APPENDIX — RC1 ADMIN PORTAL & GATEWAY REFERENCE ARCHITECTURE Evidence-Based Evaluation Frame for Vendor Paradigms (v0.2 POLISHED)

===

Purpose

This appendix documents the RC1 Gateway and Administrative Portal design because it is not merely an implementation artifact — it is the proof-of-implementability reference model that makes vendor evaluation possible.

The enterprise's initial request was framed as a product selection problem: "find us a solution we can buy to fix third-party access."

RC1 demonstrated a more fundamental truth:

Third-party exposure is not solved by connectivity alone. It is solved by governed service mediation: identity binding, protocol-aware inspection, containment, lifecycle control, and evidence generation.

Without an operational reference model, vendor claims cannot be evaluated credibly, scoping cannot be grounded, and integration cost cannot be estimated.

RC1 therefore provides the structural frame against which all vendor paradigms must be measured.

===

1. RC1 Gateway Horizontal Scaling Model

The RC1 data plane is a horizontally scalable Gateway (GW) cluster. Capacity is increased by adding nodes, not redesigning architecture.

Each node has two interfaces:

- eth0 (Public / Default VRF): Terminates tenant-facing IPsec connectivity.
- eth1 (Internal / Service-side): Routes mediated proxy traffic toward enterprise application domains.

Tenants terminate on routed loopback VIPs:

- Each tenant is assigned a unique loopback address from a shared block.
- Loopbacks exist on all nodes, with one node selected as primary.
- OSPF dynamically advertises the active tenant VIP upstream.

This enables:

- deterministic reachability
- horizontal scaling
- failover without readdressing

===

2. Tenant Isolation via VRF/VLAN/VXLAN Overlays

Each tenant is provisioned as a fully isolated logical segment:

- Tenant IP block
- Unique VRF name
- Unique VLAN ID
- Unique VXLAN ID

All gateway nodes participate in the tenant overlay, enabling multi-node service delivery while preserving isolation.

==

3. Portal as Governance Control Plane (Source of Truth)

The administrative portal is not “UI.” It is the control plane that makes governance operable.

Provisioning is executed through strict separation of duties:

- net_alloc (Allocation Authority): Assigns scarce shared resources: loopbacks, IP blocks, VRFs, VLANs, VXLAN IDs, proxy VIPs, egress IPs.

- net-imp (Implementation Authority): Applies infrastructure state: tunnels, routing, overlays, enforcement chains.

This model enables:

- deterministic automation
- audit replayability
- refusal authority through workflow gates
- lifecycle enforcement through portal governance

==

4. Why RC1 Was Required

RC1 was not discretionary. It answered three critical enterprise questions:

1. Can the theory be implemented?
2. What does “self-service governance” actually require?
3. What is the real integration cost driver?

RC1 proved that the dominant cost is workflow, not licensing. It also established the “Service Exposure Instance” as the unit of control, not the tunnel or firewall rule.

==

MATRIX 1 — FEATURE RESPONSE ALIGNMENT (Supported / Limited / Not Supported)

Capability Area Cisco Cloudflare Zscaler F5

Identity-based access control Supported Supported Supported Supported IPsec connectivity Supported Supported Limited Supported HTTP/API proxy inspection Supported Supported Supported Supported SSH/SFTP deep inspection Limited Not Supported Not Supported Supported Session recording / containment Limited Limited Not Supported Supported Self-service portal workflow Supported Limited Limited Requires build Managed service delivery option Supported Partial Partner-led Supported/Partner

Evidence notes: - Design review highlights Zscaler lacks SSH DPI and session inspection. - Cisco Secure shows limited SSH/SFTP logging depth. - Augmentation patterns (F5) align with session mediation, key injection, and protocol-aware containment.

==

MATRIX 2 — PARADIGM ALIGNMENT + GOVERNANCE CONTROL COVERAGE

Paradigm Vendor Example Governance Controls Delivered

Network Enforcement Cisco AC-4 (Info Flow Enforcement), SC-7 (Boundary Protection), Segmentation & adjacency reduction

Edge Abstraction Cloudflare SC-7 Boundary Protection, Centralized ingress governance, Edge inspection for web/API

Identity Brokerage Zscaler AC-2/AC-3 (Identity & Least Privilege), Session establishment governance, Reduced implicit trust

Service Augmentation F5 SC-8/SC-13 (Transmission Protection), AU-2/AU-12 (Audit Evidence), Protocol mediation + containment, Transaction validation overlays

Key takeaway:

Brokerage compresses unauthorized session establishment risk. Augmentation compresses unsafe service exposure risk.

The Exposure Governance Plane requires both governance workflow and mediation depth, especially in heterogeneous application estates.

==

End of Appendix