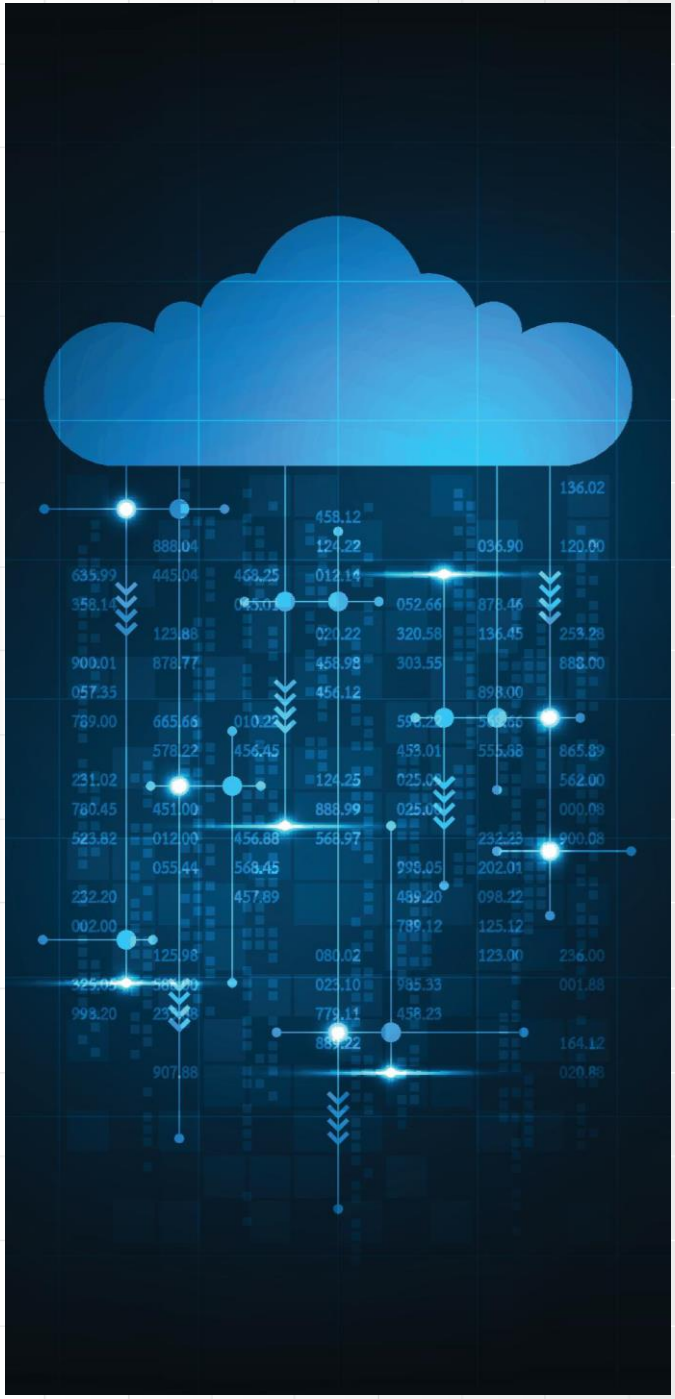
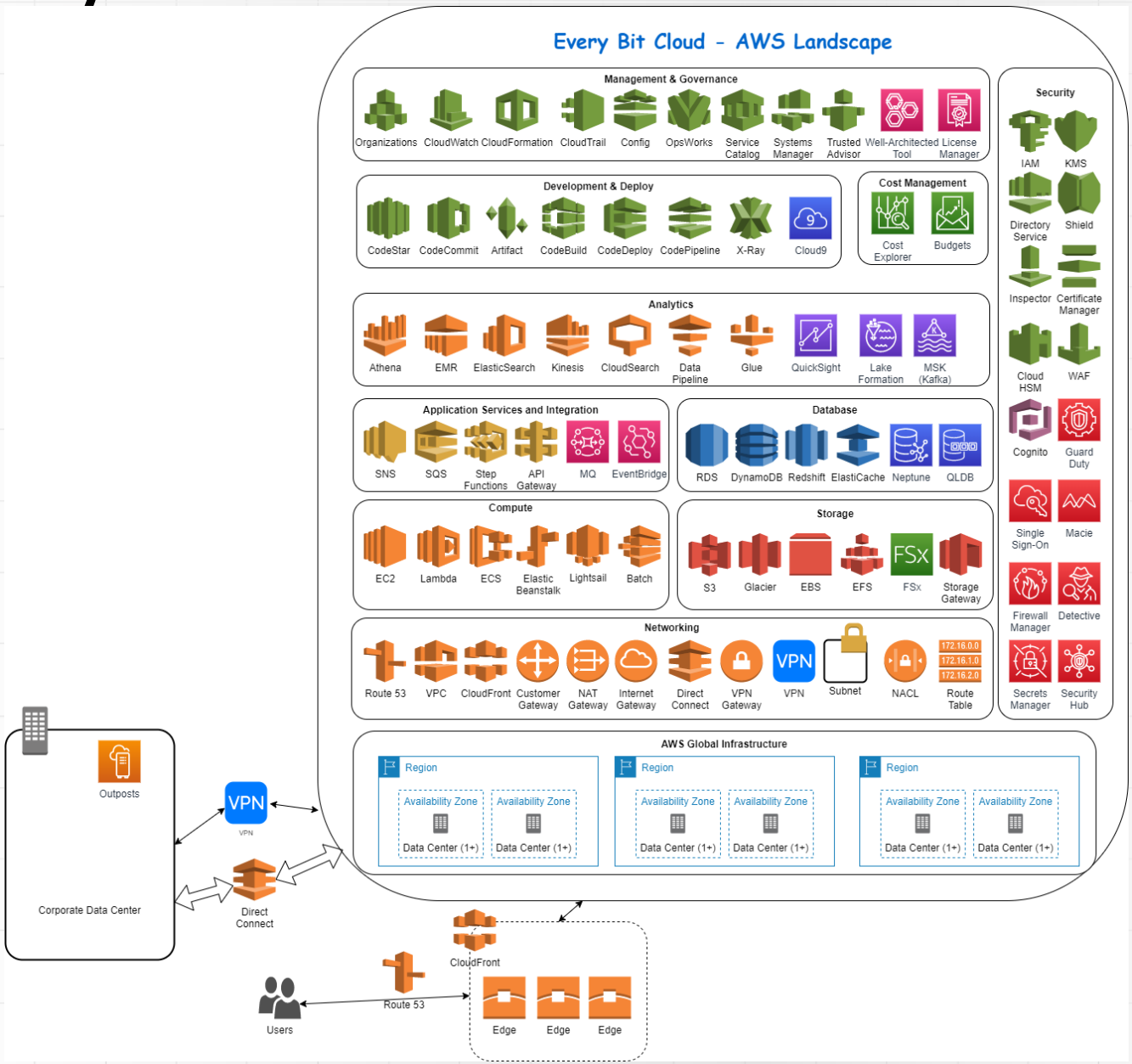


