Week 5: Software-Defined Networking (SDN)

NT524 — Cloud Architecture and Security

PhD. Nguyen Ngoc Tu

October 8, 2025

Learning Objectives (Mục tiêu)

- **Architect cloud SDN:** map control/data planes to real fabrics (Neutron/OVN, AWS VPC, Azure VNet, GCP VPC).
- **Secure by design:** enforce least-privilege microsegmentation & QoS for east–west risk reduction.
- **Network-as-Code (IaC/GitOps):** lint/test/stage/canary/rollback with policy-as-code guardrails (OPA/Conftest).
- **Operate securely:** harden controllers (mTLS/RBAC/audit), integrate SOC→SDN, collect evidence (flow logs, traces).
- **Implement on OpenStack/OVN with Ansible:** network/subnet, SG chaining, address-sets/ACL, QoS; validate with `ovn-trace`/`iperf3`.

Thuật ngữ: control plane = *mặt phẳng điều khiển*; data plane = *mặt phẳng dữ liệu*; overlay SDN = *mạng phủ*; microsegmentation = *phân đoạn vi mô*; QoS = *chất lượng dịch vụ*; policy-as-code = *chính sách như mã*; IaC = *hạ tầng như mã*; GitOps = *quy trình vận hành dựa trên Git*; RBAC = *kiểm soát truy cập theo vai trò*

Motivation (Động lực)

- **Architecture:** control/data plane separation; overlay SDN (VXLAN/Geneve); logical routers/NAT; service insertion — mapped to OpenStack Neutron/OVN, AWS VPC, Azure VNet, GCP VPC.
- **Strong multi-tenant isolation:** per-tenant overlays; SG/NSG/DFW microsegmentation; address-sets; strict project/tenant boundaries.
- **Multi-cloud & hybrid consistency:** federated policy/routing (Transit Gateway, ExpressRoute, Cloud Router, EVPN); shared tags/identity; IaC modules to prevent drift.
- **Velocity with safety (IaC/GitOps):** lint → test → stage → canary → rollback, guarded by policy-as-code (OPA/Conftest).
- **Observability, forensics & resilience:** flow logs; `ovn-trace`; packet mirroring; controller hardening (mTLS/RBAC/audit); HA; QoS for blast-radius control.

Thuật ngữ: overlay SDN = *mạng phủ*; logical router = *bộ định tuyến logic*; NAT = *biên dịch địa chỉ mạng*; service insertion = *chèn dịch vụ*; SG/NSG/DFW = *nhóm bảo mật / nhóm bảo mật mạng / tường lửa phân tán*; address-set = *tập địa chỉ*; Transit Gateway/ExpressRoute/Cloud Router/EVPN = *dịch vụ kết nối liên vùng/liên đám mây*; HA = *sẵn sàng cao*

Outline

1. Cloud SDN Big Picture
2. Cloud SDN Architecture
3. Cloud SDN Operations
4. Cloud SDN: Security challenges and perspective
5. Cloud SDN Platforms
6. Hands-on
7. Appendix

Virtual Network Overview (Recap)

- **Model: vNIC → Port → Subnet → Router → Network**; provider networks for direct external reach.
- **Underlay vs Overlay:** L3 IP fabric transports tenant overlays; MTU/PMTUD validation required for encapsulation headers.
- **Services:** DHCP, metadata, L3 routing/NAT; distributed L3 for scale and locality.
- **Encapsulation practice:** Geneve/VXLAN overlays; Geneve carries rich key/value metadata for policy.
- **Ops pattern:** drift-free config via IaC; path tests (`ping`/`tracepath`), `ovn-trace` for logic, flow logs for evidence.

Thuật ngữ: vNIC = *card mạng ảo*; Port = *cổng logic*; Subnet = *mạng con*; underlay/overlay = *mạng vật lý/ mạng phủ ảo*; MTU/PMTUD = *kích thước gói tối đa/phát hiện MTU theo đường*; distributed L3 = *định tuyến phân tán*; Geneve/VXLAN = *đóng gói tầng phủ*

Cloud SDN Big Picture — Architecture

- **Tenants:** isolated logical switches/routers; per-tenant NAT and service insertion across VPC/VNet projects.
- **Planes:** control plane (intent, policy, topology) $\leftrightarrow$ data plane (forwarding, enforcement).
- **Overlays:** Geneve/VXLAN over L3 underlay; distributed L3 & NAT for scale and locality.
- **Policy layers:** SG/NSG/DFW on ports; NACLs at subnets/edges; QoS shaping/policing.
- **Targeting:** address-sets/tags/ASGs for dynamic grouping and least-privilege rules.
- **Connectivity:** IGW/LB for ingress; NAT GW/egress policies; transit/peering for hub-and-spoke.

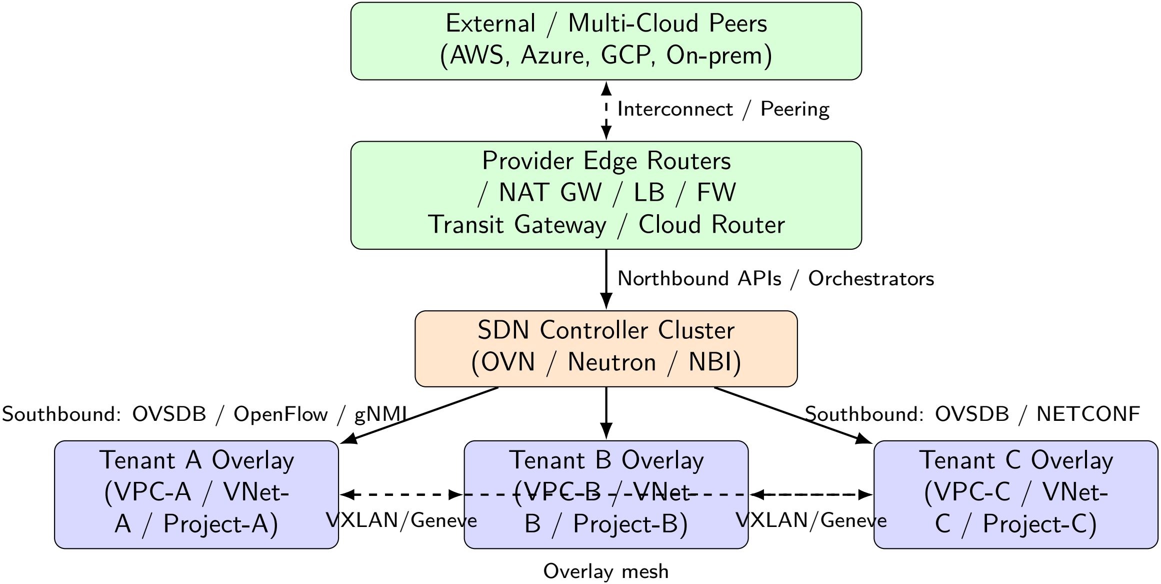
Thuật ngữ: tenant = *bên thuê*; control/data plane = *mặt phẳng điều khiển/dữ liệu*; overlay = *mạng phủ ảo*; distributed L3/NAT = *định tuyến/NAT phân tán*; SG/NSG/DFW = *nhóm bảo mật / nhóm bảo mật mạng / tường lửa phân tán*; NACL = *danh sách kiểm soát mạng*; QoS = *chất lượng dịch vụ*; address-set/tag/ASG = *tập địa chỉ/nhãn/nhóm bảo mật ứng dụng*; IGW/LB/NAT GW = *cổng Internet/cân bằng tải/cổng NAT*; transit/peering = *kết nối trung chuyển/kết nối ngang hàng*

Cloud SDN Big Picture — Operations & Platforms

- **Controller role:** single source of truth; northbound APIs for orchestration; southbound protocols for programming datapaths.
- **Multi-account/org:** hierarchical policy and shared services across accounts/subscriptions/projects.
- **IaC pipeline:** lint → test → stage → canary → rollback; policy-as-code guardrails (OPA/Conftest).
- **Observability:** flow logs, `ovn-trace`, packet mirroring; SIEM integration for evidence & forensics.
- **Threat response:** SOC→SDN automation for dynamic containment and least-blast-radius changes.
- **Platform mapping:** OpenStack (Neutron/OVN), AWS VPC (+ VPC Lattice), Azure VNet (+ Virtual Network Manager), GCP VPC (+ Hierarchical Firewalls).

