DEVIS

WHITE PAPER

The Double Imperative: Technical Architecture

Zero Trust Enforcement & Quantum-Resistant Cryptography with GABRL

The Double Imperative: Technical Architecture

Federal networks must simultaneously erase implicit trust and ensure that today's data cannot be decrypted tomorrow. Legacy perimeter VPNs fail here: static ACLs invite lateral movement, and long-lived RSA handshakes are future fodder for quantum attacks. GABRL was engineered for this exact intersection—bringing ZTA's "never trust, always verify" to the transport layer while eliminating harvestable asymmetric keys.

Architectural Overview

GABRL operates as a Layer 3 IPSec overlay that fundamentally separates the control plane (authentication, policy, certificate management) from the data plane (encrypted peer-to-peer tunnels). The management platform authorizes connections but never processes data traffic itself, eliminating man-in-the-middle risks and performance bottlenecks.

Control Plane Architecture

The GABRL control plane runs as a highly available Kubernetes cluster deployable on any cloud (AWS, Azure GCC-High, GCP), bare-metal infrastructure, or hybrid environments. The platform has been validated at scale supporting hundreds of thousands of concurrent connections with linear horizontal scaling.

Core Control Plane Functions:

- Policy orchestration and enforcement via modular Policy Engine with distributed Policy Enforcement Points (PEPs)
- Certificate Authority operations: Root/Sub-CA management with peer certificate signing
- Device provisioning and registration tracking
- OIDC/SAML integration for identity federation (Azure Entra, Okta, etc.)

The control plane operates entirely outside the data path—it authenticates endpoints and authorizes tunnel establishment but never touches application traffic. This architectural separation means control plane compromise does not expose data in transit.

The platform has been validated at scale supporting tens of thousands to millions of concurrent connections with horizontal and vertical scaling.

Cryptographic Tunnels

Once authenticated, endpoints establish direct IPSec tunnels between each other without routing through intermediary gateways. Traffic flows peer-to-peer using:

Algorithms:

- AES-256 (FIPS 197 validated)
- ML-DSA (NIST FIPS 204 standard)
- ML-KEM (NIST FIPS 203 standard)

Networking:

- All agent and control plane ports are UDP
- All AES channels are configured in tunnel mode for NAT traversal

Third-party validation:

Raytheon's 5G security team characterized GABRL as delivering "Zero Trust, one-time encrypted communication channels" where "open communications go dark with only UDP packets being visible" and "no information observable or usable."

Key Generation and Exchange Lifecycle

GABRL's cryptographic architecture eliminates the "harvest now, decrypt later" threat through **configurable ephemeral key rotation** at every layer.

Control Plane Key Custody

X.509 Certificate Issuance: By default, the control plane generates asymmetric keys and creates a Certificate Signing Request (CSR), which the control plane's Intermediate CA signs. The signed certificate and keys are encrypted using a symmetric key for secure distribution to the endpoint via API or web console. Critically, the control plane discards all key material after distribution—retaining only the certificate serial number for subsequent validation.

Alternative Custody Models: Using API integrations with OAUTH/SAML/OIDC workflows, organizations can implement full self-custody where endpoints generate their own key material and submit CSRs for signing. For DoD and classified environments, GABRL supports PIV credentials from CAC or other hardware tokens with existing trusted roots.

Control Plane Tunnel Keys: Each agent maintains a unique AES-256 symmetric key for its control plane connection, negotiated directly between agent and control plane.

Cryptographic Vault: A cryptographic vault secures all CA operations and signing functions. The master key is encrypted at rest using KMS or HSM. The Root CA is generated internally by default, but organizations can maintain an offline Root CA and import signed intermediates into GABRL.

Data Plane Key Custody

Peer Tunnel Certificates: For each peer-to-peer enclave, the agent generates its own CSR locally. The agent maintains full custody of all data plane key material—the control plane never possesses these keys.

Peer Tunnel Symmetric Keys: Each peer tunnel uses a unique AES-256 symmetric key negotiated directly between peers, with configurable rotation periods.

