Pakistan Journal of Life and Social Sciences
www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2026-24.1.0074

RESEARCH ARTICLE

Secure Overlay Network with Automated Access Management for Corporate Environments under Unstable Connectivity

A.Y. Poluyan[1*], K.S. Korovina[2]

[1]Assistant Professor - Don State Technical University, Rostov-on-Don, Russia
[2]Senior Lecturer - Don State Technical University, Rostov-on-Don, Russia

ARTICLE INFO

Received: MAY 15, 2026

Accepted: JUNE 10, 2026

Keywords

Secure remote access
Overlay network
Zero trust
Automated access management
Unstable networks
Telegram bot
Self hosted infrastructure
Information security

***Corresponding Author:**
apoluyan@donstu.ru

ABSTRACT

The digital transformation of enterprises and the widespread adoption of remote work models impose stricter requirements for secure remote access to corporate information resources. Classical VPN solutions (IPsec, OpenVPN, WireGuard) exhibit poor stability and high administrative complexity under high latency, packet loss and NAT/CG NAT conditions. Application layer proxy protocols (e.g., Hysteria 2) offer better resilience but cannot create a full fledged corporate network with transparent routing and centralized access control. This paper proposes an information system based on a self hosted overlay network that combines cryptographic link protection with automated provisioning of connection configurations. The system uses a lightweight controller, a web administration panel and a Telegram bot as the user interface. Zero trust principles are implemented, human factor risks are minimised, and stable operation under unstable network conditions is achieved. Experimental validation confirmed connection stability, centralized access control and a significant reduction in administrative overhead.

INTRODUCTION

The digitalisation of the economy and the widespread integration of information technologies into organisational activities make secure remote access to corporate information resources a highly relevant problem. Modern enterprises increasingly adopt distributed work arrangements, remote workplaces, virtual servers and cloud infrastructures, which require employees to have continuous and secure access to internal corporate services via public communication networks.

At the same time, the expansion of remote work substantially increases information security threats. Transmitting official information and personal data over open channels without specialised protection creates conditions for man-in-the-middle (MITM) attacks, traffic interception and tampering, credential compromise and unauthorised access to corporate resources. A significant fraction of security incidents is directly caused by errors in remote access organisation and insufficient automation of user rights management (National Institute of Standards and Technology, 2025).

Many regions experience unstable communication channels, high latency, widespread use of NAT and CG-NAT, as well as traffic filtering. In such environments, classical network-layer VPNs exhibit low resilience and high administrative complexity. Application-layer proxy protocols, by contrast, show high survivability but cannot form a full corporate network with transparent routing and centralised access control (Choi, 2025).

Commercial Zero Trust Network Access (ZTNA) solutions are often presented as a secure alternative to classical VPNs. However, in 2025 several serious vulnerabilities were discovered in some of these products, including authentication bypass, hard-coded credentials and SAML assertion validation errors (CVE-2024-7401, CVE-2025-3831) (National Security Agency, Cybersecurity Directorate, 2026; IonQ, Applied Research Laboratory for Intelligence and Security,

2026; ISC2 Insights, 2026). This suggests that modern ZTNA products may contain major vulnerability classes, even when deployed with private cloud-based coordination servers.

The human factor is another critical issue in remote access systems. Manual distribution of connection configurations, lack of centralised access lifecycle control, untimely revocation of rights and configuration errors significantly increase the risk of corporate network compromise.

Therefore, the aim of this work is to develop an information system that provides secure remote access to a corporate network with automated issuance of user connection configurations and centralised access management, adapted to modern network environments and independent of external proprietary services.

Threat Model and System Requirements

Based on an analysis of typical remote access scenarios, regulatory documents (NIST SP 800-207) and recent vulnerability reports, the following threat model is formulated:

- Network threats: man-in-the-middle (MITM) attacks, traffic interception and tampering, replay attacks.
- Endpoint threats: compromise of a client node to gain unauthorised access to the corporate network.
- Operational threats: untimely revocation of access rights, configuration errors, social engineering targeting administrators.
- Availability threats**:** traffic filtering, DDoS attacks, loss of connectivity with the overlay controller.
- Supply chain and data sovereignty threats: use of external coordination servers ("phone home") that may be compromised, unavailable or perform unauthorised metadata logging.

Based on the analysis of existing technologies (classical VPNs, proxy protocols, overlay networks, certified national cryptographic solutions) and the identified vulnerabilities of commercial ZTNA solutions (National Security Agency, Cybersecurity Directorate, 2026; Cybersecurity and Infrastructure Security Agency, 2023), the following mandatory requirements for the developed system are formulated:

1. Network-layer virtualization – the system must create a virtual corporate network over the Internet with internal IP addressing.
2. Cryptographic protection – confidentiality, integrity and mutual authentication using strong cryptographic algorithms.
3. Resilience to unstable networks – correct operation under NAT, CG-NAT, high latency and packet loss.
4. Centralised access management – user and device authentication, authorisation, and enforcement of least-privilege policies.
5. Automation – self-service configuration retrieval and immediate access revocation.
6. Self-hosted deployment – full control over the controller, logs and user lifecycle without dependence on external cloud services.

