AWS CERTIFIED Advanced Networking

Specialty

ANS-C01

65 Qs	170 Min	750 Pass	4 Domains	No Penalty

D1 Network Design 30%	D2 Implementation 26%	D3 Mgmt & Ops 20%	D4 Security 24%

D1 · NETWORK DESIGN 30%

VPC Architecture & Multi-Account Patterns

- TGW: hub router; up to 5,000 VPC attachments; transitive routing
- VPC Peering: point-to-point, non-transitive; no TGW for 2 VPCs
- Multiple TGW route tables: segment spoke VPCs from shared services
- TGW Blackhole route: silently drops matching CIDRs
- Shared VPC via RAM: host shares subnets to participant accounts
- TGW inter-region peering: private AWS backbone, never public internet
- PrivateLink: NLB-backed; Interface Endpoint; safe with CIDR overlap
- VPC secondary CIDRs: up to 4 additional (5 total) per VPC
- 5 reserved IPs/subnet: .0 net, .1 router, .2 DNS, .3 future, .255 bcast

Route 53 Routing Policies

Policy	Use Case	Key Fact
Weighted	A/B / canary	weight/sum of weights
Latency	Fastest region	Resolver location, not user IP
Failover	Active/Standby	Health check on primary required
Geolocation	Compliance/locale	Needs default record
Geoproximity	Bias traffic shift	Bias -99 to +99; shrinks/expands zone
ALIAS	Zone apex (root)	Free; no CNAME at apex

Route 53 Resolver — Hybrid DNS

- Inbound endpoints: ENIs in VPC; on-prem DNS forwards INTO AWS
- Outbound endpoints: AWS forwards queries OUT to on-prem DNS
- Forwarding rules: route corp.internal → on-prem resolvers
- Rules shared via RAM to all spoke VPCs in organization
- Cross-account PHZ: authorize in Account A, associate Account B VPC

CloudFront & Global Accelerator

- CloudFront: HTTP/HTTPS CDN at 400+ PoPs; caches; Lambda@Edge/CF Funcs
- Cache behaviors: path-pattern routing /api/* vs /static/* to diff origins
- Origin groups: primary + failover origin (auto-retry on 4xx/5xx)
- OAC (Origin Access Control): restricts S3 access to CF only; replaces OAI
- Global Accelerator: Anycast IPs; TCP/UDP; AWS backbone; NOT HTTP caching
- GA: static IPs per AZ; nearest PoP entry; best for gaming/IoT/VoIP
- CF vs GA: CF caches content; GA routes any TCP/UDP without caching

VPC Endpoints

Type	Services	Cost	Notes
Gateway	S3, DynamoDB	Free	Route table entry; no ENI
Interface	100+ services	$0.01/hr	ENI; private DNS; PrivateLink

BGP Attributes

Attribute	Set By	Effect
AS_PATH prepend	On-prem	Makes path less preferred by AWS
MED	AWS sets	Lower MED = preferred path inbound
Local Pref	Internal AS	Not shared across ASes
BGP Communities	Both	Route tagging for filtering policies

D2 · NETWORK IMPLEMENTATION 26%

Direct Connect Virtual Interfaces

VIF	Connects To	Route Limit	Use Case
Private	VGW → single VPC or DXGW	100	Private IP VPC access
Public	AWS public endpoints (S3)	1,000	S3/SQS over DX link
Transit	DXGW → TGW (many VPCs)	100	Enterprise multi-VPC

DX Resiliency Tiers

- Maximum (99.99%): 2 DX locations × 2 connections = 4 total connections
- High (99.9%): 2 connections at same DX location
- BFD: sub-second failure detection vs 90s BGP hold timer
- LAG: up to 4 same-speed same-location connections bundled
- MACsec: IEEE 802.1AE L2 AES-256-GCM on dedicated DX; MKA key protocol
- DXGW: global; 10 VGWs; VPCs connected via DXGW cannot talk to each other
- Backup S2S VPN recommended at all resiliency tiers for failover

Site-to-Site VPN

- 2 IPSec tunnels per connection; active-active with ECMP recommended
- ECMP + 4 VPN attachments × 2 tunnels = up to 10 Gbps aggregate on TGW
- Accelerated VPN: Global Accelerator PoP entry; best for distant customers
- Attach to VGW (single VPC) or TGW (multiple VPCs); TGW preferred

