

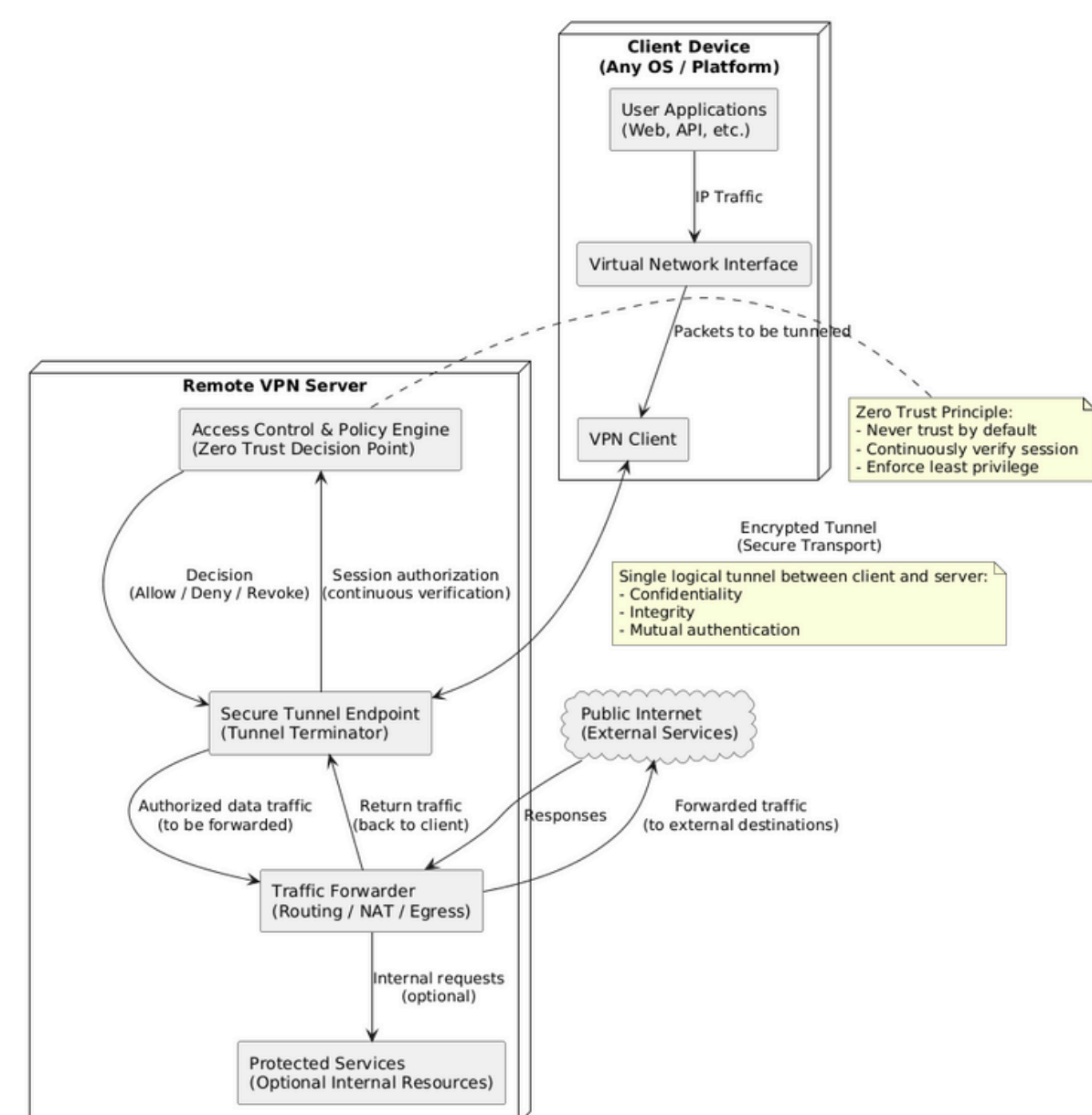
Zero Trust QUIC-based VPN

Nicat Çalışkan Onur Demir
Department of Computer Engineering, Yeditepe University



