

VIRTUAL PRIVATE CLOUD

VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

VIRTUAL PRIVATE CLOUD

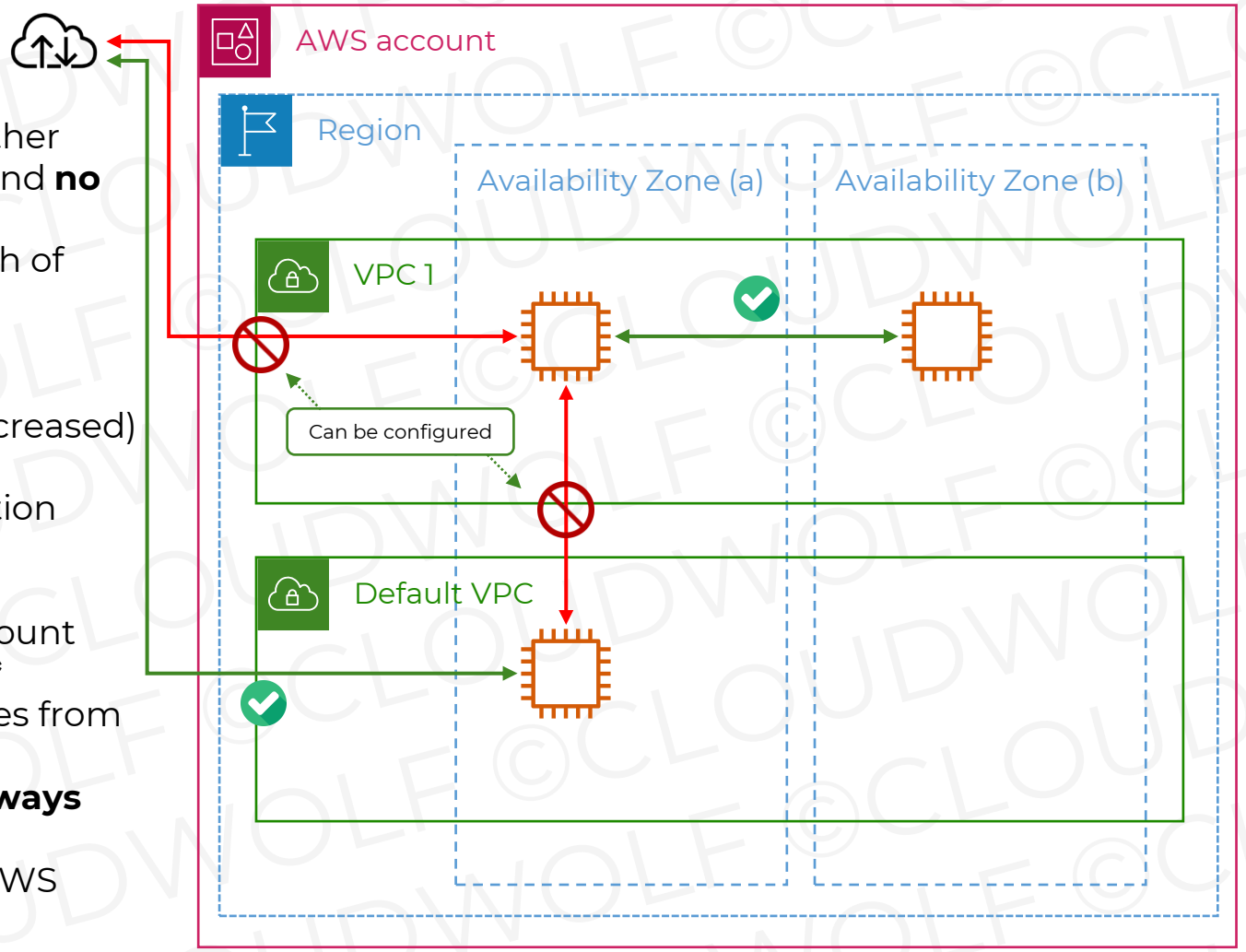
Virtual Private Cloud (VPC)

- A VPC is **a logically isolated virtual network**
- Resources inside one VPC can communicate with each other
- But by default there is **no communication across VPCs** and **no communication with the public internet**
- However, a VPC can be configured to enable either or both of these communications (coming up later in the course)

- AWS VPC is a **Regional Service**
- You can have up to 5 VPCs per region (this limit can be increased)
- Every region starts with a **Default VPC**
- The Default VPC comes pre-configured with communication to/from the public internet enabled

- A VPC is a way to separate/organize resources in your account
- A VPC is **allocated a range of private IPs (a CIDR Block)***
- Resources inside the VPC are assigned private IP addresses from this range
- EC2 Instances, Load Balancers and other resources are **always launched inside VPCs**
- Note: S3 buckets exist outside of VPCs (because S3 is an AWS public service)*

** More on this in upcoming tutorials.*





PUBLIC & PRIVATE SUBNETS

VPC



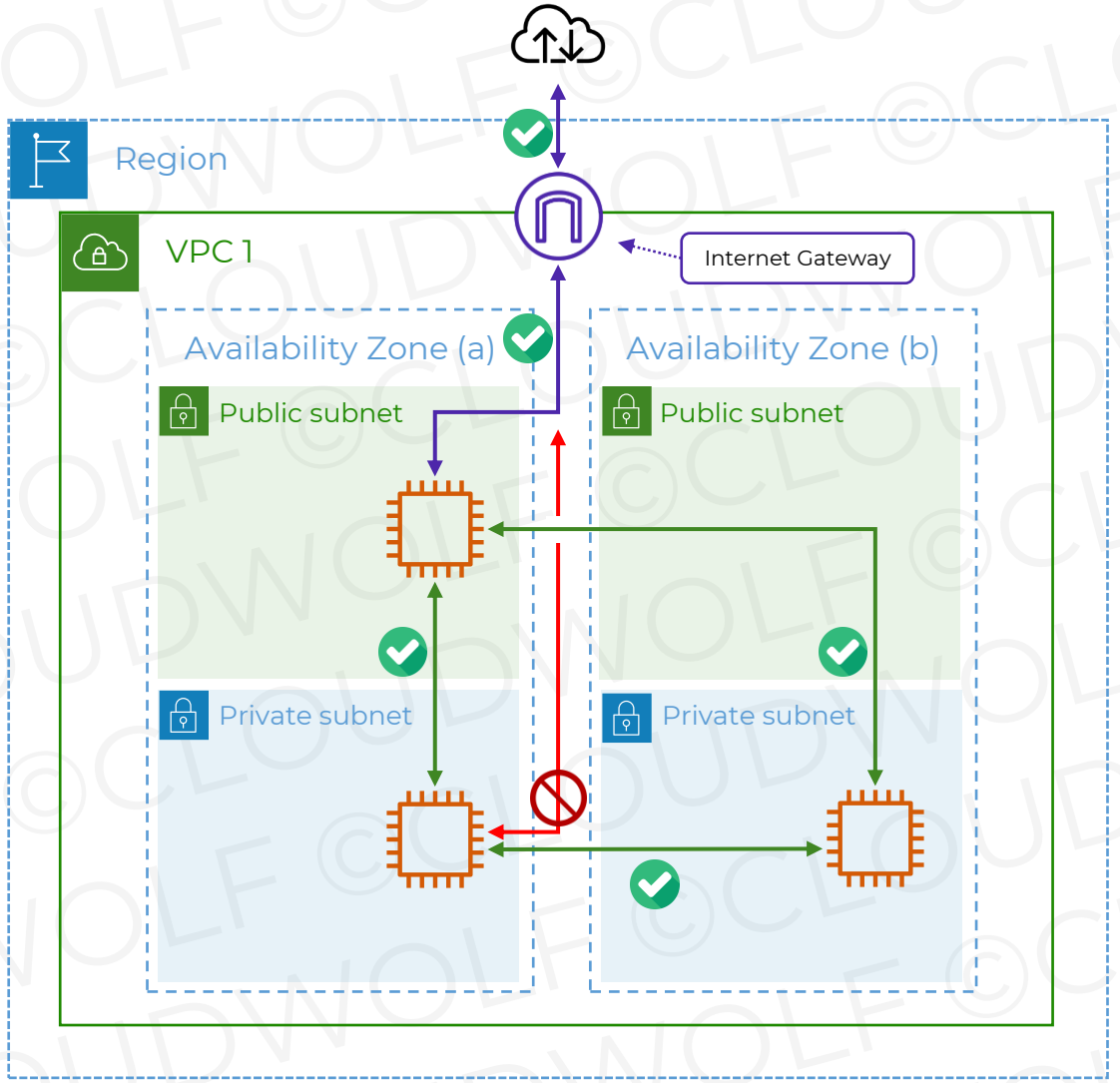
© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

PUBLIC & PRIVATE SUBNETS

Subnets:

- Inside each AZ a VPC consists of Subnets
- **A subnet is a pre-defined range of IP addresses in your VPC**
- There are two types of Subnets: Public and Private
- How you configure a Subnet will determine its type
- Public Subnets:
  - Are **configured** to allow **both outgoing and incoming** requests to/from the public internet
  - This is done by routing them to an Internet Gateway (IGW)*
- Private Subnets:
  - Are **not configured** to allow **incoming** requests from the public internet
  - But can be configured to allow outgoing requests to the public internet via a NAT Gateway*

- You can create **multiple** Public and Private **Subnets per AZ**
- Subnets inside one VPC can communicate with each other regardless of their type and AZ placement
- By default, a Region's **Default VPC** has one Public Subnet in each AZ and no Private Subnets