Network Verification: Inside vs. Outside the Enclave

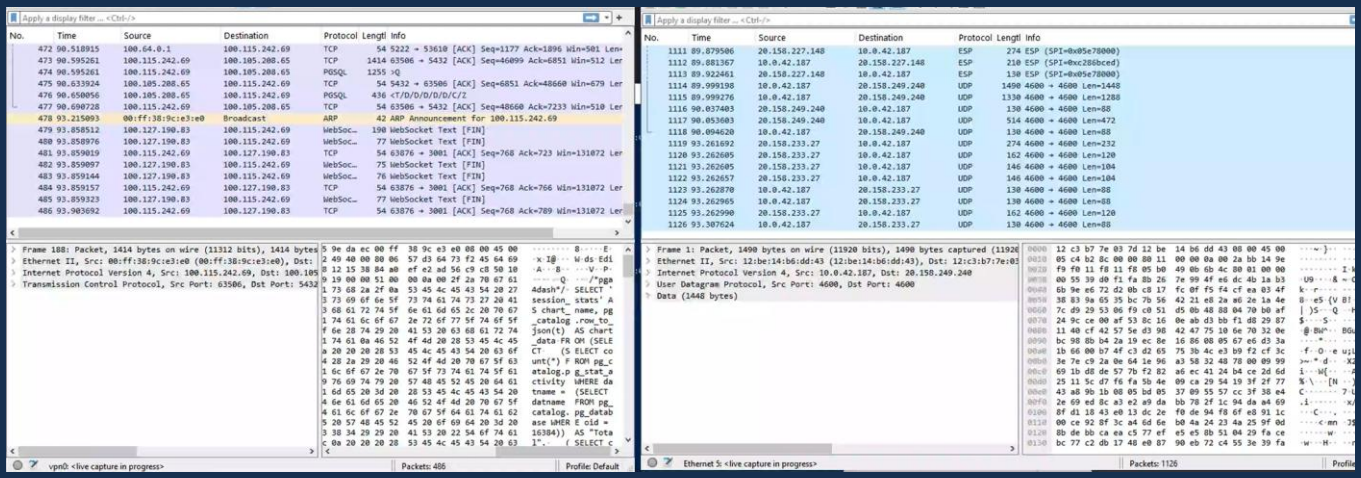

Figure 1. Wireshark captures confirm the architecture's claims. Inside the enclave (left), application-level protocols (PGSQL, WebSocket) and SQL statements are visible for operational monitoring. Outside the enclave (right), only encrypted ESP/UDP packets are observable.

Scalability and Performance

Control Plane Capacity

GABRL has been validated using a 3-node EKS cluster running r5n.4xlarge instances as the control plane. This test sustained 60,000 concurrent agents through multiple use cases over a 5-day period with no abnormalities. Agent devices were co-located on AWS but distributed across separate VPCs. Average CPU load was 60%; memory utilization was not significant (much of the load was log write and audit overhead).

Scaling Projections:

- Each additional node supports approximately 40,000–60,000 additional agents
- Modern Kubernetes supports ~1,000 nodes per cluster
- Practical limits are determined by overlay IP addressing:

Address Space	Capacity	Notes
IPv4 (CGNAT 100.64.0.0/10)	**~4 million endpoints**	Current default deployment
IPv4 (Private 10.0.0.0/8)	**~16 million endpoints**	Higher conflict risk with existing networks
IPv6	**Effectively unlimited**	Constrained only by system resources

MITRE Security Assessment

MITRE's evaluation concluded: *"No vulnerabilities or exploit chains were used to gain access" from external positions, and the "AWS cloud environment has a small external footprint that does not persist between uses, which mitigates many concerns of long-withstanding static infrastructure components."*

Network traffic analysis validated that tunnel communications show only encrypted UDP packets from external observation points—confirming no information is observable or usable to interceptors.

Performance Characteristics

Operating at Layer 3 eliminates proxy bottlenecks inherent to gateway-based architectures:

- Traffic flows directly between peers without routing through inspection points
- Protocol agnostic—handles any IP protocol (TCP, UDP, ICMP, SCTP, tactical data links)
- Low latency because GABRL encrypts only once at the source and decrypts only once at the destination. There are no intermediate decryption steps.

Identity Integration: Azure Entra Example

The diagram below illustrates GABRL's identity-driven provisioning flow using Azure GCC-High:

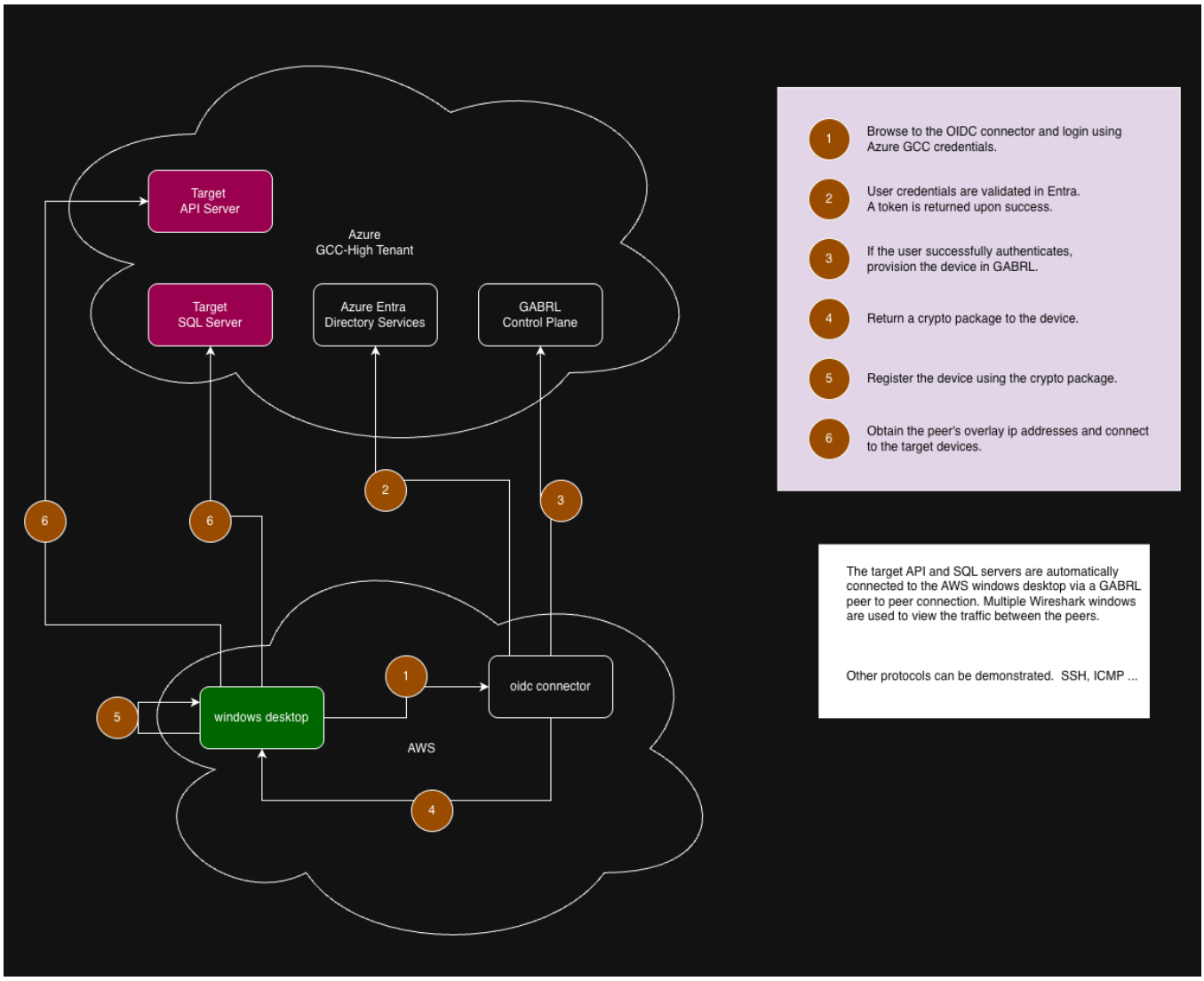

Figure 2. Cross-cloud identity integration: Endpoint in AWS authenticates via OIDC connector to Azure Entra in GCC-High tenant. GABRL control plane provisions device and returns crypto package. Endpoint registers, then establishes direct P2P tunnels to target servers.

Flow Sequence:

1. User browses to OIDC connector, enters Azure GCC credentials
2. Azure Entra validates credentials, returns signed token
3. OIDC connector forwards token; control plane provisions device
4. Control plane returns cryptographic package to endpoint
5. Endpoint registers, confirming membership
6. Endpoint establishes encrypted P2P tunnels to authorized targets

This identity-first model ensures **no connectivity exists until identity and device trust are established**. The control plane never processes data traffic—it only authorizes who may talk to whom.

CA Hierarchies as a Critical Vulnerability

GABRL's architecture addresses the dual mandate—Zero Trust enforcement and quantum-resistant cryptography—through **fundamental design choices** rather than bolted-on features:

- **Ephemeral everything:** Certificates, session keys, and tunnel state exist only as long as needed, then disappear
- **Separated planes:** Control plane authorizes; data plane encrypts; neither compromises the other
- **Peer-to-peer data flow:** No central gateway to target, harvest from, or bottleneck through
- **Post-quantum ready:** ML-KEM-768/ML-DSA operational today, not road mapped for future

Compliance Alignment

Directive / Standard	GABRL Alignment
NIST SP 800-207 (ZTA)	L3 microsegmentation, per-session validation, separated control/data planes
EO 14028	Strong encryption (AES-256), phishing-resistant MFA via OIDC federation
NSM-10	ML-KEM/ML-DSA quantum resistance
OMB M-22-09	Meets pillars: Identity, Devices, Networks, Data
OMB M-23-02	Crypto-agile design; NIST PQC algorithms operational
RMF / NIST 800-53	Aligns with AC, IA, SC control families; RMF artifacts packaged

The result is an architecture where interception yields only encrypted packets that cannot be decrypted **— not today, and not when quantum computers arrive.**

Contact Information:

Phone: (610) 608-0984

Email: hello@gabrl.com

Website: www.gabrl.com