



Glossary - Advanced Networking Specialty Ans C01

102 terms collected from the sheets in this collection; [brackets] name the source sheets

A

Accelerated Site-to-Site VPN — VPN whose tunnel endpoints are reached through Global Accelerator edge locations; only on Transit Gateway attachments. *[ANS-C01: Direct Connect, VPN and BGP]*

Allowed prefixes — On a DX gateway association with a TGW or VGW, the list of AWS-side prefixes advertised to on-premises. *[ANS-C01 Self-Assessment]*

Amazon VPC IPAM — IP address manager: pools per Region or environment, CIDR allocation rules, overlap and compliance monitoring across the organisation. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Amazon VPC Lattice — Application networking service: services and target groups joined in a service network, reachable across VPCs and accounts with IAM auth policies, no peering or TGW needed. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Appliance mode — TGW VPC-attachment setting that keeps both directions of a flow on the same AZ of an inspection VPC so stateful firewalls see symmetric traffic. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Application Load Balancer (ALB) — Layer-7 load balancer for HTTP, HTTPS and gRPC with host, path, header and query routing, authentication (OIDC, Cognito), mutual TLS and AWS WAF. *[ANS-C01: Load Balancing, Edge and IPv6]*

AS_PATH prepending — Repeating your ASN in advertisements so that path looks longer and less preferred; AWS honours it between DX paths of equal local preference. *[ANS-C01: Direct Connect, VPN and BGP]*

Asymmetric routing — Request and response taking different paths; breaks stateful firewalls and NAT. *[ANS-C01 Self-Assessment]*

AWS Certified Advanced Networking - Specialty (ANS-C01) — AWS specialty exam on designing, implementing, operating and securing hybrid and multi-VPC networks on AWS at scale. *[Advanced Networking Specialty ANS-C01: Start Here]*

AWS Client VPN — Managed OpenVPN-based remote access for users, authenticated by mutual certificates, Active Direc-

tory or SAML, with split tunnelling and authorization rules. *[ANS-C01: Direct Connect, VPN and BGP]*

AWS Cloud WAN — Managed global WAN built from a JSON core network policy: Regions as core network edges, segments (routing domains), attachment policies by tag, segment sharing and service insertion. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

AWS Direct Connect (DX) — Private physical connection from your network to AWS at a Direct Connect location, dedicated (1, 10, 100 Gbps and 400 Gbps in some locations) or hosted by a partner (50 Mbps up to 10 Gbps or more). *[ANS-C01: Direct Connect, VPN and BGP]*

AWS Firewall Manager — Organisation-wide policy service that deploys and enforces WAF, Shield Advanced, security groups, Network Firewall, DNS Firewall and third-party firewall policies across accounts. *[ANS-C01: Network Security, Compliance, Governance]*

AWS Network Firewall — Managed stateful (Suricata-compatible) and stateless network firewall deployed as firewall endpoints in dedicated subnets, with domain filtering, IPS rules and TLS inspection. *[ANS-C01: Network Security, Compliance, Governance]*

AWS Network Manager — Central console for global networks: Transit Gateway and Cloud WAN topology, route analyzer, events and on-premises sites, devices and links. *[ANS-C01: Network Management and Operation]*

AWS Shield Advanced — Paid DDoS protection with 24/7 Shield Response Team, health-based detection, automatic application-layer mitigation, cost protection and WAF included for protected resources. *[ANS-C01: Network Security, Compliance, Governance]*

AWS Verified Access — Zero-trust access to internal applications without a VPN: each request is evaluated against identity and device posture policies (Cedar). *[ANS-C01: Network Security, Compliance, Governance]*

B

BFD (Bidirectional Forwarding Detection) — Fast liveness protocol for BGP sessions; enabled by default on AWS for DX (300 ms interval, multiplier 3) once your router enables it. *[ANS-C01: Direct Connect, VPN and BGP]*

BGP (Border Gateway Protocol) — Path-vector routing protocol used between autonomous systems, and by AWS on Direct Connect, VPN, TGW Connect and Cloud WAN. *[Advanced Networking Specialty ANS-C01: Start Here]*

BGP local preference communities — Tags 7224:7100 (low), 7224:7200 (medium), 7224:7300 (high) you attach to prefixes on private and transit VIFs to tell AWS which DX path to prefer towards you. *[ANS-C01: Direct Connect, VPN and BGP]*

