HYBRID ENVIRONMENTS AND MIGRATION

Border Gateway Protocol 101

Introduction to the Border Gateway Protocol (BGP) which is a routing protocol used by some AWS services such as Direct Connect and Dynamic Site to Site VPNs.

- BGP made of AS (autonomous systems). Routers controlls by one entity; a network in BGP. Your whole company's network system is a 'black box' abstraction, BGP only cares about ingress/egress
    - Autonomous System Numbers (ASNs) are unique and allocated by IANA (0-65535), 64512-65534 are PRIVATE
- BGP operates over tcp/179 -- reliable
- BGP not automatic, peering is manually configured
- BGP is a PATH-VECTOR protocol; it exchanges the best path to a destination between peers...best path (AKA shortest path) is called ASPATH
- iBGP (internal routing within an AS) - most common, eBGP (external routing between ASs)
- ASPATH prepending: A way to make a shorter but slower path look worse than a longer but faster path (by just addking more ASs to the path route)

IPSec VPN Fundamentals

IPsec VPN negotiation occurs in two phases:

1. In Phase 1, participants establish a secure channel in which to negotiate the IPsec security association (SA)
2. In Phase 2, participants negotiate the IPsec SA for authenticating traffic that will flow through the tunnel and use IPSec Keys to exchange 'interesting traffic'

- sets up secure tunnels across insecure networks
- provides authentication and encryption; a secure connection over an insecure network
- asymmetric encryption used to establish symmetric encryption

IPSec - Two Phases

IKE Phase 1 (slower): Internet Key Exchange. IKE v1 and IKE v2 (v2 is newer)

- authentication with asummetric encryption to agree on and create a shared symmetric key
- "Diffie-Helman Private Key"/DH Key created by both sides in Phase 1.. this is what actually creates the symmetrical key for phase 2 IKE Phase 2 (faster): Getting VPN up and running
- built on phase one using the symmetric key created in phase 1
- Phase 2 can be town down and rebuilt when needed, phase 1 can stay

IPSec - VPN Types (2)

1. Policy Based. Rule sets match traffic. More difficult to configure, but more flexible than Route Based
2. Route Based. Target matching based on prefix

- difference being how they match 'interesting traffic'

AWS Site-to-Site VPN. AWS <-> on-premises VPN

AWS Site-to-Site VPN is a hardware VPN solution which creates a highly available IPSEC VPN between an AWS VPN and external network such as on-premises traditional networks.

- Quickest way to create network link between AWS and non-AWS (less than an hour)
- VPNs are quick to setup vs direct connect, don't offer the same high performance, but do encrypt data in transit.
- Runs over the public internet (unlessw otherwise specificed) EXAM - Highly Available

AWS Site-to-Site VPN - Components

- VPC. VPC connected to external network via VPN
- Virtual Private Gateway (VGW). The target one or more route tables
- Customer Gateway (CGW): Logical piece of config and the thing that the config represents
- VPN Connection

Static VS Dynamic VPN

- Static uses BGP, Border Gateway Protocol (customer router must support this). Static networking config, static routes
- Dynamic VPN: Need Direct-Connect? Dynamic. Multiple VPN connections for Higher Avail and traffic distribution
- "Route Propagation": if enabled, means routes are added to RTs automatically

EXAM - AWS speed limitation of VPNs 1.25Gbps EXAM - Virtual Private Gateway limitation is also 1.25Gbps -> 2 tunnels will be limited to 1.25Gbps in total EXAM - Latency is inconsistent as it is through Public Internet. If need low latency, maybe Direct Connect

Direct Connect (DX) Concepts

AWS Direct Connect links your internal network to an AWS Direct Connect location over a standard Ethernet fiber-optic cable. One end of the cable is connected to your router, the other to an AWS Direct Connect router. With this connection, you can create virtual interfaces directly to public AWS services (for example, to Amazon S3) or to Amazon VPC, bypassing internet service providers in your network path.

An AWS Direct Connect location provides access to AWS in the Region with which it is associated. You can use a single connection in a public Region or AWS GovCloud (US) to access public AWS services in all other public Regions.

