAS

DNS (Domain Name System) –

Sistema de nomes de domínio, que traduz nomes de domínio em endereços IP.

LAN: Local Area Network (Rede de Área Local) –
Rede que interliga computadores e dispositivos em uma área geográfica restrita, como um escritório, prédio ou casa.

WAN: Wide Area Network (Rede de Área Ampla) –
Rede que se estende por uma grande área geográfica, conectando redes LAN em diferentes localidades.

TCP: Transmission Control Protocol (Protocolo de Controle de Transmissão) –
Protocolo de comunicação que garante a entrega confiável de dados em redes de computadores.

IP: Internet Protocol (Protocolo da Internet) –
Protocolo que define o endereçamento e roteamento de pacotes de dados em redes de computadores.

UDP: User Datagram Protocol (Protocolo de Datagrama do Usuário) - Protocolo de comunicação que oferece um serviço de entrega de dados sem conexão, priorizando a velocidade em detrimento da confiabilidade.

HTTP: Hypertext Transfer Protocol (Protocolo de Transferência de Hipertexto) –
Protocolo utilizado para a comunicação na World Wide Web, permitindo a transferência de páginas da web.

HTTPS: Hypertext Transfer Protocol Secure (Protocolo de Transferência de Hipertexto Seguro) - Versão segura do HTTP, que utiliza criptografia para proteger as comunicações entre o cliente e o servidor.

DNS: Domain Name System (Sistema de Nomes de Domínio) –
Sistema que traduz nomes de domínio em endereços IP, facilitando o acesso a sites na internet.

SMTP: Simple Mail Transfer Protocol (Protocolo Simples de Transferência de Mensagens) - Protocolo utilizado para enviar e-mails.

IMAP/POP3: Internet Message Access Protocol/Post Office Protocol version 3 (Protocolo de Acesso a Mensagens de Internet/Protocolo de Escritório Postal versão 3) –
Protocolos utilizados para receber e-mails.

ICMP: Internet Control Message Protocol (Protocolo de Mensagens de Controle da Internet) - Protocolo utilizado para testar a conectividade de redes e diagnosticar problemas.

DHCP: Dynamic Host Configuration Protocol (Protocolo de Configuração Dinâmica de Host) - Protocolo utilizado para atribuir automaticamente endereços IP a dispositivos em uma rede.

MAC: Media Access Control (Controle de Acesso ao Meio) - Identificador único atribuído a cada

dispositivo de rede, utilizado para comunicação em uma rede local.

WAN (Wide Area Network): Rede de longa distância que cobre grandes áreas geográficas.

1. INTRODUÇÃO

Com o avanço da organização, uma empresa de médio porte decidiu abrir uma nova unidade em outro estado, uma decisão estratégica para aumentar sua presença no mercado e otimizar o atendimento aos clientes. A integração desta nova filial à infraestrutura da rede da matriz é essencial, já que a unidade central hospeda um sistema ERP (Enterprise Resource Planning), responsável pelo gerenciamento dos principais processos internos da organização.

Para essa comunicação, será necessária a implementação de uma rede WAN (Wide Area Network), conectando a matriz e a filial com segurança, estabilidade e agilidade. Uma vez que a rede LAN seria inviável geograficamente.

Esse projeto será estruturado em uma rede WAN que permitirá o acesso contínuo e protegido ao sistema ERP, considerando a qualidade e a segurança entre as unidades.

Além disso, a matriz enfrenta desafios de conectividade intermitente, que precisam ser solucionados para não comprometer o desempenho e a confiabilidade do sistema ERP.

A solução proposta visa, portanto, não só a conexão entre as unidades, mas também o aprimoramento da estabilidade da rede existente na matriz.

2. OBJETIVO DO PROJETO

O cenário corporativo está cada vez mais dependente da tecnologia, e as redes de computadores desempenham um papel fundamental na comunicação e na manipulação dos dados.

Este projeto visa aprimorar uma rede de comunicação eficiente e segura para conectar duas unidades de uma empresa de porte médio, garantindo uma infraestrutura de rede que atenda às demandas operacionais e de segurança.

O projeto contempla os seguintes objetivos específicos:

- Projetar uma rede eficiente e segura para conectar as duas unidades da empresa
- Diagnosticar e resolver problemas de conectividade nas redes existentes, promovendo melhorias na estabilidade e no desempenho da comunicação em ambas as unidades.
- Aplicar conceitos de segurança de redes, incluindo criptografia e protocolos de conectividade segura, para proteger os dados e garantir a privacidade das informações durante a troca entre as unidades.
- Analisar a viabilidade técnica e econômica das soluções propostas, avaliando o equilíbrio entre desempenho, custo e benefícios para garantir uma

implementação sustentável e ajustada às necessidades do negócio.

- Desenvolver um plano de ação detalhado, que considere todos os recursos necessários, um cronograma de execução bem estruturado e a alocação de equipes específicas para cada etapa, visando uma implementação eficiente e organizada.

2. PLANO DE AÇÃO

2.1. Identificação dos envolvidos

2.1.1. Gerente de TI

Responsável pela coordenação geral do projeto, garantindo que todas as etapas sejam cumpridas dentro do prazo e que os recursos sejam adequadamente alocados.

2.1.2. Equipe de TI Interna

Responsável pela configuração da rede, incluindo roteadores, firewalls, servidores e implementação da VPN.

2.1.3. Consultores de Rede e Segurança

Profissionais especializados que auxiliarão na configuração da VPN, garantindo que a comunicação entre a matriz e a filial seja segura, e na auditoria da segurança da rede.

2.1.4. Equipe de Suporte Técnico

Responsável pela manutenção pós-implementação, monitoramento da rede e resolução de problemas que possam surgir após a instalação da infraestrutura.

2.1.5. Equipe de Compras

Responsável pela aquisição dos equipamentos de rede, servidores e licenças de software.

2.1.6. Recursos Humanos

Responsável pelo treinamento da equipe interna sobre segurança.

2.2.Cronograma do projeto

A seguir a tabela, com o cronograma do projeto, com inicio em Janeiro.