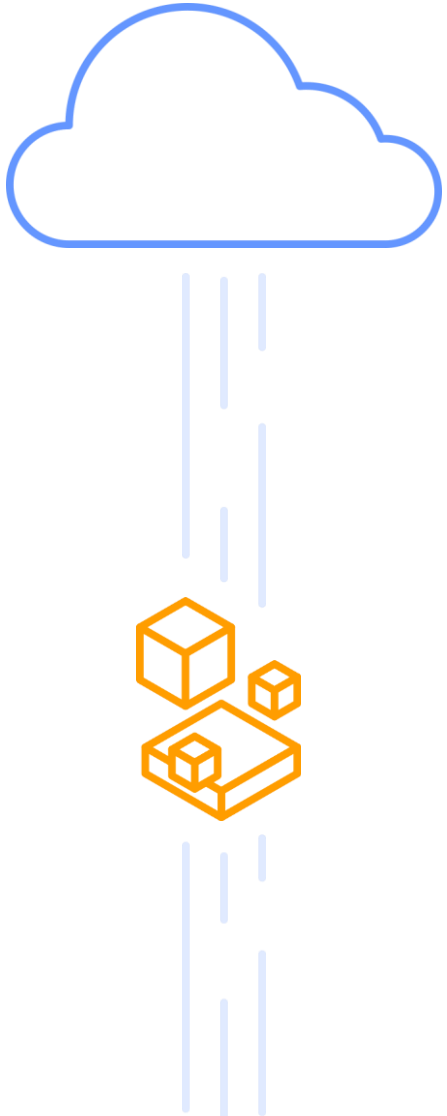


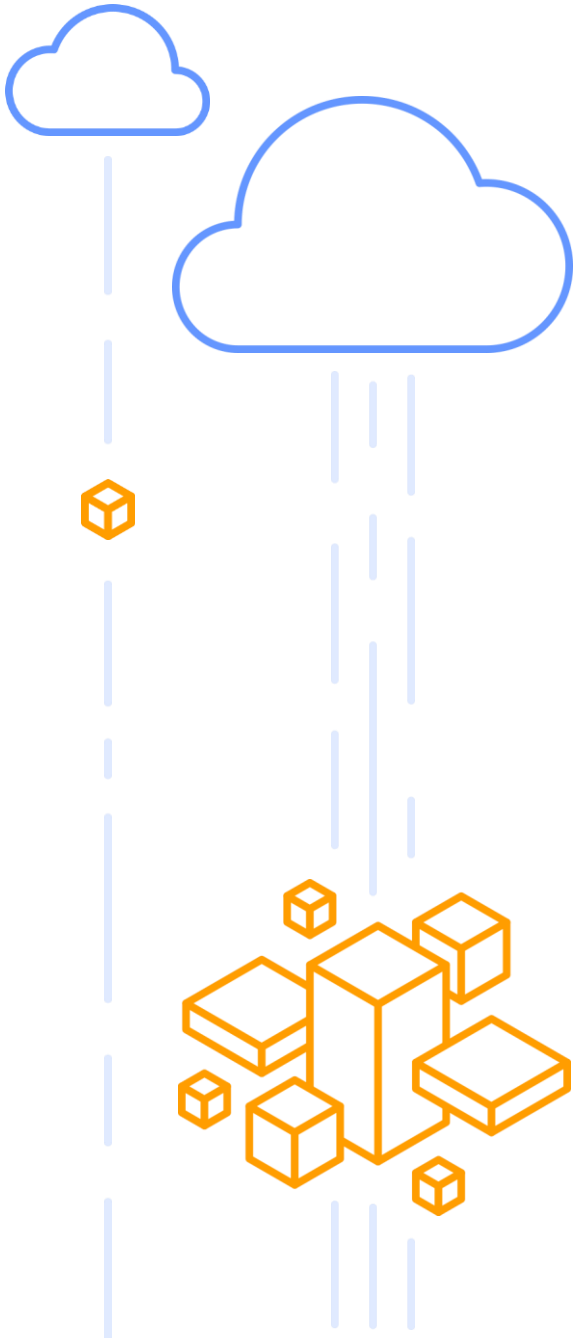
More on IGWs and NAT Gateways later in the course.

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com









UNDERSTANDING
CIDR NOTATION

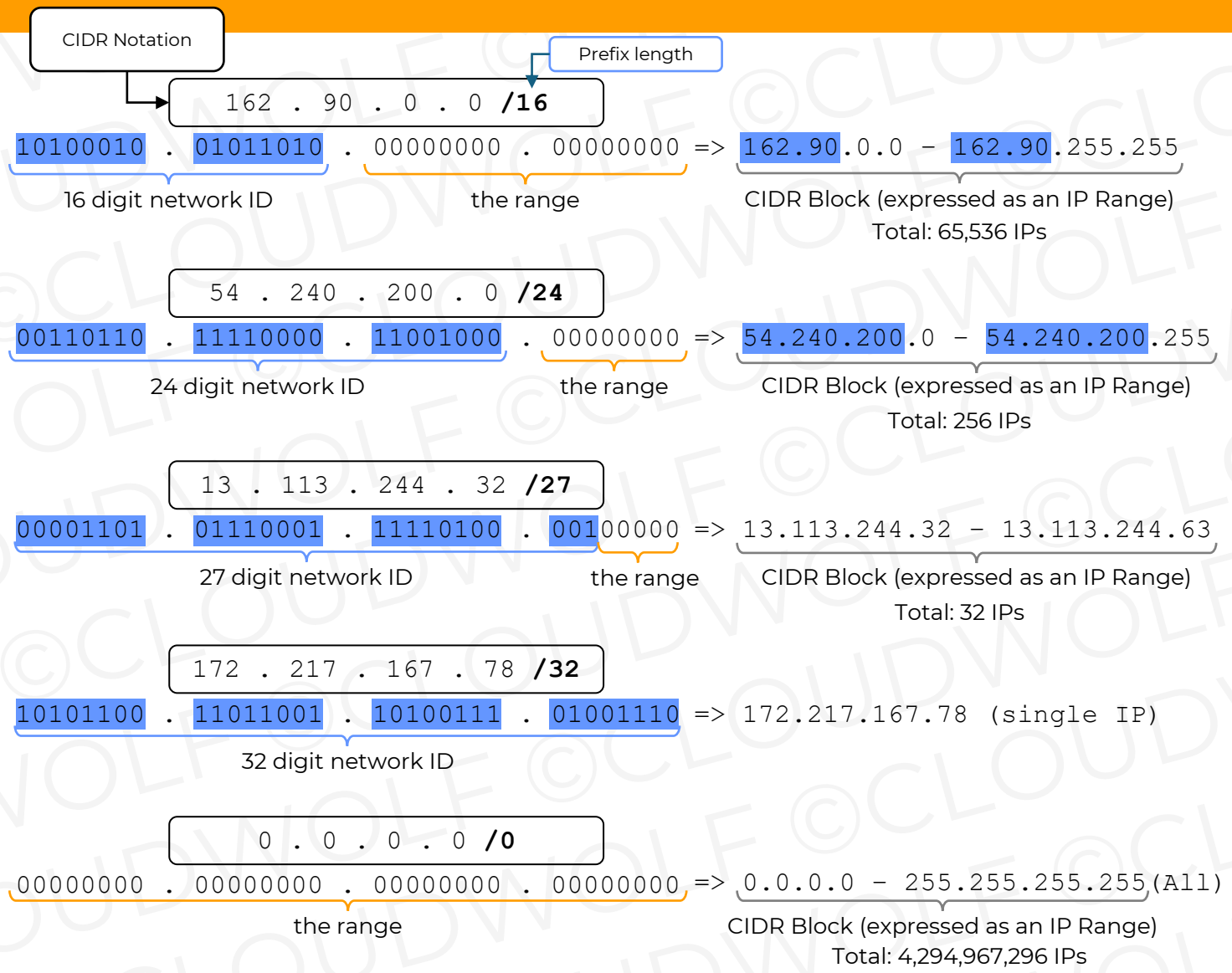
VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

CIDR NOTATION

CIDR Notation:

- Classless Inter-Domain Routing (CIDR) is a method for allocating IP addresses which the World uses today*
- A **CIDR Block** is a group of IP addresses with the same network ID
- **CIDR Notation** is a shorthand way of writing CIDR Blocks using the first IP followed by a /XX
- **/XX is referred to as the prefix length or also as "the prefix" for short**
- It determines how many digits of the IP address (in binary form) represent the network
- The remaining digits (in binary) define the range of IPs inside the CIDR block
- **The higher the /XX prefix, the smaller the network size**, e.g.:
  - a /16 CIDR block contains 65,536 IPs
  - a /24 CIDR block contains 256 IPs
  - a /32 CIDR block contains a single IP



** CIDR replaced the classful network addressing architecture*

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



PRINCIPLES OF **SUBNETTING**

VPC



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

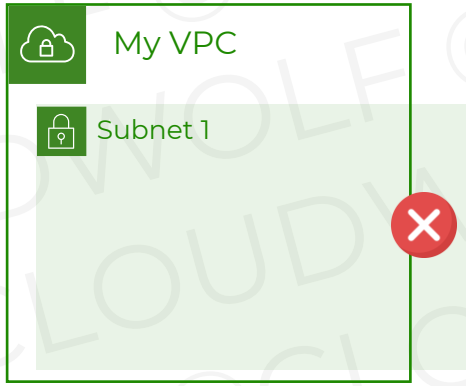
CIDR BLOCKS

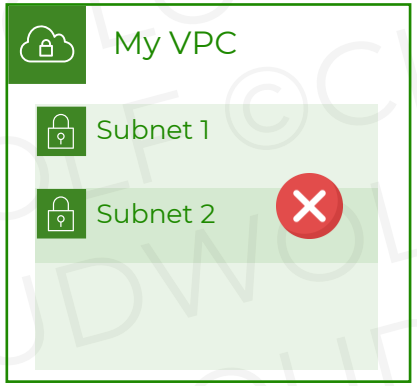
CIDR Blocks:

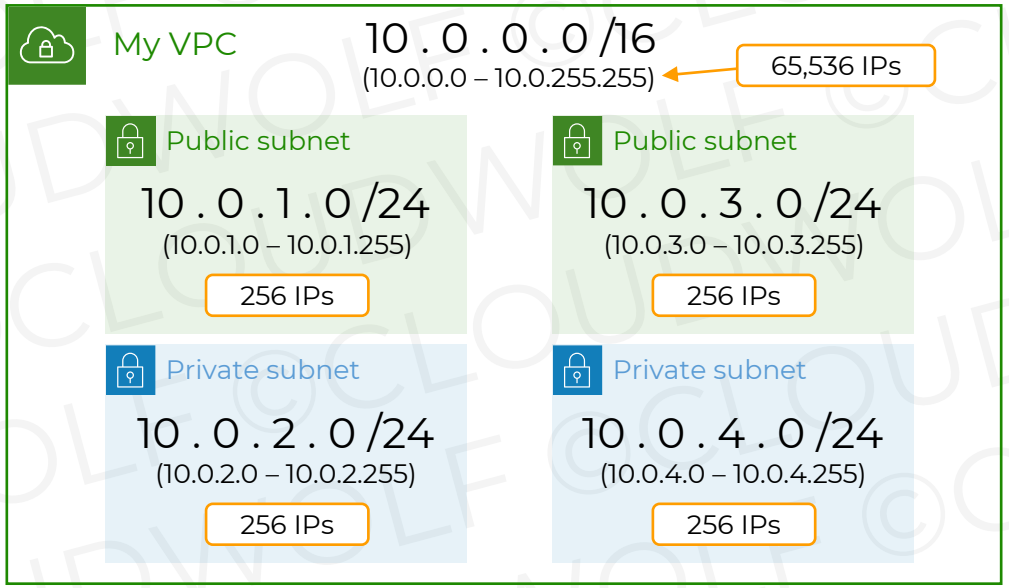
- **Subnetting – is the process of breaking down a larger network into smaller networks**
- **Each of the smaller networks will have a higher prefix**
- Two rules must be followed when creating subnets:
    1. The Subnet CIDR block has to be within the VPC CIDR block
    2. CIDR blocks of two subnets cannot overlap