Thuật ngữ: northbound/southbound = *giao diện hướng bắc/nam*; single source of truth = *nguồn dữ liệu tin cậy nhất*; hierarchical policy = *chính sách phân cấp*; IaC = *Triển khai và vận hành hạ tầng dưới dạng mã*; policy-as-code = *Triển khai và vận hành chính sách dưới dạng mã*; SIEM = *hệ thống quản lý thông tin và sự kiện bảo mật*; containment = *khoanh vùng*; VPC/VNet = *đám mây riêng ảo/mạng ảo*

Cloud SDN Big Picture — Control & Overlay Planes


External / Multi-Cloud Peers
(AWS, Azure, GCP, On-prem)
Interconnect / Peering
Provider Edge Routers
/ NAT GW / LB / FW
Transit Gateway / Cloud Router
Northbound APIs / Orchestrators
SDN Controller Cluster
(OVN / Neutron / NBI)
Southbound: OVSDB / OpenFlow / gNMI
Southbound: OVSDB / NETCONF
Tenant A Overlay
(VPC-A / VNet-A / Project-A)
VXLAN/Geneve
Tenant B Overlay
(VPC-B / VNet-B / Project-B)
VXLAN/Geneve
Tenant C Overlay
(VPC-C / VNet-C / Project-C)
Overlay mesh

Data Plane — packet-by-packet handling (1/2)

Function	AWS	Azure	GCP	OpenStack (Kolla/OVN/OVS)	Kubernetes (CNI)	VMware NSX-T
Compute vNIC & host fastpath	ENA vNIC, Nitro datapath	Accelerated Networking (Mellanox), vSwitch fastpath	gVNIC, Andromeda fastpath	virtio-net / SR-IOV vNIC; OVS kernel or OVS-DPDK datapath	CNI fastpath (TC/BPF, OVS, SR-IOV)	N-VDS / ESXi vSwitch fastpath
L2/L3 switching & routing	VPC datapath (Nitro)	VNet datapath	VPC datapath	`br-int`/`br-ex` (OVS); OVN logical pipeline → OVS flows	Plugin datapaths (Calico BPF, Cilium BPF, OVN-K, Flannel VXLAN)	DFW/LR fastpath on hosts/Edges
NAT (SNAT/DNAT)	NAT Gateway, instance NAT	NAT Gateway	Cloud NAT	qrouter namespaces (iptables/nft); OVN NAT in logical pipeline	CNI NAT (iptables/nft/BPF); Cilium/Calico egress/NAT	T0/T1 Edge NAT datapath

Note: “Data plane” = path touching **every packet** (forward/NAT/filter/LB).

Data Plane — packet-by-packet handling (2/2)

Function	**AWS**	**Azure**	**GCP**	**OpenStack (Kolla/OVN/OVS)**	**Kubernetes (CNI)**	**VMware NSX-T**
Security filtering	SG/NACL fastpath	NSG fastpath	VPC firewall datapath	SG→iptables/nft on tap/qbr; OVN ACLs→OVS flows	NetworkPolicies (Calico/Cilium BPF, iptables/nft)	DFW (distributed firewall) fastpath
Overlay encapsulation	VPC overlays (Geneve/VXLAN)	VNet overlays	Andromeda overlays	Geneve (OVN), VXLAN (OVS)	VXLAN/Geneve /WireGuard (plugin-dependent)	Geneve
L4/L7 load balancing	NLB/ALB datapath	SLB datapath	GLB/ILB datapath	Octavia amphora/OVN LB (OVS-based), HAProxy datapath	kube-proxy (IPVS/iptables) or Cilium LB/BPF, MetalLB	NSX LB datapath

Thuật ngữ: Overlay = *mạng chồng*; ACL = *danh sách kiểm soát truy cập*.

Hint: For proofs, capture `nft list ruleset`, `ovs-ofctl dump-flows`, `ovn-trace`, and pcap samples

Control Plane — programs the datapath (1/2)

Function	**AWS**	**Azure**	**GCP**	**OpenStack (Kolla/OVN/OVS)**	**Kubernetes (CNI)**	**VMware NSX-T**
API & orchestration	EC2/VPC APIs, CloudFormation	ARM (Azure Resource Manager), REST	GCE/GKE APIs, Deployment Manager	Keystone (auth), Nova, Neutron-server, Glance, Cinder	kube-apiserver, controllers, scheduler	NSX Manager / Policy API
Network controller	VPC control plane (programs Nitro)	VNet control plane	Andromeda control plane	OVN northd + NB/SB DB, ovn-controller; Neutron L3/DHCP/Metadata agents	CNI controllers/-daemons (Calico, Cilium, OVN-K)	NSX Central Control Cluster
LB control	ELB/ALB/NLB control plane	Azure LB controller	GCLB controllers	Octavia API/-Worker/Health-Mgr	Cloud Controller Manager & Ingress/LB controllers	NSX LB control

Note: Control-plane processes **install** state but do not forward packets.

Thuật ngữ: Control plane = *mặt phẳng điều khiển*; Orchestration = *điều phối*

Control Plane — programs the datapath (2/2)

Function	**AWS**	**Azure**	**GCP**	**OpenStack (Kolla/OVN/OVS)**	**Kubernetes (CNI)**	**VMware NSX-T**
Policy & SG programming	SG/NACL managers	NSG manager	Firewall policy manager	Neutron SG driver → iptables/nft or OVN ACL	NetworkPolicy controllers in plugin	DFW policy controller
Image/metadata services	SSM, IMDS	IMDS	IMDS	Nova metadata service; Neutron metadata-proxy	Cloud-init via user-data; cloud-provider IMDS	vSphere/guest tools, NSX metadata

Hint: Validate control health with `docker logs` (OpenStack), `k get pods -A` (K8s), NSX Manager status, and cloud API `describe` calls.

Thuật ngữ: Security Group = *nhóm bảo mật*; Metadata = *siêu dữ liệu*.

Traditional vs. SDN — Design & Delivery (1/2)

Khía cạnh	Truyền thống	SDN Datapath / Edges	SDN Controller (Control Plane)
Provisioning	CLI, ticket	API/IaC self-service qua orchestrator	NBI nhận *intent* → lập kế hoạch → áp dụng trạng thái
Isolation	VLAN, ACL tại thiết bị	Overlay per-tenant; SG/DFW tại cổng	Quản lý tenant/namespace, tag/ASG; mẫu *policy* dùng lại
Change	Cửa sổ bảo trì, ít kiểm thử	Pipeline: lint/test/canary/rollback	*Policy-as-code* (OPA/Conftest) làm *gate*; giao dịch & rollback nguyên khối
Scale	Phụ thuộc phần cứng	Scale-out host/switch; distributed L3/NAT	Cụm controller/DB HA; reconciliation loop, incremental updates

Thuật ngữ: NBI = *giao diện hướng bắc*; SG/DFW = *nhóm bảo mật/tường lửa phân tán*; distributed L3/NAT = *định tuyến/NAT phân tán*; HA = *sẵn sàng cao*; reconciliation = *đồng bộ hoá*

Traditional vs. SDN — Operate & Assure (2/2)

Khía cạnh	Truyền thống	SDN Datapath / Edges	SDN Controller (Control Plane)
Observability	SNMP, syslog rời rạc	Flow logs, mirror/pcap, `ovn-trace`	Audit API; ánh xạ *intent* → state; topo & diff theo commit
Security	Trust theo vị trí; ACL rải rác	Default-deny SG/NSG/DFW; egress control	mTLS, RBAC/SoD; cô lập management plane; rate-limit API
Resilience	Failover thủ công trên thiết bị	ECMP, health-check; NAT/LB dự phòng	Cluster quorum/replication; tự đồng bộ sau sự cố
Compliance	Bằng chứng thủ công	Log/pcap gắn sự kiện thay đổi	Gắn chứng cứ vào PR/ticket; chuẩn hoá *retention* & *lineage*

Thuật ngữ: RBAC/SoD = *vai trò/phân tách nhiệm vụ*; ECMP = *đa đường chi phí bằng nhau*; lineage = *chuỗi nguồn gốc*; retention = *lưu giữ*

Network Programmability (Software-defined)

- **Intent → State:** declare desired topology/policy; controllers *reconcile* actual state to intent (NB↔SB).
- **Model-driven:** REST/JSON + YANG/gNMI; Neutron/OVN NB as authoritative data models; tags/ASGs for dynamic targeting.
- **Programmable datapaths:** OVS (OpenFlow/OVN flows), eBPF/XDP, DPDK fastpath, SR-IOV bypass; selective offload to SmartNIC/DPU.
- **Policy-as-code:** SG/NSG/DFW, QoS, address-sets, L7 intents; OPA/Conftest gates for risky rules & required metadata.
- **Northbound APIs:** Neutron (REST), OVN NB (`ovn-nbctl`/IDL), cloud APIs (VPC/VNet), K8s CRDs for network policy.
- **Southbound protocols:** OVSDB (config/state), OpenFlow/OVN pipeline, NETCONF/gNMI for device domains.
- **Observability hooks:** flow logs, `ovn-trace`, IPFIX/sFlow; embed commit IDs for provenance.

