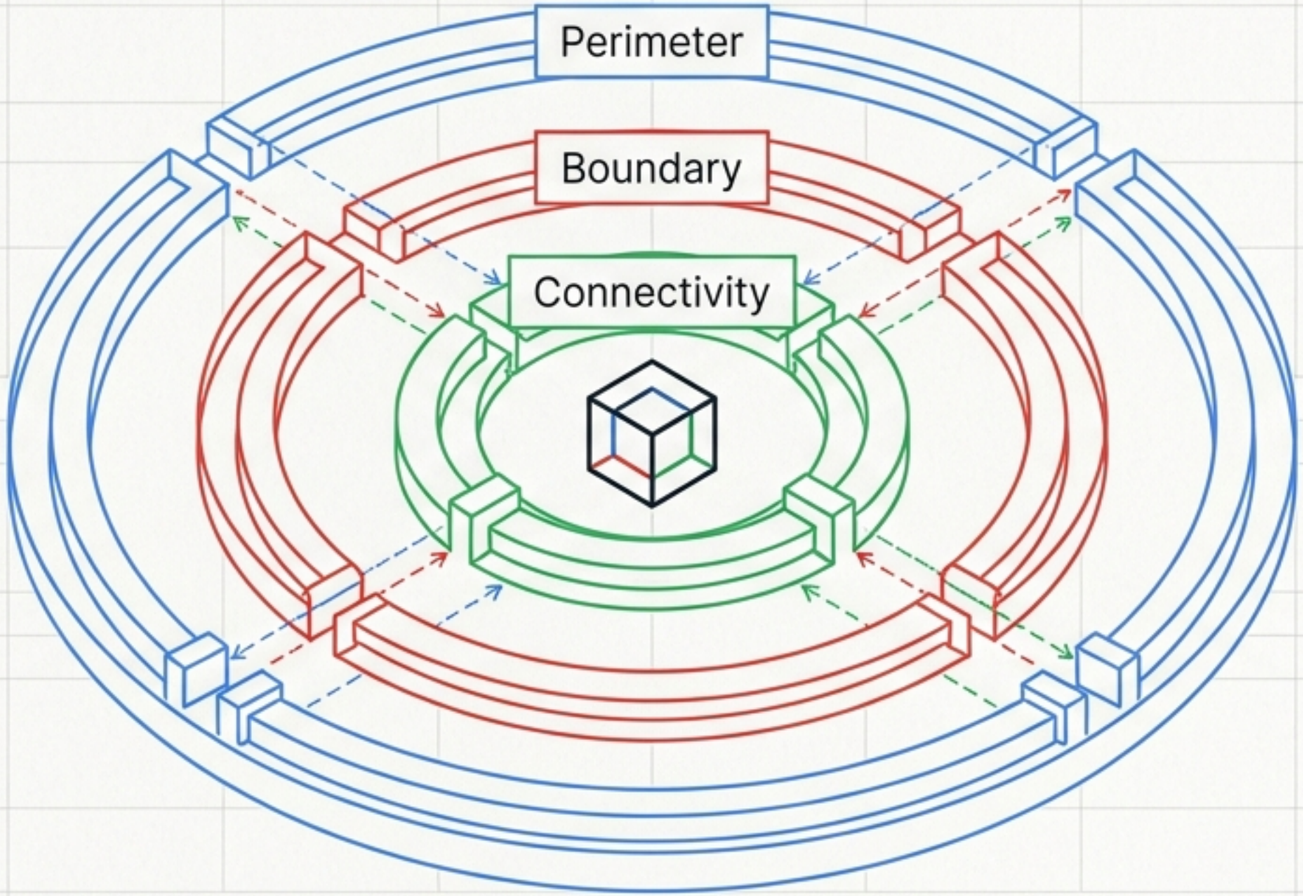
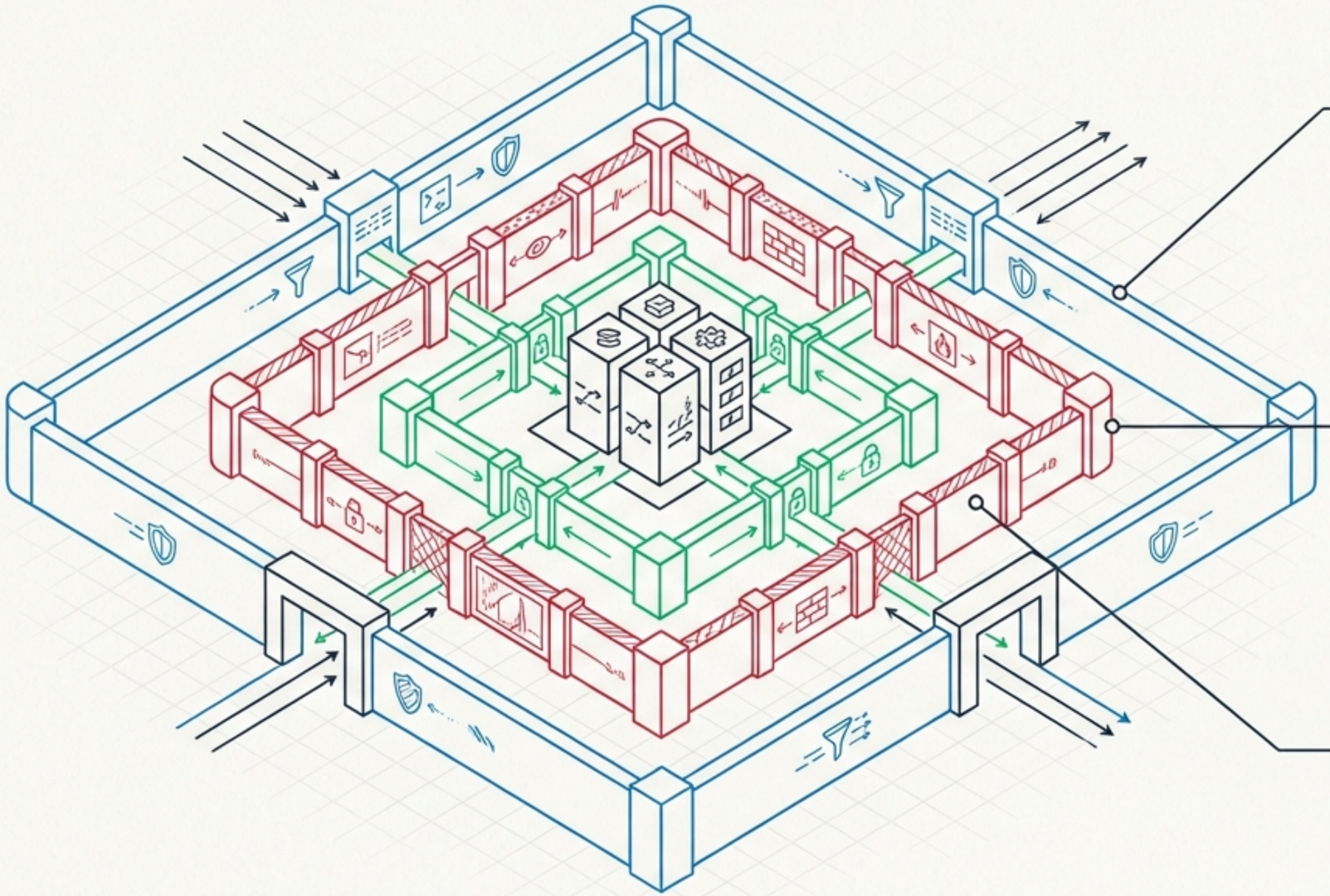
Google Cloud PSE Certification Guide: Section 2

