**Content**

[1. Udemy 2](#_Toc80203805)

[1. VPC Endpoints 2](#_Toc80203806)

[1.1.1. Gateway 2](#_Toc80203807)

[1.1.2. Interface 2](#_Toc80203808)

[1.1.3. Service VPC Endpoints 2](#_Toc80203809)

[1.1.4. Gateway Load Balancer 3](#_Toc80203810)

[2. Load Balancers deep dive 4](#_Toc80203811)

[3. DNS – Route53 5](#_Toc80203812)

[4. Hybrid networking 12](#_Toc80203813)

[1. VPN 12](#_Toc80203814)

[4.1.1. Virtual Private Gateway 12](#_Toc80203815)

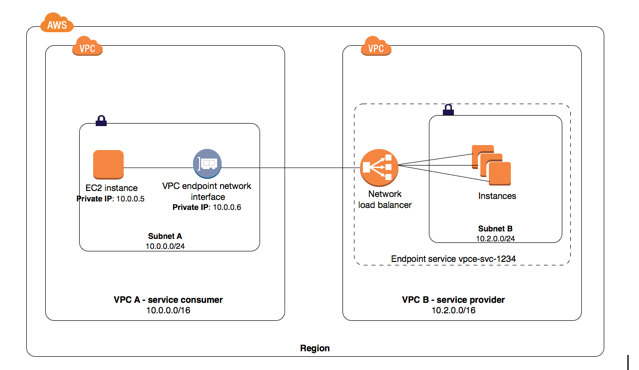
[2. Direct Connect 12](#_Toc80203816)

[5. Linuxacademy 13](#_Toc80203817)

[6. Networking tools 14](#_Toc80203818)

1. Udemy
   1. VPC Endpoints
      1. Gateway

* In gateway apporach the vpc endpoint was created outside of the VPC. Thus it is not possible to use via VPN or Direct Connect solutions
* When associated with a route table, the route table automatically updates the prefixc list ofservice and taget endpoints
* IAM or resource policies to be used to restrict access
* Highly available by default
  + 1. Interface
* An interface endpoint is an elastic network interface with a private IP address form the IP range of your subnet.
* Sits inside a subnet and needs to be in an AZ (for HA put one in each AZ)
* Has its own dns names,
* Could be used with Route 53 Resolver to return private IP addresses
* Interface endpoints enable to use of security groups to restrict access
* VPC and Direct connect are supported
* 1 vpc endpoint / vpc / subnet / az
  + 1. Service VPC Endpoints



* + 1. Gateway Load Balancer

Gateway Load Balancers enable you to deploy, scale, and manage virtual appliances, such as firewalls, intrusion detection and prevention systems, and deep packet inspection systems. It combines a transparent network gateway (that is, a single entry and exit point for all traffic) and distributes traffic while scaling your virtual appliances with the demand.

1. Load Balancers deep dive

<https://aws.amazon.com/elasticloadbalancing/features/>

1. DNS – Route53

**Authoritatiuve name servers** provide answers to queries they know about – Route53

**Non-Authoritative name servers** points to other servers or serves cachced content from other name servers‘ data

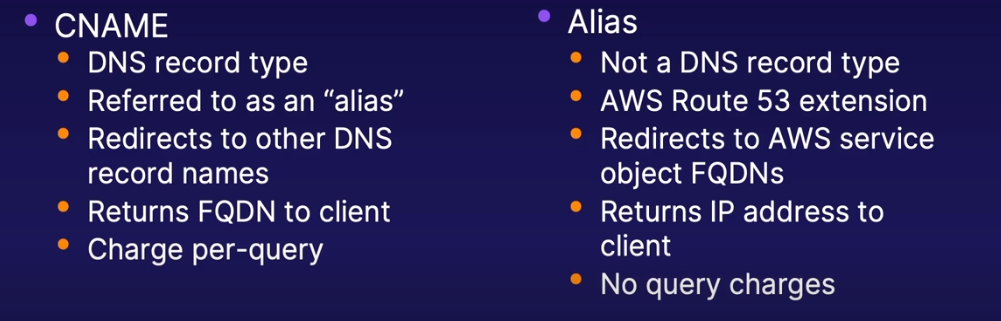
**Zones** - a zone is a container that holds important infromation about how to route traffic for domain names (example.com) and its subdomains (test.exmaple.com)

**DNS resolution** - Each web server has a unique IP address in textual form, translating it to an IP address is a process known as DNS resolution or DNS lookup. During DNS resolution, the program that wishes to perform this translation contacts a DNS server that returns the translated IP address. In practice the entire translation may not occur at a single DNS server; rather, the DNS server contacted initially may recursively call upon other DNS servers to complete the translation.