Review and Classification of Existing Solutions

Secure remote access technologies can be classified by the OSI model layer at which protection mechanisms are implemented, as well as by architectural principles of network interaction. This work distinguishes four broad technology classes.

The first group comprises classical network- and link-layer VPNs (L2–L3), including IPsec, OpenVPN, L2TP/IPsec and more recent implementations based on WireGuard. Their main advantage is transparency for application services. Disadvantages include scalability complexity, sensitivity to connection quality and high administrative requirements (Choi, 2025).

The second group consists of application-layer proxy protocols (L5–L7), including QUIC-based solutions such as Hysteria 2. They offer high resilience to packet loss, traffic masking and low sensitivity to channel quality. However, they are not designed for building full corporate networks, and their VPN-emulation (TUN) modes remain experimental.

The third, most promising group comprises overlay networks – virtual distributed networks built on top of the Internet. They provide direct encrypted end-to-end communication between nodes, automatically solving NAT traversal, dynamic routing and connection establishment over unstable channels. Implementations include both commercial proprietary solutions (Tailscale, ZeroTier) that rely on external coordination servers, and self-hosted alternatives (Headscale, Netmaker) (Gentyala, 2026). The overlay approach enables a zero-trust model where every node is independently authenticated and authorised (ATIS, 2026).

The fourth group includes certified national cryptographic solutions that comply with the requirements of the Russian FSTEC and FSB. Their advantage is formal compliance with regulatory requirements; disadvantages include high cost, closed architecture, limited flexibility and difficult integration with modern DevOps and cloud-oriented infrastructures.

Consider some vulnerabilities of commercial ZTNA products (Check Point, Netskope, Zscaler):

- Weaknesses in Identity Provider (IdP) enrollment procedures, which create conditions for authentication bypass;
- Hard-coded credentials that provide unauthorised access to logs of other customers;
- Flaws in SAML assertion validation leading to authentication errors.

Thus, using opaque proprietary cloud coordination servers introduces vulnerability risks, making the choice of a self-hosted overlay architecture well-justified.

Consequently, none of the reviewed classes is universal. From a scientific and practical standpoint, the preferred choice is an overlay network with self-hosted deployment and access management automation, as it enables full infrastructure control when operating over networks with unstable data transmission parameters.

Architecture of the Proposed System

The architectural foundation is an overlay network that provides logical connectivity between nodes of the corporate infrastructure independently of their physical location and the characteristics of the public network. Each node receives an internal network address and communicates with other nodes through encrypted channels, ensuring isolation of corporate resources and compliance with zero-trust principles.

The developed information system has a distributed architecture and includes the following main components:

- Overlay network controller – the central management element responsible for node registration, internal IP address distribution, key management and access policy enforcement.
- Web administration panel (TGadmin) – an interface for system administrators, providing user overview, access request handling, active session monitoring and forced access revocation.
- Telegram bot – a user interface for remote employees, enabling access requests and reception of automatically generated connection configurations.
- Internal corporate services subsystem – an internal DNS server, an HTTP service for connection testing, and administrative services accessible only within the overlay network.
- Client nodes – remote user devices with an installed overlay client.

All components are deployed using containerisation (Docker) and orchestration tools, which ensures isolation, reproducibility of the installation and simplified maintenance.

Automated Access Management

A key feature of the developed system is the automated access management subsystem, which automates the processes of provisioning, control and revocation of access, thereby eliminating manual client configuration and minimising human-factor risks.

The automated configuration provisioning algorithm comprises the following steps:

1. The user initiates an access request through the Telegram bot.

2. The request is registered and displayed in the web administration panel (TGadmin) with the user's Telegram ID and timestamp.

3. The administrator decides to grant or deny access.

4. If the decision is positive, the system automatically:

- generates a unique node configuration (internal IP address, cryptographic keys, access rules);
- transfers the configuration to the user over a secure channel via the Telegram bot;
- activates the node in the overlay network.

5. The user imports the configuration into the overlay client and establishes the connection.

6. Access is revoked either automatically upon expiration or by administrator initiative, immediately removing the user's node from the virtual corporate network.

All user and administrator actions are logged, enabling auditing, incident analysis and investigation of security breaches.

The use of a Telegram bot is motivated by its wide adoption, cross-platform nature and the possibility of prompt interaction without developing specialised client software. However, this introduces a dependency on a third-party messaging infrastructure – a limitation discussed in Section 7 and addressed in Section 8.

The web administration panel ensures transparency of access management processes and allows rapid incident response.

Experimental Validation

The developed system was deployed on a virtual private server (VPS) with a self-hosted overlay network controller and web administration panel. Testing was conducted under emulated unstable network conditions (100-300 ms latency, 5-10 % packet loss, NAT444). The experiment involved ten remote users accessing internal corporate services (DNS, HTTP) over a period of 30 days.