- Note: It is normal to have IP ranges inside your VPC that are not used by any Subnet. In fact, this is beneficial as it gives you the flexibility to create more subnets later if they are required

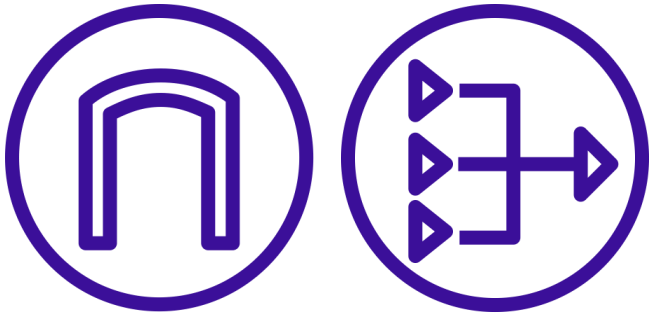
- *Advanced:*
    - *In AWS the Default VPC always has the CIDR Block 172.31.0.0/16 and Default subnets use /20 CIDRs within the default VPC CIDR*
    - *Check the documentation to see which CIDR Blocks AWS recommends for Custom VPCs*
    - *The first four IP addresses and the last IP address in each Subnet CIDR block are reserved and cannot be used by your resources*





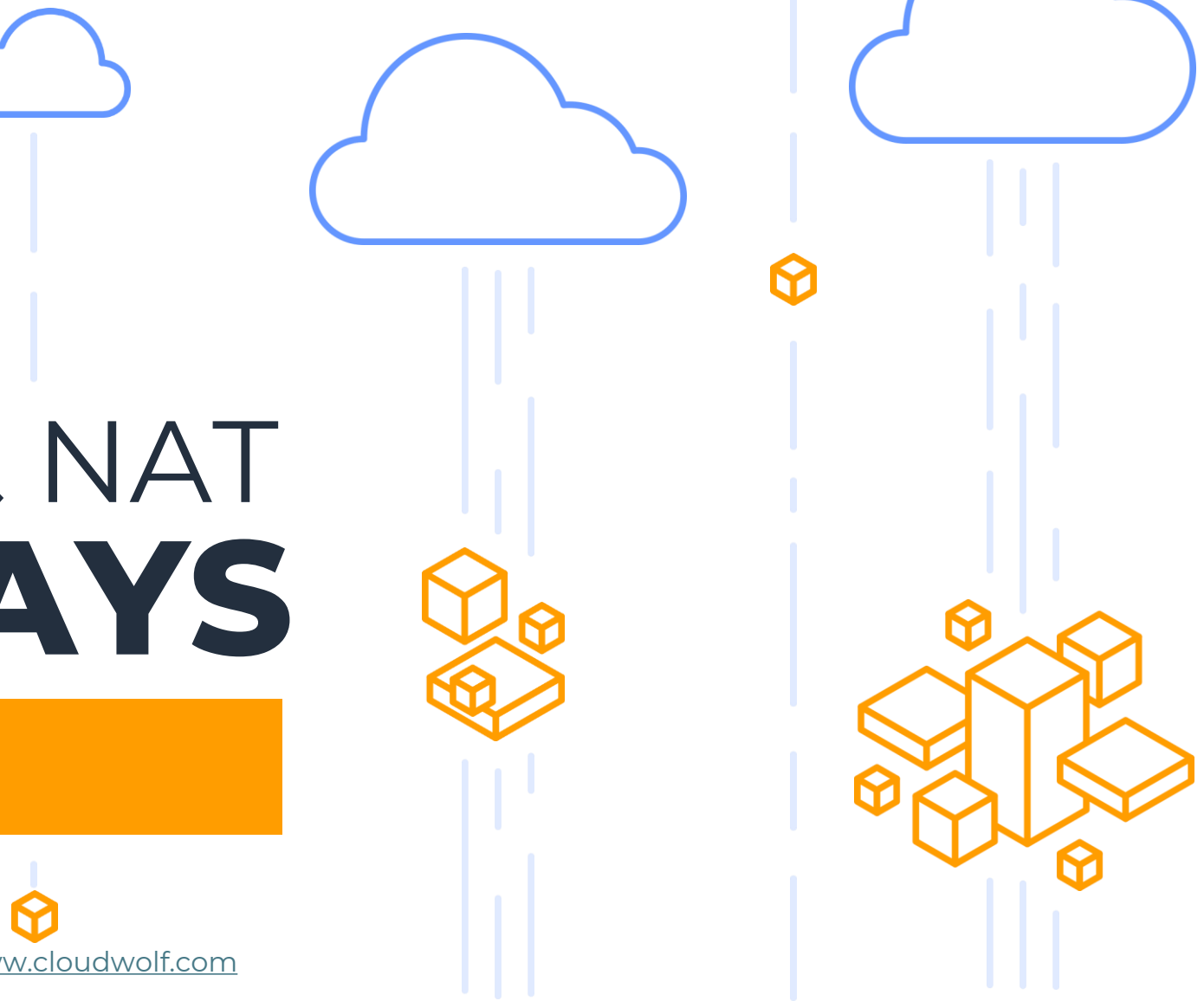


© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



INTERNET & NAT GATEWAYS

VPC



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

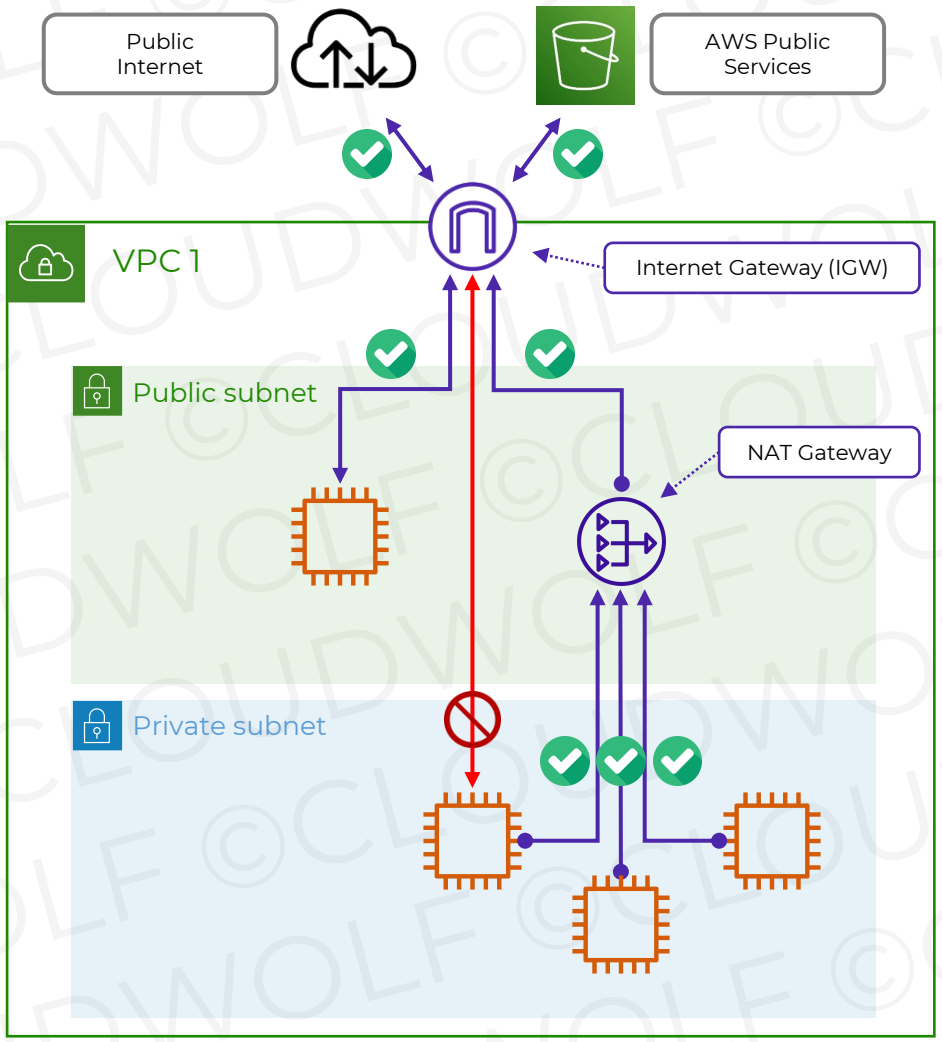
INTERNET & NAT GATEWAYS

Internet Gateway:

- A horizontally scaled, redundant and highly available VPC component
- Allows instances* in **Public Subnets** to have a **two-way connection** with the Public Internet
- Allows instances in **Public Subnets** to use **AWS Public Services****
- Only one internet gateway can be attached to each VPC
- Regionally resilient (you **don't** need one in each AZ)
- Not accessible from outside the VPC
- There's no additional charge for creating an internet gateway

NAT Gateway:

- Network Address Translation (NAT) service
- Works with a Internet Gateway (IGW):
  - NAT + IGW together allow instances in **Private Subnets** to have a **one-way connection** with the Public Internet
  - NAT + IGW together allow instances in **Private Subnets** to access **AWS Public Services****
- **Must be launched in a Public Subnet**
- AZ resilient. For regional resilience launch a NAT GW in each AZ
- Not accessible from outside the VPC
- Not free-tier eligible. Charge is for each hour that your NAT gateway is available and each Gigabyte of data that it processes



** Instance must have a Public IPv4 address. A Subnet can be set up to auto-assign Public IPv4 addresses*
*** More on this in upcoming tutorials*