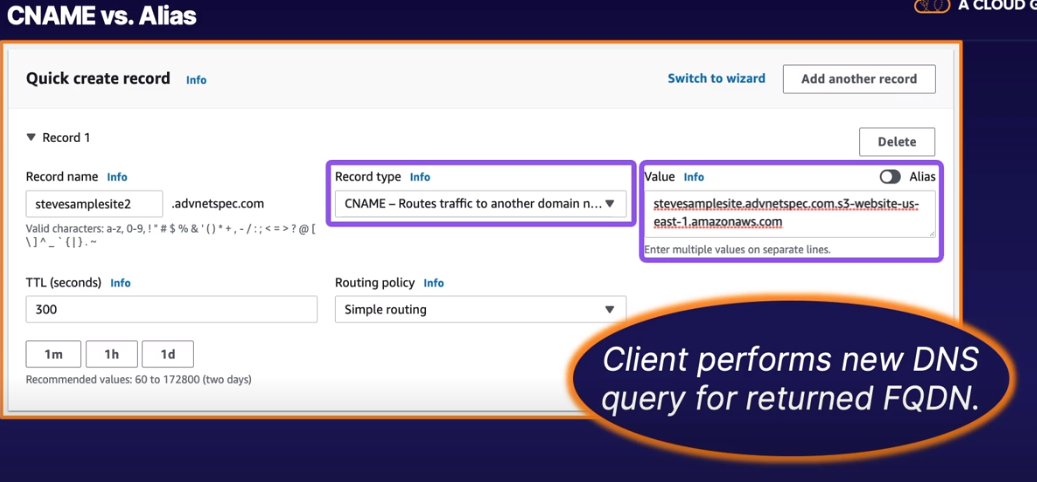
**DNS records** (aka **zone files**) are instructions that live in authoritative DNS servers and provide information about a domain including what IP address is associated with that domain and how to handle requests for that domain. These records consist of a series of text files written in what is known as DNS syntax.

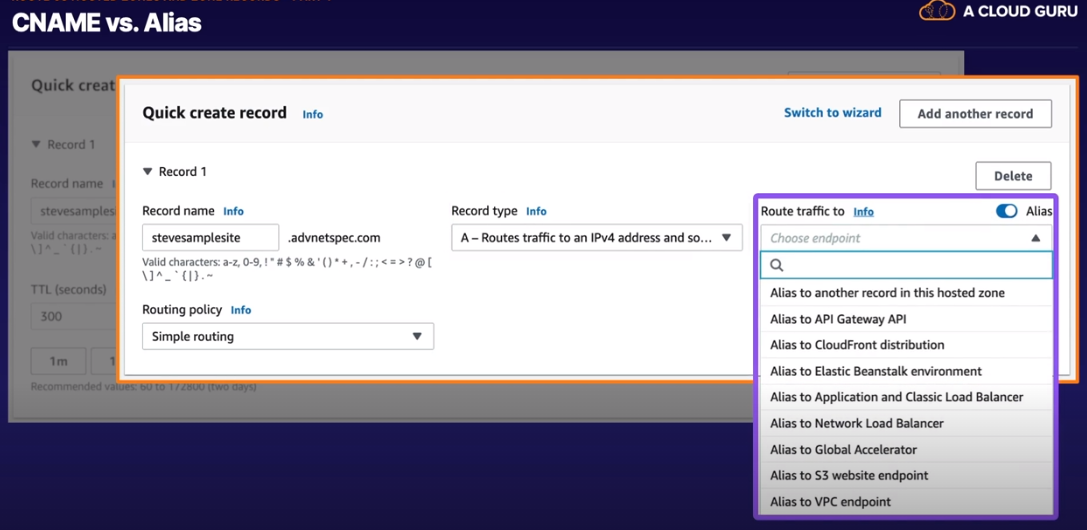
|  |  |
| --- | --- |
| A | Returns a 32-bit IPv4 address |
| AAAA | Returns a 128-bit IPv6 address |
| CAA | DNS Certification Authority Authorization, constraining acceptable CAs for a host/domain |
| CNAME | Alias of one name to another: the DNS lookup will continue by retrying the lookup with the new name. |
| NS | Name Server records direct traffic to the DNS serves taht contain the authoritative DNS records. They are identifying the DNS servers, that hold authoritative copies of your zone information. |
| MX | Maix Exchange records are used to define mail servers |
| TXT | Hold text information (unformatted) |
| PTR | Pointer records is a reverse A record lookup. Maps an IP address to a host |
| SOA | Specifies authoritative information about a DNS zone, including the primary name server, the email of the domain administrator, the domain serial number, and several timers relating to refreshing the zone. |