Securing Communications and Establishing Boundary Protection



Exam Weight: ~22% | Framework Context: Tech Equity RAD

The Layered Citadel Framework



Layer 1: Perimeter Security

Inspecting and filtering **inbound traffic** before it touches a `workload` at the network edge.

Layer 2: Boundary Segmentation

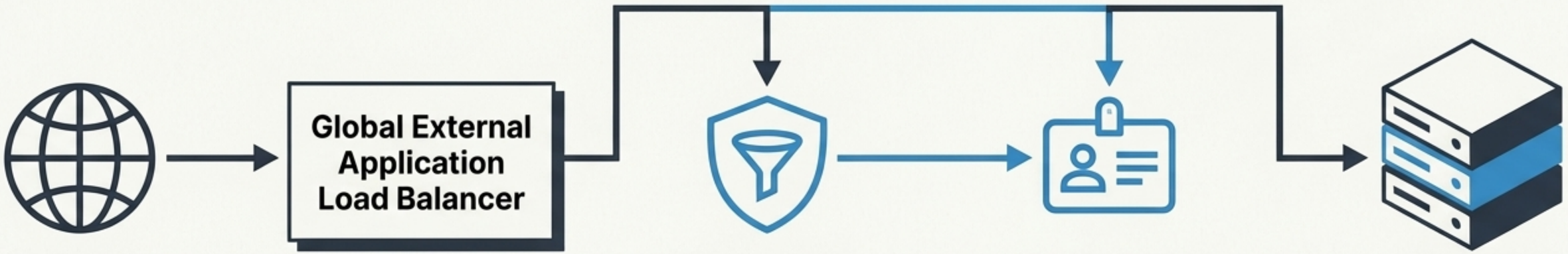
Creating `isolated zones` to contain breaches and prevent data exfiltration at the `API level`.

