Design and implement AWS networks

VPC Flow logs

- Not a packet capturing tool
- source
- destination
- port numbers
- protocol
- number of packets
- number of bytes
- start/end time
- Attached to VPC, Subnets, or ENIs
- Flow logs capture ingress and egress traffic
    - log accepted
    - log rejected
    - log all traffic
- Not real time
- Logs in Cloudwatch or S3 (IAM role)
    - Cloudwatch (each flow logs = log group, each ENI = log stream)
    - S3 (use default or custom formatting for logging output)

Reading VPC Flow Logs

Important: Source/destination addresses will always be the internal primary private ip address associated with the EMI

```
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status

2 442771530490 eni-0c6c500f8e6722890 185.137.233.160 172.31.16.38 54693 22 6 12 900 1568321893 1568321953 ACCEPT OK
```

Not captured in VPC Flow Logs:

- AWS DNS
- License Activation

- Metadata from 169.254.169.254
- Amazon Time Sync Service
- AWS DHCP and Reserved IP Addresses (VPC router)
- Traffic between Endpoint ENI and NLB ENI

Network performance

Options for High Compute Network performance:

- Instance types with enhanced networking
- Placement Groups (using clustering placement groups packs the instances close together)
  - Cluster <=
  - Partition
  - Spread
- Enabling Enhanced Networking (support 9001 MTU or jumbo frames)

Configure Network Integration with Application Services

VPC DHCP

- Client (UDP 68)
- Server (UDP 67)
- Discover
- Offer
- Request
- Acknowledge

Reserved Addresses

- .0 Network Address
- .1 VPC Router (including DHCP)

- .2 Reserved for DNS
- .3 Future Use
- .255 Broadcast

DHCP Option Sets

Only 1 DHCP option set per VPC

- Domain name (custom domain name for internal use)
- Domain name servers
- NTP servers
- NetBIOS name servers
- NetBios node type

Elastic Load Balancer ALBs, NLBs and Classic

- External or Public facing loadbalancers
  - public subnet
  - subnet must be sized /27 or larger (you cannot use /28 or smaller)
  - the subnet must have at least 8 available IP addresses
- Internal Load balancer (private VPC)

ALBs and NLBs support SNI or the ability to have multiple certificates per listener. CLBs do not.

Cloudfront

- You can have only 1 geo restriction per distribution
- Either whitelist or blacklist
- You can also configure WAF to block
- Geo restriction only by country
- OAI - Origin Access Identity (when a private s3 bucket is used)

Cloudfront Behaviors

- HTTP, HTTPS, Redirect HTTP to HTTPS

- Allowed HTTP methods (GET, HEAD, OPTIONS, ...)
- Field-level encryption (extra security layer on top of https)
- Cached HTTP Methods
- Cache Based on Selected Request Headers
- Object caching
    - Use Origin Cache Headers
    - Customize
    - TTL settings
    - Forward Cookies
    - Query String Forwarding and Caching
    - Smooth Streaming
    - Restrict Viewer Access (Use signed urls or signed cookies)
    - Compress Objects Automatically
    - Lambda Function Associations

Signed URLS and Cookies

- Signed URLS: Supported by web and RTMP origins. Used to control access to individual files. Signed Urls will change your url
- Signed Cookies: Is only supported by web origins and allows access for large groups of files. Urls are not changed.
- Origin Access Identities (OAI): Restrict Access to an S3 bucket to only a special Cloudfront user associated with you distribution.

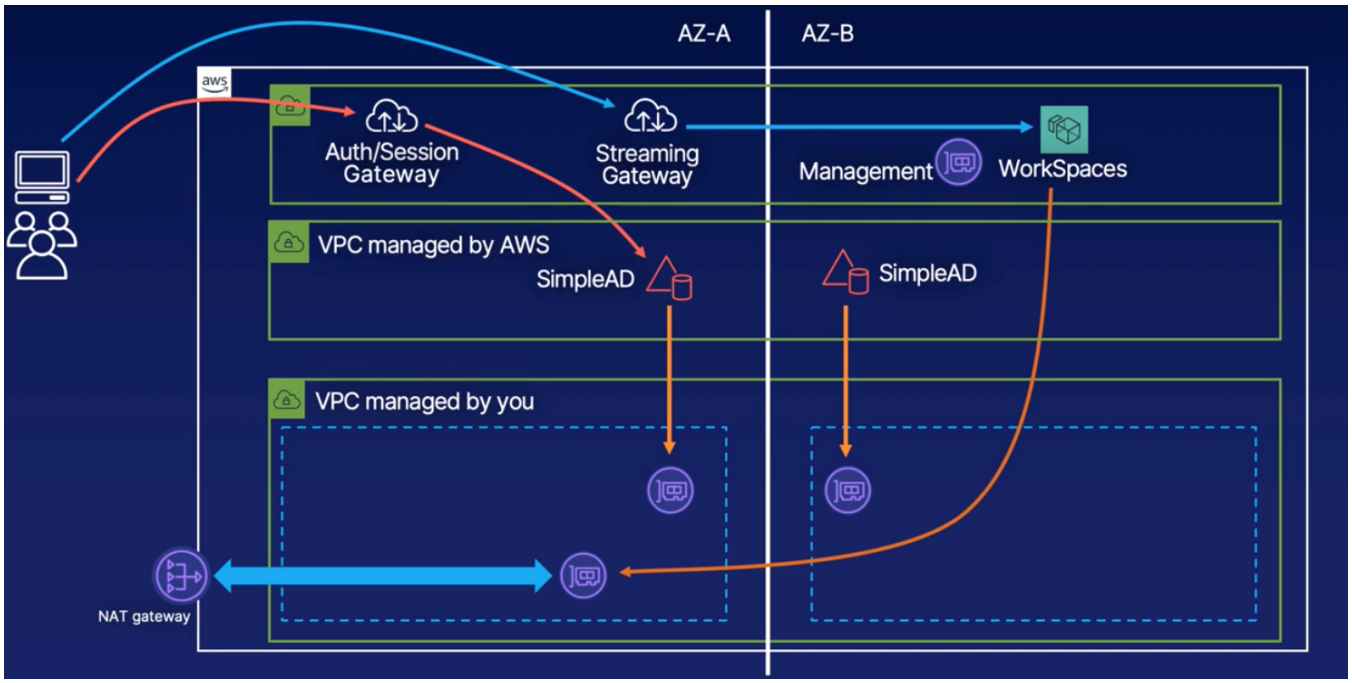
SSL/TLS encryption

- AWS Certificate Manager
    - Default Cloudfront Certificate
    - Custom SSL Certificate
    - If using ELB as origin (certificates must be issued with ACM)
    - If not using an ELB, certificates must be issues by a CA

Lambda@Edge

VPC Enpoint Services with AWS PrivateLink

Amazon Workspaces



- Desktop as a service (Windows desktop)
- spin up in minimum 2 AZs
- VPC managed by AWS (won't see vpc)
- ENIs will be launched in our VPCs (connected to SimpleAD)
- Another ENI for connecting to WorkSpaces (public IP or private IP)
- Subnet max /17 to min /28 CIDR subnet (Reserve 5 IP addresses in each subnet + 1 Directory service address in each subnet)
- Private ip use NAT translation (additional IP)
- As a Directory Service you can use:
  - AWS Managed Microsoft AD
  - Simple AD
    - small - 500 users, 2000 objects
    - large - 5000 users, 20000 objects
  - AD Connector (Proxy for redirecting requests to existing AD without caching information)
- 1 Directory can only be linked to 1 Workspace

