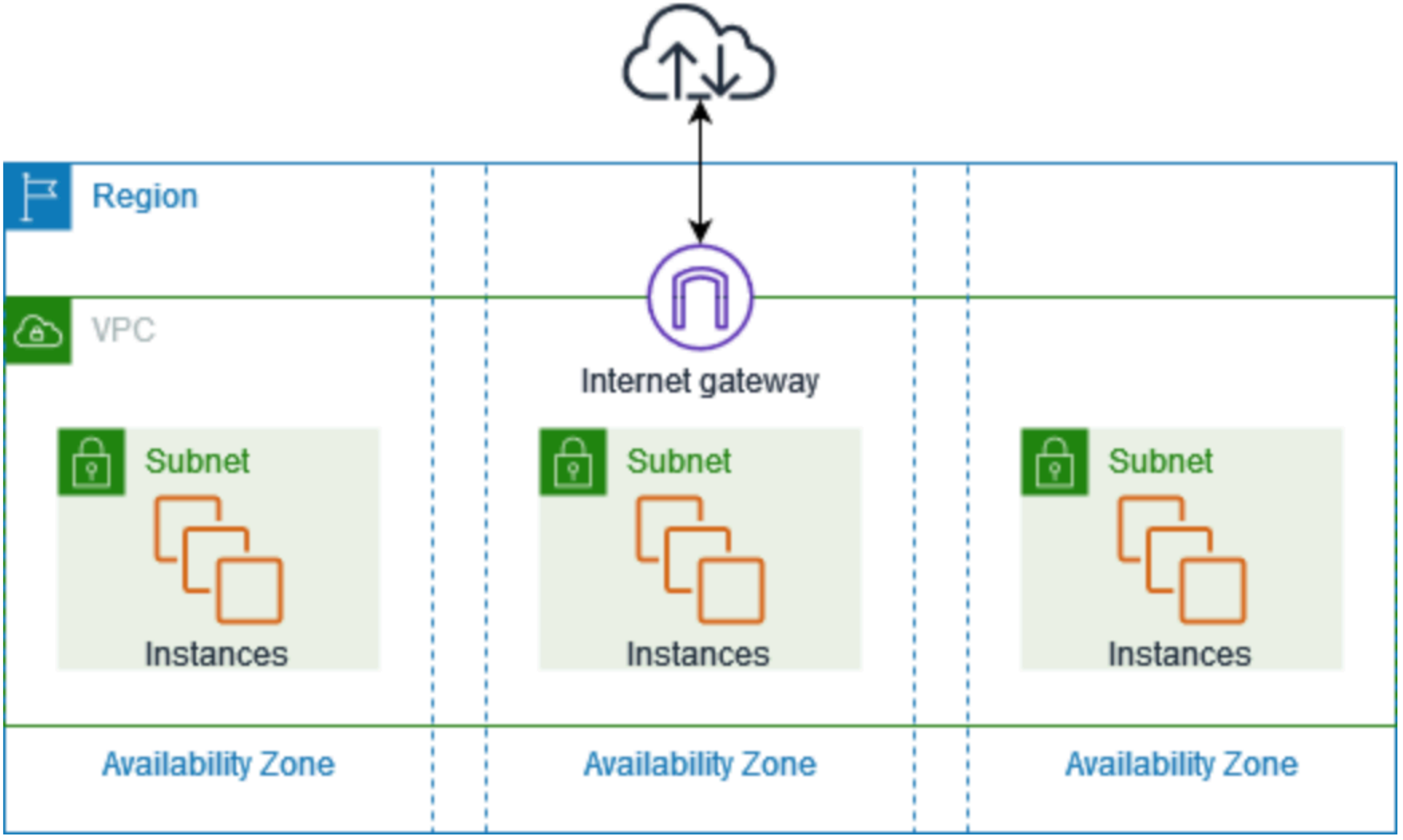
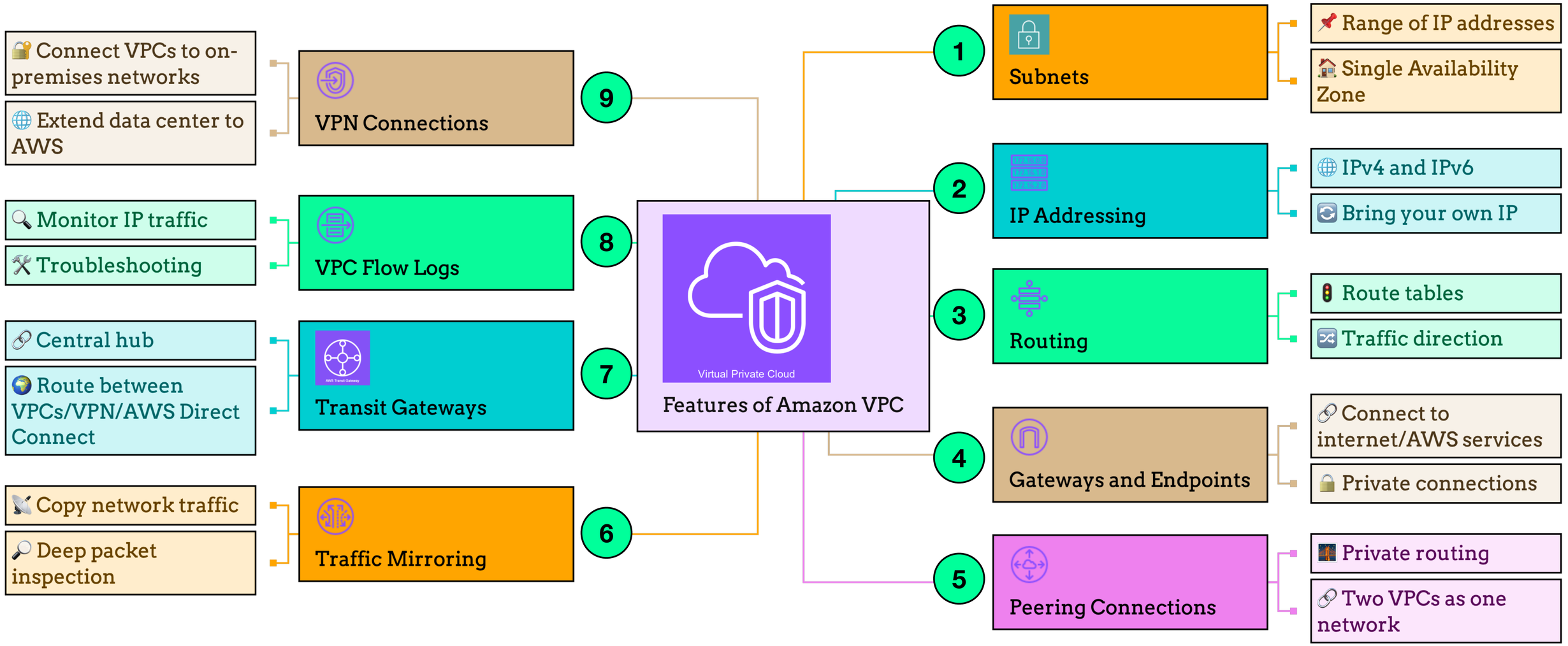
Amazon Virtual Private Cloud (VPC)

What is Amazon VPC?.

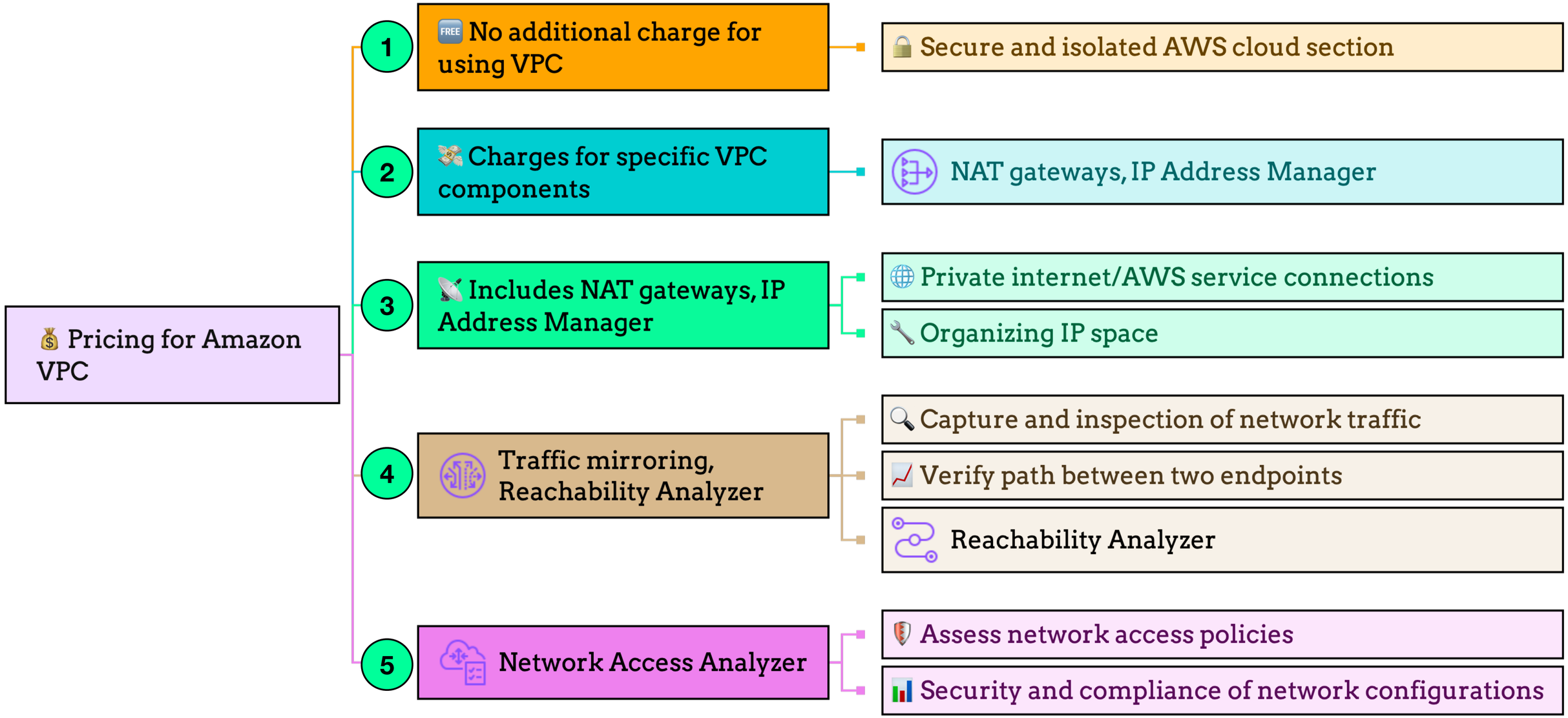
1. 🛠️ Logically isolated network
   - 🚀 Deploys AWS resources
   - 🔧 Control over networking
2. 🌍 Traditional network with scalability
   - 🔄 AWS's scalable infrastructure
3. 🌐 Internet gateway integration
   - 📡 Communicates with internet
4. 📡 Subnet creation
   - 🏢 Across Availability Zones
5. 🔒 Enhanced security and privacy
   - 🛡️ Secure instance communication


Region
VPC
Internet gateway
Subnet
Instances
Subnet
Instances
Subnet
Instances
Availability Zone
Availability Zone
Availability Zone