BYOIP (bring your own IP) — Advertising your own public IPv4 (/24 minimum) or IPv6 (/48 advertised) ranges from AWS after proving ownership with a ROA. *[ANS-C01: Load Balancing, Edge and IPv6]*

C

CloudFront Functions vs Lambda@Edge — Functions: JavaScript, sub-millisecond, viewer request/response only, no network calls; Lambda@Edge: Node.js or Python, origin events too, network access, higher latency and cost. *[ANS-C01: Load Balancing, Edge and IPv6]*

CloudFront VPC origin — 2024 feature letting CloudFront reach a private ALB, NLB or EC2 instance in a private subnet without exposing it to the internet. *[ANS-C01: Load Balancing, Edge and IPv6]*

CloudWatch Internet Monitor — Uses AWS's view of internet health to show availability and performance impact on your application's users by city and ISP. *[ANS-C01: Network Management and Operation]*

CloudWatch Network Monitor — Synthetic ICMP or TCP probes from AWS to on-premises or other targets, reporting packet loss and latency of hybrid paths (formerly Network Synthetic Monitor). *[ANS-C01: Network Management and Operation]*

Conditional forwarder — On-premises DNS setting that sends queries for one domain (such as `aws.corp.example`) to specific servers, here the inbound endpoint IPs. [*\[ANS-C01: Hybrid DNS and Route 53 Resolver\]*](#)

Customer gateway (CGW) — AWS object describing your VPN device: public IP (or private IP over DX), BGP ASN, certificate. [*\[ANS-C01: Direct Connect, VPN and BGP\]*](#)

D

Dead peer detection (DPD) — IKE keepalive that detects a dead VPN peer and triggers the configured timeout action. [*\[ANS-C01 Self-Assessment\]*](#)

Direct Connect gateway (DXGW) — Global object that links private or transit VIFs to virtual private gateways or Transit Gateways in any Region (except China); it does not route between its own attachments. [*\[ANS-C01: Direct Connect, VPN and BGP\]*](#)

DNSSEC — Signed DNS records; Route 53 signs public hosted zones with a key-signing key backed by an asymmetric KMS key in `us-east-1`, and Resolver can validate signatures. [*\[ANS-C01: Hybrid DNS and Route 53 Resolver\]*](#)

E

Edge-to-edge routing — Using another VPC's gateway (IGW, NAT, VPN, DX, gateway endpoint) through peering; not supported. [*\[ANS-C01 Exam Strategy and Scenarios\]*](#)

Egress-only internet gateway — Stateful gateway that allows outbound-only IPv6 traffic from a VPC, the IPv6 equivalent of a NAT gateway's protection. [*\[ANS-C01: Load Balancing, Edge and IPv6\]*](#)

ENA Express — Feature on supported instances using the AWS SRD protocol to raise single-flow bandwidth (up to 25 Gbps) and cut tail latency between instances in the same AZ. [*\[ANS-C01: Network Management and Operation\]*](#)

Endpoint policy — Resource policy on a VPC endpoint limiting the principals, actions and resources reachable through it. [*\[ANS-C01 Self-Assessment\]*](#)

F

Flow log custom format — Flow log fields you choose beyond the default v2 set, such as `pkt-srcaddr`, `pkt-destaddr`, `flow-direction`, `traffic-path`, `tcp-flags`, `vpc-id`, `subnet-id`, `az-id`. [*\[ANS-C01: Network Management and Operation\]*](#)

Forwarding rule — Resolver rule that sends queries for a domain (and its subdomains) to target IPs through an outbound endpoint; shareable with AWS RAM; the most specific domain wins. [*\[ANS-C01: Hybrid DNS and Route 53 Resolver\]*](#)

G

Gateway Load Balancer (GWLB) — Layer-3 load balancer that sends traffic to third-party appliances over GENEVE (UDP 6081) and back, reached through GWLB endpoints in route tables. [*\[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink\]*](#)

H

Health check (Route 53) — Endpoint, calculated or CloudWatch-alarm check that marks a record healthy or unhealthy for failover and multivalue routing. [*\[ANS-C01 Self-Assessment\]*](#)