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



UNDERSTANDING
ROUTE TABLES

VPC

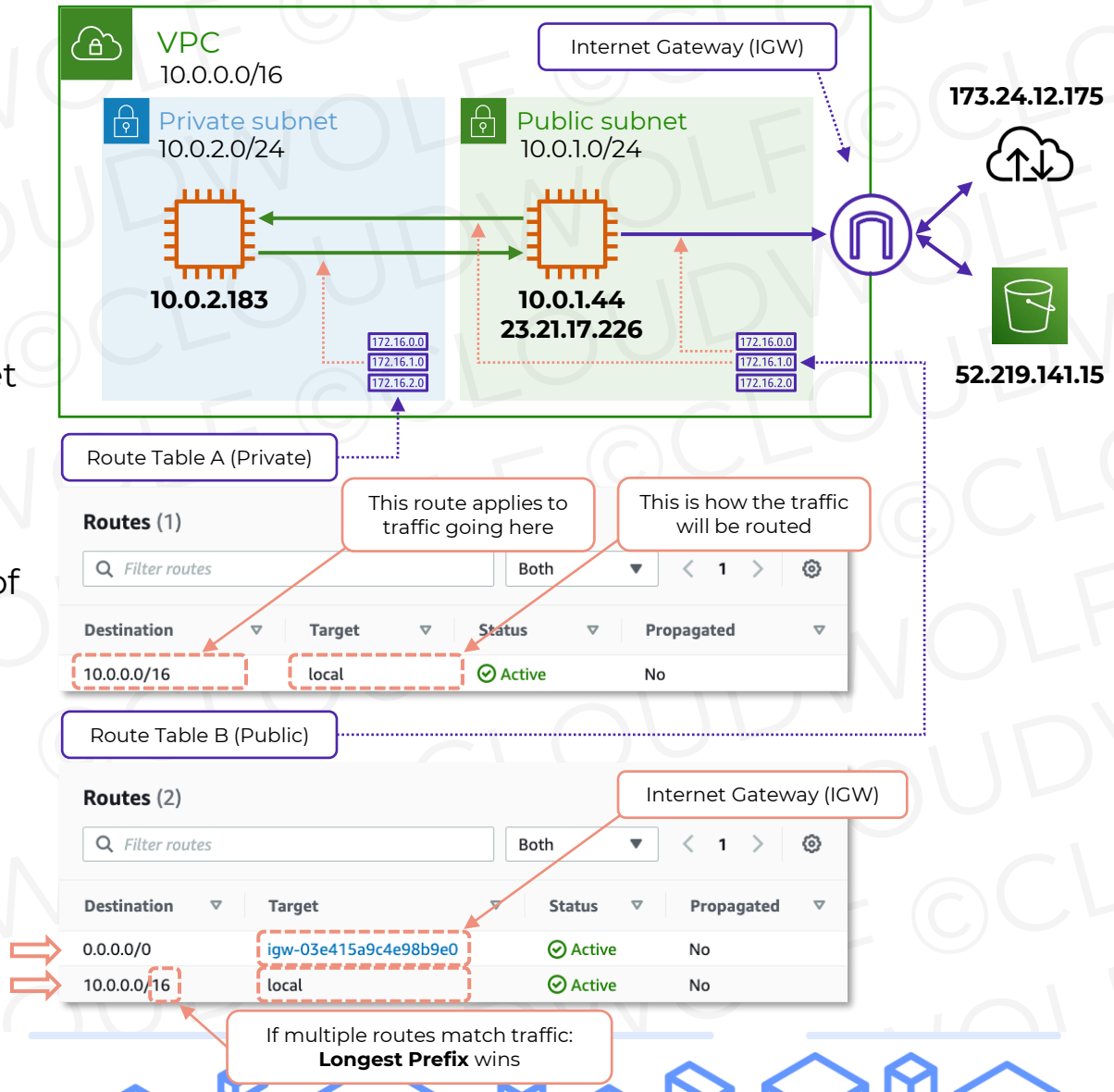


© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

ROUTE TABLES

Route Tables:

- A route table contains a set of rules, called routes, that determine where network traffic is directed
- Route tables are created at VPC level
- Route tables are assigned to ("associated with") Subnets
- **Each Subnet has to be associated with exactly one Route Table**
- Each Route Table can be associated with many Subnets
- If no Route Table is explicitly assigned to a Subnet, then that Subnet will be assigned the Main Route Table of the VPC by default
- It's common practice to have at least two route tables in a VPC:
  - **A Route Table for Private Subnets (doesn't route to IGW)**
  - **A Route Table for Public Subnets (routes to IGW)**
- Note: if a NAT GW is used, it needs to be added to the Route Table of the Private Subnet
- **If multiple routes match the traffic, the most specific matching route (longest prefix) will be used. Examples:**
- Traffic from the Public Subnet to 173.24.12.175 will be routed to the Internet Gateway:
  - **0.0.0.0/0 –> Internet Gateway *(match)***
  - 10.0.0.0/16 –> Local *(no match)*
- Traffic from the Public Subnet to 10.0.2.183 will be routed locally:
  - 0.0.0.0/0 –> Internet Gateway *(match)*
  - **10.0.0.0/16 –> Local *(match & longest prefix)***



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



STATEFUL & STATELESS

FIREWALLS

VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

FIREWALLS

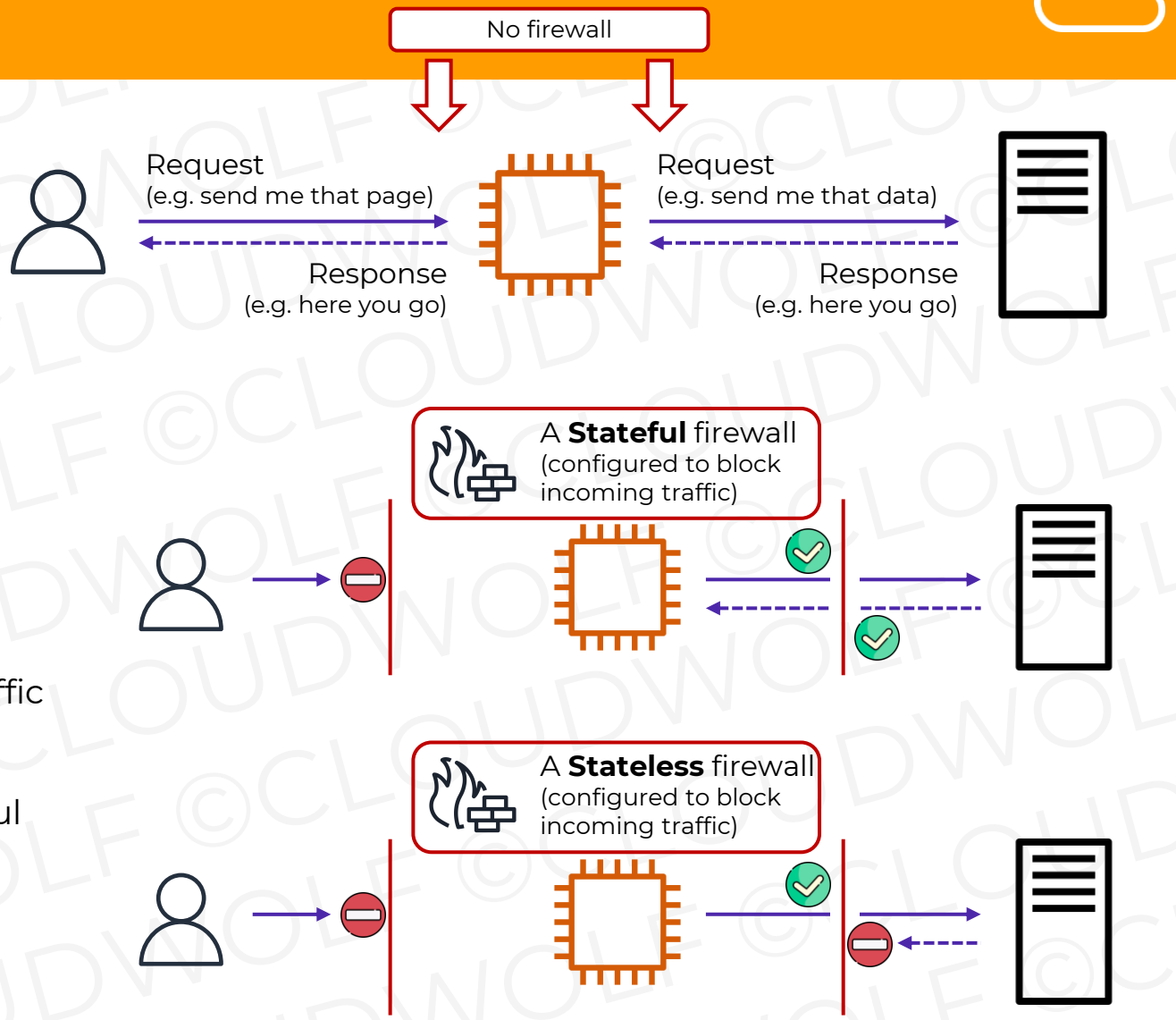
Stateful vs Stateless Firewalls:

- Every connection has two parts: **Request & Response**

- Stateful firewalls (*Security Groups in AWS*):
  - **understand the state of the connection**
  - and therefore will automatically allow any Response even if they are configured to block incoming traffic
  - cannot contain explicit denies*

- Stateless firewalls (*NACLs** in AWS*):
  - **do not understand the state of the connection (hence the name "state-less")**
  - and therefore will treat a Response like any other traffic
  - can contain explicit denies

- Due to their respective advantages and limitations, stateful and stateless firewalls are often used in combination



*Otherwise it wouldn't be able to guarantee that all Response traffic will be allowed.
**More on NACLs in an upcoming tutorial.