Amazon AppStream 2.0

- Managed Application Service (3D design, Adobe, IDEs, ...)
- You should use 2 AZ's
- You should see an ENI
- AD or SAML authentication

Chapter 4: Hybrid Networking Basics and VPN's in AWS

Virtual Private Gateway

Send traffic to the outside world:

- Internet Gateway
- Virtual Private Gateway <=
- Transit Gateway

What is Virtual Private Gateway:

- Acts as a router between you VPC and non-AWS-managed networks
- Can be associated with multiple external connections
- Can be attached only to one VPC at the time

2 types of connections:

- Site-to-Site VPN
- Direct Connect

Configuration:

- assign a name
- assign an ASN
- attach to a VPC
- once created, properties can't be modified

ASN:

- public ASN numbers => controlled by IANA
- private ASN numbers (64512 - 65534) (4200000000+)
- 16 bit and 32 bit
- default for VGW is 64512

AWS Hybrid Route Learning

2 route learnings:

- static (manual configured)
- dynamic (routing protocols => BGP)

Site-to-Site VPN:

- static
- dynamic

Direct Connect:

- only dynamic

Route propagation:

- Can be enabled in route table propagation tab
- All routes learned by the VGW are shared with the route table

When networks overlap:

- Most specific route is usually preferred, but VPC local is always preferred over any overlapping propagated routes
- VPC static routes are preferred over matching propagated routes
- Direct connect > Static VPN > BGP VPN

Border Gateway Protocol

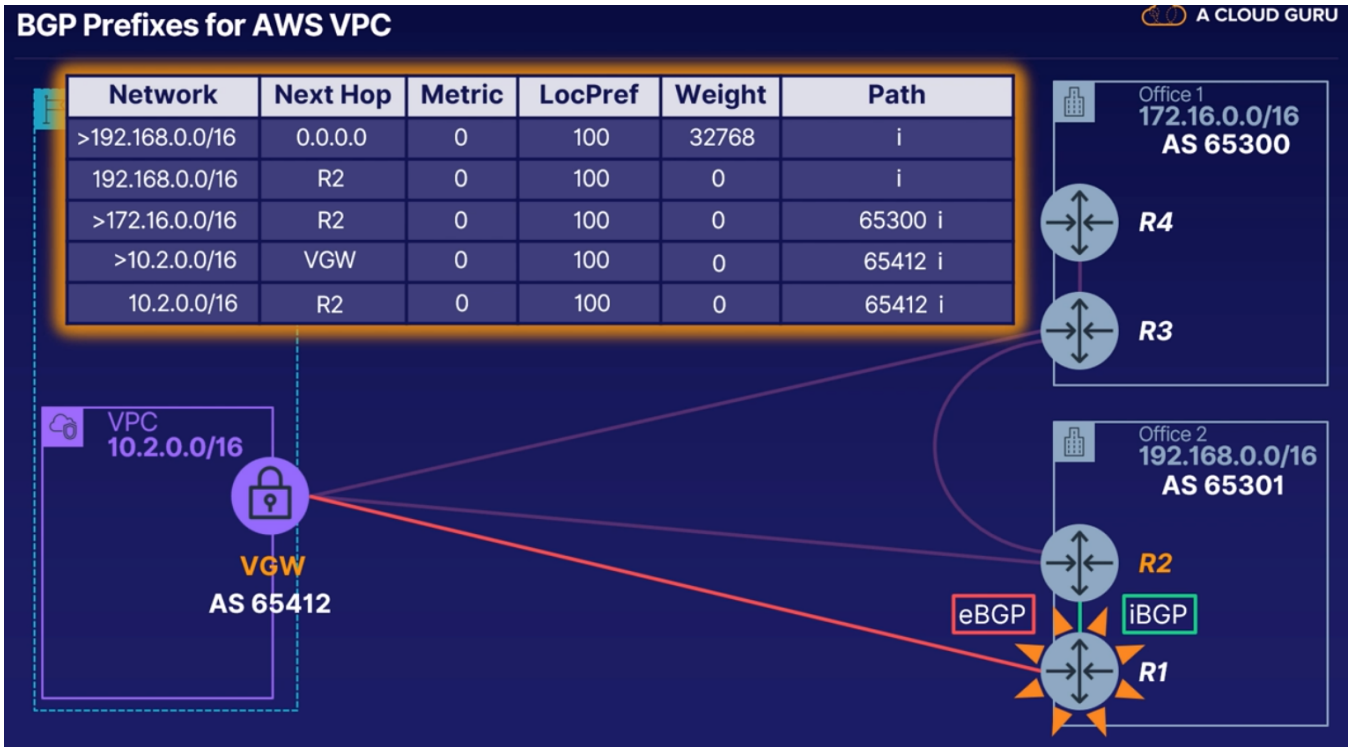
- TCP port 179
- eBGP exterior

- iBGP interior (between 2 BGP routers within the same AS)
- BGP peering and network advertisement must be manually configured.
- Does not care how peering are physically connected

BGP Prefixes and Preferences

BGP table:

- Network (which network it is directly connected to)
- Next Hop (router id or 0.0.0.0)
- Metric (default 0)
- LocPref (default 100)
- Weight (default 32768, weight 0 if learned)
- Path (default i <= internal route)



Selection best route:

1. Heighest weight
2. Highest Local Preference
3. Shortest AS Path

4. eBGP preferred over iBGP
5. Lowest Metric Value

- Only the best route is shared for a connection
- VGW automatically shares all it knows

CloudHub

Enables VGW to automatically advertise learned BGP routes over all connection supporting dynamic routing.

BGP Prefix Preference Control

BGP cannot sense network quality

- heighest weight is only used on the local BGP router (not shared)
- heighest local preference is shared only to other iBGP routers with the same ASN (remember to change the weight to 0 on the other router)
- VGW cannot not be configured => How can we modify the traffic?
    - on the on premise router, configure the path you don't want to be preferred
    - prepend-path your path with an additional entry of the same ASN (max 16 times)
        - This is parmenent! and is advertised to other possible connected BGP routers
    - An alternative to pathprepending, increase the metric of the path you don't prefer (only shared with peered BGP routers)

VPN and IPSec Overview

2 VPNs:

- Site-to-Site VPN (tunnel)
- Client-to-Site VPN
- AWS only support IPSec VPN tunnels
- VPN endpoint systems on each network must be pre-configured:
    - Identity of other endpoint

    - Shared authentication method
        - pre-shared string
        - pre-shared certificate
        - PKI infrastructure using assymetric keys
    - Security policies
    - Kind of traffic:
        - Policy-based
        - Route-based

Sequence of events:

- "interesting" traffic is detected by the local endpoint
- Internet Key Exchange (IKE) phase 1 (main mode)
    - negotiate a security policy for key exchange
    - perform the key exchange (Diffie-Hellman)
    - Mutually encrypted authentication (test)
    - a single 2 way connection
- IKE phase 2 (Quick mode)
    - no re-authentication
    - generate of refresh keys (symetric keys)
    - 2 one way connection
- IPSec tunnel is established
- IPSec tunnel is terminated if no traffic is flowing anymore

Security Associations:

- Policy-based:
    - Admin-configured rule sets define VPN-permitted traffic and security settings
    - One security association created per matched rule set
- Route-based:
    - Traffic must target destination network to use VPN
    - Only a single security association is created for all traffic.

