Escola Vai na Web

Trilha CyberSec

Proposta de Estrutura de Rede para Fictício S/A

Autor: Emily Carla Fernandes
Data: 28 de julho de 2025
Versão: 1.0

Índice

Sumário Executivo

Esta proposta tem como finalidade apresentar a documentação técnica da implantação e as recomendações para a estrutura de rede da empresa Fictício S/A, abrangendo a matriz, localizada em São Paulo, e suas duas filiais, localizadas no Rio de Janeiro e em Minas Gerais. O trabalho visa garantir melhor gestão dos ativos, aumento da segurança e preparação para crescimento futuro da organização.

Com base no briefing do cliente, é recomendada a estruturação da arquitetura lógica por meio de VLANs, uso de firewall de próxima geração e autenticação multifator para conexões remotas. Essas ações irão elevar consideravelmente o nível de controle, desempenho e proteção dos recursos de rede.

Objetivo

O principal objetivo deste projeto é definir a infraestrutura de rede da Fictício S/A, com foco em segurança, escalabilidade, segmentação e conectividade entre as unidades e preparação para escalabilidade. A proposta contempla melhorias focando na rede lógica, envolvendo a matriz em São Paulo e suas duas filiais, por meio da implantação de VLANs, VPNs e da atualização dos equipamentos críticos. A intenção é garantir maior controle de acesso, desempenho confiável e proteção contra ameaças. Entretanto, o presente trabalho não contempla elementos de infraestrutura física da empresa como cabeamento estruturado, controle do ambiente (temperatura, umidade) etc.

Escopo

O escopo técnico abrange a infraestrutura das três unidades da empresa:

- Matriz (São Paulo): 80 funcionários distribuídos nos departamentos Administrativo, Financeiro, TI e Atendimento.
- Filial Rio de Janeiro: 30 funcionários com estrutura semelhante à da matriz, em menor porte.
- Filial Minas Gerais: 10 colaboradores com necessidade de acesso remoto seguro à matriz.

As ações previstas incluem a organização da topologia, criação de sub-redes segmentadas, atualização de switches e roteadores, configuração de VPNs (site-to-site e client-to-site), e a adoção de controles de segurança, como firewall de próxima geração (NGFW) e autenticação multifator para acessos administrativos e remotos.

Metodologia

A proposta foi desenvolvida com base no briefing enviado pela empresa e em boas práticas de arquitetura de redes. Seguindo as etapas:

1. Análise do briefing e levantamento de requisitos.
2. Modelagem da topologia no software Draw.io.
3. Definição e descrição técnica do relatório.

Proposta de Arquitetura

A arquitetura de rede proposta para a Fictício S/A foi pensada para garantir segurança, segmentação e controle sobre os dados e serviços corporativos, com flexibilidade suficiente para expansão futura. Com base na análise dos objetivos do projeto, propomos um conjunto de soluções interligadas que envolvem a separação lógica da rede por setores, controle rígido de acesso à internet e aos recursos internos, e comunicação criptografada entre unidades remotas.

O primeiro passo é segmentar logicamente a rede através da criação de VLANs específicas para cada departamento da empresa. Essa divisão permite isolar os fluxos de dados, aplicar políticas de segurança distintas e controlar o tráfego de forma granular, prevenindo o acesso não autorizado entre setores e aumentando o desempenho da rede. Os principais departamentos (Administrativo, Financeiro, TI e Atendimento) serão contemplados com sub-redes independentes, conectadas a switches gerenciáveis compatíveis com 802.1Q.

Além da rede interna, será implantada uma VLAN dedicada para visitantes, restrita apenas ao acesso à internet. Essa rede será totalmente isolada das VLANs corporativas, com controle próprio de endereçamento IP (via DHCP) e monitoramento de banda, protegendo os ativos da empresa contra acessos acidentais ou maliciosos oriundos de dispositivos não confiáveis.

Para garantir comunicação segura entre a matriz e as filiais, serão utilizadas conexões VPN criptografadas. A filial do Rio de Janeiro será integrada via VPN site-

to-site, garantindo comunicação direta e permanente com a rede da matriz. Já a filial de Minas Gerais, com estrutura mais enxuta, terá acesso via VPN client-to-site, permitindo que seus colaboradores acessem os recursos internos da matriz com segurança, mesmo em situações remotas.