Thuật ngữ: intent = *ý định cấu hình*; reconcile = *đồng bộ trạng thái*; NB/SB = *hướng bắc/nam*; YANG = *mô hình dữ liệu*; CRD = *định nghĩa tài nguyên tuỳ biến*; provenance = *nguồn gốc*

Programmability Lifecycle & Safety

- **Author:** IaC + policy-as-code (networks, SGs, QoS, routes) with templates & tags.
- **Validate:** schema lint, *conftest* (OPA) policies, `-check`/dry-run, shadow rules.
- **Deliver:** CI/CD pipeline → plan → stage → canary → progressive rollout.
- **Guardrails:** invariants (default deny, no 0.0.0.0/0 on DB/SSH), blast-radius caps, rate-limited API.
- **Close the loop:** compare intent vs. live; auto-reconcile drift; rollback on SLO breach.
- **Evidence:** attach `ovn-trace`, flow logs, and diffs to PR/tickets for audit.

Thuật ngữ: IaC = *Triển khai và vận hành hạ tầng dựa trên mã*; shadow rule = *luật thử*; canary = *triển khai thăm dò*; invariant = *bất biến an toàn*; drift = *sai lệch*; SLO (Service Level Objective) = *mục tiêu mức dịch vụ*

Cloud SDN Architecture: Scope and Principles

- Scope: tenant logical networks over L3 IP fabric; SDN controller programs data-plane state.
- Principles: intent-driven policy; separation of concerns (control vs data); least privilege by default.
- Resilience: distributed routing/NAT; failure domains; HA controllers; blast-radius control.
- Portability: overlay decouples tenant topology from underlay; consistent abstractions across clouds.
- Evidence-first: every change is auditable; path proofs and flow traces accompany rollouts.

Thuật ngữ: intent-driven = *dựa trên ý định*; control/data plane = *mặt phẳng điều khiển/dữ liệu*; failure domain = *miền lỗi*; blast radius = *phạm vi ảnh hưởng*; overlay/underlay = *mạng phủ/mạng nền*

Cloud SDN Architecture: Tenant Logical Networking

- Core objects: networks, subnets, ports, logical routers, floating IPs, SG/NSG/DFW.
- Addressing: per-tenant CIDR plans; overlapping RFC1918 across tenants via overlays/NAT.
- Namespacing: project/tenant isolation boundaries; quotas for ports/FIPs/routes.
- Exposure patterns: east–west private; north–south via LB/IGW; egress via NAT GW.
- Day-0/1 baselines: default-deny SG; mandatory egress control; DHCP/metadata reachability.

Thuật ngữ: tenant = *thuê bao*; CIDR = *khối địa chỉ*; floating IP = *địa chỉ IP nổi*; SG/NSG/DFW = *nhóm bảo mật/nhóm bảo mật mạng/tường lửa phân tán*; IGW/NAT GW = *cổng Internet/cổng NAT*

Cloud SDN Architecture: Overlay Encapsulation and MTU

- Encapsulation: Geneve/VXLAN tunnels between hypervisors; payload carries tenant frames.
- Metadata: Geneve TLVs embed policy context (group, app, zone) for smart enforcement.
- MTU planning: account for tunnel headers; enable PMTUD; validate with `tracepath`/ICMP.
- NIC offloads: GRO/GSO/TSO affect throughput/latency; align with overlay MTU.
- Interop: provider networks for direct underlay access (bypass overlay when required).

Thuật ngữ: Geneve/VXLAN = *đóng gói tầng phủ*; TLV = *kiểu-độ dài-giá trị*; MTU/PMTUD = *kích thước gói tối đa/phát hiện MTU theo đường*; offload = *tăng tốc phần cứng*; provider network = *mạng nhà cung cấp*

Cloud SDN Architecture: Control Plane (Intent and Policy)

- Responsibilities: API, authN/Z, IPAM/DHCP, routing/NAT intent, policy objects, quotas.
- Data model: northbound DB for intent; southbound DB/flows for realized state.
- Interfaces: OVSDB for config/state; OpenFlow/OVN flows; NETCONF/gNMI for device domains.
- Safety: RBAC/SoD; change approvals; rate-limited controllers; mgmt-plane isolation.
- HA/DR: clustered controllers; DB replication; deterministic reconciliation on restart.

Thuật ngữ: authN/Z = *xác thực/ủy quyền*; IPAM = *quản lý địa chỉ IP*; OVSDB = *CSDL cấu hình OVS*; OpenFlow = *lập trình luồng*; RBAC/SoD = *kiểm soát vai trò/phân tách nhiệm vụ*; reconciliation = *đồng bộ hoá trạng thái*

Cloud SDN Architecture: Data Plane (Forwarding and Enforcement)

- Datapaths: OVS kernel datapath; options include DPDK/eBPF/XDP/SR-IOV for specialized performance.
- Bridges: `br-int` (logical L2), `br-ex` (egress), `br-tun` (tunnel termination).
- Enforcement points: conntrack state; per-port SG/DFW ACLs; QoS shaping/policing; NAT at logical routers.
- Scale knobs: CPU pinning/NUMA; RSS queues; offload policy on NICs; flow table sizing.
- Telemetry: `ovn-trace`, `ovs-ofctl dump-flows`, sFlow/IPFIX to SIEM.

Thuật ngữ: OVS = *Open vSwitch*; DPDK = *bộ công cụ xử lý dữ liệu*; eBPF/XDP = *xử lý gói trong nhân*; SR-IOV = *ảo hoá I/O đơn gốc*; conntrack = *theo dõi kết nối*; IPFIX = *luồng IP*

Cloud SDN Architecture: Distributed L3 and NAT

- Model: per-host logical routing pipeline; flows push L3 decisions to edges for locality.
- Benefits: fewer centralized chokepoints; better east–west latency; scale-out egress.
- NAT variants: SNAT/DNAT; floating IP; (optionally) stateless egress for high throughput edges.
- Asymmetry risks: return-path blocks by SG/NACL; ensure symmetric policies and ECMP awareness.
- Edge nodes: dedicated NAT/LB nodes for high-bandwidth tenants; health-checked failover.

Thuật ngữ: distributed routing = *định tuyến phân tán*; SNAT/DNAT = *dịch nguồn/đích*; floating IP = *IP nổi*; asymmetry = *bất đối xứng*; ECMP = *đa đường chi phí bằng nhau*

Cloud SDN Architecture: Service Insertion Patterns

- Ingress: L7/L4 load balancers terminate TLS; WAF before app tiers; policy per listener.
- East–west chain: DFW at vNIC → IDS/IPS mirror → app firewall → telemetry.
- Egress: NAT GW with egress ACLs; URL/IP category controls; rate limits and quotas.
- Bypass modes: provider networks or SR-IOV for appliances needing line-rate and fixed addressing.
- Observability: span/mirror logical ports; packet capture on `br-int` for forensic trails.

Thuật ngữ: WAF = *tường lửa ứng dụng web*; IDS/IPS = *phát hiện/ngăn chặn xâm nhập*; listener = *điểm lắng nghe*; span/mirror = *sao chép lưu lượng*

Cloud SDN Architecture: Segmentation and Isolation Models

- Microsegmentation: tiered SG/NSG/DFW (web→app→db) with default-deny posture.
- Edge segmentation: NACLs for subnet/edge stateless rules; summarized deny-lists at borders.
- Identity-aware policy: address-sets/tags/ASGs for dynamic groups; time-bounded changes via CI/CD.
- East–west controls: explicit return-path rule sets; ICMP allowance for PMTUD and diagnostics.
- Assurance: rule logging; path tests; flow-level evidence attached to change tickets.

Thuật ngữ: microsegmentation = *phân đoạn vi mô*; default deny = *mặc định từ chối*; NACL = *danh sách kiểm soát mạng*; ASG = *nhóm bảo mật ứng dụng*; diagnostics = *chẩn đoán*

Cloud SDN Architecture: VRFs, Route Domains and Interconnect

- Per-tenant VRF/route domain: isolated RIB/FIB; overlapping prefixes permitted.
- Shared services: hub VRF exposes limited services via export/import route policies.
- Inter-tenant flows: firewall + NAT at transit; service-to-service via mesh or private endpoints.
- Hybrid: EVPN/VXLAN fabrics connect to cloud via TGW/ExpressRoute/Cloud Router with route filters.
- Guardrails: prevent route leaks; max-prefix and as-path filters; blackhole for bogons.