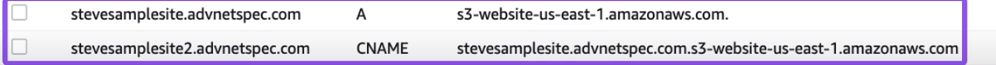
CNAME and Alias records both resolve DNS queries using other records. CNAME are DNS standards record type. An Alias in Route53 is an extention of functionality, not a DNS record type.







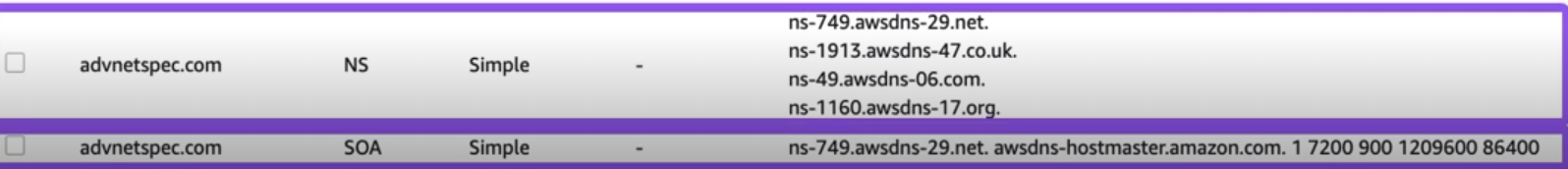


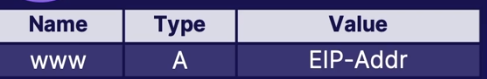
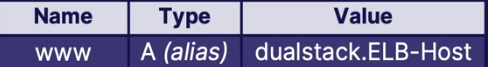


A hosted zone is an Amazon Route 53 concept. A hosted zone is analogous to a traditional DNS zone file; it represents a collection of records that can be managed together, belonging to a single parent domain name. All resource record sets within a hosted zone must have the hosted zone's domain name as a suffix.

* private (Must be associated with 1 or more VPC, which must have DNS support enabled. no need to register via ICANN)
* public hosted zones (public domain name registration, delegation of domain authority – change the name servers in case of external registration, like godaddy. Then you need to create a record)

2 records automatically pop up in case of zone creation:



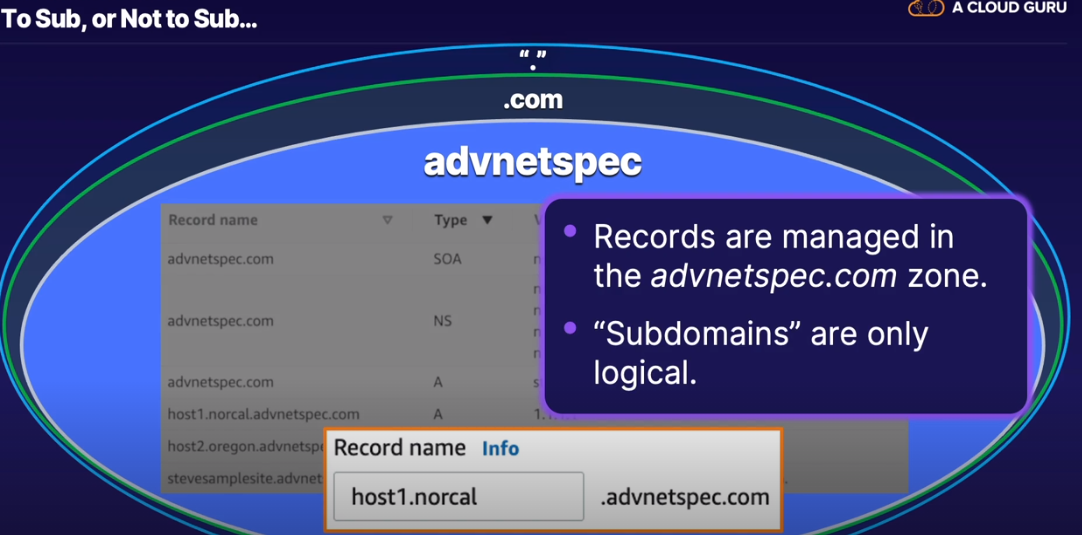
* not too good, because EC2 instances do not retain public IP addresses after stoppage
* 
* Elastic IP is a bit better
* 
* Queries against CNAME records incur charges
* Client is not given an IP address
* 
* Queries against alias records incur no charges
* Route53 returns IP address to client
* 