Layer 3: Private Connectivity

Ensuring `internal workloads` communicate and reach outbound services without traversing the `public internet`.

Pillar 1: Perimeter Security & The Edge

The Dual-Layer Edge Perimeter



External Traffic

Cloud Armor

Filters by threat signature and rate-limits at the edge. Enforces OWASP Top 10 preconfigured rule sets.

Identity-Aware Proxy (IAP)

Verifies authenticated user identity and context before any request reaches the backend.

Backend Application

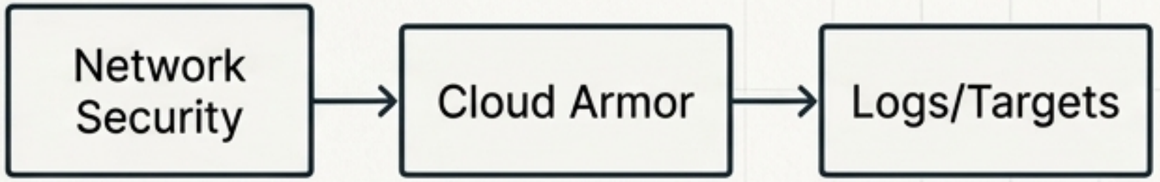
Perimeter Implementation: Theory-to-Console

Infrastructure as Code (RAD UI)

```
enable_cloud_armor = TRUE
enable_iap         = TRUE
```

Variables deployed via Group 9/13 and Group 4.

Google Cloud Console Verification



Real-World Application: Adaptive Protection

Cloud Armor Adaptive Protection detects an unexpected traffic spike from an Eastern European ASN matching a credential-stuffing pattern.

Generates a recommended rate-limiting mitigation rule for 1-click approval.

Outcome: Drops mitigation time from hours of manual firewall work to under two minutes.

Advanced Perimeter Controls

Cloud Next Generation Firewall (NGFW)

Layer 7 application inspection parsing HTTP, DNS, and TLS intent.

FQDN-based rules allow/deny traffic to domain names, not just IPs.

Hierarchical policies (Org/Folder) are enforced before Network policies (VPC).

Certificate Authority Service (CAS)

Cryptographic service identity via mutual TLS (mTLS) authentication.

Root CAs act as self-signed highest trust anchors.

Subordinate CAs are used for day-to-day dynamic certificate issuance.

Secure Web Proxy (SWP)

Explicit forward proxy for outbound HTTP(S) traffic.

Applies strict URL filtering policies and safe browsing categories.

Unlike Cloud NAT, inspects content and logs specific outbound requests for audit.

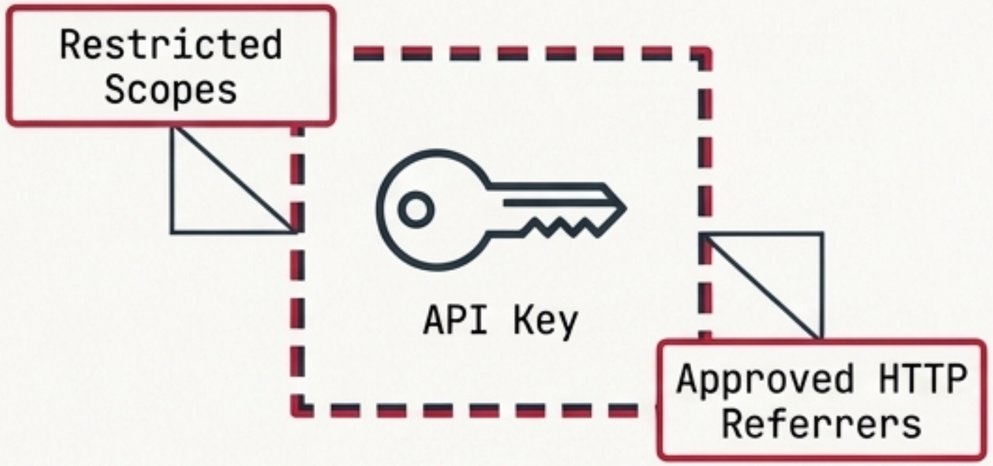
Continuous Security Posture

Cloud DNS Security

DNSSEC cryptographically signs records to prevent cache poisoning.