Programowanie w chmurze

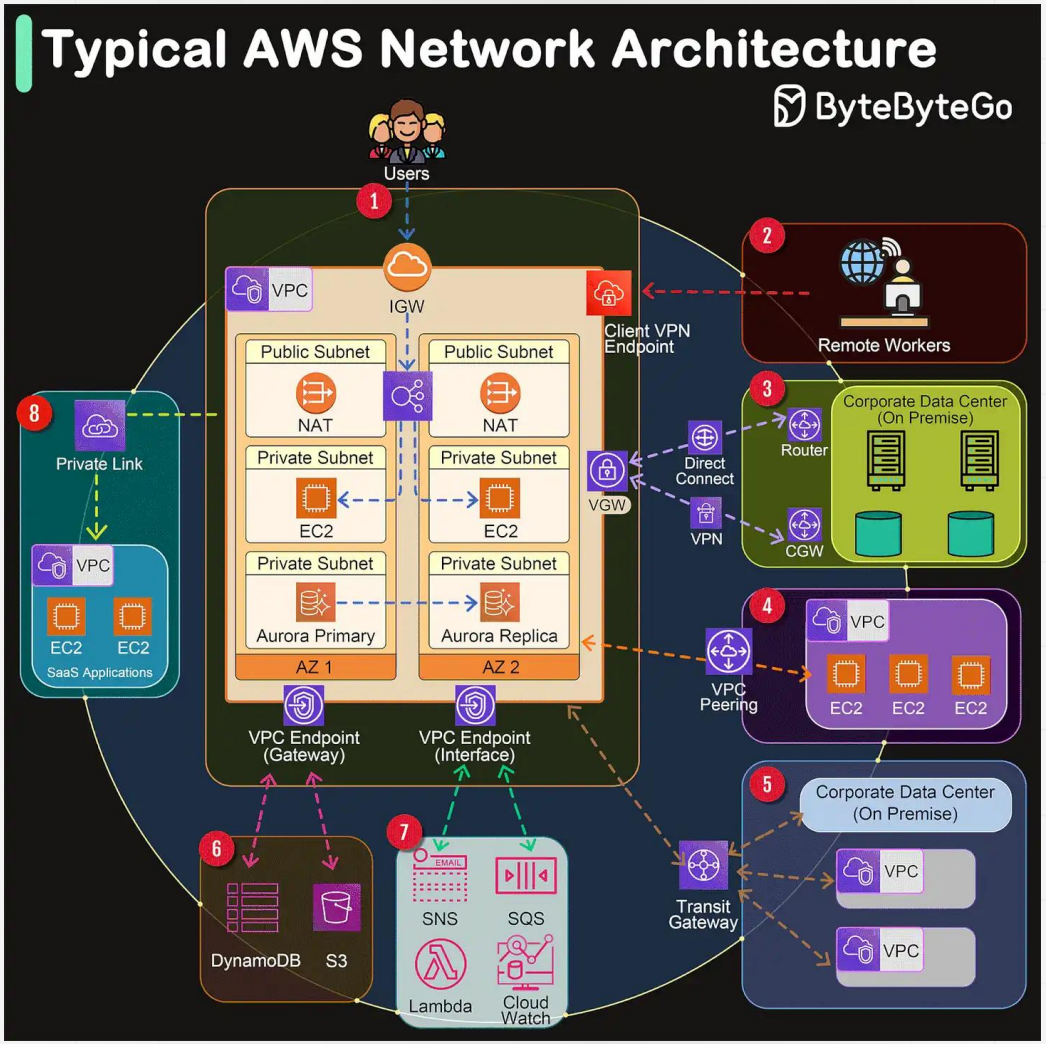
Rafał Palak

Politechnika Wrocławska

Ekosystem AWS



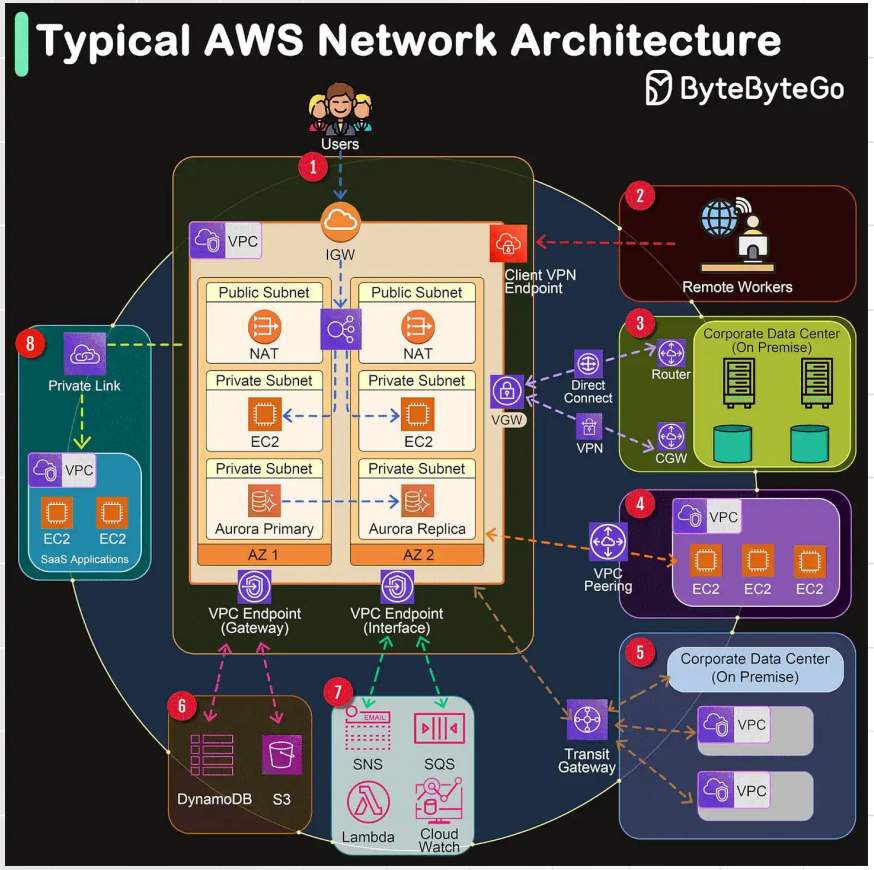
Typowa architektura AWS



https://blog.bytebytego.com/p/ep103-typical-aws-network-architecture

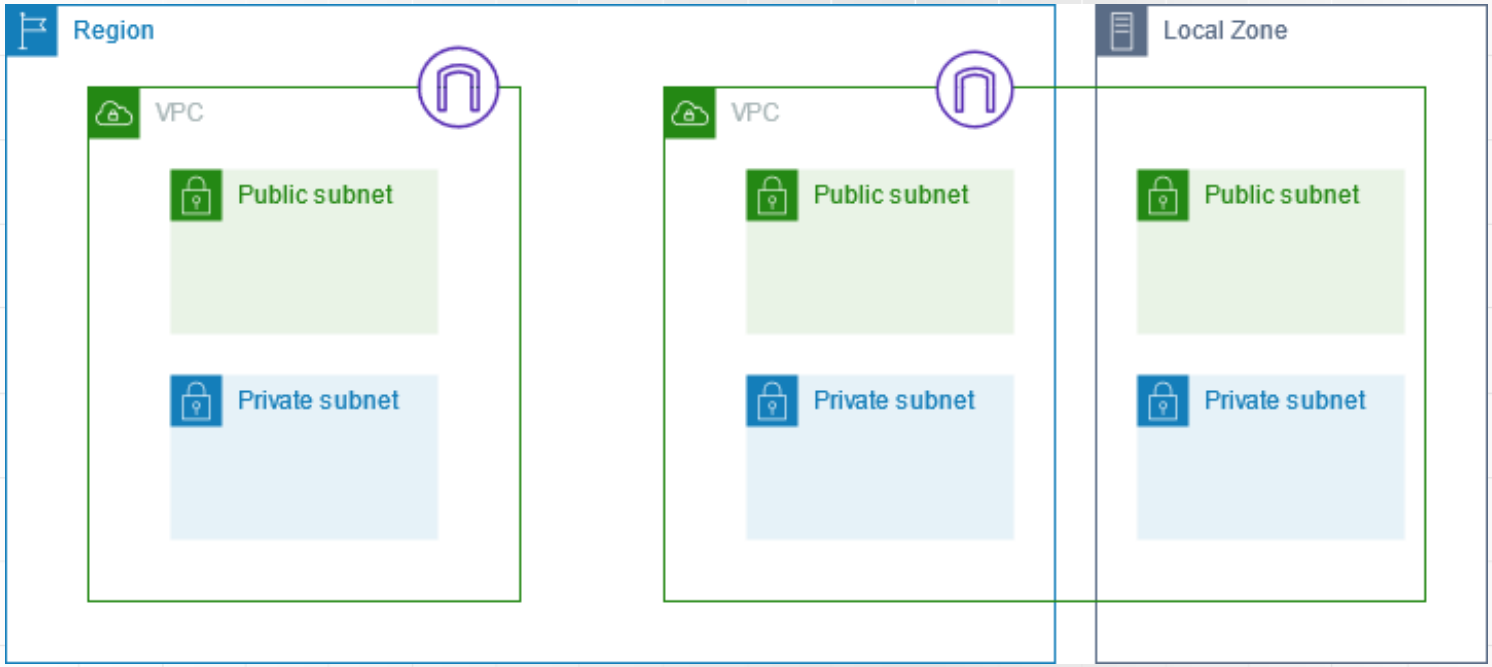
VPC (Virtual Private Cloud)

- Umożliwia uruchamianie zasobów AWS w wirtualnej sieci, którą można skonfigurować w pełni zgodnie z własnymi potrzebami.



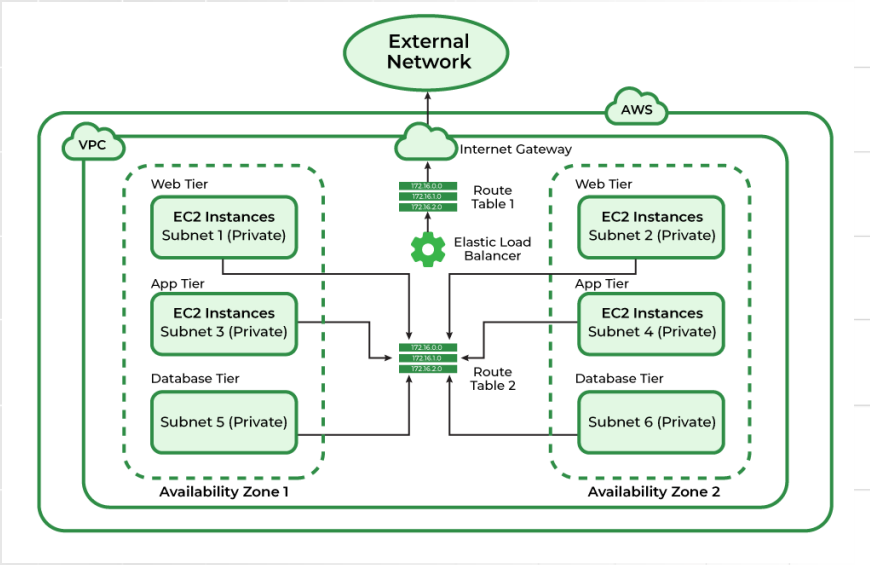
Podsieci (Subnets)

- Pozwalają na podział VPC na mniejsze, izolowane sekcje. Można tworzyć podsieci publiczne i prywatne.



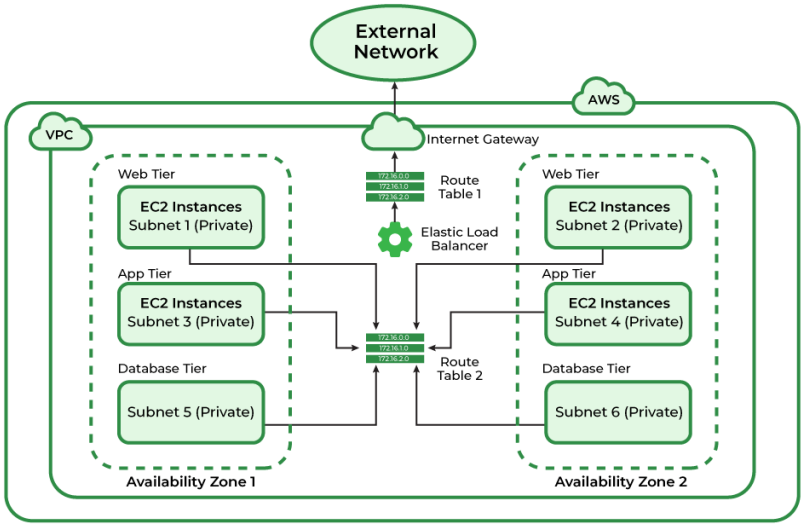
Podsieci (Subnets)

- Pozwalają na podział VPC na mniejsze, izolowane sekcje. Można tworzyć podsieci publiczne i prywatne.



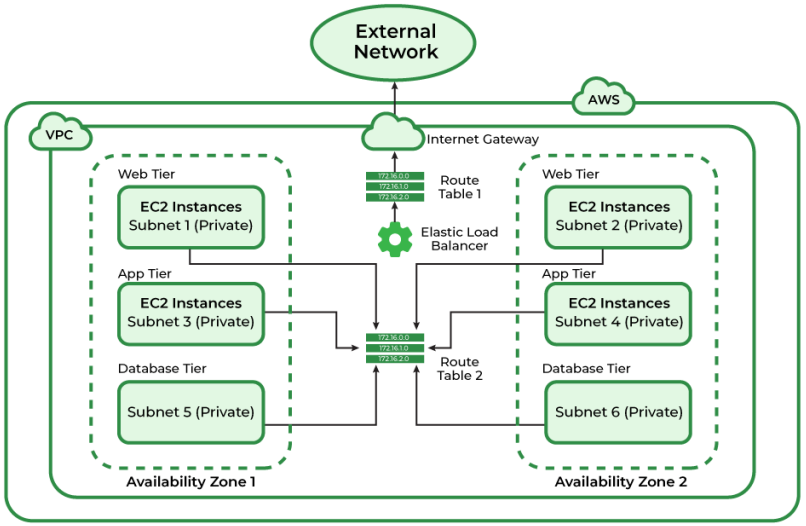
Podsieci (Subnets) – dlaczego [1]

- Segregacja ruchu sieciowego: Podsieci umożliwiają oddzielenie ruchu sieciowego pomiędzy różnymi grupami zasobów, co pomaga w zarządzaniu dostępem i kontrolowaniu przepływu danych.
- Zwiększone bezpieczeństwo: Zasoby w różnych podsieciach mogą być odizolowane od siebie, co zapobiega nieautoryzowanemu dostępowi i zwiększa bezpieczeństwo aplikacji.
- Logiczne grupowanie zasobów: Podział VPC na podsieci pozwala na logiczne grupowanie zasobów według funkcji, np. warstwa aplikacji, warstwa bazy danych.
- Łatwiejsze zarządzanie: Dzięki podziałowi na podsieci, zarządzanie zasobami staje się bardziej przejrzyste i łatwiejsze do monitorowania.