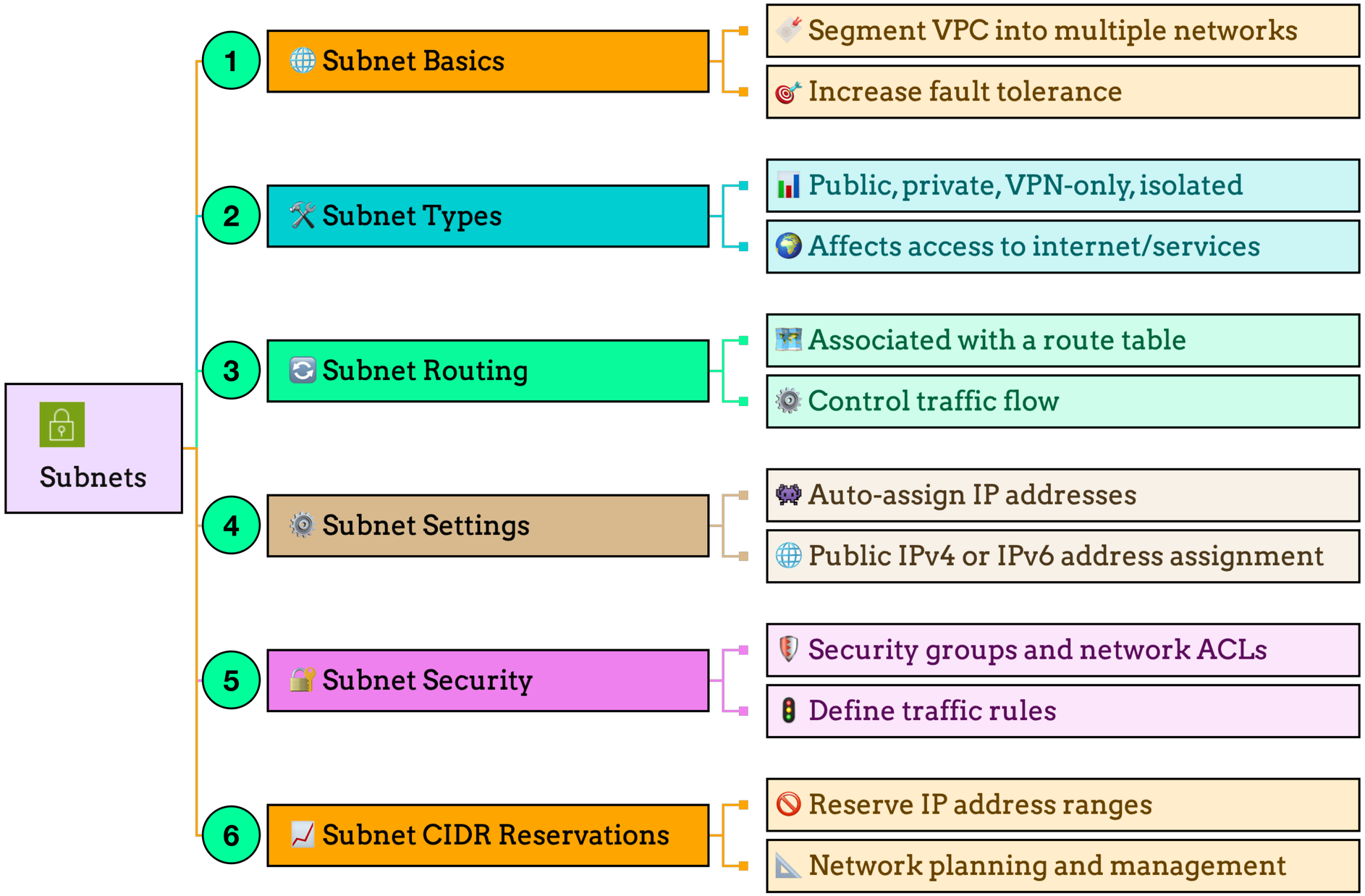
Features of Amazon VPC.



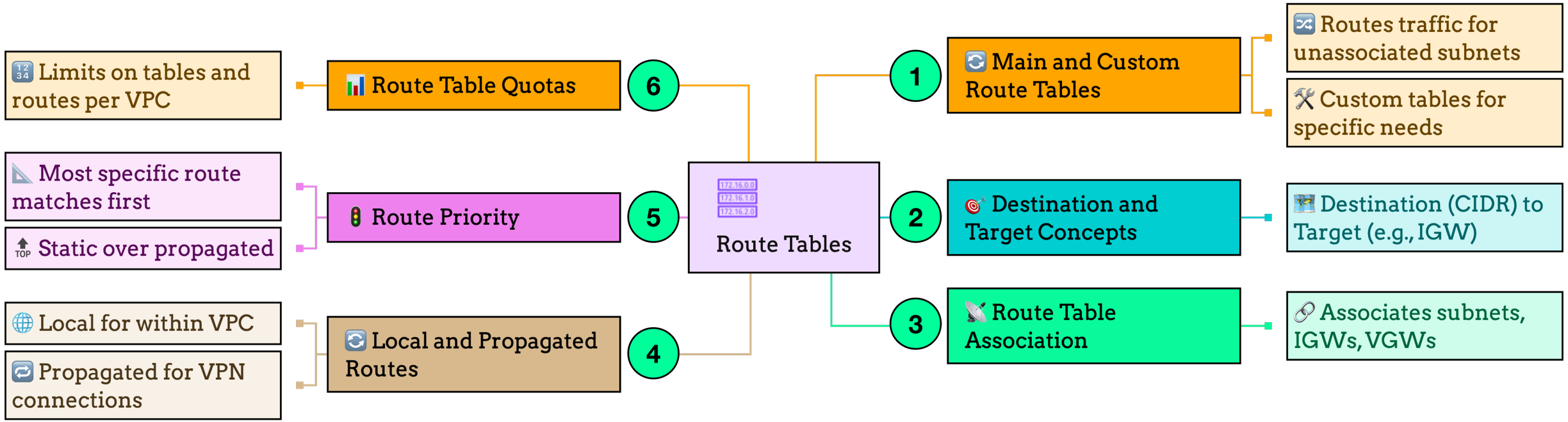
💰 Pricing for Amazon VPC.



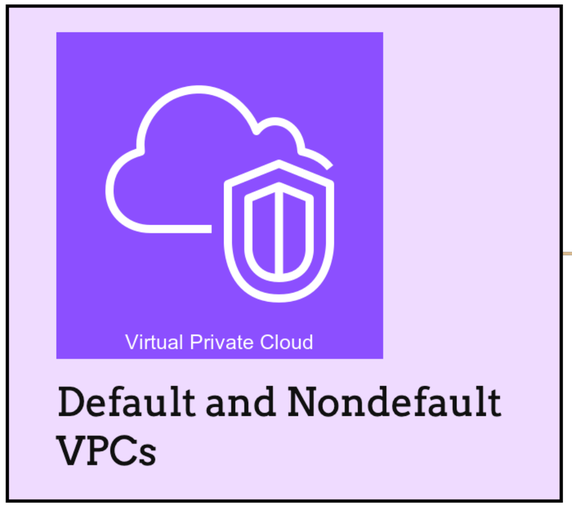
Everything You Need to Know About Subnets.



Everything You Need To Know About Route Tables.



Default and Nondefault VPCs.



1. Default VPC Features
   - After December 4, 2013
   - Subnet in each AZ
   - Internet gateway and direct access
2. Nondefault VPC Customization
   - Tailored to specific needs
   - Granular control over configurations
3. Default VPC in Every Region
   - Immediate instance deployment
   - Quick start for AWS services
4. Configurable Components
   - Add more subnets
   - Adjust route tables
   - Modify network access controls

How to Access the Internet ?

🌐 How to Access the Internet

1. Create and Attach an Internet Gateway
   - 🔗 Bridge between VPC and internet
   - 📡 Supports IPv4 and IPv6 traffic
2. Add Route to the Route Table
   - 🚦 Directs internet-bound traffic
   - 🌍 Ensures data packets navigate in and out of VPC
3. Public IP for Instances
   - 🌐 Required for internet connection
   - 🔑 Automatically assigned in certain subnets
4. 🔐 Configure Security Groups and NACLs
   - 🛡️ Manage inbound and outbound traffic
   - 🔒 Secure and controlled access
5. Use a NAT Device for Private Subnets
   - 🔧 Allows internet access without public IP
   - 🛡️ Prevents direct internet initiations

🚀 Get Started with Amazon VPC

- 🌐 **Determine your IP address ranges**: Decide on the IP address ranges for your VPC and subnets, ensuring they do not overlap with other networks you may be connected to. This is crucial for the network planning of your VPCs.
- 📍 **Select your Availability Zones**: Choose Availability Zones within an AWS Region to deploy your VPC resources. This decision impacts the redundancy and fault tolerance of your applications.
- 🌍 **Plan your internet connectivity**: Consider how your VPC will connect to the internet. This may involve setting up an internet gateway, NAT devices, or configuring route tables for your subnets.
- 🛠️ **Create your VPC**: Utilize the AWS Management Console, AWS CLI, or AWS SDKs to create your VPC. You can customize your VPC to suit your specific network requirements.
- 🚀 **Deploy your application**: Once your VPC is set up, you can start deploying applications. This involves launching AWS resources such as EC2 instances within your VPC subnets.

🌐 What is an IPv4 Address?.

🌐 What is an IPv4 Address?

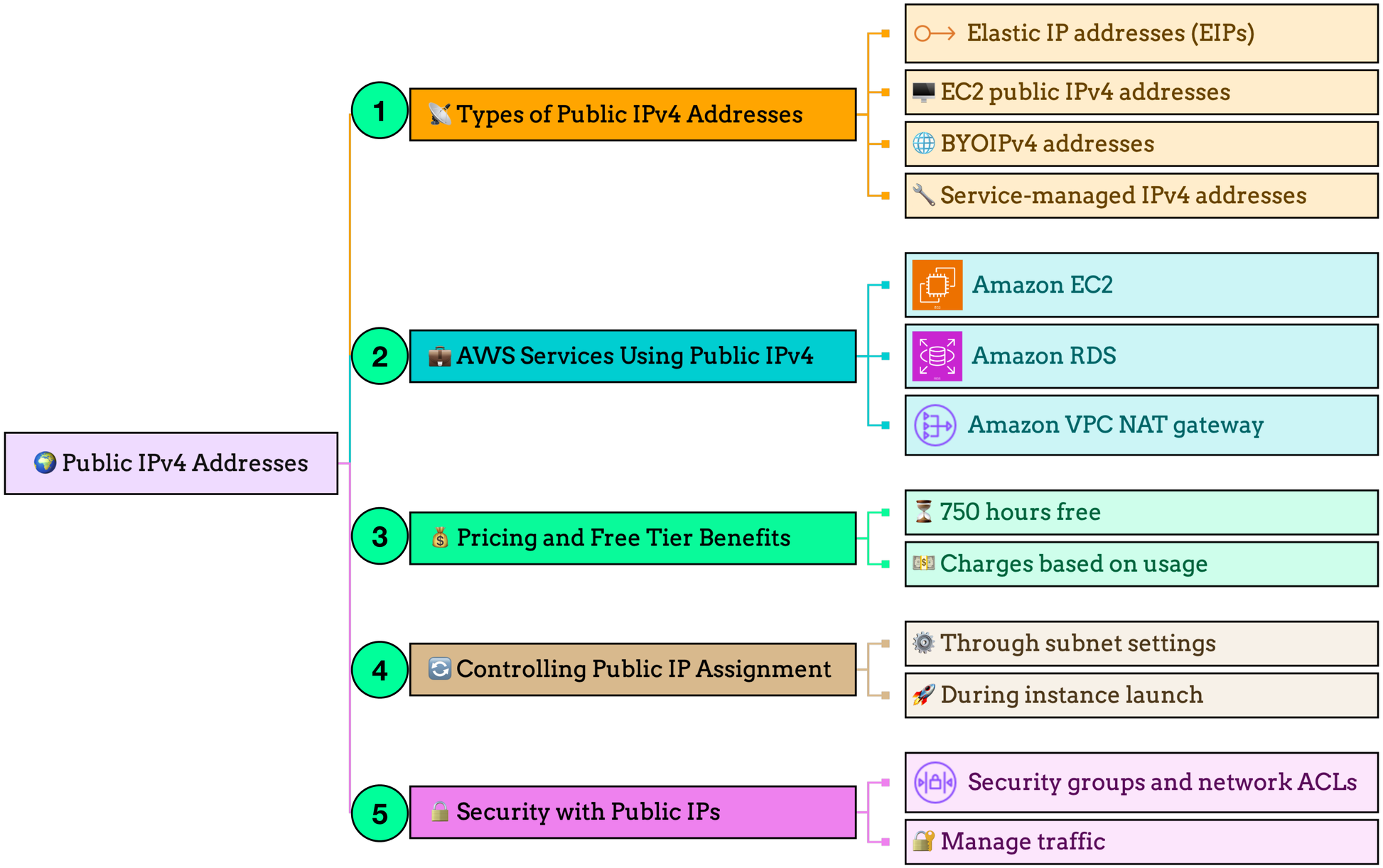
1. 📄 32-bit numerical label → 🔢 Enables unique IP addresses
2. 🌍 Represented in decimal format → 🔗 Expressed as dotted decimal
3. 🔄 Divided into 4 octets → 📊 Enhances network organization
4. 🔢 Each ranging from 0-255 → 📐 Delineates the address space
5. 📌 Example: 10.0.1.0 → 🏷️ Showcases structure and format
6. 🚀 Allows for over 4 billion unique addresses → 🌎 Caters to numerous devices globally
7. 🛣️ Essential for internet communication → 🔌 Fundamental for internet architecture

```
Valid IP Address Range: [0..255,0..255,0..255,0..255]
from 0.0.0.0 to 255.255.255.255
```