Tabela 1- Cronograma do projeto

Atividade	Responsável	Data de Início	Data de Término	Duração Estimada
Planejamento do projeto	Gerente de TI / Consultores	01/01/2025	05/01/2025	5 dias
Aquisição de equipamentos e licenças	Compras / TI	06/01/2025	15/01/2025	10 dias
Configuração do roteador e firewall	Equipe de TI	16/01/2025	20/01/2025	5 dias
Implementação da VPN (configuração IPsec)	Consultores / TI	21/01/2025	25/01/2025	5 dias
Instalação de servidores e sistemas	Equipe de TI / Suporte	26/01/2025	31/01/2025	6 dias
Testes de conectividade e segurança	Equipe de TI / Consultores	01/02/2025	05/02/2025	5 dias
Treinamento da equipe de suporte	Recursos Humanos / TI	06/02/2025	07/02/2025	2 dias
Monitoramento e ajustes pós-implementação	Equipe de TI	08/02/2025	14/02/2025	7 dias

Fonte- Autoria Própria

3. ANÁLISE DAS NECESSIDADES

De acordo com Openhaimer (2010):

> Nesta fase, o analista de rede entrevista usuários e pessoal técnico para entender os objetivos de negócios e técnicos para um novo sistema ou um sistema aprimorado. A tarefa de caracterizar a rede existente, incluindo a topologia lógica e física e o desempenho da rede, vem a seguir.

Desta forma, com base nas informações disponíveis sobre a empresa, será realizada uma análise detalhada para entender os objetivos de negócios e os requisitos técnicos da nova infraestrutura de rede.

3.1.Objetivos de Negócios

A empresa enfrenta dificuldades com interrupções frequentes e latência, o que prejudica a operação no ERP. Além disso, sabemos que a a organização está integrando uma nova filial na rede da matriz. .

Sendo assim, os objetivos técnicos definidos neste projeto visam assegurar que a nova infraestrutura de rede não apenas atenda aos requisitos de desempenho da empresa, mas também incorpore as melhores práticas de segurança, garantindo um ambiente de comunicação confiável e eficiente.

Segue os objetivos de negócios para o projeto de rede entre matriz e filial:

- **Aumentar a Eficiência Operacional:** Proporcionar uma comunicação rápida e confiável entre a matriz e a filial, reduzindo o tempo de resposta e melhorando a colaboração entre as equipes.
- **Fortalecer a Integração de Processos:** Garantir que a filial tenha acesso pleno ao sistema ERP da matriz, permitindo que todas as operações sejam alinhadas e integradas, o que resulta em maior agilidade e precisão na tomada de decisões.
- **Identificar a melhor solução para conectividade:** Propor uma solução de rede WAN baseada em tecnologia de VPN, que permite uma comunicação segura e eficiente, aproveitando a infraestrutura existente e alinhando-se aos requisitos técnicos da empresa.
- **Analisar a viabilidade técnica:** A solução proposta será tecnicamente viável, utilizando equipamentos compatíveis com a infraestrutura já disponível, garantindo uma transição suave e minimizando a necessidade de investimentos em novos recursos.
- **Garantir segurança da comunicação:** Implementar medidas robustas de segurança, como criptografia e firewalls, para assegurar que a comunicação entre as unidades seja protegida contra ameaças externas e internas.
- **Avaliar custo-benefício:** Considerar o equilíbrio entre o custo de implementação e a manutenção da solução proposta, assegurando que os recursos sejam utilizados de forma eficiente e que o retorno sobre o investimento seja positivo.
- **Assegurar estabilidade e escalabilidade:** A solução deve garantir uma conexão estável, com suporte a um aumento futuro de demanda, permitindo que a rede se adapte ao crescimento da empresa sem comprometer a qualidade do serviço.

3.2.Objetivos Técnicos

Os objetivos técnicos deste projeto serão para estruturar uma infraestrutura de rede eficaz, segura e alinhada às necessidades operacionais da empresa.

Os objetivos incluem:

- **Projetar uma Rede WAN Segura**: Implementar uma solução de rede WAN que utilize tecnologia de VPN para garantir comunicação segura entre a matriz e a filial, protegendo dados sensíveis durante a transmissão.

- **Realizar Diagnósticos de Conectividade**: Identificar e resolver problemas de conectividade existentes na infraestrutura atual, assegurando que a rede opere de maneira estável e eficiente.
- **Analisar Custo-Benefício**: Avaliar o custo de implementação e manutenção da solução proposta, garantindo que os investimentos feitos sejam justificados pelos benefícios que a nova infraestrutura trará.
- **Assegurar Estabilidade da Conexão**: Desenvolver uma rede que garanta uma conexão estável, minimizando quedas e latências, para que a comunicação entre a matriz e a filial seja contínua e eficaz.

4. DESENVOLVIMENTO DO PROJETO

4.1.Melhor Solução para o Problema de Conectividade

A solução de VPN é a mais adequada para o caso da Matriz e Filial, principalmente devido ao seu excelente custo-benefício. Implementar uma VPN utilizando a infraestrutura existente de internet pública na matriz é significativamente mais barato do que contratar links dedicados ou MPLS, o que atende perfeitamente às necessidades da empresa. Além disso, a manutenção dessa rede será mais acessível, proporcionando economia a longo prazo.

A VPN garante a segurança da comunicação entre as unidades por meio da criptografia dos dados, protegendo informações sensíveis de forma eficaz. Essa solução também é altamente escalável, o que permitirá que, no futuro, outras filiais sejam adicionadas à rede sem a necessidade de grandes investimentos em infraestrutura. Isso torna a VPN uma escolha estratégica e eficiente para o projeto.

4.2.Topologias da Rede:

Segundo Forouzan, "topologia é a maneira pela qual uma rede é organizada fisicamente, sendo a representação geométrica da relação de todos os links e os dispositivos de uma conexão". Existem quatro topologias básicas possíveis: barramento, anel, malha e estrela.

Embora todas essas topologias tenham suas particularidades e aplicações específicas, a topologia estrela é considerada a mais adequada para a empresa.

