PROJETO 2

Vai na Web

2025

VAI NA WEB

Sérgio Jesus de Souza

Proposta Técnica – Estrutura de Rede para Altrix Conectividade Empresarial S/A

Versão: 1.0

São Paulo

2025

Projeto Conceitual de Arquitetura de Rede

Empresa: Altrix Conectividade Empresarial S/A

Setor: Serviços Financeiros

Localidades: Matriz (SP), Filial RJ, Filial MG

Autor: Sérgio Jesus de Souza

Áreas: Redes de Computadores / Projeto de Infraestrutura

Professor: José Menezes

Data: 28/07/2025

São Paulo

2025

2. Sumário Executivo

A Altrix Conectividade Empresarial S/A, em expansão nacional no setor de serviços financeiros, necessita de uma rede moderna, segura e segmentada entre sua matriz e duas filiais. A proposta técnica apresentada visa garantir conectividade, segurança da informação, controle de acessos e integração com sistemas em nuvem. A arquitetura baseia-se em segmentação lógica (VLANs), VPNs entre as unidades, firewall com políticas de segurança e Wi-Fi corporativo isolado do público. O plano permite escalar a rede com baixo impacto e alto controle administrativo.

3. Objetivo

Desenvolver uma arquitetura de rede segura, escalável e segmentada, conectando matriz e filiais da Altrix Conectividade Empresarial S/A, com foco em desempenho, segurança, mobilidade e integração com serviços em nuvem, contemplando:

- Segurança e controle de acessos
- Comunicação entre unidades remotas
- Produtividade e mobilidade dos usuários
- Integração com serviços em nuvem

4. Proposta de Rede

A proposta de rede para a Altrix Conectividade Empresarial S/A visa a criação de uma infraestrutura segura, escalável e com alta disponibilidade, interligando matriz e filiais. A arquitetura utiliza segmentação por VLANs, conexões VPN para comunicação entre unidades, firewall UTM para controle de tráfego e segurança, além de integração com serviços em nuvem (Office 365 e CRM). A proposta também contempla uma rede Wi-Fi dual (corporativa e visitante), além de mecanismos de autenticação multifator e controle de conteúdo, visando garantir proteção de dados e conformidade com padrões regulatórios.

5. Escopo

Composição:

- **Matriz (São Paulo)**:
    - 80 funcionários
    - Departamentos: Administração, Financeiro, TI, Atendimento
    - Servidores internos: ERP, impressão, arquivos
    - Wi-Fi corporativo e visitantes
    - Acesso à nuvem (Office 365 e CRM)

- **Filial Rio de Janeiro**:
    - 30 funcionários
    - VPN site-to-site com matriz

- **Filial Minas Gerais**:
    - 10 funcionários
    - VPN client-to-site para acesso remoto

A solução contempla segmentação de rede, comunicação segura, e gerenciamento centralizado.

6. Metodologia

O desenvolvimento da proposta para a arquitetura de rede da Altrix Conectividade Empresarial S/A seguiu uma abordagem sistemática, com base em boas práticas de mercado e normas técnicas de segurança e infraestrutura. As etapas metodológicas foram organizadas conforme descrito abaixo:

1. Levantamento de Requisitos e Análise de Briefing

Foi realizada uma avaliação detalhada das necessidades da empresa, número de usuários, estrutura organizacional e fluxos de trabalho em cada unidade (matriz e filiais). Essa análise permitiu compreender os gargalos existentes e definir os critérios técnicos para o projeto.

2. Desenho Lógico da Arquitetura de Rede

Com base nas informações coletadas, foi elaborado um diagrama lógico contendo:

Segmentação da rede por VLANs (por departamento e para visitantes)

Conexões seguras via VPN (site-to-site e client-to-site)

Interligação com serviços em nuvem

Infraestrutura de segurança (firewalls, autenticação, filtragem)

3. Justificativas Técnicas Baseadas em Normas

Todas as decisões de arquitetura foram fundamentadas em padrões reconhecidos, como:

NIST SP 800-41 e SP 800-53 para segurança de redes e controles de acesso.

CIS Controls para práticas recomendadas de proteção e monitoramento.

ISO/IEC 27001 para gestão da segurança da informação.

4. Priorização com Modelo 80/20

Foi utilizado o princípio de Pareto (80/20) para identificar as ações com

maior impacto na segurança e desempenho da rede, garantindo que as prioridades técnicas fossem tratadas com maior urgência e foco.

