Proxy Server Security Comparison: Current vs New Implementation

Quick Comparison Table

Security Aspect	Current Server	New Plan
Password Storage	Plain text (exposed)	Hashed (nonce)
Authentication Method	Basic (cleartext)	Digest + IP-based
User Management	Shared credentials	Individual accounts
Site Blocking	None	Enabled
Office Access	Username/Password	IP-based (automatic)
Remote Access	Username/Password	Digest authentication
User Tracking	No trackability	Full traceability

Current System Critical Issues

Security Vulnerabilities

- **Exposed Credentials**: Username and password visible on internet
- **Cleartext Transmission**: Basic authentication sends credentials unencrypted
- **Shared Accounts**: Multiple users using same login credentials
- **No Access Control**: Unrestricted internet access without site blocking
- **Zero Accountability**: Cannot track individual user activities

New Plan Security Enhancements

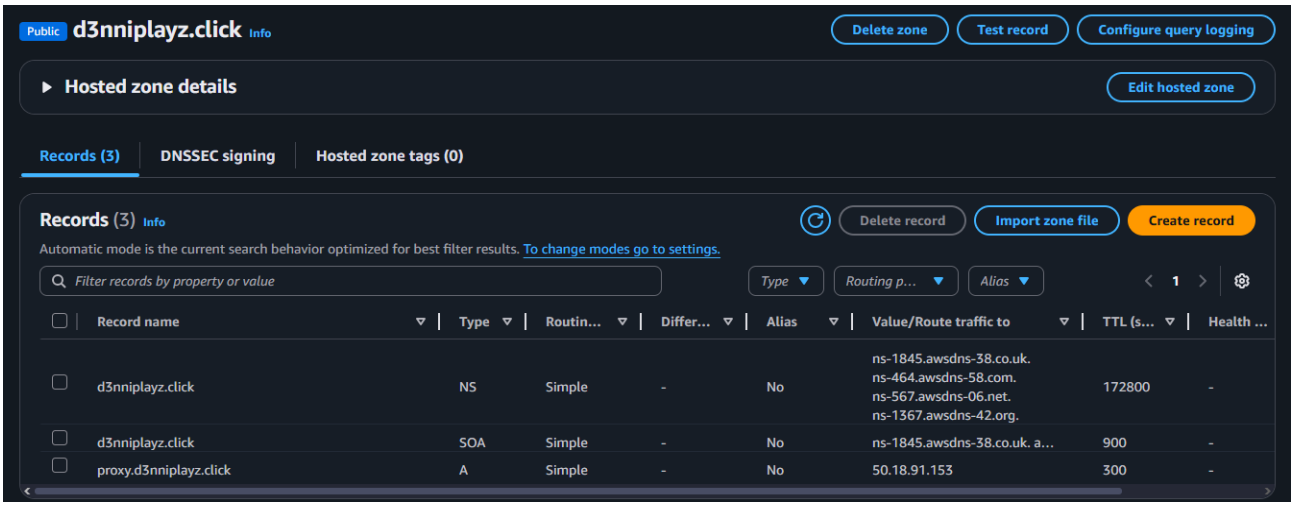
Authentication Improvements

- **Digest Authentication**: Encrypted credential transmission for remote users
- **IP-Based Office Access**: Seamless authentication for office users
- **Individual User Accounts**: Unique credentials for each user