A escolha da topologia em estrela foi baseada em suas vantagens em termos de escalabilidade, facilidade de manutenção e desempenho, características indespensaveis para a empresa.

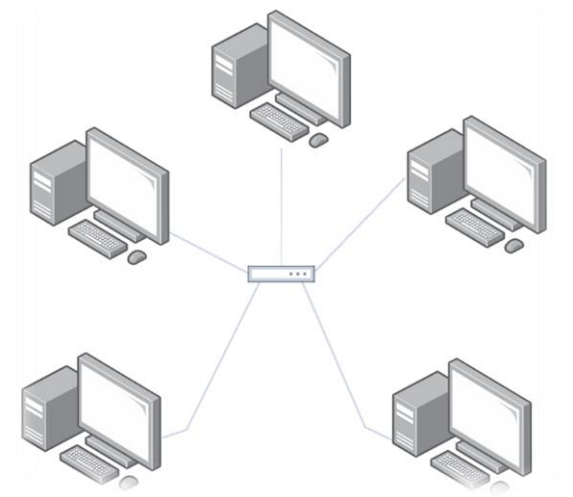
A topologia estrela se caracteriza em um nó central, e toda a informação gerada pelas estações de trabalho deve passar pelo nó, sendo ele um *hub, switch.*

De acordo com Marcelo, “a topologia estrela se diferencia dos demais por possuir a inteligência para distribuir o tráfego de rede para os demais computadores da rede. Esse nó central, é o responsavel pelo trafego e se conecta a todos os outros dispositivos”.

A vantagem dessa topologia está, principalmente na facilidade de gerenciamento, pois é fácil adicionar ou remover dispositivos sem afetar o restante da rede, além de que, caso um dispositivo falhe, os outros continuarão funcionando pois os dispositivos estão conectados individualmente.

Porém, apesar de muito usada, é necessário levar em conta as desvantagens, na topologia estrela caso o nó central fique inoperente, todos os dispositivos irão falhar.

Figura 1- Topologia Estrela



Fonte – Autoria Própria

4.3.Diferenças da WAN e LAN

De acordo com Tanenbaum (2021):

“Uma rede a longa distancia, ou WAN (Wide Area Network), abrange uma grande area geográfia, com frequência um país, continente ou até mesmo vários continentes..”

As WANs podem ser utilizadas para interligar várias LANs, permitindo que redes geograficamente distantes se conectem. E essa interconexão será essencial para a empresa de médio porte, pois possibilitará uma comunicação eficiente e o compartilhamento de recursos.

A rede LAN (Local Area Network) é uma rede que abrange uma área geograficamente limitada, como um escritório, um prédio, uma casa ou um campus universitário.

De acordo com Tanenbaum (2021), as redes LANs são muito usadas para conectar computadores pessoais e aparelhos eletronicos, para permitir que compartilhem recursos e troquem informações.

Sendo assim, para a conexão da Matriz para a Filial usaremos a rede WAN, tendo em vista que as unidades estão localizadas em estados diferentes, e cada filial terá sua **LAN**, onde os dispositivos (como computadores, impressoras, etc.) estarão interconectados em uma rede interna.

4.4.Protocolos de rede

O uso de protocolos de rede é fundamental para estabelecer uma comunicação eficiente e segura entre dispositivos. De acordo com TANENBAUM (2021), "um protocolo é um acordo acordo entre as partes que se comunicam, estabelecendo como se dará a comunicação."

Segundo Barreto, "é preciso que o estabelecimento dessa comunicação seja feito de maneira padronizada, possibilitando que equipamentos diferentes troquem informações uns com os outros"

Sendo assim, os protocolos de rede são regras e padrões para troca de informações em uma rede, garantindo que dados sejam transmitidos e recebidos corretamente entre computadores, servidores e outros equipamentos conectados.

De acordo com Barretos (2020), "elas são representadas por meio de camadas em um modelo funcional que é colocado em pratica por programas chamados protocolos."

4.5.Diferença dos modelos TCP IP e OSI

De acordo com Tanenbaum, (2021), "o modelo OSI e TCP/IP tem muito em comum. Ambos se baseiam no conceito de pilhas de protocolos independentes. Além disso, as camadas tem praticamente as mesmas funcionalidades."

Segundo Tanenbaum, "o ponto forte do modelo OSI é o modelo propriamente dito, que provou ser excecionalmente útil para discussão de rede de computadores." De acordo com ele, o modelo OSI se tornou uma referência fundamental para discutir, estudar e desenvolver redes de computadores pois o OSI organiza a comunicação em redes de forma sistemática, dividindo-a em sete camadas bem definidas, sendo elas: Aplicação, Apresentação, Sessão, Transporte, Rede, Enlace de Dados e Física

Cada camada tem funções específicas, o que torna mais fácil entender, projetar e explicar como os dados trafegam em uma rede.

Por outro lado, de acordo com Tanenbaum, "o ponto forte do modelo TCP/IP são os protocolos, que tem sido bastante utilizado." Os protocolos têm um desempenho comprovado e são robustos, tornando o modelo TCP/IP mais relevante para aplicações reais. O modelo TCP/IP não busca a perfeição teórica, mas sim a eficácia prática. E foi desenvolvido com o foco em interconectar redes de todo o mundo.

O Modelo TCP/IP (Transmission Control Protocol/Internet Protocol) se tornou o padrão de comunicação em redes, sendo amplamente utilizado como uma alternativa prática e simplificada ao modelo OSI. Ele descreve como os dados são transmitidos e recebidos entre os dispositivos em uma rede, e ele será o modelo escolhido entre a matriz e a filial da empresa.

4.5.1. Camadas do Modelo TCP/IP

O modelo TCP/IP possui 4 camadas, sendo elas: Camada de acesso à Rede, Camada de Internet, Camada de Transporte e Camada de Aplicação.

