



Dobro došli



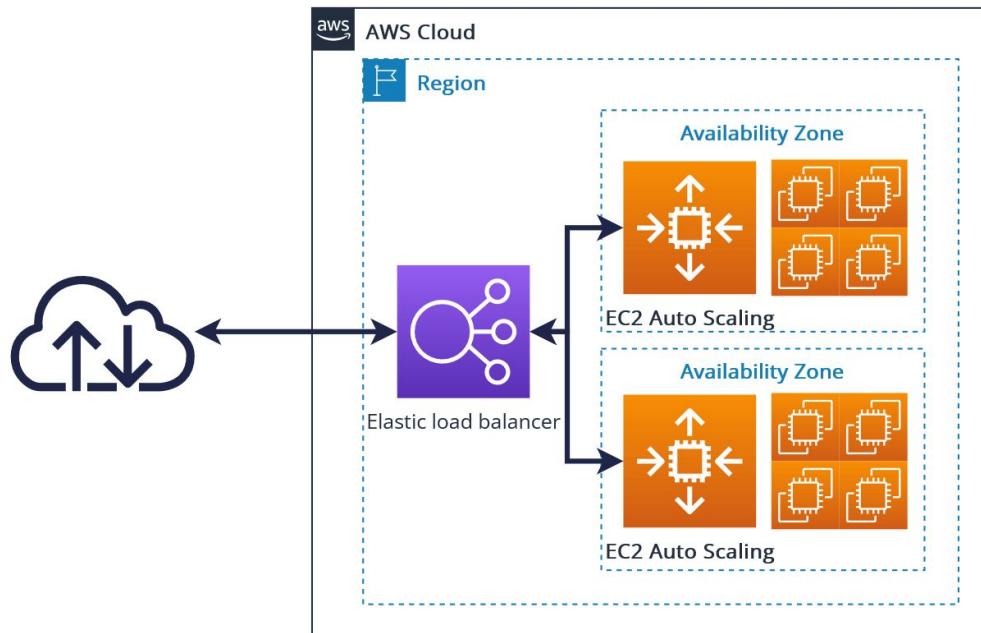
Agenda

1. Globalna infrastruktura
2. Mrežni koncepti
3. Internet saobraćaj
4. Security grupe
5. NACL
6. NAT Gateway

AWS globalna infrastruktura

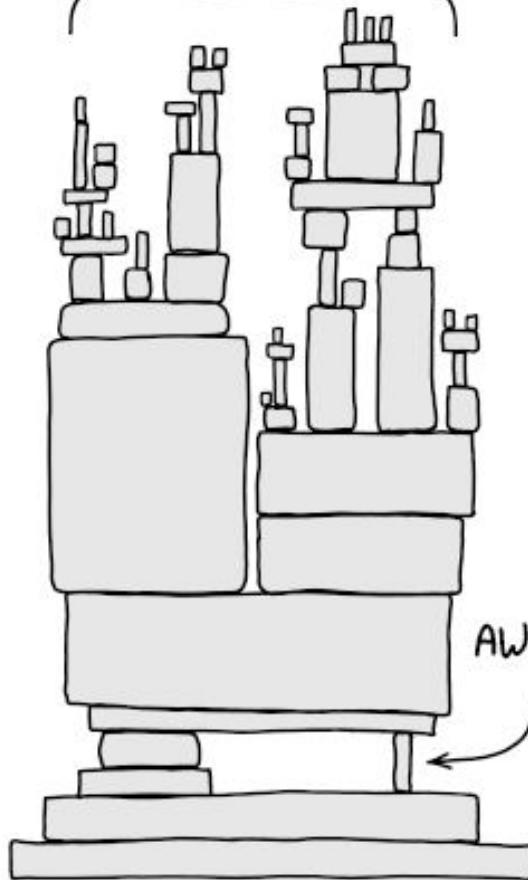
- **Regioni (Regions):** Geografske oblasti gde su grupisani AWS data centri. Svaki region je potpuno izolovan i nezavisan.
- **Zone dostupnosti (Availability Zones - AZ):** Više izolovanih lokacija unutar Regiona. Svaka AZ ima sopstveno napajanje, hlađenje i mrežu, i povezane su brzim, privatnim mrežama sa malom latencijom.
- **Edge Locations:** Mreža manjih centara podataka koja isporučuje sadržaj bliže korisnicima radi smanjenja latencije (koriste se za CloudFront i Route 53).
- <https://aws.amazon.com/about-aws/global-infrastructure>

