INSTITUTO FEDERAL DE ALAGOAS
BACHARELADO EM SISTEMAS DE INFORMAÇÃO

GUSTAVO FELIPE SANTOS DE GUSMÃO TENORIO

Implantação de Pontos de Acesso Remotos para integração do parque tecnológico entre as Promotorias de Justiça e a Procuradoria-Geral do Ministério Público Estadual de Alagoas

Maceió
Maio/2023

GUSTAVO FELIPE SANTOS DE GUSMÃO TENORIO

Implantação de Pontos de Acesso Remotos para integração do parque tecnológico entre as Promotorias de Justiça e a Procuradoria-Geral do Ministério Público Estadual de Alagoas

Trabalho de Conclusão de Curso apresentado como requisito para a obtenção do título de Bacharel em Sistemas de Informação.

Orientador: Prof. Dr. Ivo Augusto Andrade Rocha Calado
Coorientador: Msc. Flávio Vasconcelos Pais

Maceió
Maio/2023

Dados Internacionais de Catalogação na Publicação
Instituto Federal de Alagoas
Campus Maceió
Biblioteca Benevides Monte

T312i Tenório, Gustavo Felipe Santos de Gusmão.
Implantação de pontos de acesso remotos para integração do parque tecnológico para entre as promotorias de Justiça e a Procuradoria-Geral do Ministério Público Estadual de Alagoas / Gustavo Felipe Santos de Gusmão Tenório. - Maceió, 2023.
45 f. : il.

Orientação: Prof. Dr. Ivo Augusto Andrade Rocha Calado.
Coorientação: Prof. Msc. Flávio Vasconcelos Pais.
Trabalho de Conclusão de Curso (Bacharel em Sistemas de Informação) - Instituto Federal de Alagoas, Campus Maceió. Maceió, 2023.

Arquivo no formato digital em PDF do trabalho acadêmico.

1. Solução de rede - Implantação. 2. Procuradoria-Geral de Justiça. 3. VPN. 4. Pontos de acesso remoto. 5. Ministério Público Estadual de Alagoas. I. Título.

CDD: 005.4

Nalva Maria Amaral
Bibliotecária – CRB-4/989

GUSTAVO FELIPE SANTOS DE GUSMÃO TENORIO

Implantação de Pontos de Acesso Remotos para integração do parque tecnológico entre as Promotorias de Justiça e a Procuradoria-Geral do Ministério Público Estadual de Alagoas

Monografia apresentada ao Curso de Bacharelado em Sistemas de Informação, do Instituto Federal de Alagoas, *Campus* Maceió, como requisito parcial para obtenção do título de Bacharel em Sistemas de Informação.

Aprovado em 18 de Maio de 2023.

Orientador:

gov.br Documento assinado digitalmente
IVO AUGUSTO ANDRADE ROCHA CALADO
Data: 31/05/2023 15:28:39-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Ivo Augusto Andrade Rocha Calado
Instituto Federal de Alagoas - IFAL / Campus Maceió

Coorientador:

FLAVIO VASCONCELOS PAIS:04427504477
Assinado de forma digital por FLAVIO VASCONCELOS PAIS:04427504477
Dados: 2023.06.05 17:15:21 -03'00'

Msc. Flávio Vasconcelos Pais
Ministério Público Estadual de Alagoas - MPE/AL

Banca examinadora:

Prof. Msc. Breno Jacinto Duarte da Costa
Instituto Federal de Alagoas - IFAL / Campus Maceió

gov.br Documento assinado digitalmente
CRISTOFE COELHO LOPES DA ROCHA
Data: 04/06/2023 12:54:41-0300
Verifique em https://validar.iti.gov.br

Prof. Msc. Cristofe Coelho Lopes da Rocha
Instituto Federal de Alagoas - IFAL / Campus Maceió

Dedico este trabalho aos meus amados avós, Perside Leite de Gusmão Tenorio e Dermeval Tenorio de Mesquita, que foram e sempre serão uma inspiração para mim. Eles têm sido uma parte vital da minha jornada acadêmica e pessoal, e sua presença amorosa e encorajadora é inestimável.

AGRADECIMENTOS

Primeiramente, gostaria de agradecer aos meus familiares próximos, que foram uma fonte constante de amor, apoio e incentivo durante todo o meu percurso acadêmico. Agradeço aos meus pais, Franklin e Silvane, que me ensinaram desde cedo a importância da educação e me apoiaram em todas as minhas decisões. Agradeço também aos meus irmãos, em especial Geovanne, e aos meus tios, Herbert e Wallace, que sempre me apoiaram e torceram por mim. E, por último, mas não menos importante, agradeço à minha amada companheira, Nicole, por seu amor incondicional, compreensão e apoio durante todo esse tempo.

Além disso, gostaria de agradecer ao ensino público brasileiro, que me proporcionou a oportunidade de estudar e me desenvolver como pessoa e profissional. Em especial, gostaria de agradecer aos professores e demais colaboradores do curso de Sistemas de Informação do IFAL (Instituto Federal de Alagoas), que foram fundamentais para minha formação acadêmica e profissional. Agradeço aos docentes que ministraram as disciplinas que compuseram o curso, por seu conhecimento, dedicação e disponibilidade em ajudar. Agradeço também aos coordenadores e demais colaboradores do curso, por todo o apoio e suporte oferecidos.

Por fim, gostaria de agradecer a todas as pessoas que, de alguma forma, contribuíram para que eu chegasse até aqui. Cada gesto de incentivo, apoio e amizade foi essencial para que eu pudesse superar os desafios e alcançar meus objetivos. Espero que minha gratidão seja uma forma de retribuir tudo o que recebi, e que eu possa, de alguma forma, contribuir para o desenvolvimento de nossa sociedade.

RESUMO

A presente monografia tem como objetivo principal demonstrar um caso de sucesso na implantação de uma solução de rede baseada em Redes Privadas Virtuais (VPNs) e Pontos de Acessos Remotos (RAPs) que garantiram o acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça do Ministério Público Estadual de Alagoas. Para tanto, foram apresentados o contexto e as necessidades que motivaram a implantação da solução, assim como os procedimentos utilizados e suas dificuldades, além da avaliação da efetividade da solução. Os resultados indicaram que a solução foi eficaz em atender às necessidades da instituição. Também foram discutidos trabalhos correlatos que foram relacionados aos resultados apresentados neste estudo, mostrando as similaridades e diferenças entre as soluções implementadas em cada caso. Por fim conclui-se que a solução implementada é viável e pode ser replicada em outras organizações.

Palavras-chave: VPN, Pontos de Acesso Remoto, Ministério Público Estadual de Alagoas, Solução de Rede.

ABSTRACT

The main objective of this monograph is to demonstrate a successful case in implementing a network solution based on Virtual Private Networks (VPNs) and Remote Access Points (RAPs), which ensured access to the same resources and information available at the Attorney General's Office of the State Public Prosecutor's Office of Alagoas. To achieve this, the context and needs that motivated the implementation of the solution were presented, as well as the procedures used and their difficulties, in addition to the evaluation of the effectiveness of the solution. The results indicated that the solution was effective in meeting the institution's needs. Related works that were related to the results presented in this study were also discussed, showing the similarities and differences between the solutions implemented in each case. Finally, it is concluded that the implemented solution is feasible and can be replicated in other organizations..

Keywords: VPN, Remote Access Points, State Public Prosecutor's Office of Alagoas, Network Solution.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIATURAS E SIGLAS

AD	*Active Directory*
ARP	Ata de Registro de Preços
DHCP	*Dynamic Host Configuration Protocol*
DMZ	*DeMilitarized Zone*
DNS	*Domain Name System*
HPE	*Hewlett Packard Enterprise*
IKE	*Internet Key Exchange*
IP	*Internet Protocol*
Ipsec	*Internet Protocol Security Protocol*
ISO	*International Organization for Standardization*
LAN	*Local Area Network*
MAN	*Metropolitan Area Network*
MPE/AL	Ministério Publico Estadual de Alagoas
OSI	*Open Systems Interconnection*
PGJ	Procuradoria-Geral de Justiça do Estado
PGJ/AL	Procuradoria-Geral de Justiça do Estado de Alagoas
RAP	Pontos de Acessos Remotos
SMB/CIFS	*Server Message Block/Common Internet File System)*
TCP	*Transmission Control Protocol*
TCP/IP	*Transmission Control Protocol / Internet Protocol*
TI	Tecnologia da Informação
UDP	*User Datagram Protocol*
VLAN	*Virtual Local Area Network*
VoIP	*Voice over Internet Protocol*
VPN	*Virtual Private Network*
WAN	*Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

O processo de expansão da infraestrutura de TI empresarial pode criar desafios, como garantir a integração perfeita e manter a segurança do sistema, para isso redes virtuais privadas (VPNs) podem fornecer um meio seguro e eficiente de conectar unidades geograficamente dispersos e trabalhadores remotos à rede corporativa (SWANSON, 2018).

Esta expansão pode ser definitiva, como a criação de um novo espaço físico, um escritório ou filial em outra cidade até mesmo em outro estado. Por outro lado, uma expansão pode ser provisória, por exemplo um funcionário que eventualmente necessite acessar recursos da empresa remotamente em um período determinado para realizar determinada tarefa ou projeto devendo retornar ao seu escopo anterior ao término da ação (MOSNA e MORAIS, 2020).

Neste sentido, empresas vêm recorrendo a soluções tecnológicas, reduzindo distâncias entre filiais e sua matriz. Uma delas seria o uso de redes Privadas Virtuais, do inglês, *Virtual Private Networks* (VPN), uma vez que, é o mais indicado entre uma conexão doméstica e corporativa, por oferecer grande segurança durante o tráfego dos dados, bem como redução do tempo e diminuição de custos com escritório (LEAL E PEREIRA FILHO, 2021). Andrade e Castro (2004), defendem também o uso de VPNs na interligação corporativa de empresas com suas filiais, entre seus fornecedores e até mesmos clientes, processo que prevê mais uma vez a disponibilidade do acesso de qualquer ponto, de forma segura e de baixo custo.

Uma rede VPN utiliza outras redes para criar uma conexão, através de uma rede pública, como a Internet, uma VPN permite que um computador ou dispositivo envie e receba dados como se estivesse diretamente conectado a uma rede privada, usufruindo das funcionalidades, segurança e políticas de gerenciamento da rede privada, mesmo em redes compartilhadas ou públicas (MELLER, 2018).

Neste contexto de provimento de disponibilidade de serviços e suporte à conectividade remota, utilizando redes VPNs, que está inserido nesta monografia, a solução apresentada baseada na tecnologia *Aruba Networks* se mostra como uma alternativa eficiente e confiável para a expansão e integração da rede corporativa, garantindo um alto nível de segurança e confidencialidade nas comunicações institucionais.

1.1 Descrição Do Problema

A qualidade da prestação do serviço está diretamente ligada a satisfação do cliente. Conforme Kotler e Keller (2006), quando o desempenho do produto ou serviço atende ou su-

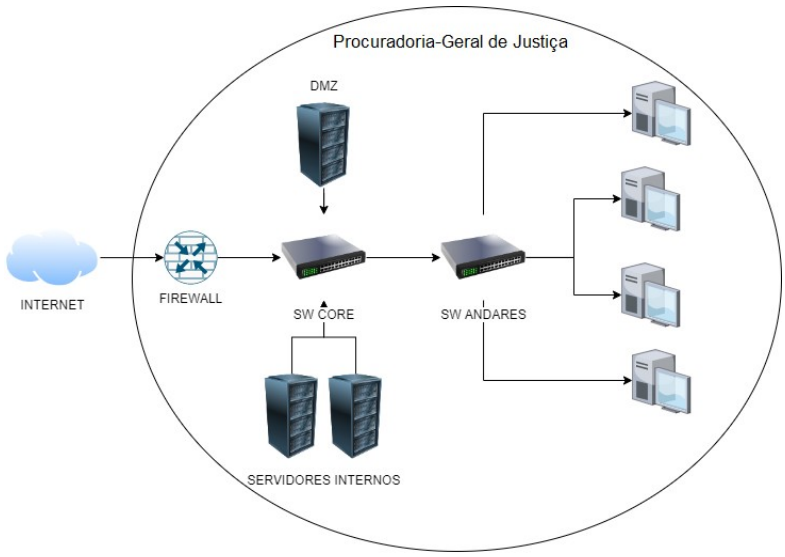
pera as expectativas do cliente, ele tende a ficar satisfeito e leal à empresa. Por outro lado, se as expectativas do cliente não forem atendidas ou superadas, ele pode ficar insatisfeito e procurar outras opções no mercado.