Toda essa estrutura será protegida por Firewalls de Próxima Geração (NGFW), posicionados nas bordas de cada unidade. Esses dispositivos serão responsáveis por controlar e filtrar o tráfego, aplicar políticas de segurança com base em aplicativos, inspecionar pacotes (DPI), bloquear tentativas de intrusão (IPS), registrar logs de eventos e permitir a gestão centralizada da segurança.

Por fim, o tráfego com sistemas em nuvem, como Office e CRM, será roteado pela matriz, passando obrigatoriamente pelos filtros do firewall principal. Isso garantirá a aplicação uniforme de políticas de acesso e monitoramento, inclusive para conexões externas originadas nas filiais.

Dessa forma, essas são as implementações previstas:

VLAN por Departamento: Cada setor da empresa será isolado em sua própria VLAN (TI, Administrativo, Financeiro e Atendimento). Isso reduz o domínio de broadcast, melhora a performance e aplica políticas de segurança personalizadas para cada área, como restrições de acesso entre setores e limitação de tráfego de dados sensíveis.

VLAN para Visitantes: Visitantes e dispositivos externos terão acesso apenas a uma rede separada com conexão restrita à internet. O isolamento previne riscos de contaminação da rede corporativa por dispositivos desconhecidos, mantendo a integridade e a confidencialidade da rede interna.

VPN entre Unidades: A filial RJ se conecta por meio de VPN site-to-site, com um túnel criptografado direto à matriz. Já a filial MG terá VPN client-to-site, possibilitando que colaboradores se conectem de forma remota à rede da matriz com autenticação reforçada e criptografia ponta a ponta.

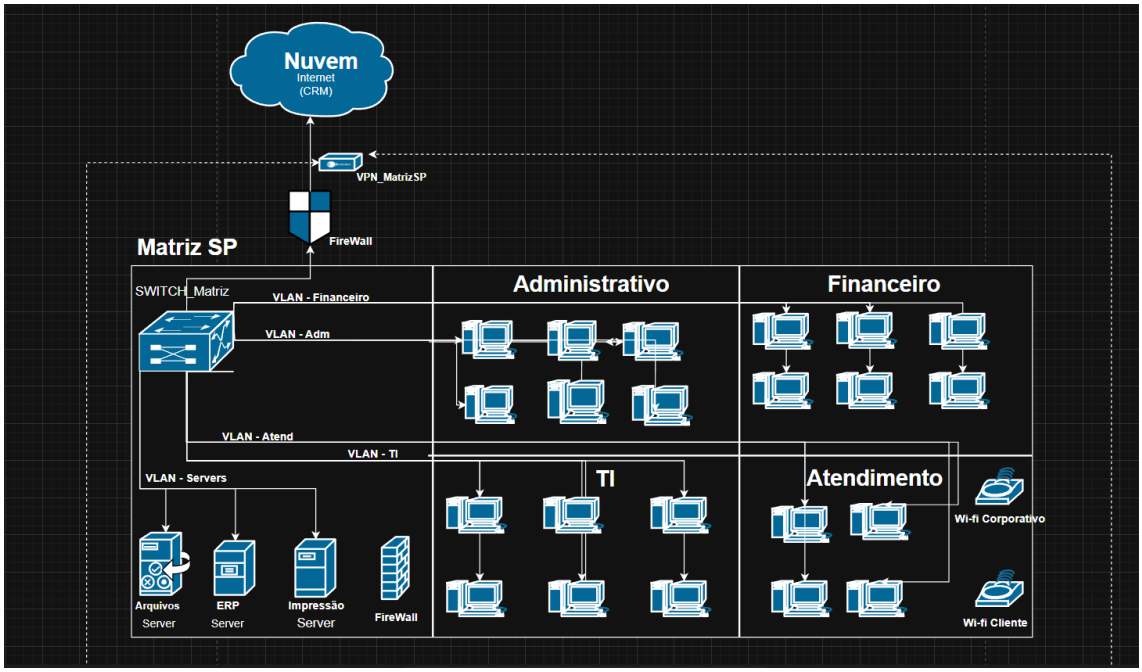
Firewall NGFW (Next Generation Firewall): Com suporte a funcionalidades como DPI (Deep Packet Inspection), IPS (Intrusion Prevention System) e controle de aplicações, os NGFWs controlarão e monitorarão o tráfego da rede. Também registrarão todos os eventos de segurança em logs para futuras auditorias.