The apex (sometimes known as the zone apex or domain apex) refers to records where the record name is the same as the zone's domain name. In the zone for example.com, a record for example.com is said to be at the zone apex



CNAME are not good for resolving the zone apex.

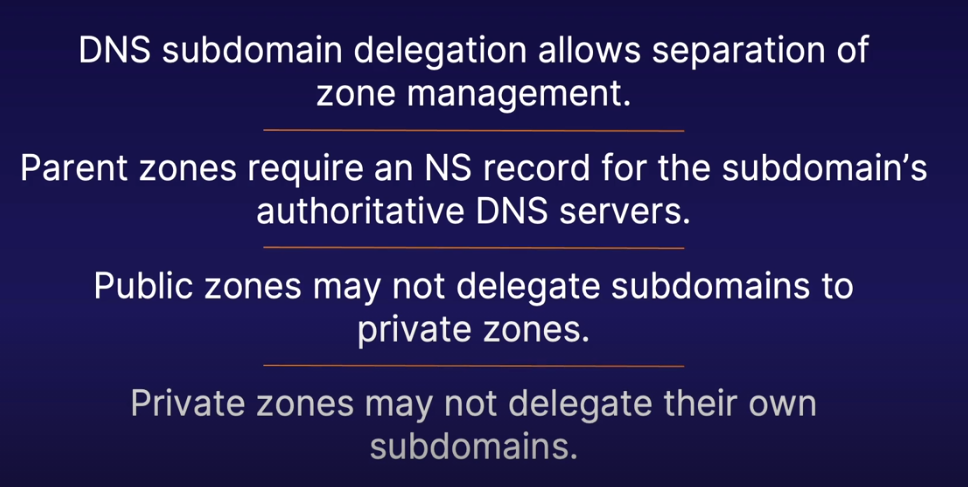
**Subdomain delegation** allows separation of zone and record management. NS records for subdomain DNS servers must be addod to parent zone.



How to create a delegated subdomain:

1. create public hosted zone
2. copy the name servers
3. create ns record in parent zone
4. add the name serevers copied from the subdomain \*all dns queries for anyting within the parent domain namespace will be sent to the name servers authoritative for the parents hosted zone. So unless the parent zone knows where to forward the request for the subdomain nothings gonna work.

Private hosted zones are not publily accessible, so cannot be a dlegated subdomain of a public zone. Private hosted zones cannot delegate their own subdomains.