Site-to-Site VPN:

- The IPSec process is identical
- Tunnels are only established by traffic flowing from on-prem to AWS!
- AWS VPN tunnels can only support a single pair of IPSec security associations.
- only supports IPv4 and IPSec

Customer Gateways

AWS Site-to-Site VPN components:

- Configure VGW or TGW
- Confirm CGD (Customer Gateway Device) meets requirements
- Configure CGW (Customer Gateway)
- VPN Connections
- Configure VPC Route tables
- Configure VPN settings on CGD (download configurations text file)

Customer Gateway Device Requirements

- must support IKE (IKEv2) (Internet Key Exchange)
- must support IPSec
- must be accessible by a static public IPv4 address
- Must support Dead Peer Detection
- BGP support is optional
- Inbound/Outbound Firewalling:
  - UDP 500
  - IP Protocol 50
- You can use NAT-Traversal behind firewall
  - include UDP 4500

Customer Gateway Configurations Parameters

- Name-tag value
- Dynamic or static routing (if Dynamic ASN number)
- CGD public ipaddress (or NAT-T if used)
- Optional Assign an ACM generated certificate for IKE authentication (used for phase 1)

Configure VPN connection

- Name-tag value
- VGW ID
- CGW ID
- Dynamic or static routing
- Tunnel options as desired (or default)
    - Pre-shared keys (default 12 chars)
    - IP CIDR for both tunnels (must be /30 in the 169.254.0.0/16 CIDR block)
    - tunnel lifetime
    - key lifetime
    - Encryption mechanisms
- Routes are propagated by the VGW as soon as the VPN connection is established
- AWS creates 2 tunnel endpoints in different AZs per VPN connection (Active/Passive mode) => Dead peer connection
- Both endpoints need to be configured at the CGD

Configure VPN settings on CGD

- Download Configuration from VPN connection
- Select your Device software

AWS VGW and VPN Limitations

1. VGW are not VPC transitive (VGW is attached to one vpc and does not know of other VPCs peered to this VPC) => solution: created another VGW for the other VPCs
2. VGW VPN throughput is capped to 1.25 Gbps (Attaching another won't fix this issue, this will half the throuhput of the first and second connection)
3. VGW always used a single VPN tunnel endpoint when returning traffic to a network
4. Each AWS VPN IPSec tunnel only supports a single pair of one-way security associations (Use a single policy matching all possible VPN traffic or use route-based

VPN)

5. AWS S2S VPN only supports IPSec
6. AWS S2S VPN only supports IPv4
7. AWS S2S VPN cannot receive client-to-sit connections.

Solutions

- All can be solved by using Software VPN on EC2
  - For issue 1. Transitive networking, the route table can direct traffic to other peered VPC using the route table it runs in.
- 1, 2, 3 can be solved using TGW

Traffic Isolation within VPC

- point to point VPN connections between ec2
  - named overlay network
  - Provide encryption
  - multicasting
- By default only unicasting is supported (overlay network solves this issue)

AWS Client VPN service

- managed openVPN service
- VPN endpoint for client to site connections
- Authenticate via Active Directory or private certificates (imported in ACM)
- Controlled access to VPC and anything connected to that VPC
- Client VPN Split tunneling can be configured so that only matching routes are send through the VPN (Default all traffic is send through the VPN)
- openvpn file shared with the client

AWS VPN Monitoring and Optimization

Is it working as we expect?

- Cloudwatch metrics
  - TunnelState (1/0)

    - TunnelDataIn
    - TunnelDataOut
    - Dimensions: per VPN connection, per tunnel endpoint, or over all tunnels
    - For EC2 (standard metrics EC2), custom metric through cloudwatch agent
- Cloudwatch Logs
    - VPC flowlogs
    - EC2 - published log streams
    - AWS Client VPN authentication attempts (enable)

Can performance be improved?

- managed controlled by AWS
- EC2 software based (instance type - enhanced networking)

What can make it stop working?

- Misconfigurations:
    - Security groups
    - NACLs
    - Authentication
    - Customer Gateway Devices
    - OpenVPN client configuration
    - IAM insufficient permissions
- Hardware failure
    - Dead peer connections
    - Customer Gateway (Setup 2 Customer Gateway for high availability) => max throughput issue
    - EC2 software VPN (high availability)
- Client 2 Site VPN
    - Attach VPN endpoint to at least 2 subnets

AWS VPN Cost Optimization

- AWS VPN Connection: 0.05/hour
- Customer Gateway: Cost?
- Client VPN => VPN endpoint subnet association: 0.10/hour double for HA

- Client VPN connection time: 0.05/hour per client
- EC2 software VPN: EC2 cost HA

AWS Direct Connect and Hybrid DNS

When VPN is not a solution:

- Established connection only from on-prem to AWS
- VPN traffic used public infrastructure
- VPN's "out to internet" data transfer billing
- VGW is limited to maximum of 1.25 Gbps for all VPN connections

DX connections:

- always on in both directions
- Dedicated infrastructure
- Reduced rates for Data transfer
- Flat hourly port charge
- 10 Gbps max speed
- Multiple connections/simultaneously

Hybrid DNS:

- private DNS resolutions on-prem/AWS

AWS Direct Connect Locations & Hardware

- Dedicated high throuput low latency connection to an AWS Region
- Access via globally places DX locations (Gov included)
  - Own hardware implementation in DX location
  - Work with DX partner
- Customer traffic is isolated using VLANs

Requirements:

- Single-mode fibre
- Either 1000BASE-LX (for 1 Gbps) or 10GBASE-LR (for 10 Gbps) transceivers

- Disable auto-negotiation on all ports used with DX
- 802.1Q VLAN encapsulation must be supported across entire connection
- Devices must support BGP and BGP MD5 authentication
- Bidirectional Forwarding Detection (BFD) is supported but not required

Customer responsible for connecting their on-prem to DX Location. DX location Hardware depends using your own or partner

DX Connections

Dedicated Connections

- AWS hardware at DX Location connects directly to customer-managed hardware at DX location
- Support either 1 Gbps or 10 Gbps connection speeds to AWS Region
- Soft limit of 10 dedicated connections per Region, per account

How:

- Create new connection request using Console, CLI or API
- Information:
  - Name tag
  - DX location
  - Sub-location if applicable
  - Port speed
  - Direct Connect Partner if applicable
  - Optional additional tags
- New requests may take up to 72 hours for AWS to process
- Only tags and its values can be modified afterwards
- Letter of Authorization - Connecting Facility Assignment (LOA-CFA)
  - Authorizes DX location to connect your hardware to a specific port on AWS-owned hardware
  - Valid for 90 days
  - Contact AWS support if download link is not available after 72 hours

- Send LOA-CFA to DX location to initiat the process (send to AWS DX Partner if applicable)

Hosted Connections

- AWS hardware at DX location connects directly to AWS DX Partner-managed hardware
- Wider range of bandwith options:
  - Mbps - 50 - 500
  - Gbps - 1 -10 (only supported by certain partners)

Once AWS Partner creates the connection, it must be accepted by the AWS customer.