Acesso Centralizado à Nuvem: Todo o tráfego relacionado aos serviços de nuvem corporativos será inspecionado no firewall da matriz, o que permite aplicar regras padronizadas de segurança e registrar tentativas de acesso suspeitas. Esse controle é essencial para garantir conformidade e evitar acessos não autorizados.

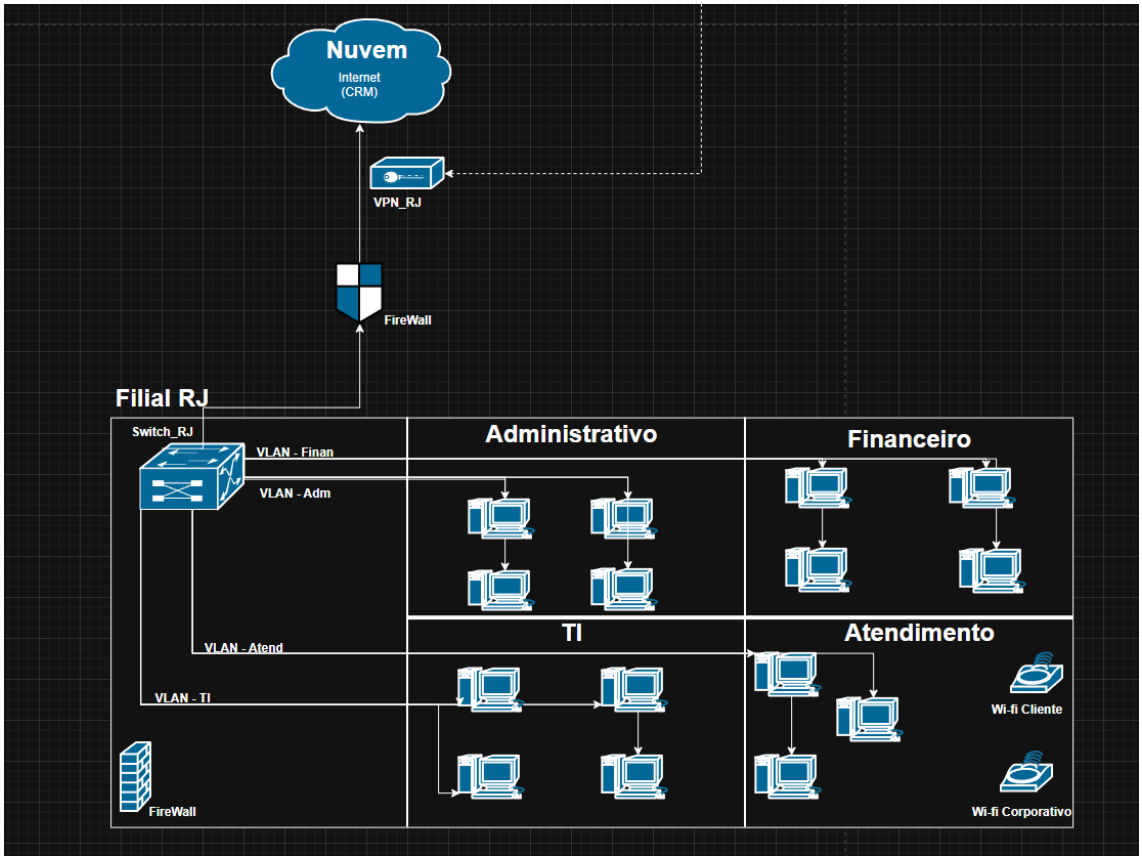
Diagramas de Rede

As imagens a seguir são diagramas que representam, de maneira ilustrativa e hipotética, a estrutura da rede de cada unidade da empresa, de maneira separada e com uma visão geral das redes conectadas entre as filiais e a matriz.