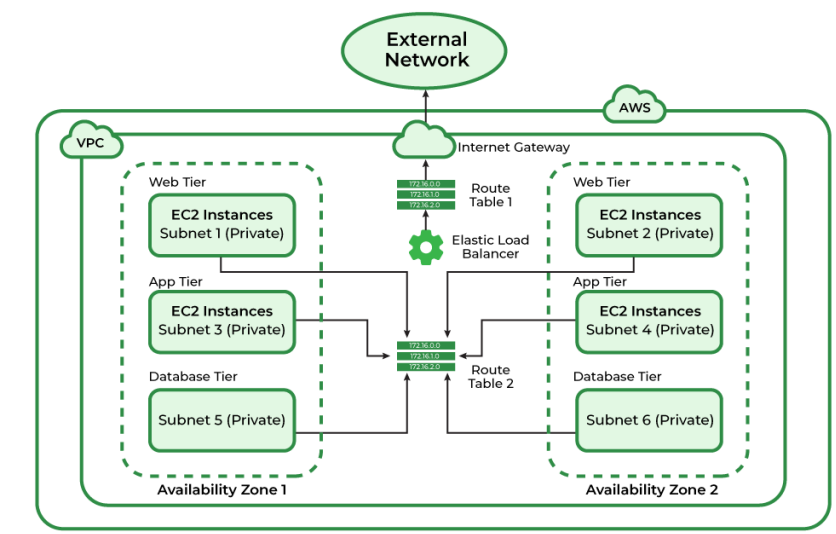
Podsieci (Subnets) – dlaczego [2]

- Publiczne i prywatne podsieci: Podsieci mogą być skonfigurowane jako publiczne (dostępne z Internetu) lub prywatne (dostępne tylko wewnętrznie), co pozwala na kontrolowanie dostępu do zasobów.
  - Publiczne podsieci: Hostują zasoby, które muszą być dostępne z Internetu, np. serwery webowe.
  - Prywatne podsieci: Hostują zasoby, które nie muszą być bezpośrednio dostępne z Internetu, np. bazy danych.
- Optymalizacja wydajności: Segmentacja sieci na podsieci pozwala na optymalizację ruchu sieciowego i zasobów, co może poprawić wydajność aplikacji.
- Lepsza kontrola nad ruchem sieciowym: Możliwość tworzenia dedykowanych tras routingu dla różnych podsieci pozwala na lepszą kontrolę i optymalizację ruchu sieciowego.



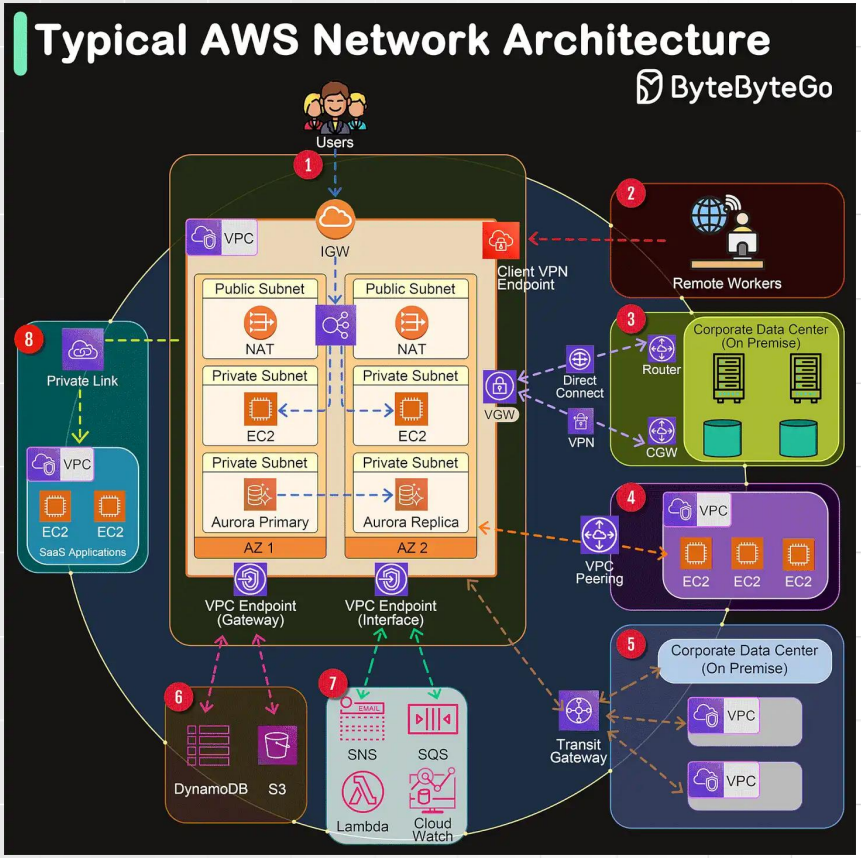
Podsieci (Subnets) – dlaczego [3]

- Zgodność z politykami bezpieczeństwa: Podział na podsieci pozwala na spełnienie wymogów regulacyjnych i polityk bezpieczeństwa poprzez izolację i kontrolę dostępu.
- Monitorowanie i audyt: Możliwość monitorowania ruchu sieciowego i działań w różnych podsieciach pozwala na lepszy audyt i zgodność z wymogami bezpieczeństwa.



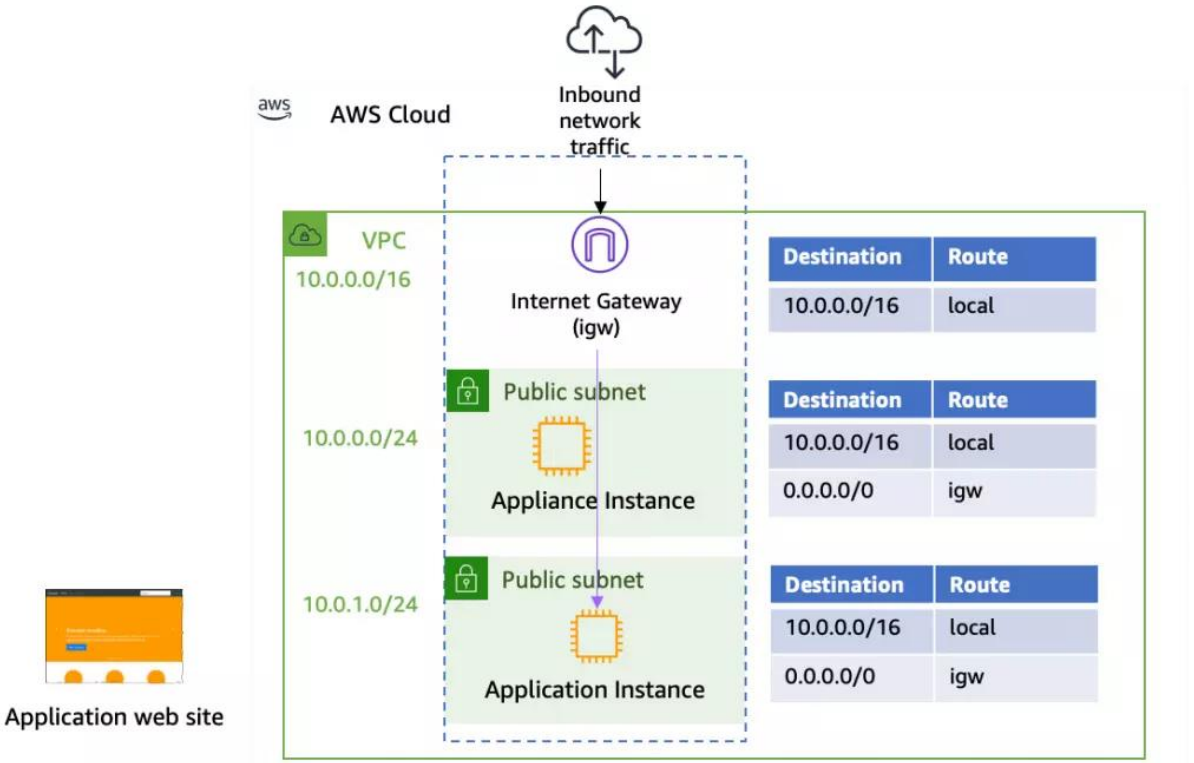
Podsieci (Subnets) – przykładowe scenariusze

- Aplikacja Webowa:
  - Publiczna podsieć: Serwery aplikacyjne, load balancery.
  - Prywatna podsieć: Bazy danych, serwery aplikacyjne back-endu, które nie wymagają dostępu z Internetu.
- Środowisko Dev/Test:
  - Publiczna podsieć: Serwery do testowania, które muszą być dostępne z zewnątrz.
  - Prywatna podsieć: Zasoby deweloperskie i testowe, które powinny być odizolowane od publicznego ruchu.
- Hybrydowe Środowisko Chmurowe:
  - Publiczna podsieć: Bramka VPN do połączeń z lokalnymi centrami danych.
  - Prywatna podsieć: Zasoby produkcyjne i dane, które muszą pozostać w bezpiecznym, prywatnym środowisku.