Virtual Interfaces

Private VIF:

- connects to VGW
- connects to a single Direct Connect Gateway (multiple regions)

Transit VIF:

- connecting DX to TGW

Public VIF:

- AWS public services (like S3)

L2 networks can be logically devided into VLAN's

VIF configuration:

- VIF type
- VIF name
- DX connection name
- VIF owner
- Gateway (private and transit VIFs)
- VLAN ID
- BGP ASN
- other BGP settings

- Jumbo MTU (private and transit VIFs)
- Tags

After creation:

- only tags may be edited afterwards
- Router configuration file may be downloaded

DX dedicated connections support:

- Up to 50 public or private VIFs
- Only 1 Transit VIF
- Hard limits

DX hosted connections only support a single VIF

A Hosted VIF:

- share that connection with other accounts
- allows a DX connection owned by one AWS account to be used by a different account.
- are created by the owner of the DX connection and offered to the other AWS account.
- the router configuration file can only be downloaded by the creator, not the consumer.

Virtual LANs

VLANs needs to be configured at DX location and on-prem.

untagged/access ports => Ports belonging to a single VLAN

Traffic entering an untagged port may only be sent to another port that is a member of the same VLAN

tagged/trunk ports => ports belonging to more than 1 VLAN (used for communication between switches)

untagged ports:

- send traffic with standard ethernet frame
- knows the VLAN by the ingress port

tagged ports:

- traffic leaving a tagged port is using a 802.1Q ethernet frame
- contains 802.1Q Tag

Hosted DX connection only supports one VIF:

- establish multiple hosted DX connections
- Use aggregated VLANs!

Aggregated/Nested VLANs

- On-prem and DX location devices are configured to recognize a specific "type" of VLAN tag
- Tagged traffic with configured type is handled normally (8100 default to most switches)
- Tagged traffic of any other type is treated as untagged traffic

At the provider incomming traffic from Customer VLAN:

- the 802.1Q Tag Frame is not recognized and is again encapsulated with an 802.1Q frame to forward traffic within the VLAN of the provider switches.

Virtual Interfaces & BGP

BGP Prefix Advertisements

Customer to AWS:

- VIFs have maximum number of prefixes that can be advertised:
  - Private VIFs - 100
  - Public VIFs - 1000
- Exceeding this limit will cuase the BGP sessions to go to the IDLE state

AWS to Customer:

- VGWs associated with private VIFs advertise all known routes.
- VGWs associated with DX gateways must specify allowed prefixes to be advertised.

    - Only CIDRs matching - or smaller than - listed prefixes will be advertised
- For public VIFs, AWS advertised prefixes for:
    - All public services in all public AWS Regions
    - Non-Region services such as Cloudfront and Route53
- Control outbound traffic to these prefixes at your on-prem router.
    - Filter outbound traffic with ACLs or firewalls
    - Filter learned prefixes using BGP communities

BGP communities:

- A means of labelling BGP prefixes
- BGP routers can be configured to handle incoming or outgoing prefixes based on their community values.
- Comprised of 16-bit ASN and a 16-bit, organization-defined number.

AWS automatically applies the following communities to prefixes advertised to public VIFs:

- 7224:8100 - routes to services from the same region as the DX connection.
- 7224:8200 - routes to services from the same continent as the DX connection.
- No value - routes to global services.

AWS advertised prefixes also include the “no_export” BGP community.

Customer to AWS:

- Customer prefix advertisement is controlled at public VIF
- Use BGP communities to control where AWS can propagate customer prefixes:
    - Local AWS Region - 7224:9100
    - All Regions in a continent - 7224:9200
    - All Public Regions - 7224:9300

Link Aggregation Groups (LAGs)

What:

- A collection of multiple physical links combined into a single, logical link.

- Traffic sent to the LAG is distributed across all member links.
- Aggregates throughput of member links.
- Provides resiliency in the event of member link failure.

Requirements:

- All DX connections in a LAG must:
  - Use the same bandwidth.
  - Terminate at the same DX location.
- Maximum of four connections per LAG.
- Maximum of 10 LAGs per Region.

Creation:

- Use existing connections, request new connections, or a mix of both.
- You cannot create a LAG with new connections if you would exceed the overall connection limit for the Region.
- Adding existing connections to a LAG will temporarily interrupt connectivity.

Properties:

- LAG name
- Existing connections to use
- Number of new connections to request
- Minimum links
- Optional tags.
- Minimum links identifies the minimum number of functional connections necessary for the entire link to be functional.
  - If the number of active links drops below the minimum, the entire LAG connection will become non-operational.
  - Default value is 0 (no minimum).
- New or existing connections may be added to existing LAGs.
- Connections may not be removed from LAGs if it crosses the minimum links threshold.

LAGs and VIFs:

- VIFs may be attached to a LAG instead of a single DX connection.

- VIFs may be attached to a LAG instead of a single DX connection.
- A corresponding customer LAG must be created at the on-prem hardware. (see diagram ACG)
- Add LAG primary port to VIF VLAN.

Direct Connect Gateways

- Global services that facilitate DX connectivity to multiple AWS regions
- A bridge between Private or Transit VIFs and AWS networking objects
- No interaction with public VIFs
- Free to use

Private VIFs and DX Gateways

- By itself, a private VIF can only connect to a single VGW
- DX gateways may connect a single private VIF with up to 10 VGWs in any public region
- Up to 30 private VIFs may connect to the same DX gateway

How to connect to different regions

- Create a private VIF
- Connect that private VIF to a DX gateway
- Associate DX gateway to with the VGWs that are attached to the VPC in the different regions.
- VPCs connecting through a DX gateway cannot have overlapping IP ranges
- Only sessions via a single VIF to one connected VPC at a time are allowed. (f.e. multiple VIFs talking to the same VPC)
- You cannot send traffic:
  - from one associated VPC to another
  - from one connected VIF to another
  - from a connected VIF through a VPN connection using an associated VGW

DX Gateways and Transit VIFs

- DX gateways are also used when attaching DX connections to Transit Gateways
- Attach a Transit VIF to the DX gateway that is then attached to a Transit Gateway

- A DX Gateway may connect with either:
  - Private VIFs and VGWs
  - Transit VIFs and TGWs
  - but noth both !!!

Other stuff to know about DX Gateways

- VGWs in one AWS account may request association with a DX gateway in a different account.
- DX gateways may only be associated with VGWs attached to a VPC
- Each VIF and VGW may only be associated with a single DX gateway
- A VGW can be simultaneously attached to both a single private VIF and a single DX gateway (connected to a different private VIF)
- DX Gateways may be associated to up to 3 TGWs

Configure DX Gateway

- Name
- Amazon side ASN
- Attach to VIF
- Associate with VGW or TGW

Well-architected Direct Connect

(see slides)

Hybrid DNS

- Private DNS resolution across hybrid networks:
  - AWS resources are able to use on-prem DNS zones.
  - On-prem resources are able to use Route53 private zones or VPC DNS

Route53 Resolver

- Provides default DNS resolution within VPCs
- "VPC + 2" IP address.