Thuật ngữ: VRF = *bảng định tuyến ảo*; RIB/FIB = *bảng thông tin/tuyến chuyển tiếp*; EVPN = *mạng riêng ảo Ethernet*; TGW = *Transit Gateway*; route leak = *rò rỉ định tuyến*; bogon = *địa chỉ không hợp lệ*

Cloud SDN Architecture: Path Validation and Evidence

- **Path-of-intent**: verify service chains and return paths (ICMP/PMTUD allowed where needed).
- **Flow reasoning**: use `ovn-trace` to simulate logical pipeline decisions before rollout.
- **Data-plane truth**: inspect `ovs-ofctl dump-flows` on `br-int`/`br-tun` for enforcement.
- **Evidence bundle**: include path tests, flow traces, and rule logs in change tickets.
- **Regression safety**: canary a subset of ports/tenants; auto-rollback on SLO breach.

Thuật ngữ: path-of-intent = *đường đi theo ý định*; logical pipeline = *chuỗi xử lý logic*; enforcement = *thi hành chính sách*; evidence = *bằng chứng*; canary = *triển khai thăm dò*

Cloud SDN Operations: Network-as-Code Foundations

- Treat network intent as source code: version-controlled, peer-reviewed, and linted before deployment.
- Declarative IaC: desired state described in YAML/JSON; controller enforces convergence.
- Change management: PR→test→stage→approve→apply; every diff audited.
- Rollback readiness: immutable history and tagged releases.
- Evidence: merge commit links to topology diffs and path validations.

Thuật ngữ: Network-as-Code = *Triển khai và quản lý mạng bằng mã*; IaC = *triển khai và quản lý hạ tầng bằng mã*; declarative = *Khai báo trạng thái*; convergence = *hội tụ cấu hình*; rollback = *hoàn tác (khôi phục cấu hình trước)*

Cloud SDN Operations: Controllers as Single Source of Truth

- Controller databases (Neutron/OVN NB–SB DB) define the authoritative network state.
- APIs and automation agents reconcile actual vs. intended state periodically.
- Drift detection: periodic `ovn-nbctl show` vs live flows; GitOps diff pipelines.
- Audit integration: signed transactions, traceable to user identity and change request.
- External sync: export intent to CMDBs and inventory tools for enterprise visibility.

Thuật ngữ: single source of truth = *Nguồn cấu hình chuẩn duy nhất*; drift detection = *phát hiện sai lệch*; reconciliation loop = *vòng đồng bộ trạng thái*; CMDB(Configuration Management Database) = *cơ sở dữ liệu cấu hình*

Cloud SDN Operations: CI/CD for Network Configuration

- **CI (validate intent):** schema & YAML lint (Terraform/OpenTofu, Pulumi, Ansible), policy tests (OPA/Conftest, Sentinel), dry-run/plan (`terraform plan`, `ansible --check`, `ovn-trace` proofs).
- **CD (deliver safely):** push-based (Ansible/AWX, Terraform/Pulumi Cloud, Azure DevOps, Jenkins) *v.s.* pull-based (Argo CD/Flux) for controller state.
- **Promotion:** dev → stage → prod with approvals (Jira/ServiceNow), change windows, and rate-limited rollout.
- **Progressive strategies:** canary/blue–green tenants, feature/policy toggles, blast-radius caps, auto-rollback on SLO breach.
- **Ephemeral envs:** short-lived sandboxes (stack leases) + automated teardown to prevent config sprawl & stale state.
- **Drift & reconcile:** detect drift against controller/Cloud APIs; reconcile or fail the pipeline with evidence attached.
- **Metrics (DORA+):** lead time / change failure rate / MTTR / rollback count; policy-violation rate as a quality signal.
- **Provenance:** sign plans/artifacts (Sigstore/cosign), embed build/commit IDs in controller audit logs.

Cloud SDN Operations: IaC / Ops Workflow in Practice

- **Source of intent:** declarative IaC stored in SCM (Git, Mercurial, Azure Repos) *or* IaC SaaS (Terraform/OpenTofu Cloud, Pulumi Cloud, Ansible Automation Platform).
- **Pipelines:** GitHub Actions, GitLab CI, Jenkins, Azure DevOps, AWS CodePipeline; *pull-based* CD with Argo CD / Flux; PR-driven runners (Spacelift, Atlantis).
- **Plan & drift:** plan/diff vs. controller intent (OVN NB/Neutron) and cloud APIs; state backends (S3+DynamoDB, Consul, TF Cloud) with drift detection & auto-reconcile.
- **Policy gates:** OPA/Conftest; HashiCorp Sentinel; cloud guardrails (AWS Config/Control Tower, Azure Policy, GCP Org Policy/Hierarchical Firewall).
- **Progressive delivery:** stage → canary → progressive rollout; rate-limit & blast-radius caps; auto-rollback on SLO breach.
- **Provenance & supply chain:** signed artifacts (Sigstore/cosign), SBOM, SLSA levels; embed build/commit IDs into controller audit for *provenance*.
- **Evidence & observability:** attach `ovn-trace`, flow logs, plan diffs to PR/tickets; export events/metrics to SIEM.

Thuật ngữ: SCM = *quản lý mã nguồn*; pull-based CD = *triển khai do cụm kéo*; drift = *sai lệch*; SLO = *mục tiêu mức dịch vụ*; SBOM = *danh mục thành phần phần mềm*; SLSA = *mức bảo đảm chuỗi cung ứng*

Cloud SDN Operations: Policy-as-Code Guardrails — Design and Enforcement

- **Author & Scope:** Rego policies define allowed/denied configurations for networks, SG/NSG/DFW, QoS, NAT, routes, tags, and ownership.
- **Execution stages:**
  - *Pre-commit:* Conftest checks IaC before merge.
  - *CI/Plan:* diff validation; block unsafe plans.
  - *Admission:* OPA sidecar/webhook rejects non-compliant API calls.
  - *Runtime:* drift monitor re-evaluates live vs. intended state.
- **Cross-ecosystem integration:** Sentinel (Terraform/OpenTofu), Azure Policy, AWS Config/Control Tower, GCP Org Policy / Hierarchical Firewall.
- **Risk patterns (examples):** deny 0.0.0.0/0 on SSH / DB; enforce default-deny; tag validation; QoS min/max limits.
- **Outcome:** deterministic enforcement before deployment, preventing security drift.

Thuật ngữ: Rego = *ngôn ngữ chính sách OPA*; admission webhook = *điểm kiểm soát trước khi áp dụng*; Sentinel/Azure Policy . . . = *các khung chính sách đám mây*; drift = *sai lệch trạng thái*

Cloud SDN Operations: Policy-as-Code Guardrails — Operations and Governance

- **Exception handling:** time-boxed *waivers* with ticket ID, approver, expiry, and auto-revert; logged to PR / change record.
- **Performance & scale:** partial evaluation + data bundles; centralized OPA with distributed cache; batched decision logs → SIEM.
- **Policy registry:** versioned repository / artifact store (S3, Git, OCI registry); signed bundles (Sigstore/cosign); automatic sync to controllers.
- **Provenance & audit:** embed policy pack ID + commit hash in controller audit logs; export decision events for compliance evidence.
- **Metrics & feedback:**
  - Policy coverage (% plans checked)
  - Waiver count / mean waiver duration
  - Policy evaluation latency & cache hit ratio
- **Outcome:** measurable, auditable policy lifecycle with continuous improvement loop.

Thuật ngữ: waiver = *ngoại lệ có thời hạn*; partial evaluation = *đánh giá trước một phần*; provenance = *nguồn gốc cấu hình*; SIEM = *hệ thống giám sát sự kiện bảo mật*

Cloud SDN Operations: Closed-Loop Enforcement — Detection and Response

- **Detect → Decide:** SIEM/XDR/IDS raises IOC (IP, domain, JA3, tag). ML/rule engine defines *action* (quarantine, deny, throttle) and *scope* (tenant, SG, port, address-set).
- **Automated Act:** controller programs mitigation via southbound APIs:
  - insert deny ACL / SG rule or update OVN address-set;
  - apply QoS throttle or blackhole route;
  - isolate compromised port, VM, or container namespace.
- **Safeguards:** TTL on temporary rules; idempotent changes; API rate-limit; approval tiers for high-impact scopes.
- **Verification:** controller confirms state; synthetic probes / `ovn-trace` validate blockage; flow logs show hit counters; incident ticket auto-updates with change hash.

