**Secure Direct Automation Access to DMZ Servers Aligned to FRB DMZ Policy**

**Purpose:**

This guide establishes the *compliant method* for enabling Ansible and VMware vRA automation platforms to access servers in the DMZ, in accordance with Federal Reserve DMZ policy and Cisco ACI micro-segmentation standards.

**1. Principles and Compliance**

* The DMZ is a **high-risk transition zone**; access must be tightly controlled and auditable (“deny by default”).
* No automation or orchestration tools are deployed in the DMZ; all automation originates from the secure internal zone.
* Access is only permitted via **explicit, minimal contracts** (Cisco ACI), in line with FRB DMZ policy prohibiting generic, broad, or open access.
* **No inbound flows** from DMZ to internal are allowed under any circumstance.
* **Separation of duties** is maintained; changes and access are reviewed and approved by Security Architecture.

**2. Network Segmentation & EPGs (ACI)**

* **Automation Tools (Ansible, vRA):**  
  Assigned to “Automation EPG” in the trusted/internal segment.
* **DMZ Target Servers:**  
  Assigned to “DMZ EPG” in the DMZ segment.
* No application or mediation services share hosts between zones.

**3. ACI Contract and Firewall Policy**

* **Create explicit ACI contract:**  
  Allow only necessary protocols—SSH (22/TCP), WinRM (5986/TCP), HTTPS (443/TCP)—from Automation EPG to DMZ EPG.
* **Restrict contracts** to the specific source IPs of automation systems; *wildcards or broad subnets are forbidden*.
* **No inbound DMZ-to-internal contract.**
* **All contract creation/changes require change control and Security review.**
* **All access is logged and monitored** per FRB policy.

**4. Automation Security Controls**

* **Key/certificate-based authentication only**; passwords are not allowed.
* Automation service accounts are least-privilege and specific to automation (never root/admin).
* Inventories and playbooks must be scoped only to required DMZ targets—never allow broad or wildcard targeting.
* **All credentials are managed securely** (Ansible Vault, vRA credential store); credentials must be rotated regularly.

**5. Logging, Monitoring, and Review**

* **Logging of all access and contract hits** between Automation and DMZ is required and reviewed regularly.
* Automation activity logs and credential access logs must be retained in accordance with FRB audit policy.
* **Change management and regular review** of EPG assignments and contracts is mandatory.

**6. Operational Checklist (FRB Policy)**

* Confirm EPG assignments (no co-residency of security and application services).
* Contract is explicit, minimal, and applied only as needed.
* No inbound contracts or flows from DMZ to internal.
* Source/destination in contract are specific and documented.
* All credentials are vaulted and rotated.
* All access and policy changes are logged and reviewed.
* No deviations without Security Architecture approval.

**Summary:**

This direct automation method enables secure, rapid access to DMZ resources **while maintaining full compliance with FRB DMZ policies**—including zero-trust, separation of duties, auditable access, and least-privilege design.  
**All exceptions or changes must be reviewed and approved by Security Architecture.**