🔒 Private IPv4 Addresses

- 🚫 **Not internet-reachable**: Private IPv4 addresses are isolated from the internet, ensuring secure internal communications within the VPC.
- 🌐 **Communication within VPC**: These addresses facilitate seamless interaction between instances housed in the same virtual private cloud.
- 🏷️ **Assigned at instance launch**: When an instance is launched within a VPC, it automatically receives a primary private IPv4 address from the subnet's address range.
- 📝 **Support for multiple addresses**: Instances can be assigned additional private IP addresses, known as secondary addresses, for flexible network configurations.
- 🔄 **Reassignable secondary addresses**: Secondary private IPv4 addresses can be moved from one network interface to another, offering dynamic network management.
- 🚦 **Governed by CIDR range**: The allocation of private IPv4 addresses is determined by the IPv4 CIDR range specified for the VPC, usually within RFC 1918 designated private address spaces.
- 🛡️ **Private (non-publicly routable)**: These addresses reside within designated IP ranges that are not routable on the internet, enhancing security and network integrity.

Public IPv4 Addresses.



🔗 IPv6 Addresses.

- 🔗 IPv6 Addresses
  1. 🆕 Introduction to IPv6
     - 🔄 Supplement and replace IPv4
     - 🚫 Solves address exhaustion
  2. 📈 Expanded Address Space
     - 🔢 128 bits long
     - 💡 Significantly more addresses
  3. 🌐 IPv6 Address Format
     - ✏️ Eight groups of four hexadecimal digits
     - 📏 Larger address space than IPv4
  4. 🔍 Unique Local Addresses (ULAs)
     - 🏠 For local network communication
     - 📊 Larger scope for uniqueness
  5. 📡 Global Unicast Addresses
     - 🌍 Globally unique and internet-routable
     - 🖥️ For public internet-facing resources
  6. 🛠️ IPv6 in AWS
     - ✔️ Supported across various services
     - 🔗 Including Amazon VPC
  7. 🚀 Benefits of Using IPv6
     - ❌ Eliminates need for NAT
     - 🔧 Simplifies address assignment
     - 🔒 Enhances security features

340,282,366,920,938,463,463,374,607,431,768,211,456 addresses

The size of an IPv6 address is 128 bits, compared to 32 bits in IPv4. The address space therefore has 2^{128}=340,282,366,920,938,463,463,374,607,431,768,211,456 addresses (340 undecillion, approximately 3.4×10^{38}). Some blocks of this space and some specific addresses are reserved for special uses.

🌐 IPv4 VPC CIDR Blocks

- 📐 **Range of allowed block sizes**: When creating a VPC, you must specify an IPv4 CIDR block. The allowed sizes range from /16 netmask (65,536 IP addresses) to /28 netmask (16 IP addresses). Associating additional IPv4 CIDR blocks with the VPC is possible after its creation.
- 🏠 **Recommended private IPv4 address ranges**: It's recommended to specify a CIDR block from the private IPv4 address ranges defined in RFC 1918 (e.g., 10.0.0.0/16, 172.31.0.0/16, and 192.168.0.0/20).
- 🚫 **Avoid using 172.17.0.0/16 CIDR range**: Some AWS services use the 172.17.0.0/16 range. To prevent conflicts, this range should not be used for creating your VPC. Conflicts might arise with services like AWS Cloud9 or Amazon SageMaker.
- 🔍 **Publicly routable CIDR blocks**: You can create a VPC with a publicly routable CIDR block that falls outside the private IPv4 address ranges specified in RFC 1918. However, these are still considered private IP addresses within the context of your VPC.
- ✅ **Service-specific configuration requirements**: When creating a VPC for use with an AWS service, it's essential to check the service documentation for any specific configuration requirements.

Total VPC Calculation - 1

RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	192.168.0.0/20

```
You can create 256 Unique VPCs with a netmask of "/16" within 10.0.0.0 - 10.255.255.255
CIDR Range.

VPC1=10.0.0.0/16
VPC2=10.1.0.0/16
VPC3=10.2.0.0/16
VPC256=10.255.0.0/16

Each VPC can have 256*256=65,536 IP Addresses.
```

Total VPC Calculation - 2

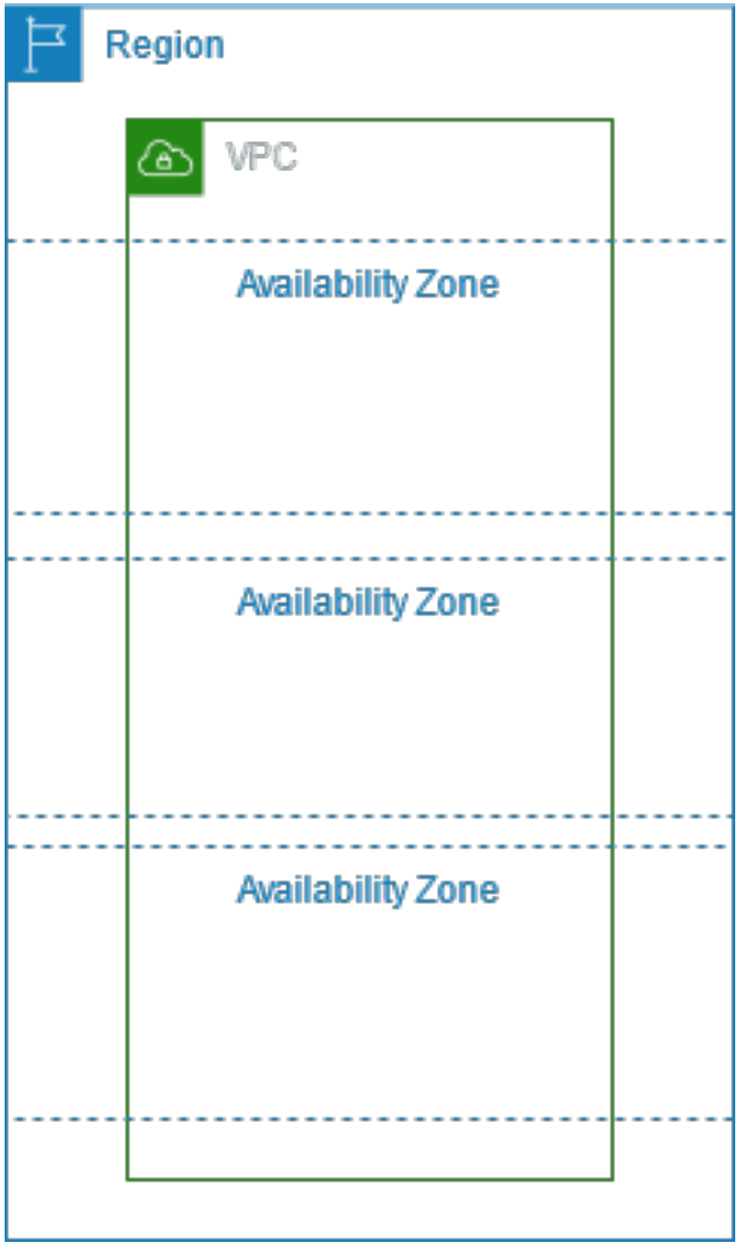
RFC 1918 range	Example CIDR block
10.0.0.0 - 10.255.255.255 (10/8 prefix)	10.0.0.0/16
172.16.0.0 - 172.31.255.255 (172.16/12 prefix)	172.31.0.0/16
192.168.0.0 - 192.168.255.255 (192.168/16 prefix)	192.168.0.0/20

```
You can create 16 Unique VPCs with a netmask of "/16" within 172.16.0.0 - 172.31.255.255
CIDR Range.

VPC1=172.16.0.0/16
VPC2=172.17.0.0/16
VPC3=172.18.0.0/16
VPC16=172.31.0.0/16

Each VPC can have 256*256=65,536 IP Addresses.
```

Subnet CIDR Blocks.

1. 📊 CIDR notation for subnet IP addresses
   - 🌐 Classless Inter-Domain Routing
   - 🔁 Identical or subset of VPC's CIDR
2. 🔄 Subset creation for multiple subnets
   - 🔢 Divide VPC's CIDR block
   - 👥 Supports multiple IP addresses
3. 🛠️ Tools for subnet CIDR block calculation
   - 🔍 Online calculators and tools
   - 🌍 Determine IPv4 and IPv6 blocks
4. 🚫 Reserved IP addresses in subnets
   - 🚷 First four and last IP not assignable
   - 🛑 Includes network, VPC router, AWS DNS
5. 📐 Allowed CIDR block sizes for IPv4 and IPv6
   - 📏 IPv4: /28 to /16 netmask
   - 📏 IPv6: /44 to /64 in /4 increments

