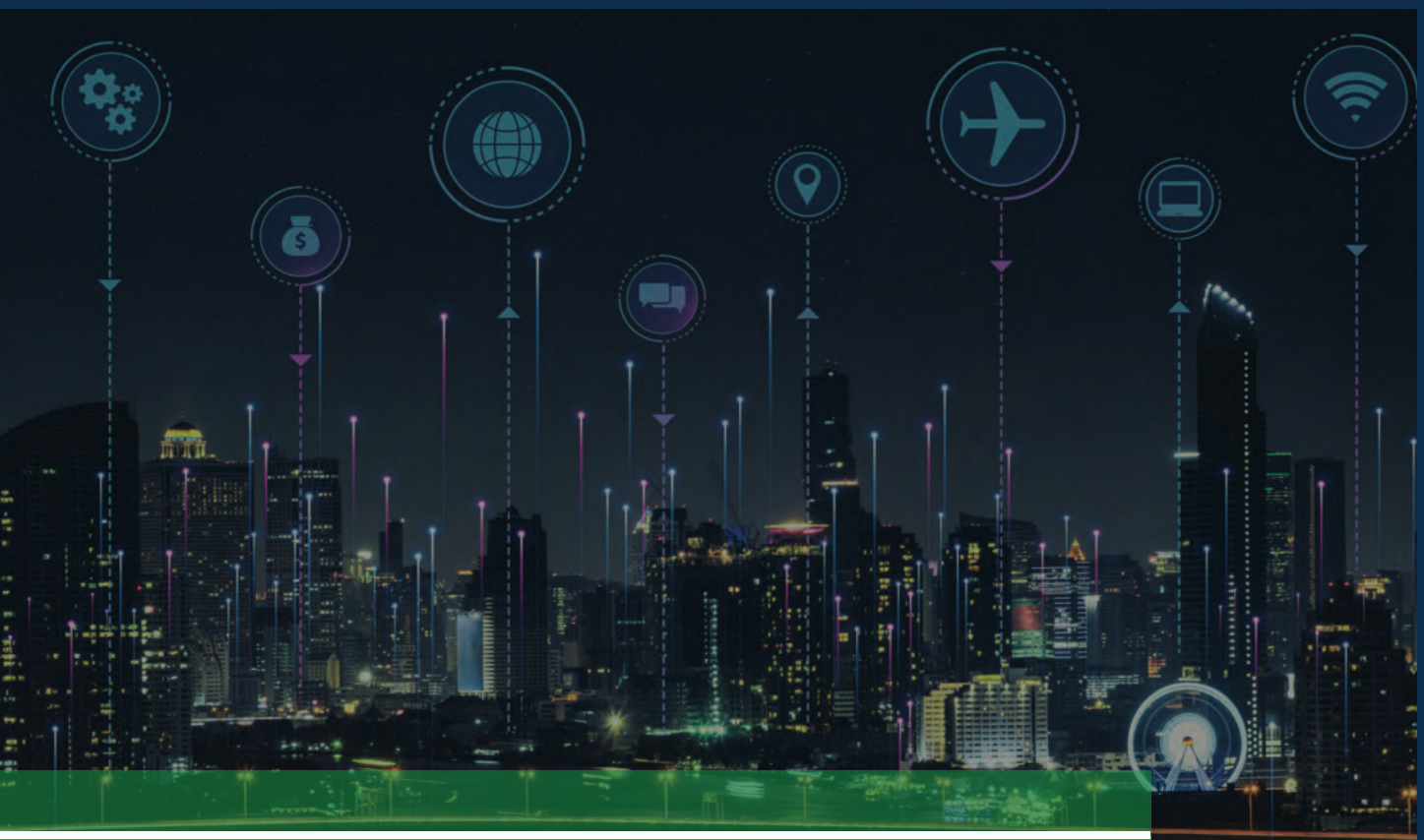
GABRL
Secure. Stealthy.
Quantum Resistant.

