Proposta Técnica – Estrutura de Rede para InfraSecure Brasil

Autor: Jorge Luis Dos Santos
Data: 27/07/25
Versão: 1.0
Cargo: Analista de Redes

Sumário Executivo

No dia 16/05/2024, a empresa infraSecure Brasil estava fazendo grandes mudanças na sua instrutura de rede e filias. Com o advento da I.A no mercado, e novas tecnologias que vieram com ela, a empresa precisa urgentemente acompanha suas adiversarias no mercado de finanças. A empresa tem varias filias, que ajudam no processo conjunto da matriz, mas com o aumento da demanda por causa da I.A, a equipe de TI solicitou a uma reorganização da infraestrutura da rede da empresa, para aumenta a segurança, desempenho e longevidade da rede empresarial. Atendendo todas as necessidades futuras, como integração em nuvem e controle de acesso.

Objetivo

O objetivo proposto, é projetar uma rede corporativa moderna e segura que conecte de maneira eficiente a matriz e suas filias com segmentação por departamentos, isolamentos para visitantes e acesso remoto e seguro via VPN, conforme pedido pela equipe de TI da empresa.

Escopo

Para realizar essa proposta, vamos contempla os seguintes requisitos:

- A estruturação da rede matriz (SP) e suas filias (RJ e MG);
- Cada departamento vai ser segmentado via VLAN;
- Criação de VLAN para visitantes;
- VPN entre matriz e filiais, tipo site-to-site e remoto;
- Integração com serviços em nuvem (CRM e Office);
- Acesso seguro a servidores internos (ERP, arquivos e impressão).

Proposta de Arquitetura

Com base na análise das necessidades operacionais e estratégicas da infraSecure Brasil, propõe-se uma arquitetura de rede moderna, escalável e segura. Essa estrutura contempla segmentação lógica de rede, conectividade segura entre unidades e integração com recursos corporativos locais e em nuvem.

1. Segmentação de rede

O meio proposto para a segmentação de rede, será realizado por meio da criação de VLANs, permitindo isolar logicamente os departamentos e controlar o tráfego de rede. Isso vai garantir maior segurança, organização e desempenho da infraestrutura

- **VLAN por Departamento:**

Serão criadas VLANs especificas para os setores Administrativo, Financeiro, TI e Atendimento. Essa separação lógica limita o acesso entre setores, minimiza risco de propagação de ameaças internas e facilita o monitoramento da rede.

- **VLAN para Visitantes:**

O acesso WI-FI destinado a visitantes será isolado da rede corporativa, utilizando uma VLAN própria. Essa medida impede que dispositivos não autorizados tenham acesso a dados e serviços internos, mesmo que conectados fisicamente à infraestrutura.

- **WI-FI Corporativo:**

A rede sem fio interna será protegida com autenticação robusta (por exemplo, WPA2 Enterprise) e politicas de controle de acesso com base me perfil de usuário ou dispositivos. Isso garante a segurança no trafego de dados e impede conexões indevidas.

2. Conectividade Segura

Para assegurar comunicação segura entre as unidades e acesso remoto confiável, será implementada infraestrutura VPN com diferentes abordagens:

- **VPN Site-to-Site (RJ – SP)**

A matriz (São Paulo) e a filiado do rio de janeiro serão interligados por meio de uma VPN site-to-site. Essa conexão estabelece um túnel criptografado direto entre os roteadores de ambas unidades, permitindo que as redes funcionem como uma extensão segura uma da outra

- **VPN Remota para Filial MG:**

A filial Minas Gerais, por ter um porte reduzido, contara com acesso remoto via VPN SSL ou IPsec. Usuário autorizada poderão se conectar de forma segura a rede da matriz utilizando autenticação e criptografia de dados.

- **Firewall Centralizado:**

Será implementado um firewall com políticas de acesso bem definidas, monitoramento em tempo real e geração de logs. Isso possibilita o bloqueio de tráfego indesejado, controle granular por aplicação e auditoria das conexões.

3. Servidores e Recursos Corporativos

A infraestrutura da matriz contará com servidores físicos ou virtuais dedicados ás operações internas da empresa.

- **Servidores Locais**

Servidores de ERP, arquivos e impressão estarão hospedados na matriz com controle de acesso por departamento e backup regulares. O acesso a esses servidores será feito de forma segura via autenticação e com base nas permissões de cada VLAN.

- **Integração com Sistemas em Nuvem (Office 365 E CRM):**

A rede será preparada para garantir conectividade eficiente e segura com serviços golpeados na nuvem, como o pacote Office 365 e sistema de CRM utilizado pela empresa. Politicas de QoS (QUality of Services) poderão ser aplicadas para priorizar o tráfego desses serviços.

Justificativas Técnicas

A arquitetura proposta foi elaborada com base em boas práticas de segurança da informação, desempenho de rede e governação de TI. Abaixo estão as justificativas para cada uma das decisões técnicas adotadas:

- **Segmentação por VLANs:** reduz o trafego desnecessário e melhora a segurança isolando os departamentos.
- **VPN entre unidades:** garante comunicação seguram protegendo dados em trânsito
- **Isolamento da rede visitante:** evita acesso não autorizado á rede interna.
- **Firewall com logging:** permite controle granular e auditoria de acessos.
- **Acesso remoto seguro:** facilita o trabalho de equipes moveis ou pequenas filiais sem comprometer a segurança.
- **Lista de Equipamentos:** os equipamentos para viabilizar a arquitetura proposta, vai fica a escolha da empresa, e do departamento de TI.

Plano de Implementação (80/20)

Ação	Impacto	Facilidade	Priotidade
Implementar VLANs por setor	Alto	Média	Alta
Configurar VPN site-to-site(RJ)	Alto	Alta	Alta
Implantar acesso remoto seguro (MG)	Médio	Alta	Média
Criar VLAN para visitantes	Médios	Alta	Média
Implantar firewall com controle	Alto	Média	Alta

Conclusão

A proposta apresentada está alinhada com os requisitos estratégicos e operacionais identificados no briefing da InfraSecure Brasil. A arquitetura sugerida proporciona uma rede corporativa moderna, segura, escalável e longilínea, capaz de atender as demandas atuías e futuras da organização