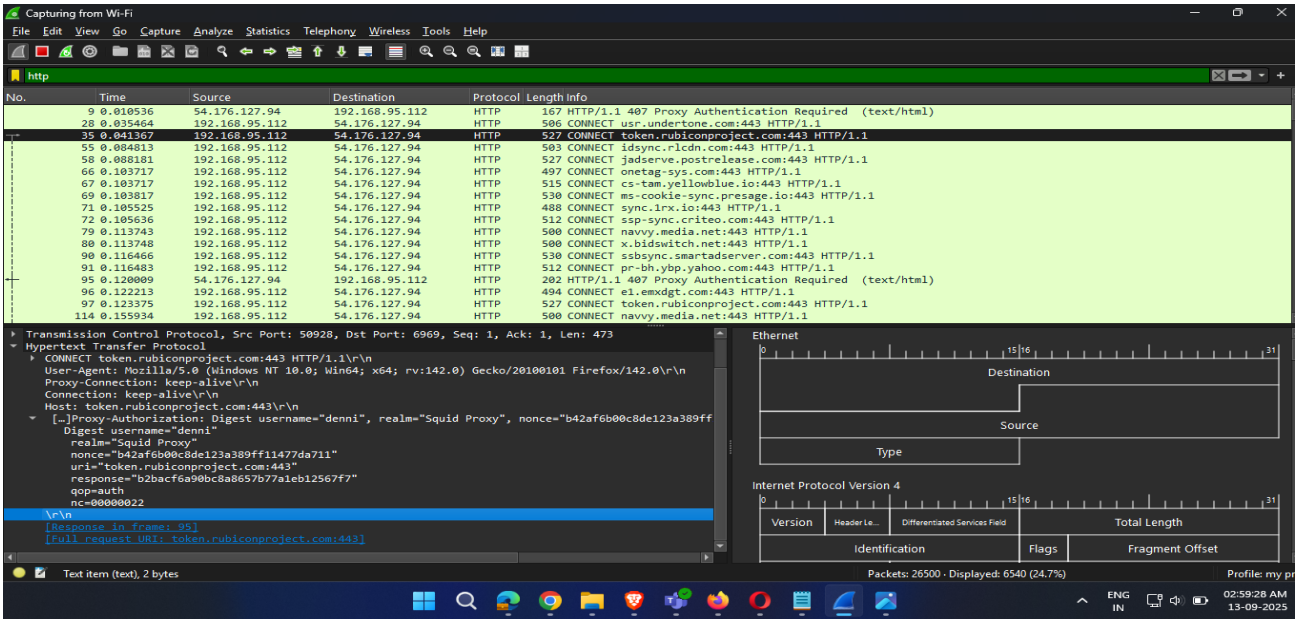
Access Control Features

- **Site Blocking**: Content filtering to block malicious and inappropriate websites
- **Comprehensive Logging**: Full audit trail of all user activities
- **User Accountability**: Complete traceability of actions to individuals
- **TLS/SSl Encryption**: - Full Encryption: TLS ensures that both user traffic, TLS adds confidentiality, integrity,

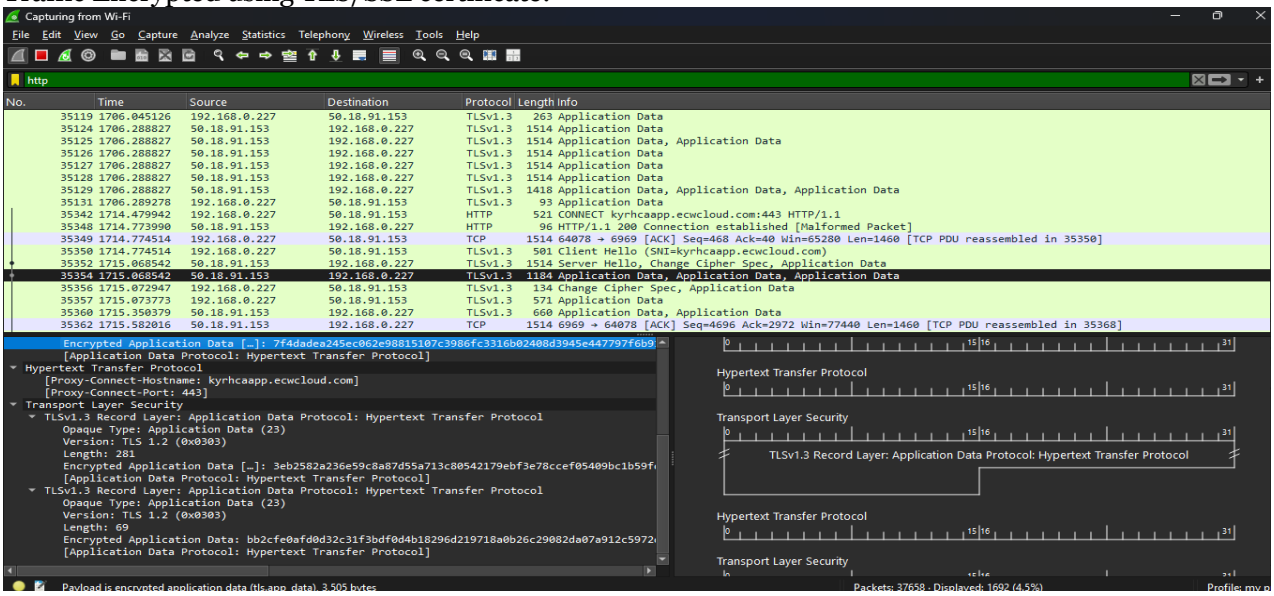
DNS domain created in AWS route 53:



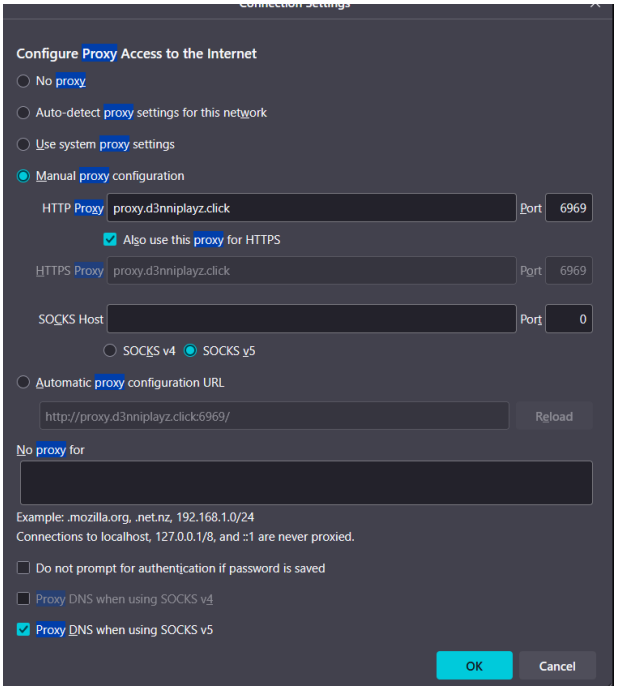
Digest Auth:



Traffic Encrypted using TLS/SSL certificate:



Connect using the dns



Add the squid config file and other dependent file in github.