Basic VPC



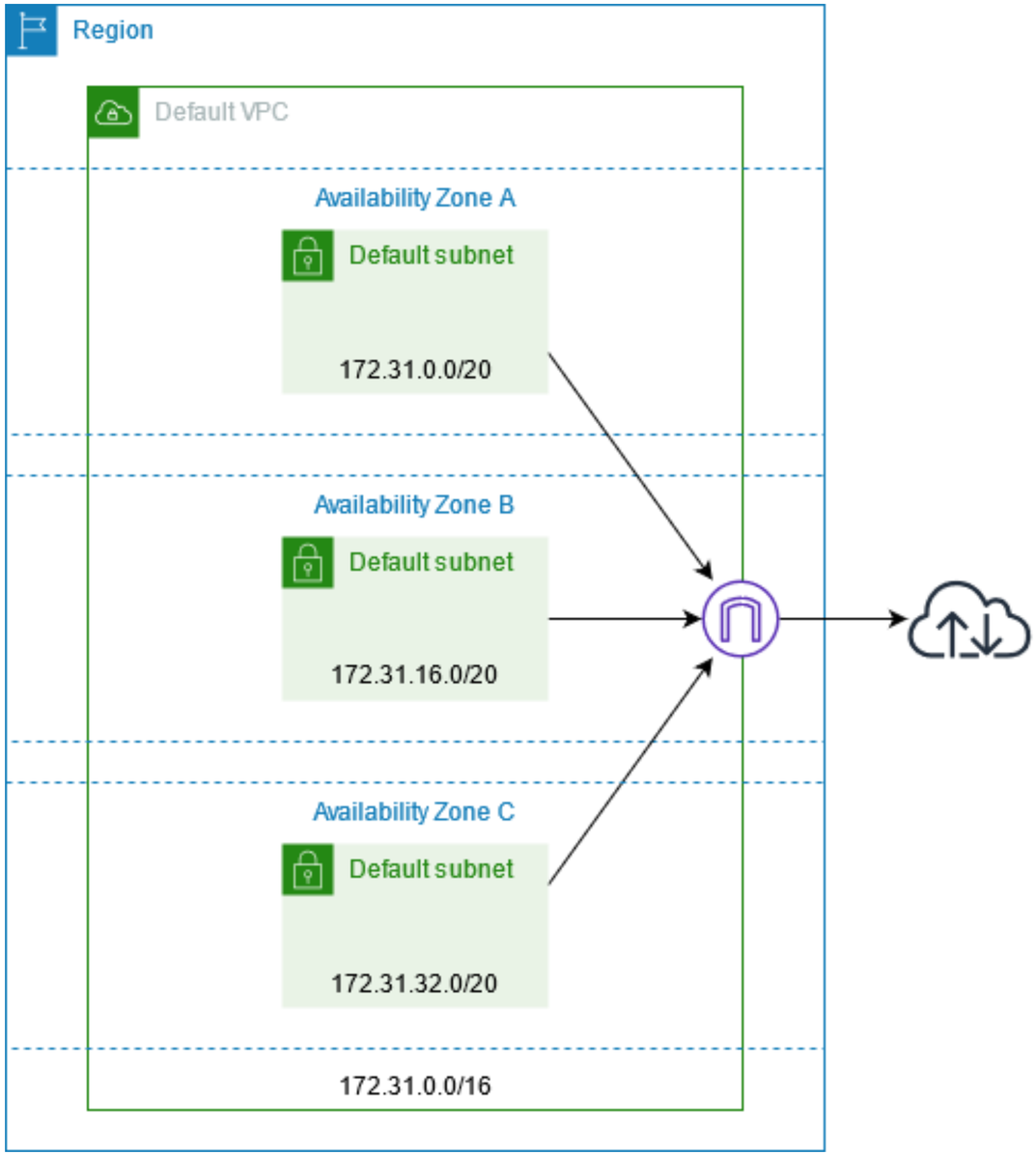
Each VPC automatically comes with the following resources:

1. Default DHCP option set
2. Default network ACL
3. Default security group
4. Main route table

You can create the following resources for your VPC:

1. Network ACLs
2. Custom route tables
3. Security groups
4. Internet gateway
5. NAT gateways

Default VPC



The following diagram shows a Default VPC with a default subnet in each of the Availability Zones.

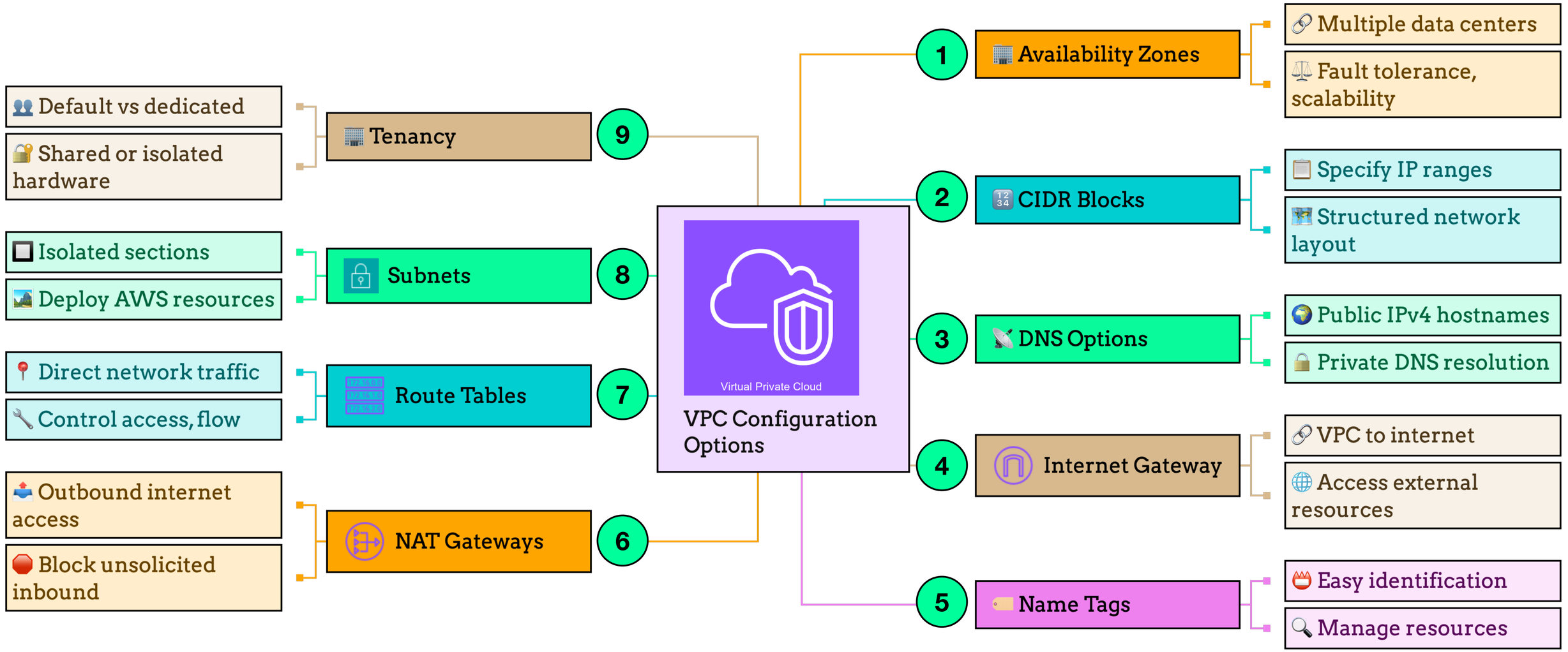
VPC's CIDR Range is 172.31.0.0/16.

The 3 Subnets have a range of 172.31.0.0/20, 172.31.16.0/20 and 172.31.32.0/20 respectively.

The Route Table contains an entry to allow egress public internet connectivity via the internet gateway.

Destination	Target
172.31.0.0/16	local
0.0.0.0/0	*internet_gateway_id*

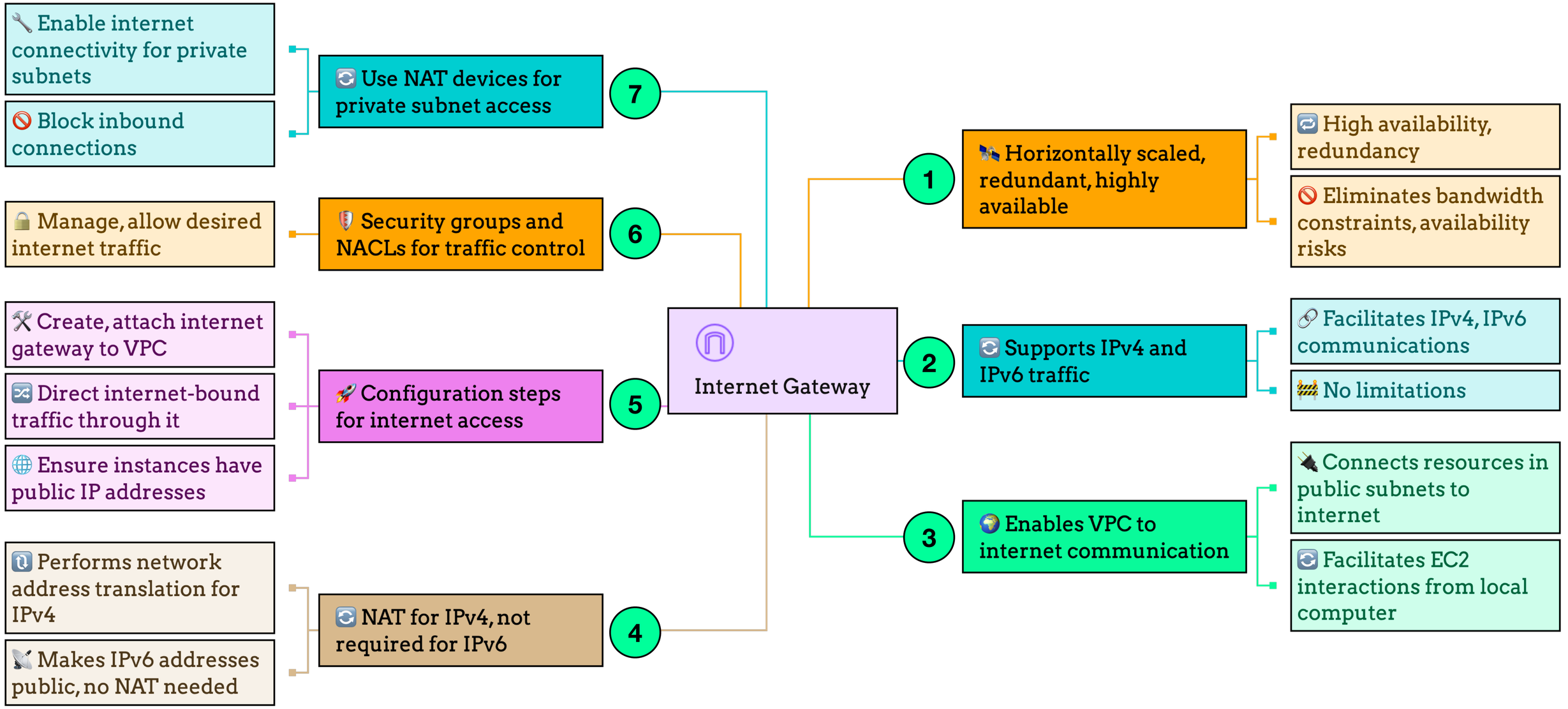
VPC Configuration Options.



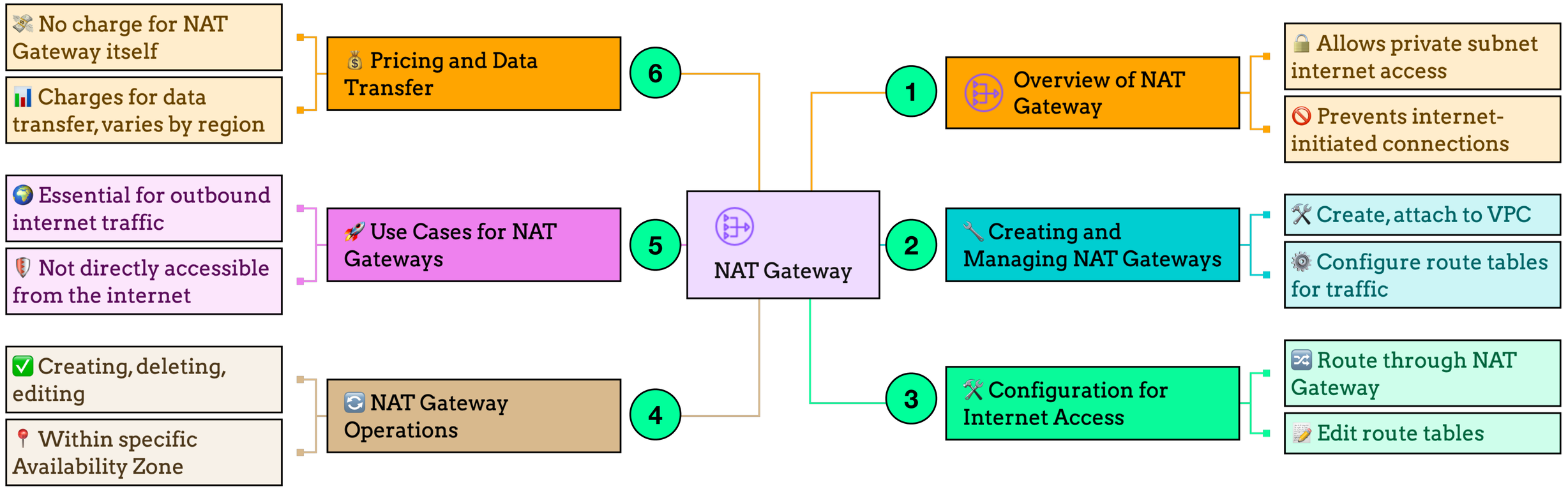
🌐 How to Create a VPC

- 🖥️ **Open Amazon VPC Console**: Navigate to `https://console.aws.amazon.com/vpc/` to access the VPC management console.
- ➕ **Choose "Create VPC"**: On the VPC dashboard, click the "Create VPC" button to initiate the process.
- 📝 **Specify VPC and Subnet Details**: Choose between creating a VPC with additional resources or a VPC only. Provide Name tags as desired.
- 🌍 **Set IPv4 and IPv6 CIDR Blocks**: Enter the IPv4 address range mandatory for the VPC and optionally set the IPv6 CIDR block for dual-stack IP addressing.
- 🔄 **Select Tenancy Option**: Decide whether EC2 instances will run on shared hardware (Default) or dedicated hardware (Dedicated).
- 🏞️ **Choose Availability Zones**: For high availability, select at least two Availability Zones (AZs) for your subnets.
- 🌐 **Configure Subnets**: Determine the number of public and private subnets and their respective CIDR blocks.
- 🔧 **Optional Configurations**: Include configurations like NAT gateways, Egress-only Internet Gateways, VPC Endpoints, and DNS options as needed.
- 🏷️ **Add Additional Tags**: Optionally, add tags for easier management and identification of your VPC resources.
- ✅ **Review and Create**: Finalize your configurations in the Preview pane and then click "Create VPC" to provision your new VPC.