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



NACLs

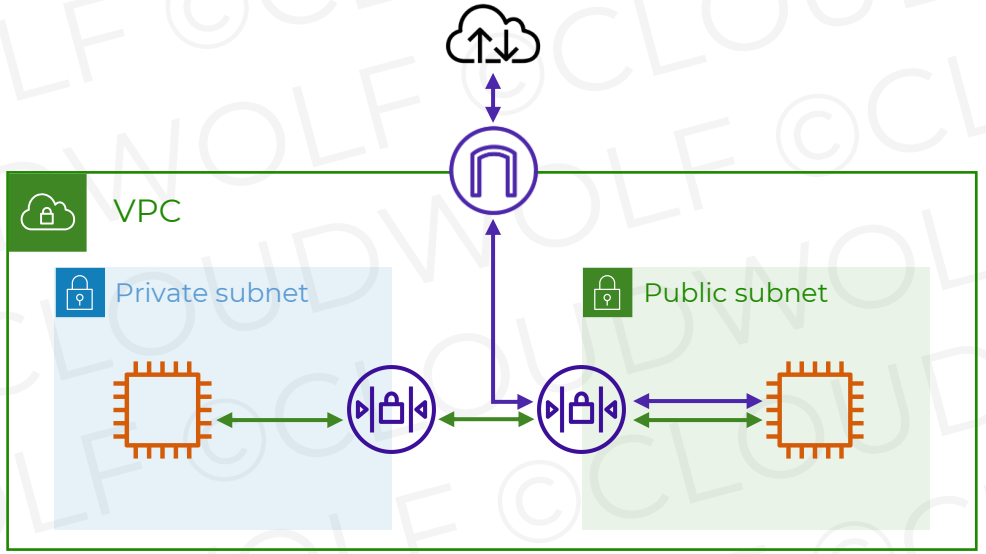
VPC

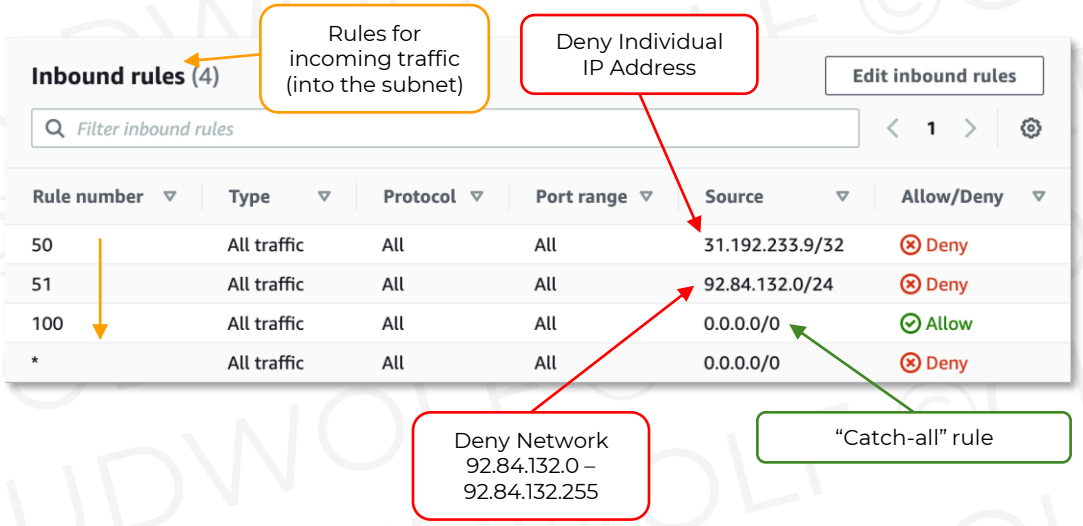
© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

Network ACLs

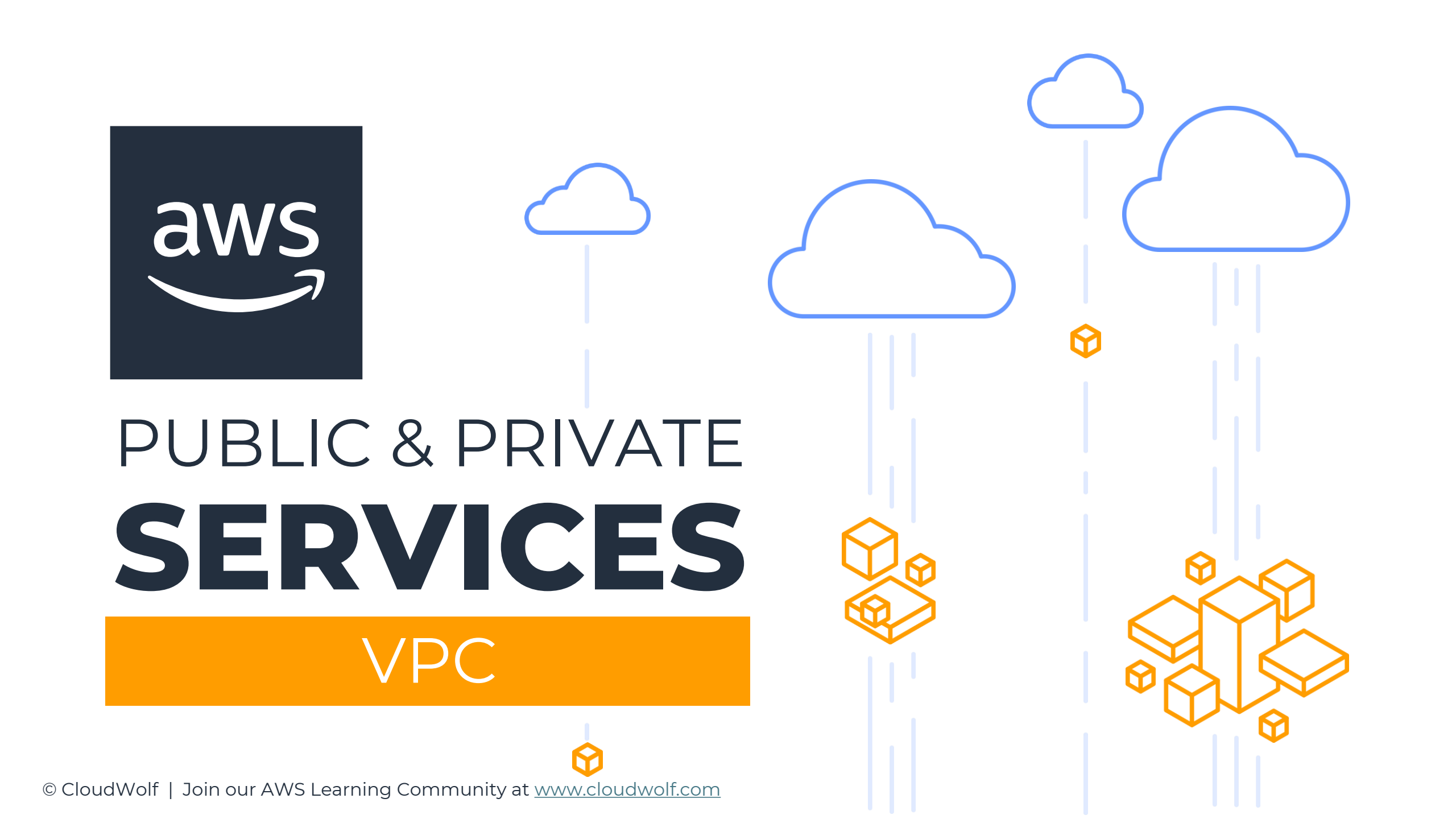
Network Address Control Lists (NACLs):

- A Network ACL (NACL) is a **Subnet-level firewall**
- A NACL is simply a list of rules: for Outbound and Inbound traffic
- Each VPC has a Default NACL and can have multiple Custom NACLs
- These NACLs are then assigned to ("associated with") Subnets
- Each Subnet **has to be associated with exactly one NACL**
- Each NACL can be associated with any number of Subnets
- **Note: a NACL cannot be attached to an individual resource** (unlike a Security Group)
- NACLs affect all traffic that **crosses the Subnet boundary**
  - This includes traffic within the VPC
  - And traffic going to/from the Public Internet
- **NACLs do not affect traffic flow within the same subnet**
- **NACLs are stateless firewalls,** i.e. they treat Responses like they treat any other traffic
- **NACLs can contain explicit denies** (useful for blocking malicious users, websites and networks)
- NACL Rule application:
  - For each connection **NACL Rules are processed in ascending order (based on rule number)** until a match is found
  - Once a match is found, **only that rule is applied**
  - Note: Default NACLs contain an explicit "Catch-all" rule: Allow
  - If no match is found, then the final (*) rule is applied: Deny





© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



PUBLIC & PRIVATE SERVICES

VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

PUBLIC & PRIVATE SERVICES

AWS Public & Private Services:

In AWS there are two types of services: Public and Private

Public Services:

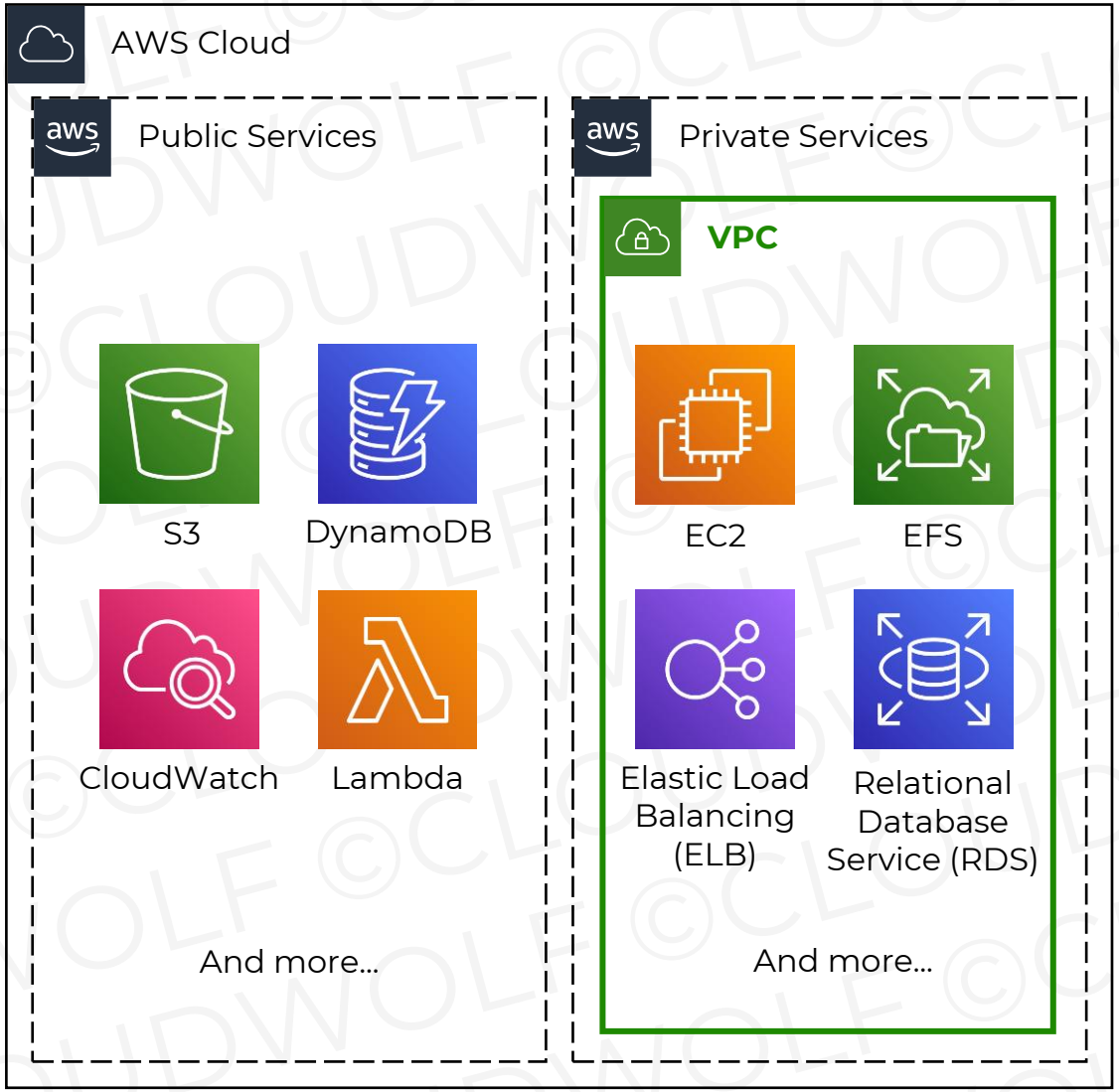
- Have Public IP Addresses (endpoints) which are used to connect to these services
- Are accessible from anywhere on the Public Internet
- Examples include S3, DynamoDB, CloudWatch, Lambda, ...