No Ministério Publico Estadual de Alagoas (MPE/AL), nome fantasia para Procuradoria-Geral de Justiça do Estado de Alagoas (PGJ/AL), os clientes que usufruem dos serviços de tecnologia da informação (TI) ofertados, além dos cidadãos, são os membros, servidores, estagiários, terceirizados e cedidos que atuam na instituição, onde parte destes colaboradores estão lotados em Promotorias de Justiça (PJ) remotas à sede da Procuradoria-Geral de Justiça (PGJ), local onde ficam hospedados estes serviços de TI e por isso esses usuários tinham uma experiência limitada dos serviços prestados.

Esse fator limitante afetava diretamente a população, pois ferramentas essenciais que agilizam o trabalho dos usuários institucionais não podem ser acessados através da Internet de forma tradicional devido à políticas de segurança da informação estabelecidas pela instituição. Outro ponto negativo da topologia antiga é a falta de monitoramento, gerenciamento e suporte a esses locais remotos, visto que o único meio de comunicação era um link local de Internet.

A Figura 1 é uma representação da antiga topologia de rede da Procuradoria-Geral de Justiça, na qual é amplamente utilizada como padrão em diversas organizações. Por motivos de segurança, não serão mostrados os blocos de endereços IP nem informações sensíveis da rede corporativa.

Figura 1 – Topologia de rede antiga.



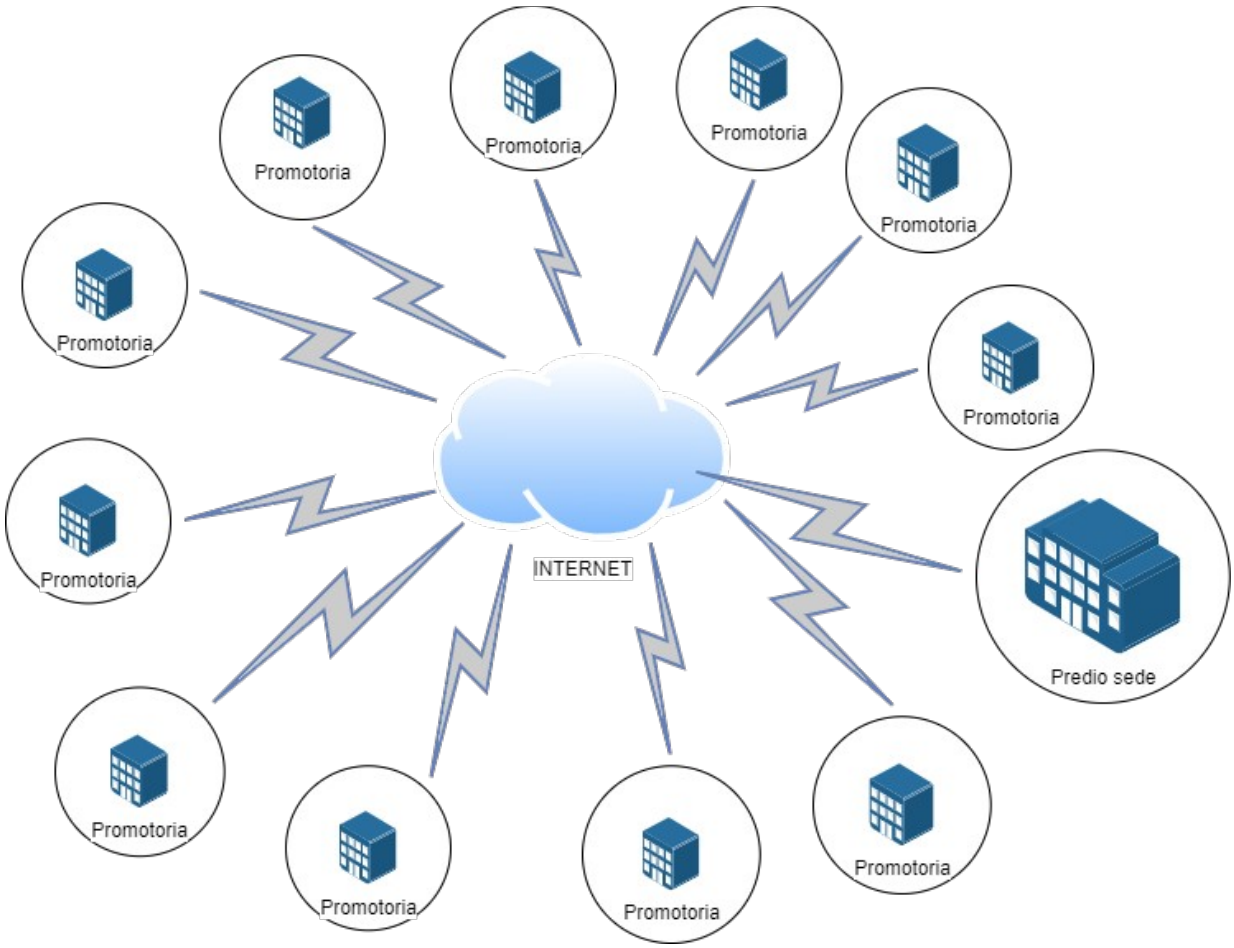
Fonte: Elaborado pelo autor (2023)

Este modelo não permite que os usuários institucionais que estão localizados nas Promotorias de Justiça do interior consigam acessar serviços disponíveis na rede interna. Estes têm apenas acesso à zona desmilitarizada, *DeMilitarized Zone*, ou DMZ, que é uma rede que

age como área intermediária entre a rede interna (geralmente a rede local) e a rede externa (geralmente a Internet), ou seja, serve como uma ponte entre uma rede confiável (rede local) e não confiável, como a Internet (JUNIOR, 2010).

Na Figura 2, é possível observar que as Promotorias de Justiça que estão espalhadas pelo Estado de Alagoas e o prédio sede fazem parte cada uma de uma rede isolada ligada a um provedor de Internet, então cada prédio conta com uma infraestrutura própria.

Figura 2 – Promotorias de Justiça em todo estado de Alagoas.



Fonte: Elaborado pelo autor (2023)

Foi relatado que as topologias representadas pelas figuras 1 e 2 apresentavam diversas desvantagens, sendo elas:

- Na maioria das Promotorias de Justiças (PJs) não havia disponibilidade de rede WiFi. E quando havia, o equipamento era de uso doméstico. Em sua grande maioria eram utilizados roteadores com baixa capacidade de processamento de dados. Muitas vezes, o próprio Promotor de Justiça comprava o roteador com recursos próprios. Havia dificuldade da equipe técnica em configurar o

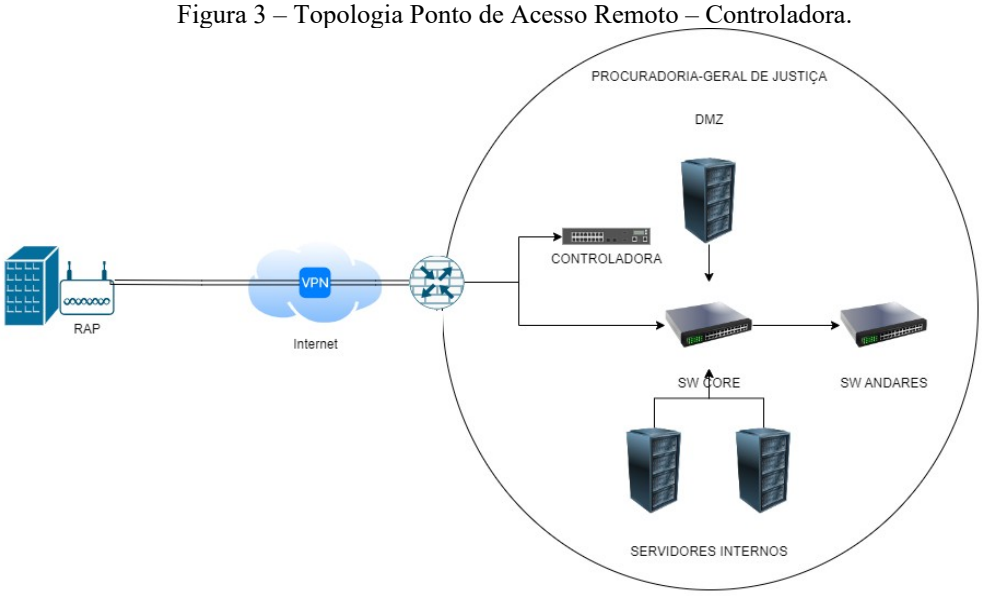
equipamento, visto que muitas vezes as senhas de administração do equipamento não eram de conhecimento;

- Grande dificuldade por parte do suporte técnico de prestar atendimento às PJs, devido principalmente, aos dispositivos de Informática (*desktops*, *notebooks* e impressoras) estarem fora da rede corporativa, ou seja, existia apenas uma rede isolada em cada promotoria. Eventualmente, as estações de trabalho apresentavam usuários e senhas desconhecidas, dificultando o acesso à equipe técnica;
- O gerenciamento de risco e ameaças digitais é praticamente inexistente, contando apenas com o antivírus instalado nos *desktops* e *notebooks,* que recebiam atualizações aleatórias e sem política de segurança.;
- Não contavam com nenhuma proteção de borda da rede, como por exemplo, um *firewall*, que consegue operar auditando através da camada de aplicação, nem controle de qualidade de serviço da rede e do enlace de Internet;
- Na maioria das Promotorias de Justiça não exista sistemática de compartilhamento de arquivos adequada, onde na maior parte dos casos era utilizado o *desktop* de algum funcionário como servidor de arquivos improvisado;
- Não existia *backup* centralizado. As cópias de segurança eram de responsabilidade dos próprios funcionários da unidade, salvo exceção o prédio sede da Procuradoria-Geral de Justiça e Promotorias de Justiça da capital e Arapiraca, que possuíam servidores de arquivos e *backup;*
- Não era possível ter uma visão detalhada do consumo do enlace de Internet, quais aplicações estavam sendo utilizadas e qual seu impacto na performance da rede ou até mesmo, qual usuário estava acessando a rede. Por exemplo, em muitos casos, a equipe de TI verificou que o motivo da lentidão na rede era o horário aleatório em que o sistema operacional *Windows* executava a atualização da máquina;
- A rede de telefonia das Promotorias de Justiça eram ramais de rede convencional, sem maior detalhamento do uso das linhas.

Uma alternativa encontrada capaz de eliminar as desvantagem listadas foi a utilização de Pontos de Acessos Remotos (RAPs), que essencialmente utilizam redes VPNs em sua implementação. Esta solução muda logicamente a topologia anterior, fazendo com que todas as Promotorias de justiça que possuírem um ponto de acesso remoto se conectem a uma

controladora virtual localizada na sede através de um túnel VPN. Esta controladora é a responsável por gerenciar todo trafego entre os Pontos de Acesso Remotos e a rede corporativa do MPE/AL, resultando em uma nova topologia, representada pela Figura 3.

Figura 3 – Topologia Ponto de Acesso Remoto – Controladora.



Fonte: Elaborado pelo autor (2023)

Diante do exposto, esta monografia tem como pergunta de pesquisa: *Como manter a politica de segurança entre as Promotorias de Justiça geograficamente distribuídas e a Procuradoria-Geral de Justiça do Ministério Público do Estado de Alagoas para que compartilhem os mesmos recursos tecnológicos disponibilizados?*

1.2 Objetivos

Nesta seção são apresentados o objetivo principal e os objetivos específicos desta monografia.

1.2.1 Objetivo Principal

Esta monografia tem como objetivo principal descrever como foi feita a implantação da solução de rede baseada em redes VPNs e RAPs que garantiu todas as Promotorias de Justiça do Ministério Público Estadual de Alagoas acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça, de forma eficiente e segura.

1.2.2 Objetivos Específicos

Neste sentido, para atingir o objetivo principal esta solução tem como objetivos específicos os seguintes itens:

- Apresentar o contexto e as necessidades que motivaram a implantação da solução de rede;
- Descrever os procedimentos utilizados na implantação da solução de rede;
- Identificar os desafios encontrados durante a implantação;

- Avaliar a efetividade da solução de rede em garantir o acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça.