- Part of EC2 service hardware
  - Good availability and performance (cache within AZ)
  - Only accessible froom within AWS infrastructure
- Route 53 Private Zones must be associated to VPCs
- Resolver search sequence:
  - Route 53 Private Zones
  - VPC DNS domain
  - Public DNS

The hybrid DNS Challenge

- EC2 instances always use Route 53 Resolver by default
- On-prem systems cannot reach Route 53 Resolver

Customer-implemented DNS Resolvers

- EC2 hosted DNS resolvers are provisioned within VPC
- VPC configured to use EC2 resolver instead of Route 53
- Resolver forwards matching request to on-prem DNS
- On-prem DNS resolvers configured to forward matching request to EC2 resolver
- AWS Directory services Simple AD can provide the same functionality
- Configure on-prem DNS to forward to Simple AD DNS addresses.

Problems

- Single Ec2-ENI limited to 1024 queries/sec
- only 1 AZ, you would need HA
- Most DNS clients don't load-balance across multiple servers.
- DNS resolver services can loadbalance

Route53 Resolver Endpoints

- Provides IP accessible endpoints to the AWS Route 53 Resolver service.
- Enpoints support 2 to 8 ENIs

- Each ENI supports up to 10.000 queries/second
- Endpoints are created within a single VPC, but may be used by other VPCs in the same Region
- Secured by a single VPC security group
    - Group assignment cannot be changed after creation.
- Each endpoint can handle either inbound or outbound DNS requests.
- Endpoint ENI's are AZ-scoped resources (use-multi-az)
- ENIs use either dynamic or customer-assinged IP addresses
- IP addresses are persistent for the lifetime of the endpoint
- Pricing per ENI, per hour

Inbound Endpoints

- Handles request forwarding from on-prem to AWS DNS resolver
- Requests are sent to the IP address fo an ENI
- Request from on-prem DNS resolver instead of client for better performance
- Private hosted zones must be associated to the VPC where resolver endpoints reside

Outbound Enpoints

- Handle forwarding for requests originating within AWS
- Can be associated with multiple VPCs in a Region
- Specify forwarding action for requests matching defined FQDN Patterns.
- Forward rules forward requests to IPv4 address of on-prem DNS
- System rules forward requests to Route 53 Resolver

Traffic rules

- System rules are automatically created for:
    - Private hosted zones
    - VPC domain names
    - Publicly reserved domain names

If rules conflict, resolver prefers:

- Most specific FQDN

- Forward rules over system rules

Transitive Networking

Inter-VPC connectivity

VPC Sharing

VPC sharing allows a subnet in one AWS account to be shared with other AWS accounts:

- Accounts must be part of the same AWS Organization.
- Subnets are shared via AWS Resource Access Manager.
- Once shared, other accounts may provision resources within that subnet as if it were native to their account.
- Only the owner account has management control over that subnet.

VPC Peering

- VPC peering connections do not allow transitive connectivity.
- VPC peering is not restricted by AWS account or region.
- Data transfer charges apply to inter-VPC traffic.
- Minimum required configuration allows broad inter-VPC connectivity. (all access to that vpc)

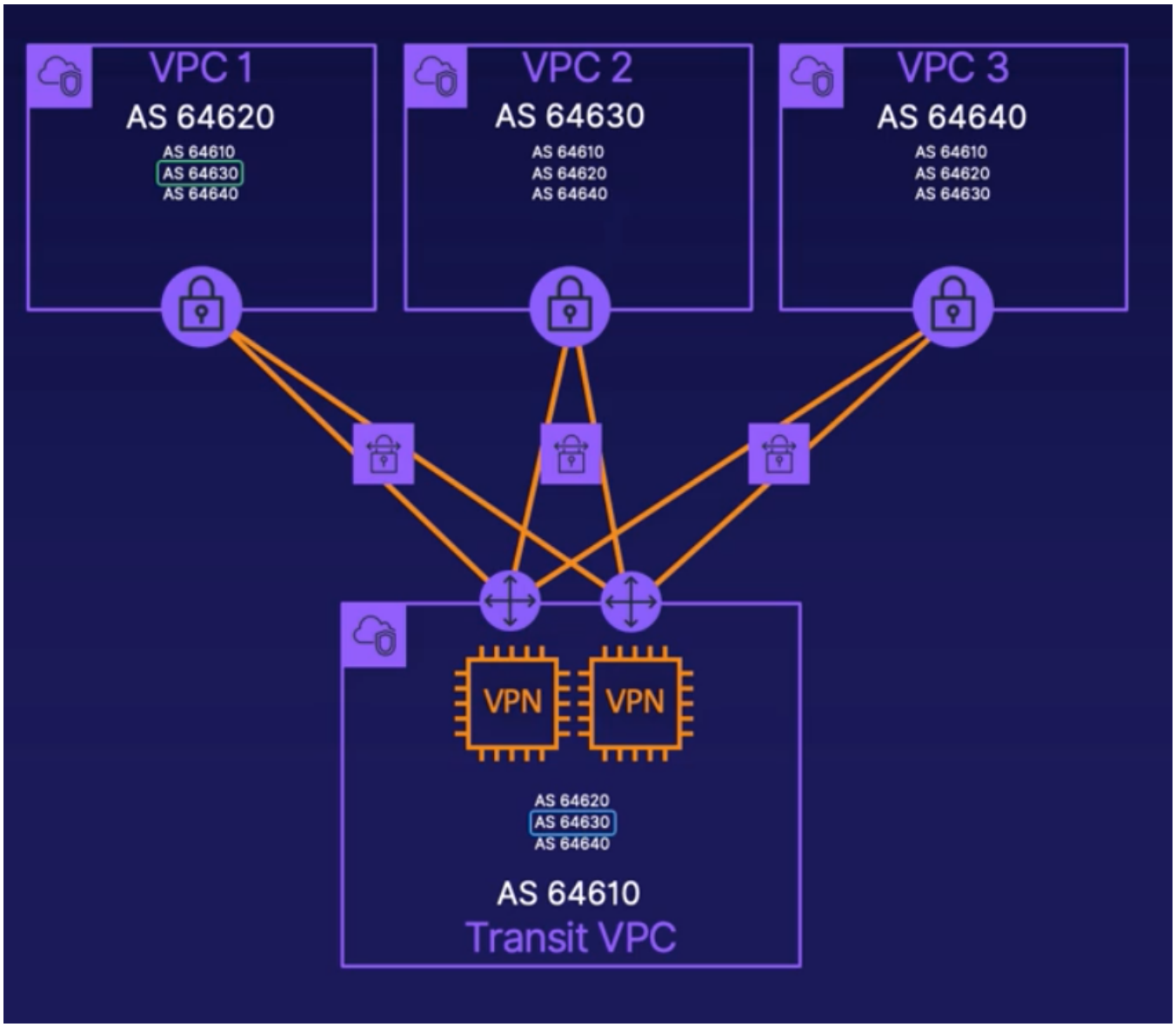
VPC Endpoint Services

- Exposed an NLB-frontend application to slected consumers in the same region.
- Consumers connect to application by creating a VPC interface Endpoint.
- Access can be restricted by AWS account, IAM user, or IAM role.