Thuật ngữ: IOC = *chỉ báo xâm nhập*; SG = *nhóm bảo mật*; ACL = *danh sách kiểm soát truy cập*; QoS = *chất lượng dịch vụ*; TTL = *thời hạn*; idempotent = *lặp lại không đổi*

Cloud SDN Operations: Closed-Loop Enforcement — Governance and Resilience

- **Rollback & expiry:** automatic removal on TTL or incident close; maintain allowlist for false positives; restore prior policy snapshot.
- **Audit & evidence:** attach controller logs, `ovn-trace` outputs, and change diffs to SOC case; sign events (Sigstore/cosign) for provenance.
- **Learning loop:** feed metrics (detection→action latency, FP rate, rollback count) to tuning pipeline; reinforce OPA/Conftest guardrails with new indicators.
- **Platform mapping:** OVN ACL + address-set, AWS NFW/SG, Azure Firewall/NSG Admin Rules, GCP Hierarchical Firewall, K8s NetworkPolicy controllers.
- **Resilience drills:** simulate IOCs in digital twin (staging SDN/K8s); chaos test controller API saturation; verify rollback safety under load.
- **Outcome:** provable mean-time-to-containment reduction, minimal blast radius, and traceable evidence chain across SOC ↔ SDN boundary.

Thuật ngữ: provenance = *nguồn gốc cấu hình*; FP = *dương tính giả*; chaos test = *kiểm thử hỗn loạn*; blast radius = *phạm vi ảnh hưởng*; digital twin = *mô phỏng ảo song song*

Cloud SDN Operations: Observability & Flow-Log Pipeline — Sources and Architecture (1/2)

- **Sources (multi-layer):** OVN flow logs/IPFIX; `ovs-ofctl` counters; controller audit/events (Neutron/OVN NB); hypervisor/host (tc, conntrack, NIC stats); packet capture/ERSPAN; DNS/HTTP logs; cloud flow logs (AWS VPC, Azure NSG, GCP VPC); K8s (Hubble/Tetragon, kube-audit).
- **Normalization & enrichment:** add tenant/project, SG/NSG/DFW rule IDs, tags/labels, topology (port, LRP/LSP), change *commit ID*, rule priority, zone/region; redact PII; hash sensitive fields.
- **Transport (reliable):** Fluent Bit/Fluentd/Vector → Kafka/Kinesis/PubSub/OTLP; batching, compression, *backpressure*; schema registry (Avro/Protobuf).
- **Storage & tiering:** hot: OpenSearch/Elasticsearch/ClickHouse/BigQuery for 7–14d low-latency search; cold: S3/GCS with Object Lock or Glacier/Archive for $\geq$ 180d compliance.
- **Resilience & security:** at-least-once delivery, DLQ (dead-letter), replay windows; mTLS on agents, signed artifacts, access by least-privilege roles.

Thuật ngữ: IPFIX = *định dạng xuất lưu lượng*; OTLP = *giao thức Telemetry OpenTelemetry*; backpressure =

Cloud SDN Operations: Observability & Flow-Log Pipeline — Analytics, Forensics and Evidence (2/2)

- **Correlation:** join flows with tenant/project/user, SG/NSG rule IDs; build change timeline (PR/commit → policy → flows).
- **Operational analytics:** top talkers/ports, east–west vs egress mix, policy *hit/miss*, congestion & drop rates, latency heatmaps, MTU/PMTUD outliers.
- **Forensics:** `ovn-trace` to reproduce decisions; differential path (before/after change); targeted PCAPs; session reconstruction; graph view of path through LRs/LBs/NATs.
- **Detections & guardrails:** default-deny violations, shadow rules, overly broad CIDRs, sudden egress to new ASNs; anomaly baselines with seasonal thresholds.
- **Evidence & compliance:** attach `ovn-trace` output, flow snippets, screenshots, and plan diffs to tickets; legal hold on cold tier; RBAC'd access; audit queries scripted.
- **SLOs & feedback:** MTTD/MTTC, change failure rate, rollback count; feed findings back to OPA/Conftest and QoS limits; refine sampling rates & retention by risk.

Thuật ngữ: hit/miss = *khớp/không khớp*; PMTUD = *khám phá MTU theo đường*; MTTD/MTTC = *thời gian phát hiện/khoanh vùng*; RBAC = *kiểm soát theo vai trò*

Cloud SDN Operations: High-Availability and Fault Domains — Control Plane (1/2)

- **Controller/DB clustering:** OVN NB/SB DB in Raft with *quorum*; northd/ovn-controller active–active; fenced leadership.
- **Transaction safety:** idempotent writes, bounded retries, SB backpressure; slow-follower eviction; schema-version guards.
- **Upgrade strategy:** rolling DB & northd upgrades; live schema migration; feature flags/dual-write; blue–green controllers for fast rollback.
- **Disaster recovery:** periodic snapshots, WAL shipping to object storage; tested RTO/RPO; region evacuation runbooks; PITR drills.
- **Control SLOs/alerts:** replication lag, leader churn, northd backlog, SB apply latency, reconcile loop duration; alert on quorum loss/split-brain.
- **Auditability:** leadership changes, failovers, policy freezes logged & signed; evidence attached to change tickets.

Thuật ngữ: HA = *sẵn sàng cao*; Raft = *thuật toán đồng thuận*; quorum = *tối thiểu thành viên đồng thuận*; WAL = *nhật ký ghi trước*; PITR = *khôi phục theo thời điểm*; RTO/RPO = *mục tiêu thời gian/phục hồi dữ liệu*

Cloud SDN Operations: High-Availability & Fault Domains — Datapath and Ops (2/2)

- **Datapath resilience:** ECMP paths; health-checked edges; BFD for fast failover; graceful restart; *per-tenant* NAT/LB redundancy with state sync (where supported).
- **Fault-domain design:** node → rack → AZ → region; avoid single-chassis choke points; place edges/controllers across FDs.
- **Plane isolation:** separate *management*, *control*, *data* networks; ACLs/RBAC on mgmt; rate-limit controller APIs.
- **Blast-radius control:** shard tenants by FD; cap concurrent changes; staged rollouts/change windows for high-impact scopes.
- **Ops signals:** flow install latency, edge health, drop/error counters, NAT/LB failover events; synthetic probes & `ovn-trace` gates pre-rollout.
- **Chaos & validation:** kill DB node / flap edge link / AZ drain in staging "digital twin"; verify rollback safety & policy continuity.

Thuật ngữ: ECMP = *đa đường chi phí bằng nhau*; BFD = *phát hiện lỗi nhanh*; FD = *miền lỗi*; RBAC = *kiểm soát theo vai trò*; synthetic probe = *kiểm thử giả lập*; blast radius = *phạm vi ảnh hưởng*

Cloud SDN Operations: Rollback Strategies — Design and Execution (1/2)

- **Immutable snapshots:** versioned controller DB (e.g., NB/SB), policy bundles, and IaC state (S3/TF Cloud/Consul) per release.
- **Transactional changes:** apply as atomic change-sets; fail fast and *rollback all* on error; verify schema compatibility before commit.
- **Progressive safety nets:** canary & blue–green controllers/tenants; feature flags, shadow rules, dual-write during migrations.
- **Rollback triggers:** SLO breach (latency/packet loss), guardrail violation (OPA/Conftest), health-check or flow-install latency spikes.
- **Restore procedures:** one-click/CLI restore of DB snapshot; idempotent re-apply of last good policy; state hashing to confirm parity post-restore.
- **Blast-radius control:** tenant/namespace-scoped rollbacks first; rate-limit large reversions; freeze high-risk policy during recovery.
- **Evidence chain:** link rollback to PR/Change ID; archive diffs, `ovn-trace` proofs, controller audit logs in the incident record.

Cloud SDN Operations: Drift Control — Detect and Reconcile (2/2)

- **Sources of drift:** emergency hotfixes, manual device edits, API partial failures, multi-cloud propagation lag, orphaned objects.
- **Detection:** scheduled plan/diff vs live (controller & cloud APIs); intent↔state checks; OVN NB vs. OVS/OpenFlow diffs; config checksums.
- **Auto-reconcile:** safely reapply intent for additive changes; quarantine unknown objects; require human approval for destructive diffs.
- **Stability guards:** exponential backoff, *circuit breaker* on flapping resources; rate-limit reconciles; per-tenant concurrency caps.
- **Governance:** drift alerts to SIEM; time-boxed waivers (TTL) with approver & reason; management-plane RBAC; change windows for high impact.
- **Metrics & learning:** drift rate, MTTD/MTTR, re-drift after fix,
- **Prevention:** policy-as-code invariants (default-deny, no 0.0.0.0/0 on DB/SSH), API admission checks, strong tagging/ownership rules.