A seguir, explicaremos cada camada e os protocolos escolhidos para o projeto

4.5.2. Camada de Internet

Nesta camada, o protocolo principal é o IP (Internet Protocol), que define o caminho dos dados entre os dispositivos conectados à rede, como entre a matriz e a filial. O IP garante que cada pacote de dados seja enviado ao destino correto. Para isso, são utilizados endereços IP públicos, já que a comunicação entre a matriz e a filial ocorre através de uma VPN, com roteadores configurados para encaminhar os pacotes entre as unidades. Como a comunicação entre a matriz e a filial ocorre através de uma VPN (Virtual Private Network), os roteadores das duas unidades serão configurados para encaminhar os pacotes de dados entre elas de forma segura.

Também será aplicado o protocolo IPsec (Internet Protocol Security) utilizado na VPN para garantir a segurança da comunicação, oferecendo criptografia, autenticação e integridade dos dados em trânsito. Isso criará um "túnel" seguro, protegendo os dados de interceptações e garantindo que apenas dispositivos autorizados possam acessar as informações.

Além deles, será aplicado o protocolo ICMP (Internet Control Message Protocol), que auxilia no diagnóstico e controle de rede, permitindo verificar a conectividade e a resposta de dispositivos.

4.5.3. Camada de Transporte

A camada de Transporte é responsável por garantir que os dados sejam entregues de forma confiável e eficiente.

E para garantir que os dados, como os acessos ao ERP e transferências de arquivos, sejam entregues corretamente entre as unidades da empresa, utilizaremos o TCP e o UDP. O TCP é essencial para garantir a entrega confiável dos dados. Ele fragmenta os dados em pacotes e controla o fluxo para que cheguem na ordem correta. Este protocolo é ideal para aplicações onde a integridade dos dados é crítica, como no acesso ao sistema ERP ou na transferência de arquivos entre a matriz e a filial. O UDP é utilizado para serviços que exigem maior velocidade e podem

tolerar perdas eventuais de pacotes, como transmissões de vídeo e voz em tempo real.

4.5.4. Camada de Aplicação

Os protocolos implementados nessa camada para a comunicação segura entre as unidades são o HTTPS para garantir que as transmissões de dados, como acessos ao sistema ERP, sejam criptografadas. O DNS será usado para resolver nomes de domínio de forma correta, e o SMTP e IMAP/POP3 eles permitirão a troca de e-mails entre as unidades da empresa.

4.5.5. Camada de Acesso à Rede

A Camada de Acesso à Rede é responsável pela transmissão de dados entre dispositivos, como a comunicação local das unidades da empresa. Ela inclui tecnologias como Ethernet (para redes cabeadas) e Wi-Fi (para conexões sem fio). Além disso, essa camada gerencia o endereçamento físico dos dispositivos, utilizando endereços MAC para identificar os dispositivos na rede.

A comunicação entre a matriz e a filial será gerida pela VPN configurada, com a utilização de IP público e protocolos de segurança para garantir a privacidade e integridade dos dados.

4.6.VPN (Virtual Private Network)

Uma VPN (Virtual Private Network) é uma rede privada criada sobre uma rede pública, como a internet. No caso da matriz e da filial, a VPN será utilizada para garantir uma comunicação segura e eficiente entre as duas unidades da empresa.

Segundo Lacerda, “as VPNs geralmente são criadas sobre redes públicas como a internet ou a rede telefônica pública. Uma VPN conta com autenticação do usuário e um sistema de criptografia, oferecendo suporte a serviços de intranet.” Além disso, conforme o autor, "a VPN criptografa os dados, empacota-os em um pacote IP para compatibilidade com a internet e os envia, por um túnel, para então serem descriptografados na outra extremidade.”

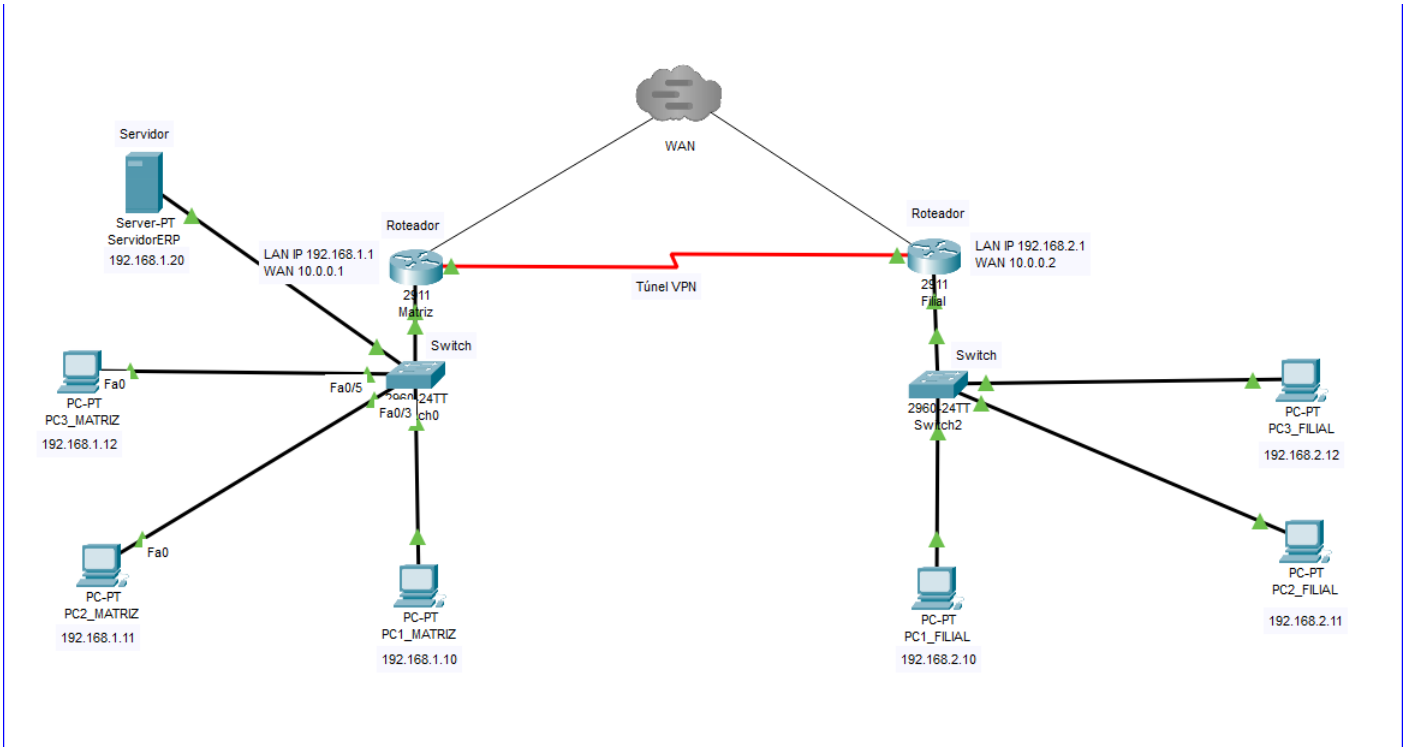
A VPN criará um túnel seguro entre as redes locais de cada unidade, criptografando os dados transmitidos e permitindo que os dispositivos de uma unidade se conectem à outra de forma transparente, como se estivessem na mesma rede local.

