INTRODUÇÃO

Com o avanço da transformação digital, as empresas passaram a depender cada vez mais de serviços de rede para garantir comunicação eficiente, acesso a sistemas online e funcionamento contínuo de suas operações.

Neste contexto, para a instalação destes serviços destaca-se o Technitium DNS Server, uma solução gratuita, de código aberto e multiplataforma, que oferece interface gráfica acessível, suporte a lista de bloqueio, e gerenciamento completo de zonas e registros. Ele tornou-se a escolha ideal a ser aplicada na Supera Comercial, uma microempresa localizada em Camacupa, que possui uma infraestrutura de rede extremamente limitada.

.1 Situação Problemática

1.4 Objectivo Geral

1.5 Objectivos Específicos

CAPÍTULO I: FUNDAMENTAÇÃO TEÓRICA.
1.1 O Sistema de Nomes de Domínio
O DNS é um sistema hierárquico e distribuído de gerenciamento de nomes que traduz domínios legíveis por humanos em endereços IP numéricos, permitindo a comunicação eficiente entre dispositivos na Internet MOCKAPETRIS (1987).

1.1.2 Arquitetura do DNS e a Hierarquia de Servidores Autoritativos DNS

■ Servidor DNS Recursivo
■ Servidor DNS Autoritativo

Hierarquia de Servidores Autoritativos DNS
1. Servidor Autoritativo de nomes raiz
2. Domínio de Primeiro Nível (TLD - Top-Level Domain)
. Domínio de Segundo Nível

Classificação dos TLDs

.2 Importância do DNS em Pequenas Empresas
1.2.1 Benefícios da Implementação do DNS Local

■ Melhoria na Velocidade de Acesso: Um servidor DNS local armazena em cache as resoluções de nomes mais frequentemente acessadas, reduzindo significativamente o tempo de resposta ao carregar sites e serviços. Essa otimização minimiza a latência e melhora a produtividade dos colaboradores.
■ Maior Controle sobre o Tráfego de Rede: Ao utilizar um servidor DNS local, a empresa pode gerenciar e filtrar acessos, aplicando políticas de uso da internet para aumentar a eficiência operacional. Isso permite restringir sites não autorizados, otimizar a largura de banda e reduzir riscos de acesso a conteúdos potencialmente perigosos.
■ Monitoramento e Análise de Dados: As requisições DNS fornecem informações

valiosas sobre os padrões de tráfego na rede da empresa. Com a implementação de um servidor DNS local, é possível coletar e analisar dados detalhados, identificando tendências de uso, problemas de conectividade e até mesmo ameaças potenciais.

Impacto na Segurança e Desempenho da Rede

Proteção contra Ameaças Cibernéticas: Uma estratégia eficaz de segurança envolve a filtragem de DNS para impedir o acesso a domínios maliciosos. Esse mecanismo ajuda a bloquear ataques de phishing, malware e ransomware antes mesmo que os usuários possam acessá-los, reduzindo significativamente os riscos de comprometimento da rede.
Resiliência contra Ataques de DNS: Ataques como envenenamento de cache (DNS cache poisoning) e negação de serviço distribuída (DDoS) podem comprometer a estabilidade de uma rede empresarial. A implementação de servidores DNS locais robustos, aliados a tecnologias como DNSSEC, garante a integridade das requisições e dificulta tentativas de manipulação maliciosa.
Otimização do Desempenho da Rede: O tempo de resposta das conexões pode ser reduzido consideravelmente ao minimizar consultas externas desnecessárias. Com um servidor DNS interno, as resoluções de nomes ocorrem de forma mais rápida e eficiente, melhorando a experiência dos usuários e garantindo u

Introdução ao Technitium DNS Serve

1.3.1 Características e Funcionalidades
O Technitium DNS Server oferece um conjunto robusto de funcionalidades que o tornam uma das soluções mais versáteis para gerenciamento de DNS. Entre suas principais características, destacam-se:
Código Aberto e Gratuito: Disponível sob licença open-source, permitindo total transparência, auditoria de código e personalização conforme as necessidades do usuário.

Interface Web Intuitiva: Diferente de soluções mais complexas, como BIND, o Technitium oferece um painel web amigável para configuração e monitoramento em tempo real, simplificando o gerenciamento de servidores DNS.
Filtragem Avançada de Domínios: Possui suporte nativo para bloqueio de domínios específicos, impedindo rastreamento online, anúncios invasivos e domínios maliciosos associados a malware e phishing.
Suporte a DNS-over-HTTPS (DoH) e DNS-over-TLS (DoT): Garante maior privacidade e segurança, criptografando as consultas DNS para evitar espionagem e manipulação de dados durante a transmissão.
Cache DNS Avançado: Melhora a performance da rede ao armazenar respostas DNS localmente, reduzindo a latência e otimizando a resolução de nomes de domínio.
Integração com Listas de Bloqueio Personalizadas: Permite a inclusão de listas personalizadas para bloquear domínios indesejados, oferecendo maior flexibilidade para administradores de rede que desejam implement

1.3.2 Comparação com Outras Soluções de DNS

■ Pi-hole: Especialmente projetado para bloqueio de anúncios em toda a rede. Embora também suporte DoH/DoT, sua função principal não é atuar como um servidor DNS

primário completo.
■ BIND (Berkeley Internet Name Domain): Um dos servidores DNS mais utilizados em grandes corporações, com alto nível de personalização, mas complexidade elevada na configuração.
■ Unbound: Um resolvedor de DNS rápido e eficiente, ideal para redes privadas e locais. Suporta DoH/DoT, mas não possui interface web nativa e exige configurações manuais avançadas.
■ Technitium DNS Server: Destaca-se por unir simplicidade, desempenho e segurança, sendo uma alternativa viável para usuários que desejam controle total sobre o DNS sem a complexidade do BIND (TECHNITIUM, 2024).
O Technitium DNS Server é uma excelente alternativa para empresas que desejam gerenciar eficientemente o DNS, proteger a privacidade dos usuários e aumentar o desempenho da rede. Sua interface amigável e recursos avançados, como suporte a DoH/DoT e filtragem de domínios, tornam-no uma solução ideal para redes domésticas, pequenas empresas e ambientes corporativos

CAPÍTULO II: FUNDAMENTAÇÃO METOGOLOGICA.
2.1 Desenho Metodológico
3 Dados Estatísticos

CAPÍTULO III: PROPOSTA DE IMPLEMENTAÇÃO E ESTUDO DE CASO
Cenário Prático para a Configuração do Servidor DNS Local
A seguir, será descrito o ambiente de rede, os requisitos mínimos e os procedimentos para instalação e configuração do servidor DNS local na empresa Supera Comercial.
3.1.1. Estrutura Atual da Rede
Atualmente, a rede da empresa é extremamente simples e composta por:
■ 1 computador de mesa;
■ Roteador doméstico fornecido pela operadora de internet;
■ Servidor DNS utilizado: público (automático da operadora);
■ Sem configurações de IP estático ou qualquer tipo de servidor interno;
■ Sem firewall ou políticas de segurança definidas.
Essa estrutura mostra uma forte dependência da operadora e ausência de recursos de controle, o que implica diretamente na lentidão percebida na navegação e resolução de nomes.
“A ausência de um servidor DNS local pode comprometer a eficiência da rede, mesmo em ambientes de pequeno porte.” KUROSE; ROSS (2013
3.2 Passo a Passo da Instalação do Technitium DNS Server

conclusoes e recomendaçoes