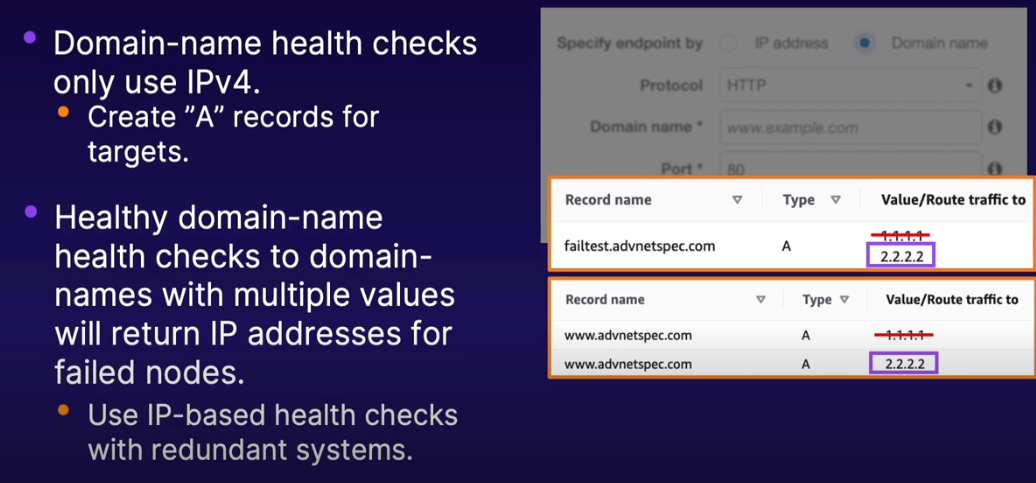


Routing policies

|  |  |
| --- | --- |
| Simple | Plain and simple routing. Default. Single logical resouce (e.g. LB). You can have multi values and round robin (equal distribution). |
| Weighted | Percentage routing (AB testing) If set to 0 it will ot be in the pool of active records. Health check possible. |
| Latency-based | Fastest connection. Latency analysis in the background. If you have multiple web apps in AU, USA and EU this routing will decide where to route Africa. |
| Failover | One ro the other routing. If first env fails, the trafiic goes to 2nd. If both A and B are unhealthy, A will get 100% of the traffic. Active backup and DR. |
| Geolocation | Location based routing (Europe goes for eu customers – local currency, local language whatever). Starts with the most specific (state, country). To lock user to a specific region, consider not setting a default location. It will return error. The IP address is from the DNS resolver. Geolocation rounting is not always accurate. To imporve the accuracy use the edns-client-subnet extension.   * default * contintent * countries * states |
| Multi-value Response Routing Policy | Responds with multiple hosts. It returns multiple IP addresses (up to 8 healthy responses). This can imporve the availability and load balancing ability. |

**Health Checks**

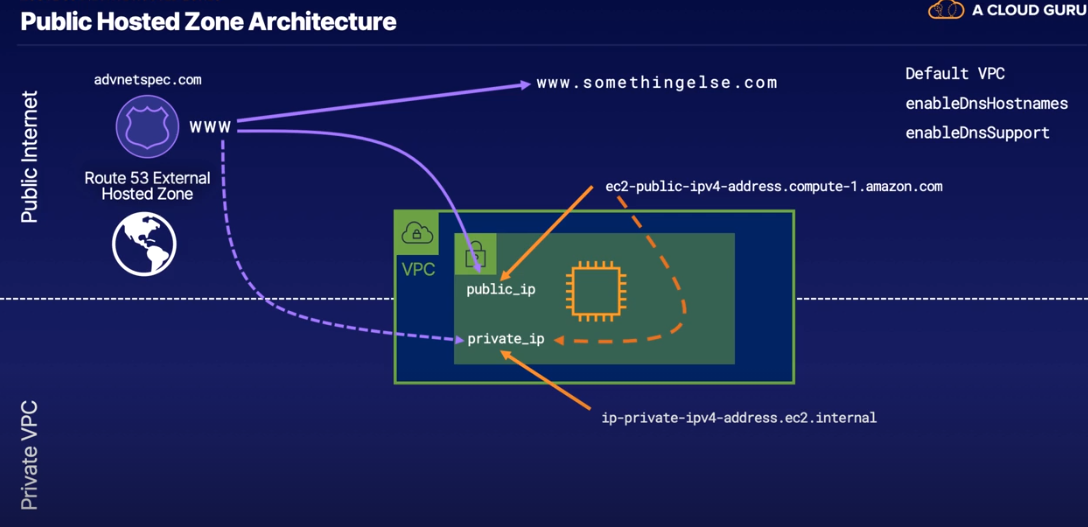
* endpoint healthchecks – tests endpoints reponsiveness. (ip/domain, protocol, port, path). Failover needs alternatives, health check is not enough. Health ckecks for alias records are unnecessary. They are intrinsically redundant infrastructure. Domain name health checker is looging for A record target (ipv4).
  + HTTP
  + HTTPS
  + TCP
* Other health checks – tests other health checks
* Cloudwatch alarms – health if alarm status OK.



18% the magic line, under which health becomes unhealthy.