Dessa forma, o túnel VPN será configurado nos roteadores da matriz e da filial para garantir a comunicação segura entre as unidades. Isso assegura que informações sensíveis, como dados do sistema ERP ou e-mails corporativos, sejam transmitidas de forma protegida. A configuração utilizará endereços IP públicos e o protocolo IPSec, garantindo a criptografia, a integridade e a confidencialidade dos dados durante o tráfego.

5. DIAGRAMA DA REDE

No diagrama a seguir, mostrarei os aspectos lógicos da rede, como por exemplo o fluxo de informações. Ele mostra como a comunicação flui entre os diferentes dispositivos e como cada dispositivo será conectado.

Figura 2- Diagrama da rede



Fonte – Autoria Própria. Criado pelo aplicativo Cisco Packet Tracer.

6. EQUIPAMENTOS E CONFIGURAÇÕES

A seguir, está a tabela com todos os equipamentos que serão utilizados na matriz e filial, funções e as configurações principais de cada um.

Tabela 2- Equipamentos

Equipamento	**Localização**	**Função**	**Configurações Principais**
2 Roteadores	Matriz/filial	Encaminha o tráfego de dados entre a rede local e a VPN entre a matriz e a filial.	Endereçamento IP da Matriz e Filial Configuração de VPN (IPSec) Protocolo de roteamento (RIP)
2 Switchs	Matriz/filial	Conectará os dispositivos locais da Matriz e Filial(computadores, servidores, etc.) dentro da rede LAN.	Configuração de VLANs para segmentação de tráfego Portas de acesso para conectar dispositivos
1 Servidor	Matriz	Hospedagem do sistema ERP, e-mail e outros serviços essenciais.	Backup regular de dados importantes, incluindo dados de aplicações e sistemas operacionais. Atribuição de um endereço IP fixo ao servidor para garantir que sua localização na rede seja sempre a mesma.
Firewall	Matriz / Filial	Protege a rede interna contra acessos não autorizados e garante a segurança da VPN.	Configuração de VPN e monitoramento de tráfego
PCs	Matriz / Filial	Usuários finais que acessam os sistemas e serviços fornecidos pela rede.	Conexão via cabo Ethernet
Cabos Cat 6	Matriz/ Filial	Fará a conexão dos roteadores, switches e computadores.	-

Fonte: Autoria Própria

7. CONEXÃO ENTRE MATRIZ E FILIAL:

A matriz e a filial serão conectadas por um link WAN entre os roteadores. E para garantir segurança, e utilizaremos uma VPN com rotas estáticas.

7.1.Roteadores

Em cada roteador, será configurado rotas estáticas para garantir que os pacotes possam ser

encaminhados entre a Matriz e a Filial, **e** será utilizado cabos **Cat 6a** sendo uma escolha para garantir alta performance e escalabilidade futura, com maior estabilidade e largura de banda para **10 Gbps** a **100 metros**.

7.1.1. Matriz

Configuração LAN (conectada ao Switch): 192.168.1.1

Configuração WAN (conectada ao Roteador da Filial): 10.0.0.1

Cabos: Cat 6a

7.1.2. Filial:

Configuração LAN (conectada ao Switch): 192.168.2.1

Configuração WAN (conectada ao Roteador da Matriz): 10.0.0.2

Cabos Cat 6a

7.2.Endereçamento IP e Sub-redes

O endereçamento IP e a divisão em sub-redes são cruciais para garantir que os dispositivos dentro da rede possam se comunicar de maneira eficiente e segura.

A seguir, a tabela com o endereçamento IP de cada computador, levando em consideração as sub-redes para a matriz e a filial.

Tabela 3- Endereçamento IP e Sub-redes

Dispositivo	Interface	Endereço IP	Máscara de Sub-rede	Gateway Padrão	Servidos DNS
Roteador (Matriz)	**LAN**	192.168.1.1	255.255.255.0	-	192.168.1.1
	WAN	10.0.0.1	255.255.255.252	-	10.0.0.1
Servidor (Matriz)	-	192.168.1.20	255.255.255.0	192.168.1.1	192.168.1.1
PC1_Matriz	-	192.168.1.10	255.255.255.0	192.168.1.1	192.168.1.1
PC2_Matriz	-	192.168.1.11	255.255.255.0	192.168.1.1	192.168.1.1
PC3_Matriz	-	192.168.1.12	255.255.255.0	192.168.1.1	192.168.1.1
Roteador (Filial)	**LAN**	192.168.2.1	255.255.255.0	-	192.168.2.1
	WAN	10.0.0.2	255.255.255.252	10.0.0.1	10.0.0.2
PC1_Filial	-	192.168.2.10	255.255.255.0	192.168.2.1	192.168.2.1
PC2_Filial	-	192.168.2.11	255.255.255.0	192.168.2.1	192.168.2.1

PC3_Filial	-	192.168.2.12	255.255.255.0	192.168.2.1	192.168.2.1
Switch Matriz	Interconectando os dispositivos da LAN Matriz sem necessidade de configuração.				
Switch Filial	Interconectando os dispositivos da LAN Filial sem necessidade de configuração.				