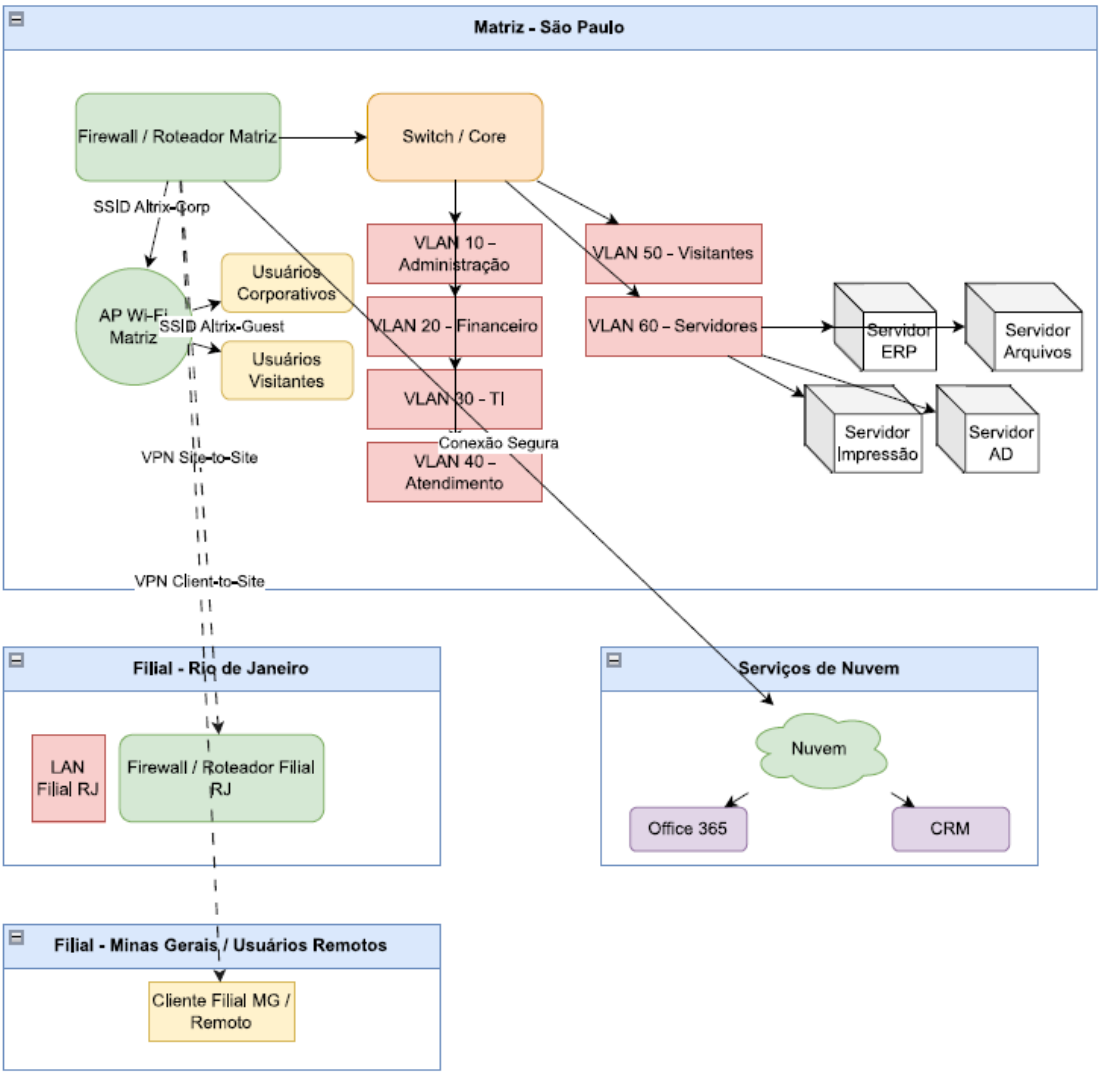
5. Documentação Final

Todo o projeto foi documentado com clareza e objetividade, incluindo: relatório técnico, plano de ação, diagrama lógico, recomendações, justificativas, e referências técnicas.

7. Diagrama da Rede

O diagrama contém:

- **Matriz com VLANs e servidores internos**
- **Firewalls e roteadores**
- **VPN site-to-site (RJ)**
- **VPN client-to-site (MG)**
- **Conexões com a nuvem**
- **Wi-Fi segmentado (SSID corporativo e visitante)**



8. Diagnóstico (ou Proposta)

Situação Atual (Identificada no briefing):

- Falta de segmentação por setor
- Acesso remoto sem controle
- Wi-Fi único para todos os dispositivos
- Ausência de registro e filtragem de tráfego

Proposta:

- VLANs por setor para segmentação de tráfego
- Firewall UTM com controle e logs
- VPN site-to-site (RJ) e client-to-site (MG)
- SSIDs distintos com controle de acesso e autenticação
- Servidores locais e conexão segura com serviços em nuvem

9. Recomendações

Área	Recomendação Técnica
Segmentação	Criar VLANs para cada departamento e rede visitante
Segurança	Instalar firewall com inspeção de pacotes, logs e autenticação
Mobilidade	VPN client-to-site com autenticação multifator
Acesso à Internet	Filtragem de conteúdo e controle de banda
Wi-Fi	Separar Wi-Fi corporativo e visitante com políticas distintas
Nuvem	Integrar com Office 365, CRM e backup em nuvem

10. Justificar Técnicas

Segmentação da Rede (VLANs):

Segmentar a rede por departamentos isola o tráfego interno, reduz a superfície de ataque e melhora o desempenho e a capacidade de diagnóstico. Essa prática também facilita a aplicação de políticas de segurança específicas para cada grupo de usuários.