Private Services:

- Allow you to launch Private Resources* inside a VPC
- Examples include EC2, EFS, ELB, RDS, ...

There are several ways connect to Public Services from inside a VPC**:

- Using an Internet Gateway
- Using a Gateway Endpoint
- Using an Interface Endpoint



** Private Resources will be accessible from the Public Internet if placed in a Public Subnet*
*** More on this in upcoming tutorials*

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



GATEWAY & INTERFACE

ENDPOINTS

VPC



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

GW & INTERFACE ENDPOINTS

Gateway Endpoint:

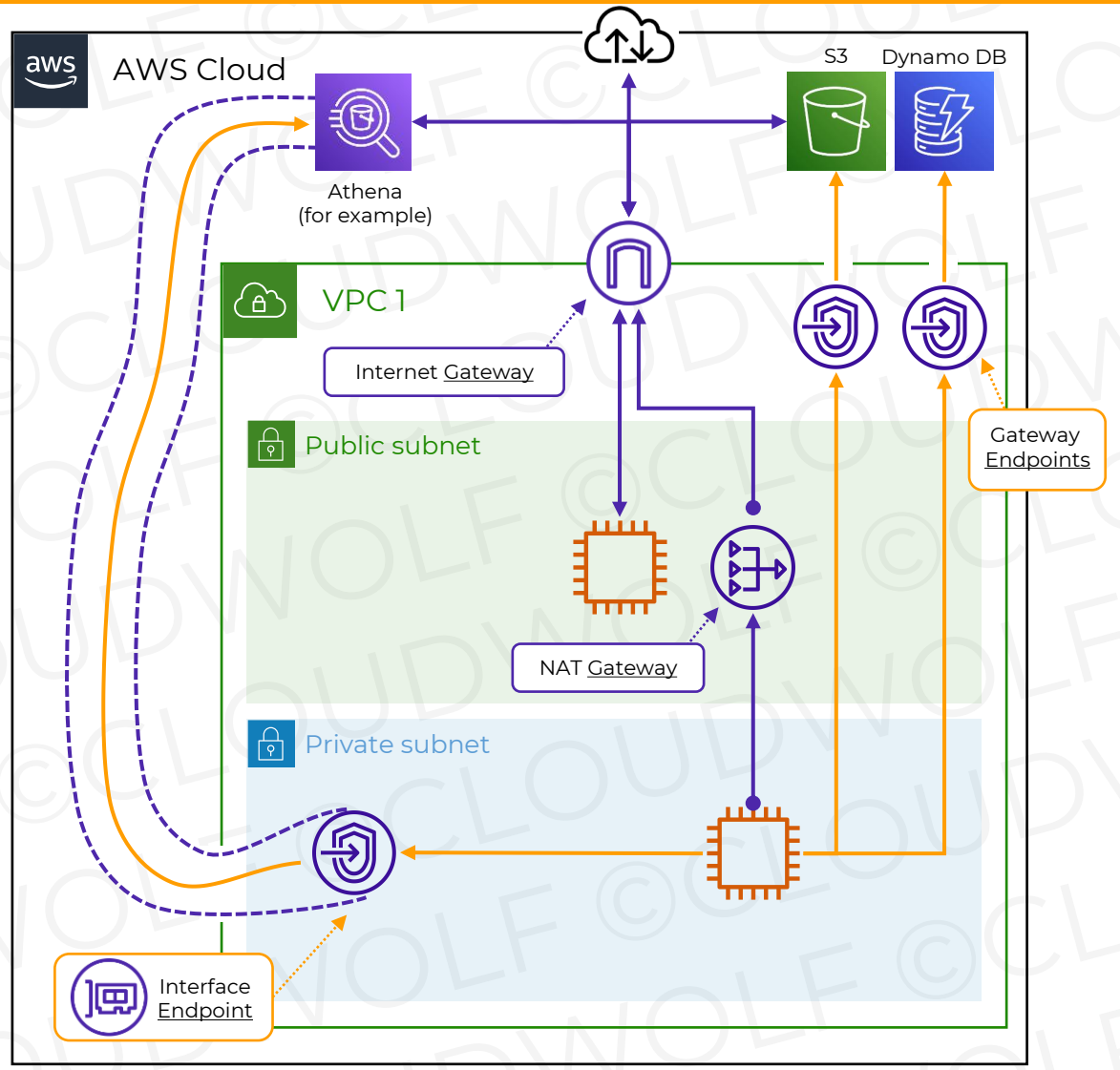
- Access AWS Managed Services bypassing the public internet
- Only for **S3 & Dynamo DB**
- GW Endpoint is a regional service
- GW Endpoints are attached to the VPC, not to Subnets
- Not accessible from outside the VPC

Interface Endpoint:

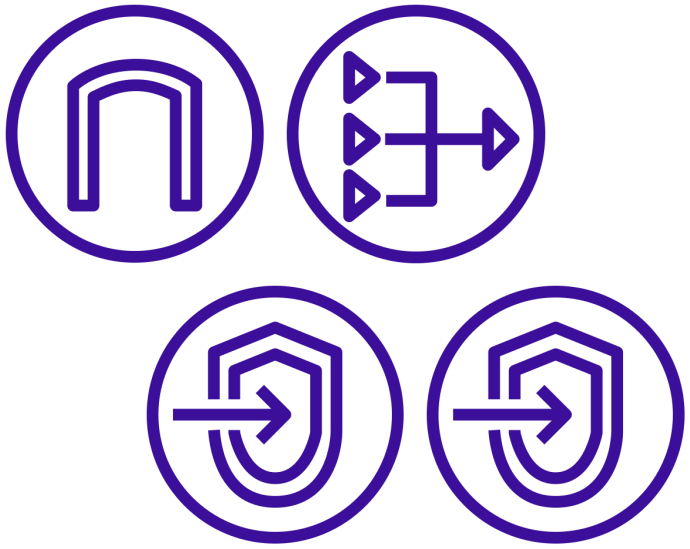
- Access AWS Managed Services bypassing the public internet
- For all other services
- Note: S3 is also supported
- Interface endpoint needs to be placed in a Subnet
- Can be placed in Public or Private Subnet
- Not accessible from outside the VPC

VPC Endpoint = Gateway / Interface Endpoint

- The term “VPC Endpoint” can refer to either a Gateway Endpoint or an Interface Endpoint depending on the context.