Fonte - Autoria Própria

8. MONITORAMENTO E TESTE DE CONECTIVIDADE

Após a configuração dos dispositivos de rede (roteadores, firewalls, VPN, servidores), foi realizado um conjunto de testes para garantir que as configurações de roteamento, VPN e ACLs (Listas de Controle de Acesso) estejam funcionando corretamente.

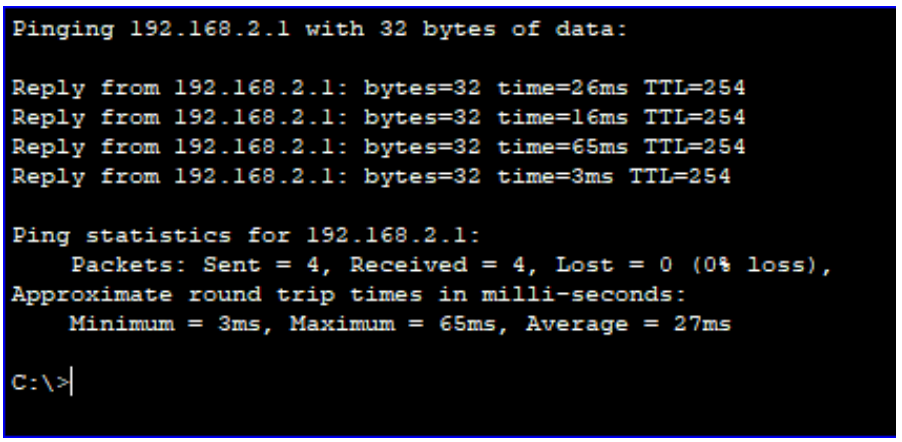
Sendo eles:

8.1.Teste de Ping (ICMP)

Verificar a conectividade básica entre os PCs da Matriz e da Filial, usando o protocolo ICMP (ping).

a) Ping do computador da Matriz para roteador Filial

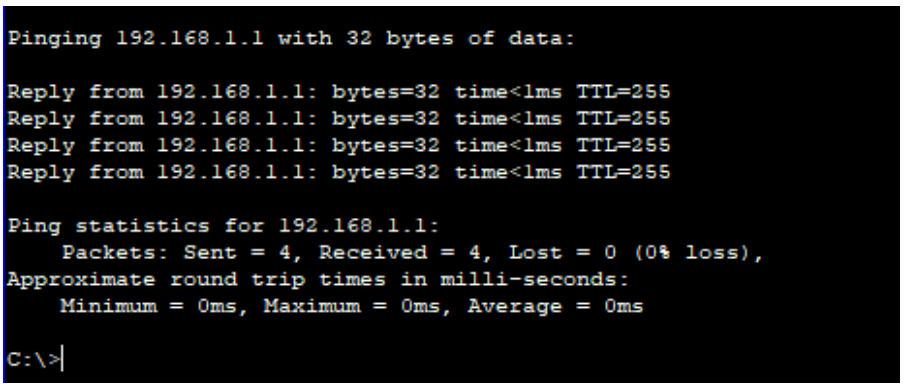
Figura 3 - Conectividade da Matriz para a Filial



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

b) Ping do computador da filial para o roteador da matriz

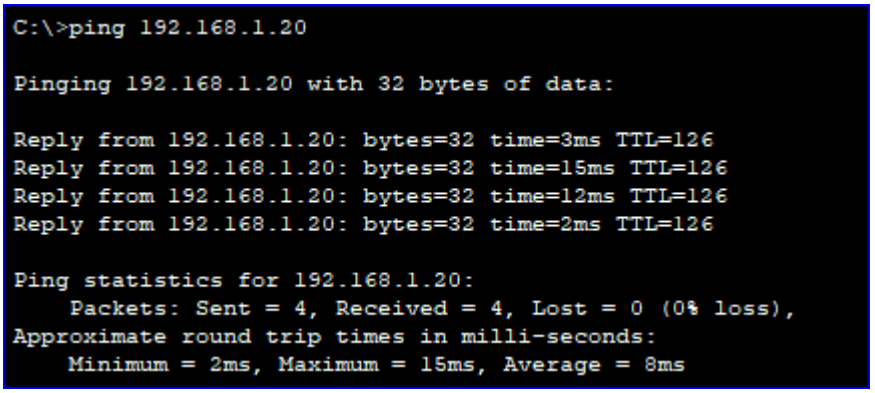
Figura 4 - Conectividade da filial para a Matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

c) Ping do servidor a partir de um computador da Filial

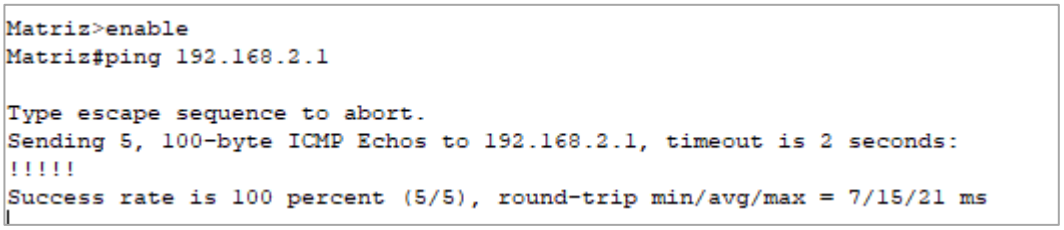
Figura 5- Ping do Pc da filial à matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

d) Ping do roteador da matriz para o roteador da filial

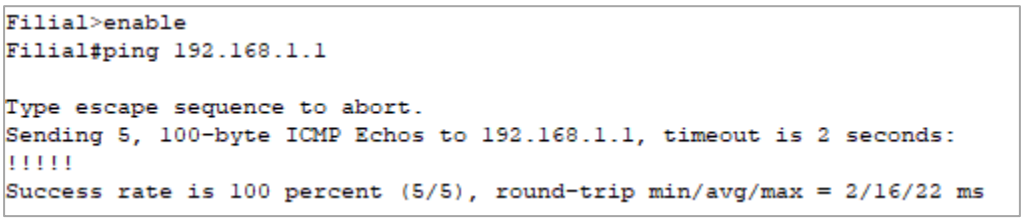
Figura 6 - ping do roteador da filial á matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