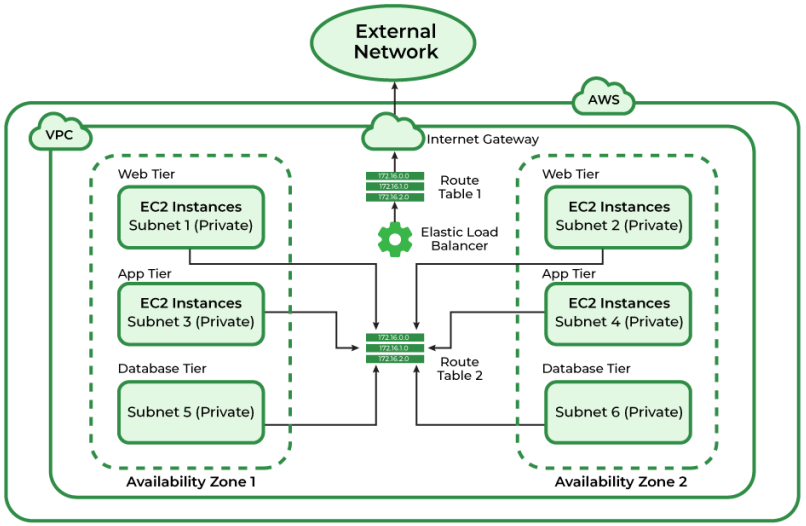
Tablice tras (Route Tables)

- To zestawy reguł (tras), które określają, jak ruch sieciowy jest kierowany w wirtualnej sieci VPC.



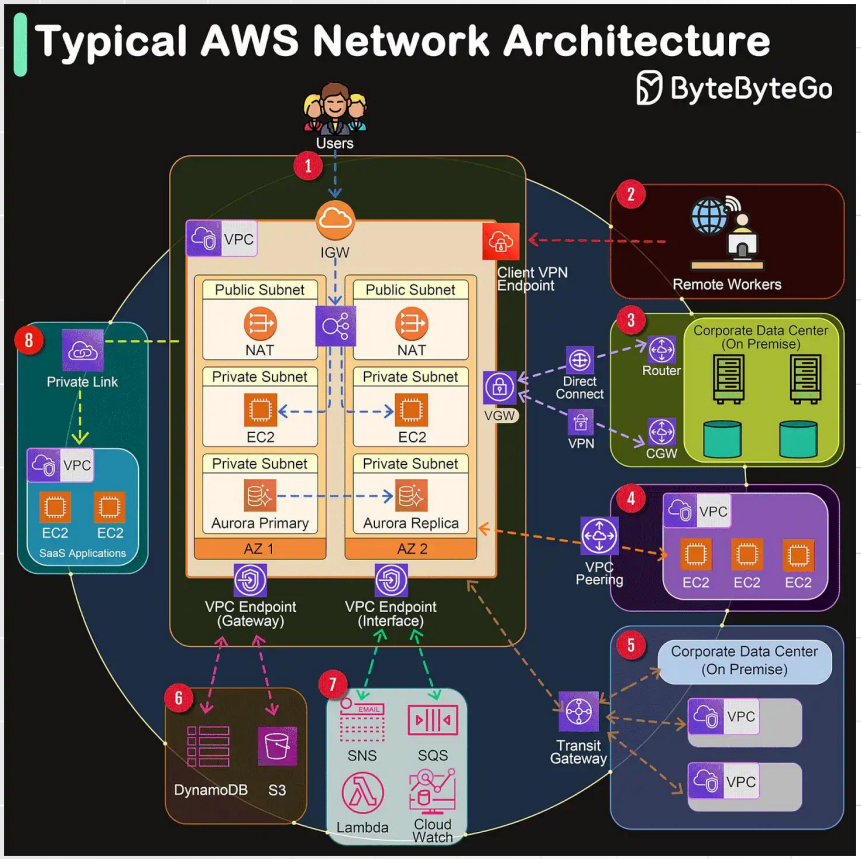
Tablice tras (Route Tables) – dlaczego

- Reguły Tras: Każda tablica tras zawiera zestaw reguł tras, które określają, gdzie kierować ruch sieciowy w zależności od jego docelowego adresu IP.
- Domyślna Tablica Tras: Każdy VPC posiada domyślną tablicę tras, która automatycznie kieruje ruch wewnątrz VPC.
- Podziały Podsieci: Każda podsieć w VPC musi być skojarzona z tablicą tras. Podsieci mogą mieć różne tablice tras, co pozwala na segmentację sieci i kontrolę ruchu.
- Izolacja Podsieci: Umożliwia izolowanie ruchu między różnymi podsieciami, co zwiększa bezpieczeństwo i kontrolę nad siecią.



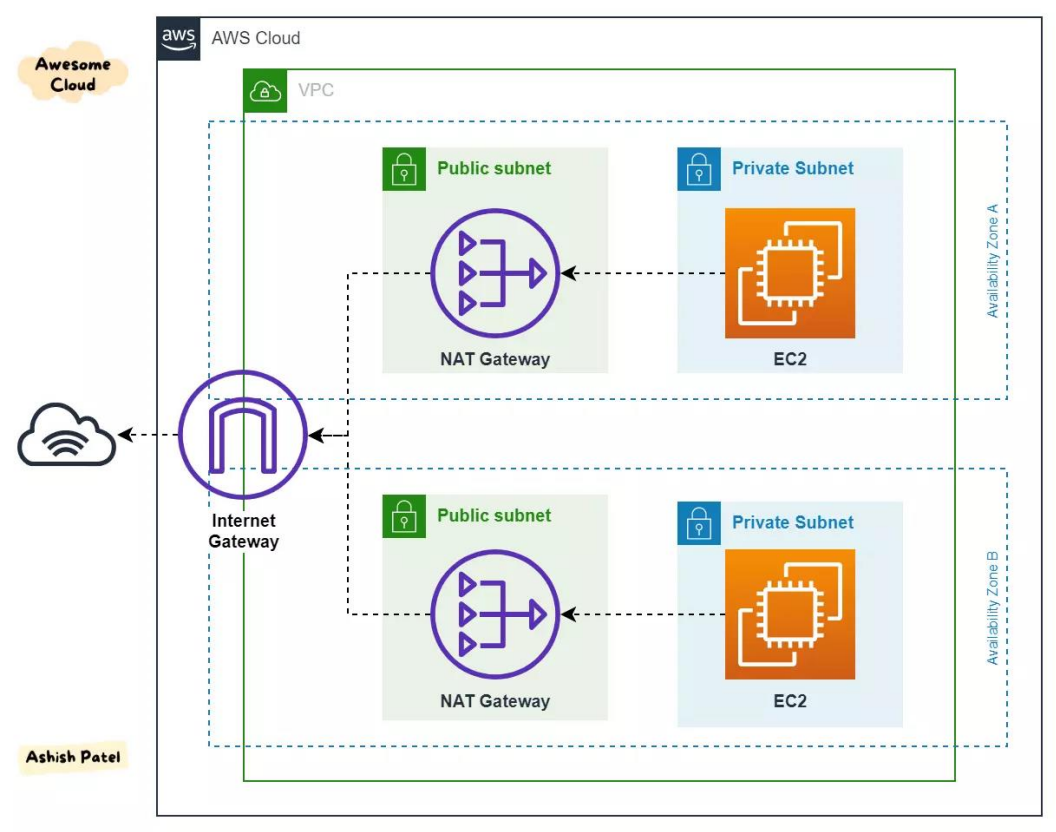
Tablice tras (Route Tables) – przykładowe scenatiusze

- Internet Gateway: Route Tables mogą zawierać trasy kierujące ruch do Internetu za pośrednictwem Internet Gateway.
- NAT Gateway: Umożliwiają prywatnym podsieciom dostęp do Internetu bez ujawniania ich prywatnych adresów IP.
- VPN Gateway i Direct Connect: Umożliwiają połączenie z lokalnymi sieciami poprzez bezpieczne połączenia VPN lub dedykowane połączenia Direct Connect.
- VPC Peering: Route Tables mogą zawierać trasy umożliwiające komunikację między różnymi VPC w ramach tej samej lub różnych regionów AWS.



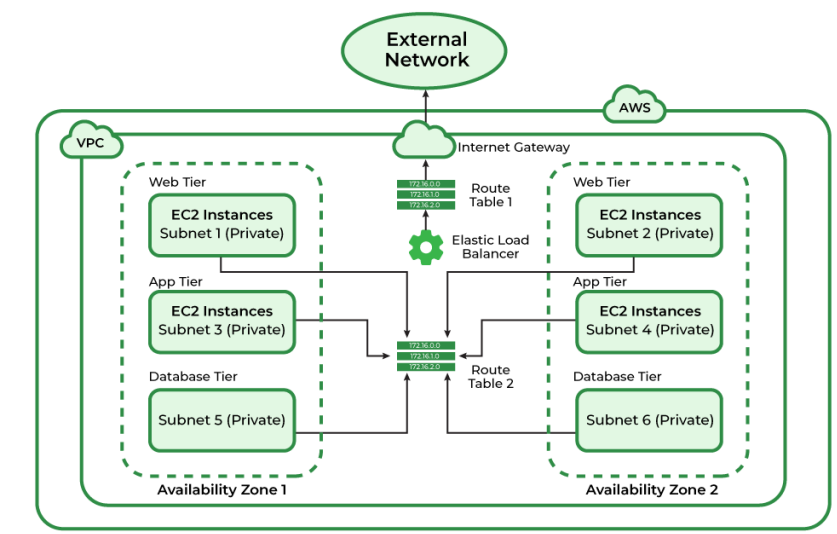
Internet Gateway

- Komponent VPC, który umożliwia komunikację między zasobami w VPC a Internetem.