Direct connect = physical connection between business premises (owned by you) and DX Location (not owned by AWS) and AWS Region (owned by AWS)

- 1, 10, or 100GBps
- when you order Direct Connect (DX), you're really ordering a Port Allocation at the DX Location
- Cannot access internet
- DX Location is NOT owned by AWS, it has 2 "cages":
    - 1 cage for AWS owned equipment (AWS routers -> port allocation happens here): connected to AWS region
    - 1 customer or shared partner Cage: with customer router and connected on premise router

    - both cages are physically connected
- Low latency, high speeds. No resilience (at it's literally 1 cable)
- requires VIFs (virtual interfaces) for the networking over DX to AWS

Direct Connect (DX) Resilience

Initially, DX has NO resilience as it only has 1 cable. For resilience, you need to lay multiple DX connections / provision multiple ports. Lots of single points of failure by default.

- Best practice... multiple DX Connect Locations... Multiple Customer Premises. Two ports in each DX location, dual routers at customer locations (2)
- At DX Connect Location... Multiple AWS routers, multiple customer routers

Direct Connect (DX) - Public VIF + VPN (Encryption)

How to use these things to achieve end-to-end encrypted access to private VPC networks across Direct Connect

- Neither public or private VIFS offer any form of encryption.
- Public VIFs+IPSec VPN is a way to provide access to private VPC resources, using an encrypted IPSEC tunnel for transit.

Transit Gateway

The AWS Transit gateway is a network gateway which can be used to significantly simplify networking between VPC's, VPN and Direct Connect.

- It can be used to peer VPCs in the same account, different account, same or different region and SUPPORTS TRANSITIVE ROUTING between networks.
- VPC peering can become complex when you have many VPCs, Transit Gateway simplifies this a lot
- Single network object that is highly available and scalable
- create "attachements" to other network types: valid attachments -> VPC, site-to-site VPN, DX Gateway
- Can use "peering attachments" to ve cross-region/cross-account (cross account = AWS RAM Ressource Access Manager)
- Supports transitive routing (which is basically why it exists, since VPCs don't which causes too much complexity) EXAM - REMEMBER: TRANSIT gateway supports TRANSITIVE ROUTING (which VPC peering can't do) -- this simplifies vpc-to-vpc

Storage Gateways - Volume, Tape, File

Storage Gateway - Volume

Storage gateway is a product which integrates local infrastructure and AWS storage such as S3, EBS Snapshots and Glacier.

Storage Gateway - Volume Stored Mode

EXAM - ALL stored locally on on-premise volume, which means low latency access

- Data copied into S3 in the form of EBS Snapshots EXAM - Use: Full disk backups of volume EXAM - Use: Assists with disaster recovery through created EBS volumes from snapshots in AWS EXAM - VSM does NOT improve or extend data center capacity because volumes are stored fully on-premise.
- Something something iSCSI

Storage Gateway - Volume Cached Mode

Instead of having a local storage volume on prem, you have a local cache. Actual data stored in S3, and does EBS Snapshot backups EXAM - Use Case: To extend your data center (since data is stored in S3 and frequent accessed data is cached locally)

Storage Gateway - Tape (VTL) - Virtual Tape Library

Storage gateway in VTL mode allows the product to replace a tape based backup solution with one which uses S3 and Glacier rather than physical tape media

- Max size of virtual tape is 5 TiB, same as size of S3 bucket
- Pretends to be an iSCSI tape library, changer, and drive. S3 serves as Virtual Tape Library, Glacier is the Virtual Tape Shelf
- Uses: Backup platform migrations or data center extensions

Storage Gateway - File

File gateway bridges local file storage over NFS (linux)/SMB(windows) with S3 Storage

- It supports multi site, maintains storage structure, integrates with other AWS products and supports S3 object lifecycle Management
- Files stored this way (to mount point) are visible as objects in an S3 bucket
- Read/Write caching ensure LAN-like performance
- 1 file share + 1 S3 = 1 bucket share. Can have 10 Bucket Shares per file gateway
- Primary data stored in S3
- File Gateway doesn't support Object Locking--use Read Only Mode on other shares or tightly control file access

Snowball / Edge / Snowmobile [NEW VERSION COMING SOON]

Snowball, Snowball Edge and Snowmobile are three parts of the same product family designed to allow the physical transfer of data between business locations and AWS.

Snowball

- Order physical device from AWS. Encrypted using KMS. 50TB or 80TB. EXAM - Range of data to use it for 10TB - 10PB EXAM - Can order multiple devices / to multiple premises EXAM - STORAGE ONLY, no compute

Snowball Edge

EXAM - Has both storage and compute

- Larger capacity VS snowball

- Faster networking with Edge
- 3 types of Edge: 1. Storage Optimized 2. Compute Optimized 3. Compute Optimized with GPU EXAM - Ideal for remote sites or where data processing on ingestion is needed

Snowmobile

Portable data center within a shipping container on a truck (mobile, duh)

- Ideal for single location with 10PB+ is required
- 10PB - 100PB
- NOT for multi-site (unless HUGE) or sub 10PB

Directory Service

What are directories? Identity and asset info storage. Stores objects with structure (inverse tree).