Visoka dostupnost (High Availability)



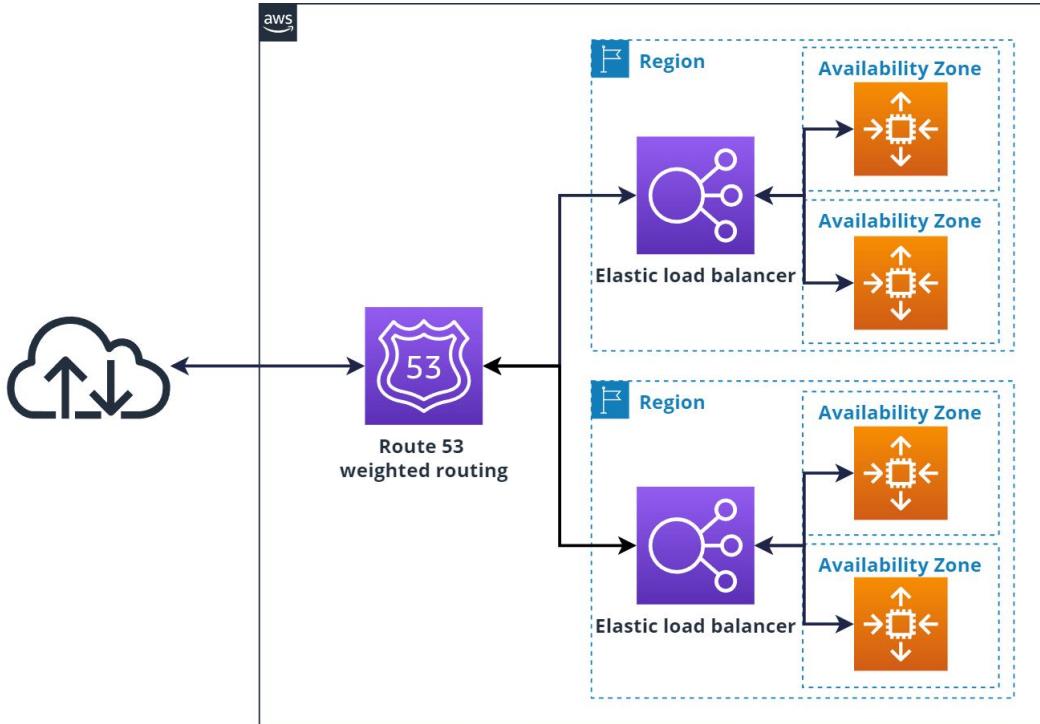
- Visoka dostupnost omogućava neprekidan rad aplikacija
- Smanjuje uticaj potencijalnih prekida ili kvarova sistema
- Postiže se distribucijom opterećenja kroz različite AZ
- Automatsko prebacivanje na rezervne instance u slučaju kvara
- Omogućava brzo oporavljanje od svih vrsta incidenata
- Osigurava konstantan pristup podacima i uslugama

ALL MODERN DIGITAL
INFRASTRUCTURE



Otpornost na greške (Fault tolerance)

- Fault tolerance je sposobnost sistema da funkcioniše bez otkaza.
- Postiže se automatskim prebacivanjem na rezervne resurse.
- Sistem nastavlja sa radom i pored pojedinačnih otkaza



Virtuelni Privatni Oblak (VPC)

- VPC je izolovana virtuelna mreža unutar AWS oblaka
- Logički je potpuno odvojena od svih drugih AWS korisnika
- Sami definišete opseg IP adresa (CIDR blok) za vašu mrežu
- Omogućava potpunu kontrolu nad virtuelnim mrežnim okruženjem

CIDR Opseg u AWS-u

- CIDR (Classless Inter-Domain Routing) blok definiše celokupan opseg privatnih IP adresa.
- Prikazuje raspon adresa u Virtuelnom Privatnom Oblaku.
- Primer CIDR notacije je 10.0.0.0/16 u AWS-u.
- Koristi se za logičko razdvajanje mreža i podmreža.