Hosted VIF — A virtual interface created by one account on its DX connection and offered to another account, which accepts it. [*\[ANS-C01 Self-Assessment\]*](#)

Hybrid connectivity — Network links between on-premises and AWS: Direct Connect, Site-to-Site VPN, SD-WAN through TGW Connect or Cloud WAN. [*\[ANS-C01 Exam Strategy and Scenarios\]*](#)

Hybrid network — A network spanning on-premises sites and cloud VPCs joined by private links or VPNs with shared routing and DNS. [*\[Advanced Networking Specialty ANS-C01: Start Here\]*](#)

I

Inbound endpoint — Resolver ENIs (at least two AZs) whose IPs on-premises DNS servers forward to, so on-prem clients can resolve private hosted zones and VPC names. [*\[ANS-C01: Hybrid DNS and Route 53 Resolver\]*](#)

Inter-Region peering — VPC peering between Regions, encrypted on the AWS backbone, MTU 1500, no security group referencing across Regions. [*\[ANS-C01 Self-Assessment\]*](#)

J

Jumbo frame — Ethernet frame above 1500 bytes; inside a VPC up to 9001 bytes MTU, but traffic leaving through an IGW, peering across Regions or VPN is limited to 1500 (or less). [*\[ANS-C01: Network Management and Operation\]*](#)

L

Landing zone — Pre-built multi-account AWS environment (often with Control Tower) including the shared network account, logging and guardrails. [*\[Advanced Networking Specialty ANS-C01: Start Here\]*](#)

Least operational overhead — Qualifier preferring managed AWS networking features (TGW, Cloud WAN, Network Firewall, Route 53 Profiles) over self-managed appliances or scripts. [*\[ANS-C01 Exam Strategy and Scenarios\]*](#)

Link aggregation group (LAG) — LACP bundle of dedicated DX connections of the same speed at the same location, acting as one; a minimum-links setting takes the LAG down below a threshold. [*\[ANS-C01: Direct Connect, VPN and BGP\]*](#)

Longest prefix match — Routing rule: the most specific matching route (largest prefix length) wins before any other preference. [*\[ANS-C01 Self-Assessment\]*](#)

M

MACsec — IEEE 802.1AE layer-2 encryption on dedicated 10, 100 and 400 Gbps DX connections at supported locations. [*\[ANS-C01: Direct Connect, VPN and BGP\]*](#)

Managed prefix list — Named set of CIDRs referenced in security groups and route tables; AWS-managed lists include CloudFront origin-facing and S3. [*\[ANS-C01: Network Security, Compliance, Governance\]*](#)

Minimum links — LAG setting: the number of member connections that must be up for the LAG to stay operational. [*\[ANS-C01 Self-Assessment\]*](#)

Multi-Region active-active — Design where several Regions serve traffic at once, steered by Route 53 latency/geoproximity or Global Accelerator. [*\[ANS-C01 Exam Strategy and Scenarios\]*](#)

Multi-VPC architecture — Many VPCs (often one or more per account) connected through peering, Transit Gateway, Cloud WAN, PrivateLink or VPC Lattice. [*\[Advanced Networking Specialty ANS-C01: Start Here\]*](#)

N

NAT64 / DNS64 — Resolver DNS64 synthesises `64:ff9b::/96` AAAA records for IPv4-only names, and the NAT gateway translates that IPv6 traffic to IPv4, so IPv6-only subnets reach IPv4 services. [*\[ANS-C01: Load Balancing, Edge and IPv6\]*](#)

Network Access Analyzer — VPC tool that finds network paths matching a scope you define (for example any path from the internet to a database subnet) to prove segmentation. *[ANS-C01: Network Management and Operation]*

Network design (ANS domain 1) — Choosing edge, DNS, load balancing, hybrid connectivity, multi-account and multi-Region topologies; the heaviest ANS-C01 domain. *[Advanced Networking Specialty ANS-C01: Start Here]*

Network engineer (cloud) — Engineer who designs and runs connectivity, routing, DNS, load balancing and network security across on-premises and cloud. *[Advanced Networking Specialty ANS-C01: Start Here]*

Network implementation (ANS domain 2) — Building and automating the designed connectivity: DX, VPN, TGW, endpoints, DNS, IaC. *[Advanced Networking Specialty ANS-C01: Start Here]*