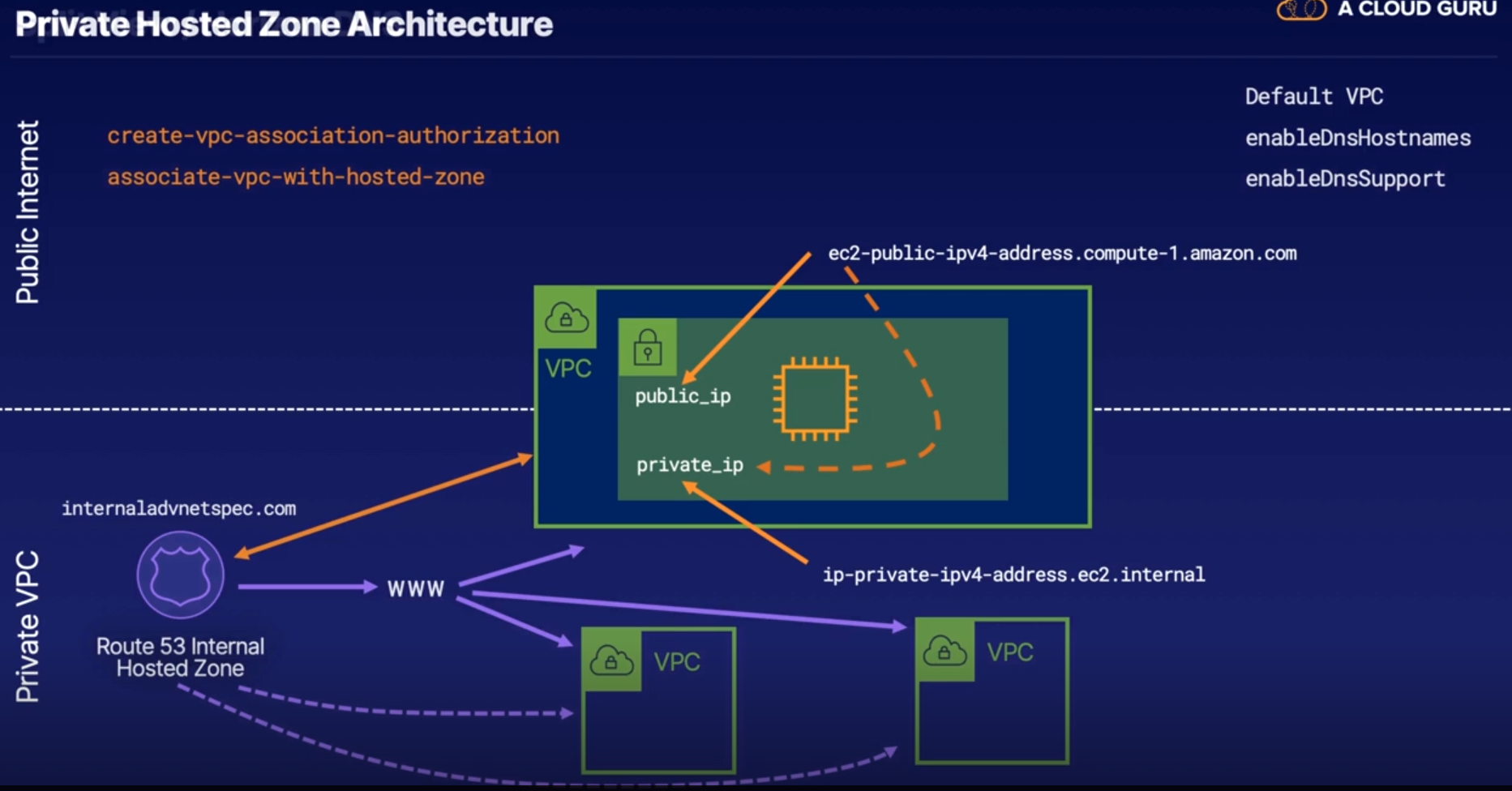
Latency based routing is checking the latency against the regional endpoints, not ur server. So the traffic will be routed even to unhealthy, unless you do not set up a health check.

