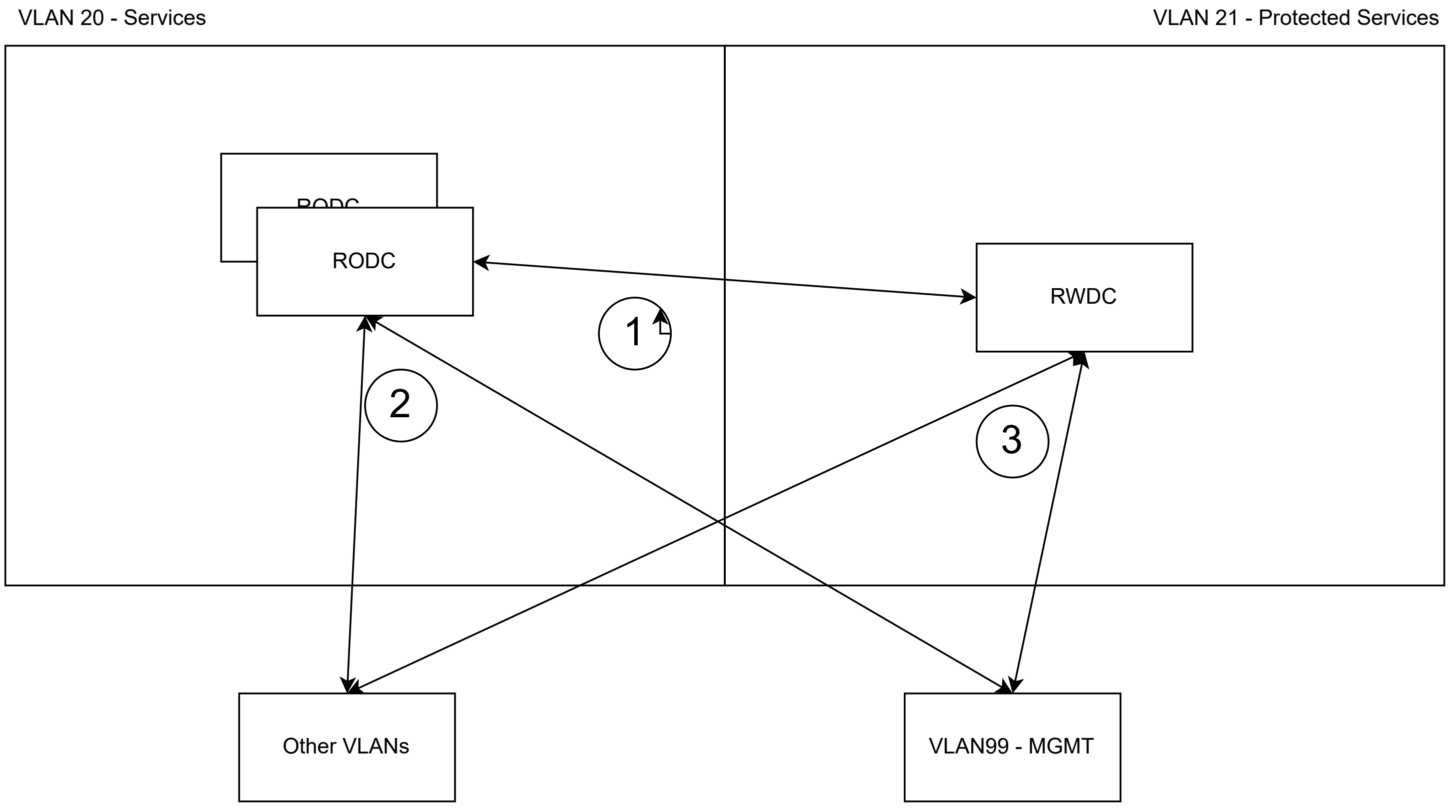
Identity Services Ecosystem Data Flows



Data Flows

ID	Port/Proto	Description	Controls
1	636/TCP 3269/TCP 88/TCP-UDP 53/TCP-UDP 135/TCP 49152-65535/TCP 445/TCP	Domain Controller Replication, including LDAPS, Global Catalog, Kerberos, DNS, and RPC control and data, and SMB.	Inter-VLAN traffic will be evaluated at the core firewall level, and restricted with Proxmox VM-level firewalls.
2	88/TCP-UDP 53/UDP 445/TCP	Read-Only operations, including Kerberos, DNS lookups, and GPO downloads.	SRV record weights preference all hosts to RODCs for all operations, which refer write operations to WDCs. Site segmentation also ensures DC Locator will locate RODCs first in all cases except for the Protected Services VLAN. Inter-VLAN traffic will be evaluated at the core firewall level and restricted with Proxmox VM-level firewalls.
3	88/TCP-UDP 53/UDP 445/TCP 5986/TCP	Must-Write operations and domain admin functions, including declarative specifications for the domain, users, and groups, as well as adhoc changes included Group Managed Service Accounts (gMSAs).	SRV record weights preference all hosts to RODCs for all operations, which refer write operations to WDCs. Site segmentation also ensures DC Locator will locate RODCs first in all cases except for the Protected Services VLAN. Inter-VLAN traffic will be evaluated at the core firewall level and restricted with Proxmox VM-level firewalls.

Active Directory Site Architecture				
ID	Site Name	Subnets	DC Type	Description
1	Protected-Core	10.0.21.0/24	W	Only the protected services get direct access to the WDCs via DC Locator. This IP Space correlates with the Core physical site.
2	Primary-Core	10.0.20.0/24 10.0.40.0/24 10.0.99.0/24	RO	The Primary set of IP spaces at the Core Physical Site, associated with the RODCs at the Core site.
3	DMZ-Core	10.0.30.0/24	RO	The DMZ at the Core physical site.

Must-Write Use Cases			
ID	Application	Function	Description

Version/Date: v1.0 / 11 AUG 2025
Scope: Identity Services Ecosystem Architectural Diagrams
https://github.com/integrateddefense/lab_infra