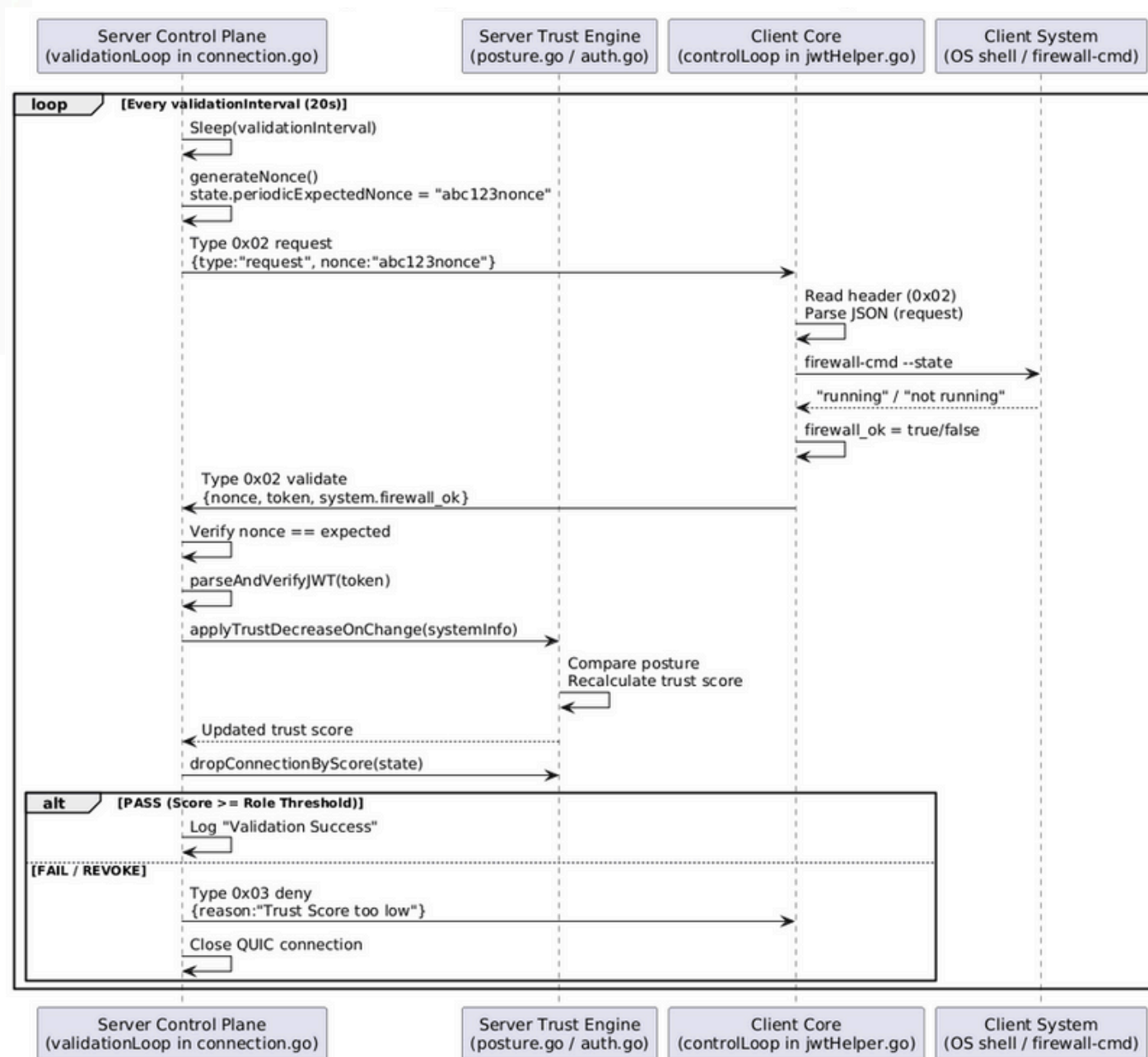
Abstract

Virtual Private Networks (VPNs) are very important for secure remote access, but traditional solutions often trust the user completely after just one authentication. This "connect once, access all" way creates big security risks if a hacker hijacks an active session or steals valid credentials. This project presents the design and implementation of a new VPN system that uses the QUIC transport protocol with a Zero Trust security model. We chose QUIC because it solves the delay problems of TCP while adding the reliability and built-in encryption that UDP lacks. The proposed system changes security from checking only at the beginning to continuous checking, using dynamic trust scores and identity rules to control access. The aim of this project is implementing a multi-client VPN architecture that combines the high speed of the QUIC protocol with the continuous security of the Zero Trust model.



Control Plane – QUIC Streams

The control plane is responsible for authentication, authorization, and continuous trust verification in the VPN system. It is implemented using QUIC streams, which provide reliable, ordered, and encrypted communication. The control plane handles device authentication with mutual TLS, user login, JWT token issuance, periodic nonce-based validation, and trust score evaluation. By using QUIC streams, the system ensures that all security-critical messages are delivered correctly and in order, enabling immediate session revocation when Zero Trust requirements are no longer satisfied.



Zero Trust Architecture

The proposed VPN follows a Zero Trust model where client access is never trusted permanently. After initial authentication, the server continuously verifies the client during the session using short-lived JWTs and nonce-based validation. At each periodic check, the client proves its identity by presenting a valid token together with current system posture information, and the server re-evaluates the trust score.