Network Load Balancer (NLB) — Layer-4 load balancer for TCP, UDP and TLS with one static IP (or Elastic IP) per AZ, client IP preservation, very high throughput, and PrivateLink support. *[ANS-C01: Load Balancing, Edge and IPv6]*

Network management and operation (ANS domain 3) — Monitoring, troubleshooting, optimising and maintaining routing and connectivity. *[Advanced Networking Specialty ANS-C01: Start Here]*

Network security, compliance, and governance (ANS domain 4) — Controls, encryption, logging and policy enforcement for AWS networks. *[Advanced Networking Specialty ANS-C01: Start Here]*

Nitro encryption in transit — Automatic hardware encryption of traffic between supported Nitro instance types in the same or peered VPCs within a Region, with no performance cost. *[ANS-C01: Network Security, Compliance, Governance]*

O

Origin Shield — Extra CloudFront caching layer in one chosen Region in front of the origin, raising hit ratio and cutting origin load. *[ANS-C01: Load Balancing, Edge and IPv6]*

Outbound endpoint — Resolver ENIs that send queries matching forwarding rules to target DNS servers, for example on-premises domain controllers. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Overlapping CIDRs — Two networks using the same address range; rules out peering, TGW and routed VPN without NAT,

points to PrivateLink, VPC Lattice or private NAT. *[ANS-C01 Exam Strategy and Scenarios]*

P

pkt-srcaddr — Flow log field with the original source IP of the packet, which differs from srcaddr when traffic passes a NAT gateway or other ENI on the way. *[ANS-C01: Network Management and Operation]*

PMTUD (Path MTU Discovery) — Senders learn the smallest MTU on a path through ICMP 'fragmentation needed' (IPv4) or 'packet too big' (IPv6) messages; blocking that ICMP breaks large transfers. *[ANS-C01: Network Management and Operation]*

Prefix list — Named group of CIDRs (customer-managed or AWS-managed) referenced in route tables and security groups and shareable with AWS RAM. *[ANS-C01 Self-Assessment]*

Private hosted zone (PHZ) — Route 53 zone answered only inside the VPCs associated with it; requires enableDnsSupport and enableDnsHostnames on those VPCs. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Private NAT gateway — NAT gateway without internet access that translates traffic from a non-routable (overlapping) range to a routable range for connectivity through TGW or VPN. *[ANS-C01 Exam Strategy and Scenarios]*

Proxy protocol v2 — Header an NLB can add to TCP connections carrying the original client address, needed when client IP preservation is off (for example IP targets or PrivateLink). *[ANS-C01: Load Balancing, Edge and IPv6]*

Public IPv4 charge — Since February 2024 AWS bills every public IPv4 address (in use or idle) at 0.005 USD per hour, a push towards IPv6 and private designs. *[ANS-C01: Load Balancing, Edge and IPv6]*

R

Rate-based rule — WAF rule that blocks or counts requests from an IP (or other key) above a threshold within an evaluation window (1, 2, 5 or 10 minutes). *[ANS-C01: Network Security, Compliance, Governance]*

Reachability Analyzer — Static configuration analysis between a source and a destination (ENI, instance, IGW, TGW, endpoint) that names the blocking or allowing components. *[ANS-C01: Network Management and Operation]*

Requirement anchor — The one constraint in a stem that eliminates most options: overlapping CIDRs, encryption, static IP, bandwidth, latency, cost, no internet. *[ANS-C01 Exam Strategy and Scenarios]*

Resolver query logging — Logs every DNS query from VPCs (name, type, response code, source) to CloudWatch Logs, S3 or Firehose. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Route 53 Profiles — 2024 feature that bundles PHZ associations, Resolver rules and DNS Firewall rule groups and applies them to many VPCs and accounts through AWS RAM. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Route 53 Resolver — The DNS resolver every VPC gets (AmazonProvidedDNS) at the VPC base address +2 and 169.254.169.253, answering private hosted zones, VPC names and public names. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Route 53 Resolver DNS Firewall — Filters outbound DNS queries from VPCs against domain lists (yours or AWS managed threat lists) with ALLOW, BLOCK or ALERT actions and fail-open or fail-closed mode. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Route Analyzer — Network Manager tool that checks the Transit Gateway route path between two IPs across route tables and peerings. *[ANS-C01: Network Management and Operation]*