Load Balancer Comparison

Feature	ALB	NLB	GWLB
Layer	L7 HTTP	L4 TCP/UDP	L3 GENEVE
Source IP	X-Forwarded-For	Native preserved	Preserved
Static IP	No	Elastic IP/AZ	N/A
Routing	Host/path/header	Port/protocol	Bump-in-wire
WAF	Yes (direct)	No	No
Cross-zone	ON default	OFF default	N/A
Algorithm	RR or LOR	Flow hash	5-tuple hash

PrivateLink & Interface Endpoints

- Provider: NLB in front of service → create VPC Endpoint Service
- Consumer: Interface Endpoint (ENI with private IP) in their VPC
- No VPC peering; no CIDR overlap issues; cross-account by acceptance
- Private DNS: enable on endpoint + VPC DNS settings for hostname override
- Endpoint policy: IAM resource policy; aws:ResourceOrgID prevents exfil
- ECR private: ecr.api + ecr.dkr (Interface) + S3 (Gateway) endpoints needed

ALB Advanced Routing

- Host-based: api.example.com vs www.example.com → different TGs
- Path-based: /api/* → backend TG; /static/* → S3 TG
- Header/query string conditions supported in listener rules
- Authenticate action: Cognito or OIDC IdP before forwarding
- Security Policy: controls TLS version (1.2/1.3) and cipher suites
- LOR (Least Outstanding Requests): better than round-robin for variable load

D3 · NETWORK MGMT & OPERATIONS 20%

Monitoring & Observability Tools

Tool	What It Captures	Key Fact
VPC Flow Logs	IP metadata: IPs, ports, bytes, ACCEPT/REJECT	NOT packet payload; S3+Athena for SQL
Traffic Mirroring	Full packet payloads from ENI	IDS/forensics; NLB/ENI target; per-GB cost
Reachability Analyzer	Logical path analysis (no traffic sent)	Tests ONE src→dst path; CI/CD pipeline use
Network Access Analyzer	All resources matching a pattern	Scale audit: find ALL EC2s open on port 22
R53 Query Logging	All DNS queries from VPC resources	Detect DNS tunneling; central S3 cross-account
CloudWatch DX	ConnectionState, ConnectionBps	Alarm on ConnectionState=0 for DX failure
CloudWatch VPN	TunnelState, TunnelDataIn/Out	Alarm on TunnelState=0; check both tunnels
CloudWatch NAT GW	ErrorPortAllocation, PacketsDropCount	55K conn/dst IP:port limit; add more NAT GWs

Reachability Analyzer vs Network Access Analyzer

Feature	Reachability Analyzer	Network Access Analyzer
Scope	One specific src→dst path	All resources matching a pattern
Traffic sent	No — config analysis only	No — config analysis only
Example	Can EC2-A reach RDS-B:3306?	Which EC2s are open on port 22?
CI/CD	API: NetworkPathFound=false → fail	Bulk compliance scan

Troubleshooting Quick Reference

Symptom	Tool	What to Check
No internet despite IGW	VPC route table	0.0.0.0/0 → igw-xxx missing from subnet route table
Instance unreachable	Reachability Analyzer	SG inbound, NACL, route table, IGW/NAT GW
DNS failure	R53 Resolver logs	Forwarding rules, PHZ association, VPC DNS flags
VPN tunnel down	CW TunnelState	IKE params mismatch; DPD settings; PSK
DX high latency	CW ConnectionBps	Asymmetric BGP routing; check MED/AS_PATH
NAT port exhaustion	ErrorPortAllocation	Deploy more NAT GWs; 55K conn limit per dst
Connection resets over DX	Traffic Mirroring	TCP RST/retransmit; check MTU/jumbo frame config
Unintended exposure	Network Access Analyzer	SG 0.0.0.0/0 inbound; public subnet placement

Automation & Compliance

- AWS Config "restricted-ssh": detects SG with 0.0.0.0/0 on port 22 → NON_COMPLIANT
- Config auto-remediation: SSM Automation AWS-DisablePublicAccessForSecurityGroup
- Config "vpc-flow-logs-enabled": marks VPCs without Flow Logs NON_COMPLIANT
- CloudFormation Drift Detection: finds manual changes; trigger via EventBridge
- Reachability Analyzer in CI/CD: fail pipeline if NetworkPathFound=false post-deploy
- GuardDuty UnauthorizedAccess:EC2/TorClient: auto-detects Tor exit node connections
- Centralize Flow Logs: S3 bucket in security account + Athena for SQL queries
- Route 53 Health Checkers: allow inbound from ROUTE53_HEALTHCHECKS IP ranges in SG