DEVIS



WHITE PAPER

GABRL: Zero Trust Secure Communications for the Modern Enterprise

Executive Summary

In today's evolving threat landscape, organizations require security architectures that eliminate implicit trust while maintaining operational efficiency. GABRL (Global Access Boundary Reinforced Link) by Devis delivers software- based, peer-to-peer encrypted communications that fundamentally transform enterprise security through Zero Trust principles. By implementing direct connections between endpoints with ephemeral certificates and Layer 3 encryption, GABRL eliminates network hairpinning, reduces attack surfaces, and enforces granular access controls—all without the performance penalties associated with traditional security approaches. This white paper examines how GABRL's architecture addresses critical security challenges, enhances network performance, reduces costs, and provides a practical path to comprehensive Zero Trust security.

The Problem: The Changing Security Landscape

Network security paradigms have fundamentally shifted. The traditional perimeter-based security model is increasingly inadequate against sophisticated threats and modern operational realities like distributed workforces and multi-cloud environments. Key challenges include:

Distributed Workforce Adoption: Remote work is now standard, demanding secure access from unmanaged networks globally. Traditional VPNs often create bottlenecks and grant overly broad network access.

Multi-Cloud Migration: Applications spanning multiple clouds dissolve traditional network boundaries, requiring security that transcends individual provider controls.

IoT Proliferation: The surge in connected devices expands the attack surface, often without adequate built-in security.

Sophisticated Threat Evolution: Advanced persistent threats exploit centralized architectures and implicit trust, as seen in major supply chain attacks like SolarWinds.

Regulatory Requirements: Mandates like Executive Order 14028 require Zero Trust implementations, emphasizing continuous verification and least privilege.

Traditional VPNs and security tools were not designed for this dynamic environment. They often funnel traffic through central gateways, creating performance bottlenecks, single points of failure, and vulnerabilities to lateral movement if compromised. A new approach, built on Zero Trust principles, is essential. GABRL provides this new approach through an innovative, software-defined architecture.

The Solution: GABRL Technology Overview

GABRL replaces traditional network security with a software-only solution built on Zero Trust principles. Its architecture consists of integrated components working together:

Endpoint Agents:
Lightweight software (minimal CPU/memory/disk impact) for diverse platforms (Windows, Linux, macOS, iOS, Android, IoT/embedded) that implements local Layer 3 encryption (IPSec/AES-256), enforces policy, and verifies identity.

Management Platform:
A central service for policy orchestration, authentication, authorization, and certificate management. Crucially, it operates outside the data path, enhancing security and scalability. Deployed in the customer's cloud or data center.

Encrypted P2P Tunnels:
Direct, ephemeral IPSec tunnels are established dynamically between authenticated and authorized endpoints, bypassing intermediaries.

This architecture fundamentally separates the control plane (authentication, policy) from the data plane (encrypted communications). The management platform authorizes connections but never processes the data traffic itself. This eliminates man-in-the-middle risks and performance bottlenecks associated with centralized processing.

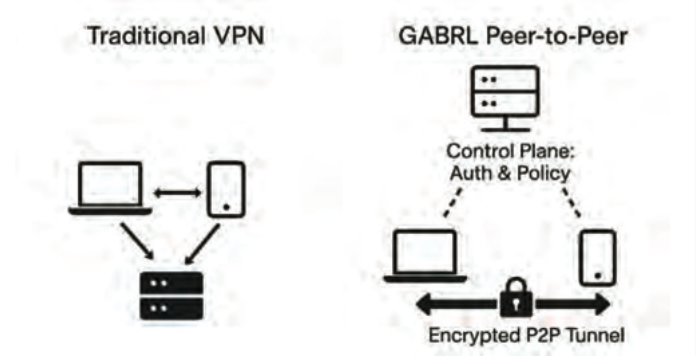


Figure 1: Architectural Comparison: Traditional VPN vs. GABRL Peer-to-Peer Model

Left: Traditional VPN Architecture - Endpoints (laptops, mobiles) route all traffic through a central VPN concentrator, which then connects to the corporate network. This creates a single point of failure and adds latency from hairpinning.

Right: GABRL Peer-to-Peer Model - Endpoints establish direct, encrypted tunnels between each other. A separate management platform handles authentication and policy, but never touches the data traffic. This reduces latency, removes bottlenecks, and enforces Zero Trust controls at the network layer.