Response Policy Zones (RPZ) override responses to block command-and-control resolution.

API Attack Surface Reduction

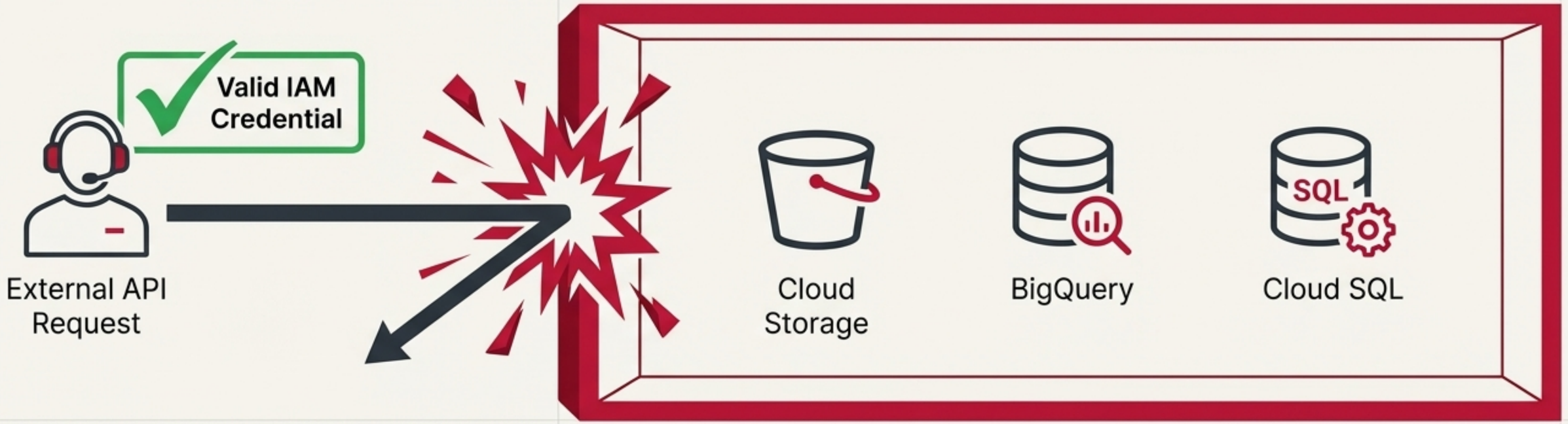


Organization Policy constraints actively shrink the attack surface.

`constraint: constraints/serviceuser.services`

Continuously monitors and restricts unused APIs to limit impact of key compromise.

Pillar 2: Boundary Segmentation



The Exfiltration Rule

IAM controls WHO can access resources.

VPC Service Controls (VPC SC) dictate FROM WHERE resources can be accessed.

Real-World Context

A stolen credential used from an attacker's home network attempts to download pre-trade research reports. Despite valid IAM, the request generates a VPC SC violation and is blocked at the boundary line.

Implementing Boundaries & Microsegmentation

Private-IP Cloud SQL

IP | Internal IP Only

No Public IP Routing

Accessible exclusively from workloads within the same VPC. Zero public internet exposure.

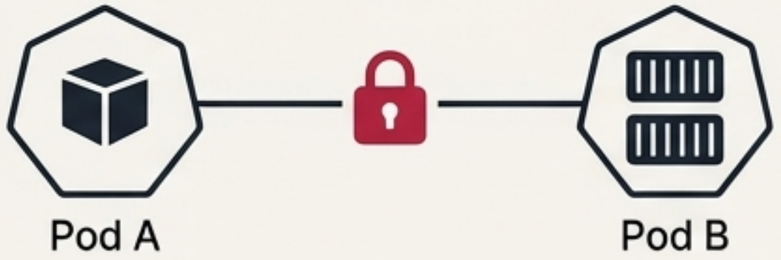
VPC Service Perimeter

`enable_vpc_sc = TRUE` → Security > VPC Service Controls

Isolates Google APIs (Cloud Storage, BigQuery) behind private boundaries independent of IAM.

