PROPOSTA TÉCNICA – PROJETO DE REDE CORPORATIVA

Cliente: Werneck S/A

Autor: Adriel Shimaski Alves da Cruz

Curso: Cybersec -Vai na web/kensei

Data: 28/07/2025

Versão: 1.0

SUMÁRIO EXECUTIVO

A Werneck S/A está em processo de crescimento e precisa de uma rede moderna e segura para conectar sua sede em São Paulo e as filiais no Rio de Janeiro e em Minas Gerais.

A proposta tem como objetivo criar uma estrutura de rede organizada, com divisões claras entre os setores da empresa, controle sobre quem acessa o quê e proteção das informações. Também considera a possibilidade de expansão futura da empresa.

Para isso, será implantada uma rede segmentada por áreas (usando VLANs — que separam os departamentos na rede, como TI, Financeiro, etc.), interligada por conexões seguras (VPNs — uma espécie de túnel protegido que conecta os escritórios pela internet). Um firewall (sistema que controla o que entra e sai da rede) será utilizado para aplicar regras de acesso e proteger contra ameaças. Além disso, será criada uma rede separada para visitantes, mantendo a segurança da rede principal.

Essa solução oferece mais proteção, desempenho e flexibilidade, dando à empresa uma base tecnológica sólida e preparada para o crescimento.

OBJETIVO

O objetivo desta proposta é criar uma rede moderna e bem organizada para a empresa Werneck S/A, conectando a matriz em São Paulo com as filiais no Rio de Janeiro e em Minas Gerais.

SEGURANÇA

A nova estrutura deve garantir segurança, desempenho e controle de acessos, permitindo que cada setor da empresa tenha sua área de rede separada, evitando acessos indevidos.

CRESCIMENTO

Além de atender às necessidades atuais, essa rede será planejada pensando no crescimento da empresa, permitindo futuras expansões sem comprometer a estabilidade ou a proteção dos dados.

ESCOPO

Este projeto propõe a criação de uma rede de computadores para a matriz em São Paulo e as filiais no Rio de Janeiro e Minas Gerais. O objetivo é garantir que a rede funcione de forma segura, organizada e eficiente para todas as unidades.

SEGMENTAÇÃO POR VLANS

Isso significa dividir a rede em partes menores para separar os departamentos, como Administrativo, Financeiro, TI e Atendimento, e também criar uma rede separada para visitantes. Essa separação ajuda a proteger as informações e evita que problemas em uma parte da rede afetem o restante.

VPN SITE-TO-SITE

É uma conexão segura que liga as diferentes unidades da empresa (matriz e filiais), permitindo que elas compartilhem dados de forma protegida pela internet, como se estivessem na mesma rede local.

ACESSO REMOTO SEGURO

Permite que funcionários autorizados se conectem à rede da empresa mesmo estando fora do escritório, usando conexões protegidas para garantir a segurança das informações.

FIREWALL

É um sistema de proteção que controla quem pode acessar a rede e o que pode ser feito nela, ajudando a impedir ataques e manter os dados seguros. Além disso, ele registra atividades para que a equipe de TI possa monitorar o que acontece na rede.

INTEGRAÇÃO COM SERVIÇOS EM NUVEM

A rede será preparada para funcionar com ferramentas online que a empresa utiliza, como o Office 365 e sistemas de CRM, garantindo que o acesso a esses serviços seja rápido e seguro.

METODOLOGIA

ANÁLISE DO BRIEFING

Primeiro, analisamos o briefing do cliente para entender as necessidades da empresa, o número de funcionários, os departamentos e as filiais.

IDENTIFICAÇÃO DE REQUISITOS

Em seguida, identificamos os requisitos técnicos, como a necessidade de segurança, segmentação da rede, acesso remoto e integração com serviços em nuvem.

ELABORAÇÃO DO PLANO

Por fim, elaboramos um plano de ação para implementar a rede, focando nas ações mais importantes primeiro, usando o modelo 80/20.

DESENHO DA ARQUITETURA

Com essas informações, desenhamos a arquitetura da rede, definindo as VLANs para separar os departamentos, as conexões VPN entre matriz e filiais, e as políticas de segurança.