1.3 Organização Do Trabalho

Inicialmente é apresentado um referencial teórico contendo os conceitos fundamentais para a compreensão do trabalho, tais como: Redes de computadores (conceitos e uso corporativo), Modelos de Referência (OSI e TCP/IP), Protocolos (IP, DHCP, DNS, VoIP), Serviços (*Active Directory*), VLANS, Segurança de Redes (conceitos, *firewall,* criptografia e antivírus), Redes Privadas Virtuais (VPNs e suas principais implementações e trabalhos correlatos).

No Capítulo 3 são descritos os instrumentos de coleta de dados, os materiais e métodos de análise dos dados e a metodologia. O Capítulo 4 é destinado à apresentação dos resultados obtidos a partir do estudo realizado e sua discussão. No capítulo final encontram-se as conclusões oriundas do trabalho.

2. REVISÃO DE LITERATURA

Neste capítulo serão abordados conceitos importantes para compreensão da solução de integração de redes de computadores proposta neste estudo. Assim, o referencial teórico discorrerá sobre os conceitos básicos de redes de computadores, citando alguns autores que balizam o assunto proposto.

2.1 Rede De Computadores

O conceito de rede de computadores abrange a ideia de um grupo de computadores que estão conectados entre si através de uma única tecnologia, com o objetivo de compartilhar recursos e informações. Essas redes possuem ainda variados tamanhos, modelos e formas. A Internet, por exemplo, não é formada por uma única rede de computadores, mas sim uma rede de redes, uma vez que as conexões podem ser realizadas através de diversos meios de comunicação como fios de cobre, fibras ópticas, micro-ondas, infravermelho e satélites de telecomunicações (TANENBAUM, 2003).

Piazza (2015) mostra que existem diversas subdivisões para as redes de acordo com sua extensão geográfica, mas algumas das mais comuns são:

- LAN (*Local Area Network*): rede de pequeno alcance que interliga computadores localizados em um mesmo espaço físico, como empresas, instituições públicas, escolas, residências, entre outros.
- MAN (*Metropolitan Area Network*): rede de médio alcance que interconecta diversas redes locais dentro de um raio de dezenas de quilômetros. As fronteiras de uma cidade representam a área de atuação de uma MAN.
- WAN (*Wide Area Network*): rede de grande alcance capaz de abranger grandes áreas, como um país ou um continente.

2.1.2 Rede Corporativa

Redes corporativas são compostas por diversos elementos, como servidores, roteadores, *switches* e *firewalls*, que permitem a interconexão de computadores, dispositivos móveis e outros equipamentos, de forma a garantir a comunicação e o compartilhamento de recursos entre os diversos setores de uma organização (TANENBAUM, 2011).

Uma rede corporativa funciona conectando as estações de trabalho aos roteadores, utilizando cabeamento *Ethernet* ou *Wi-Fi*. Cada um destes dispositivos é designado com um número de identificação de rede (*Hostname*), cada usuário deve ser estabelecido com uma

conta única que permite cada funcionário ter suas credenciais verificadas. Cabe aos administradores de rede definirem regras e restrições de *firewall* no acesso à Internet de acordo com os requisitos da organização. Um servidor local pode ser usado para executar aplicativos de banco de dados e outros softwares aos funcionários, como os servidores Web e de arquivos compartilhados. O acesso ao servidor de rede local normalmente é limitado apenas a funcionários autenticados (VMWARE, 2022).

2.2 Modelos De Referência

2.2.1 *Open Systems Interconnection* (OSI)

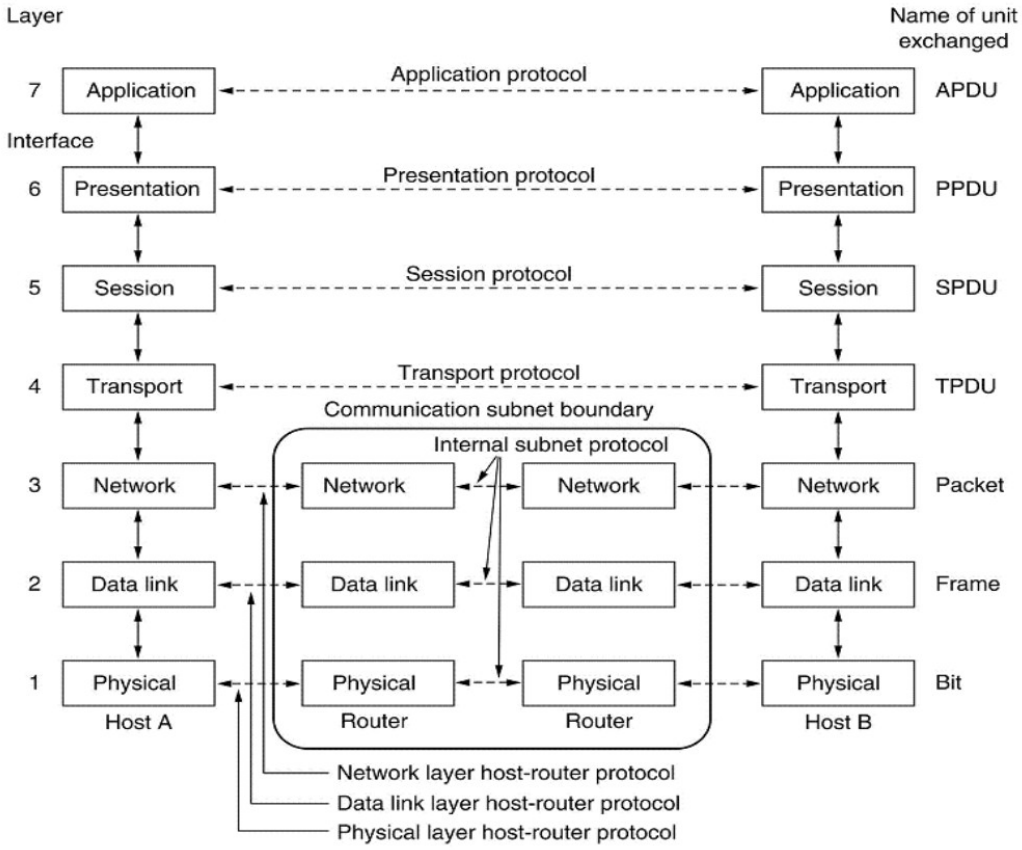
O modelo de referência OSI, Interconexão de Sistemas Abertos, não é um conjunto de protocolos, mas sim um modelo de referência para a arquitetura de redes de computadores. O modelo OSI define uma arquitetura em camadas para a comunicação entre sistemas abertos, visando garantir a compatibilidade e a interoperabilidade entre diferentes tecnologias de rede desenvolvidas por fabricantes diversos (FOROUZAN, 2010).

O modelo OSI foi desenvolvido na década de 1970 pela ISO (I*nternational Organization for Standardization*) e é composto por sete camadas: física, enlace, rede, transporte, sessão, apresentação e aplicação (MENDES, 2007). Tanenbaum (2003) descreve cada camada do modelo OSI (Figura 4) da seguinte forma:

- Primeira camada, a Camada Física, é responsável pela transmissão e recepção de dados brutos sobre um meio físico;
- Segunda camada, a Camada de Enlace de Dados, é responsável por garantir a transferência confiável de dados entre dispositivos em um link físico;
- Terceira camada, a Camada de Rede, gerencia o envio e o roteamento de pacotes entre *hosts* em uma rede, independentemente da topologia física;
- Quarta camada, a Camada de Transporte, é responsável por garantir que os pacotes cheguem ao seu destino de forma confiável e sem erros;
- Quinta camada, a Camada de Sessão, gerencia a comunicação entre aplicativos em diferentes dispositivos;
- Sexta camada, a Camada de Apresentação, lida com a conversão de dados entre o formato da rede e o formato usado pelos aplicativos e

- Sétima camada, a Camada de Aplicação, fornece serviços aos usuários finais, como e-mail, transferência de arquivos e login remoto.

Figura 4 – Modelo de Referência OSI



Fonte: Tanenbaum (2003)

2.2.2 TCP/IP

O conjunto de protocolos TCP/IP foi desenvolvido antes do modelo OSI e, como resultado, as camadas do TCP/IP não correspondem exatamente às camadas do modelo OSI (Figura 5), o TCP/IP originalmente foi definido como um conjunto de quatro camadas de software construídas sobre o hardware, que incluía as camadas de interface de rede, Internet, transporte e aplicação, no entanto, ao longo do tempo, o TCP/IP evoluiu e passou a ser considerado um modelo de cinco camadas, as camadas adicionais foram adicionadas para melhorar a funcionalidade e a flexibilidade do modelo, e essas camadas foram nomeadas de forma semelhante às camadas do modelo OSI (FOROUZAN, 2010).

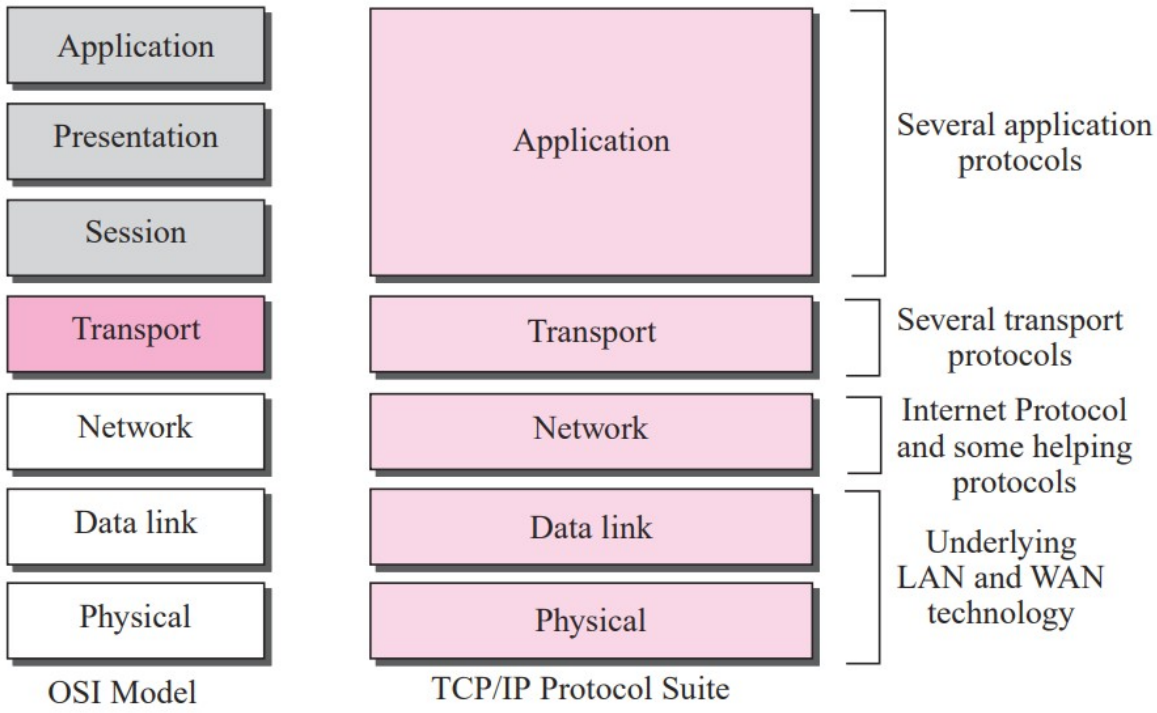
Segundo Forouzan (2010), o modelo TCP/IP é composto pelas seguintes camadas, da mais baixa para a mais alta: camada física, camada de enlace de dados, camada de rede, camada de transporte e camada de aplicação e podem ser definidas da seguinte forma:

- Camada de Física: O TCP/IP não especifica um protocolo específico para a camada física, mas é compatível com todos os protocolos padrão e proprietários utilizados para transmissão de dados. Nessa camada, a

comunicação ocorre entre dois nós e a unidade básica de transmissão é o bit, que é tratado individualmente pela camada física.