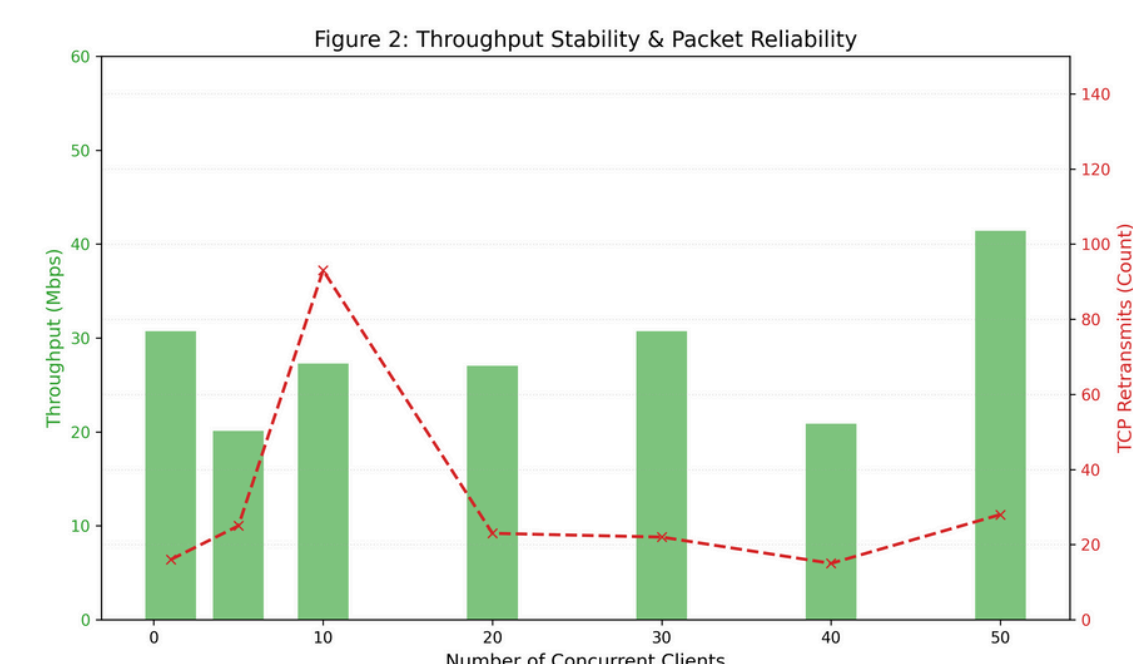
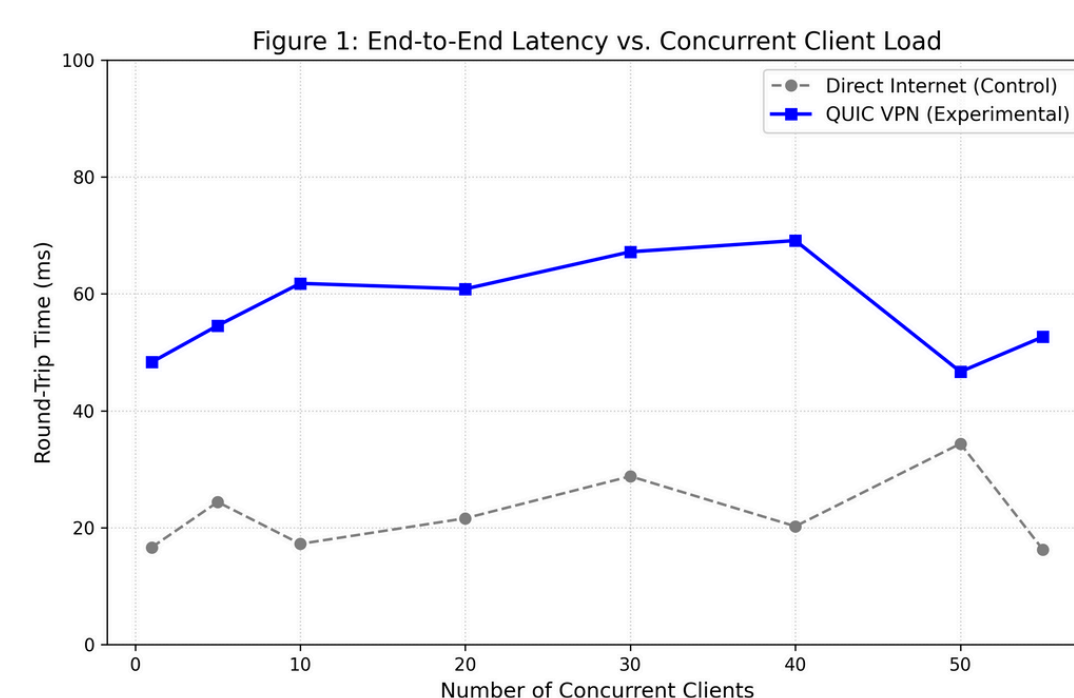
In addition to periodic checks, access to protected internal services triggers an immediate authorization request. The server validates the JWT, role, scope, and trust score before allowing the request. If any verification fails, the session is revoked instantly, preventing further traffic forwarding.

Contact

onur.demir@yeditepe.edu.tr
nicat.caliskan@std.yeditepe.edu.tr

Results of the Model

The system was tested under increasing load with up to 55 concurrent VPN clients. The results show that latency and throughput remain stable as the number of active sessions increases



Future work

As a future work, improving device posture collection, extending Zero Trust control to multiple internal services, enabling dynamic service registration, and strengthening security with advanced identity and cryptographic mechanisms could make the system very powerful.

References

- Iyengar, J., & Thomson, M. (2021). QUIC: A UDP-Based Multiplexed and Secure Transport (RFC 9000). Internet Engineering Task Force (IETF).
- Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication 800-207). National Institute of Standards and Technology (NIST).
- Behl, A., & Behl, K. (2017). Virtual Private Networks: A Survey. International Journal of Computer Applications, 165(2), 1–6.