Thuật ngữ: drift = *sai lệch trạng thái*; reconcile = *đồng bộ hoá*; circuit breaker = *ngắt mạch bảo vệ*; TTL = *thời hạn*; MTTD/MTTR = *thời gian phát hiện/phục hồi*; RBAC = *kiểm soát theo vai trò*

Operational Maturity Model (Level 0 → 4)

- **L0 Manual:** ad-hoc CLI changes; limited audit.
- **L1 Scripted:** task automation scripts; partial repeatability.
- **L2 Declarative:** IaC models, config repos, lint tests.
- **L3 GitOps:** CI/CD pipelines, policy-as-code, automated drift fix.
- **L4 Autonomous:** closed-loop SOC→SDN feedback; predictive scaling & self-healing.

Thuật ngữ: maturity model = *mô hình trưởng thành vận hành*; declarative = *khai báo mong muốn*; self-healing = *tự phục hồi sự cố*

Threat Landscape in Cloud SDN (2024–2025)

- Misconfig & identity risk dominate: exposed assets, weak identities, excessive trust paths.
- Multicloud attack paths: cross-account/project exposure chains to crown jewels are common.
- Data exposure persists: publicly reachable storage/services & leaked secrets increase breach blast radius.
- Shared responsibility gaps: provider controls exist, but tenant policy/ops maturity lags.
- Operational takeaway: make segmentation & identity controls default; prove with evidence on every change.

Thuật ngữ: misconfiguration = *cấu hình sai*; attack path = *đường tấn công*; blast radius = *phạm vi ảnh hưởng*; shared responsibility = *mô hình trách nhiệm chia sẻ*; crown jewels = *tài sản trọng yếu*

Control/Data Plane Risks & Hardening

- Control-plane CVEs: OVN BFD parsing can trigger cluster DoS; patch/disable unneeded BFD, restrict mgmt.
- Data-plane pitfalls: kernel/OVS bugs; conntrack exhaustion; asymmetric paths breaking return rules.
- Supply chain & APIs: dependency bugs, token leakage; enforce mTLS, short-lived creds, least-privilege RBAC.
- Hardening: management-plane isolation; rate limits; HA clusters; signed/verified change pipelines.
- Zero Trust lens: authenticate & authorize every flow hop; no implicit trust by network location.

Thuật ngữ: control plane = *mặt phẳng điều khiển*; data plane = *mặt phẳng dữ liệu*; BFD = *phát hiện lỗi liên kết song hướng*; DoS = *tấn công từ chối dịch vụ*; Zero Trust = *không tin cậy mặc định*

Segmentation & Hierarchical Policy (Cross-Cloud)

- Org-level guardrails: hierarchical policies above per-VPC/VNet rules for consistent baselines.
- Azure: Virtual Network Manager *Security Admin Rules* (global allow/deny/always-allow) precede NSGs.
- GCP: Hierarchical Firewall applies org/folder policies; delegate with `goto_next`; tag-aware rules.
- Zero-trust access: AWS Verified Access enforces identity/device context for app access (beyond IP/VPN).
- Practice: codify baselines in Terraform/Ansible; test propagation across accounts/subscriptions/projects.

Thuật ngữ: hierarchical policy = *chính sách phân cấp*; NSG = *nhóm bảo mật mạng*; `goto_next` = *chuyển đánh giá xuống tầng dưới*; zero-trust access = *truy cập không tin cậy mặc định*

Detection, Forensics & Evidence

- Flow evidence: OVN/flow logs + controller audit logs; correlate with tenant/project/user.
- Pipeline: collectors → stream bus → indexed search → SIEM dashboards & alerts.
- Forensics: `ovn-trace` pre-rollout proofs; packet capture/mirroring on `br-int` for incidents.
- Retention & compliance: hot (7–14d), cold (≥180d); legal hold; immutable storage options.
- SOC loop: IOC → ACL injection → verify → auto-rollback when cleared.

Thuật ngữ: SIEM = *quản lý sự kiện & thông tin bảo mật*; mirroring = *sao chép lưu lượng*; immutable = *không thể sửa đổi*; IOC = *chỉ báo xâm nhập*

Perspective: eBPF, Service Mesh & SmartNIC/DPUs

- Sidecarless meshes (eBPF): lower overhead; debate on isolation vs performance; evaluate per-risk profile.
- Cilium/ambient models: kernel-level L4/L7 enforcement; observability (Hubble/Tetragon) reduces blind spots.
- DPU/SmartNIC offload: move ACL/NAT/crypto onto NIC; watch for isolation, lifecycle & firmware supply chain.
- Strategy: treat mesh/DPUs as part of the trust boundary; sign artifacts; continuous attestation & patching.
- Roadmap: combine ZTA (NIST 800-207A) with kernel offloads & org-level policies for scalable, auditable control.

Thuật ngữ: eBPF = *mở rộng bộ lọc gói Berkeley*; sidecarless = *không dùng proxy cạnh dịch vụ*; DPU/SmartNIC = *bộ xử lý dữ liệu/thẻ mạng thông minh*; attestation = *xác thực tính toàn vẹn*

Industry Perspective

- **Cloud-scale SDN:** hyperscalers dùng overlay + whitebox + controller riêng (ý tưởng: VPC/VNet).
- **Vendors:** Cisco ACI (APIC), VMware NSX-T, Juniper Tungsten Fabric (OpenContrail), OpenDaylight/ONOS, Calico/Cilium (eBPF).
- **Integration challenges:** nối giữa VM (Neutron) & containers (CNI), hybrid cloud, multi-tenant compliance.
- **Ops transform:** network-as-code, shared ownership với platform/SRE, observability-by-default.

Industry Perspective & Platform Trends

- Hyperscalers adopt overlay fabrics (Quantum, Andromeda, Azure SCN) with custom data planes.
- Convergence: containers + VMs on unified SDN (e.g. OVN-K8s, Cilium, Calico + NEAT).
- Zero-trust adoption: identity-aware routing, device posture integrated at network layer.
- Consistency layers: network policy abstraction frameworks (Crossplane, Istio, Azure NM).
- Future direction: programmable DPUs, disaggregated control planes, AI-based policy feedback.

Thuật ngữ: hypervisor = *siêu giám sát*; K8s = *Kubernetes*; NEAT = *"network egress autoscaling"*; DPU = *bộ xử lý dữ liệu*

Platform Policy Models

- Layered policy: org / subscription / project / VPC / NSG / SG hierarchies.
- Override vs baseline: admin rules that cannot be shadowed vs developer rules.
- Tag/label-based matching: policy scopes by resource tags, namespaces, identity groups.
- Policy versioning: drift tracking, policy rollbacks, policy diff previews.
- Cross-cloud policy alignment: Terraform modules, OPA policy libraries, Conftest, kube-lint attachments.

Thuật ngữ: namespace = *không gian tên*; override = *ghi đè*; baseline = *ngưỡng khởi đầu*; label = *nhãn tài nguyên*

OpenStack Neutron / OVN: ML2 Drivers

- ML2 plugin supports OVS, Linux bridge, and OVN drivers; OVN recommended for scale.
- Network types: VLAN, VXLAN, Geneve, flat, local; provider networks for external routing.
- DVR / DVRHA: distributed L3 routing (DVR) and high availability DVR (DVRHA) to avoid bottlenecks.
- L3 HA: VRRP/keepalived on routers or OVN HA routers with internal election.
- Distributed routing: route tables distributed across compute nodes, logical routers, avoids central choke.

Thuật ngữ: DVR = *định tuyến phân tán*; DVRHA = *DVR với sẵn sàng cao*; VRRP = *giao thức định tuyến dự phòng*

OpenStack Neutron / OVN: Scalability & HA

- Keepalived + VRRP on chassis for active/passive L3 nodes.
- Controller clustering: ovn-northd in HA mode; keep database replicas synchronized.
- Scalability: distributed L3, modular agents for DHCP/LB/Firewall; avoid central "compute agent" chokepoint.
- Performance tuning: batch OVN transaction commits, reduce sync overhead, use incremental updates.
- Fault handling: self-healing of OVN DB splits, reconciliation after partition recovery.

Thuật ngữ: northd = *daemons điều phối OVN*; VRRP = *giao thức định tuyến dự phòng*; reconciliation = *đồng bộ trạng thái*

AWS VPC & Lattice: Multi-account Networking

- VPC per account / per workload; Transit Gateway hubs for inter-VPC connectivity.
- VPC Lattice: cross-account service connectivity abstraction + policy enforcement.
- Reachability Analyzer: validate routing, security group, and NACL paths pre-deploy.
- Network Firewall: stateful network firewall at VPC edges; inspection and intrusion protection rules.
- Integration: share VPCs (Resource Access Manager), VPC endpoints, PrivateLink for service exposure.