- Camada de Enlace de Dados: Nesta camada também não é especificado algum protocolo especifico, mas é compatível com todos os protocolos padrão e proprietários utilizados para transmissão de dados nessa camada. Na camada de enlace de dados, a comunicação também ocorre entre dois nós, e a unidade básica de transmissão é um pacote chamado quadro. Esse quadro é um pacote que encapsula os dados recebidos da camada de rede com um cabeçalho adicionado e, às vezes, um trailer.
- Camada de Rede: Na camada de rede, o TCP/IP suporta o Protocolo de Internet (IP), que é o mecanismo de transmissão utilizado pelos protocolos TCP/IP. O IP transporta dados em pacotes chamados datagramas, que são transmitidos separadamente e podem percorrer diferentes rotas, podendo chegar fora de ordem ou serem duplicados. No entanto, o IP não rastreia as rotas nem tem a capacidade de reordenar os datagramas quando chegam ao destino.
- Camada de Transporte: A camada de transporte e a camada de rede têm uma diferença principal: enquanto todos os nós em uma rede precisam ter a camada de rede, apenas um dos dois computadores que estão se comunicando precisam ter a camada de transporte. A camada de rede é responsável por enviar datagramas individuais do computador A para o computador B, enquanto a camada de transporte é responsável por entregar a mensagem completa, chamada de segmento, datagrama do usuário ou pacote, de A para B. Como os segmentos podem consistir em vários datagramas, cada datagrama deve ser entregue à camada de rede para transmissão, e como a Internet define uma rota diferente para cada datagrama, eles podem chegar fora de ordem ou serem perdidos. O computador B precisa esperar até que todos os datagramas cheguem para montá-los em um único segmento. Tradicionalmente, a camada de transporte era representada no conjunto TCP/IP por dois protocolos: *User Datagram Protocol* (UDP) e *Transmission Control Protocol* (TCP).
- Camada de Aplicação: A camada de aplicação no TCP/IP é similar à sessão, apresentação e camadas de aplicação no modelo OSI combinadas. A camada de aplicação possibilita que usuários acessem serviços da Internet privada ou global, com muitos protocolos definidos para fornecer serviços como correio eletrônico, transferência de arquivos e acesso à *World Wide Web*.

Figura 5 – Comparação Modelo de Referência OSI e TCP/IP



Fonte: Forouzan (2010)

2.3 Protocolos De Rede

Em linhas gerais, trata-se de um conjunto de regras, procedimentos e formatos de dados que gerenciam a comunicação entre dispositivos de rede, como computadores, servidores, roteadores e outros dispositivos de rede. Os protocolos em redes de computadores, são as regras que governam o comportamento dos dispositivos de rede, permitindo que eles possam se comunicar e cooperar em conjunto (TANENBAUM, 2011). Os protocolos de rede desempenham um papel fundamental na comunicação entre computadores e dispositivos em uma rede, permitindo que informações sejam transmitidas de maneira eficiente e segura (STEIN ET AL., 2010).

Nos tópicos subsequentes serão abordados alguns protocolos que são amplamente utilizados em empresas, instituições públicas e ate mesmo em redes domésticas, como o IP (*Internet Protocol*), o DHCP (*Dynamic Host Configuration Protocol*), o DNS (*Domain Name System*) e o VoIP (*Voice over Internet Protocol*).

2.3.1 IP

O endereço IP é um identificador único de um dispositivo em uma rede que utiliza o protocolo de Internet para comunicação. A sigla IP significa *Internet Protocol* e é utilizada para identificar, no nível lógico, um dispositivo conectado a uma determinada rede. O endereço IP é composto por um conjunto de números que identificam exclusivamente o

dispositivo na rede e permitem que ele se comunique com outros dispositivos (MOSNA E MORAES, 2020).

2.3.2 DHCP

O protocolo DHCP é utilizado em redes corporativas para automatizar a atribuição de endereços IP para as máquinas clientes, este atua na camada de aplicação do modelo TCP/IP ou na camada de rede do modelo OSI. Isso é necessário em redes com grande quantidade de dispositivos, pois seria inviável realizar a configuração manualmente em cada máquina. O DHCP permite que as máquinas clientes obtenham automaticamente um endereço IP a partir de um servidor central.

O DHCP funciona com base nas solicitações dos clientes que enviam pacotes de broadcast na rede em busca de um servidor DHCP. O servidor recebe essas solicitações e envia pacotes de resposta com informações de configuração, como endereços IP, máscaras de rede e gateways padrão para os clientes. Com essas informações, os clientes podem se configurar automaticamente e se conectar à rede com as configurações corretas (MORIMOTO, 2006).

2.3.3 DNS

O DNS é responsável pela resolução de nomes para endereços IP em redes corporativas e esta posicionado na camada de aplicação de ambos modelos de referencia. Ele possui um banco de dados distribuído e hierárquico, que armazena informações sobre nomes de domínio e seus correspondentes endereços IP. Quando um usuário digita um nome de domínio em seu navegador, o DNS é acionado para localizar o endereço IP correspondente a esse nome, permitindo que a comunicação na rede seja estabelecida (KUROSE, 2010).

2.3.5 VoIP

O protocolo VoIP (Voice over Internet Protocol) é uma tecnologia que possibilita a transmissão de voz e outras formas de comunicação multimídia por meio da Internet. Em suma, VoIP permite a realização de chamadas telefônicas através da Internet, utilizando o protocolo IP para transferir dados de áudio em tempo real. A implementação de sistemas de VoIP pode proporcionar uma significativa redução de custos em relação à telefonia tradicional, já que a transmissão de voz é realizada através da infraestrutura de rede existente, eliminando a necessidade de linhas telefônicas dedicadas e reduzindo os custos de manutenção (STALLINGS, 2014).

2.4 Serviços

Os serviços de rede são as funcionalidades ou recursos oferecidos em uma rede de computadores para permitir a comunicação, troca de informações e compartilhamento de

recursos entre dispositivos conectados à rede. Esses serviços podem ser disponibilizados por meio de diferentes protocolos de rede (RIOS, 2011).

2.4.1 Gerenciamento De Usuários E Recursos

O gerenciamento de usuários em redes é uma tarefa crítica para garantir a segurança e eficiência no uso dos recursos e serviços disponíveis, responsável por políticas de segurança, como a configuração de senhas fortes, restrições de acessos, entre outras medidas para proteger a rede contra ameaças externas e internas.

2.4.2 *Active Directory*

O serviço de diretório é uma ferramenta de gerenciamento de rede que permite armazenar informações sobre os usuários, dispositivos e recursos da rede em um local centralizado. Ele fornece uma estrutura hierárquica de diretórios e subdiretórios, que permite organizar as informações de forma eficiente e fácil de acessar (ROVER, 2012).

Ao usar um serviço de diretório, os administradores de rede podem economizar tempo e recursos valiosos. Segundo Stanek (2009), em vez de gerenciar cada usuário, dispositivo e recurso individualmente, os administradores de redes podem usar o serviço de diretório para gerenciar todos esses itens de forma centralizada. Isso permite uma melhor organização da rede, facilitando a administração e a manutenção da rede como um todo.

O protocolo responsável por permitir operações de arquivos em redes, como leitura, escrita e renomeação, como se fossem arquivos locais da máquina, é o SMB/CIFS (*Server Message Block/Common Internet File System*). Esse protocolo é amplamente utilizado em ambientes de rede corporativa para compartilhar recursos de arquivos e impressoras entre as máquinas conectadas à rede. Com o SMB/CIFS, é possível acessar, manipular e compartilhar arquivos de forma transparente e segura em toda a rede (BARREIROS, 2001).

Barreiros (2001) também demonstra o funcionamento deste protocolo que se dá por meio do envio de pacotes do cliente para o servidor, com cada pacote baseado em uma requisição de algum tipo, como a abertura ou leitura de um arquivo, o servidor recebe o pacote, verifica se a requisição é válida e executa a operação solicitada, retornando um pacote de resposta ao cliente, o cliente analisa o pacote de resposta para determinar se a requisição foi executada com sucesso.

2.4.3 Sistema de Automação da Justiça

O Sistema de Automação da Justiça (SAJ) é um sistema de gestão processual utilizado por diversos tribunais no Brasil. Ele oferece funcionalidades para o registro e acompanhamento de processos judiciais, controle de prazos, gestão de documentos, peticionamento eletrônico, entre outros recursos que agilizam os procedimentos judiciais.

Com o SAJ, é possível realizar o trâmite processual de forma eletrônica, reduzindo a necessidade de uso de papel e proporcionando uma maior eficiência na movimentação dos processos. Além disso, o sistema permite a consulta pública de processos, facilitando o acesso à informação para as partes envolvidas e para o público em geral. O SAJ utiliza o modelo cliente-servidor, onde o cliente é a interface utilizada pelos usuários e o servidor é responsável por armazenar os dados e processar as requisições. O sistema disponibiliza tanto a opção de conexão via Internet quanto a opção de conexão local, dependendo das necessidades.

2.5 VLAN

As VLANs (Redes Locais Virtuais) são úteis em instituições setoriais, é implementada na camada de Enlace de Dados nos modelos de referência OSI e TCP/IP, pois permitem a criação de domínios de broadcast diferentes para cada setor, o que ajuda a dividir uma rede local em várias redes lógicas e tornar a navegação mais organizada. Além disso, a segmentação da rede por VLAN pode ser uma solução eficaz para a segurança das máquinas de uma empresa, pois, em caso de infecção por vírus ou malware por meio da rede, apenas os dispositivos conectados naquela VLAN específica podem ser afetados (SANTOS E ALBERTIN, 2021).

2.6 Segurança De Redes

Nesta seção serão apresentados alguns conceitos e praticas mais comuns utilizados na manutenção de uma rede segura, onde dispositivos como *firewalls* e softwares antivirus podem mitigar ataques internos ou externos que comprometam as informações e dados de uma instituição.

2.6.1 *Firewall*

Ao contrário de um roteador, que apenas encaminha o tráfego entre redes, um *firewall* é um sistema ou grupo de sistemas que aplicam uma política de controle de acesso em diferentes pontos da rede, seu objetivo é garantir que somente o tráfego permitido pela política de controle de acesso seja autorizado a entrar ou sair da rede. Assim, é responsabilidade do *firewall* assegurar que a política de controle de acesso seja respeitada por todos os usuários (BRENTON E HUNT, 2001).

A função principal do *firewall* é atuar como uma barreira de segurança entre a rede interna e externa, controlando o acesso de pacotes de dados. Por essa razão, ele é frequentemente colocado na borda externa da rede, entre a Internet e os dispositivos locais, para filtrar o tráfego que entra e sai da rede. Além disso, o *firewall* também pode ser utilizado para separar e controlar o tráfego entre diferentes LANs, restringindo o acesso de usuários não autorizados (PIAZZA, 2015).

2.6.2 Antivírus

Um software antivírus é projetado para detectar, identificar e remover *malware* (software malicioso) que possa infectar um computador ou dispositivo. Existem vários tipos de *malware*, incluindo vírus, *worms*, cavalos de Troia, *spyware* e *ransomware*, entre outros (LORIATO E LORIATO 2008). De acordo com Bhardwaj (2007), a detecção de vírus é frequentemente realizada por meio de assinaturas, que são uma coleção de padrões e comportamentos de softwares maliciosos que os programas antivírus utilizam para identificar e eliminar ameaças.

2.6.3 Criptografia

Para proteger informações é necessário utilizar técnicas de criptografia, que consistem em transformar uma mensagem original em uma mensagem cifrada usando um algoritmo de encriptação acompanhado de uma chave de segurança. Essa técnica garante a confidencialidade da mensagem, impedindo que terceiros possam compreendê-la. A chave de segurança, normalmente uma senha, é essencial para descriptografar a mensagem e recuperar o seu conteúdo original. O uso de criptografia é importante para proteger informações sensíveis, como dados pessoais, transações financeiras e comunicações sigilosas.

A criptografia, é uma prática antiga e ao longo do tempo, com o avanço da matemática e da computação, surgiram diversas outras formas de criptografia, ela pode ser classificada em simétrica ou assimétrica e sua segurança está diretamente ligada à chave utilizada, que é uma sequência de bits e dependendo do tipo utilizado quanto maior a chave, maior será a segurança obtida.(FAGUNDES, 2007).

A utilização da criptografia na sociedade está amplamente difundida, sendo encontrada em diversos serviços de mensagens que garantem a confidencialidade e a integridade das mensagens. Na área da saúde, por exemplo, os dados sensíveis dos pacientes são protegidos por meio dessa tecnologia. Além disso, a criptografia é amplamente aplicada em transações seguras realizadas por meio de aplicativos bancários, conhecidos como *internet bankings* (RAMIRO E CANTO, 2020).

Os autores Ramiro e Canto (2020) destacam 2 tipos de criptografia, que são:

- **Criptografia de chave privada ou criptografia simétrica:** É a técnica mais simples, pois a mesma chave é usada tanto para criptografar quanto para descriptografar a mensagem. Isso significa que o emissor e o receptor devem ter a mesma chave compartilhada previamente e mantê-la em segredo. Porém, há o risco de interceptação durante a transmissão da chave privada do emissor para o receptor da mensagem.