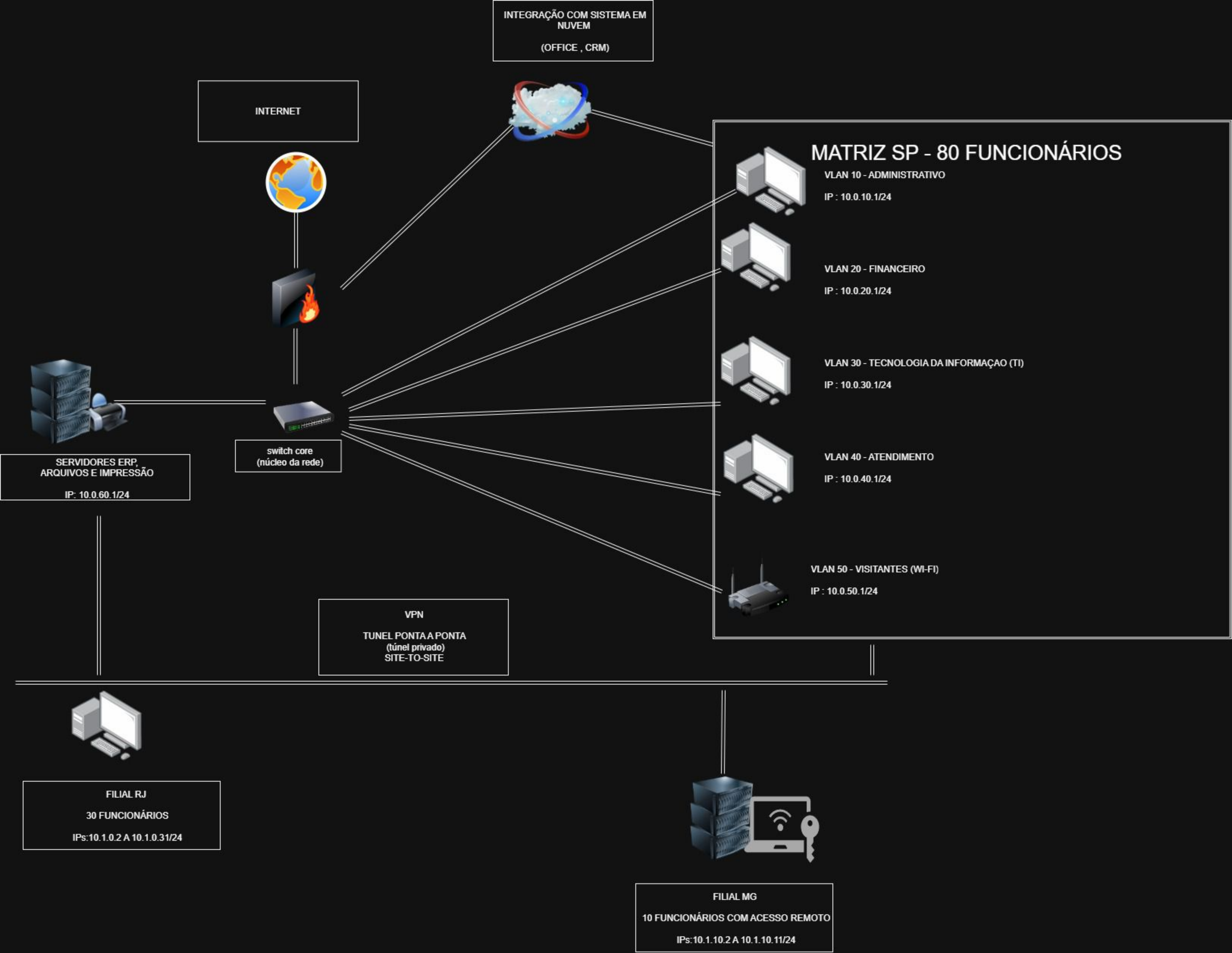
CRIAÇÃO DO DIAGRAMA

Criamos o diagrama lógico da rede, que é uma representação visual para ajudar a entender como a rede vai funcionar.

JUSTIFICATIVA TÉCNICA

Depois, justificamos as escolhas técnicas feitas, explicando por que cada solução foi escolhida, focando em segurança, desempenho e facilidade de manutenção.