**Private Hosted Zones**

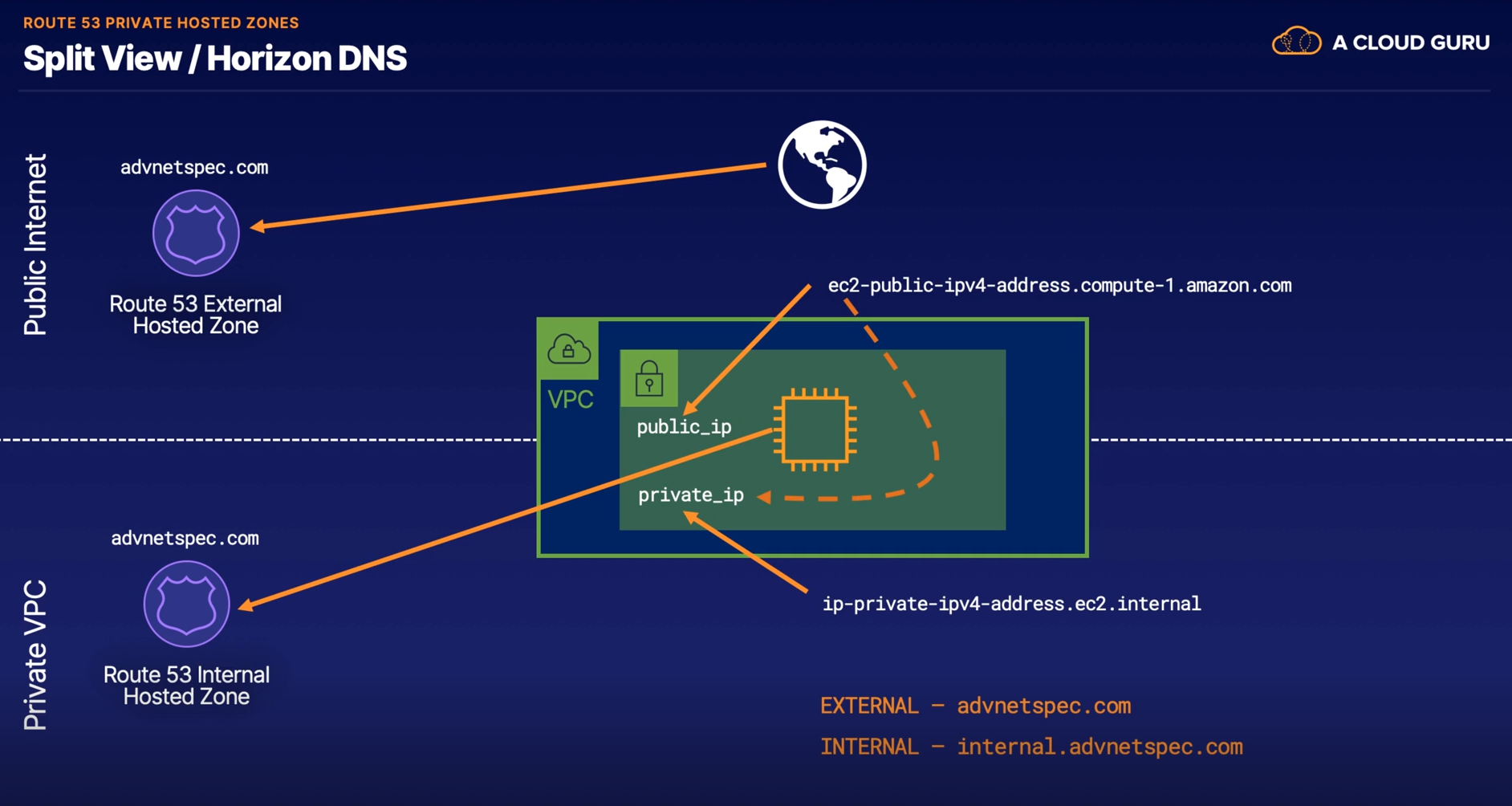


If traffic comes from the public, the public or a peered VPC, DNS is resolved to a public ip. If traffic comes from private VPC, it gets resolved to a private IP address.

We can point our record in the public hosted zone to a private IP address, resolution would happen but it would not be routable outside of the private network.



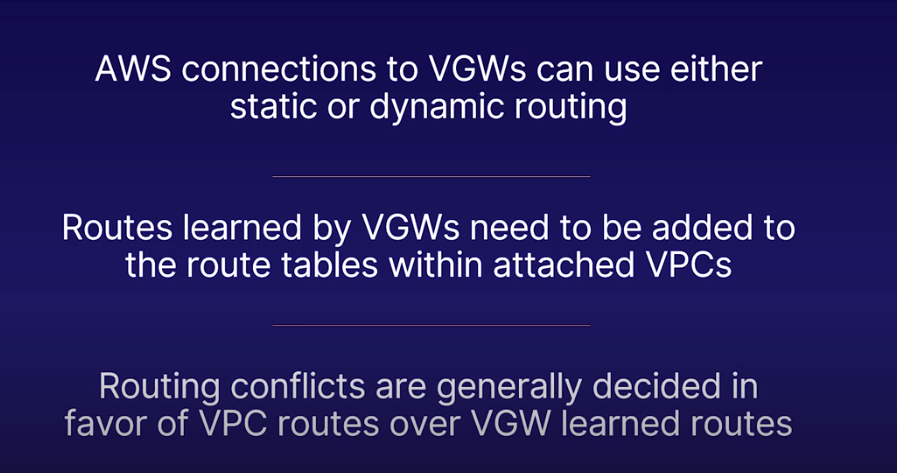
**Split View / Horizon DNS** – with fully overlapping namespaces – not required, but can be possible. The only records that will be returned to people on the internet are out of the public hosted zone. Internal can see both private and public.



