PROPOSTA TÉCNICA – ESTRUTURA DE REDE CORPORATIVA

FICTÍCIO S/A

Proposta Técnica – Estrutura de Rede para Cliente Fictício S/A

Autor: Arestides Durante Neto
Data: 17 de julho de 2025
Versão: 1.0

Sumário Executivo

Esta proposta técnica detalha uma arquitetura de rede corporativa segura, escalável e segmentada para a empresa Fictício S/A, que atua no setor de serviços financeiros e está em expansão. O objetivo é atender aos requisitos de segurança, produtividade e controle de acessos, com foco na matriz (São Paulo) e suas duas filiais (Rio de Janeiro e Minas Gerais). A solução proposta inclui segmentação por VLANs, comunicação segura via VPN e controle de acesso robusto, garantindo a proteção dos dados e a eficiência operacional.

Objetivo

Desenhar uma arquitetura de rede corporativa segura, escalável e segmentada para a empresa Fictício S/A, com base no briefing recebido, atendendo às necessidades de expansão, produtividade e controle de acessos.

Escopo

O escopo desta proposta abrange a estruturação da rede para a **matriz em São Paulo** (80 funcionários, com departamentos Administrativo, Financeiro, TI e Atendimento, servidores internos para ERP, arquivos e impressão, Wi-Fi para funcionários e visitantes, e integração com sistemas em nuvem), a **filial no Rio de Janeiro** (30 funcionários, estrutura similar à

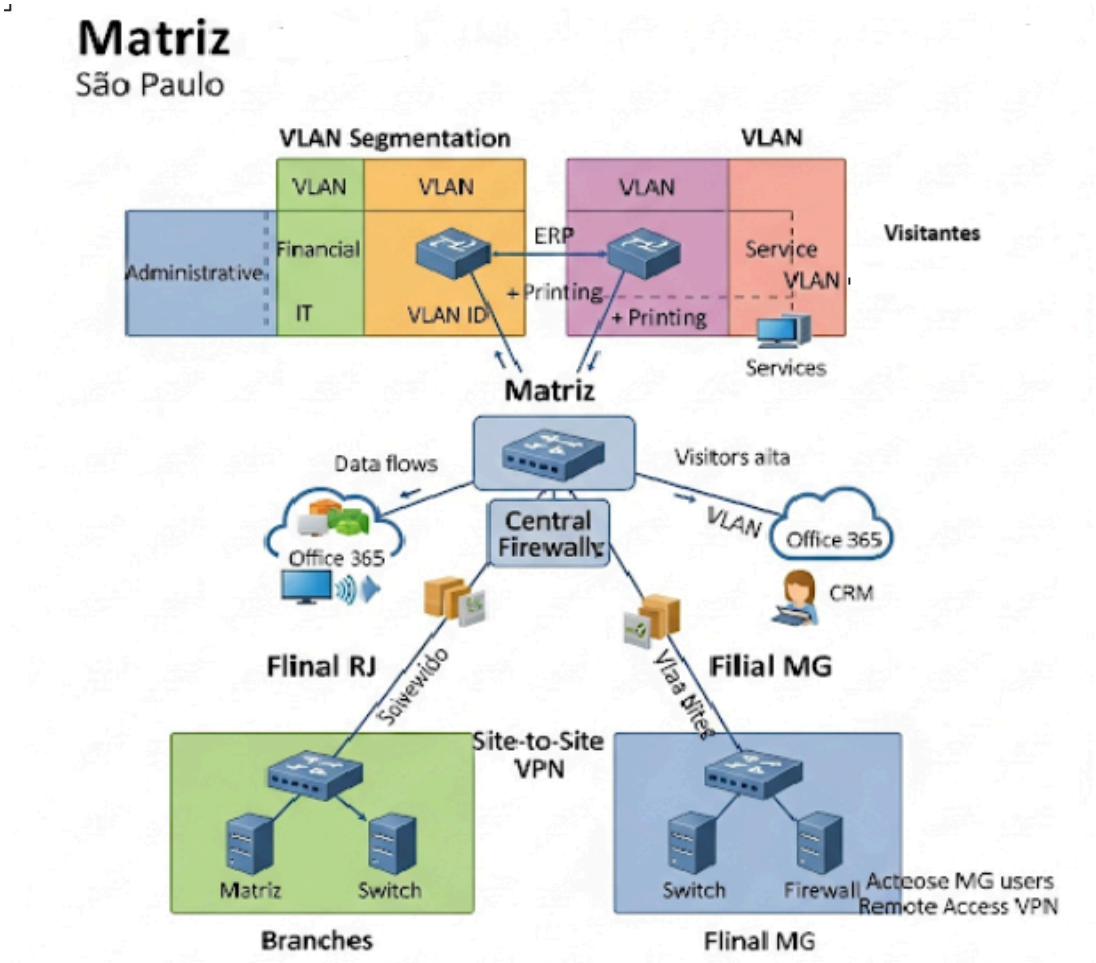
matriz, porém menor), e a **filial em Minas Gerais** (10 funcionários, necessitando de acesso remoto seguro à matriz). Inclui a conectividade entre matriz e filiais, acesso remoto para equipes, servidores internos e integração com sistemas em nuvem.