This unique architecture enables several core capabilities that differentiate GABRL from traditional solutions.

Core Capabilities and Differentiators

GABRL delivers comprehensive Zero Trust security through distinct capabilities:

Layer 3 Peer-to-Peer Encryption:

- Implements IPSec/AES-256 encryption at the network layer (Layer 3), protecting all application traffic automatically (unlike Layer 7 solutions).
- Direct P2P tunnels eliminate "hairpinning," reducing latency (testing shows 30-40% reduction vs. VPNs), lowering bandwidth costs (15-25% typical reduction), and removing single points of failure.

Ephemeral X.509 Certificates:

- Generates unique, single-use X.509 certificates for each session, existing only in memory and destroyed upon termination.
- Provides perfect forward secrecy and eliminates traditional PKI management burdens (revocation lists, rotation).

Multi-Factor Authentication (MFA) & Strong Identity:

- Integrates robust MFA (knowledge, possession, inherence, context) before authorizing connections, aligning with EO 14028.
- Verifies both user identity and device posture.

Micro-segmentation & Least Privilege:

- Enforces fine-grained access controls based on identity and policy. Resources not explicitly authorized remain invisible.
- Prevents lateral movement by creating logical security boundaries independent of network topology. Policy updates are pushed in real-time.

Quantum Resistance:

- Incorporates quantum-resistant cryptographic features, including hybrid classical + post-quantum handshakes (e.g., using Kyber), protecting against "harvest now, decrypt later" attacks.

Single Packet Authorization (SPA):

- Optionally makes protected resources invisible to unauthorized scans. Requires a cryptographically signed packet for initial connection; unauthorized probes receive no response, disrupting reconnaissance.

Software-Only & Flexible Deployment:

- 100% software solution, requiring no specialized hardware appliances.
- Deploys flexibly in any cloud (AWS, Azure, GCP), on-premises data centers, or hybrid environments, with the management platform fully controlled by the customer.

Key Differentiators

True P2P
Direct encrypted tunnels, no central data processing.

Layer 3 Security
Protects all applications, not just web traffic.

Ephemeral Credentials:
Session-unique certificates eliminate PKI overhead and risk.

Software-Only
No hardware required, flexible deployment.

Quantum-Ready
Built-in protection against future threats.

Customer Control
Management platform deployed in your network.

These capabilities translate into tangible benefits across various deployment scenarios.

Benefits and Use Cases

Implementing GABRL provides significant advantages across federal and enterprise

Environments:

Key Benefits:

- **Enhanced Security:**
  Dramatically shrinks attack surface, prevents lateral movement, eliminates MITM risks, provides quantum resistance, and aligns with Zero Trust mandates (EO 14028, NIST SP 800-207).
- **Improved Performance:**
  Direct P2P connections minimize latency and reduce bandwidth consumption compared to traditional VPNs.
- **Lower Costs:**
  Avoids hardware costs and vendor lock-in; integrates with existing infrastructure; reduces administrative overhead through automation.
- **Operational Flexibility:**
  Deploys anywhere and supports diverse endpoints.
- **Streamlined Compliance:**
  Meets key requirements of NIST and CISA guidelines, simplifying authorization processes.

Use Cases:

Key Benefits:

- **Secure Tactical Operations:**
  Covert, resilient, encrypted links in contested environments over any available network (Wi-Fi, LTE, Satcom).
- **Zero Trust Remote Access:**
  Replaces legacy VPNs for secure remote work aligned with OMB mandates.
- **Inter-Agency & Coalition Collaboration:**
  Creates ephemeral secure enclaves for controlled, sensitive data sharing (e.g., DHS-DoD).
- **Classified Data Protection:**
  Enables secure transmission aligned with CSfC requirements.

Benefits and Use Cases

Implementing GABRL provides significant advantages across federal and enterprise environments

VPN/MPLS Replacement:
Secure, high-performance connectivity over the internet, reducing costs.

Branch Office Connectivity:
Direct, secure tunnels between locations without site-to-site VPN complexity.