S

Security group referencing — A rule whose source is another security group: allowed in the same VPC, peered VPCs in the same Region and, since 2024, across a Transit Gateway in the same Region (when enabled). *[ANS-C01: Network Security, Compliance, Governance]*

Segment — Cloud WAN routing domain (like a VRF): attachments in one segment reach each other; segments share routes only when the policy says so. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Service insertion — Steering traffic through inspection appliances or firewalls on its way between segments or to the internet. *[ANS-C01 Exam Strategy and Scenarios]*

SNI (Server Name Indication) — TLS extension carrying the requested host name, letting one ALB or NLB listener serve several certificates. *[ANS-C01: Load Balancing, Edge and IPv6]*

Specialty exam — AWS certification level that tests deep expertise in one domain; long scenario stems, several valid-looking

designs, one best fit. *[ANS-C01 Exam Strategy and Scenarios]*

Split-horizon DNS — Same domain name answered differently inside and outside: a private hosted zone for associated VPCs, a public hosted zone for the internet. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

Strict rule order — Network Firewall stateful evaluation mode where rule groups and rules run in the priority order you set, with a default action such as drop established, instead of pass-drop-alert action order. *[ANS-C01: Network Security, Compliance, Governance]*

System rule — Resolver rule that makes Resolver answer a sub-domain itself, overriding a broader forwarding rule. *[ANS-C01: Hybrid DNS and Route 53 Resolver]*

T

TGW association — The single TGW route table an attachment uses to look up where its traffic goes. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

TGW Connect — Attachment type that runs GRE tunnels with BGP over a VPC or DX transport attachment, for SD-WAN appliances. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

TGW propagation — An attachment installing its routes (VPC CIDRs, BGP prefixes) into one or more TGW route tables. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Traffic dial — Global Accelerator per-endpoint-group percentage (0-100) controlling how much traffic a Region receives, for blue/green or maintenance. *[ANS-C01: Load Balancing, Edge and IPv6]*

Traffic Mirroring — Copies packets from a Nitro instance ENI to an ENI, NLB or GWLB endpoint target with filters, for IDS, packet capture and troubleshooting. *[ANS-C01: Network Management and Operation]*

Transit Gateway (TGW) — Regional layer-3 hub connecting VPCs, VPNs, Direct Connect gateways, Connect (GRE/BGP) attachments and other TGWs, with its own route tables. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

Transitive routing — Traffic passing through one network to reach a third; unsupported over VPC peering, VGWs and gateway endpoints, supported by Transit Gateway and Cloud WAN. *[ANS-C01 Exam Strategy and Scenarios]*

V

Virtual interface (VIF) — An 802.1Q VLAN plus a BGP session on a DX connection: private VIF (VPCs via VGW or DX gateway), public VIF (AWS public endpoints) or transit VIF (Transit Gateways via DX gateway). *[ANS-C01: Direct Connect, VPN and BGP]*

Virtual private gateway (VGW) — VPN and DX termination attached to one VPC; Amazon-side ASN default 64512. *[ANS-C01: Direct Connect, VPN and BGP]*

VPC Block Public Access — 2024 account and Region setting that blocks internet gateway traffic to VPCs (bidirectional or ingress-only) with exclusions per VPC or subnet. *[ANS-C01: Network Security, Compliance, Governance]*

VPC endpoint service — Your service exposed through AWS PrivateLink from behind a Network Load Balancer (or Gateway Load Balancer) to consumer VPCs in other accounts, one-way, overlapping CIDRs allowed. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

VPC sharing — An owner account shares subnets through AWS RAM; participant accounts launch resources in them while the owner keeps routing, NACLs and gateways. *[ANS-C01: Transit Gateway, Cloud WAN, PrivateLink]*

W

WCU (WAF capacity unit) — Cost unit of a WAF rule's complexity; a web ACL includes 1,500 WCU by default and can use more (up to 5,000) for an extra fee. *[ANS-C01: Network Security, Compliance, Governance]*

Web ACL — AWS WAF set of rules (managed rule groups, custom, rate-based) attached to CloudFront, ALB, API Gateway, AppSync, Cognito, App Runner or Verified Access, measured in WAF capacity units. *[ANS-C01: Network Security, Compliance, Governance]*