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



GATEWAYS vs ENDPOINTS

SIDE BY SIDE

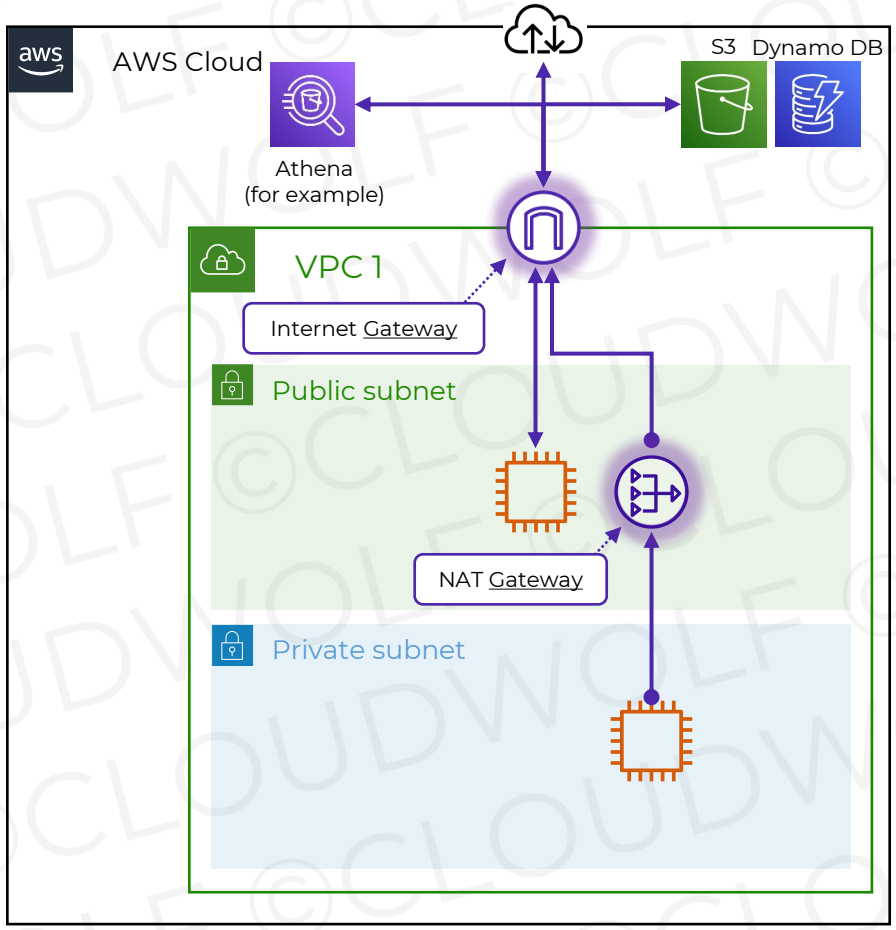
VPC

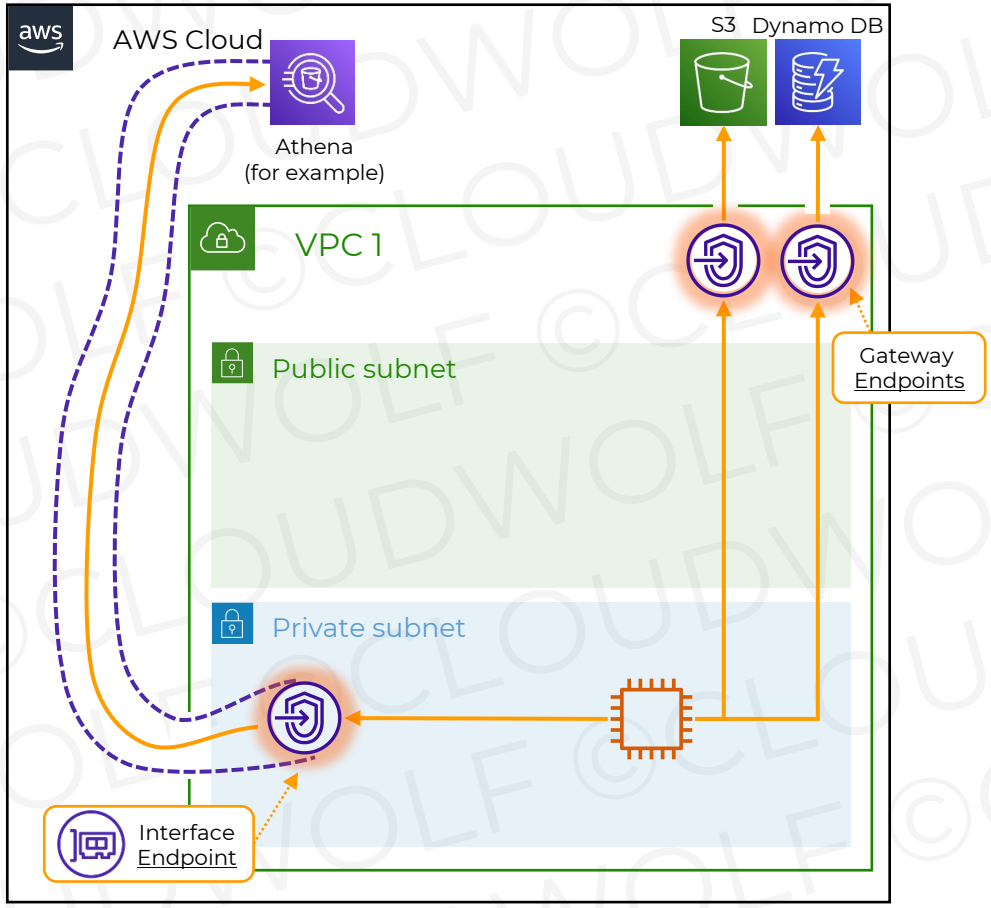


© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

GATEWAYS VS ENDPOINTS

Internet & NAT **Gateways** VS Gateway & Interface **Endpoints**





© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



PRIVATELINK

VPC



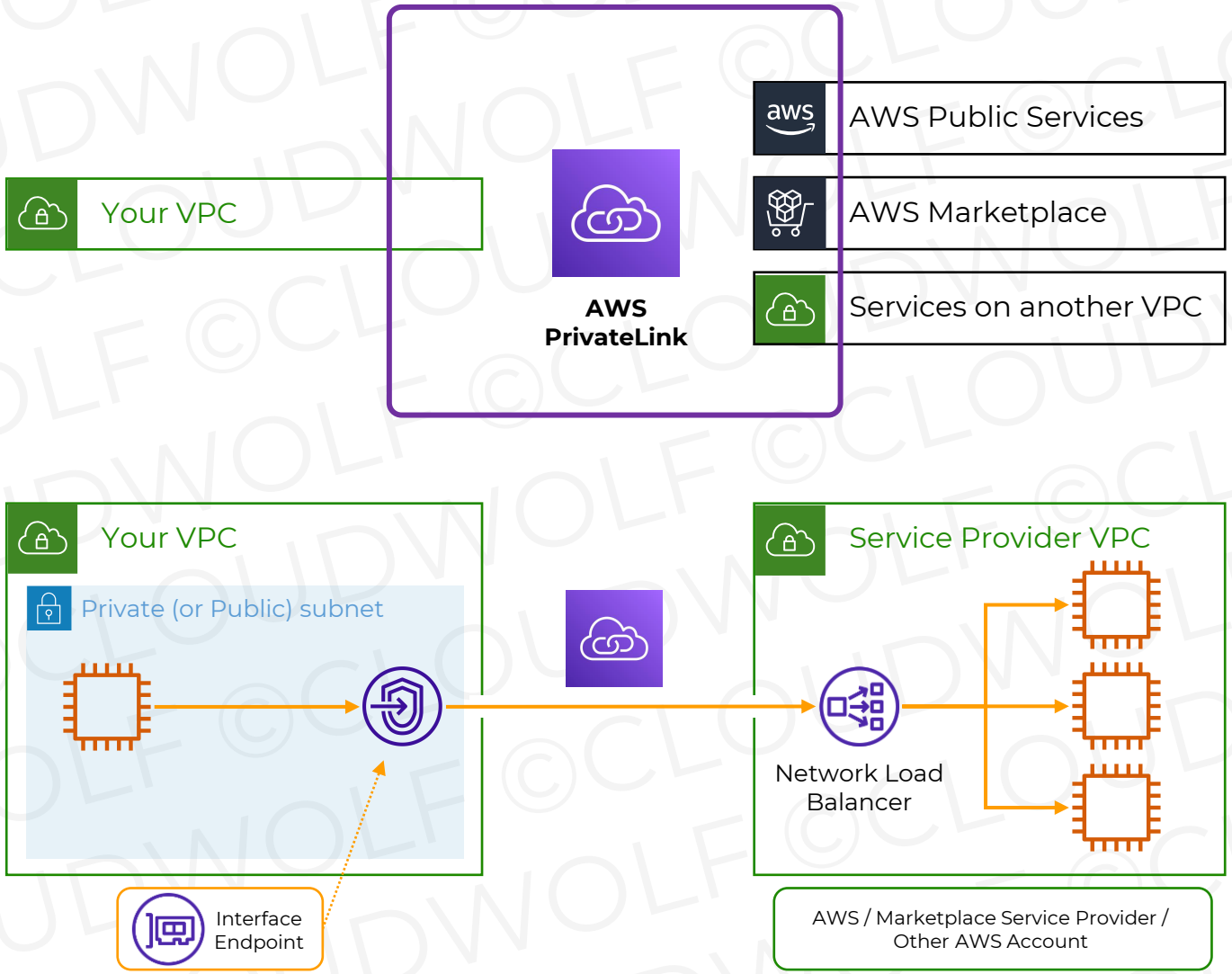
© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

PRIVATELINK

AWS PrivateLink:

- AWS PrivateLink is a highly available, scalable **technology** that enables you to **privately connect** your VPC to services as if they were in your VPC
- Traffic between your VPC and the services **does not leave the AWS Network**
- Service providers include AWS, Marketplace Service Providers, and other AWS Accounts

- PrivateLink is not a service, it's a technology
- PrivateLink is used by VPC Endpoints* (specifically by Interface Endpoints)
- PrivateLink does not require an Internet Gateway
- PrivateLink can work cross-region



(Advanced) Note: Gateway Endpoints do not use PrivateLink

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



VPC PEERING **CONNECTION**

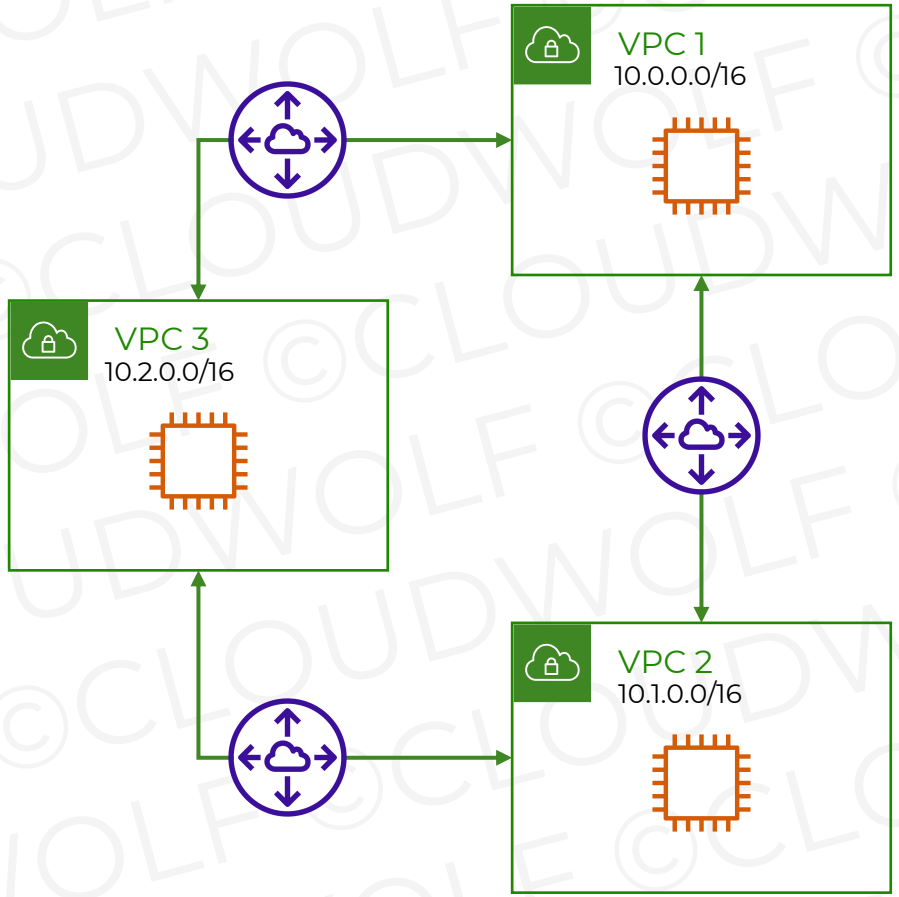
VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

VPC PEERING

VPC Peering:

- A VPC peering connection is a networking connection that enables you to **route traffic between two VPCs using private IP addresses**
- VPC peering traffic is isolated from the Public Internet, meaning that it is a **private connection**
- Instances in either VPC can communicate with each other as if they are within the same network*
- **CIDR Blocks of the two VPCs cannot overlap**
- VPCs can be in different accounts
- VPCs can be in different regions
- VPC Peering is **not transitive**
- There is no charge to create a VPC peering connection. However, usual charges for data transfer apply



** (Advanced) Note: After peering two VPCs, Routing Tables in each VPC will need to be modified to direct traffic accordingly and Security Groups will need to be configured to allow resources to communicate*