Remote Workforce Security:
Granular, resource-specific access for remote employees.

IoT/OT Security:
Protects vulnerable IoT devices and Industrial Control Systems (ICS/SCADA) at Layer 3 without impacting performance.

Supply Chain Security:
Provides least-privilege access for vendors and partners.

GABRL's performance advantages and minimal resource needs make it suitable for these diverse use cases.

Performance and Resource Considerations

GABRL is designed for efficiency, delivering enhanced security without compromising performance or requiring excessive resources.

Performance Advantages:

- **Latency Reduction:**
  30-40% lower latency compared to typical VPNs due to direct P2P routing.
- **Bandwidth Efficiency:**
  15-25% reduction in bandwidth consumption by eliminating traffic duplication at concentrators.
- **Throughput Scaling:**
  Scales linearly with endpoints; no central bottlenecks limit throughput.
- **Connection Density:**
  No central connection limits; supports massive endpoint counts.

Minimal Resource Requirements:

- **Endpoint Impact:**
  <50MB disk space, ~25MB runtime memory, <2% average CPU utilization, negligible battery impact. Supports Windows, macOS, Linux, iOS, Android, and embedded systems.
- **Management Infrastructure:**
  Modest virtual or physical server requirements (e.g., 4-8 cores, 16-32GB RAM for up to 10,000 endpoints), scaling linearly.
- **Administrative Overhead:**
  Reduced burden through automated certificate management, centralized policy, templates, and API integration.

Implementation and Integration

Devis utilizes a proven, four-phase methodology for GABRL deployment, ensuring a smooth transition to Zero Trust.

Implementation Methodology:

- **Discovery & Planning:**
  Assess current state (network, security, identity, apps), define requirements (security, performance, compliance), and plan the project (timeline, resources, risks).

- **Demonstration & Scoping:**
  Validate GABRL capabilities in a lab/pilot environment against use cases, finalize the deployment architecture (cloud, on-prem, hybrid), and plan capacity.

- **Funded Pilot:**
  Deploy to a limited user group, test core policies (potentially starting in monitor-only mode), integrate with production systems, measure performance, and refine operational processes.

- **Production Deployment:**
  Phased rollout across the organization, implement comprehensive policies, integrate monitoring, train staff, and establish continuous optimization.

Integration Capabilities:

GABRL integrates seamlessly with existing enterprise systems:

- **Network:**
  Standard protocols (IPSec/UDP), compatible with existing routing, firewalls, load balancers, QoS, NAT traversal.

- **Identity:**
  AD/LDAP, SAML 2.0, OAuth/OIDC, PKI integration.

- **Security Operations:**
  SIEM (Syslog), REST API, SNMP, email alerts, webhooks.

- **DevOps:**
  API-driven configuration, Terraform/Ansible support, containerized components.

- **Device Management:**
  Integrates with MDM/EDR for device posture assessment.

This integration strategy leverages existing investments, reducing complexity and cost during the transition to Zero Trust. GABRL offers a comprehensive, practical, and high-performance solution for modern enterprise security.

Lorem ipsum

Modern Security Demands GABRL

Traditional security architectures, built on outdated assumptions of perimeter trust, fail to address the complexities of modern IT environments and the sophistication of current threats. **GABRL** provides a fundamental shift, delivering true Zero Trust security through its innovative software-based, peer-to-peer encrypted communication model.

By eliminating implicit trust, enforcing least privilege via micro-segmentation, using ephemeral credentials, and enabling direct, high-performance connections, GABRL significantly enhances security posture, improves user experience, and reduces infrastructure costs. Its alignment with federal mandates (EO 14028, NIST SP 800-207) and proven success in demanding environments make it an ideal solution for organizations seeking comprehensive security transformation without compromise.

Ready to transform your security with Zero Trust?

Contact Devis today to schedule a demonstration and learn how GABRL can secure your modern enterprise. Visit https://www.devis.com/gabrl or reach out to info@devis.com.

Contact Information:

Phone: (610) 608-0984

Email: info@devis.com

Website: www.devis.com