Podmreže (Subnets)

- Podmreže dele ukupan opseg IP adresa vašeg VPC-a.
- Svaka podmreža mora biti u potpunosti smeštena u jednoj AZ.
- Javne i Privatne podmreže se razlikuju po rutiranju.
- Privatne podmreže nemaju direktni pristup internetu.

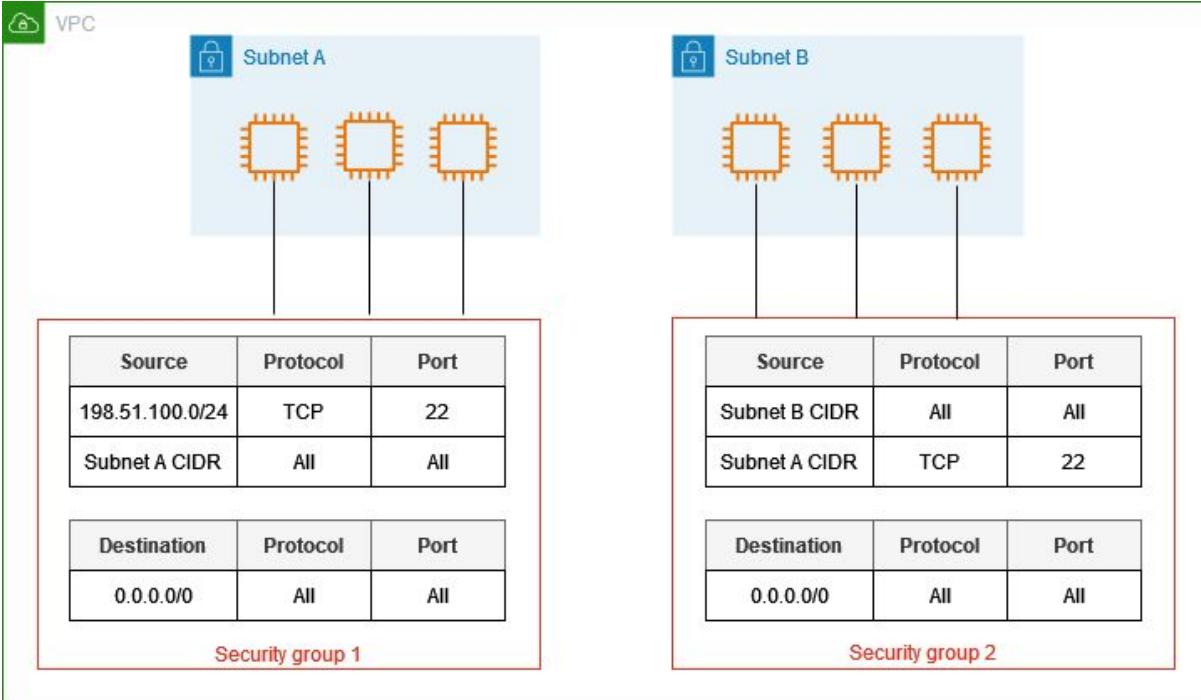
Internet Gateway (IGW) u AWS-u

- Omogućava komunikaciju između VPC-a i Interneta.
- IGW je redundantna komponenta VPC-a sa visokom dostupnošću.
- Podmreža sa rutom ka IGW postaje Javna Podmreža.
- Instancama omogućava direktni pristup javnom Internetu.