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



FLOW LOGS

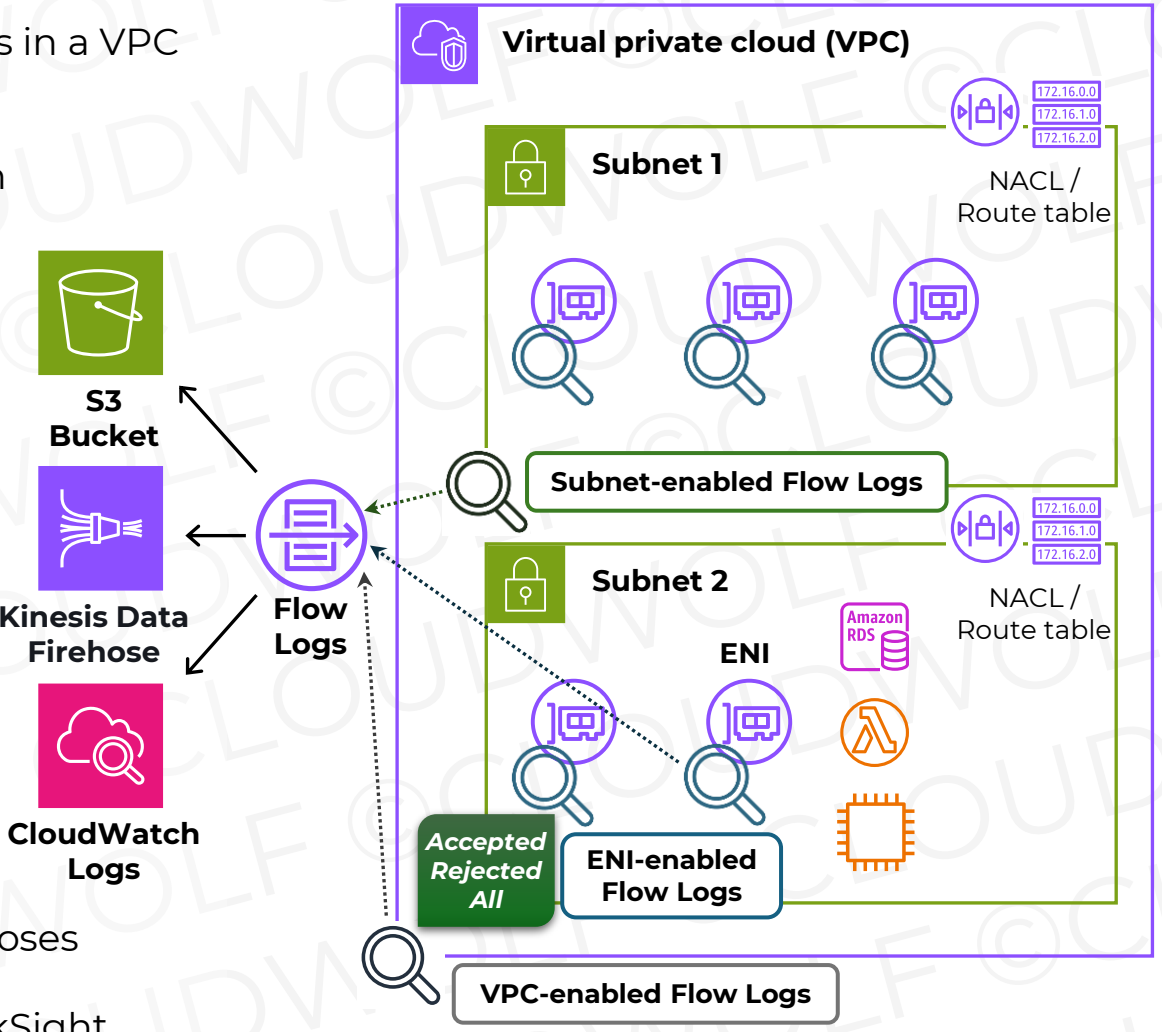
VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

VPC FLOW LOGS

VPC Flow Logs:

- **Capture detailed information about IP traffic** going to & from ENIs in a VPC
- Capture different levels of detail based on the filter specified: **accepted, rejected or all traffic**
- Always excluded traffic: DHCP within VPC, DNS requests to Amazon DNS servers and instance metadata (169.254.169.254)
- Logs data include: ENI, source/destination IPs, ports, protocol and acceptance/rejection status
- Ability to specify **custom log format** to incl./excl. metadata fields
- Each flow is aggregated into a unique flow log record within a **maximum aggregation interval** (set to either 1 or 10 minutes)
- Flow Logs can be created at different **scope** levels:
  - **ENI**
  - **Subnet** (all ENIs in that subnet)
  - **VPC** (all subnets and ENIs in that VPC)
- Flow Logs can be configured to **send data to**:
  - **CloudWatch Logs**
  - **Kinesis Data Firehose**
  - **S3 buckets**
- **Use-cases:**
  - Monitor traffic patterns and troubleshoot connectivity issues
  - Detailed network traffic log for forensics and compliance purposes
  - Insights into network efficiency and resource optimization
  - Analytics and reporting using services such as Athena or QuickSight



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



BASTION

VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

Bastion Hosts

EC2-based Bastion Host

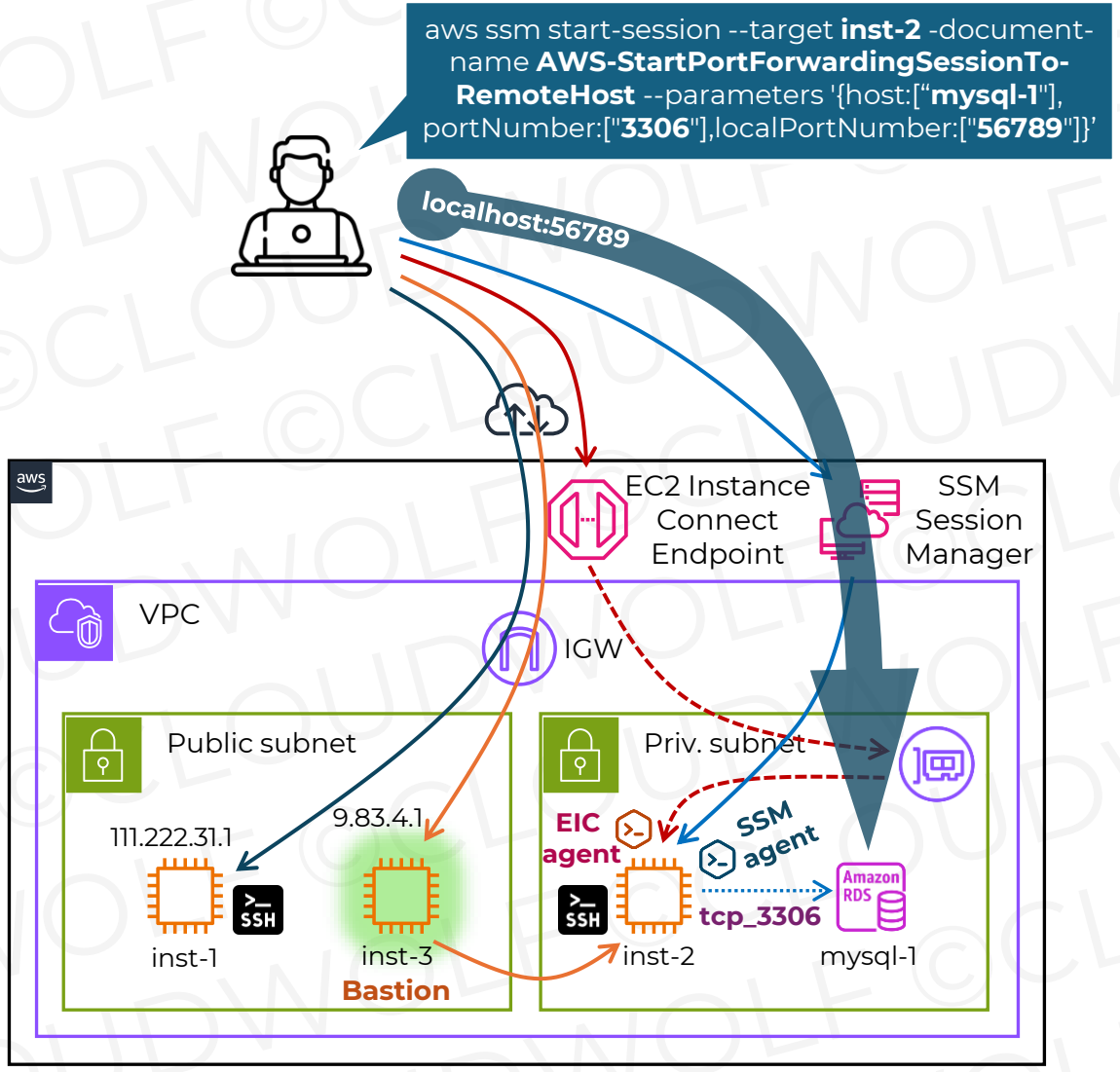
- Fortified entry point within a VPC for central management
- DIY approach: **install on EC2**, set-up access control, patches, etc.
- Security groups: allow traffic from bastion host to EC2 instances

EC2 Instance Connect Endpoint

- Managed bastion service, no need to set-up any bastion on EC2
- EC2 instances must have **EC2 Instance Connect agent** installed
- No need for the EC2 instances to have internet access
- Private connection from the client to the EIC endpoint via the AWS console, CLI, or SSH client
- Leverages **IAM-based permissions** for improved security
- Security groups: allow traffic from EIC endpoint to EC2 instances

SSM Session Manager

- Secure EC2 instance management via the AWS console or CLI
- No need to open SSH or RDP access on the EC2 instances
- Required on EC2 instances:
  - **SSM agent** (native in some AMI)
  - IAM role with appropriate permissions
  - Outbound connectivity to internet or to an SSM VPC endpoint
- Include a **port-forwarding feature** allowing to establish a private tunnel to access a specified host/port (only via AWS CLI)
  - Security groups: allow traffic from the EC2 instance to the specified host/port



© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com



IPv6

VPC

© CloudWolf | Join our AWS Learning Community at www.cloudwolf.com

IPv6 Support

IPv6 support in VPC:

- Amazon VPC supports **both IPv4 and IPv6** for most resources in a VPC
- IPv6 CIDR blocks can be allocated to VPCs (/56 mask) and subnets (/64 mask) to enable IPv6 communication
- IPv6 addresses can be assigned to EC2 instances, ENIs, ELBs, and other relevant resources
- All IPv6 addresses are publicly addressable - **no need for EIP**
- Use an **egress-only internet gateway** to provide internet connectivity for IPv6-only resources within **private subnets** (outbound-only traffic)
- Route tables need to be configured to direct IPv6 traffic properly within a VPC and to external networks
- Other VPC features that support IPv6:
  - NACLs
  - Security groups
  - VPC endpoints
  - VPC peering
  - Transit gateway
  - Direct connect
  - Client VPN and site-to-site VPN
  - Flow logs