- Multiple trees grouped into a FOREST
- Commonly used with Windows environments
- Users, devices, groups, servers, file shares -- things that can be objects in a directory

AWS Directory Service is an AWS managed implementation of a directory that runs in a VPC

- High availability, deploy into multiple AZs
- Amazon Workspaces NEEDS the AWS Directory Svc to function
- can be isolated or integrated with an on-premise system

Directory Service - Three Modes

1. Simple AD - An implementation of Samba 4 (compatibility with basics AD functions)

- cheapest / simplest mode
- 500 - 5000 users
- Simple AD is based off of Samba 4 (an open-source version of Microsoft AD)
- Simple AD designed to be used in isolation

2. AWS Managed Microsoft AD - An actual Microsoft AD DS Implementation

- AWS presense while having an existing on-premises directory
- Primary location is at AWS. TRUST relationships created between AWS and on-premmise

3. AD Connector which proxies requests back to an on-premises directory

- An entity made to integrate with AWS services. It has NO local functionality - great for hosting Workspaces
- If private connectivity fails, AD fails and AWS-side related svd would be interrupted

When to pick one of the 3 ADs?

Simple AD - The default. Simple reqs. A directory in AWS Microsoft AD - Apps in AWS which req MS AD, or you need to TRUST AWS AD Directory Service AD Connector - To use AWS p&s that require a directory without actually housing one on AWS side (as you have it on prem), use AD connector

DataSync

AWS DataSync is a product which can orchestrate the movement of large scale data (amounts or files) from on-premises NAS/SAN into AWS or vice-versa

- Data transfer service To and FROM AWS
- Designed to work at HUGE scale
- Keeps metadata (permissions/timestamps)
- Built-in data validation
- Scalable: 10Gbps/agent (~100TB/day)
- FEATURES EVERYWHERE... Bandwidth limiters, incremental/scheduled xfer options, compression and encryption, auto recovery from transit errors, svc integration with S3 EFS FSx, bidirectional transfer EXAM - The DataSync agent needs to be intalled LOCALLY on-prem EXAM - communicates via NFS/SMB w/ on-prem storage

DataSync Components

- tasks: a "job"
- agent: the software living on-prem that reads/writes to on-prem data stores using NFS/SMB
- location: every task has a TO and FROM location

FSx for Windows Servers

FSx for Windows Servers provides a native windows file system as a service which can be used within AWS, or from on-premises environments via VPN or Direct Connect

- FSx is an advanced shared file system accessible over SMB, and integrates with Active Directory (either managed, or self-hosted).
- It provides advanced features such as VSS, Data de-duplication, backups, encryption at rest and forced encryption in transit.
- Integrats with Directory Service or Self-Managed Active Directory
- Single or Multi-AZ within a VPC
- on-demand/scheduled backups
- accessible using VPC, peering, VPN, Direct Connect
- FSx is dedicated to Windows Environments, the similar EFS is for Linux/Unix
- File level versioning; support volume shadow copies; file-level restores EXAM - Key words to look for: VSS (user driven restores), native file system over SMB (SMB=windows), uses Windows permissions model, supports DFS (distributed file system), integrates with Directory Service and YOUR OWN directory

FSx For Lustre

FSx for Lustre is a managed file system which uses the FSx product designed for high performance computing

- It delivers extreme performance for scenarios such as BIG DATA, MACHINE LEARNING and FINANCIAL MODELING -- FSx for Lustre is a managed Lustre high compute system. Linux clients (POSIX)

- Two deploment types: Persistent or Scratch -- Scratch: highliy optimized for short-term. No replication and fast. not HA -- Persistent: Longer term, high avail in one AZ, self-healing EXAM - If Lustre, POSIX mentioned... FSx for Lustre, ML/big data/fin-modeling

AWS Transfer Family

Managed file transfer service using these protocols: SFTP, FTP, FTP Transfer, AS2 EXAM - supports transferring data over the following protocols: SFTP, FTPS, and FTP transfer

- Managed File Transfer Workflows (MFTW) - serverless file workflow engine (for tagging and stuff)
- Using FTP? Since not secure, you can only use FTP protocol within VPC (not public)