Pravila Rutiranja

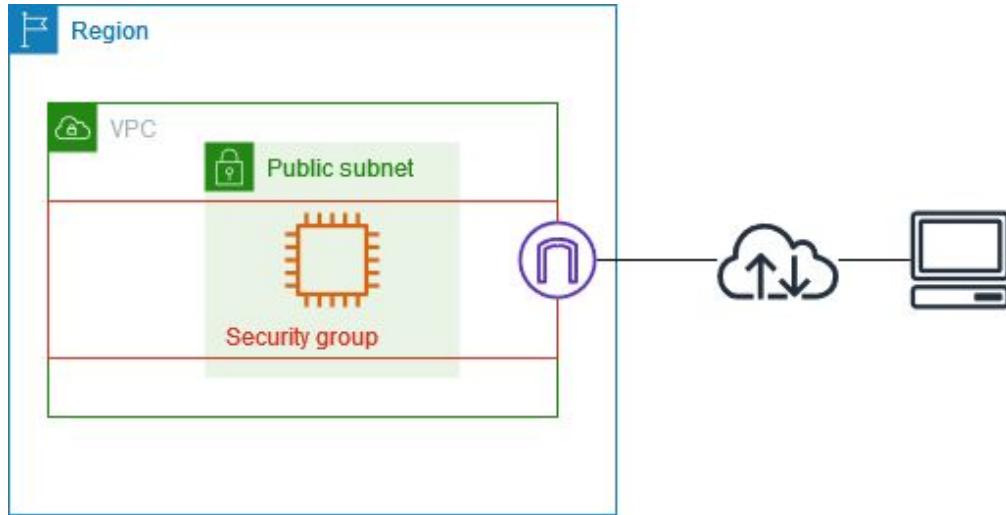
- Skup pravila za usmeravanje mrežnog saobraćaja.
- Određuju gde saobraćaj iz podmreže ide.
- Na primer, saobraćaj ka Internetu ide na IGW.
- Lokalni saobraćaj ostaje unutar vašeg VPC-a.

Mrežna zaštita - arhitektura i zašto?



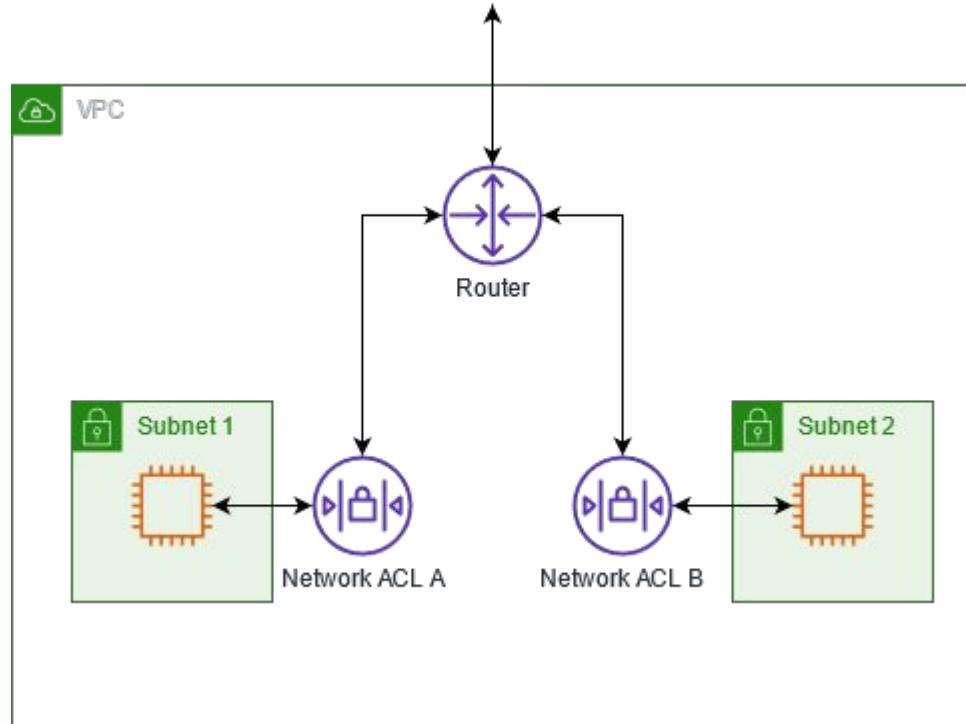
Security grupe - Kako rade?