Transit VPCs (older way)

- Transit VPCs contain an EC2-hosted VPN solution
- EC2 VPN solution is the customer gateway for AWS VPN connections to spoke VPCs.
- VPN connections over the internet allow VPCs to be in any AWS account in any region.

Transit VPC Routing



- Dynamic routing is strongly recommended but is not a requirement.
- Spoke VPC VGWs advertise their local CIDR prefix to transit VPC VPN systems.
- VPN systems advertise all prefixes back to spoke VPCs.
- Spoke VPC VGWs route traffic to other spoke VPCs via transit VPCs VPN systems.
- Transitive connections are controlled by restricting the advertisement of route prefixes from the transit VPC.

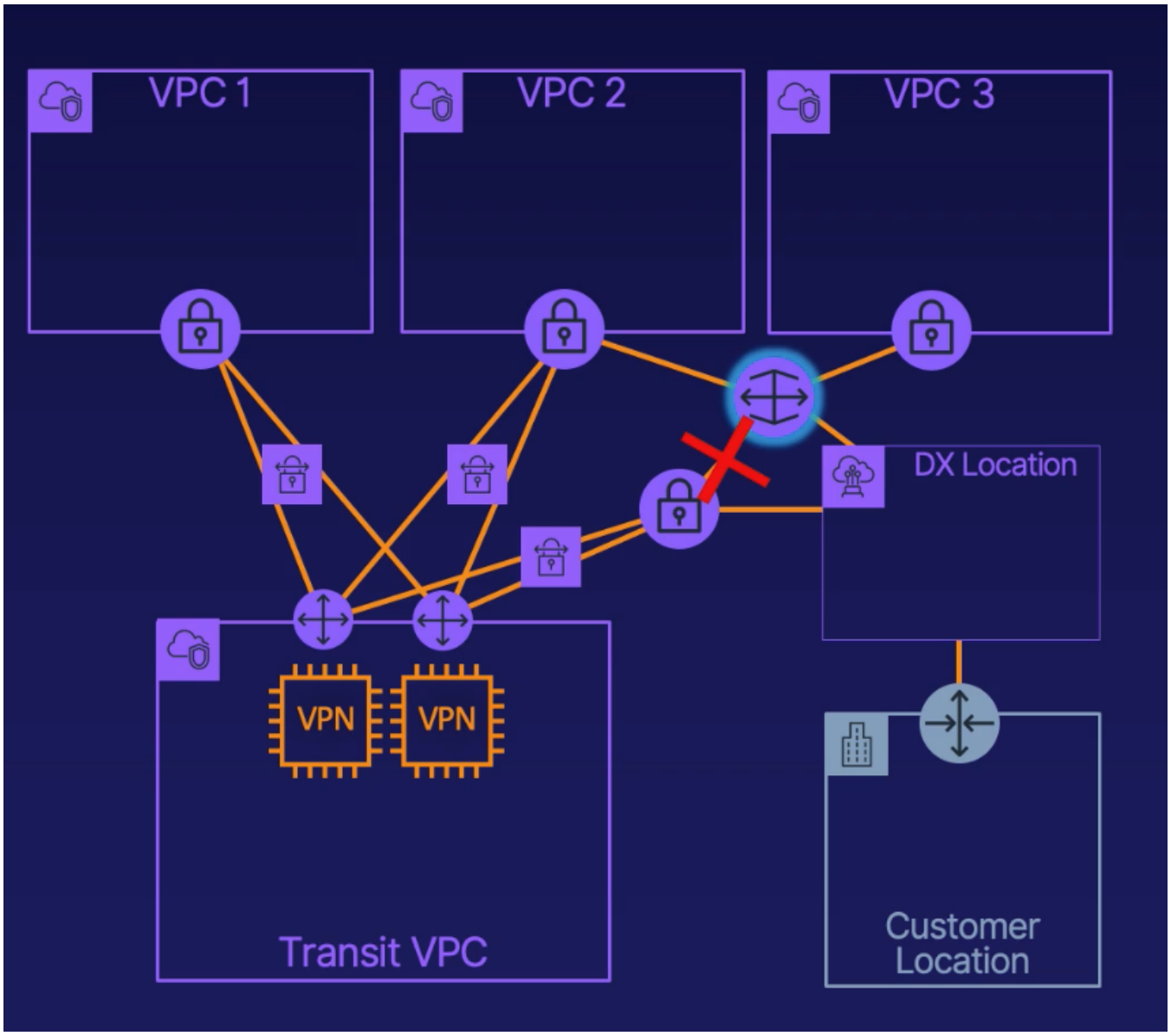
Transit VPCs and Hybrid Connectivity

VPNs

- VPNs form on-prem networks should connect to the VPN system in the Transit VPC.
- Optionally, AWS VPN connections may be established with trusted spoke VPCs.
- AWS VPN connections to a VGW in the transit VPC cannot forward traffic to other VPCs.

Direct Connect

- Public VIFs - Allows access to AWS public services without traversing the internet.
- Private VIFs
    - Can connect to a single VGW to access attached VPC.
    - Can connect to a Direct Connect Gateway
    - Up to 10 VGWs in any public region may connect to a DX Gateway (Except China)



- If Direct Connect traffic must pass through the transit VPC, then a detached VGW must be created in the region the DX location connects to.
- Private VIF is associated with detached VGW.
- The VPN systems in the transit VPC connect with AWS VPN connections
- Must enabled dynamic routing.
- If spoke VPCs must be accessed directly, new private VIFs could be connected to their VGWs directly.
- Direct Connect Gateway can be used to connect to multiple spoke VPCs
- DX Gateway cannot associate with floating VGW.

Jumbo Frame Roundup

- Traffic with a larger MTU than the network can support will be fragmented.
- Enabling "Do Not Fragment" IP header flag will cause large traffic to be dropped instead.
- Default size: 1500 bytes
- Max supported MTU sizes:
  - VPC: 9001
  - DX Private VIF: 9001
  - DX Transit VIF: 8500
  - DX Public VIF: 1500
  - VPC Peering: 1500
  - Internet: 1500

Transit Gateway Configuration

Within a single region, TGWs can attach to:

- VPCs from multiple AWS accounts
- VPN Customer Gateways
- Direct Connect Gateways (Transit VIF)
- can peer with TGWs in other regions.

Create

- All properties are optional.
- Only tags may be modified after creation.
- Amazon side ASN must be private ASN (16- or 32 bit).
- Accounts can have up to 5 TGWs per region.

Default settings:

- ASN 64512
- Cross VPC public DNS name resolution enabled
- Equal Cost Multipath enabled for VPN attachments
- New attachments use -and prefixes are propagated to - the default route table
- Attachment requests from other AWS accounts must be manually approved.