D4 · NETWORK SECURITY & COMPLIANCE 24%

Security Control Layers

Control	L	Stateful	Scope	Key Feature
Security Group	L4	Yes	ENI	Allow only; SG-to-SG refs
NACL	L3/4	No	Subnet	Allow+Deny; rule number order
Network Firewall	L3-7	Both	VPC	Suricata IPS; domain filter; TLS inspect
WAF	L7	Yes	ALB/CF	HTTP; managed rules; rate-based
Shield Advanced	L3-7	Yes	Acct	DDoS+DRT+cost protection
Firewall Manager	All	Both	Org	Central mgmt; auto-covers new accounts

NACL Rules — Critical Facts

- Stateless: MUST allow BOTH inbound (port 443) AND outbound (ephemeral 1024-65535)
- Rule evaluation: ascending number order; first match applied; * = deny-all fallback
- Lower-number DENY overrides higher-number ALLOW for same traffic
- Default NACL: allows all. Custom NACL: denies all by default.
- NACLs evaluated BEFORE Security Groups; NACL deny blocks before SG is reached

AWS Network Firewall

- Stateless rules: fast per-packet L3/L4 pass/drop; processed first
- Stateful rules: Suricata IPS/IDS; connection-tracked; domain-based filtering
- Domain filtering: SNI inspection for HTTPS; blocks *.facebook.com without IP lists
- TLS inspection: ACM Private CA cert; decrypt-inspect-re-encrypt outbound HTTPS
- Centralized: all spoke traffic → TGW → inspection VPC w/ NF → internet
- Distributed: NF in each VPC; independent control; higher operational cost
- Firewall Manager: deploy NF policy org-wide; auto-covers new accounts
- Alert logs: rule match events with rule group name, rule ID, packet details

AWS WAF & Shield

Feature	Description
Managed rule groups	AWS+Marketplace: SQLi, XSS, CommonRuleSet, OWASP Top 10
Rate-based rule	Auto-block IPs > threshold req/5-min; min 100 req; auto-unblock
Geo match	Block/allow by country for compliance or DDoS mitigation
Bot Control	Detect/challenge bots; managed add-on rule group
Shield Standard	FREE; automatic L3/L4 DDoS protection for all resources
Shield Advanced	$3K/month org; L7+WAF; 24/7 DRT; DDoS cost protection

Encryption in Transit

Method	Layer	Use Case
MACsec	L2 (wire)	Dedicated DX; AES-256-GCM; MKA key protocol
IPSec / VPN	L3	Site-to-Site VPN tunnels; AES-256-GCM
TLS / ACM	L4-L7	ALB, CloudFront, API GW; free public certs
NF TLS Inspect	L7	Network Firewall decrypt-inspect-re-encrypt
AWS internal	L2 (HW)	All EC2 traffic encrypted at NIC within region

Data Exfiltration Prevention

- VPC endpoint policy: aws:ResourceOrgID blocks S3 writes to external buckets
- SCP + aws:SourceVpc: restrict S3/DynamoDB access only from approved VPCs
- Interface Endpoint private DNS: prevents resolution to public service IPs
- Network Firewall domain filtering: block uploads to unauthorized external domains
- VPC Flow Logs + GuardDuty: detect and alert on anomalous data transfer patterns