- Virtuelni zaštitni zid (firewall) za instance
- Kontroliše dolazni i odlazni saobraćaj
- Stateful - Povratni saobraćaj je automatski dozvoljen
- Primenuju se na nivou instance, ne podmreže (subnet)
- Pravila su “allow-only” (samo dozvole)



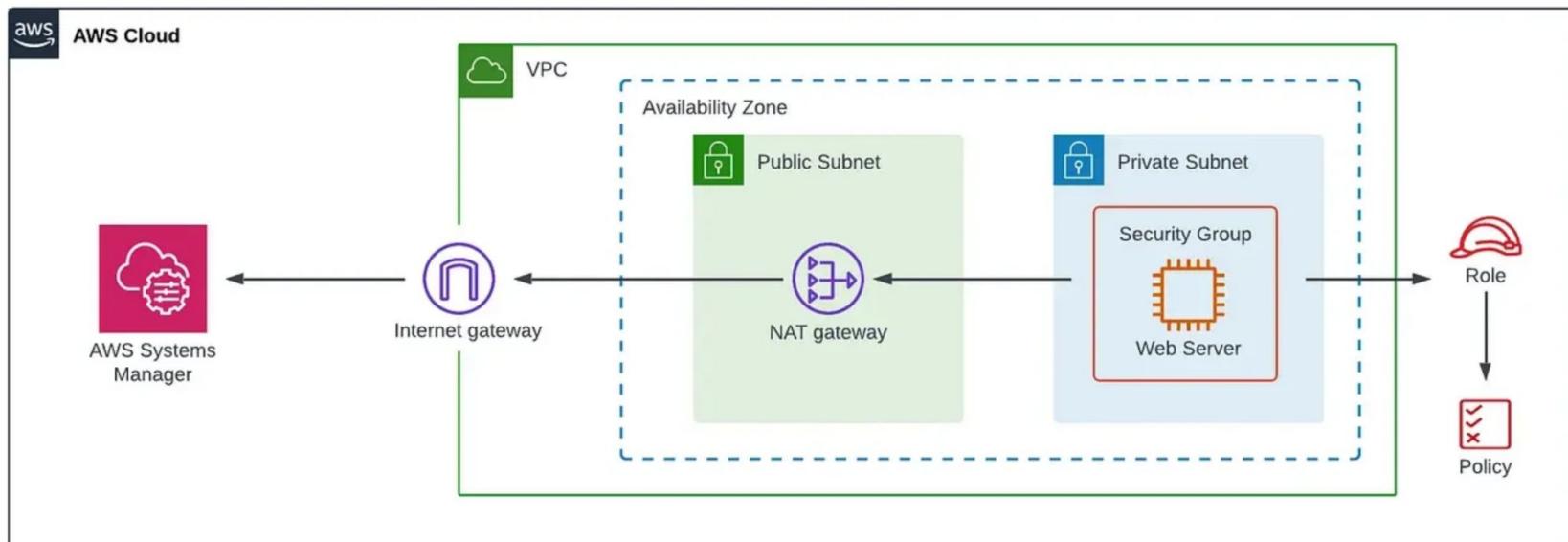
Network Access Control Lists - NACLs

- Stateless, firewall na nivou subnet-a.
- Kontroliše saobraćaj koji ulazi i izlazi iz celog subnet-a.
- Ključna razlika - NACL eksplisitno dozvoljava ili odbija saobraćaj na osnovu pravila.



NAT Gateway

- Omogućavainstancama u privatnom subnet-u da iniciraju odlazne konekcije ka internetu.
- (Primer - ažuriranje softvera)
- Istovremeno sprečava dolazne konekcije sa interneta



PITANJA