DIAGRAMA


INTEGRAÇÃO COM SISTEMA EM NUVEM
(OFFICE , CRM)
INTERNET
MATRIZ SP - 80 FUNCIONÁRIOS
VLAN 10 - ADMINISTRATIVO
IP : 10.0.10.1/24
VLAN 20 - FINANCEIRO
IP : 10.0.20.1/24
VLAN 30 - TECNOLOGIA DA INFORMAÇAO (TI)
IP : 10.0.30.1/24
VLAN 40 - ATENDIMENTO
IP : 10.0.40.1/24
VLAN 50 - VISITANTES (WI-FI)
IP : 10.0.50.1/24
SERVIDORES ERP, ARQUIVOS E IMPRESSÃO
IP: 10.0.60.1/24
switch core (núcleo da rede)
VPN
TUNEL PONTA A PONTA
(túnel privado)
SITE-TO-SITE
FILIAL RJ
30 FUNCIONÁRIOS
IPs:10.1.0.2 A 10.1.0.31/24
FILIAL MG
10 FUNCIONÁRIOS COM ACESSO REMOTO
IPs:10.1.10.2 A 10.1.10.11/24

EXPLICAÇÃO DO DIAGRAMA DE REDE E ROTAS FEITAS

1 NÚCLEO DA REDE (SWITCH CORE)

Tudo parte do **Switch Core**, que centraliza o tráfego de rede na **Matriz SP**. Esse switch está conectado:

- Ao **firewall**, que fornece acesso à Internet.
- Às VLANs internas.
- Aos **servidores ERP, arquivos e impressão**.
- Às conexões VPN (site-to-site) com as filiais (RJ e MG).

2 TRÁFEGO DENTRO DA MATRIZ SP

1. COMUNICAÇÃO ENTRE VLANS (INTERNA):

Dispositivos das VLANs 10, 20, 30, 40 e 50 estão todos ligados ao Switch Core. Supondo que ele tenha **de camada de rede** (com capacidade de roteamento), ele permite que:

- Um computador na **VLAN 10** (`10.0.10.10`) envie dados para um servidor da **VLAN 30** (`10.0.30.10`).
- Um funcionário do Financeiro acesse arquivos no servidor `10.0.60.1` da VLAN ERP, por exemplo.

Isso é feito por **roteamento interno** entre as sub-redes definidas nas VLANs.

3 TRÁFEGO COM INTERNET

2. SAÍDA PARA A INTERNET:

- Todos os pacotes destinados à internet são enviados do Switch Core para o **firewall**.
- O firewall realiza a tradução dos endereços da rede (NAT) convertendo os IPs internos em um endereço válido para acesso externo e, em seguida, libera o tráfego para a **internet**..
- Esse firewall também deve aplicar regras de segurança, restringindo o acesso externo às VLANs sensíveis (TI, Financeiro, etc.).

4 TRÁFEGO COM AS FILIAIS (VPN)

A VPN está configurada como **site-to-site**, o que significa que:

- Existe um **túnel criptografado permanente** entre a matriz e cada filial.
- O Switch Core conhece as rotas para as redes das filiais.

3. COMUNICAÇÃO COM A **FILIAL RJ**:

- A rede da filial RJ usa o bloco `10.1.0.0/24`.
- Exemplo: um dispositivo da **VLAN 30 (TI)** na matriz (`10.0.30.10`) acessa um PC da filial RJ (`10.1.0.10`).
- O pacote vai do host até o **Switch Core**, que detecta que o destino está na rede da VPN.
- Encaminha o tráfego pelo **túnel VPN** → chega à filial RJ → é entregue ao host destino.

4. COMUNICAÇÃO COM A **FILIAL MG**:

- Rede da filial MG: `10.1.10.0/24`.
- O tráfego segue a mesma lógica que a filial RJ:
- Do host da matriz → Switch Core → túnel VPN → destino na filial.

5 INTEGRAÇÃO COM SISTEMAS EM NUVEM (OFFICE 365, CRM)

A rede proposta também foi planejada para **permitir o uso seguro de serviços em nuvem**, como o Office 365 (e-mails, documentos, videoconferência) e sistemas de CRM (gestão de relacionamento com o cliente).

Esses sistemas são acessados pela internet, mas é importante que isso ocorra **de forma segura e controlada**. Por isso, o tráfego que vai para a nuvem passa antes pelo **firewall**, que aplica regras de segurança e protege os dados da empresa contra acessos não autorizados ou ameaças externas.