Attachments

- TGWs are connected to AWS network objects via attachments
- TGW attachments are AWS objects with their own AWS-assigned numbers (tgw-attach-xxxx)
- TGWs can have attachments to VPCs, VPN Customer Gateways, DX Gateways and peered TGWs.
- Traffic from an attached network arrives at the TGW from that network's attachment.
- Customers are billed hourly per operational TGW attachment.
- VPC:
  - Attachments to VPCs must connect to a subnet in at least 1 AZ.
- VPN:
  - VPN attachments require a customer gateway to be configured.
  - Creating a VPN attachment creates an AWS VPN connection.
  - Only the basic VPN tunnel options are available during creation.
  - After creation, subsequent management is performed from the site-to-site VPN connections console.
  - If static routing is selected, static routes are added via the TGW route tables
  - All appropriate AWS VPN connection charges will be applied.
- DX Gateway:
  - Attachments to a DX gateway are created from the Direct Connect Service.
  - DX connections to TGWs requires the creation of a Transit VIF.
  - The DX Gateway and TGW must be configured with different ASNs.
- TGWs:
  - TGWs in different regions may be joined by a Peering Connection attachment.
  - Requires static routes

Route Tables:

- TGW route tables identify which attachment outbound traffic should be forwarded to.
- Each TGW begins with a single initial route table (default).
- Each TGW can support up to 20 route tables.

Routes

- Routes in a TGW route table pair a destination CIDR with a TGW attachment ID that matching traffic will be forwarded to.
- Traffic arriving from an attached network object will be resolved using a route from the route table associated with that object's attachment.
- Traffic to destinations not represented int he route table will be dropped.

Associations

- Each object attached to a TGW will be associated to a single route table.
- Incoming attachment traffic is forwarded according to the associated route table.
- A TGW route table may be associated with more than one attachment.

Propagations

- Attachments may be configured to automatically propagate known CIDR ranges into one or more TGW route tables.
- Attachments do not need to be associated with a route table in order to propagate to it.
- VPCs will propagate their local CIDR.
- VPN CGWs and DXGWs will propagate customer prefixes advertised via BGP.
- Disabling TGW route propagation will require static route configuration.

Static routes

- Static routes may be added to point select traffic towards a specific attachment.
- Only one "default" route per route table
- Blackhole routes drop traffic matching the CIDR.
- Required to forward traffic to a peered TGW.

Propagations to attached networks

- Routes from VPCs to TGW attached networks must be manually added to VPC route tables.
- Routes form VPN CGWs to the TGW will be learned via BGP.
- Prefixes advertised via DXGWs are specifically declared when configuring the TGW attachment.

Monitoring

- Cloudwatch metrics:
  - BytesIn/Out
  - PacketsIn/Out
  - PacketDropCountBlackhole
  - BytesDropCountBlackhole
  - BytesDropCountNoRoute
  - PacketDRopCountNoRoute
- Flow logs only within the attached VPCs
- Greater control or visibility into transitive traffic requires a transit VPC.

Billing

- TGW Attachments billed per partial hour:
  - VPC owner (VPC attachment)
  - TGW owner (VPN attachment)
  - DX owner (DX attachment)
  - Both TGW owners (TGW peering)
- Charge per GB of data processed by TGW.
- No charge for data processed via peering.
- VPN connection charges

Transit Gateway Routing

Propagations

=> Identify which TGW attachments automatically add prefixes to that route table.

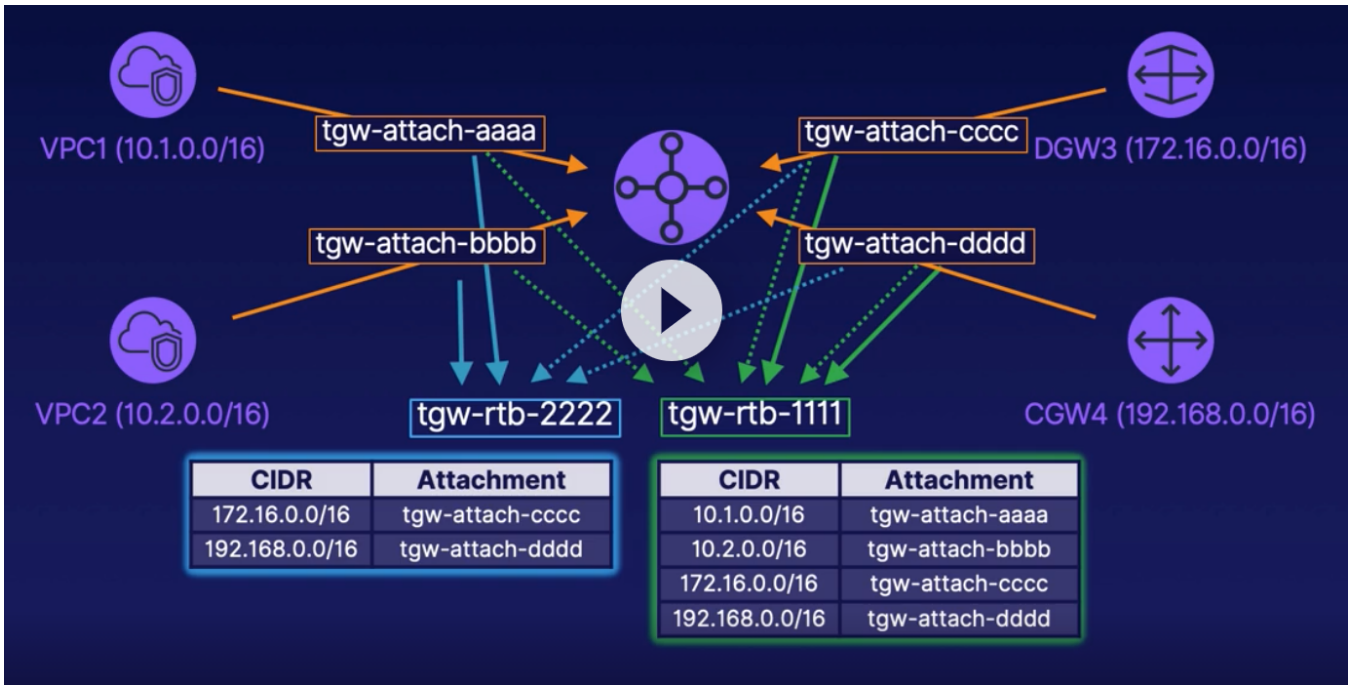
=> An attachment may propagate to many route tables

Associations

=> Identify which TGW attachments use that route table to determine the destination attachment for outbound traffic.

=> An attachment may only be associated with a single route table.

Isolated VPCs



Routing conflicts

1. Route with longest prefix
2. Static routes over propagated routes
3. VPC over DX over VPN

Network size limits

VPC Peering

- Only connects 2 specific VPCs
- A VPC may support up to 50 VPC Peering Connections
- Routes must be manually added to VPC route tables to support traffic flow.

VPC Endpoint Services

- NLBs can handle around 55.000 simultaneous connections.