GKE Dataplane V2 Microsegmentation

Cilium/eBPF Enforced Isolation

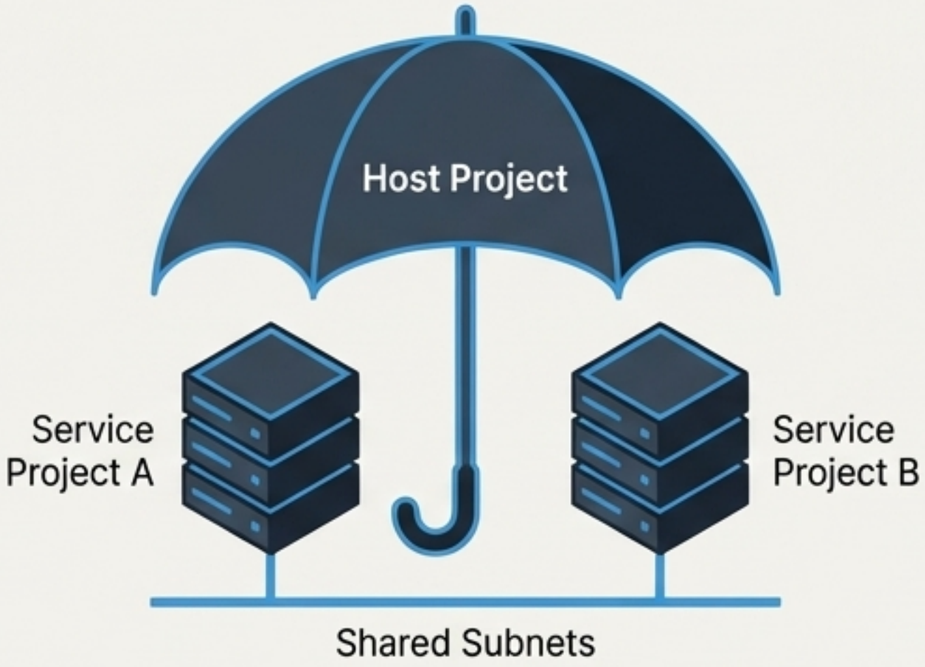



```
$ kubectl get networkpolicies -A
$
```

Enforces explicit pod-to-pod traffic rules. Only explicitly permitted microsegmentation traffic is allowed.

Structural Network Isolation

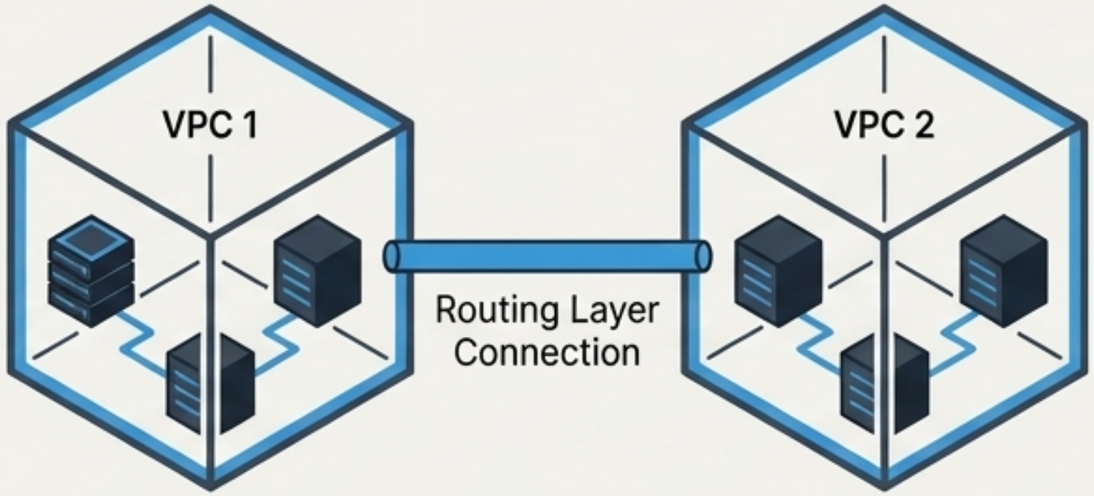
Shared VPC Architecture



Centralized network security administration (`firewall rules`, `routes`) with delegated resource management.

Use Case: Centralized security governance and single-team network administration.