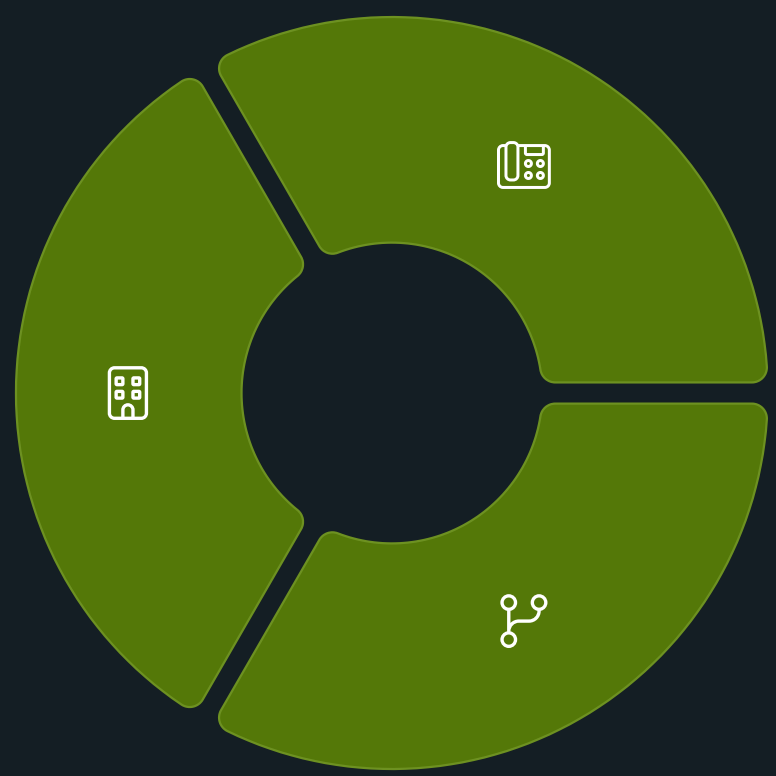
Com essa integração, os funcionários da matriz e das filiais conseguem acessar as ferramentas de produtividade e gestão a qualquer momento, mesmo estando fora da empresa, desde que autorizados. Isso **aumenta a mobilidade**, **a colaboração** entre equipes e **a eficiência no trabalho diário**.

Além disso, manter esses sistemas em nuvem reduz a dependência de servidores locais e facilita atualizações, backups e suporte técnico, o que é ideal para uma empresa em crescimento.

RESUMO SIMPLIFICADO

> O Switch Core (Núcleo de rede) conecta todas as VLANs da matriz, bem como os servidores e o firewall. Através de VPNs site-to-site, ele também conecta as filiais RJ e MG. Assim, qualquer máquina autorizada pode acessar recursos internos ou remotos conforme necessário, graças ao roteamento entre VLANs e às rotas configuradas para os túneis VPN.

O diagrama acima representa a estrutura lógica da rede proposta, mostrando as conexões entre a matriz em São Paulo e as filiais no Rio de Janeiro e Minas Gerais, incluindo as VLANs departamentais, conexões VPN e sistemas de segurança.



JUSTIFICATIVAS TÉCNICAS

A proposta da rede foi pensada para garantir segurança, organização e eficiência. As principais escolhas técnicas foram:

- **Segmentação da rede (VLANs):** Separar a rede por departamentos ajuda a evitar que um problema em uma parte (como um vírus ou ataque) se espalhe para toda a empresa. Também permite controlar melhor quem acessa o quê.
- **VPN entre unidades:** A VPN (Rede Privada Virtual) cria uma conexão segura entre a matriz e as filiais, mesmo que estejam em cidades diferentes. Assim, as informações trafegam com segurança pela internet, como se todos estivessem na mesma rede.
- **Isolamento de visitantes e dispositivos IoT:** Visitantes e dispositivos como impressoras ou câmeras devem ficar separados da rede interna da empresa, para evitar riscos de segurança. Isso é feito criando redes separadas (VLANs) que não se comunicam com a rede principal.

INTEGRAÇÃO COM SISTEMAS EM NUVEM

A estrutura de rede proposta oferece suporte seguro ao uso de serviços em nuvem como Office 365 e sistemas de CRM. Esses serviços são fundamentais para a produtividade e a gestão dos clientes da empresa.