Thuật ngữ: Transit Gateway = *cổng trung chuyển mạng*; VPC Lattice = *mô hình liên kết dịch vụ VPC*; NACL = *danh sách kiểm soát mạng*

Azure VNet & Network Manager

- Hub-and-spoke model: central VNet acts as backbone; spoke VNets peer/distribute traffic.
- Virtual Network Manager: global security admin rules (deny rules, always-allow) inherited.
- Policy propagation: apply tags/subscriptions based policy from central to VNets.
- Peer/S2S ExpressRoute: route filters, BGP propagation control, egress greenfield connectivity.
- Integration: Azure Firewall DNS proxy, DDoS protection, centralized monitoring.

Thuật ngữ: Virtual Network Manager = *Trình quản lý mạng ảo*; hub-and-spoke = *mẫu trung tâm–vệ tinh*; BGP = *giao thức định tuyến biên*

GCP VPC & Hierarchical Firewall

- Shared VPC: host project hosts subnets; service projects attach resources.
- Hierarchical Firewall: org/folder policies override VPC-level rules; `goto_next` semantics.
- Cloud Router & Peering: BGP sessions for on-prem & interconnect; route exchange with filters.
- Firewall Analytics: flow logs & aggregated metrics view; security dashboards.
- Network Service Tiers: Premium vs Standard pathing and cost/sla tradeoffs.

Thuật ngữ: Hierarchical Firewall = *tường lửa phân cấp*; shared VPC = *VPC chia sẻ*; `goto_next` = *đi tiếp tầng sau*; Cloud Router = *bộ định tuyến đám mây*

Kubernetes CNI Integration & SDN Bridging

- OVN-Kubernetes: extend OVN overlay to connect pods and VMs under same logical network.
- Calico + BGP/eBGP: route distribution via BGP, policy at L3/L4 using eBPF datapath.
- Cilium: eBPF-based L3/L7 enforcement; observability (Hubble, Tetragon) for auditing.
- Multi-tenant bridging: isolate pod networks per team/namespace mapped to tenant SGs in SDN.
- Service mesh interplay: Istio/Linkerd leverage underlying SDN for circuit-level routing + policy.

Thuật ngữ: pod = *đơn vị triển khai Kubernetes*; namespace = *không gian tên*; BGP = *giao thức định tuyến biên*; eBPF = *xử lý gói trong nhân*; service mesh = *lưới dịch vụ*

Platform Comparison Matrix

Feature	OpenStack	AWS	Azure	GCP	K8s
Multi-account	7	3	3	✓	via tenant
Policy hierarchy	Plugin	IAM	Manager rules	Org policies	Namespace
HA routing	DVRHA	TGW redundancy	FW HA	Peering redundancy	CNI HA
Network firewall	Neutron FW ext	AWS Firewall	Azure Firewall	Cloud FW	NetworkPolicy+Envo
Connectivity	Overlay	TGW, VPC Peering	VNet Peering	Cloud Router	mesh + CNI
Observability	flow logs	VPC Flow	NSG flow	FW logs	eBPF tracing

Thuật ngữ: DVRHA = *DVR với sẵn sàng cao*; TGW = *Transit Gateway*; goto_next = *chuyển kiểm tra tầng tiếp theo*; CNI = *giao diện mạng container*

Platform Challenges & Future Directions

- Policy drift across clouds: ensure versioned policies and drift detection in multicloud.
- Seamless identity binding: federated identity to map network rules across platforms.
- Edge/IoT extension: SDN policies to edge gateways with intermittent connectivity.
- DPU adoption: offload policies to SmartNICs – maintain consistent behavior across hosts.
- AI/ML for anomalies: detect misconfiguration or unexpected flows; auto-heal within guardrails.

Thuật ngữ: identity binding = *liên kết danh tính*; drift = *sai lệch cấu hình*; DPU = *bộ xử lý dữ liệu*; auto-heal = *tự sửa lỗi*

Hands-on Objectives & Evaluation Scope

- Build a 3-tier app fabric: overlay + distributed L3/NAT, least-privilege SG chaining.
- Operate via **Network-as-Code**: repo, PR review, plan→apply, rollback on breach.
- Enforce **policy-as-code**: OPA/Conftest checks for risky rules & tagging baselines.
- Observe & prove: flow logs, `ovn-trace`, packet capture; attach evidence to changes.
- Contain incidents: SOC→SDN automation for targeted deny & reversible blocks.

Thuật ngữ: Network-as-Code = *mạng như mã*; policy-as-code = *chính sách như mã*; distributed L3/NAT = *định tuyến/NAT phân tán*; rollback = *hoàn tác*; evidence = *bằng chứng*

Lab Environment & Prerequisites

- **Platform**: OpenStack with Neutron (ML2/OVN), provider network for Internet egress.
- **Tooling**: Ansible, Python venv, Git, OPA & Conftest, `iperf3`, `tcpdump`, `ovn-trace`.
- **Access**: API creds for OpenStack; read access to OVN NB/SB if permitted.
- **Safety**: non-prod tenant/project; quota for networks/ports/FIPs; time-boxed changes.
- **Deliverables**: repo link, evidence bundle (logs, traces), runbook, post-lab review.

Thuật ngữ: provider network = *mạng nhà cung cấp*; tenant/project = *thuê bao/dự án*; quota = *hạn ngạch*; runbook = *sổ tay xử lý*

Project Skeleton (Repo Layout)

```
wk5-sdn/
 inventory/
  hosts.yaml
 group_vars/
  all.yaml # cidr, names, qos values
 playbooks/
  net.yml # networks, subnets, router, fip
  sg.yml # SG baseline & chaining
  qos.yml # QoS policies & attachment
  soc_block.yml # IOC -> deny ACL
  evidence.yml # logs, traces, pcaps
 policy/
  neutron.rego # OPA guardrails
 .pre-commit-config.yaml
 .github/workflows/net-ci.yaml
```

Thuật ngữ: inventory = *tệp kiểm kê*; guardrail = *rào chắn an toàn*; workflow = *quy trình tự động*

Lab 1 — Overlay Provision (Network/Subnet, Part 1)

```
- hosts: controller
  vars:
    net_name: wk5-net
    cidr: 10.50.1.0/24
    ext_net: public-ext
  tasks:
    - openstack.cloud.network:
        state: present
        name: "{{ net_name }}"
        provider_network_type: vxlan
    - openstack.cloud.subnet:
        state: present
        name: wk5-subnet
        network_name: "{{ net_name }}"
        cidr: "{{ cidr }}"
        enable_dhcp: yes
        dns_nameservers: ["1.1.1.1","8.8.8.8"]
```

Thuật ngữ: overlay = *mạng phủ*; DHCP = *cấp phát IP động*

Lab 1 — Overlay Provision (Router, Part 2)

```
- hosts: controller
  vars:
    ext_net: public-ext
  tasks:
    - openstack.cloud.router:
        state: present
        name: wk5-router
        network: "{{ ext_net }}"
    - openstack.cloud.router:
        state: present
        name: wk5-router
        interfaces: [wk5-subnet]
```

Thuật ngữ: provider type = *kiểu mạng nhà cung cấp*

Lab 2 — Security Baseline (SG Chaining, Part 1)

```
- hosts: controller
  tasks:
    - openstack.cloud.security_group: {state: present, name: sg-web}
    - openstack.cloud.security_group_rule:
        security_group: sg-web
        protocol: tcp
        port_range_min: 80
        port_range_max: 80
        remote_ip_prefix: 0.0.0.0/0
    - openstack.cloud.security_group_rule:
        security_group: sg-web
        protocol: tcp
        port_range_min: 443
        port_range_max: 443
        remote_ip_prefix: 0.0.0.0/0
```

Thuật ngữ: SG chaining = *xâu chuỗi nhóm bảo mật*

Lab 2 — Security Baseline (SG Chaining, Part 2)

```
- hosts: controller
  tasks:
    - openstack.cloud.security_group: {state: present, name: sg-app}
    - openstack.cloud.security_group_rule:
        security_group: sg-app
        protocol: tcp
        port_range_min: 8080
        port_range_max: 8080
        remote_group: sg-web
    - openstack.cloud.security_group: {state: present, name: sg-db}
    - openstack.cloud.security_group_rule:
        security_group: sg-db
        protocol: tcp
        port_range_min: 5432
        port_range_max: 5432
        remote_group: sg-app
```