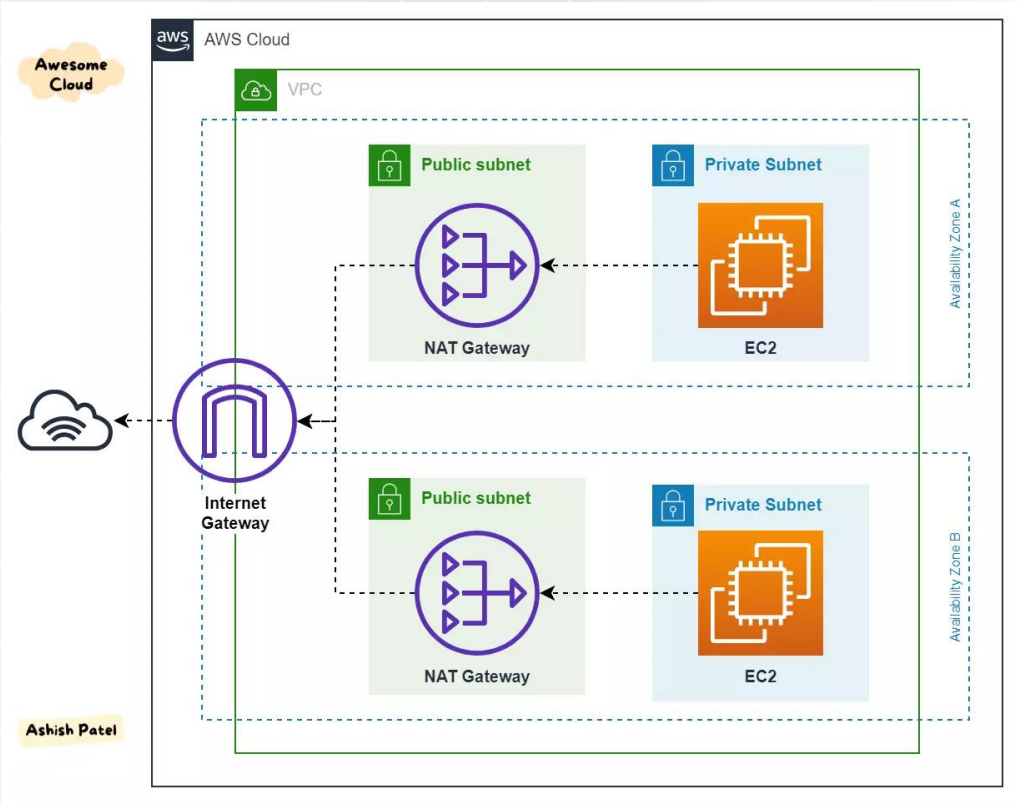
Internet Gateway - dlaczego

- Umożliwia zasobom w publicznych podsieciach (subnets) wysyłanie i odbieranie ruchu z Internetu.
- Zapewnia dostęp do Internetu dla instancji EC2 oraz innych usług AWS w publicznych podsieciach.
- Działa jako bramka, która obsługuje trasowanie ruchu internetowego do i z VPC.
- W połączeniu z tablicami tras (route tables) definiuje, które podsieci mają dostęp do Internetu.
- Zapewnia automatyczną skalowalność, aby obsługiwać zmienne natężenie ruchu.
- Wysoka dostępność dzięki redundancji, co zapewnia niezawodność połączenia z Internetem.



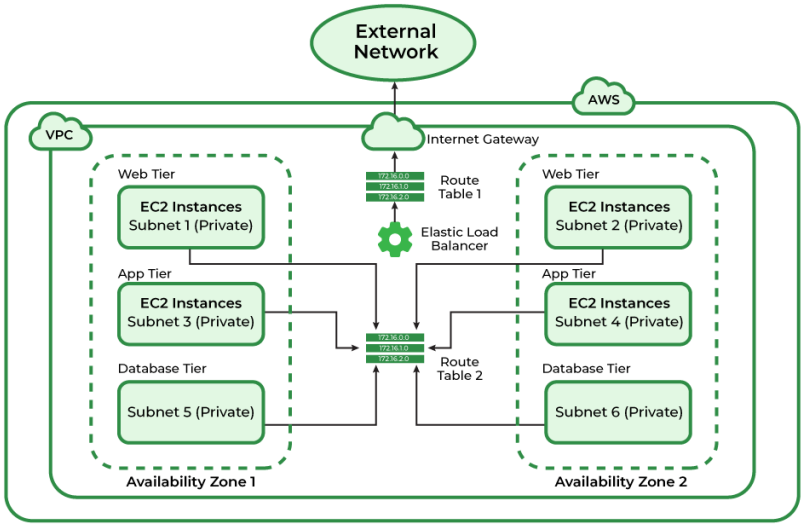
NAT Gateway

- Jest kluczowym elementem infrastruktury sieciowej w Amazon Web Services (AWS). Służy do umożliwienia instancjom w prywatnych subnetach (podsieciach) dostępu do Internetu lub innych usług AWS bez ujawniania ich prywatnych adresów IP.



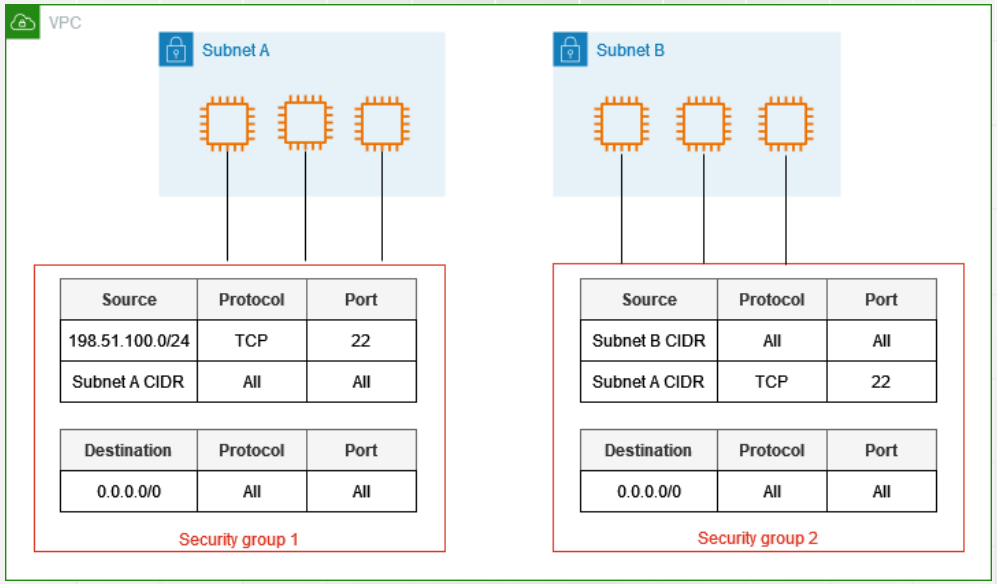
NAT Gateway – dlaczego?

- Instancje w prywatnych podsieciach są chronione przed bezpośrednim dostępem z Internetu. Używając NAT Gateway, można zapewnić, że instancje te będą mogły inicjować połączenia wychodzące, ale nie będą mogły otrzymywać bezpośrednich połączeń przychodzących z Internetu.
- NAT Gateway jest zarządzaną usługą AWS, co oznacza, że AWS zajmuje się skalowaniem, zarządzaniem i utrzymaniem. Użytkownicy nie muszą sami konfigurować i zarządzać instancjami NAT, co upraszcza zarządzanie infrastrukturą.
- NAT Gateway jest automatycznie skalowana i redundantna w obrębie strefy dostępności (Availability Zone), co zapewnia wysoką dostępność i odporność na awarie.



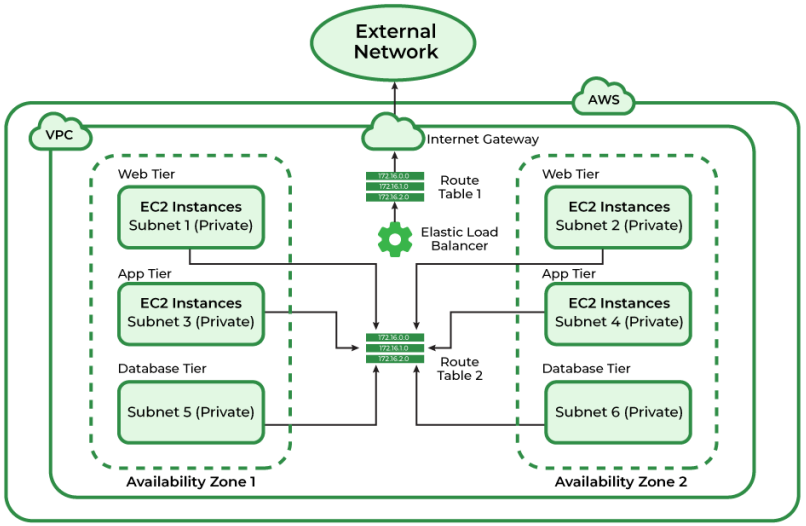
Security Groups

- To wirtualne zapory ogniowe (firewalle), które kontrolują ruch przychodzący i wychodzący do zasobów uruchamianych w Amazon VPC. Są to zestawy reguł, które definiują, jaki ruch jest dozwolony do i z instancji EC2 oraz innych zasobów w ramach VPC.



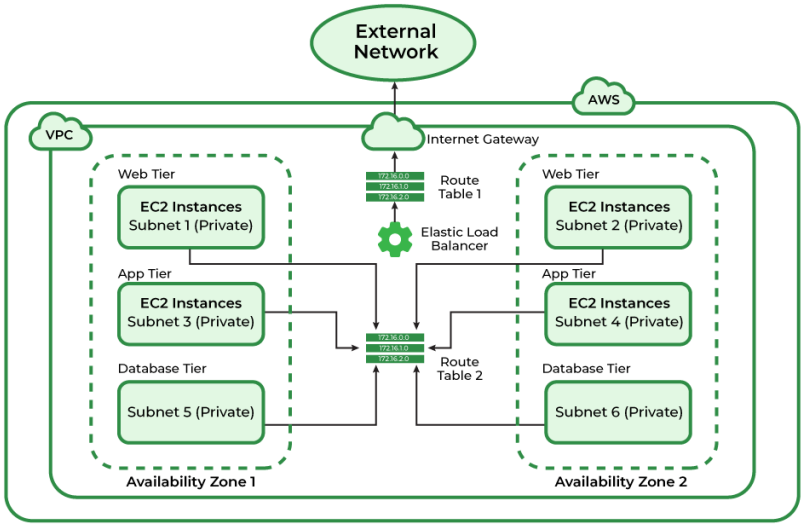
Security Groups – dlaczego?

- Security Groups pozwalają definiować reguły, które określają, jaki ruch przychodzący jest dozwolony do zasobów przypisanych do danej grupy.
- Reguły te mogą obejmować specyfikację protokołów (TCP, UDP, ICMP), portów oraz źródłowych adresów IP lub zakresów CIDR.
- Można także definiować reguły określające, jaki ruch wychodzący z zasobów przypisanych do Security Group jest dozwolony.
- Reguły wychodzące działają podobnie jak przychodzące, pozwalając na specyfikację protokołów, portów i docelowych adresów IP.



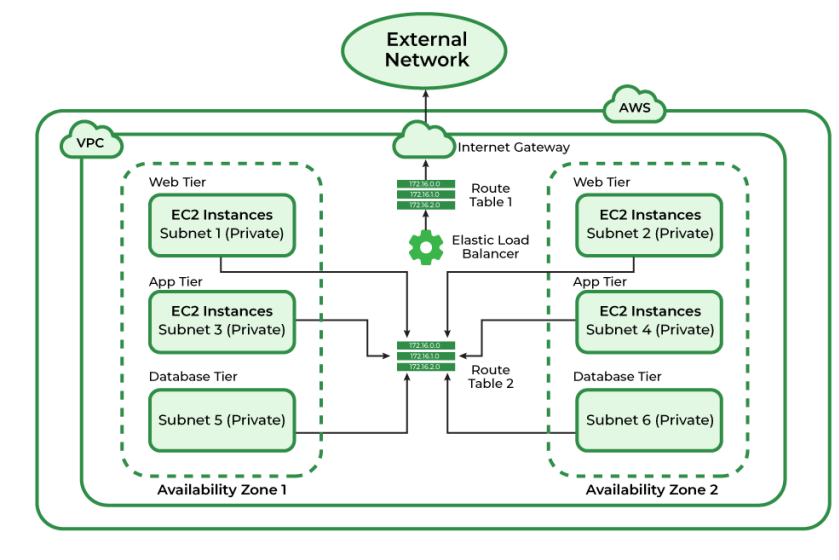
Security Groups – dlaczego?