Everything You Need to Know About Internet Gateway.



Everything You Need To Know About NAT Gateway.



Thanks for Watching

Amazon Virtual Private Cloud (VPC) - Part 2

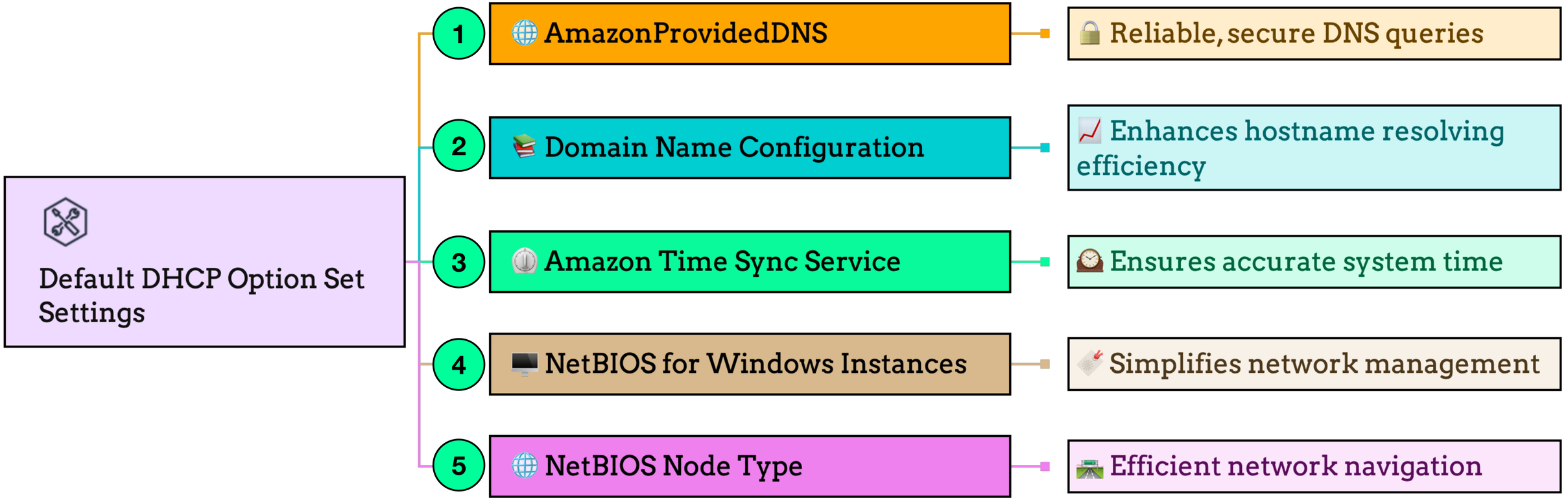
🔄 What is DHCP?

- 🌍 **TCP/IP Network Requirement**: Every device on a TCP/IP network needs an IP address to communicate. Previously, IP addresses were assigned manually to each device.
- 🔄 **Dynamic IP Assignment**: Nowadays, IP addresses are assigned dynamically using the Dynamic Host Configuration Protocol (DHCP), streamlining network administration.
- 📡 **Communication with Amazon DHCP Servers**: Applications on EC2 instances can interact with Amazon DHCP servers to retrieve their IP address lease or other network configuration details, such as the DNS server's IP address.
- 🛠️ **DHCP Option Sets Configuration**: You can customize network configurations provided by Amazon DHCP servers using DHCP option sets, allowing for specific network settings within your VPC, enhancing network setup flexibility.

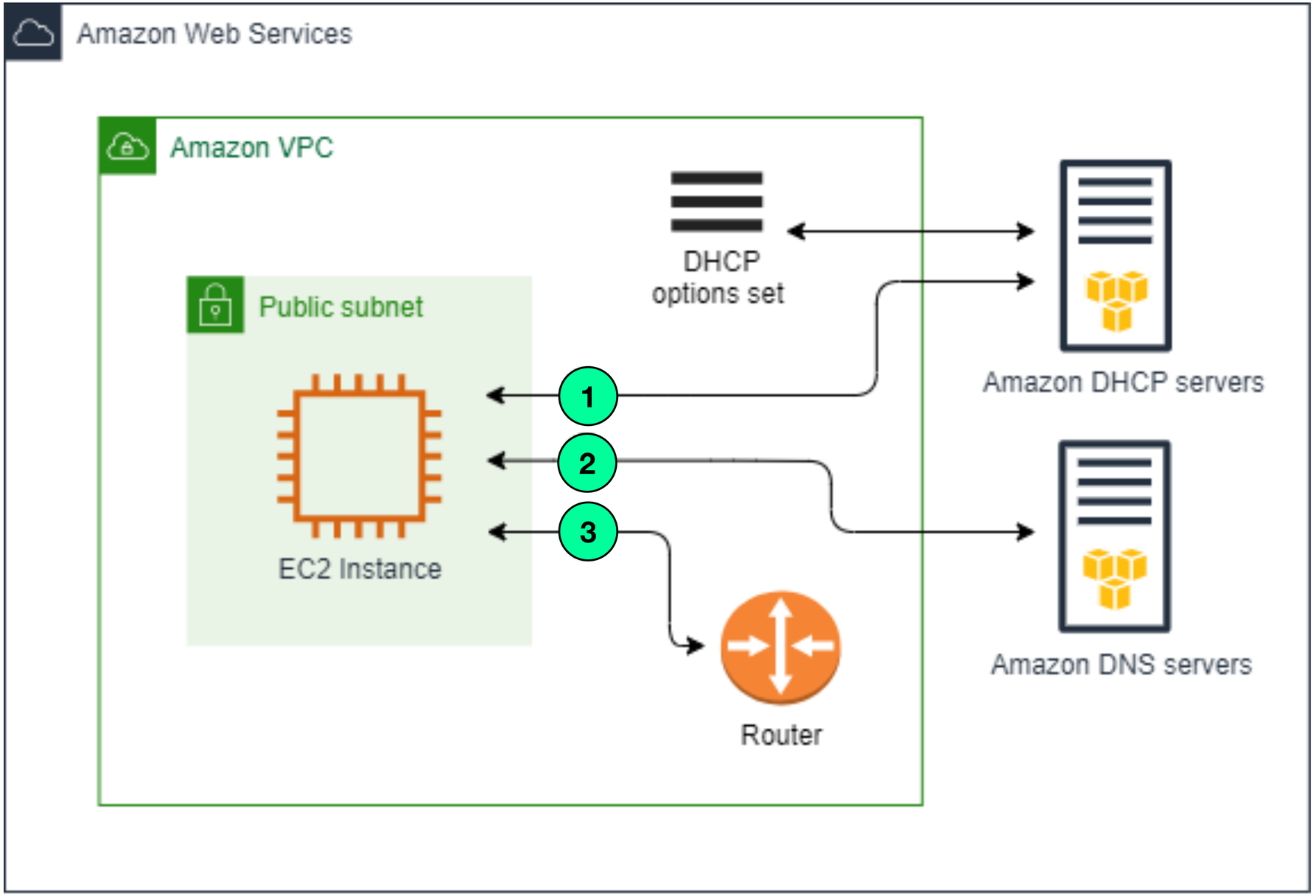
🌐 DHCP Option Sets in Amazon VPC

- 🔄 **Default and Custom DHCP Option Sets**: Amazon VPC uses a default DHCP option set for each region, enabling EC2 instances to communicate over the virtual network. Custom option sets can be created and associated with a VPC for specific network configurations.
- 🛠️ **Configuring DHCP Option Sets**: Customizing DHCP settings, such as DNS servers, domain names, and more, allows for enhanced network configuration within your VPC. Only one DHCP option set can be associated with a VPC at a time.
- 📡 **Impact on Internet Access**: Without an associated DHCP option set, instances in a VPC may not access the internet due to the lack of DNS server access. This highlights the importance of DHCP settings for network connectivity.

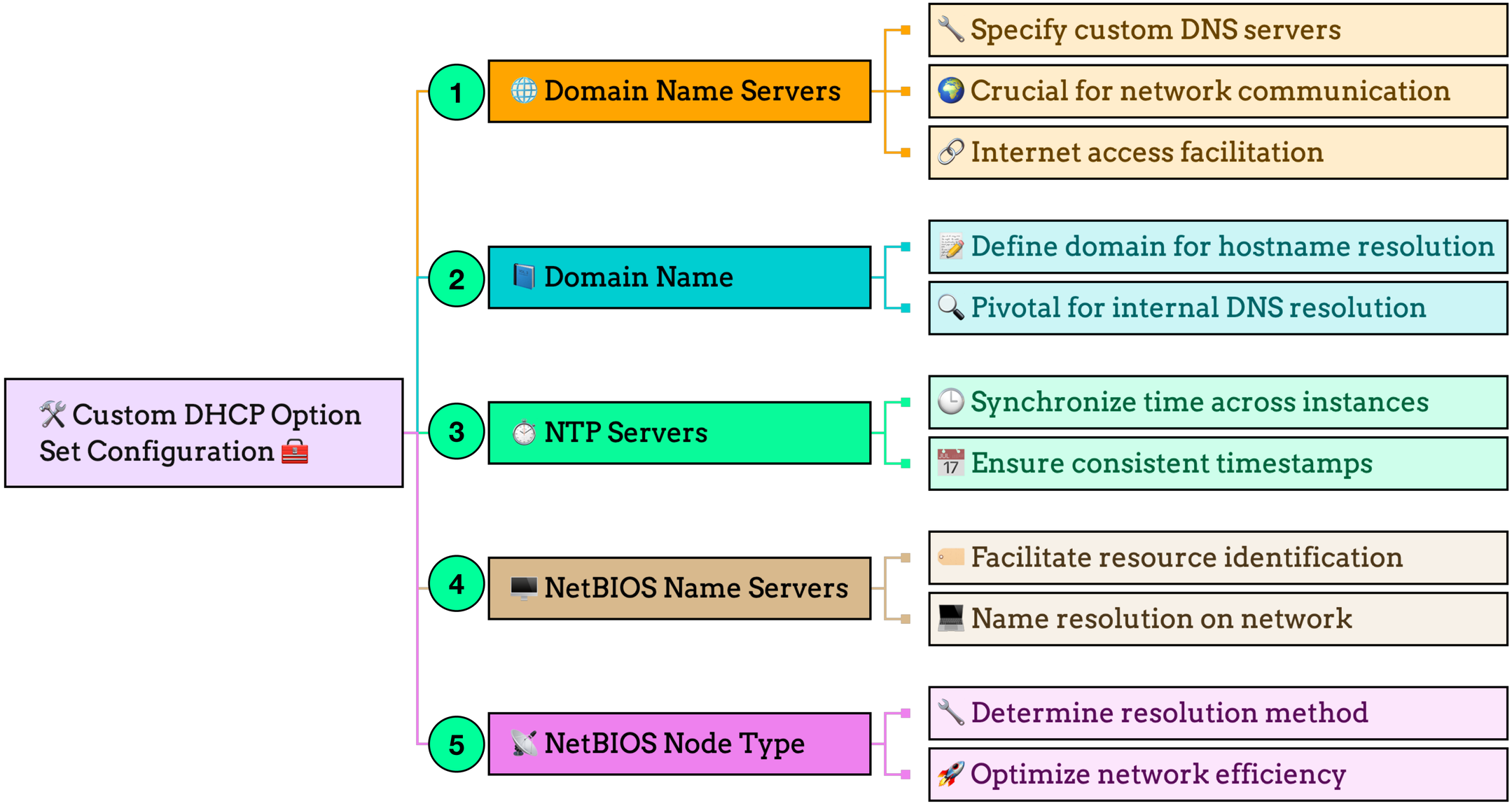
Default DHCP Option Set Settings.



