Zbornik radova Fakulteta tehničkih nauka, Novi Sad

UDK: 004.56
DOI: https://doi.org/10.24867/29BE31Gordic

ANALIZA MEHANIZAMA MREŽNE BEZBEDNOSTI NA AWS

ANALYSIS OF NETWORK SECURITY MECHANISMS ON AWS

Nebojša Gordić, *Fakultet tehničkih nauka, Novi Sad*

Oblast – RAČUNARSTVO I AUTOMATIKA

Kratak sadržaj – *Izrada sistema sastavljenog od više aplikacija/servisa sa akcentom na postavljanje istih ua AWS cloud i njihovu zaštitu firewall-om.*

Ključne reči: *Firewall, AWS, Bezbjednost, Cloud, Amazon Web Service, Bezbjednosne grupe*

Abstract – *Creation of a system composed of several applications/services with an emphasis on placing them in the AWS cloud and protecting them with a firewall.*

Keywords: *Firewall, AWS, Security, Cloud, Amazon Web Service, Security Groups*

1. UVOD

U savremenom digitalnom dobu, internet komunikacija je ključna za funkcionisanje poslovnih sistema i aplikacija, omogućena putem internet protokola kao što su TCP/IP. HTTP i HTTPS su osnovni za pregledanje i transfere web sadržaja. Web aplikacije postaju suštinski alati za pružanje usluga globalno, omogućavajući jednostavnu interakciju između korisnika i kompleksnih sistema [1].

Sa porastom upotrebe web aplikacija dolaze i izazovi vezani za bezbijednost i zaštitu osjetljivih podataka. Mrežna bezbijednost, uključujući firewall rješenja, postaje kritična za zaštitu podataka. Firewall djeluje kao prva linija odbrane, kontrolišući mrežni saobraćaj putem bezbjednosnih pravila [2]. Tehnologije firewall-a su se razvile i postale su ključne u cloud okruženjima gdje je potrebna fleksibilna i skalabilna zaštita. Ispravna konfiguracija firewall-a omogućava zaštitu i optimizaciju mrežnog saobraćaja.

Rad se fokusira na analizu konfiguracije i poređenje firewall mogućnosti kod cloud provajdera. Cloud tehnologija je transformisala globalno poslovanje pružajući skalabilnost, fleksibilnost i dostupnost. Sa sve više aplikacija i podataka u cloudu, bezbijednost zauzima centralno mjesto, zahtijevajući inovativne pristupe za zaštitu podataka.

Istraživanje uključuje razvoj minimalne web aplikacije za ilustraciju praktične primjene rješenja. Uključuje analizu sajber bezbijednosti na AWS Cloud-u, razmatra prijetnje poput neovlašćenog upada i DDoS napada, te predlaže firewalle kao rješenje.

NAPOMENA:
Ovaj rad proistekao je iz master rada čiji mentor je bio dr Željko Vuković, docent.

Cilj je pružiti sveobuhvatni uvid u upravljanje bezbjednosnim izazovima cloud provajdera, identifikujući prednosti i izazove u primjeni firewall-a, kako bi razvojni timovi mogli unaprijediti bezbijednost svojih cloud instalacija putem efikasnih strateških smjernica.

2. Izazovi sajber bezbijednosti AWS Cloud i u drugi okruženjima

U savremenom digitalnom okruženju, bezbijednost web aplikacija i infrastrukture je od kritičnog značaja, posebno kod cloud usluga kao što je Amazon Web Services (AWS). Cloud platforme omogućavaju organizacijama postavljanje aplikacija na skalabilnu infrastrukturu, ali donose izazove u osiguravanju zaštite od sajber prijetnji. Web aplikacije u cloudu često su dostupne preko interneta, čineći ih metama za bezbijednosne prijetnje poput DDoS napada, neovlašćenog pristupa, krađe podataka i ubrizgavanja zlonamjernog koda.

Bezbijednosni problemi mogu nastati zbog:

1. Neovlašćenih upada, gdje nedozvoljeni korisnici pokušavaju pristupiti osjetljivim informacijama.
2. DDoS napada, koji preopterećuju sistem i čine ga nedostupnim legitimnim korisnicima.
3. Presretanja i manipulacije podataka, ugrožavajući integritet sistema.
4. Neadekvatnih konfiguracija bezbijednosnih politika.

Rješenje ovih izazova je implementacija robusnih firewall rješenja. AWS kao jedan od vodećih pružalaca cloud usluga [3], uključuje napredne mjere sigurnosti kao što je AWS WAF (Web Application Firewall), koji omogućava definisanje pravila za blokiranje ili dozvoljavanje saobraćaja.