- Security Groups są stanowymi zaporami sieciowymi, co oznacza, że jeśli ruch jest dozwolony w jednym kierunku, to odpowiadający ruch w przeciwnym kierunku jest automatycznie dozwolony.
- Security Groups pomagają w izolacji i ochronie zasobów w VPC, umożliwiając szczegółowe kontrolowanie dostępu do każdej instancji lub grupy instancji.



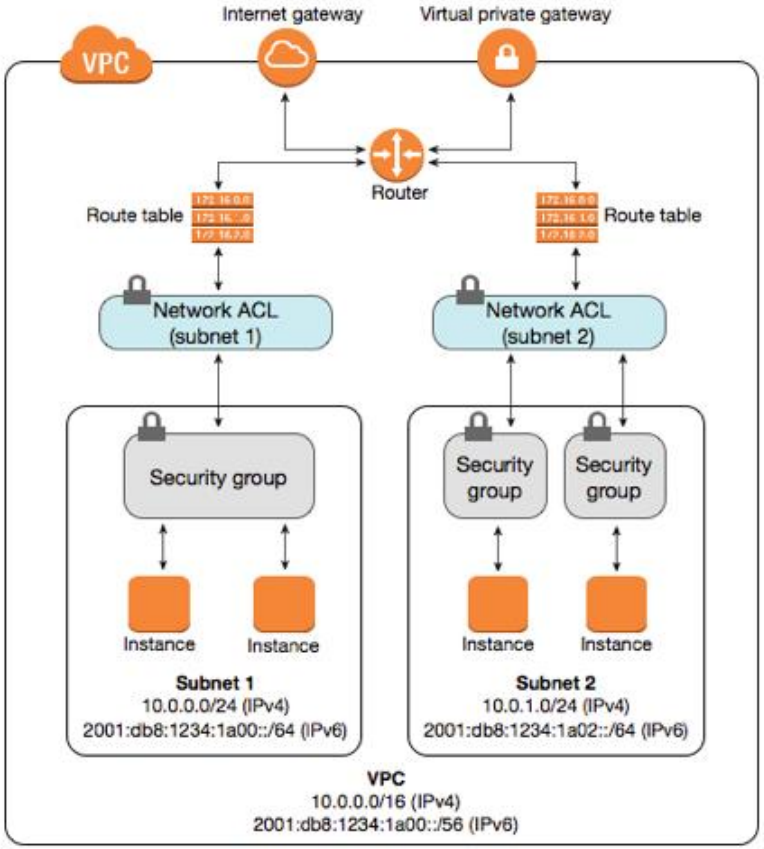
Security Groups – działanie

- Administratorzy mogą tworzyć reguły w Security Groups, które określają dozwolone połączenia.
- Przykładowo, można utworzyć regułę, która zezwala na ruch przychodzący na port 80 (HTTP) z dowolnego adresu IP.
- Security Groups są przypisywane do instancji EC2 i innych zasobów podczas ich tworzenia lub w dowolnym momencie później.
- Jedna instancja może mieć przypisane wiele Security Groups, a każda Security Group może być przypisana do wielu instancji.
- Zmiany w regułach Security Groups są natychmiast stosowane do wszystkich przypisanych do nich instancji, co ułatwia zarządzanie bezpieczeństwem.



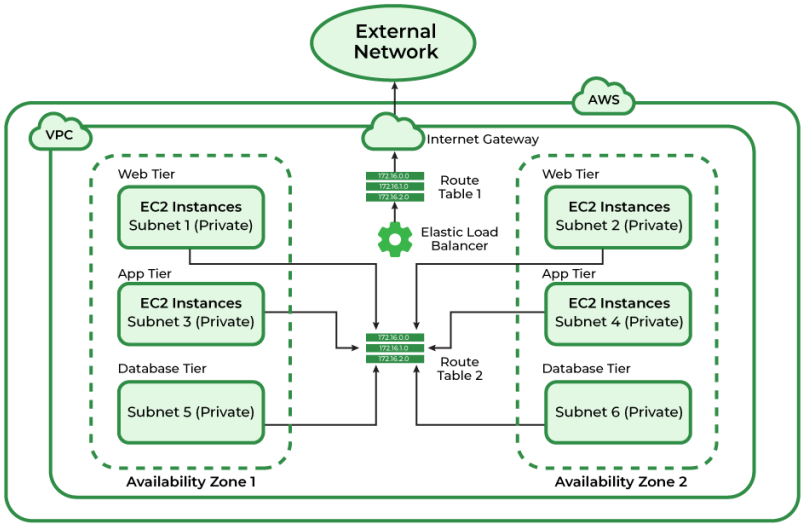
Network ACLs (Access Control Lists)

- To jedna z warstw zabezpieczeń w Amazon VPC, które pełnią ważną rolę w zarządzaniu ruchem sieciowym do i z podsieci. Główne cele:
  - Zarządzanie ruchem sieciowym: Network ACLs kontrolują ruch przychodzący i wychodzący na poziomie podsieci, umożliwiając określenie, które ruchy są dozwolone, a które zablokowane.
  - Dodatkowa warstwa zabezpieczeń: Działają jako dodatkowa warstwa zabezpieczeń obok Security Groups, które działają na poziomie instancji.



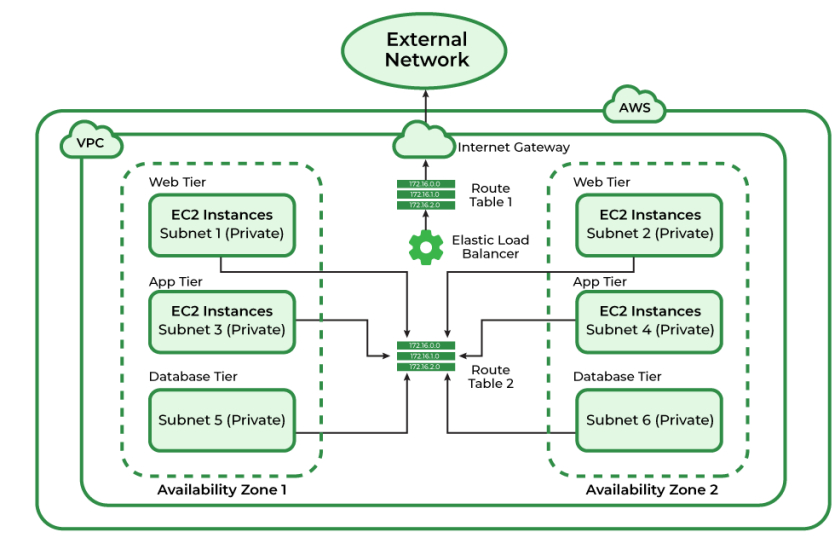
Network ACLs – kluczowe funkcje

- Inbound Rules (Reguły przychodzące): Określają zasady dla ruchu przychodzącego do podsieci.
- Outbound Rules (Reguły wychodzące): Określają zasady dla ruchu wychodzącego z podsieci.
- Stateless: Network ACLs są stateless, co oznacza, że każda reguła ruchu jest analizowana niezależnie. Dla każdego pakietu przychodzącego i wychodzącego wymagana jest osobna reguła.



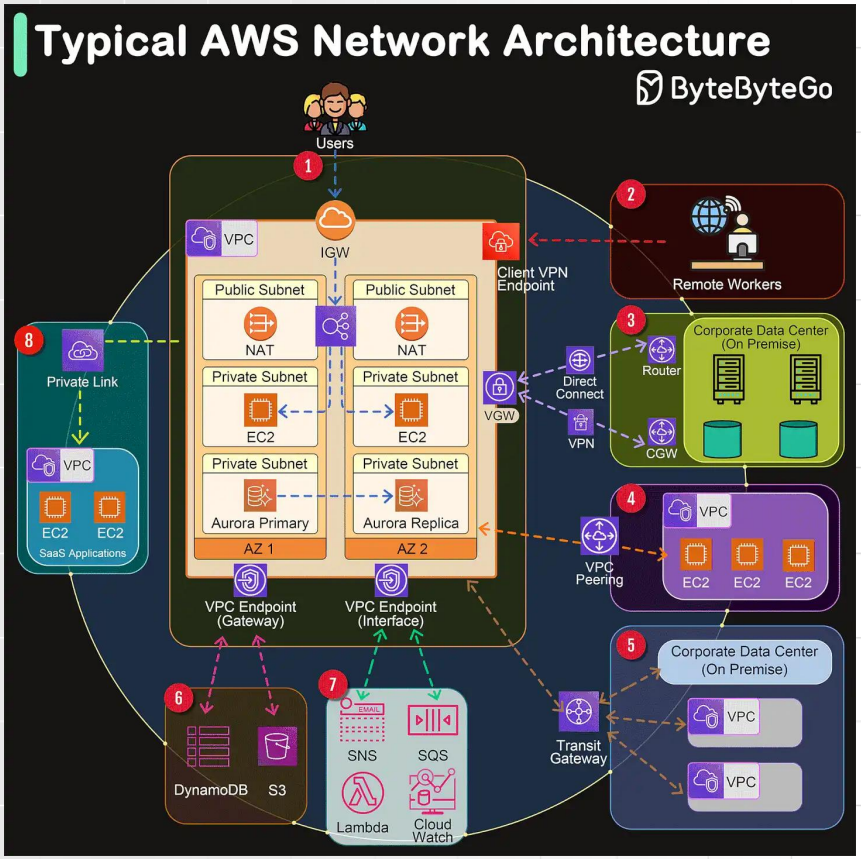
Network ACLs – zasady działania

- Numerowanie reguł: Każda reguła jest numerowana, a przetwarzanie odbywa się od najniższego do najwyższego numeru. Pierwsza pasująca reguła jest zastosowana.
- Domyślne reguły: Domyślna Network ACL pozwala na cały ruch (inbound i outbound). Można to zmienić, aby bardziej restrykcyjnie kontrolować ruch.
- Zablokowane i dozwolone ruchy: Każda reguła może pozwalać (allow) lub blokować (deny) określony rodzaj ruchu na podstawie protokołu, numeru portu i adresu IP źródłowego/destynacji.