Thuật ngữ: least privilege = *đặc quyền tối thiểu*

Lab 3 — Policy-as-Code Guardrails (OPA/Conftest)

```
package neutron.guardrails

deny[msg] {
  input.kind == "security_group_rule"
  input.protocol == "tcp"
  input.port_range_min <= 22
  input.port_range_max >= 22
  input.remote_ip_prefix == "0.0.0.0/0"
  msg := "SSH must not be exposed to the Internet"
}

deny[msg] {
  input.kind == "qos_policy"
  not input.tags["owner"]
  msg := "QoS policies must include an ’owner’ tag"
}
```

Thuật ngữ: OPA = *Open Policy Agent*; Conftest = *kiểm thử chính sách*; tag = *nhãn*

Lab 4 — CI/CD: Plan → Apply with Gates

```
name: net-ci
on: [pull_request, push]
jobs:
  plan:
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - run: pip install ansible conftest
      - run: conftest test artifacts/plan.json
      - run: ansible-playbook playbooks/net.yml --check
  apply:
    if: github.ref == ’refs/heads/main’
    needs: plan
    runs-on: ubuntu-latest
    steps:
      - uses: actions/checkout@v4
      - run: pip install ansible
      - run: ansible-playbook playbooks/net.yml
```

Thuật ngữ: plan = *kế hoạch thi hành*; gate = *cổng kiểm soát*; –check = *chạy thử không áp dụng*

Lab 5 — Observability & Evidence Pack

- Flow logs: enable/export; correlate with tenant/project and SG hit/miss.
- `ovn-trace`: validate web→app (8080) & app→db (5432) before rollout.
- Packet capture: `tcpdump -i br-int` on both ends to confirm path/MTU.
- Evidence bundle: `ovn-trace` output, flow logs, screenshots of SGs; link to PR.
- Retention: 14d hot, 180d cold; attach to ticket for audit.

Thuật ngữ: observability = *khả năng quan sát*; hit/miss = *khớp/không khớp*; retention = *lưu giữ*

Lab 6 — Closed-Loop SOC→SDN (IOC → ACL)

```
- hosts: controller
  vars:
    ioc_url: "https://siem.local/api/iocs"
    ls_name: "ls-wk5"
  tasks:
    - name: Fetch IOC list
      uri: { url: "{{ ioc_url }}", method: GET }
      register: iocs
    - name: Insert deny rules
      command: >
        ovn-nbctl acl-add {{ ls_name }} to-lport 100
        "ip4.src=={{ item }} && tcp" drop
      loop: "{{ iocs.json }}"
    - name: Verify path is blocked
      command: ovn-trace --ct new {{ ls_name }} ’inport=="{{ ls_name }}-web" && ip4.src=={{
          item }}’
      loop: "{{ iocs.json }}"
```

Thuật ngữ: IOC = *chỉ báo xâm nhập*; ACL = *danh sách kiểm soát truy cập*

(Optional) OVN Address Sets & ACL

```
# Using ovn-nbctl via Ansible command
- hosts: controller
  tasks:
    - name: Create address sets
      command: >
        ovn-nbctl create Address_Set name=as-web addresses="10.50.1.10 10.50.1.11"
    - name: Allow web to app 8080
      command: >
        ovn-nbctl acl-add ls-wk5 to-lport 1001 "ip4.src==\$as-web && tcp && tcp.dst==8080"
             allow
```

Mini Lab

1. Tạo wk5-net (VXLAN), subnet, router ra `public-ext`. Khởi tạo 3 VM: Web, App, DB.
2. Áp SG: `sg-web`, `sg-app`, `sg-db`. Kiểm thử: Web→App (8080) OK; App→DB (5432) OK; Internet→Web (80/443) OK; chặn còn lại.
3. (Tuỳ chọn) OVN ACL với address-sets; bật QoS egress và đo bằng `iperf3`.

Threat Model Lite (STRIDE) cho SDN

- **Spoofing:** thiết bị giả mạo join overlay ⇒ PKI/mTLS, allowlist.
- **Tampering:** sửa policy/flow ⇒ IaC + review, drift detection.
- **Repudiation:** thiếu audit ⇒ controller logs, flow logs, SIEM.
- **Information Disclosure:** lộ lưu lượng lateral ⇒ microsegmentation, egress controls.
- **DoS:** flood control/data plane ⇒ rate limit, HA controllers, backoff.
- **EoP:** lạm dụng quyền controller ⇒ RBAC/SoD, JIT admin, MFA.

Wrap-up — Key Takeaways

- **Design:** overlays + distributed L3/NAT enable scale; security is *microsegmentation-first*.
- **Operate:** Network-as-Code with GitOps gates; controller is the single source of truth.
- **Secure:** policy-as-code guardrails; closed-loop SOC→SDN containment.
- **Observe:** flow logs + `ovn-trace` + mirroring → evidence on every change.
- **Map:** Neutron/OVN concepts align with AWS/Azure/GCP/K8s primitives.

Thuật ngữ: Network-as-Code = *mạng như mã*; policy-as-code = *chính sách như mã*; containment = *khoanh vùng*; mirroring = *sao chép lưu lượng*

Wrap-up — Outcomes & Evidence

- **Outcomes:** 3-tier overlay reachable per design; SG chaining least-privilege; QoS limits effective; IOC→ACL containment works.
- **Evidence pack:**
  - `ovn-trace` proofs (web→app 8080; app→db 5432; blocked IOC).
  - Flow logs + SG/NACL hit/miss summaries.
  - Packet captures (`tcpdump -i br-int`) confirming path/MTU.
  - PR links & controller audit entries for change lineage.
- **Readiness for Week 6:** storage threats model + encryption/IAM patterns applied with the same *policy-as-code* discipline.

Thuật ngữ: hit/miss = *khớp/không khớp*; lineage = *chuỗi nguồn gốc*; IAM = *quản lý danh tính & truy cập*

Zero Trust with SDN (Không tin cậy mặc định)

- **Least privilege**: Web→App (8080), App→DB (5432), deny-by-default.
- **Giới hạn bán kính thiệt hại**: nhóm/tag; tránh 0.0.0.0/0 cho cổng nhạy cảm.
- **Hạn chế di chuyển ngang**: SG/ACL theo cặp dịch vụ; overlay per-tenant.
- **An toàn thay đổi**: shadow rules, staged enablement, rollback tự động.

Controller Plane Hardening (Gia cố mặt phẳng điều khiển)

- **mTLS** giữa thành phần; xoay vòng chứng thư; pin CA.
- **RBAC & SoD**: quyền tối thiểu; JIT admin; audit bắt buộc.
- **Cách ly**: mgmt plane riêng; rate limit; HA controllers.
- **Log bất biến**: forward về SIEM, lưu giữ bằng chứng.

Network-as-Code (GitOps)

- **Pre-commit**: yamllint, ansible-lint; policy check (OPA/Conftest).
- **CI**: dry-run (`–check`), molecule, lưu diff kế hoạch.
- **CD**: canary, progressive; rollback khi SLO vi phạm.
- **Bằng chứng**: đính kèm log/ảnh chụp/ovn-trace vào ticket.

Policy-as-Code Guardrail (Conftest/OPA)

```
package neutron.policy

deny[msg] {
  input.resource == "security_group_rule"
  input.protocol == "tcp"
  input.port_range_min <= 5432
  input.port_range_max >= 5432
  input.remote_ip_prefix == "0.0.0.0/0"
  msg := "DB port 5432 must not be exposed to the Internet"
}
```

Closed-Loop Security: SOC → SDN

Luồng: SIEM (IOC) ⇒ API controller ⇒ chèn ACL ⇒ kiểm thử ⇒ lưu bằng chứng.

```
- hosts: controller
  tasks:
    - name: Fetch IOC list
      uri: { url: "https://siem.local/api/iocs", method: GET }
      register: iocs
    - name: Block malicious sources
      command: >
        ovn-nbctl acl-add ls-tenant to-lport 100
        "ip4.src=={{ item }} && tcp" drop
      loop: "{{ iocs.json }}"
```

Observability & Forensics (Quan sát & Pháp y)

- **Flow introspection**: `ovn-trace`, `ovs-ofctl dump-flows`, `tcpdump -i br-int`.
- **Mirroring**: SPAN logical switch/port → Zeek/Suricata; lưu PCAP.
- **Chuỗi bằng chứng**: băm cấu hình; snapshot DB controller; export log.
- **SLO**: MTU/PMTUD; DHCP/RA success; error budget kết nối.

Industrial Labs

1. **A**: Tự động hoá overlay (VXLAN/Geneve), router ra provider, 3-tier app.
2. **B**: Microsegmentation & QoS; address-sets + ACL; `iperf3` xác nhận.
3. **C**: **SOC-driven containment**: nhận IOC → chèn deny ACL → ovn-trace → rollback.