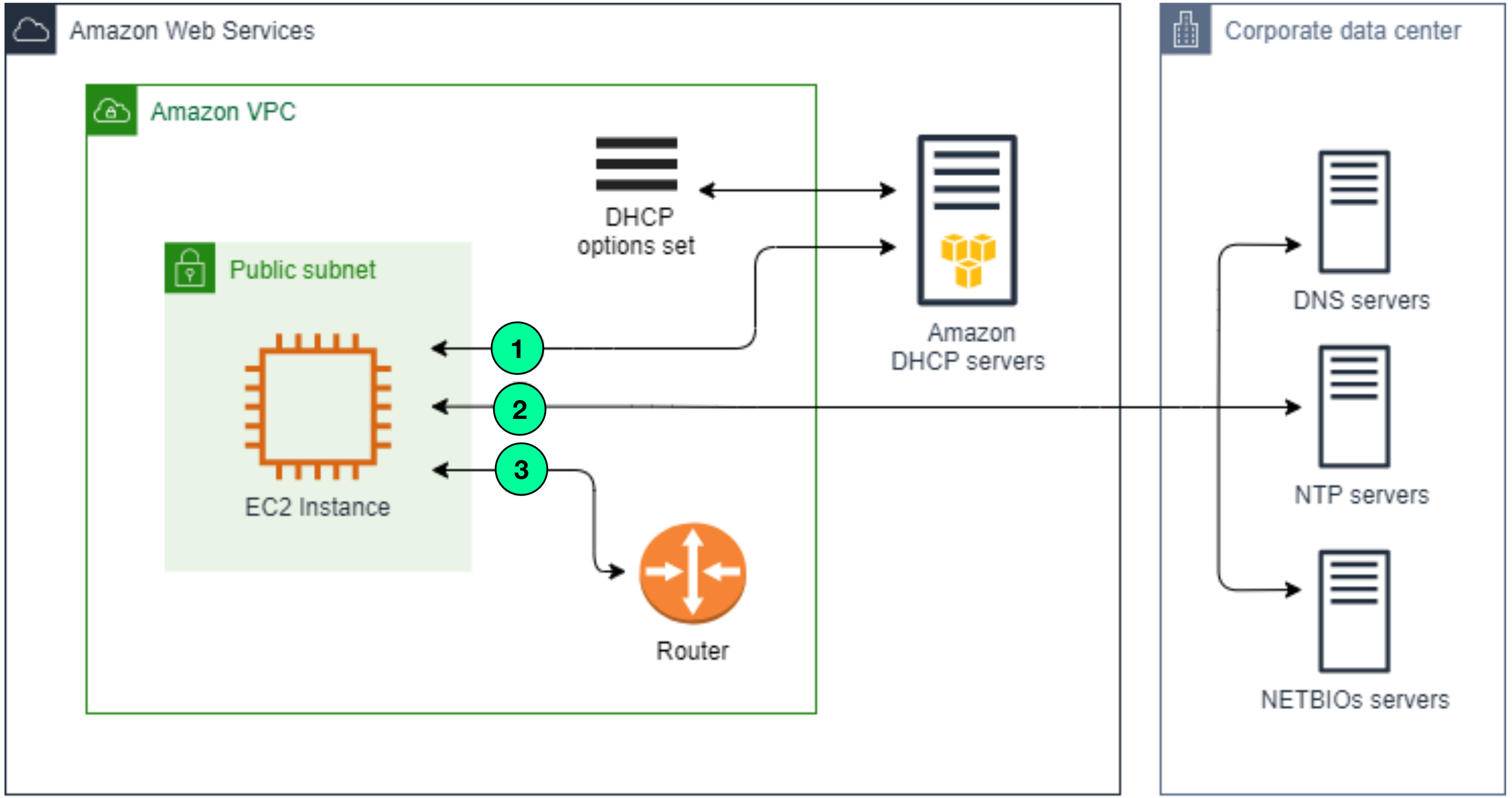
Default DHCP option set



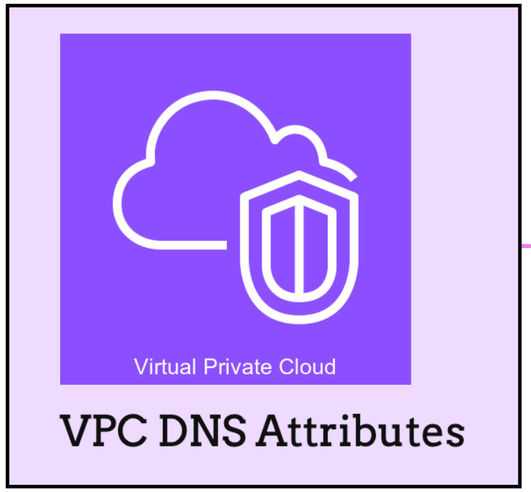
🛠️ Custom DHCP Option Set Configuration 🧰



Custom DHCP option set



VPC DNS Attributes.



1. 📡 Enable/Disable DNS Hostnames
   - 🔍 Determines public DNS hostname assignment
2. ☑️ Enable/Disable DNS Support
   - 🛠️ Controls Amazon-provided DNS server usage
3. 🔄 DNS Resolution and Domain Name
   - 🌍 Affects DNS hostnames to IP resolution
4. 🌍 Public and Private DNS Hostnames
   - 🔀 Resolves public and private IPs accordingly
5. 🚀 Custom Domain Names and Private Hosted Zones
   - 🛡️ Enables custom DNS names within VPC

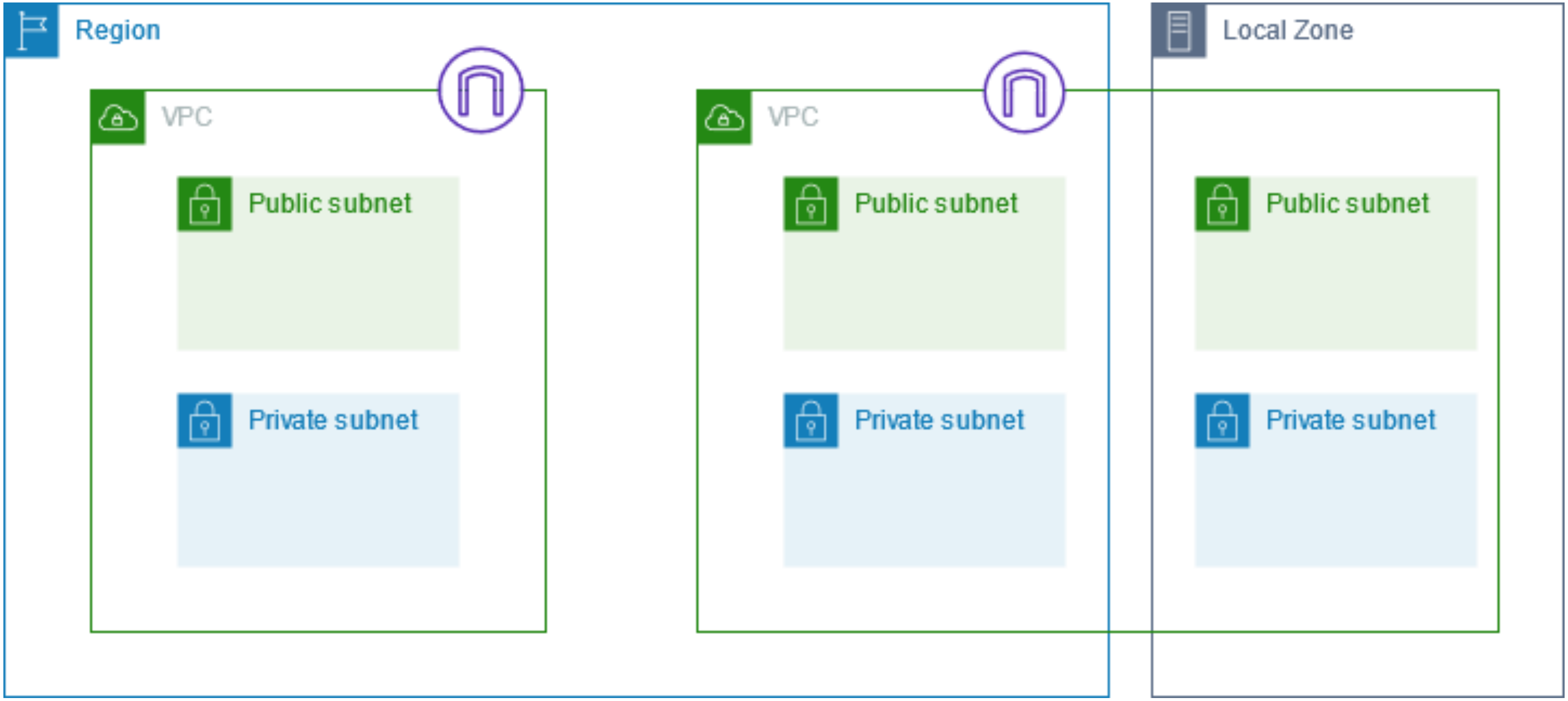
Subnet IP Address Range Configuration

- 🖥️ **IPv4 Only Subnets**: These subnets support only IPv4 CIDR blocks and all resources must communicate over IPv4.
- 🌐 **Dual Stack Subnets**: Subnets with both IPv4 and IPv6 CIDR blocks allow resources to communicate over both IP versions.
- 📶 **IPv6 Only Subnets**: These are configured with only an IPv6 CIDR block, requiring all resources to use IPv6 for communication.

🌐 Subnet Types in Amazon VPC

- 🔓 **Public Subnet**: Configured with a route to an internet gateway, allowing resources to access the internet directly.
- 🔒 **Private Subnet**: Does not have a direct route to the internet. Resources use a NAT device to access the internet.
- 🛡️ **VPN-only Subnet**: Has a route to a Site-to-Site VPN connection and no direct internet access.
- 🏝️ **Isolated Subnet**: No routes to the internet or VPN, restricting access to within the VPC only.