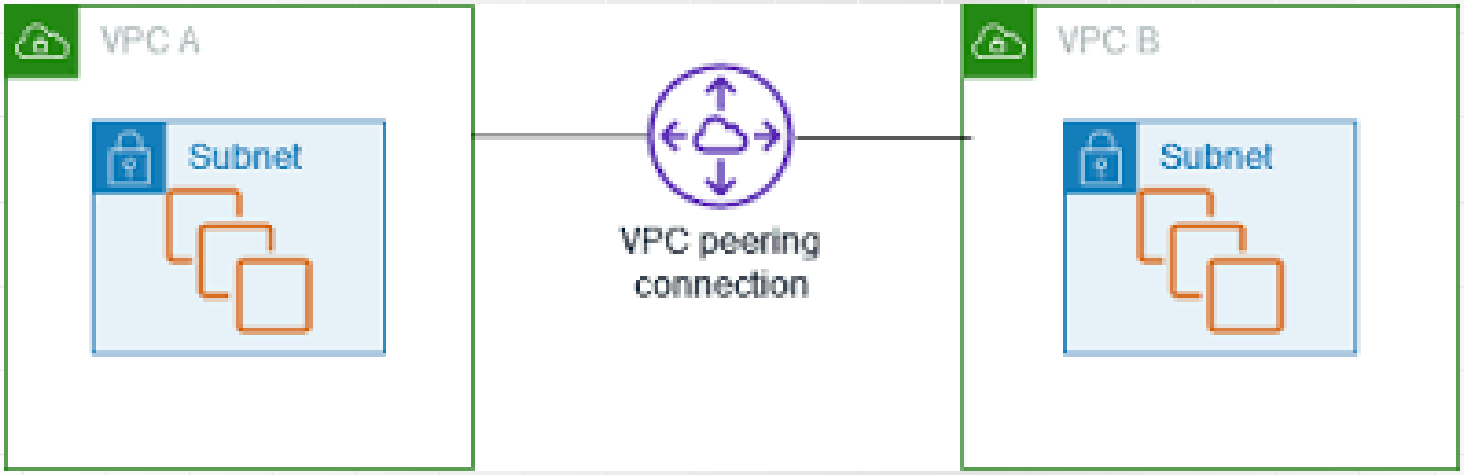
Network ACLs – przykładowe zastosowania

- Ochrona Podsieci Publicznych i Prywatnych
  - Publiczne Subnety: Network ACLs mogą być skonfigurowane, aby pozwalać na ruch HTTP/HTTPS (porty 80 i 443) oraz blokować inne niepotrzebne protokoły.
  - Prywatne Subnety: Mogą blokować cały ruch zewnętrzny, pozwalając jedynie na komunikację z określonymi, zaufanymi źródłami.
- Zarządzanie Zgodnością i Bezpieczeństwem
  - Reguły zgodności: Umożliwiają dostosowanie ustawień sieci do wymagań zgodności z regulacjami branżowymi, np. PCI-DSS.
  - Segmentacja sieci: Poprawiają bezpieczeństwo przez segmentację sieci i ograniczenie komunikacji między podsieciami.
- Redukcja Ruchu Niechcianego
  - Blokowanie złośliwego ruchu: Umożliwiają szybkie blokowanie ruchu z nieznanych lub złośliwych adresów IP.



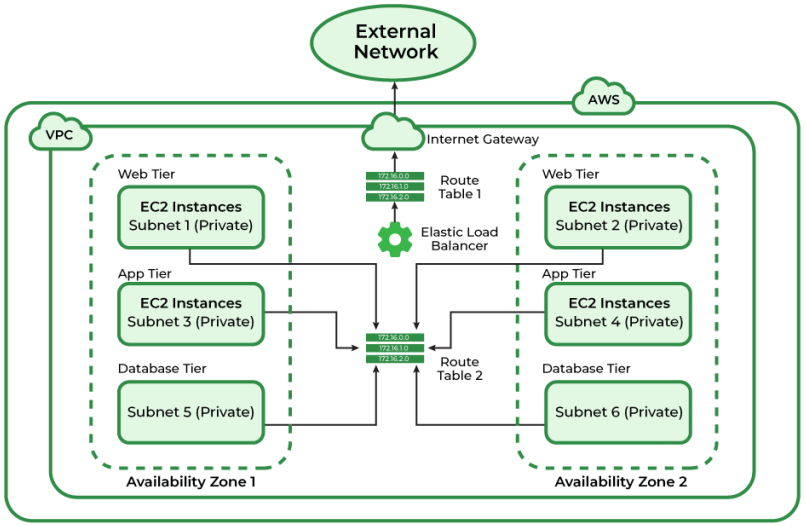
Peering VPC

- Umożliwia prywatne połączenie dwóch różnych Virtual Private Clouds (VPC) w ramach tej samej lub różnych regionów AWS. Dzięki peeringowi VPC zasoby w jednym VPC mogą komunikować się z zasobami w drugim VPC, tak jakby znajdowały się w tej samej sieci.



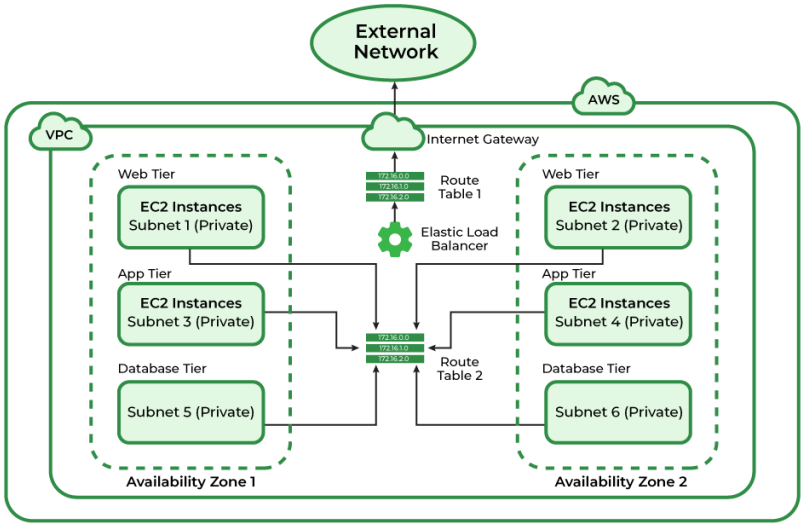
Peering VPC – dlaczego?

- Łączenie środowisk produkcyjnych i testowych: Umożliwia połączenie różnych środowisk (np. produkcyjnego i testowego) w celu uproszczenia zarządzania i monitorowania.
- Konsolidacja zasobów: Łączenie różnych VPC w ramach jednej organizacji, aby uprościć dostęp do wspólnych zasobów, takich jak bazy danych, usługi plikowe, itp.
- Unikanie publicznego internetu: Zapewnia bezpieczną komunikację bez konieczności przechodzenia przez publiczny Internet, co zwiększa bezpieczeństwo i redukuje opóźnienia.
- Zachowanie prywatności danych: Dane przesyłane między VPC przez połączenie peeringowe pozostają w



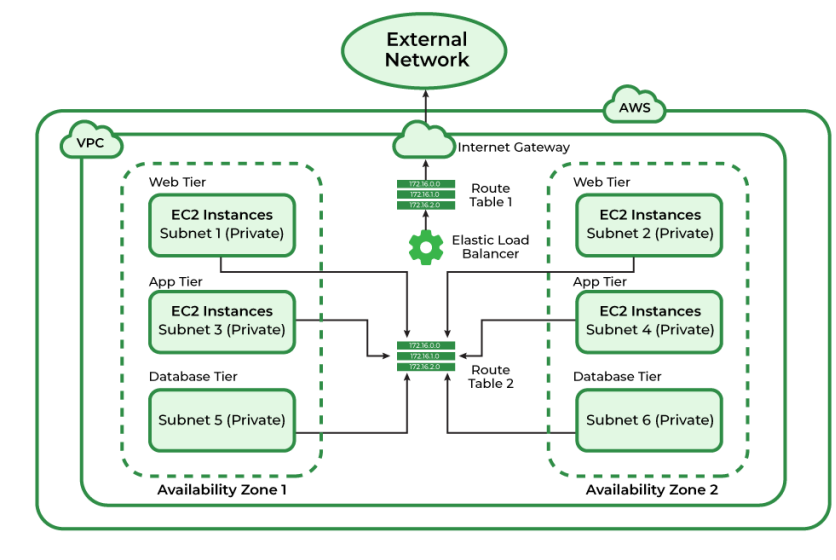
Peering VPC – dlaczego?

- Rozdzielanie obciążeń: Rozdzielanie różnych komponentów aplikacji na różne VPC w celu lepszego zarządzania i skalowania.
- Zwiększanie elastyczności: Możliwość dodawania nowych VPC bez konieczności zmiany istniejącej architektury sieciowej.
- Współpraca między firmami: Umożliwia bezpieczne połączenie infrastruktury sieciowej z partnerami biznesowymi lub klientami bez konieczności korzystania z publicznego Internetu.



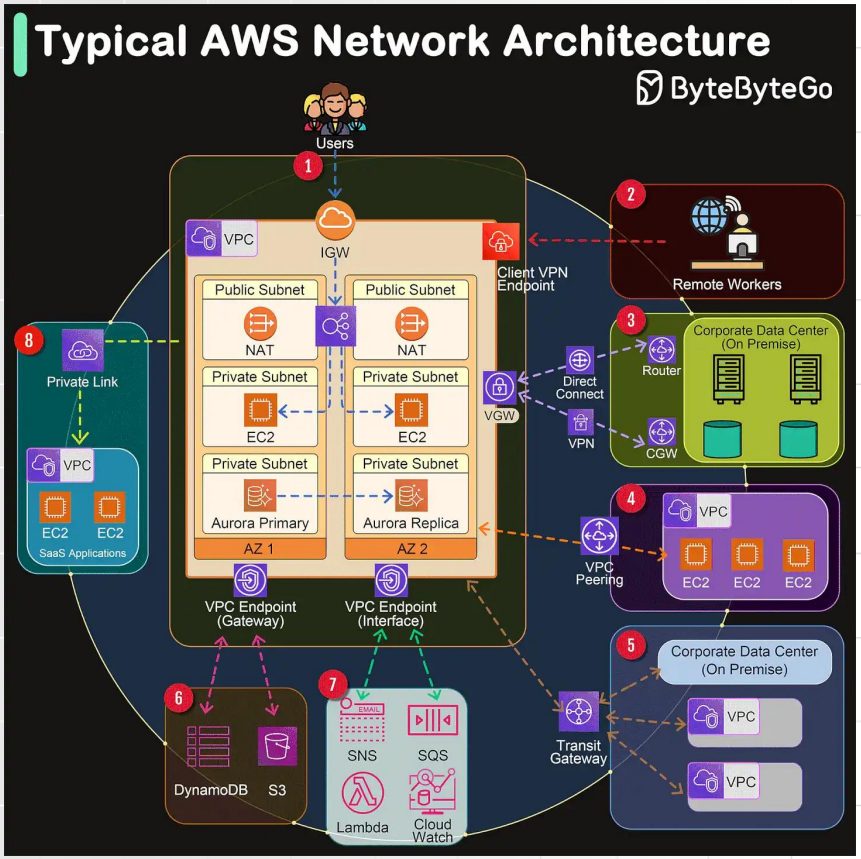
Peering VPC – zalety peeringu VPC

- Niskie Opóźnienia: Połączenia peeringowe zapewniają niskie opóźnienia, co jest kluczowe dla aplikacji wymagających szybkiej komunikacji między komponentami.
- Wysoka Przepustowość: Zapewnia wysoką przepustowość dla transferów danych między VPC.
- Elastyczność i Skalowalność: Możliwość elastycznego skalowania infrastruktury i dodawania nowych VPC w miarę rozwoju potrzeb.
- Łatwość Konfiguracji: Konfiguracja połączenia peeringowego jest stosunkowo prosta i nie wymaga skomplikowanych ustawień.