e) Ping do roteador da filial para o roteador da matriz

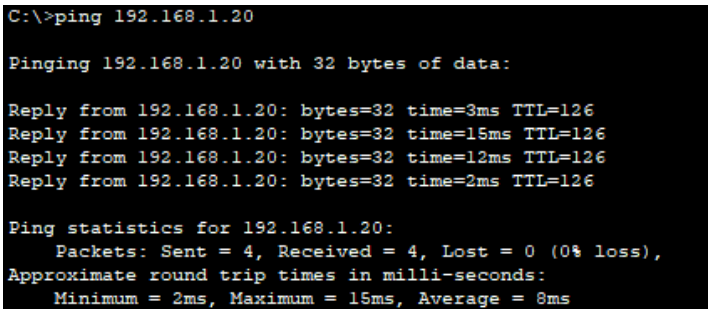
Figura 7- Ping do roteador da filial à matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

a) Ping do computador da filial para o servidor localizado na matriz

Figura 8 - ping do computador da filial para o servidor na matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

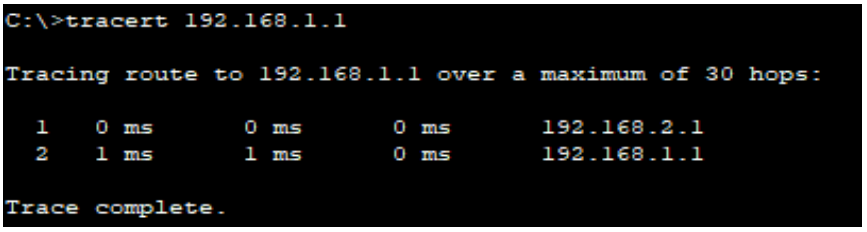
8.2.Teste de Roteamento (Traceroute)

O teste de roteamento servirá para verificar o caminho que os pacotes seguem entre as duas unidades e confirmar se os roteadores e VPN estão configurados corretamente.

Testes:

a) Rota do computador da Filial para a Matriz

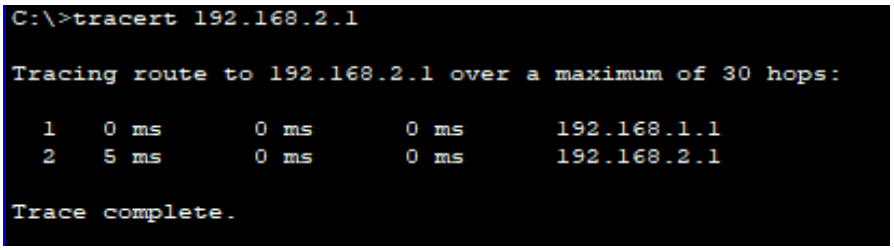
Figura 9 – Verificação da Rota Filial para a Matriz



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

b) Rota do computador Matriz para a filial

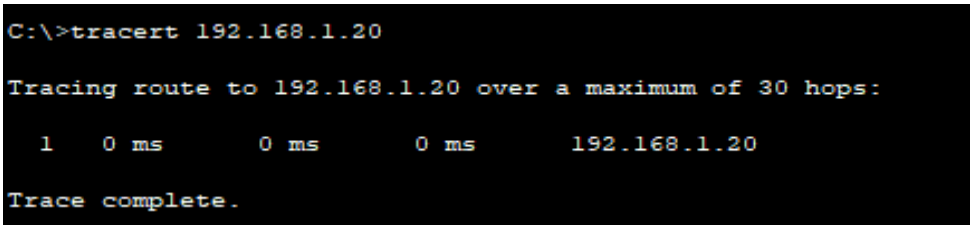
Figura 10- Verificação da rota da Matriz para a Filial



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

c) Rota do computador da matriz para o servidor

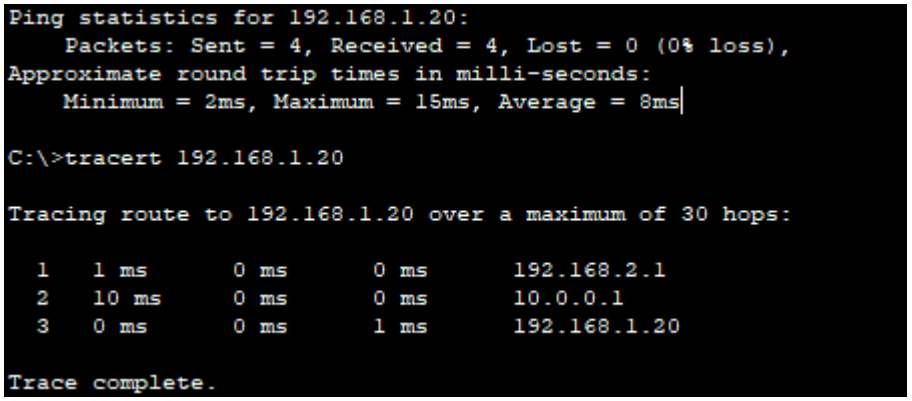
Figura 11 - Da matriz para o servidor



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

d) Rota do computador da filial para o servidor na matriz

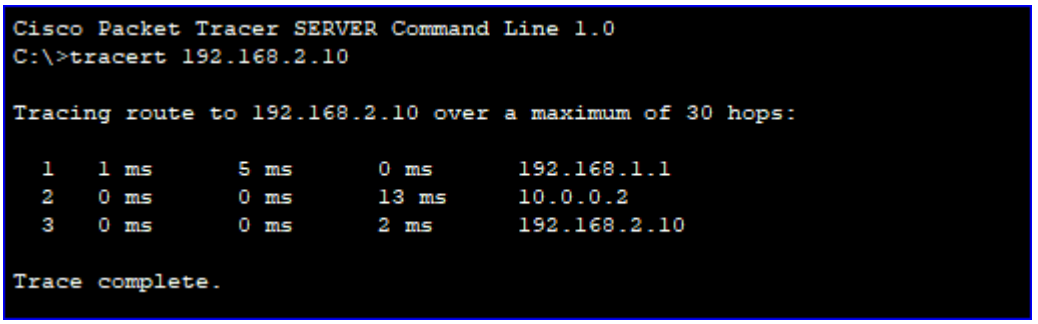
Figura 12- rota do computador da filial para o servidor



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

a) Rota do servidor para um computador na filial

Figura 13- Rota do servidor para computador na filial



Fonte: Autoria Própria. Captura criada no Cisco Packet Tracer

Conforme vizualizado nas figuras, os roteadores da matriz e da filial foram configurados com os endereços IP, máscaras de sub-rede e gateways adequados, tanto para as interfaces LAN quanto WAN. E todos os testes de conectividade foram bem-sucedidos.