AWS Site-to-Site VPN

- Default per-Region limits (soft limits):
  - 5 VGWs
  - 10 VPN connections per VGW
  - 50 Site-to-Site VPN connections and Customer Gateways

Transit VPCs

Limited by:

- 3rd party VPN platform
- VPC route table limits:
  - 50 non-propagated (static)
  - 100 propagated
- 100 dynamic routes for VGWs

DX Gateways

- Up to 30 Private VIFs
- Up to 10 VGWs

OR

- Up to 30 Transit VIFs
- Up to 3 TGWs

Transit Gateways

- Can support up to 5000 attachments (max of 20 DX Gateway attachments)
- Up to 50 peering attachments.
- Up to 20 Route tables per TGW
- Up to 10.000 static routes per TGW

Design and implement for Security and Compliance

Traffic Control

AWS Shield:

- DDos protection
- Hosted cloudfront, Global Acceleration and Route53 Edge locations
- Covers 96% of known layer 3 and 4 attacks

2 pricings:

- Standard tier (automatically)
- Advanced tier:
  - Additional protection
  - Detailed monitoring
  - WAF no charge
  - 24/7 DDos response team
  - EDos (economic denial of sustainability) coverage (when scaling costs occur)

WAF:

- Layer 7
- Allow/Deny HTTP/HTTPS using ACL
- Applicable to API Gateway, Cloudfront, ALB (ALB and API are region restricted)
- newer version has been released (WAF and WAF classic)

Conditions:

- Cross-site scripting
- Country of origin
- IP address
- Size of request properties
- SQL queries
- String/Regex

Each condition contains one or more filters. Multiple conditions are OR-ed

Rules:

- One or more conditions

- Specify match or not match
- Multiple conditions are AND-ed
- normal/rate-based (cloudwatch)
- rate-based will result (count) after 5 minutes (cannot be changed)

Customers may purchase managed rule-sets

ACL:

- one or more rules
- allow/deny/count
- Sequential order (count exception will only count, other acls still apply till match)
- Default actions

Price:

- Per ACL/month
- Per Rule/month
- Per 1 million requests

Limits per account/per region:

- 50 ACLS
- 100 Rules
- 5 rate-based rules
- 100 of each condition type except
- 10 regex conditions (cannot be increased)

Maximum 10 conditions per rule

Maximum 10 rules per ACL

Cloudfront

Enforce traffic going through cloudfront

- S3 bucket origins - restrict traffic using CF Origin Access Identity (bucket policy)
- Custom origins (ec2, albs) - only accept requests that include signed URLs, cookies, or custom headers added by the CF distribution.

S3

- S3 access points allow the creation of customized access points for an s3 bucket
- Each access point:
  - has a unique host name
  - has distinct permissions and network controls
  - can be limited to VPCs
- Can be managed by AWS Organizations SCP's

Security groups

- Applied to ENIs
- Up to 5 per ENI

ALB

Authentication can be offloaded to the ALB

- Traffic matching a listener rule is send to a configured identity provider

Traffic Protection

- PKI (Public Key Infrastructure) is a collection of systems used to verify identities and secure electronic data transfer
- Certificates are used by PKIs to verify identities and ownership of encryption keys

Digital certificates

contains information to validate the identity of the holder as well as the issuer:

- Name of the certificate holder
- Other information about the holder
- Purpose of the certificate
- Expiration date
- Identity of the issuer (Let's Encrypt)
- Means of validating the authenticity of the certificate

###SSL/TLS

- AWS recommends using TLS 1.2 wherever possible

AWS Certificate Manager (ACM)

- Certificates in AWS can be managed using either ACM or IAM
  - ACM not available in all regions
  - IAM cannot be used to create certificates (only imports)
  - ACM certificates cannot be imported by IAM
  - IAM certificates cannot be managed from the Console
  - Certificates in format X.509 can be imported into ACM
- Services that integrate with ACM
  - ELB
  - Cloudfront
  - API Gateway
  - CloudFormation
  - Elastic Beanstalk

Validation of domain ownership:

- DNS (Add TXT record to zone)
- Email (automatically sent to zone contacts)

Important notes:

- Certificates are provisioned on a per-region basis
- Certificates used by Cloudfront must be provisioned in us-east-1
- ACM certificates can only be used by AWS services integrated with ACM
- ACM certificates and their private keys may not be downloaded

AWS Certificate Manager PRivate Certificate Authority (ACM PCA)

- Crate your own private CA infrastructure
  - SSL/TLS certificates to identify internal resources
  - $400/month per CA
  - Charge per private certificate

S3 Https condition policy

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
      ],
      "Condition": {
        "Bool": {
          "aws:SecureTransport": "false"
        }
      },
      "Principal": "*"
    }
  ]
```

Protecting infra-AWS traffic - Cloudfront

- Settings configured per origin
- Origin Protocol Policy
  - HTTP only (default)
  - HTTPS Only
  - Match Viewer
- Origin-type specifics:
- Certificate at custom origin servers must be from a Mozilla-trusted CA
- S3 bucket origins are always "Match viewer"
- S3 buckets as websites do not support HTTPS

Traffic Awareness

VPC Traffic Mirroring

- Duplicates inbound and outbound traffic processed by a single ENI to either another ENI or a NLB

- Only one source ENI per mirror session
- Multiple sessions per target
  - NLB - unlimited
  - ENI - 100 max for dedicated instances, otherwise max of 10
- Mirror sessions may include a filter with up to 10 rules to accept or rejct matching traffic
- Traffic is analyzed at customer-managed instances
- Source and target can be in different AWS accounts
- Source and target must be in VPCs connected by peering or TGW
- All VPC routing must be correctly configured
- Mirrored traffic is not captured in flow logs
- Production traffic has highter priority than mirrored traffic
- Hourly charge per source ENI

Cloudwatch

WAF:

- AllowedRequests
- BlockedRequests
- CountedRequests
- PassedRequests

Shield:

- DDoSDetected
- DDoSAttackBitsPerSecond
- DDoSAttackPacketsPerSecond
- DDoSAttackRequestsPerSecond

Route53 & Cloudfront metrics located in us-east-1

VPC Traffic Mirroring Metrics (in EC2):

- NetworkMirrorIn/Out
- NetworkPacketsMirrorIn/Out
- NetworkSkipMirrorIn/Out
- NetworkPacketsSkipMirrorIn/Out

Note: Always at standard 5 minute reporting (even if enhanced monitoring is enabled)

AWS GuardDuty

- AWS-managed threat detection
- Automatically analyzes data from Cloudtrail, VPC flow logs, and AWS DNS resolvers to identify known threats and suspicious behaviors
- GuardDuty findings can be viewed in the Console, CLI, API and Cloudwatch Events
- Pricing based off the amount of data analyzed.

AWS Inspector

- Performs network accessibility and host vulnerability assessments on EC2 instances
- OS agent must be installed for host vulnerability and process-level network accessibility assessments.
- Assessments use rule packages created and maintained by AWS security researchers
- Findings include details from both Common Vulnerability Scoring System and the Center of Internet Security
- Recommends steps to fix issues
- Can be run as needed or scheduled
- Pricing is per assessment, per package

EC2

- Packet Capture and Analysis
    - Can only capture traffic arriving at local interfaces
    - ENI can be a target for VPC traffic mirroring sessions
        - Only supported on Nitro based images
        - Packet capture software must support VXLAN decapsulation
- Intrusion Detection/Prevention
    - Often sandwiched between ELB layers
    - IDS monitors netowrk and reports events
    - IPS can modify traffic or service configurations in response to events
        - Agent software might be required to configure services
    - Service appliances available in the AWS AMI Marketplace

Governance and compliance