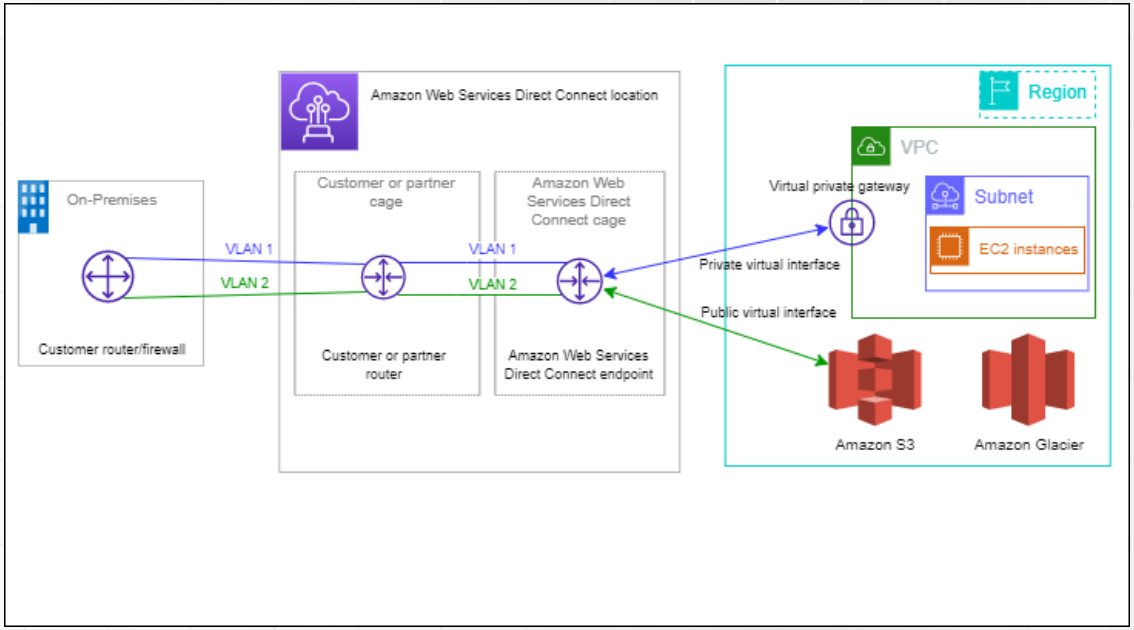
Peering VPC – przykładowe zastosowanie

- Multiregionalne Aplikacje
  - Rozproszone bazy danych: Umożliwia synchronizację danych między bazami danych zlokalizowanymi w różnych regionach AWS.
  - Globalne aplikacje: Połączenie różnych regionalnych VPC w celu zapewnienia globalnej dostępności aplikacji.
- Współdzielone Usługi
  - Centralne usługi logowania: Umożliwia centralne gromadzenie logów z różnych VPC w jednym miejscu.
  - Wspólne bazy danych: Dostęp do wspólnych baz danych przez różne VPC w ramach jednej organizacji.



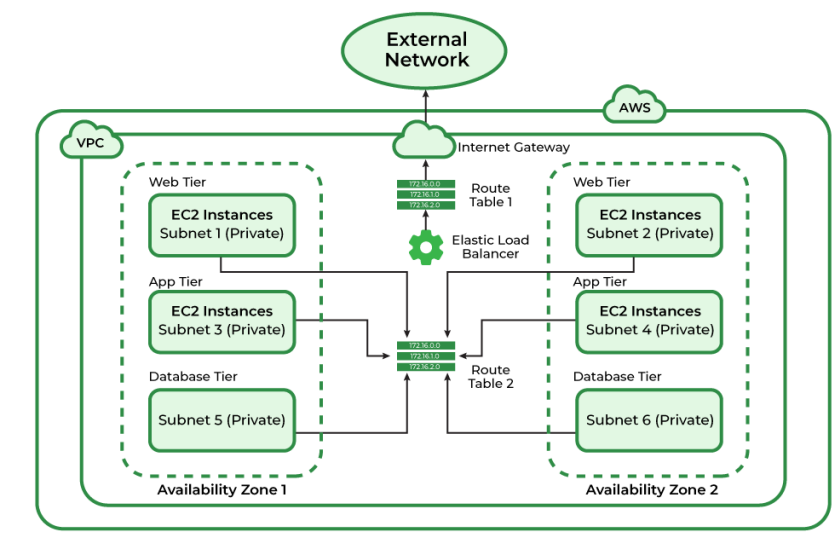
Amazon Direct Connect

- To usługa umożliwiająca nawiązanie dedykowanego połączenia sieciowego między lokalnym centrum danych a AWS, zapewniającym bardziej przewidywalne i niezawodne połączenie niż tradycyjne połączenia internetowe.



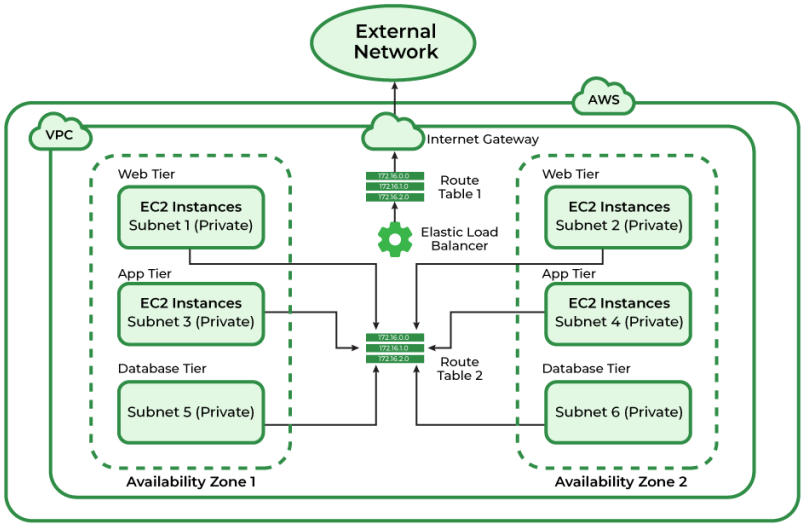
Amazon Direct Connect – dlaczego? [1]

- Stabilność połączenia: Bezpośrednie połączenie omija publiczny Internet, co minimalizuje opóźnienia i wahania w jakości połączenia.
- Przewidywalna wydajność: Połączenie dedykowane zapewnia stałą przepustowość i stabilną wydajność.
- Izolacja od publicznego Internetu: Połączenie bezpośrednie minimalizuje ryzyko związane z atakami i przechwytywaniem danych.
- Bezpieczne przesyłanie danych: Możliwość zastosowania dodatkowych mechanizmów szyfrowania.



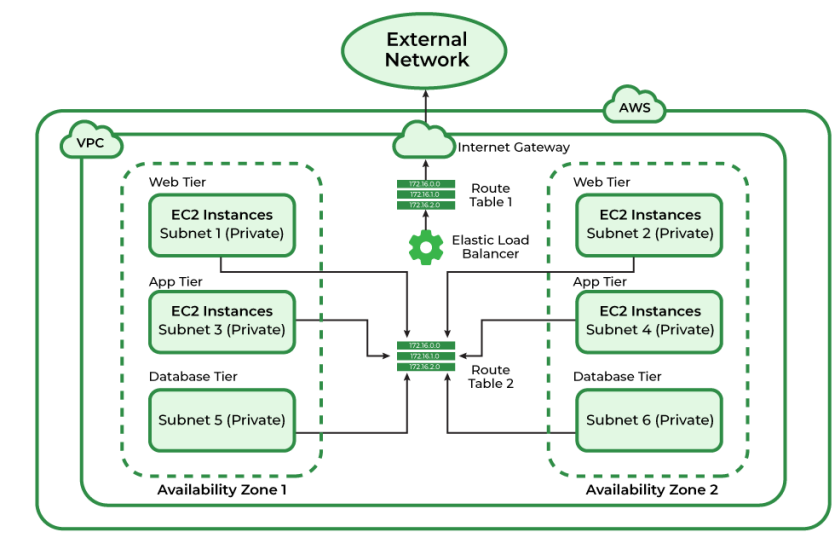
Amazon Direct Connect – dlaczego? [2]

- Redukcja kosztów transferu danych: Koszty transferu danych mogą być niższe w porównaniu do tradycyjnych połączeń internetowych, zwłaszcza przy dużych wolumenach przesyłanych danych.
- Mniejsze opłaty za egress: Niższe opłaty za transfer wychodzący z AWS w porównaniu do transferu przez publiczny Internet.
- Elastyczność przepustowości: Możliwość dostosowania przepustowości połączenia do bieżących potrzeb, od 50 Mbps do 10 Gbps lub więcej.
- Integracja z innymi usługami AWS: Bezproblemowa współpraca z VPC, S3, EC2 i innymi usługami AWS.



Amazon Direct Connect – dlaczego? [3]

- Pełna kontrola nad połączeniem: Umożliwia zarządzanie ruchem i konfiguracją sieci zgodnie z wymaganiami biznesowymi.
- Wysoka dostępność: Możliwość konfiguracji redundantnych połączeń dla zapewnienia wysokiej dostępności i niezawodności.



Wrocław
University
of Science
and Technology

Dziękuję za uwagę