Implementação de VPNs:

As conexões VPN garantem a comunicação criptografada entre as unidades e o acesso remoto seguro. A escolha por VPN site-to-site para a filial do RJ e client-to-site para MG permite flexibilidade e controle, conforme o porte de cada unidade.

Firewall com UTM:

A adoção de firewalls com funcionalidades de gerenciamento unificado de ameaças (UTM) permite controle de tráfego, geração de logs, inspeção profunda de pacotes (DPI) e autenticação de usuários. Isso eleva o nível de segurança e facilita auditorias.

Wi-Fi Corporativo e Visitante com SSIDs Isolados:

A separação física e lógica entre os acessos corporativos e visitantes evita comprometimentos de dispositivos não autorizados e mantém o desempenho da rede para aplicações críticas.

Integração com Serviços em Nuvem:

A conexão segura com plataformas como Office 365 e CRM permite mobilidade, escalabilidade e continuidade dos negócios com menor dependência de infraestrutura local.

11. Plano de Implementação

Abaixo, um plano de implementação simplificado, estruturado em fases:

Fase	Ação	Responsável	Duração Estimada
1	Levantamento técnico e inventário	Equipe de TI	3 dias
2	Criação e configuração de VLANs na matriz	Equipe de Redes	2 dias
3	Instalação e configuração de firewall UTM	Fornecedor terceirizado	2 dias
4	Configuração de VPN site-to-site (RJ)	Equipe de Redes	1 dia
5	Configuração de VPN client-to-site (MG)	Equipe de Redes	1 dia
6	Separação da rede Wi-Fi (SSID visitante e corporativo)	Suporte Técnico	1 dia
7	Integração com serviços em nuvem (CRM e Office 365)	Administrador de Sistemas	2 dias
8	Testes de segurança e conectividade	Equipe de TI	2 dias
9	Treinamento básico de usuários	RH + TI	1 dia

12. Plano de Ação (modelo 80/20)

Ação	Impacto	Facilidade	Prioridade
Implementar VLANs por setor	Alto	Média	Alta
Configurar VPN site-to-site (RJ)	Alto	Alta	Alta
Configurar VPN client-to-site (MG)	Médio	Média	Média
Instalar firewall UTM com logs	Alto	Média	Alta
Criar Wi-Fi com SSIDs segmentados	Médio	Alta	Média
Integrar Active Directory	Alto	Média	Alta

13. Recomendações de Segurança

Para garantir a integridade, disponibilidade e confidencialidade da informação, as seguintes práticas de segurança são recomendadas:

Segmentação lógica da rede (VLANs): Isola os departamentos e reduz a superfície de ataque.

Firewall UTM com inspeção profunda de pacotes (DPI): Monitora e bloqueia tráfego malicioso.

VPNs criptografadas com autenticação multifator: Protegem os acessos remotos e comunicação entre sites.

Política de senhas e autenticação forte (MFA): Aumenta a segurança de sistemas internos e nuvem.

Controle de acesso baseado em funções (RBAC): Permite acesso apenas ao que é necessário para cada colaborador.

Backup em nuvem com criptografia: Protege os dados contra perdas e ataques de ransomware.

Monitoramento contínuo de logs: Utilizando SIEM ou ferramentas integradas ao firewall para análise de eventos e auditoria.

Treinamento de usuários sobre segurança: Com foco em phishing, engenharia social e boas práticas no uso da rede.

Conclusão

O projeto proposto para a Altrix Conectividade Empresarial S/A apresenta uma solução completa, segura e escalável para conectar suas unidades distribuídas de forma eficiente. A arquitetura de rede recomendada contempla não apenas a conectividade entre as localidades, mas também oferece controles rigorosos de segurança, segmentação lógica por áreas, políticas de acesso e integração com plataformas em nuvem.

A adoção de boas práticas de governança de TI, associadas ao uso de tecnologias como VPNs, VLANs, firewalls UTM e autenticação multifator, assegura maior resiliência contra ameaças, continuidade operacional e maior controle sobre os recursos da rede. Além disso, o modelo proposto está preparado para futuras expansões, tanto em número de usuários quanto na integração com novas soluções tecnológicas.

Com base nas recomendações e plano de ação descritos, a Altrix poderá modernizar sua infraestrutura de rede, mitigar riscos operacionais e sustentar seu crescimento de forma inteligente e segura no setor financeiro.