MAIN RESULTS

- Connection stability: overlay connections remained operational under all emulated degradation conditions, whereas IPsec and OpenVPN tunnels failed or required manual reconnection in more than 30 % of cases.
- Automation efficiency: the average time from user request to active connection dropped from 45 minutes (manual configuration distribution) to 2.5 minutes (fully automated process).
- Access revocation: administrative revocation immediately removed the node from the network; subsequent unauthorised access was impossible.
- Reduction in administrative load: the volume of routine configuration tasks decreased by 95 %.

During the experimental period, no information security incidents (unauthorised access, credential leakage) were recorded. Log integrity was preserved, and all user/administrator actions were fully auditable.

COMPARATIVE ANALYSIS AND DISCUSSION

A comparison of the developed system with existing approaches is presented in Table 1.

Table 1: Comparative characterisation of remote access solutions

Criterion	Classical VPN (IPsec/OpenVPN)	Proxy protocol (Hysteria 2)	Commercial ZTNA (Zscaler, Netskope) (National Security Agency, Cybersecurity Directorate, 2026)	Proposed overlay system
Network-layer transparency	Yes	No (TUN experimental)	Partial	Yes
Resilience to loss/NAT	Low	High	Medium	High
Automated config provisioning	No/manual	No	Limited (JIT)	Yes (Telegram bot)
Centralised management & revocation	Partial	No	Yes	Yes
Self-hosted deployment	Yes	Yes	No	Yes

The developed system retains the full network-layer integration of classical VPNs while achieving the resilience of modern proxy protocols. The Telegram-based automation layer significantly reduces human-factor risks. The self-hosted controller and the absence of "phone-home" calls to third-party cloud servers satisfy data sovereignty requirements and eliminate threats related to compromise or unavailability of external coordination services, as demonstrated in several commercial ZTNA products (National Security Agency, Cybersecurity Directorate, 2026).

LIMITATIONS

1. The current implementation places the overlay controller on a single VPS, creating a single point of failure. A distributed or mesh controller would improve fault tolerance.

2. The Telegram bot introduces a dependency on a third-party messaging infrastructure, which may be unacceptable for organisations with high confidentiality requirements.

3. The revocation mechanism is control-plane-driven and assumes network connectivity between the controller and client nodes at the time of revocation.

CONCLUSION AND FUTURE WORK

This paper presents an information system for secure remote access that combines an overlay network architecture with automated access management via a Telegram bot and a web administration panel. The system operates stably under unstable network conditions (high latency, packet loss, NAT/CG-NAT) and implements zero-trust principles through centralised authentication, segmentation policies and immediate revocation. Experimental validation confirmed a 95 % reduction in administrative load, improved security and connection stability.

Future research directions include:

1. Integration with SIEM systems (e.g., Wazuh, ELK Stack) for advanced anomaly detection and security event correlation.

2. Support for hybrid transport (QUIC + TCP fallback) to improve resilience under aggressive traffic filtering.

3. Replacement of the Telegram bot with a fully self-hosted solution (Matrix, Mattermost) to eliminate dependency on third-party services.

4. Formal security verification of the configuration generation pipeline (including correctness analysis of ACLs and segmentation policies).

5. Post-quantum cryptographic agility – enabling replacement of encryption and authentication algorithms in accordance with NIST recommendations for post-quantum standards.

REFERENCES

ATIS. 5G Policy Management for Zero Trust. ATIS White Paper. 2026, April. https://www.atis.org/wp-content/uploads/2026/04/ATIS-5G-Zero-Trust-WP.pdf

Choi YB. A certainty-based approach to implementing zero trust architecture using NIST SP 800-207 and NIST SP 1800-35. KAUPA Lett 2025,13:11. https://doi.org/10.5703/1288284318461

Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model Version 2.0. 2023, April. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf

Gentyala, S. Reimagining the browser as a critical policy enforcement point: A Zero Trust Security Architecture for modern enterprises. Cloud Security Alliance (CSA). 2026, January 14. https://cloudsecurityalliance.org/articles/reimagining-browser-as-policy-enforcement-point

IonQ, Applied Research Laboratory for Intelligence and Security (ARLIS). SEQCURE Program: Zero Trust Security Framework for Mission-Critical Quantum Architectures. 2026. https://www.ionq.com/news/ionq-and-arlis-partner-to-establish-zero-trust-security-framework-for-mission-critical-quantum-architectures

ISC2 Insights. Building a Zero Trust Certification Roadmap for enterprise enforcement. 2026, April 29. https://www.isc2.org/Insights/2026/04/zero-trust-certification-for-enterprise-enforcement

National Institute of Standards and Technology. Implementing a Zero Trust Architecture: High-Level Document. NIST Special Publication 1800-35. Gaithersburg, MD; 2025. https://doi.org/10.6028/NIST.SP.1800-35

National Security Agency, Cybersecurity Directorate. Zero Trust Implementation Guidelines: Primer and Discovery Phase. 2026. https://media.defense.gov/2026/Jan/08/2003852320/-1/-1/0/CTR_ZERO_TRUST_IMPLEMENTATION_GUIDELINE_PRIMER.PDF