- **Criptografia de chave publica ou criptografia assimétrica:** Para combater os casos de interceptação de chave no modelo simétrico, o modelo assimétrico utiliza pares de chaves: uma chave pública, que é divulgada amplamente, e uma chave privada, conhecida somente pelo proprietário. As chaves de cifração e decifração são diferentes, sendo uma usada para criptografar a mensagem e a outra para descriptografá-la.

2.7 *Virtual Private Networks*

Segundo Braga(2012), redes virtuais privadas, em inglês, *Virtual Private Networks* (VPN), trata-se de uma rede de computadores criada sobre uma rede preexistente, tem como principal característica o tráfego privado, onde toda informação é transmitida de forma segura utilizando encriptação dos dados ou até mesmo realizando encapsulamento por outro protocolo de transporte, formando um túnel de acesso direto entre as duas pontas. Duas redes separadas fisicamente, podem se comunicar como um único enlace utilizando VPN (REZENDE, 2004).

> *"Para a realização dessa comunicação através de uma rede pública como a Internet, as VPNs se fundamentam em dois conceitos básicos, a criptografia e o tunelamento"* (REZENDE, 2004 p. 11)

O uso dessa tecnologia é variado, mas três notáveis aplicações são: intranet VPN, extranet VPN e acesso remoto VPN (CHIN; MIRANDA, 1998, 2002). Rossi e Franzin (2000) descrevem o acesso remoto sendo utilizado por usuários móveis que necessitam acessar a rede corporativa e podem fazê-la a partir de um computador em sua residência ou até mesmo por uma conexão *wireless* independente do lugar. Este tipo de conexão serve para conectar a empresa a seus colaboradores mesmo estando distante fisicamente(SILVA, 2016).

Miranda (2002) ressalta que uma autenticação rápida e eficiente do usuário remoto deve ser implementada para que o administrador possa garantir a identidade do usuário, bem como seu gerenciamento, que deve ser centralizado, pois é possível ter acesso de diversos usuários remotos e para efeitos de autenticação devem estar concentrados em um único lugar. A segurança destas redes são muito importantes, pois elas estão expostas a uma rede pública e uma vez conectado, temos informações sendo acessadas diretamente da empresa, uma medida de proteção física já não será possível, sendo necessário o uso de fortes sistemas de autenticação (REZENDE E GEUS, 2002).

Em seu trabalho Mosna e Moraes (2020), mostram a importância do acesso remoto ser feito de maneira segura, livre de interceptações indevidas e não autorizadas garantindo a

integridade, autenticidade, confiabilidade e a disponibilidade da informação, pilares da segurança dos dados.

> *"A VPN pode designar-se em uma alternativa segura para transmitir dados através de redes privadas ou públicas, uma vez que já ofertam recursos de autenticação e criptografia, com diversos níveis de segurança, proporcionando a eliminação dos links dedicados, de longa distância e de custos elevados, na conexão de WANs."*(MOSNA E MORAES, 2020)

Ao propor um sistema de gerenciamento unificado de ameaças, onde o uso de VPN interliga 2 filiais de uma mesma empresa, Piazza (2015) conclui que essas redes podem substituir circuitos MPLS e reduzir os custos dessa conexão remota e pode ser feita entre duas ou mais redes, de uma mesma companhia ou de diferentes parceiros/fornecedores.

Quanto a suas topologias, é possível dividir em dois grupos, a VPN *Remote Access,* do inglês, acesso remoto, também chamadas de *client-to-gateway* e VPNs *site-to-site*, também chamadas de *gateway-to-gateway* (NAKARUMA; GEUS, 2007; LAKBABI et al., 2012).

2.7.1 *Remote access* VPN

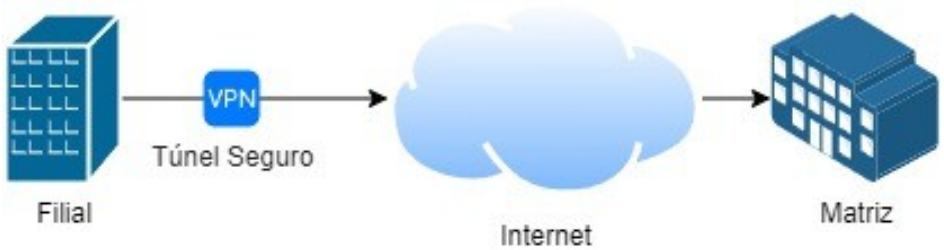
Através do uso de um cliente (software) que se conecta diretamente ao concentrador de VPN, é possível que usuários móveis trabalhem a partir de locais remotos como se estivessem conectados diretamente à rede corporativa, sem comprometer a segurança da corporação. Essa tecnologia permite que funcionários, usuários portáteis e escritórios remotos tenham acesso seguro aos recursos da rede como se estivessem diretamente conectados aos servidores da empresa (ELKEELANY et al., 2004).

2.7.2 *Site-To-Site* VPN

Site-to-site VPN é um tipo de conexão VPN permanente criada entre duas redes remotas separadas, permitindo a comunicação segura e contínua entre elas(LAKBABI et al., 2012) . Piazza (2015) mostra em seu estudo 3 sub-divisoes para a vpn site-to-site, sendo elas:

- **VPN *Site-to-Site* convencional:** Uma conexão entre dois pontos que permite que duas redes privadas diferentes se comuniquem e compartilhem recursos de rede (Figura 6).

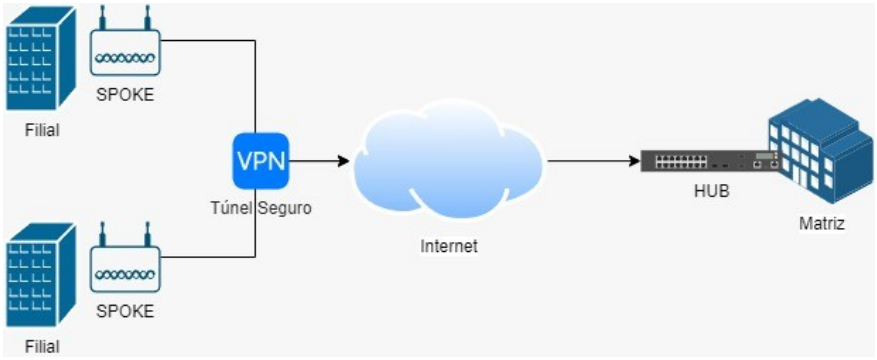
Figura 6 –VPN Ponto a Ponto convencional .



Fonte: Adaptado de Cisco(2022).

- **VPN *Site-to-Site Hub and Spoke*:** É uma modalidade em que há um ponto central de concentração entre os túneis VPN, geralmente atribuído à unidade matriz, e que todas as comunicações entre as redes remotas passam obrigatoriamente por esse ponto central de comunicação como na Figura 7.

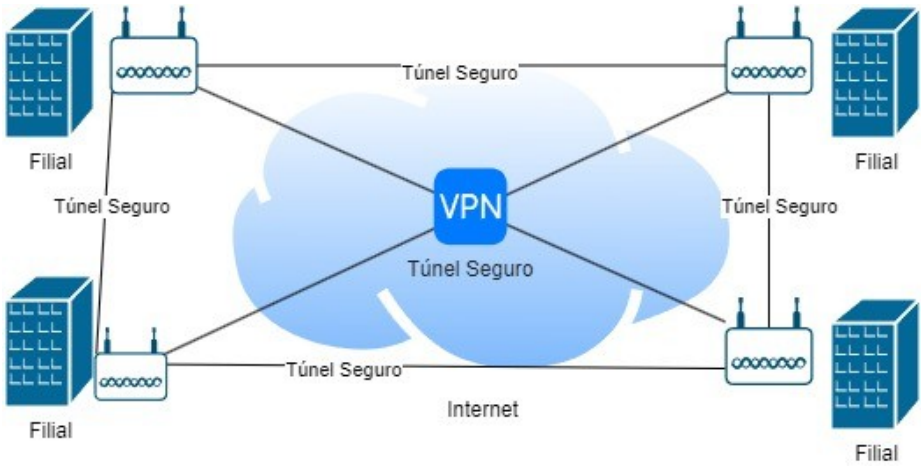
Figura 7 –VPN Hub and Spoke



Fonte: Adaptado de Cisco(2022).

- **VPN *Site-to-Site Mesh*:** É uma modalidade de VPN em que várias redes privadas se conectam diretamente entre si através de um túnel VPN independente e direto, sem depender de um ponto central de comunicação (Figura 8).

Figura 8 –VPN Site-to-Site Mesh



Fonte: Adaptado de Cisco(2022).

2.7.3 IPSec

IPsec é um conjunto de protocolos que protege as comunicações IP através da autenticação e criptografia de cada pacote IP em um fluxo de dados. Ele inclui protocolos para estabelecer a autenticação mútua entre os agentes no início da sessão de negociação e para usar chaves criptográficas durante a sessão. O IPsec pode ser usado para proteger o fluxo de dados entre um par de *hosts*, entre um par de *gateways* de segurança, como roteadores ou firewalls, ou entre um *gateway* de segurança e um host (MELLER, 2018).

O conjunto de protocolos IPsec possui três componentes principais: o cabeçalho de autenticação (AH) que garante a integridade dos pacotes e autêntica a sua origem, o cabeçalho de encapsulamento do *payload* (ESP) que provê a confidencialidade dos dados transmitidos pela rede pública e autenticação, e o protocolo de negociação e troca de chaves (*Internet Key Exchange* - IKE), que permite a negociação segura das chaves de comunicação entre as organizações, realizando autenticação e escolha das chaves criptográficas (NAKARUMA E GEUS,2007; ZHANG *et al* 2009; LUIS *et al*. 2003; DIAB *et al*. 2008; NARAYAN *et al*., 2009).

IPsec oferece dois modos diferentes de criptografia: modo de transporte e modo túnel. No modo de transporte, os dados protegidos pelo IPsec são transmitidos diretamente entre os *hosts*, fornecendo criptografia apenas para a parte de dados (*payload*) de cada pacote. Já no modo túnel, a segurança é fornecida entre duas redes, geralmente por meio de *gateways* IPsec, protegendo todo o pacote IP. O modo túnel é mais seguro, pois criptografa tanto o cabeçalho quanto o conteúdo. Ambas as modalidades são usadas para construir VPNs intranet e extranet (DIAB et al., 2008; NARAYAN et al., 2009; NAKARUMA; GEUS, 2007).

2.7.4 Trabalhos Relacionados

A integração de redes remotas utilizando VPNs é um tema de grande importância para a comunicação e segurança de dados em organizações. Nesse sentido, foram encontrados trabalhos correlatos que se aproximam da proposta deste trabalho.

Um dos trabalhos encontrados foi o de Silva (2017), que teve como objetivo implementar uma rede VPN para garantir a comunicação segura entre filiais de uma empresa. Para isso, o autor utilizou roteadores Cisco com suporte para VPN, implementando a topologia de rede ponto a ponto. Essa abordagem se assemelha à proposta deste trabalho, que também visa implementar uma solução de VPN para integrar redes remotas.

Outro trabalho que se aproxima da proposta deste trabalho é o de Santos (2018), que implementou uma solução de VPN para integrar redes de duas instituições de ensino. O autor utilizou o protocolo OpenVPN para a implementação da VPN, e obteve resultados satisfatórios em relação à segurança e performance da rede. Essa abordagem também é relevante para a proposta deste trabalho, que busca garantir a segurança e eficiência na comunicação entre redes remotas.

Por fim, destaca-se o trabalho de Oliveira (2019), que implementou uma solução de VPN utilizando a plataforma *pfSense* para garantir a comunicação segura entre as unidades de uma empresa. O autor utilizou o protocolo IPsec para a implementação da VPN, e obteve resultados satisfatórios em relação à segurança e performance da rede. Essa abordagem

também se aproxima da proposta deste trabalho, que buscou demonstrar através de estudo de caso a utilização de solução VPN para interligar redes remotas do Ministério Público Estadual de Alagoas.

Portanto, esses trabalhos correlatos são relevantes para a proposta deste trabalho, pois apresentam abordagens similares de implementação de VPN para integrar redes remotas, além de terem obtido resultados satisfatórios em relação à segurança e performance da rede.

3 METODOLOGIA

Este capitulo tem como objetivo descrever a metodologia utilizada na elaboração deste trabalho como, o tipo de pesquisa e suas abordagens, os instrumentos para a coleta de dados e o método de análise dos dados obtidos.