VPC Peering

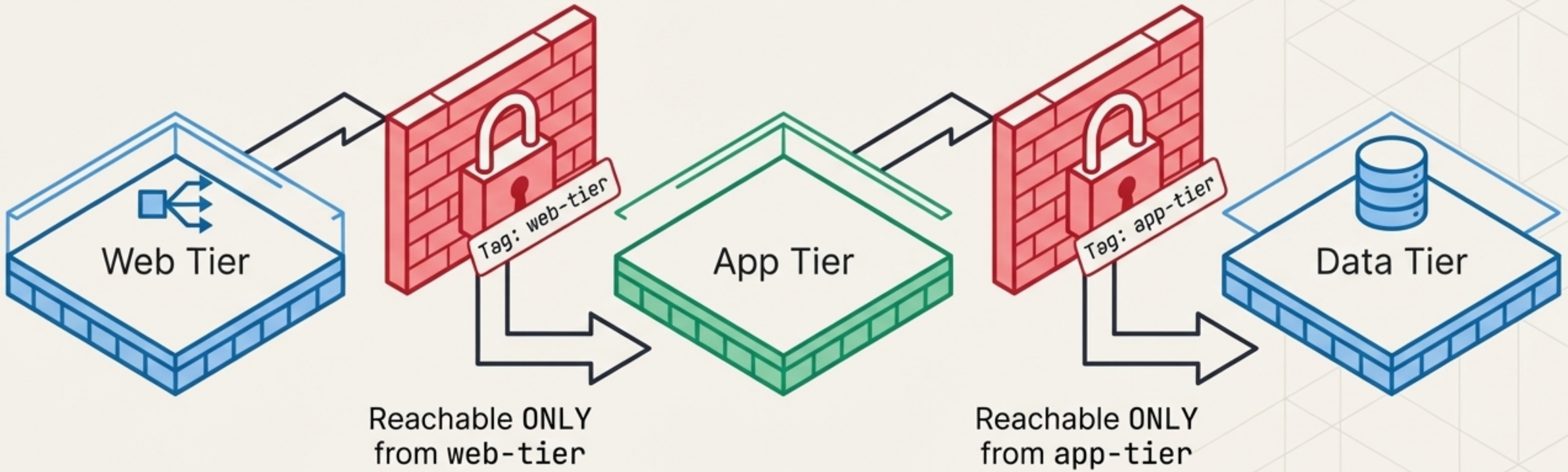


Non-transitive connection requiring `non-overlapping IP ranges`.

Each VPC retains entirely separate firewall administration and independent security policies.

Use Case: Distinct business units or external partner networks requiring strict administrative separation.