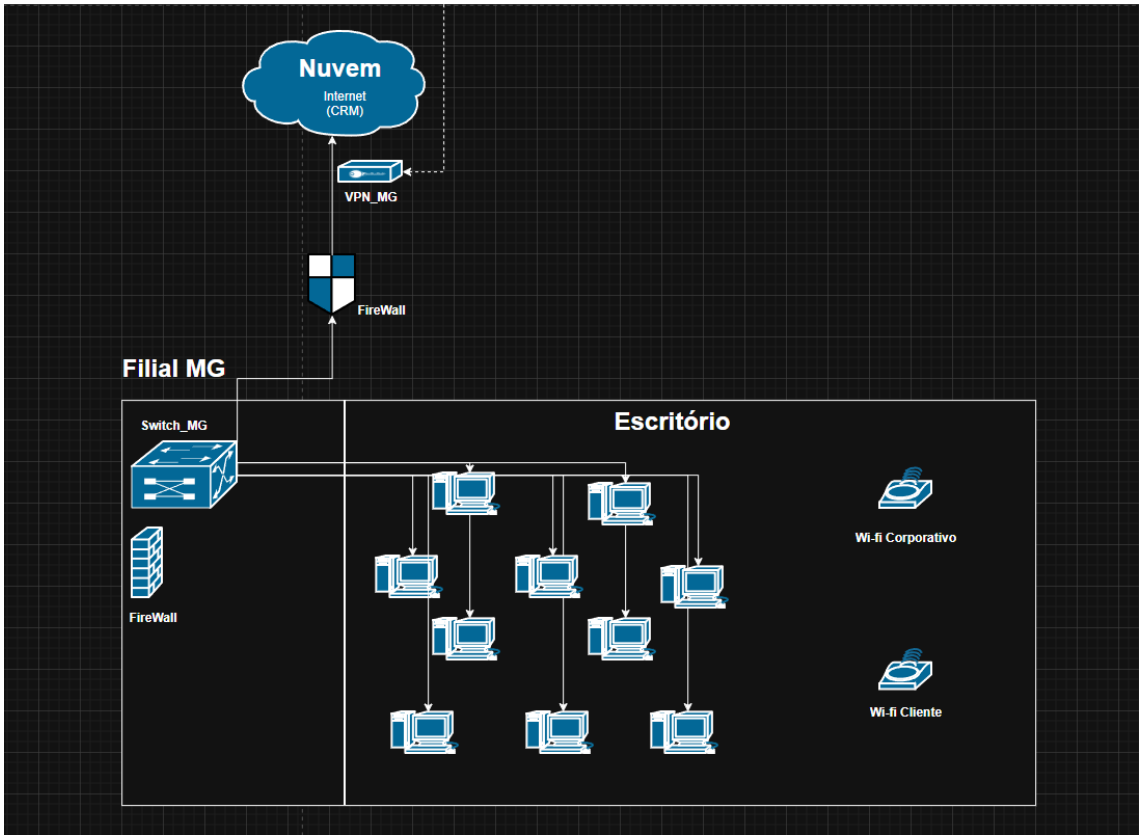
Matriz(SP)