3.1 Tipo De Pesquisa

A pesquisa adotada neste trabalho é do tipo exploratória, pois se busca obter um maior conhecimento sobre o objeto de estudo, visando aprimorar o entendimento acerca do problema em questão (GIL, 2010). O estudo de caso é a estratégia de pesquisa escolhida para este trabalho. Estudo de caso é particularmente útil para investigar questões relacionadas a políticas públicas, organizações e instituições, bem como para explorar as relações entre diferentes fatores que influenciam o problema em questão pois permite uma análise detalhada e aprofundada de um caso específico (YIN 2015).

3.2 Coleta De Dados

A escolha dos instrumentos de coleta de dados foi baseada nas orientações de Gil (2008), que destacam a importância de selecionar instrumentos adequados à questão de pesquisa, ao objetivo do estudo e à natureza dos dados disponíveis. Esta que foi realizada por meio de entrevistas não estruturados com os responsáveis pela implantação da solução de rede, além de análise de documentos e registros relacionados à implantação e observação direta do processo de implantação.

3.3 Analise De Dados

A análise dos dados será realizada por meio da técnica de análise de conteúdo, que tem como objetivo identificar e interpretar as mensagens contidas nos dados coletados (BARDIN, 2011). A partir da análise dos dados, será possível descrever os procedimentos utilizados na implantação da solução de rede, apresentar as dificuldades encontradas durante o processo e avaliar a efetividade da solução de rede em garantir o acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça.

4. RESULTADOS E DISCUSSÕES

Os resultados da pesquisa foram obtidos a partir da análise de documentos oficiais, registros da implantação da solução de rede, entrevistas com os responsáveis pelo projeto e observação direta. Nesta seção, serão apresentados as informações obtidas, como o detalhamento da infraestrutura computacional necessária para implantação, além dos resultados que serão mostrados e discutidos com base nos objetivos específicos estabelecidos na introdução.

4.1 Infraestrutura Computacional

Os Pontos de Acesso Remotos (RAPs) utilizados foram da *Aruba Networks,* o modelo é o 303H (Figura 9), que possui um tamanho compacto e recursos como a facilidade de instalação em superfícies planas, três portas com fio (ethernet) para conexões locais, rádio Wi-Fi, opções de alimentação via energia e suporte a saída PoE (*Power over Ethernet*) para alimentar dispositivos de escritório, como cameras IP e telefones VoIP.

Figura 9 – Aruba AP-303H.

Fonte: Autor (2023)

Nessa implantação também foi utilizada a *Aruba Mobility Controller Virtual Appliance (ArubaMC-VA),* um dispositivo virtual conhecido por controladora, que permite aproveitar a infraestrutura de virtualização já existente para implantação uma rede sem fio corporativa em larga escala. Além disso, O Ministério Publico Estadual de Alagoas conta com infraestrutura própria de datacenter. Esta infraestrutura possui as tecnologias necessárias para a implementação desta solução, como:

- **Hipervisor:** Conhecido também por, monitor de máquina virtual, é responsável pelo gerenciamento e hospedagem de máquinas virtuais, neste estudo foi usado o *VMware ESXi* na versão *6.5;*
- **Firewall:** *Palo Alto Networks* PA-3020, será o responsável pelo gerenciamento de todo trafego de entrada e saída da rede;
- **Controlador de Domínio do Active Directory:** Este como maquinha convidada (virtualizada) no hipervisor, esta rodando em uma máquina Windows Server 2019.

4.2 Contexto E Necessidades Que Motivaram A Implantação

A implantação da solução de rede baseada em redes VPNs e RAPs foi motivada pela necessidade de garantir que todas as Promotorias de Justiça do Ministério Público Estadual de Alagoas tivessem acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça, de forma eficiente e segura. Antes da implantação da solução de rede, cada Promotoria de Justiça tinha sua própria rede, porém isolada sem integração, o que dificultava o compartilhamento de informações e recursos.

O Ministério Público é responsável por atuar como titular da ação penal pública na área criminal e pode realizar investigações criminais, especialmente em operações de combate ao crime organizado. Os Promotores de Justiça e servidores do Ministério Público de Alagoas atuam em todas as comarcas do Estado, o que garante uma cobertura mais ampla na defesa dos direitos dos cidadãos. Estas promotorias estão distribuídas em todo o estado, porém não estão em todos municípios, no interior do Estado as promotorias de justiça estão em sua maioria lotadas nos fóruns das comarcas do Tribunal de Justiça de Alagoas. Em cidades que possuem mais de uma promotoria como: Arapiraca (12 Promotorias de justiça), Penedo (6), Rio Largo (5), Delmiro Gouveia (3), Porto calvo (2), entre outras, estas possuem prédio próprio do MPE/AL.

Já na capital o cenário é diferente a maioria das promotorias estão lotadas no prédio das promotorias de justiça da capital, totalizando 23 promotorias, outras promotorias da capital estão distribuídas por Maceió em prédios próprios do MPE/AL, Fóruns e Juizados. A Estrutura do Ministério Público Estadual de Alagoas conta também com a Procuradoria-Geral de Justiça, sua sede, localizada também em Maceió.

Portanto, é neste contexto que se faz importante ter uma solução que garanta uniformidade no acesso aos recursos e informações disponíveis na Procuradoria-Geral de Justiça, com eficiência e segurança na comunicação e compartilhamento de dados, para otimizar o trabalho dos Promotores e servidores e garantir a entrega ágil e efetiva da justiça em todas as regiões do estado.

4.3 Procedimentos Utilizados Na Implantação Da Solução

Esta seção está dividida em outras três subseções que descreverão os procedimentos utilizados na aquisição, configuração e distribuição da solução.

4.3.1 Aquisição

Órgãos públicos estão submetidos a uma série de normas e regulamentações que visam garantir a legalidade, impessoalidade, moralidade, publicidade e eficiência na utilização do dinheiro público. Desta forma, para realizar uma compra, é necessário seguir um processo licitatório que visa garantir a escolha da melhor proposta dentre as apresentadas por empresas interessadas em fornecer o bem ou serviço, além de assegurar transparência e competitividade.

Nesse sentido a Ata de Registro de Preços (ARP) é uma alternativa à aquisição convencional que pode ser utilizada pelos órgãos e entidades da Administração Pública, de acordo com a Lei nº 8.666/93 (Lei de Licitações e Contratos). Esta modalidade de contratação é utilizada quando se pretende realizar uma aquisição conjunta de bens ou serviços para mais de um órgão ou entidade, ou quando não é possível definir previamente o quantitativo que será demandado pela Administração Pública.

Portando a aquisição dos pontos de acesso remotos utilizados neste estudo foi feito a partir da adesão à Ata de Registro de Preços nº 044/2017 – Pregão nº 117/2016-POE/MA da Comissão Central Permanente de Licitação - CCL do Estado do Maranhão. O quadro a seguir mostra os bens e serviços que foram fornecidos pela empresa que ganhou o processo licitatório.

Quadro 1 – Bens e serviços adquiridos por ARP.

Quantidade	DESCRIÇÃO DE HARDWARE E SOFTWARE
30 Und.	**Aruba IAP-305 (RW)** 802.11n/ac Dual 2x2:2/3x3:3 MU-MIMO Radio Integrated Antenna Instant AP
70 Und.	**Aruba AP-303H (RW)** Dual-radio 802.11ac 2x2 Unified Hospitality AP with Internal Antennas
100 Und.	**JW472AAE - Aruba LIC-AP** Controller per AP Capacity License E-LTU
100 Und.	**JW473AAE - Aruba LIC-PEF** Controller Policy Enforcement Firewall Per AP License E-LTU
100 Und.	**JW474AAE - Aruba LIC-RFP** Controller RFProtect Per AP License E-LTU
1 Und.	**JY900AAE Aruba MC-VA-250** Mobility Controller Virtual Appliance (RW) with Support for up to 250 AP E-LTU
	DESCRIÇÃO DOS SERVIÇOS
Instalação e configuração dos Pontos de Acesso;	

Atendimento e assistência técnica “on-site” da solução implementada por um período de 36 (trinta e seis) meses;

Implementação de controladora virtual WLAN integrando solução de segurança para políticas de acesso.

Fonte: Ministério Publico Estadual de Alagoas (2018)

4.3.2 Configuração

Após a aquisição e entrega dos bens e serviços adquiridos previsto na Adesão de Registro de Preços, a implantação da controladora virtual foi feita pela mesma empresa que forneceu os pontos de acesso, as licenças e o suporte técnico, este último, foi responsável pela instalação inicial da controladora virtual na infraestrutura do Ministério Publico Estadual de Alagoas.

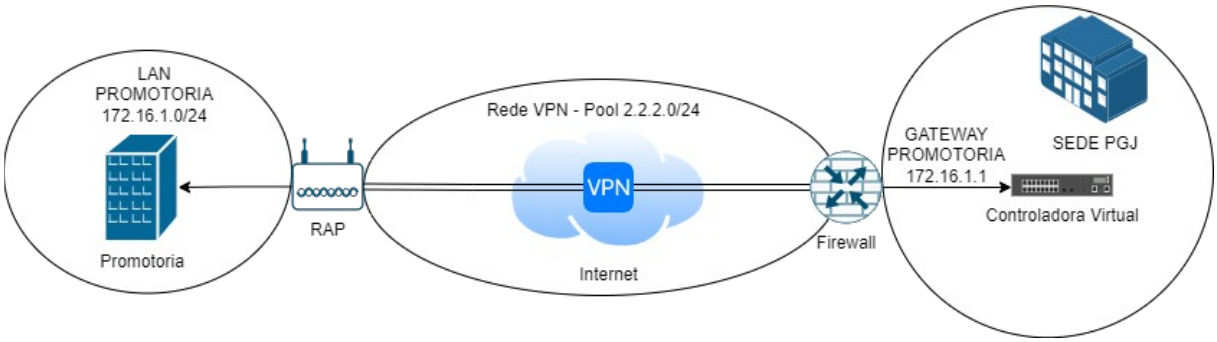
Além do provisionamento da controladora virtual, o suporte técnico contratado também foi o responsável pela migração da rede sem fio (WLAN) da antiga controladora para esta, bem como a integração com a autenticação do tipo *Protected Extensible Authentication Protocol Microsoft Challenge Handshake Authentication Protocol version 2* (PEAP-MS-CHAPv2), que utiliza as credenciais da conta do usuário (nome de usuário e senha) armazenadas nos Serviços de Domínio *Active Directory* para autenticar clientes de acesso sem fio.

Até então a solução ainda estava restrita apenas à sede, onde foi instalada a controladora virtual, a esta altura, um ponto de acesso que for provisionado junto a controladora será capaz de propagar o sinal da rede WLAN criada na configuração inicial e o usuário, capaz de autenticar utilizando suas credenciais do AD, porém para que os pontos de acesso pudessem funcionar de forma remota foram necessárias a aplicação de configurações que foram descritas em entrevista, pela equipe da Seção de Administração de Redes e Apoio Operacional na seguinte ordem:

- **Configurar VPN no *Mobility Controller*:** Como IP *pools*, Configurações de IPSec e criptografia*;*
- **Definir grupos para pontos de acesso:** Foi feito pensando em atender todas as promotorias lotadas em uma determinada cidade/comarca, onde para cada grupo criado foi atribuída uma sub-rede e uma VLAN;
- **Provisionar os pontos de acessos:** Nesta fase os pontos de acesso foram submetidos a uma configuração chamada de provisionamento, que torna aquele equipamento gerenciável pela controladora, onde esta fica responsável por suas configurações, como por exemplo a atribuição aos grupos anteriormente criados, modo de operação entre outras;

- **Disponibilizar os serviços TI a toda rede VPN:** Com os pontos de acesso provisionados e seus grupos definidos chegou a hora de integrar esta rede e garantir o acesso aos mesmos recursos e informações disponíveis na Procuradoria-Geral de Justiça, de forma eficiente e segura e o grande responsável por isso foi o *firewall* e a controladora que se comunicam entre si e fazem o roteamento entre as redes criadas, desta forma, é possível gerenciar e direcionar todo trafego de entrada e saída (Figura10).

Figura 10→ Firewall de borda e Tunel VPN.



Fonte: Autor (2023).