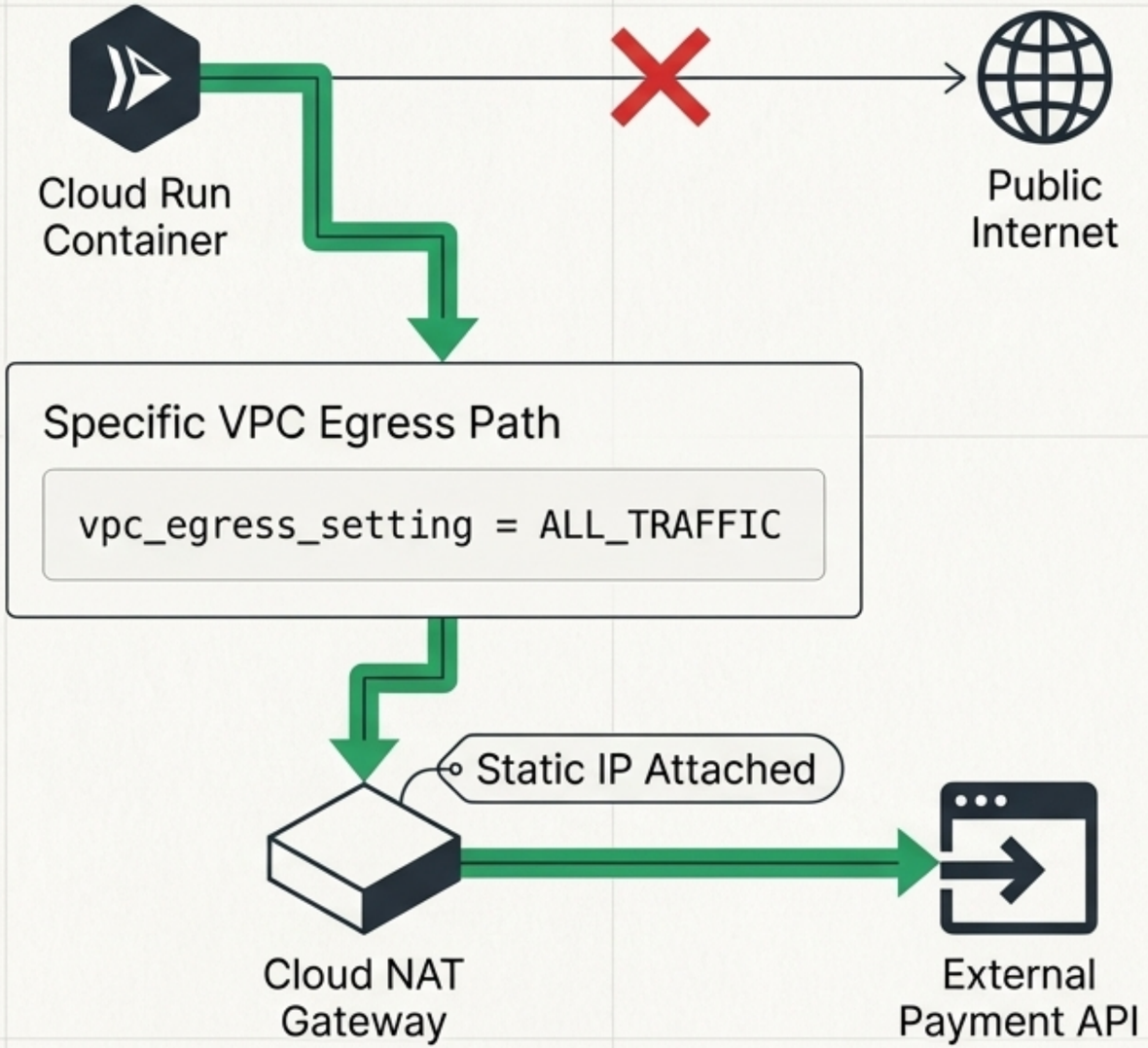
N-Tier Application Network Design



Functional Network Tags

Network tags construct precise, directional access control completely independent of rigid IP addresses. Lateral movement is structurally restricted at each tier boundary.

Pillar 3: Establishing Private Connectivity



Security Outcome: Direct VPC Egress

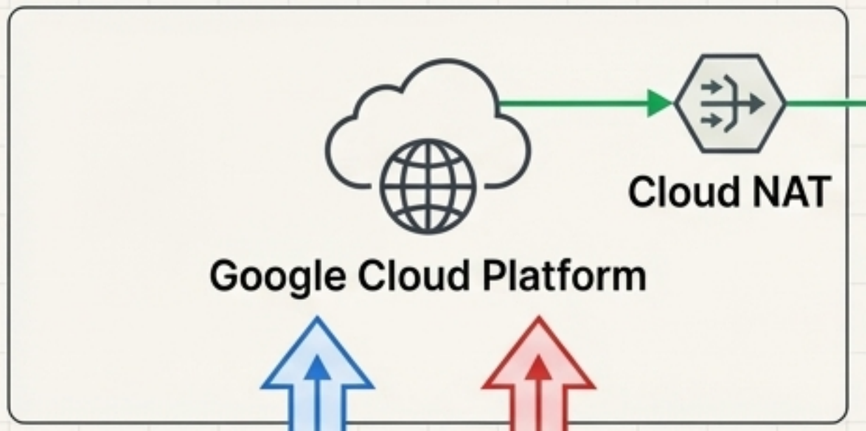
- Forces all external public API calls through the internal VPC first.
- Enables strict Cloud NAT logging, centralized firewall rule inspection, and consistent egress IP visibility.
- Allows external vendors to perform strict IP allowlisting based on the static NAT IP.

Accessing Google APIs Privately

Standard Private Google Access (PGA)	Restricted Private Google Access	Private Service Connect (PSC)

Route Target:
`private.googleapis.com`
 	
VIP Range:
`199.36.153.8/30`
 	
Enabled per subnet. Allows VMs with no external IPs to reach standard Google APIs via Google's private network.
	Route Target:
	`restricted.googleapis.com`
	
	VIP Range:
	`199.36.153.4/30`
	
	Crucial security constraint: Only allows APIs compatible with VPC Service Controls, structurally blocking exfiltration via unsupported APIs.
		Route Target:
		`Internal Consumer VPC IPs`
		
		VIP Range:
		`VPC Assigned`
		
		Consumes Google Cloud APIs through private IP addresses strictly internal to the consumer VPC. API traffic completely avoids shared public API endpoints.