O teste de ping realizado entre os dispositivos locais e seus respectivos roteadores retornou sem perda de pacotes e com baixa latência, indicando que a comunicação interna da rede está estável.

Além disso, a conexão VPN entre a matriz e a filial foi estabelecida com sucesso, permitindo a integração segura entre as duas unidades, o que também foi validado com testes de ping entre as duas redes. Por fim, os servidores DNS configurados também estão operando corretamente, garantindo a resolução adequada de endereços de rede. Com isso, a infraestrutura de rede está totalmente funcional e pronta para suportar as operações da empresa sem interrupções ou problemas de conectividade.

CONSIDERAÇÕES FINAIS

Esse projeto reflete a implementação e configuração de uma infraestrutura de rede eficiente e segura, atendendo às necessidades de conectividade entre a matriz e a filial da empresa. Através da configuração cuidadosa de dispositivos, como roteadores e switches, e da implementação de uma rede WAN conectando as duas unidades, foi possível garantir a comunicação entre todos os dispositivos, com destaque para a criação de um túnel seguro por meio de VPN, assegurando a integridade e confidencialidade dos dados.

Os testes realizados, como o ping entre dispositivos locais e roteadores, bem como entre a matriz e a filial, demonstraram que as configurações estão operando normalmente com tempos de resposta adequados e sem perda de pacotes. Esse teste garante que as atividades da empresa devem ser realizadas de forma eficiente e sem interrupções causadas por problemas de conectividade.

Além disso, a rede foi estruturada de maneira a possibilitar o acesso contínuo ao sistema ERP, um dos principais pilares da operação da empresa, sem comprometer o desempenho ou a segurança. O trabalho também abordou a integração dos sistemas de comunicação com a infraestrutura existente, com foco na melhoria da conectividade e na resolução de problemas de rede. A escolha de soluções como VPN e a configuração de endereçamento IP estático foram adequadas, levando em consideração às necessidades específicas da empresa e proporcionando um ambiente de rede robusto e seguro.

Em conclusão, o projeto atendeu aos objetivos propostos, proporcionando à empresa uma solução eficiente e escalável para a conectividade entre suas unidades, com alta disponibilidade e segurança. Essa infraestrutura é a base para o suporte contínuo das operações da empresa e garante que a comunicação interna e externa seja feita de forma confiável e eficiente.

REFERÊNCIAS

ALENCAR, Marcelo Sampaio de. **Engenharia de redes de computadores**. 1. ed. São Paulo: Érica, 2012. 286 p. ISBN 9788536504117.

BARBOSA, C. S.; et al**. Arquitetura TCP/IP I**. Porto Alegre: Sagah, 2020.

BARRETO, J. S.; ZANIN, A.; SARAIVA, M. O. **Fundamentos de redes de computadores**. Porto Alegre: Sagah, 2018.

CLOUDFLARE. O que é uma WAN?. Disponível em: https://www.cloudflare.com/pt-br/learning/network-layer/what-is-a-wan/. Acesso em: 25 out. 2024.

FOROUZAN, Behrouz A. **Comunicação de dados e redes de computadores**. 4. ed. São Paulo: McGraw Hill, 2008.

FOROUZAN, B. A.; FEGAN, S. C. **Protocolo TCP/IP. 3**. ed. Porto Alegre: AMGH, 2009.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down**. 3. ed. São Paulo: Pearson Addison Wesley, 2006. 634 p.

LOUREIRO, C. A. H.; et al. **Redes de computadores III: níveis de enlace e físico**. Porto Alegre: Bookman, 2014.

SCHMITT, M. A. R.; PERES, A.; LOUREIRO, C. A. H. **Redes de computadores: nível de aplicação e instalação de serviços**. Porto Alegre: Bookman, 2013.

TANENBAUM, A. S.; FEAMSTER, N.; WETHERALL, D. J. **Redes de computadores.** 6. ed. São Paulo: Bookman, 2021.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a internet: uma abordagem top-down**. 5. ed. São Paulo: Pearson, 2009.

LACERDA, P. S. P. et al. **Projeto de redes de computadores**. Porto Alegre: SAGAH, 2021.

ANEXOS

Anexo A – Video explicativo do Projeto

O vídeo a seguir apresenta um resumo do projeto detalhando os principais conceitos e justificativas técnicas empregados no planejamento da rede.

Link do vídeo: [Clique aqui]

Anexo B – Apresentação do Projeto no PowerPoint

A apresentação em PowerPoint complementa o vídeo e detalha visualmente os aspectos do projeto de rede. Incluindo objetivo, desafios, escolha de equipamentos. A apresentação também explica de forma gráfica e objetiva as soluções para garantir conectividade e segurança.

Link da apresentação: [Clique aqui]

Anexo C – Diagrama do projeto

Para facilitar a visualização e o entendimento da arquitetura proposta, deixo o diagrama do projeto disponível no link a seguir:

Link do diagrama: [Clique aqui]

Anexo D – Imagens dos testes

Para facilitar a visualização, deixo as imagens resultantes dos testes do projeto.

Link da pasta com todas as imagens: [Clique aqui]

Anexo E– PDF das perguntas

Respostas das perguntas solicitas no projeto da Matriz e Filial

Link do PDF: [Clique aqui]