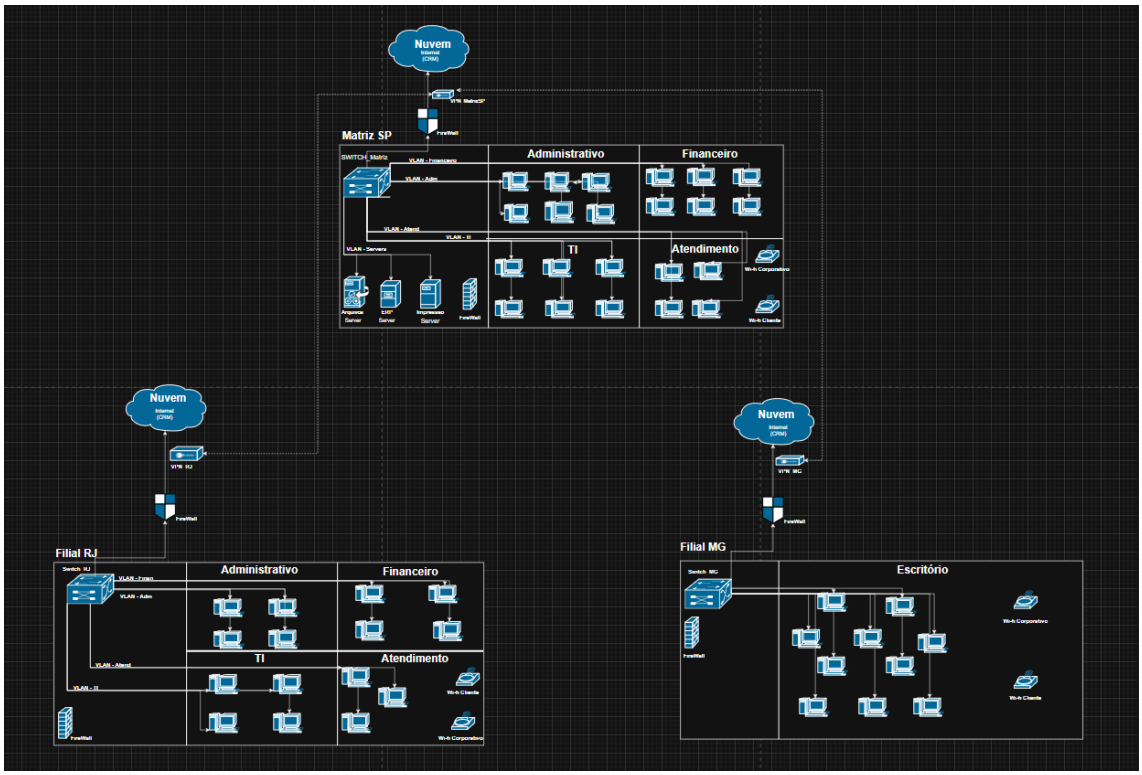
Filial RJ


Nuvem
Internet
(CRM)
VPN_RJ
FireWall
Filial RJ
Switch_RJ
VLAN - Finan
VLAN - Adm
VLAN - Atend
VLAN - TI
FireWall
Administrativo
Financeiro
TI
Atendimento
Wi-fi Cliente
Wi-fi Corporativo

Filial MG



Rede Interligada



Justificativas técnicas e Recomendações

A arquitetura proposta visa fortalecer a segurança, a eficiência e a escalabilidade da rede da Fictício S/A. A segmentação com VLANs permite isolar setores críticos, dificultando a propagação de ameaças e facilitando o controle de acessos. A utilização de VPNs criptografadas garante a confidencialidade da comunicação entre unidades e colaboradores remotos, mesmo em redes públicas.

O isolamento da rede de visitantes em uma VLAN dedicada impede que dispositivos externos acessem recursos internos, reduzindo riscos de invasão ou contaminação. Já os firewalls de próxima geração (NGFW) são responsáveis por inspecionar o tráfego, aplicar políticas de segurança, detectar ameaças em tempo real e registrar eventos relevantes para auditoria.

Com base nesse cenário, recomendamos:

- Capacitar a equipe de TI para operar VLANs, VPNs e NGFW: Garante o uso correto dos recursos implementados e minimiza riscos operacionais.

- Implantar monitoramento contínuo e análise dos logs gerados: Permite identificar falhas, acessos indevidos e anomalias em tempo real.

- Realizar auditorias de rede e testes de penetração semestrais: Valida a eficácia da segurança e antecipa correções antes de incidentes.

- Manter o firmware dos dispositivos atualizado regularmente: Corrige vulnerabilidades conhecidas e garante estabilidade dos sistemas.

- Adotar autenticação multifator (MFA) para acessos administrativos: Reforça a segurança contra acessos indevidos em áreas críticas da rede.

Plano de Implementação (80/20)

Ação	Impacto	Facilidade	Prioridade
Implantação de VLANs por setor	Alto	Média	Alta
Criação de VLAN para visitantes com DHCP isolado	Médio	Alta	Alta
Configuração de VPN site-to-site(RJ) e cliente-to-site(MG)	Alto	Alta	Alta
Instalação e configuração de firewalls NGFW	Alto	Média	Alta
Ativação de autenticação multifator(MFA) para VPNs	Alto	Média	Média
Treinamento da equipe de TI	Médio	Média	Média
Documentação de IPs, topologia e políticas	Médio	Alta	Média

Conclusão

A proposta apresentada foi cuidadosamente elaborada para atender de forma abrangente aos requisitos da Fictício S/A, com foco em segurança, escalabilidade e controle. A segmentação da rede com VLANs e a implementação de VPNs garantem um ambiente robusto contra ameaças e comunicação segura entre as unidades. A inclusão de firewalls NGFW proporciona visibilidade e proteção contínua da infraestrutura.

Esta proposta representa um passo estratégico rumo à estabilidade digital da Fictício S/A, estando pronta para ser implementada com rapidez e eficiência.