4.3.3 Distribuição

Com os equipamentos devidamente configurados foi montada uma força tarefa para realizar a entrega dos pontos de acessos pelo interior do Estado, bem como sua instalação no local, que necessita apenas de uma conexão com a Internet, que é responsável pela conexão do RAP com a Controladora, quando conectado nenhuma outra conexão será necessária, os computadores, switchs, impressoras e câmeras, que se conectarem ao RAP estarão aptos a usufruir todos serviços que antes eram disponibilizados na sede PGJ.

4.4 Desafios Encontrados

Durante a implantação da solução de rede baseada em redes VPNs e RAPs, foram encontrados alguns desafios que demandaram esforços adicionais da equipe responsável pelo projeto. Um dos principais desafios foi adicionar todas as estações de trabalho ao controlador de domínio, bem como a criação dos usuários no *active directory*, onde muitos usuários eram cedidos das prefeituras e tiveram que entrar em contato com a Diretoria de Recursos Humanos para atender a regulamentação exigida. Muitas pessoas que não eram do MPE/AL utilizavam os recursos de Internet antes da implantação da solução justamente por não ter a necessidade de autenticação dos usuários e faziam com que o serviço apresentasse lentidão para quem estava realizando as atividades ministeriais.

Embora as redes VPN tenham diversas vantagens como foram citadas diversas vezes ao longo desta monografia, também foram observadas algumas desvantagens, tais como: Velocidade, Complexidade, Segurança, Dependência do fornecedor e Custos.

4.5 Efetividade Da Solução De Rede Em Garantir O Acesso Aos Mesmos Recursos E Informações Disponíveis Na Procuradoria-Geral De Justiça

O teste de conexão foi realizado com o objetivo de avaliar a Efetividade da solução VPN, para isso, foi comparado com mais três tipos de conexões, conexão local, Internet Banda Larga e Internet móvel, o serviço mais acessado, o SAJ, foi o serviço escolhido para o teste e o protocolo ICMP foi escolhido devido à sua capacidade de fornecer informações sobre a conectividade e a latência de rede, todos os testes foram realizados por volta das 10 horas, considerado horário de pico da utilização desta aplicação. Então o teste foi conduzido utilizando quatro conexões de internet distintas: a solução VPN, conexões local de um computador localizado na sede onde fica hospedado o servidor, outra conexão uma utilizando um modem 4G e por fim a Internet banda larga. Para todas as conexões, foram enviados pacotes com tamanho de 1460 bytes, totalizando um evento de 300 pacotes, para os testes realizados com a solução VPN e conexão local diretamente conectada o endereço apresentado será o IP privado utilizado pelo servidor que disponibiliza a aplicação, já para as conexões externar será apresentada um IP publico, valido na internet para roteamento. Os resultados obtidos foram:

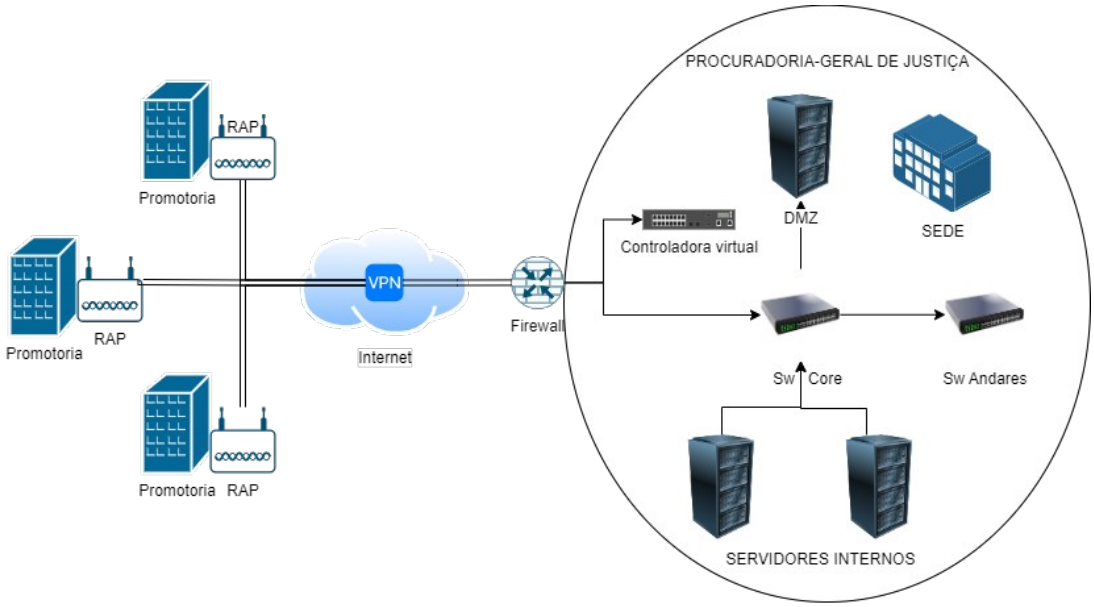
- **Solução VPN:** Estatísticas do Ping para 192.168.253.11:
  Pacotes: Enviados = 300, Recebidos = 300, Perdidos = 0 (0% de perda), latência em milissegundos: Mínimo = 2ms, Máximo = 90ms, Media = 4ms.
- **Conexão Local:** Estatísticas do Ping para 192.168.253.11:
  Pacotes: Enviados = 300, Recebidos = 300, Perdidos = 0 (0% de perda), latência em milissegundos: Mínimo = 1ms, Máximo = 50ms, Media = 1ms.
- **Internet Móvel 4g:** Estatísticas do Ping para 177.12.227.123:
  Pacotes: Enviados = 300, Recebidos = 300, Perdidos = 0 (0% de perda), latência em milissegundos: Mínimo = 78ms, Máximo = 1087ms, Media = 110ms.
- **Internet Banda larga:** Estatísticas do Ping para 177.12.227.123:
  Pacotes: Enviados = 300, Recebidos = 296, Perdidos = 4 (1% de perda), latência em milissegundos: Mínimo = 37ms, Máximo = 232ms, Media = 58ms.

4.6 Discussão

A análise de conteúdo de Bardin (2011) foi utilizada para relacionar os resultados e discussões desta pesquisa com os objetivos propostos. Através da pesquisa exploratória, identificou-se que a implantação da solução de rede baseada em redes VPNs e RAPs foi motivada pela necessidade de garantir o acesso eficiente e seguro a recursos e informações disponíveis na Procuradoria-Geral de Justiça para todas as Promotorias de Justiça do Ministério Público Estadual de Alagoas. Essa análise foi conduzida com base na documentação fornecida, entrevistas com os responsáveis e da observação direta.

Os resultados indicaram que a implantação da solução resultou em nova topologia de rede (Figura 11), esta foi responsável por sanar as desvantagens observadas pela topologia antiga, além de garantir o acesso seguro a recursos e informações disponíveis na Procuradoria-Geral de Justiça para todas as Promotorias de Justiça, algo que não existia anteriormente, seu impacto foi significativo na eficiência e segurança do trabalho dos membros, servidores e outros colaboradores.

Figura 11→ Topologia final.



Fonte: Autor (2023)

Entretanto os desafios encontrados na implantação demonstrou que após a distribuição dos equipamentos foi necessário um esforço grande por parte da equipe em adicionar os computadores ao controlador de domínio que antes não faziam parte da rede corporativa, a criação de novos usuários para se autenticarem e ter acesso à rede e seus recursos, além de fatores determinantes na escolha do uso de redes VPNs como:

- **Velocidade:** a criptografia dos dados pode reduzir a velocidade da conexão, especialmente em redes mais lentas ou que necessitam de baixa latência, o que pode afetar a qualidade do serviço.
- **Complexidade:** configurar e gerenciar uma rede VPN pode ser uma tarefa complexa, especialmente para usuários menos experientes, o que pode levar a problemas de segurança e desempenho.
- **Segurança:** embora as VPNs sejam projetadas para aumentar a segurança da rede, também podem apresentar vulnerabilidades e serem alvos de ataques cibernéticos.
- **Dependência do fornecedor:** muitas empresas que fornecem serviços de VPN têm controle total sobre a rede e os dados do usuário, o que pode levantar questões de privacidade e segurança. Principalmente, quando se trata de tecnologia proprietária como é o caso do equipamento HPE Aruba.
- **Custos:** em alguns casos, as VPNs podem ser mais caras do que outras soluções de rede, especialmente se a empresa precisar de recursos avançados ou personalizados.

No caso do MPE/AL, as vantagens superaram as desvantagens. Um dos pontos de destaque levados em conta é a mobilidade de implantação da solução. Sem burocracias, é possível realizar a conexão utilizando inclusive redes do TJAL, como no Fórum do Barro Duro, bem como em eventos realizados no TCE/AL, Centro de Convenções, entre outros. Bastando apenas uma conexão à Internet para levar toda a configuração de segurança ao local, em um evento no centro de convenções, por exemplo, todos os dispositivos móveis dos integrantes do MPE/AL se conectariam automaticamente como ocorre quando estão em qualquer unidade ministerial.

Quanto a sua efetividade a solução VPN apresentou a menor latência, em comparação com outros acessos externos, ficando atrás apenas da conexão local que fez uma média de 1ms, indicando uma resposta rápida e eficiente entre o emissor e o receptor. A Solução VPN registrou uma média de latência de 4ms, também considerada baixa, proporcionando uma boa qualidade de conexão.

Por outro lado o modem 4G apresentou uma média de latência de 110ms, indicando um tempo de resposta relativamente mais longo devido à natureza das redes móveis. Já a Internet Banda Larga registrou uma média de latência de 58ms, posicionando-se em um nível intermediário em relação às demais conexões, além disso, é importante ressaltar que a

conexão banda larga apresentou uma taxa de perda de pacotes de 1%, o que indica uma pequena proporção de pacotes não recebidos com sucesso em relação ao total enviado.

A análise de conteúdo de Bardin (2011) também permitiu relacionar os resultados e discussões desta pesquisa aos trabalhos correlatos, ao comparar a solução proposta neste trabalho com os trabalhos correlatos de Silva (2017), Santos (2018) e Oliveira (2019), pode-se observar que todos eles apresentaram soluções para a integração de redes remotas utilizando VPNs.

Silva (2017) propôs implementar uma rede VPN para garantir a comunicação segura entre filiais de uma empresa. A solução de Silva apresentou bons resultados no que diz respeito à segurança das conexões, mas a implantação da solução foi complexa e exigiu conhecimentos técnicos específicos além do uso de diversos equipamentos que em larga escala se torna custoso a instituição.

Santos (2018), por sua vez, apresentou uma solução para a integração de redes remotas utilizando o protocolo IPSec. A solução proposta por Santos mostrou-se eficiente e de fácil implementação, mas a segurança das conexões foi considerada um ponto fraco da solução.

Já Oliveira (2019) apresentou uma solução de integração de redes remotas utilizando o protocolo SSL VPN. A solução proposta por Oliveira mostrou-se segura e de fácil implementação, mas apresentou problemas de desempenho em grandes redes.

Ao comparar com esses trabalhos, a solução proposta neste estudo apresentou bons resultados tanto no que diz respeito à segurança das conexões, quanto à eficiência e desempenho da solução, por exemplo esta solução conta com aparelhos que além de serem APs possuem a função de *switch, firewall,* VPN, entre outros, este equipamento multifuncional reduziu custos, se comparado a utilização de uma solução tradicional mostrada nos estudos correlatos onde, cada unidade deveria possuir um *Firewall*, *Switch*, AP para ter acesso aos mesmos recursos, informações e serviços que a controladora Aruba e RAPs proporcionaram ao MPE/AL. A instituição precisaria de recursos financeiros e humanos significativos para manter tudo funcionando sem gestão centralizada.

Portanto, pode-se concluir que a solução descrita neste trabalho apresentou resultados positivos e superou alguns desafios encontrados em outras soluções apresentadas na literatura. No entanto, é importante destacar que cada instituição possui necessidades específicas e, portanto, a solução proposta deve ser avaliada e adaptada de acordo com as necessidades de cada organização.

5. CONCLUSÕES

A partir dos resultados apresentados, pode-se concluir que a implantação da solução de rede baseada em redes VPNs e RAPs atingiu seus objetivos, proporcionando acesso seguro por meio da adoção de políticas de segurança institucionais entre as Promotorias de Justiça geograficamente distribuídas e a Procuradoria-Geral de Justiça do Ministério Público do Estado de Alagoas, para que compartilhem os mesmos recursos tecnológicos disponibilizados.