Para garantir a segurança desses acessos, o tráfego de dados passa pelo firewall, que filtra e protege a comunicação. Isso permite que funcionários autorizados utilizem as ferramentas online com segurança, tanto dentro da empresa quanto em trabalho remoto.

A integração com a nuvem permite:

- Uso de e-mails corporativos e agendas compartilhadas;
- Armazenamento e edição colaborativa de documentos;
- Videoconferências e comunicação em tempo real;
- Acesso remoto aos sistemas, sem comprometer a segurança;
- Redução da carga sobre servidores locais.

Essa abordagem moderniza a infraestrutura da empresa, facilita a expansão e aumenta a produtividade.

As decisões técnicas adotadas como o uso de VLANs, VPNs e firewall com registro de logs oferecem uma infraestrutura eficiente e compatível com os princípios de segurança da informação. Isso resulta em uma rede segmentada, resistente a falhas e adaptável às necessidades corporativas.

DIAGNÓSTICO / PROPOSTA TÉCNICA

Com base nas necessidades apresentadas pelo cliente, foi desenvolvido um projeto de rede que prioriza segurança, organização e facilidade de expansão. A rede será dividida em áreas separadas chamadas VLANs, onde cada departamento como Administrativo, Financeiro, TI e Atendimento terá sua própria rede isolada. Essa separação facilita o controle de acessos e ajuda a evitar que problemas em um setor afetem os outros.

Além disso, haverá uma rede específica para visitantes, garantindo que eles não tenham acesso ao ambiente interno da empresa. Na matriz, localizada em São Paulo, serão instalados servidores para os sistemas internos da empresa, como ERP, arquivos e impressão. Esses servidores ficarão em uma área segura da rede e somente usuários autorizados terão acesso a eles.

As filiais do Rio de Janeiro e Minas Gerais serão conectadas à matriz por meio de VPNs site-to-site. Essas conexões funcionam como túneis protegidos na internet, garantindo uma comunicação segura entre os escritórios. Para a filial de Minas Gerais, que é menor, será configurado também um acesso remoto seguro, permitindo que colaboradores autorizados possam trabalhar de fora do escritório com segurança.

Para proteger toda essa estrutura, será utilizado um firewall, que é um sistema responsável por controlar o que pode ou não entrar e sair da rede. Ele também aplica regras de segurança e registra os acessos em arquivos de log, que servem para monitoramento e auditorias.

O projeto atende diretamente às necessidades da Werneck S/A ao propor uma rede estruturada com foco em isolamento de setores, controle de acessos e comunicação segura entre unidades. A arquitetura facilita o crescimento da empresa sem comprometer a integridade ou a gestão da infraestrutura.

RECOMENDAÇÕES E PLANO DE AÇÃO

1

SEPARAR VISITANTES DA REDE INTERNA

A criação de uma rede exclusiva para visitantes evita que dispositivos externos tenham acesso à rede corporativa, protegendo dados sensíveis e reduzindo o risco de contaminações com vírus ou acessos não autorizados.

2

CRIAR POLÍTICAS CLARAS DE ACESSO REMOTO

Definir regras para quem pode acessar a rede da empresa de fora (como em home office ou viagens) é essencial. Isso inclui configurar conexões seguras e garantir que apenas pessoas autorizadas possam acessar os sistemas internos.

3

USAR FIREWALL COM LOGGING

O firewall atua como uma barreira de segurança que controla o tráfego da rede. Ativar o registro de atividades (logs) permite que a empresa acompanhe tentativas de acesso, bloqueios e outros eventos importantes, facilitando auditorias e a identificação de problemas.

4

ACESSO SEGMENTADO POR VLANS

Separar a rede por setores (como TI, Financeiro e Atendimento) ajuda a limitar o acesso entre áreas diferentes. Isso melhora o controle, evita que falhas se espalhem pela rede inteira e aumenta a segurança geral.

5

VPN SITE-TO-SITE ENTRE MATRIZ E FILIAL

Essa tecnologia cria um "túnel" seguro entre os escritórios da empresa, permitindo que as unidades se comuniquem como se estivessem na mesma rede, mesmo estando em cidades diferentes. Isso garante proteção dos dados em trânsito e facilita o trabalho colaborativo.