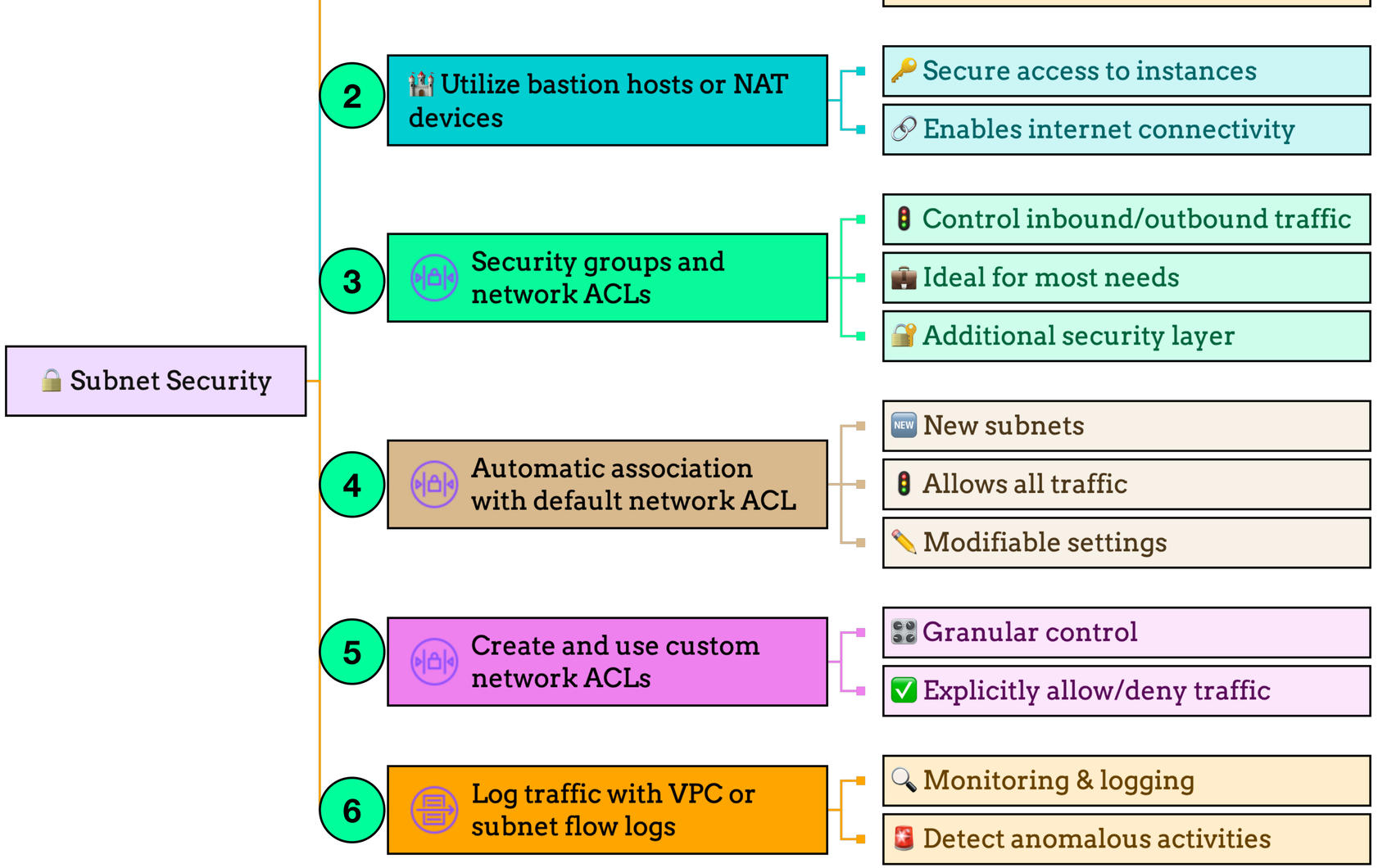
Subnet Diagram



Subnet Routing

- 🔄 **Each subnet must be associated with a route table**: This ensures that each subnet in your Amazon VPC has a defined path for outbound traffic, allowing for controlled network communication.
- 🌐 **Route tables define routes for outbound traffic**: Route tables contain rules to direct outbound traffic from the subnet to different destinations, such as the internet or other subnets.
- 📄 **Automatic association with the main route table**: Upon creation, subnets are automatically associated with the VPC's main route table, but this association can be changed to meet specific network requirements.
- ✏️ **Customizable associations and route table contents**: Users have the flexibility to modify which route table a subnet is associated with, as well as the rules contained within the route table, to tailor the network to their application's needs.

Subnet Security.



Route Table Concepts

- 🏠 **Main route table**: Automatically assigned to your VPC, controlling routing for all subnets not linked to another route table.
- ✏️ **Custom route table**: User-created route tables within a VPC for customized network traffic routing.
- 🎯 **Destination CIDR**: Specifies the IP address range where traffic is directed.
- 🌉 **Target gateway or interface**: Defines the gateway, network interface, or connection through which traffic is sent.
- 🔗 **Route table associations**: Links a route table with a subnet, internet gateway, or virtual private gateway.
- 🛤️ **Subnet and gateway route tables**: Designate route tables associated specifically with subnets or gateways for targeted routing.
- 📡 **Local and propagated routes**: Local routes allow VPC internal communication; propagated routes automate VPN connection routing.
- 🚦 **Edge and transit gateway route tables**: Utilized for routing inbound VPC traffic to an appliance and managing traffic through a transit gateway, respectively.

🔢 Routes in Amazon VPC

- 🎯 **Destination and Target Concept**: Each route in a table specifies a destination CIDR block and a target (e.g., internet gateway) for where the traffic should go.
- 🌍 **Internet Access via Internet Gateway**: To enable a subnet to access the internet, a route with a destination of 0.0.0.0/0 and the target as the internet gateway is added.
- 🔄 **IPv4 and IPv6 CIDR Blocks**: Routes for IPv4 and IPv6 are treated separately, requiring distinct routes for each type of traffic.
- 📋 **Customer-Managed Prefix Lists**: Groups of CIDR blocks can be managed together using prefix lists, simplifying route table entries.

🔢 Routes in Amazon VPC

- 🎯 **Destination and Target Concept**: Each route in a table specifies a destination CIDR block and a target (e.g., internet gateway) for where the traffic should go.
- 🌍 **Internet Access via Internet Gateway**: To enable a subnet to access the internet, a route with a destination of 0.0.0.0/0 and the target as the internet gateway is added.
- 🔄 **IPv4 and IPv6 CIDR Blocks**: Routes for IPv4 and IPv6 are treated separately, requiring distinct routes for each type of traffic.
- 📋 **Customer-Managed Prefix Lists**: Groups of CIDR blocks can be managed together using prefix lists, simplifying route table entries.
- 🔄 **Local Route for VPC Communication**: Every route table includes a local route for internal VPC traffic, automatically added to facilitate VPC communication.
- 📏 **Rules for Specific Routes**: More specific routes can be added to route tables, directing traffic to different targets like NAT gateways or network interfaces.
- 🚫 **Restrictions on Certain IPv4 and IPv6 Ranges**: Certain IP ranges are reserved and cannot be used for routes within VPCs, ensuring AWS services' accessibility.
- 🛣️ **Middlebox Appliances in Routing Paths**: Middlebox appliances can be incorporated into VPC routing for specialized network functions.

Main Route Table in Amazon VPC

- 🚀 **Automatic main route table creation**: Each VPC is equipped with a main route table upon creation. This table is used by default for any subnet without a specified route table.
- 📌 **Default local route inclusion**: Initially, the main route table contains only a local route. Adding a NAT gateway prompts automatic inclusion of relevant routes.
- ✏️ **Route modification capabilities**: Users have the freedom to add, remove, and modify routes within the main route table to tailor traffic flow.
- 🚫 **Restrictions on deletion and type change**: The main route table cannot be deleted or set as a gateway route table, ensuring stable network operation.
- 🔄 **Replacement and explicit association**: Associating a custom route table with a subnet allows for main route table replacement. Explicitly associating a subnet with the main route table is advisable after such changes to maintain traffic flow as intended.

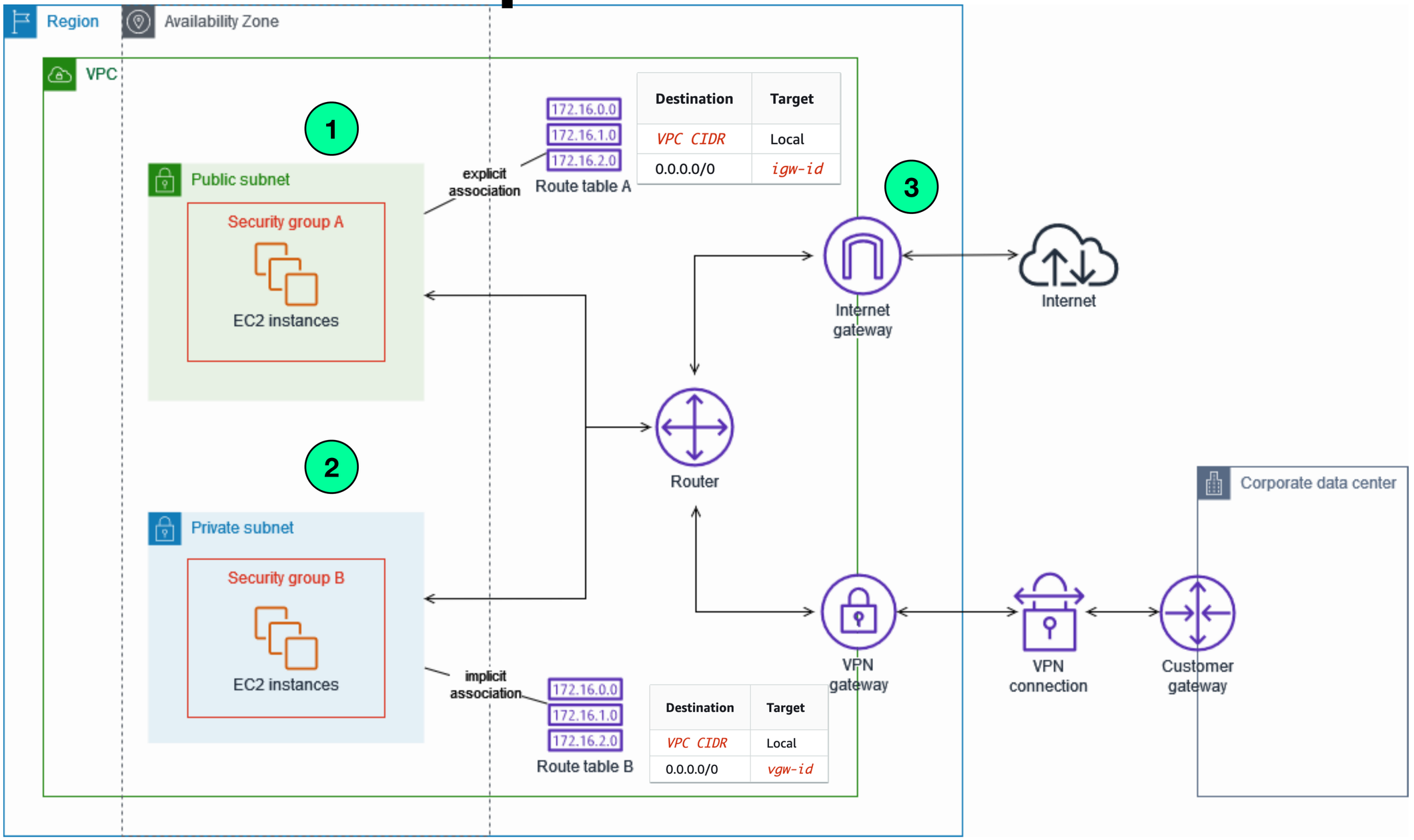
🛣️ Custom Route Tables in Amazon VPC

- 🚦 **Local route for VPC communication**: Every route table starts with a local route allowing communication within the VPC itself.
- 🌐 **Internet gateway route for public subnets**: Creating a VPC with a public subnet triggers the addition of an internet gateway route to the custom route table.
- 🛡️ **Protecting your VPC**: Keeping the main route table in its default state and explicitly associating new subnets with custom route tables can enhance your VPC's security.
- ✏️ **Modifying custom route tables**: Custom route tables offer the flexibility to add, remove, and modify routes as needed.
- 🗑️ **Deleting custom route tables**: A custom route table can be deleted only if it has no remaining associations.