1. Hybrid networking
   1. VPN
      1. Virtual Private Gateway

* Managed by AWS, acts as a router between ytour VPC and non-AWS-managed netwroks. Whether its a server, a virtualized server onprem or something in Azure VGW does not care.
* Can be associated with multiple external connections
* Can attach to only one VPC at a time, but can connect to multiple AWS VPN or Direct Connect connections
* ASN number is needed, 16bit private range: 64512-65534. Public ASNs are controlled by IANA. Only private ASNs may be used for VGW configuration.

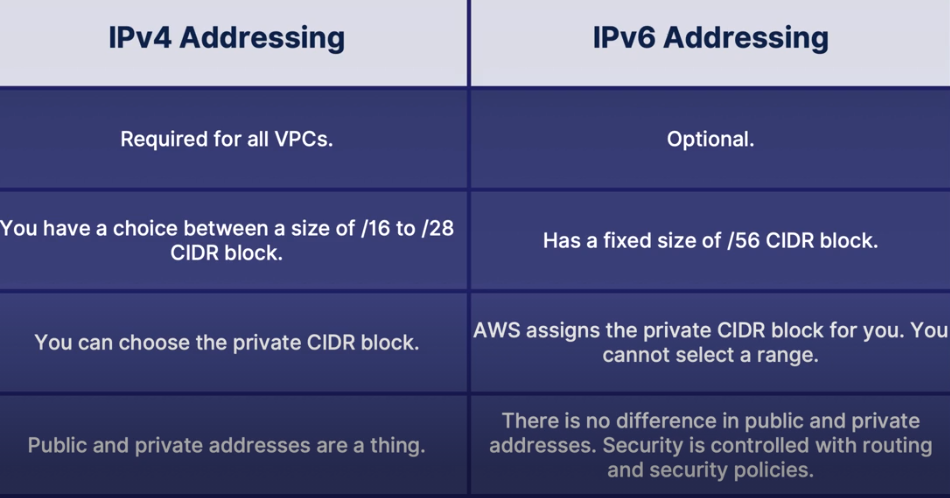
1. The most specific route wins
2. Static route over matching propagated
3. Direct connect > static vpn > bgp vpn



**BGP** network routes (prefixes) are shared between mutually-configured peers (admin on aws side, admin on our side). No automatic propagation of all routes, all prefixes must be manually shared. Best path selection algorithm. TCP 179.

1. Highest weight (cisco spec, not passed on)
2. Highest Local Preference (passed further, use this to change the priorieties according to link quality)
3. Shortest AS Path
4. eBGP over iBGP (! exteriors are preferred)
5. Lowest Metric
   1. Direct Connect
6. Linuxacademy

VPC tenacy: IF enalbed the ec2 instance will be run in a dedicated mode, what is more costly, but no ther aws accounts have access to the hardware you are using.



You will have IPv4 addresses aassigned to every resurce i your VPC. Even if you use Ipv6 ur still limited by Ipv4 address count.

Subnets can be VPN only

1. Networking tools

* tcpdump
* Ping

A very widely used command line utility that tests remote host availability and reports on roundtrip time, packet loss, and jitter.

* Ifconfig

A command line system query that returns the current host’s IP addressing statuses.

* NetStat

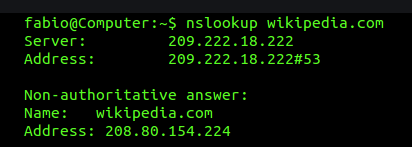
Displays both incoming and outgoing connections active on the current system.

* Dig

A utility that enables you to test your current DNS server.

* NSLookup

A DNS lookup and reverse lookup mechanism.



* Route

View or alter entries in the local routing table.

* Host

A DNS name lookup and reverse lookup tool.

* ARP

Address Resolution Protocol implementation checker. Reads the mapping between IP addresses and MAC addresses.

* EthTool

A command line tool that enables the Ethernet adapter settings to be viewed or edited.

* IWConfig

View a wireless adapter configuration and edit it.

* Hostname

View and change the host name of the current system.