IMPLEMENTAÇÃO DE UMA REDE LAN UTILIZANDO AS TECNOLOGIAS TRUNK E TRUST

Estudo de Caso: PROCENTER

INTRODUÇÃO

Com o aumento das ameaças digitais e da dependência das empresas por redes internas, torna-se essencial adotar modelos de segurança modernos que garantam proteção, organização e controle rigoroso dos acessos. A maioria das organizações ainda utiliza redes tradicionais, baseadas em confiança implícita, onde qualquer dispositivo conectado pode circular livremente pela infraestrutura. Esse modelo expõe a empresa a riscos, principalmente em ambientes com falta de segmentação e ausência de políticas claras de acesso. Este trabalho propõe a implementação de uma rede baseada no modelo Zero Trust, combinada com segmentação por VLANs e trunking, oferecendo uma arquitetura mais segura, organizada e preparada para ataques internos e externos.

PROBLEMÁTICA DA PESQUISA

A empresa apresenta uma rede interna desorganizada, sem segmentação entre departamentos, sem controle de acessos e sem mecanismos avançados de autenticação. Esta falta de estrutura possibilita que qualquer falha humana, ataque interno ou invasão comprometa rapidamente toda a rede.

PROBLEMA DE PESQUISA

Como implementar um modelo de segurança Zero Trust combinado com VLANs para segmentar departamentos e controlar acessos de forma segura e escalável, considerando recursos limitados?

HIPÓTESE

- A implementação de uma rede segmentada por VLANs reduz significativamente a movimentação lateral e aumenta a segurança interna.
- O uso de autenticação 802.1X e mecanismos NAC diminui a entrada de dispositivos não autorizados na rede.
- A aplicação de QoS e melhoria de uplinks aumenta a performance das aplicações críticas utilizadas pela empresa.
- A inclusão de um sistema de monitorização e logs centralizados permite detetar
- incidentes mais rapidamente, reduzindo riscos operacionais.

OBJETIVO GERAL

Desenhar e implementar uma rede empresarial baseada no modelo Zero Trust, integrada com VLANs e trunking.

OBJETIVOS ESPECÍFICOS

- Segmentar a rede usando VLANs.
- Implementar políticas Zero Trust.
- Configurar firewall e regras entre setores.
- Usar autenticação centralizada com RADIUS e GPO.
- Criar intranet organizada e segura - Reduzir riscos de ataques.
- Demonstrar viabilidade com poucos recursos.
- Garantir acesso mínimo necessário.

JUSTIFICATIVA

Implementação de uma Rede Zero Trust com Segmentação por VLANs em Ambiente Empresarial A escolha deste tema justifica-se pela crescente necessidade das empresas modernas adotarem modelos de segurança mais robustos, especialmente em ambientes onde a infraestrutura tecnológica está em processo de reconstrução ou apresenta fragilidades significativas. O modelo de segurança tradicional baseado em perímetro já não é suficiente para proteger redes corporativas contra ameaças internas e externas, o que torna o conceito de Zero Trust fundamental.

Ao mesmo tempo, muitas empresas ainda utilizam redes planas, sem segmentação, permitindo que qualquer ataque interno, falha humana ou invasão individual comprometa toda a estrutura. A combinação de Zero Trust com VLANs e trunking resolve exatamente este problema, criando uma arquitetura em que cada departamento é isolado, monitorado e controlado de forma granular. Além disso, a empresa em questão enfrenta desafios reais: falta de internet estável, departamentos sem comunicação estruturada, risco de movimentação lateral, partilha insegura de arquivos e inexistência de mecanismos formais de autenticação e gestão de acessos. A implementação de um modelo Zero Trust, aliado a uma rede segmentada, garante que a organização possa operar de forma segura mesmo antes de adquirir equipamentos sofisticados, tornando este projeto totalmente viável para estudantes com recursos limitados.

O projeto também se justifica pela sua relevância acadêmica e prática, pois permite aplicar conceitos essenciais da área de redes — como VLAN, trunk, firewall, políticas de segurança, RADIUS, GPO e autenticação — associados a metodologias modernas de cibersegurança. A solução apresentada melhora a proteção, organiza a comunicação interna, reduz riscos operacionais e estabelece uma base sólida para futuras expansões da infraestrutura, incluindo integração com internet, cloud e VPN corporativa.

Por fim, este tema demonstra um alto grau de inovação para a realidade local, pois propõe uma arquitetura de segurança adotada por grandes empresas, adaptada de forma eficiente a um contexto com recursos limitados. Assim, a escolha deste tema não só aborda um problema real da empresa, como também contribui para a formação técnica dos estudantes, preparando-os para desafios atuais do mercado de trabalho em redes e cibersegurança

DELIMITAÇÃO DA PESQUISA

O projeto foi delimitado exclusivamente em Angola, província de Luanda, Cassequel do Lourenço – Edifício Procenter.