MASTER QUICK REFERENCE — KNOW THESE COLD

Service / Concept	Dom	The Key Fact to Remember
Transit Gateway	D1	Hub router; 5,000 VPC attachments; multiple route tables for segmentation; TGW peering uses private backbone
VPC Peering	D1	Non-transitive; no CIDR overlap; 45 connections for 10 VPCs; only 2 VPCs: peering OK, 3+: use TGW
PrivateLink	D1	NLB-backed endpoint service; Interface Endpoint in consumer VPC; no CIDR overlap needed; cross-account
Shared VPC (RAM)	D1	Host shares subnets to participant accounts; participants deploy into shared subnets; centralized network mgmt
Route 53 Resolver Inbound	D1	ENIs in VPC; on-prem DNS forwards queries to ENI IPs to resolve AWS private hosted zones
Route 53 Resolver Outbound	D1	Forwarding rules route corp.internal → on-prem; rules shared via RAM to all spoke VPCs
Global Accelerator	D1	Anycast static IPs; nearest PoP entry; AWS backbone routing; TCP/UDP; NOT HTTP caching (that is CF)
Egress-Only IGW	D1	IPv6 outbound-only; blocks inbound IPv6; ::/0 route entry; equivalent of NAT GW but for IPv6
VPC reserved IPs	D1	5 per subnet: .0 network, .1 router, .2 DNS, .3 future, .255 broadcast; /24 = 251 usable IPs
R53 Latency routing	D1	Uses resolver location not user IP; user in Singapore may go to us-east-1 if resolver is there
ALIAS vs CNAME	D1	ALIAS can be at zone apex; CNAME cannot; ALIAS queries free; ALIAS points to AWS resources
BGP MED	D1	AWS sets MED; lower MED = preferred path; influences on-prem inbound path selection
AS_PATH prepend	D1	On-prem sets; longer path = less preferred by AWS; influences AWS egress path to on-prem
DX Private VIF	D2	VGW (single VPC) or DXGW; BGP private ASN; 100-route limit
DX Transit VIF	D2	DXGW → TGW; one Transit VIF per DX connection; reach thousands of VPCs
DX Public VIF	D2	AWS public service endpoints (S3) over DX link; 1,000-route limit; public BGP ASN
DX Maximum Resiliency	D2	2 DX locations × 2 connections = 4 total; 99.99% SLA; different devices per location
MACsec	D2	IEEE 802.1AE L2 AES-256-GCM; dedicated DX only; MKA key protocol; wire-level encryption
BFD on DX	D2	Sub-second failure detection vs 90s BGP hold; required for fast DX → VPN failover
VPN ECMP via TGW	D2	4 VPN × 2 tunnels × 1.25 Gbps = 10 Gbps aggregate; same prefix on all tunnels required
GWLB	D2	GENEVE port 6081; Ingress Route Table on IGW; appliance fleet for N-S inspection; bump-in-wire
NLB source IP	D2	Native preservation for instance targets; Proxy Protocol v2 for TCP targets needing header
ALB LOR	D2	Least Outstanding Requests; routes to instance with fewest in-flight requests; better for variable-cost workloads
VPC Flow Logs	D3	Metadata (IPs/ports/bytes/ACCEPT-REJECT); NOT packet content; S3+Athena for SQL analysis
Traffic Mirroring	D3	Full packet capture from ENI → NLB/ENI target; for IDS/IPS/forensics; filter by port/proto
Reachability Analyzer	D3	Logic path analysis; no traffic sent; ONE specific path; API in CI/CD = fail on false
Network Access Analyzer	D3	All resources matching pattern at scale; find ALL EC2s open on port 22 across VPC
NAT GW port limit	D3	55,000 connections per unique dst IP:port; ErrorPortAllocation metric; add more NAT GWs
R53 Health Checkers	D3	Originate from specific IP ranges; allow ROUTE53_HEALTHCHECKS in SG or health checks fail
Security Group	D4	Stateful; ENI-level; allow only; SG-to-SG refs for tier segmentation; return traffic auto-allowed
NACL	D4	Stateless; subnet-level; allow+deny; MUST allow ephemeral ports 1024-65535 outbound; rule order matters
NACL vs SG order	D4	NACL evaluated first at subnet; if NACL denies, packet dropped before SG is even reached
Network Firewall	D4	Suricata IPS; domain filtering via SNI; TLS inspect (ACM Private CA); centralize via TGW inspection VPC
WAF rate-based rule	D4	Auto-block IPs > threshold per 5-min; min 100 req; auto-unblock when rate drops; no manual action
Shield Advanced	D4	$3K/month org; L7 DDoS+WAF; 24/7 DRT proactive; cost protection; use Firewall Manager for org
Firewall Manager	D4	Centrally manage WAF+Shield+SG+NF+DNS Firewall org-wide; auto-applies to new accounts/VPCs
VPC Endpoint Policy	D4	IAM resource policy on endpoint; aws:ResourceOrgID prevents data exfil to external S3 buckets
AWS-internal encryption	D4	All EC2 traffic encrypted at L2 (NIC hardware) within same region; no customer action needed

EXAM TIPS: 750/1000 to pass | 65 Qs | 170 min | No penalty — guess all | Mark & review

HOT TOPICS: TGW route tables | DX VIF types | Resolver hybrid DNS | NACL stateless | NF Suricata domain rules

ALWAYS: TGW > peering | PrivateLink for CIDR overlap | MACsec L2 | NF before WAF for VPC | Shield Adv for L7 DDoS