Vladyslav Karakai
Kyiv National University of Technologies and Design
(Kyiv, Ukraine)
Liudmyla Roienko
Kyiv National University of Technologies and Design
(Kyiv, Ukraine)

SEAMLESS ROAMING TECHNOLOGY OF THE WIREGUARD PROTOCOL AS THE FOUNDATION FOR THE STABLE WORK OF MOBILE EMPLOYEES

The shift towards hybrid work models necessitates reliable enterprise network access. Traditional virtual private network solutions often fail to maintain stable connections during network transitions. This paper examines the seamless roaming capabilities of the WireGuard protocol. By utilizing a connectionless architecture and cryptokey routing, WireGuard provides uninterrupted connectivity for mobile employees. The implementation of this protocol on modern enterprise edge routers is also discussed, highlighting its efficiency and business value in maintaining continuous corporate operations.

Modern enterprise operations rely heavily on constant connectivity. Employees frequently switch between different network environments, such as home wireless networks, corporate infrastructure, and cellular data connections. Maintaining secure access to corporate resources like internal databases or secure shell sessions during these transitions is a significant technical challenge. Traditional virtual private network solutions often struggle with these environment changes, resulting in dropped sessions and lost productivity. This paper proposes the adoption of the WireGuard protocol as a primary solution for enterprise mobility, focusing strictly on its built-in roaming mechanics and architectural simplicity.

Legacy network protocols were designed primarily for static connections. They rely on stateful connection models to maintain secure tunnels. When a client device changes its external internet protocol address due to a network switch, the underlying

transmission control protocol or complex stateful user datagram protocol sessions break. The client must then renegotiate the connection with the server. This renegotiation involves a heavy cryptographic handshake, exchanging certificates, and establishing a completely new session state. For an employee working in transit, this means frozen applications and the need to manually reconnect to internal services, causing operational delays and increasing the load on technical support departments.

WireGuard introduces a fundamentally different approach based on a minimalistic design and modern cryptographic primitives. Instead of managing complex session states, it operates primarily as a connectionless protocol. The core concept enabling this functionality is cryptokey routing. In this architecture, every peer network node possesses a strictly defined public and private key pair. The server associates each public key with a specific list of allowed internal network addresses. When an encrypted packet arrives, the server checks if it can be decrypted using the sender's known public key. If the decryption is successful and the internal source address matches the allowed list, the packet is processed. This elegant logic eliminates the need for maintaining a persistent session state in the traditional sense, treating network tunnels more like standard routing interfaces.

The connectionless nature of this protocol is the absolute foundation of its seamless roaming technology. The central server continuously keeps track of the latest external address and port from which it received a valid, properly authenticated packet from a specific peer. This external address is known within the protocol logic as the endpoint. If an employee's mobile device switches from a local wireless network to a cellular data network, its external address changes instantly. The client device simply continues sending encrypted packets to the server routing interface. As soon as the server receives and successfully decrypts the first packet originating from the new network address, it automatically updates the endpoint associated with that specific peer. The internal tunnel address remains completely unchanged throughout this process. Consequently,

application-layer connections experience zero interruption. The user simply continues their work without noticing the underlying network transition.

Deploying this technology within a corporate environment typically involves edge routing equipment. Modern network operating systems, including the open-source VyOS platform and proprietary systems used in enterprise routers, provide native kernel-level support for this protocol. Implementing this architecture on such enterprise routers is highly efficient. The industry transition of network hardware towards modern architectures, specifically ARM64, has significantly improved the processing of cryptographic workloads. Edge routers can now handle high-throughput encrypted tunnels with minimal central processing unit overhead. The configuration process is radically simplified compared to legacy enterprise protocols, requiring only the exchange of public keys and the definition of allowed routing ranges.

The implementation of modern connectionless tunneling addresses a critical bottleneck in enterprise mobility. By abandoning strict stateful session management in favor of cryptokey routing and dynamic endpoint updating, the protocol guarantees stability for users switching between physical networks. This technical reliability translates directly into tangible business value by minimizing connectivity-related downtime and ensuring the continuous productivity of mobile employees.

REFERENCES:

1.Donenfeld J. A. (2020) WireGuard: Next Generation Kernel Network Tunnel. *NDSS Symposium*. [Electronic resource] URL: WireGuard: Next Generation Kernel Network Tunnel (date of access: 27.04.2026).

2.MikroTik. WireGuard. *MikroTik Documentation*. [Electronic resource]URL: WireGuard - RouterOS - MikroTik Documentation (date of access: 28.04.2026).

3.VyOS Networks. WireGuard. *VyOS Documentation*. [Electronic resource] URL: WireGuard — VyOS rolling release (current) (date of access: 01.05.2026).