Hybrid Egress & On-Premises Connectivity



Outbound Web Egress Logging

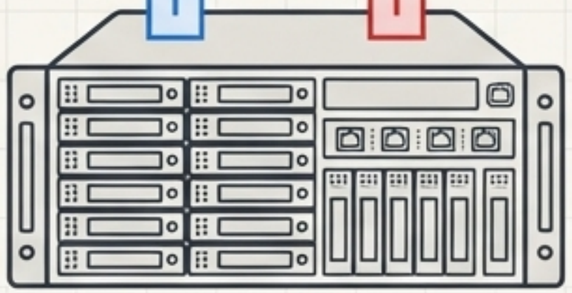
Provides source IP masquerading. Native logs capture every outbound connection's source IP, destination, and port for mandatory auditing and anomaly detection.

Encrypted site-to-site tunnels.
BGP required. 99.99% SLA.
~3 Gbps throughput per tunnel.

HA VPN

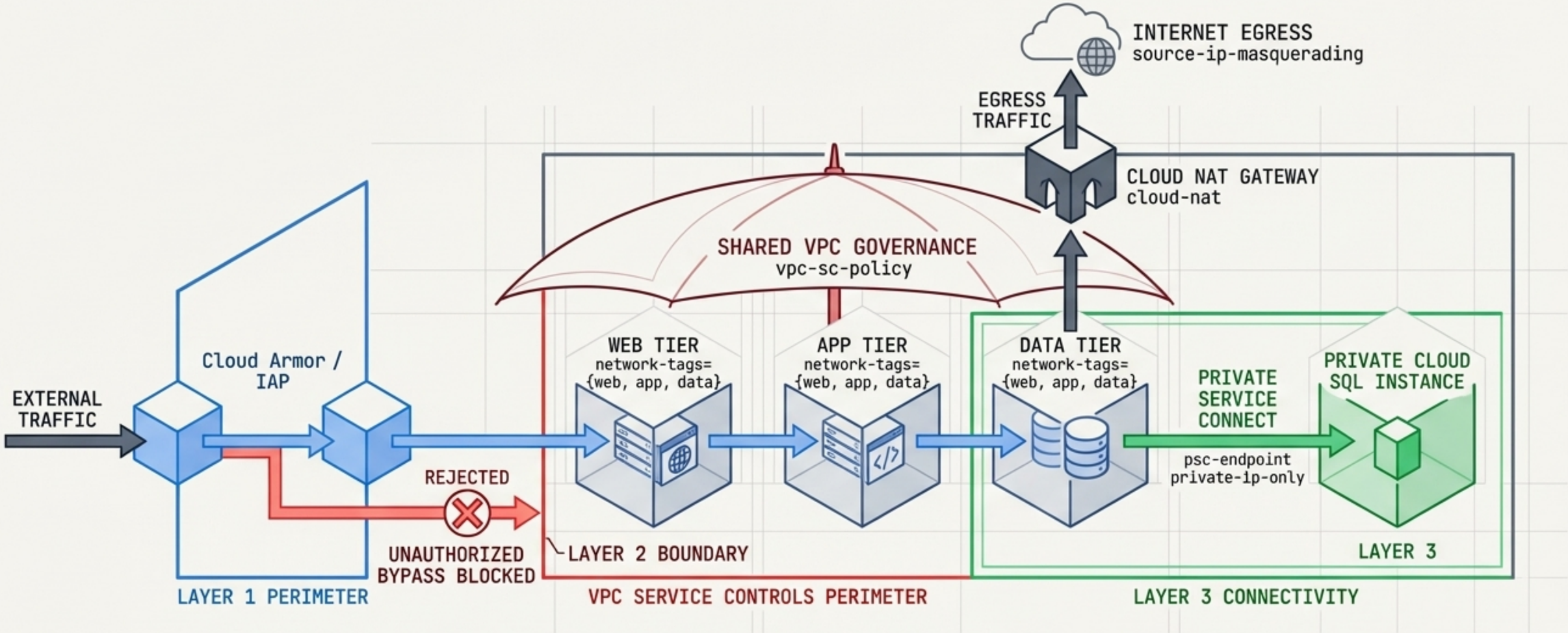
Cloud Interconnect

Direct physical connection.
BGP required. 10 or 100 Gbps.
Unencrypted by default (requires MACsec).



On-Premises Data Center

Synthesis: The Complete Cloud Fortress Architecture



Defense-in-depth is an interlocking routing architecture: the failure of any single layer is immediately contained by the explicit structural restrictions of the next.