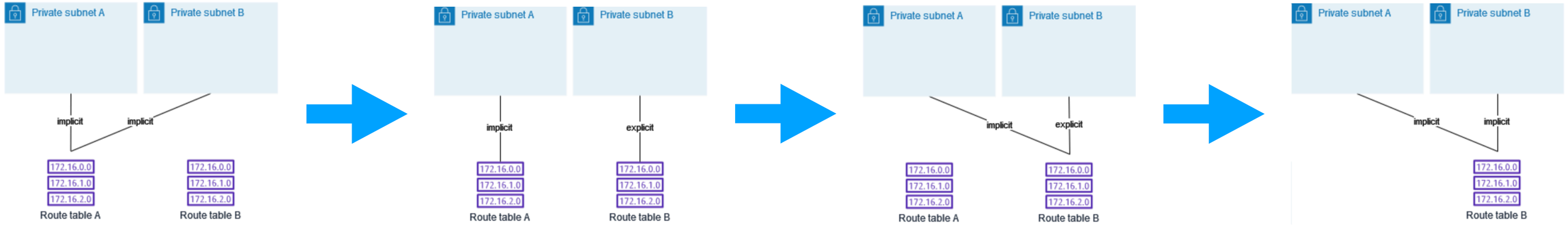
🔗 Subnet Route Table Association

- 🔄 **Each subnet must be associated with a route table**: Every subnet within a VPC must be linked to a route table, either the main route table by default or a custom route table through explicit association.
- 🛠️ **Custom vs. Main Route Table**: The main route table is the default routing table for all subnets not associated with another table. Custom route tables are created for specific routing needs within the VPC.
- 🎯 **Explicit and Implicit Associations**: Subnets can be explicitly associated with custom route tables or implicitly fall back on the main route table. This distinction allows for more granular traffic routing control within the VPC.
- 🌍 **Outposts VPCs Special Routing**: For VPCs associated with AWS Outposts, subnets can target a local gateway for routing, a unique feature compared to standard AWS VPCs.
- 🔄 **Replacing the Main Route Table**: To change the VPC's default routing without affecting existing traffic flows, a custom route table can be tested and then set as the new main route table, ensuring all new and unassociated subnets use this routing by default.

Implicit and explicit subnet association



Replacing the main route table



1. Initial State
2. Association Change
3. Main Route Table Replacement
4. Final State (Optional)

Gateway Route Tables.

Gateway Route Tables

1. Association with Gateways
   - Internet or Virtual Private Gateway
   - Manages traffic flow
2. Fine-grain Traffic Control
   - Detailed routing control
   - Precise traffic management
3. Intercepting Traffic via Middlebox
   - Directs to security device
   - Enhances monitoring, security

Gateway Route Table Routes.

- 🛣️ Gateway Route Table Routes
  - 1 🎯 Supports Various Targets
    - 🌍 Internet Gateway
    - 🏠 Virtual Private Gateway
    - 🔒 Default Local Route
    - 🔄 Gateway Load Balancer Endpoint
    - 🛡️ Network Interface for Middlebox
  - 2 🗺️ Specific Routing Destinations
    - 🌐 IPv4/IPv6 CIDR Block VPC
    - 🧩 Subnet within VPC
  - 3 🔄 Flexibility in Route Targeting
    - 🔧 Changeable Local Route Target
    - 🔙 Restorable to Default Target
  - 4 🚫 Rules and Considerations
    - 🚧 Restrictions on Association
    - 🚦 Types of Routes and Targets
    - 💡 Middlebox Traffic Reachability
    - 🔗 Running Instance Requirement

Routing Examples

Destination	Target
0.0.0.0/0	*igw-id*
::/0	*igw-id*

Routing to an internet gateway: You can make a subnet a public subnet by adding a route in your subnet route table to an internet gateway. To do this, create and attach an internet gateway to your VPC, and then add a route with a destination of 0.0.0.0/0 for IPv4 traffic or ::/0 for IPv6 traffic, and a target of the internet gateway ID.

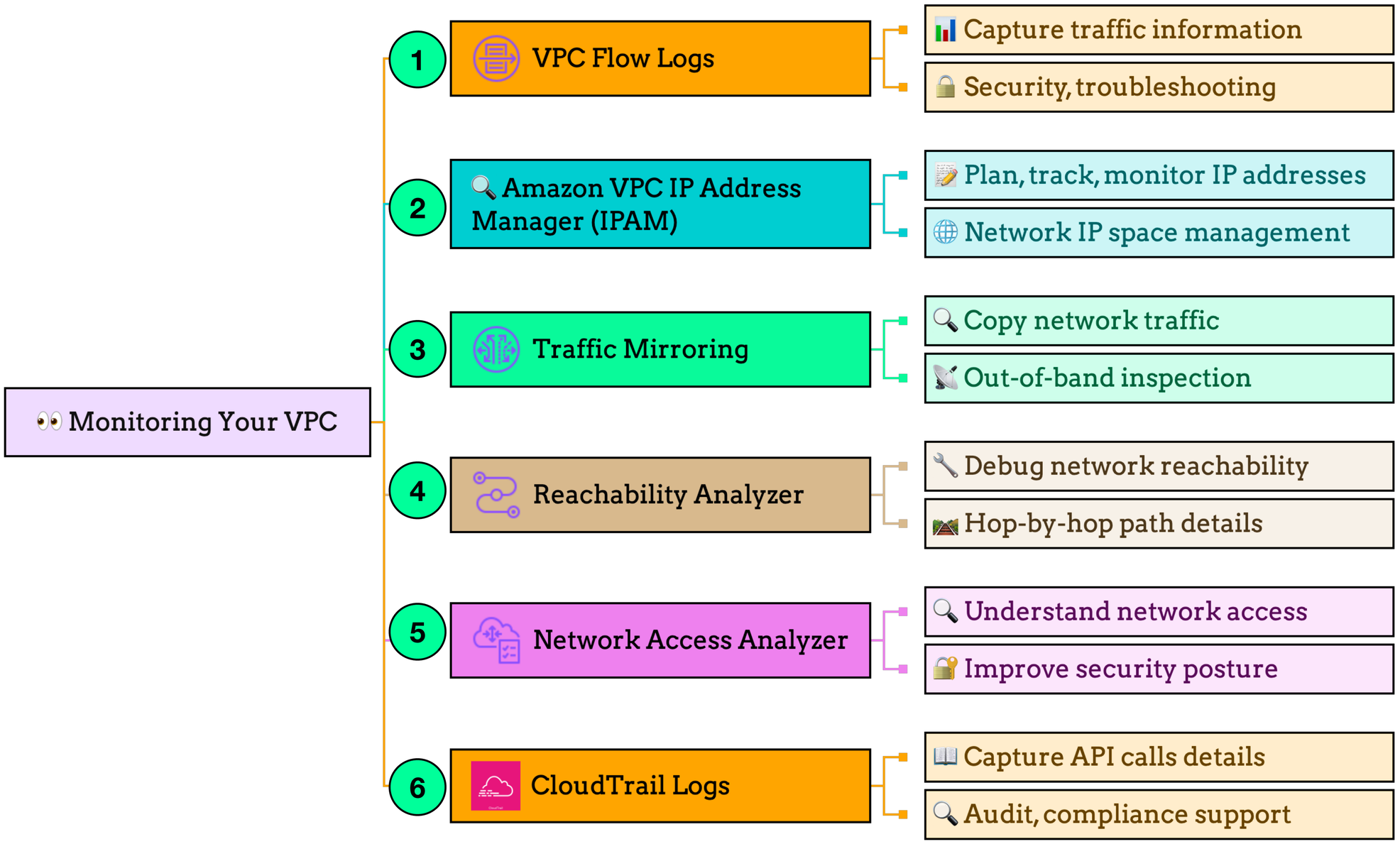
Destination	Target
0.0.0.0/0	*nat-gateway-id*

Routing to a NAT device: To enable instances in a private subnet to connect to the internet, you can create a NAT gateway or launch a NAT instance in a public subnet. Then add a route for the private subnet's route table that routes IPv4 internet traffic (0.0.0.0/0) to the NAT device.

Destination	Target
10.0.0.0/16	*vgw-id*

Routing to a virtual private gateway: You can use an AWS Site-to-Site VPN connection to enable instances in your VPC to communicate with your own network. To do this, create and attach a virtual private gateway to your VPC. Then add a route in your subnet route table with the destination of your network and a target of the virtual private gateway.

👀 Monitoring Your VPC.



Security in Amazon Virtual Private Cloud.

Security in Amazon Virtual Private Cloud

1. Data Protection in Amazon VPC
2. Identity and Access Management for Amazon VPC
3. Infrastructure Security in Amazon VPC
4. Control Traffic to Your AWS Resources Using Security Groups
5. Control Traffic to Subnets Using Network ACLs

🔒 Data Protection in Amazon VPC

- 🌐 **Internetwork Traffic Privacy**: Amazon VPC ensures that all data in transit within the AWS global network is automatically encrypted, providing robust privacy safeguards.
- 🔑 **Encryption Options**: Users can leverage AWS services such as Amazon VPC VPN, AWS Direct Connect, along with customer-managed keys for enhanced data protection.
- 🛡️ **AWS Key Management Service Integration**: Integration with AWS KMS allows for secure management of encryption keys used within VPC, ensuring that data at rest is also protected.

🔐 Identity and Access Management for Amazon VPC

- 🆔 **IAM Roles and Policies**: Utilize IAM to assign roles and policies that precisely define who can manage or access VPC resources, enhancing security.
- 🎛️ **Fine-grained Access Controls**: IAM policies allow for detailed access management, ensuring only authorized operations can be performed on VPC resources.
- 📊 **VPC Resource Monitoring**: Leverage IAM to monitor and log access to VPC resources, providing visibility into usage patterns and potential security breaches.

🚧 Infrastructure Security in Amazon VPC

- 🛑 **Network Isolation and Segmentation**: VPCs provide a segregated environment for your AWS resources, allowing for secure network architecture designs.
- 🚦 **Traffic Filtering and Inspection**: Utilize network ACLs and security groups to filter incoming and outgoing VPC traffic, enhancing security posture.
- 🚨 **Intrusion Detection and Prevention**: Implement AWS services like AWS Shield and AWS WAF for real-time traffic analysis and threat mitigation.

🔐 Control Traffic to Your AWS Resources Using Security Groups

- 🛡️ **Virtual Firewall for Resources**: Security groups act as a virtual firewall for your EC2 instances and other AWS resources, controlling both inbound and outbound traffic.
- 📐 **Customizable Inbound and Outbound Rules**: You can create security groups with specific rules that define the allowed source port range and protocol for inbound traffic, and the destination port range and protocol for outbound traffic.
- 🚦 **Traffic Control for Instances**: For instance, associating a security group with an EC2 instance allows you to manage the traffic that reaches and leaves the instance. Rules can be set to allow specific types of traffic, enhancing security and control.
- 💸 **No Additional Charge**: Utilizing security groups for traffic control and security does not incur any additional costs, making it a cost-effective solution for securing your AWS resources.

🔒 Control Traffic to Subnets Using Network ACLs

- 🚧 **Allows or Denies Traffic at the Subnet Level**: Network ACLs (Access Control Lists) provide a layer of security that allows or denies inbound or outbound traffic specific to subnets within your VPC (Virtual Private Cloud), offering granular control over the network traffic.
- 🛠️ **Customizable for Enhanced Security**: You have the flexibility to use the default network ACL that comes with your VPC or create custom network ACLs. These custom ACLs can have rules similar to those in your security groups, allowing for an additional layer of security tailored to your VPC's needs.
- 💸 **No Additional Charge**: Utilizing network ACLs to manage and control traffic to and from your subnets does not incur any additional costs, ensuring you can secure your network traffic economically.

Thanks for Watching