A análise dos dados coletados permitiu constatar que a solução de rede implementada foi efetiva em garantir a integração e compartilhamento de informações entre as unidades do MPE/AL, facilitando a comunicação e a troca de informações entre as Promotorias de Justiça e a Procuradoria-Geral de Justiça.

Como foi possível observar, a implantação da rede VPN demonstrou ser uma solução eficaz para propor o acesso seguro aos recursos tecnológicos compartilhados, proporcionando benefícios significativos à organização. Através da adoção de políticas de segurança adequadas, foi possível proteger as informações sensíveis e minimizar riscos de acesso não autorizado. Além disso, a utilização dessa tecnologia permitiu que colaboradores, parceiros e fornecedores pudessem ter acesso à rede de forma remota, mantendo a produtividade e a colaboração mesmo em ambientes distribuídos geograficamente.

A partir dos procedimentos utilizados na implantação da solução de rede, foi possível perceber a importância da elaboração de um plano de projeto bem definido e detalhado, que contemplasse as necessidades específicas do MPE/AL, além da escolha adequada dos equipamentos e softwares utilizados na solução.

Diante do exposto, é possível afirmar que a implantação da solução de rede descrita neste trabalho atendeu aos objetivos propostos e é possível afirmar que trouxe benefícios significativos para a rotina de trabalho do Ministério Público Estadual de Alagoas. Espera-se que este trabalho possa servir como referência para outras instituições que buscam soluções semelhantes para seus desafios de conectividade e compartilhamento de informações.

REFERÊNCIAS

ANDRADE E CASTRO, Robledo. Uma análise de Soluçoes VPN em redes corporativas de alta capilaridade. 2004. Dissertação (Mestrado Profissional) - Universidade Estadual de Campinas, Instituto de Computação, [S. l.], 2004.

BARDIN, L. Análise de conteúdo. 3. ed. São paulo: Edições 70, 2011.

BARREIROS, Carlos Carone. O SMB/CFIS. [S. l.], 2001. Disponível em: https://www.gta.ufrj.br/grad/01_2/samba/samba.htm. Acesso em: 1 mar. 2023.

BHARDWAJ, P. K. A+, Network+, Security+ Network security exams in a nutshell. 1. ed. [S. l.]: O'Reilly, 2007. 787 p.

BRAGA, V. Soluções Open-source para os Serviços de Fax e VPN numa Rede Empresarial. 2012. Dissertação (Mestrado Engenharia Electrotécnica e de Computadores) - Faculdade de Engenharia da Universidade do Porto, FEUP -Departamento de Engenharia Informática, [S. l.], 2012.

BRENTON, C.; HUNT, C. Active Defense - A Comprehensive Guide to Network Security 1 ed. Alameda: Ed. Sybex, 2001. 723 p.

CHIN, Liou Kuo. Rede Privada Virtual - VPN. Boletim bimestral sobre tecnologia de redes, [s. l.], v. 2, 13 nov. 1998. Disponível em: https://memoria.rnp.br/newsgen/9811/vpn.html. Acesso em: 21 fev. 2023.

CISCO , Systems, Inc. User Guide for Cisco Security Manager 4.26: Managing Site-to-Site VPNs: The Basics. Cisco, [S. l.], p. 1, 14 dez. 2022. Disponível em: https://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/426/User/csm-user-guide-426/chapter25-managing-site-to-site-vpns.html. Acesso em: 19 dez. 2022.

DIAB, Wafaa Bou; TOHMÉ, Samir; BASSIL , Carole. VPN Analysis and New Perspective for Securing Voice over VPN Networks. Fourth International Conference on Networking and Services, [s. l.], p. 73-78, 2008. Disponível em: https://www.researchgate.net/publication/4325818_VPN_Analysis_and_New_Perspective_for_Securing_Voice_over_VPN_Networks. Acesso em: 17 jan. 2023.

ELKEELANY, O.; MATALGAH, M. M.; QADDOUR, J. Remote access virtual private network architecture for high-speed wireless internet users. Wireless Communications and Mobile Computing, v. 4, n. 5, p. 567–578, 2004. ISSN 15308669.

FAGUNDES , Bruno Alves. Uma Implementação de VPN. 2007. TCC (Bacharelado Tecnologia da Informação e da Comunicação) - FUNDAÇÃO DE APOIO À ESCOLA TÉCNICA DO ESTADO DO RIO DE JANEIRO INSTITUTO SUPERIOR DE TECNOLOGIA EM CIÊNCIA DA COMPUTAÇÃO LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA, Rio de Janeiro, 2007.

FOROUZAN, Behrouz A. Protocolo TCP/IP. 3ª ed. Porto Alegre: Amgh, 2010.

GIL, A. C. Como elaborar projetos de pesquisa. 4. ed. São Paulo: Atlas, 2008.

Gil, A. C. Como elaborar projetos de pesquisa.5. ed. São Paulo: Atlas, 2010.

JUNIOR, Raul F. da Silva. DMZ-DeMilitarized Zone: Tratativas, métricas e zonas de segurança em redes LAN. Instituto Nacional de Pesquisas Espaciais-INPE, 2010

KOTLER, P.; KELLER, K. L. Administração de Marketing. 12. ed. São Paulo: Pearson Prentice Hall, 2006. 750 p.

KUROSE, James F. Camada de Aplicação. In: KUROSE, James F. Redes de computadores e a internet: uma abordagem Top-Down. 5. ed. São Paulo/SP: Pearson, 2010. cap 2. Pag. 96 – 102.

LAKBABI, A. et al. VPN IPSEC & SSL Technology. Next Generation Networks and Services NGNS, n. December, p. 2–4, 2012.

LEAL, Matheus Carvalho; PEREIRA FILHO, Marcelo Renato do Carmo. A IMPORTANCIA DA VPN (VIRTUAL PRIVATE NETWORK) DURANTE A PANDEMIA COVID19: UMA REVISÃO DE LITERATURA. Facit Business and Technology Journal, [s. l.], n. 31, ed. 1, 1 out. 2021.

LORIATO, L. A.; LORIATO, L. A. PROTÓTIPO DE ANTI-VÍRUS ESTÁTICO COM VERIFICAÇÃO ONACCESS EM AMBIENTE WINDOWS UTILIZANDO A ENGINE DO CLAMAV. 2008. Dissertação (Graduado em Engenharia de Sistemas e Computação) - Instituto Militar de Engenharia, [S. l.], 2008. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2008-Loriatos.pdf. Acesso em: 14 fev. 2023.

LUIS, A. et al. IPSec Segurança de Redes – INF542. 2003. 1–49 p.

MELLER, Felipe Jhonas. Comparativo dos protocolos IPSec e SSL na utilização de VPNs corporativas. 2018. Trabalho de Conclusão de Curso (Bacharelado em Ciência da Computação) - Universidade Tecnológica Federal do Paraná, Medianeira, 2018.
MENDES, Douglas Rocha. Redes de computadores: Teoria e Prática. São Paulo: Novatec,2007.

MIRANDA, I. C. VPN - Virtual Private Network: Rede Privada Virtual. Universidade Federal do Rio de Janeiro - UFRJ, Departamento de Engenharia Eletrônica e de Computação - DEL, Rio de Janeiro. 2002

MORIMOTO, Carlos E. Endereços e Compartilhamentos. In: MORIMOTO, Carlos E. Redes e servidores linux guia prático. 2.ed. Porto Alegre: Sul Editores, 2006. p. 60-65.

MOSNA, Eduardo, MORAES, Matheus Pissaia de. Configuração de VPN site-to-site e client-to-site com OpenVPN e routerboard MikroTik, 2020. Relatório técnico (Curso Superior de Tecnoclogia em Segurança da Informação) - Faculdade de Tecnologia de Americana, 2020

NAKARUMA, E. T.; GEUS, P. L. de. Segurança de Redes: em ambientes cooperativos. 1. ed. Sao Paulo: Novatec, 2007. 482 p

NARAYAN, S.; BROOKING, K.; VERE, S. D. Network Performance Analysis of VPN Protocols : An empirical comparison on different operating systems. 2009.

OLIVEIRA, F. A. Implementação de VPN utilizando a plataforma pfSense para comunicação segura entre unidades de uma empresa. 2019. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores) - Instituto Federal de Educação, Ciência e Tecnologia de São Paulo, São Paulo, 2019.

PIAZZA, Tiago. Análise da implantação e utilização de sistemas de gerenciamento unificado de ameaças (Unified Threat Management – UTM) em empresas de diferentes portes. 2015. Monografia (Graduação em Engenharia da Computação) – Universidade do Vale do Taquari - Univates, Lajeado, 27 nov. 2015.

RAMIRO, André; CANTO, Mariana. A importância social e econômica da Criptografia. Recife: Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), 2020. Disponível em: https://cartilhacriptografia.direitosnarede.org.br/cartilhacriptografia.pdf. Acesso em: 1 fev. 2023.

REZENDE, E. R. S. Segurança no acesso remoto VPN. 2004. 127 f. Dissertação (Mestrado em mestrado em ciência da computação). Instituto de Computação Unicamp, Campinas, SP, 2004

REZENDE, E.; GEUS, P. Uma solução segura e escalável para acesso remoto VPN. SCIENTIA Revista de Computação da Unisinos, 2002.

RIOS, Renan Osório. Protocolos e serviços de redes: curso técnico em informática. Protocolos e serviços de redes, [S. l.], p. 1-80, 30 jan. 2010. Disponível em: http://redeetec.mec.gov.br/images/stories/pdf/eixo_infor_comun/tec_inf/ 081112_protserv_redes.pdf. Acesso em: 11 jan. 2023.

ROSSI, M.; FRANZIN, O. VPN - Virtual Private Network (Rede Privada Virtual). GPr Sistemas/ASP Systems. Ago. 2000.

ROVER, Marinho. O que é Active Directory, topologia física e lógica? Parte1, 2012. Disponível em: <https://technet.microsoft.com/pt-br/library/jj206711.aspx>.Acesso em: 16 jun. 2022.

SANTOS, Fabiana Helena; ALBERTIN, Leonardo Antônio. SEGMENTAÇÃO DE REDES COM VLANEM UMA EMPRESA DE TELECOMUNICAÇÃO. 7º Congresso Tecnológico da Fatec Mococa, [s. l.], 25 out. 2021. Disponível em: https://congresso.fatecmococa.edu.br/index.php/congresso/article/view/227. Acesso em: 26 out. 2022.

SANTOS, J. S. Implementação de uma solução VPN para integrar redes de duas instituições de ensino. 2018. Trabalho de Conclusão de Curso (Graduação em Redes de Computadores) - Universidade Federal do Ceará, Fortaleza, 2018.

SILVA, A. R. Implementação de uma rede VPN para garantir a comunicação segura entre filiais de uma empresa. 2017. Trabalho de Conclusão de Curso (Graduação em Sistemas de Informação) - Faculdade de Tecnologia Senac Pelotas, Pelotas, 2017.

SILVA, C. Descubra por que usar uma VPN e veja como escolher a melhor. Canaltech. 2016. Disponível em: https://canaltech.com.br/internet/descubra-por-que-usar-uma-vpn-e-veja-como-escolher-a-melhor . Acesso em: 15 jun. 2022

STALLINGS, W. Comunicação de Dados e Redes de Computadores.2014 (8th ed.). São Paulo: Pearson Education.

STANEK, William R.; BANIN, Gilson. Arquitetura do Active Directory. In: STANEK, William R.; BANIN, Gilson. Windows server 2008: guia completo. Porto Alegre: Bookman, 2009. Cap 29, p. 1023-1042.

STEIN, Clifford et al. Algoritmos – Teoria e Prática. 2ª edição. São Paulo: Cengage Learning, 2010.

SWANSON, E. B. (2018). Information technology and organizational learning: Solving the management paradox. Routledge.

TANENBAUM, A. S. Redes de Computadores 4ª Ed., Rio de Janeiro Editora Campus (Elsevier), 2003. 946 p.

TANENBAUM, A. S. Redes de Computadores 5ª Ed., Rio de Janeiro Editora Campus (Elsevier), 2011.

VMWARE. O que é rede corporativa?. 2022. Disponível em: https://www.vmware.com/br/topics/glossary/content/enterprise-networking.html | Glossário da VMware | BR. Acesso em 14/06/2022.

YIN, R. K. Estudo de caso: planejamento e métodos. 5. ed. Porto Alegre: Bookman, 2015.

ZHANG, Y. et al. A New Approach for Accelerating IPSec Communication. International Conference on Multimedia Information Networking and Security, 2009.