Proposta de Arquitetura

A arquitetura de rede proposta para a Fictício S/A visa a segurança, a segmentação e a otimização do tráfego. As principais características são:

- **Sub-redes por departamento (VLANs)**: Criação de VLANs específicas para os departamentos Administrativo, Financeiro, TI e Atendimento, tanto na matriz quanto na filial do RJ. Isso garantirá o isolamento do tráfego e a aplicação de políticas de segurança.
- **VLAN para visitantes separada da rede interna**: Uma rede Wi-Fi dedicada e isolada será implementada para visitantes, garantindo que não haja acesso à rede corporativa interna.
- **VPN site-to-site entre matriz e filiais**: Será configurada uma VPN site-to-site entre a matriz (São Paulo) e a filial do Rio de Janeiro para comunicação segura e transparente entre as unidades.
- **Acesso VPN para times remotos**: Para a filial de Minas Gerais e outros colaboradores que necessitem de acesso remoto, será implementada uma solução de VPN de acesso remoto seguro à matriz.
- **Firewall com controle de acesso e logs**: Um firewall será a pedra angular da segurança, controlando o tráfego de entrada e saída, inspecionando pacotes e registrando eventos para auditoria e monitoramento.
- **Servidores internos**: Os servidores de ERP, arquivos e impressão estarão localizados na matriz, acessíveis de forma segura pelos departamentos e filiais via rede interna ou VPN.
- **Integração com sistemas em nuvem**: A conectividade com Office 365 e CRM em nuvem será otimizada e protegida, garantindo acesso seguro e eficiente aos serviços.

Diagrama da Rede



Este diagrama representa visualmente a segmentação por VLANs, as conexões VPN entre matriz e filiais, a localização dos servidores internos, o firewall central e a integração com os sistemas em nuvem

---

Justificativas Técnicas

As escolhas técnicas propostas são fundamentadas nos requisitos do cliente para segurança, desempenho e controle:

- **Segmentação para limitar propagação de ataques**: A utilização de VLANs e sub-redes distintas para cada departamento e para visitantes é crucial para conter a propagação de ataques. Caso uma sub-rede seja comprometida, o impacto é minimizado, pois o ataque fica restrito àquele segmento, protegendo o restante da rede corporativa.
- **VPN para comunicação segura entre unidades e acesso remoto**: A implementação de VPNs (site-to-site para filiais e acesso remoto para colaboradores) garante que toda a comunicação entre a matriz e as filiais, bem como o acesso de equipes remotas, seja criptografada e autêntica. Isso protege dados sensíveis de serem interceptados ou adulterados durante o trânsito pela internet, um requisito essencial para uma empresa do setor financeiro.
- **Isolamento de visitantes e IoT**: Criar uma VLAN separada para a rede de visitantes e quaisquer dispositivos IoT (se aplicável no futuro) evita que esses usuários e dispositivos, que podem ter níveis de segurança desconhecidos, acessem a rede corporativa interna. Isso previne vulnerabilidades e acessos não autorizados.
- **Firewall com controle de acesso e logs**: O firewall é o ponto central de aplicação das políticas de segurança, controlando quem pode acessar o quê. Além de proteger contra ameaças externas, ele permite a criação de regras de comunicação entre as VLANs, garantindo que apenas o tráfego autorizado flua. A capacidade de registrar logs é fundamental para auditorias, detecção de incidentes e análise forense em caso de violação.
- **Otimização do desempenho e gerenciamento**: A segmentação da rede não só aumenta a segurança, mas também otimiza o desempenho ao reduzir o domínio de broadcast e facilitar o gerenciamento do tráfego.

Plano de Implementação (80/20)

O plano de implementação foca nas ações de maior impacto e prioridade para estabelecer a base da nova arquitetura de rede.

Ação	Impacto	Facilidade	Prioridade
Implementar VLANs por setor na Matriz e Filial RJ	Alto	Média	Alta
Configurar VPN site-to-site entre Matriz e Filial RJ	Alto	Alta	Alta
Criar política de acesso Wi-Fi para Funcionários e Visitantes	Médio	Alta	Média
Configurar firewall com regras de acesso e NAT	Alto	Média	Alta
Implementar VPN para acesso remoto (Filial MG e times remotos)	Alto	Média	Alta
Mapear e migrar servidores internos (ERP, arquivos) para novas VLANs	Alto	Média	Alta
Testar conectividade e segurança de todas as novas	Alto	Alta	Alta

configurações			

Conclusão

A proposta de arquitetura de rede apresentada para a Fictício S/A atende plenamente aos requisitos de segurança, escalabilidade e controle. Com a implementação de VLANs, VPNs e um firewall robusto, a empresa terá uma infraestrutura de rede resiliente, capaz de suportar seu crescimento, proteger seus dados sensíveis e garantir a produtividade de seus colaboradores, tanto na matriz quanto nas filiais e para times remotos.

> Lista de Equipamentos Sugeridos

Esta seção apresenta uma lista simplificada de categorias de equipamentos de rede sugeridos para a Fictício S/A.

---

1. Firewall de Próxima Geração (NGFW)

- **Função**: O principal ponto de segurança, controla tudo que entra e sai da rede e gerencia as conexões seguras (VPNs).
- **Exemplos de Fabricantes**: Fortinet (FortiGate), Cisco Firepower.

---

2. Switches de Rede (Camada 3 e Camada 2)

- **Função**: Conectam todos os computadores, servidores e outros dispositivos da rede. Switches de Camada 3 ajudam a dividir a rede em segmentos (VLANs) para melhor segurança e desempenho, enquanto os de Camada 2 conectam os dispositivos diretamente.
- **Exemplos de Fabricantes**: Cisco Catalyst, HP Aruba, Dell EMC Networking

---

3. Access Points (APs) Wi-Fi Empresariais

- **Função**: Fornecem o acesso Wi-Fi para funcionários e visitantes, permitindo que as redes sejam separadas e seguras.

- **Exemplos de Fabricantes**: Ubiquiti UniFi, Cisco Meraki,

---

4. Servidores Internos

- **Função**: Máquinas poderosas que armazenam os sistemas essenciais da empresa, como o ERP (sistema de gestão), arquivos e programas de impressão.
- **Exemplos de Fabricantes**: Dell PowerEdge, Lenovo ThinkSystem.

---

5. Solução de Backup e Recuperação

- **Função**: Garante que os dados da empresa estejam seguros e possam ser restaurados em caso de problemas (falha de hardware, ataques).
- **Exemplos de Soluções**: Acronis Cyber Protect, soluções de backup em nuvem (Azure Backup, AWS Backup).