PLANO DE AÇÃO (80/20)

Este plano segue a abordagem 80/20: focar nas ações que geram o maior impacto com esforço razoável. Abaixo estão listadas as principais etapas iniciais para implantação da rede:

Ação	Impacto	Dificuldade	Prioridade
Implementar VLANs por setor	Alto	Média	Alta
Configurar VPN site-to-site	Alto	Alta	Alta
Criar políticas de acesso ao Wi-Fi	Médio	Alta	Média
Isolar rede de visitantes	Alto	Média	Alta
Configurar regras no firewall	Alto	Média	Alta

A proposta apresentada atende aos principais requisitos do cliente, oferecendo uma rede corporativa moderna, segura e bem estruturada. A segmentação por áreas, o controle de acessos e a utilização de conexões seguras (VPN) garantem uma comunicação eficiente entre as unidades, proteção dos dados e flexibilidade para o crescimento da empresa.

Com essa estrutura, a Werneck S/A estará preparada para expandir suas operações de forma organizada e com uma base tecnológica sólida, garantindo desempenho, segurança e facilidade de gerenciamento.

CONCLUSÃO

A proposta apresentada atende aos principais requisitos do cliente, oferecendo uma rede corporativa moderna, segura e bem estruturada. A segmentação por áreas, o controle de acessos e a utilização de conexões seguras (VPN) garantem uma comunicação eficiente entre as unidades, proteção dos dados e flexibilidade para o crescimento da empresa.

Com essa estrutura, a Werneck S/A estará preparada para expandir suas operações de forma organizada e com uma base tecnológica sólida, garantindo desempenho, segurança e facilidade de gerenciamento.

LISTA DE EQUIPAMENTOS SUGERIDOS

MATRIZ (SÃO PAULO)

SWITCH GERENCIÁVEL -(COM SUPORTE A VLANS)

Modelos: Cisco Catalyst 2960 ou TP-Link T1600G-28TS

Quantidade: 2 unidades (core e distribuição)

FIREWALL CORPORATIVO

Modelos : Fortigate 60F , Sophos XGS 87 ou pfSense.

Quantidade: 1 unidade

ROTEADOR

Modelos :MikroTik RB4011 ou Cisco ISR 1100

Quantidade: 1 unidade

PONTO DE ACESSO WI-FI(ACCESS POINTS)

Modelos : Ubiquiti UniFi UAP-AC , Aruba Instant On ou TP-Link EAP245

Quantidade: 3 a 5 unidades (dependendo da área de cobertura)

SERVIDORES LOCAIS
FUNÇÕES: ERP, ARQUIVOS E IMPRESSÃO

Modelos : Dell PowerEdge T40 ou similar
Quantidade: 2 a 3 servidores

LISTA DE EQUIPAMENTOS SUGERIDOS

FILIAL RIO DE JANEIRO

SWITCH GERENCIÁVEL

Modelos:TP-Link T1600G-18TS

Quantidade: 1 unidades

FIREWALL BÁSICO / ROTEADOR COM VPN

Modelos : Fortigate 40F, MikroTik hEX S ou pfSense.

Quantidade: 1 unidade

ROTEADOR

Modelos :MikroTik RB4011 ou Cisco ISR 1100
Quantidade: 1 unidade

PONTO DE ACESSO WI-FI (ACCESS POINTS)

Modelos : Ubiquiti UniFi UAP-AC

Quantidade: 2 unidades

LISTA DE EQUIPAMENTOS SUGERIDOS

FILIAL MINAS GERAIS

ROTEADOR COM SUPORTE A VPN

Modelos : MikroTik hAP ac² ou TP-Link ER605
Quantidade: 1 unidade

PONTO DE ACESSO WI-FI (ACCESS POINTS)

Modelos : TP-Link EAP225

Quantidade: 1 unidades

OBSERVAÇÕES

- Todos os equipamentos devem suportar VLANs e conexões seguras (VPN).
- É recomendável padronizar marcas e modelos para facilitar o suporte técnico.
- A escolha pode variar conforme o orçamento, mas é importante garantir que todos os dispositivos suportem as funcionalidades propostas (VLAN, VPN, logs, autenticação, múltiplas SSIDs, etc.).