Firewall rješenja pomažu u kontroli i upravljanju saobraćajem prema dinamičkim pravilima, zaštiti od ranjivosti i održavanju integriteta, povjerljivosti i dostupnosti podataka.

3. UPOTREBLJENE TEHNOLOGIJE I ALATI

3.1. Frontend Tehnologija: React

React je popularna biblioteka za izgradnju brzih i interaktivnih korisničkih interfejsa. Kada se koristi sa TypeScript-om, omogućava tipizirani JavaScript, pružajući prednosti kao što je garantovanje tipova, što smanjuje broj grešaka. TSX sintaksa poboljšava rad u timovima, a podrška za TypeScript u IDE-u povećava produktivnost. Virtualni DOM u React-u omogućava brze i efikasne promjene u korisničkom interfejsu.

3.2. Backend Tehnologija: Node.js i Express

Node.js je platforma koja omogućava izvršavanje JavaScript-a na serveru, sa asinhronim I/O što je čini efikasnom za rukovanje brojnim zahtjevima. Express je lagan okvir za upravljanje HTTP zahtjevima, savršen za red aplikacija u realnom vremenu.

3.3. Baza podataka: PostgreSQL i Sequelize

PostgreSQL je odabran zbog svojih naprednih mogućnosti. Sequelize, kao ORM alat, olakšava rad s PostgreSQL kroz objektnu-orijentaciju u JavaScript-u.

3.4. Integracija sa udaljenim servisima

Axios se koristi za slanje HTTP zahtjeva, omogućavajući laku komunikaciju sa eksternim API-jevima poput Trello-a.

3.5. Slanje e-pošte: Nodemailer

Nodemailer, kao jedna od popularnijih biblioteka za slanje e-pošte [4], je korišten za integraciju funkcionalnosti slanja e-pošte, omogućavajući jednostavno slanje različitih formata poruka i dodavanje priloga.

3.6. AWS Servisi

Za hosting aplikacije izabrani su AWS EC2 i AWS Amplify servisi. EC2 pruža skalabilnost u oblaku, dok Amplify pojednostavljuje razvoj i deployment frontenda, omogućavajući brzu integraciju AWS usluga i sigurno hostovanje [5].

4. IMPLEMENTACIJA RADA SA PODACIMA IZ Trello Servisa

4.1. Opis arhitekture aplikacije

Arhitektura sistema zamišljena je kao modularni mikro-servisni sistem koji uključuje napredni frontend interfejs i fleksibilan backend, omogućavajući integraciju sa eksternim platformama kao što je Trello, uz podršku infrastrukture hostovane na AWS-u.

Frontend (React + TypeScript):

React se koristi za kreiranje dinamičnog i intuitivnog korisničkog interfejsa sa jakom tipskom sigurnošću, omogućenom kroz TypeScript. Korisnici mogu upravljati zadacima pomoću interaktivnih komponenti kao što su boards, lists i cards.

Komponente poput AuthService, BoardService i OrganizationService olakšavaju komunikaciju s backendom putem REST API-ja.

Backend (Node.js + Express):

Node.js i Express pružaju strukturu za obradu HTTP(S) zahtjeva koristeći kontrolere (poput AuthController, BoardController) za autentifikaciju i upravljanje podacima. JWT tokeni i AuthMiddleware brinu se za sigurnu autentifikaciju korisnika.

ErrorHandlerMiddleware omogućava centralizovanu obradu grešaka.

Baza podataka (PostgreSQL + Sequelize):

PostgreSQL čuva korisničke podatke i zadatke, dok Sequelize ORM omogućava manipulaciju podacima kroz JavaScript API pozive.

Integracija sa eksternim servisima:

TrelloIntegrationService omogućava sinhronizaciju i upravljanje Trello boardovima u realnom vremenu. Mail Sender servis koristi Nodemailer za automatizaciju slanja e-pošte korisnicima.

AWS Hosting i Skaliranje:

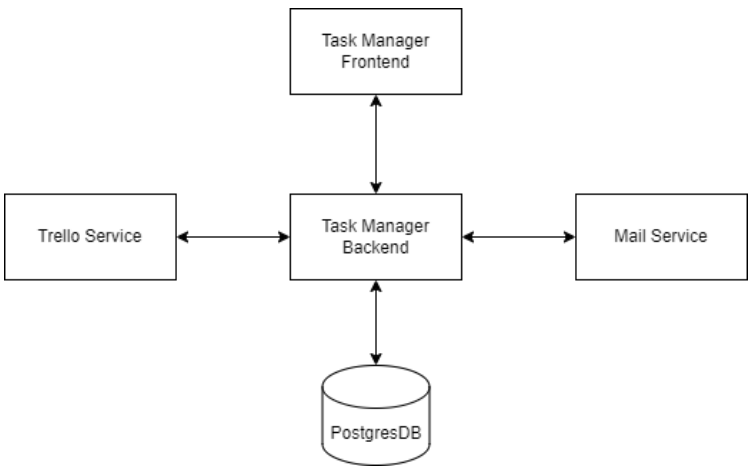
Infrastruktura i usluge:

1. EC2 Instance: Backend aplikacija i baza podataka PostgreSQL hostovani su na EC2 instanci, omogućavajući kontrolu i konfiguraciju servera.
2. AWS Amplify: Frontend aplikacija je hostovana na AWS Amplify-u, što omogućava lako ažuriranje i skalabilnost.

Bezbijednost i upravljanje pristupima:

1. AWS IAM omogućava precizno upravljanje pristupom i definisanje dozvola.
2. AWS Security Groups i Network ACLs djeluju kao virtualni firewal-ovi za kontrolu mrežnog saobraćaja i implementaciju sigurnosnih politika.

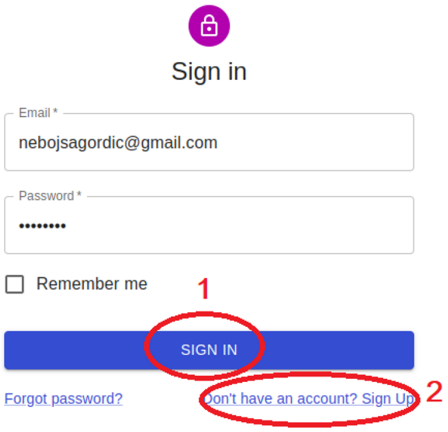
Ova struktura obezbjeđuje bezbjedan i skalabilan rad aplikacije, optimizovano upravljanje resursima i prilagođavanje zahtjevima korisnika.



Slika 1. *Arhitektura aplikacije*

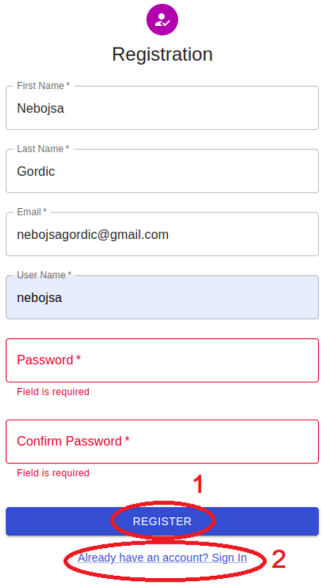
4.2. Opis rada aplikacije

Forntend aplikacija nudi niz mogućnosti.



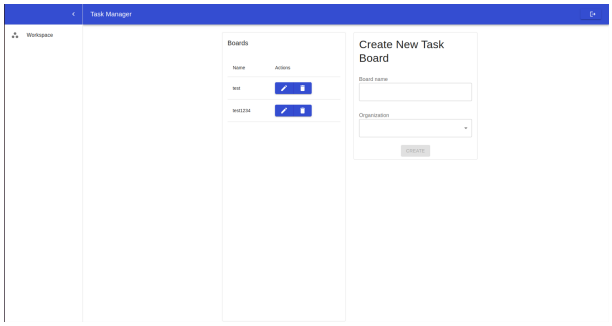
Slika 2. *Forma prijavu korisnika*

Na slici 2 prikazana je početna strana aplikacije sa dugmetom za prijavu u elipsi 1 ili registraciju u elipsi 2.



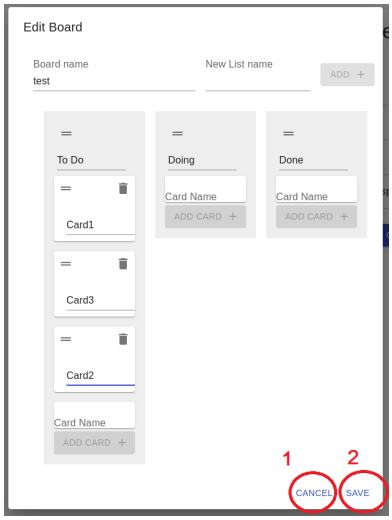
Slika 3. Forma za registraciju korisnika

Na slici 3 se može uočiti forma za registraciju novih kroisnika koja se potvrđuje klikom na dugme u elipsi 1 ili prelazak na prijavu klikom na dugme u elipsi 2.



Slika 4. Radna površina

Nakon prijave korisniku se prikazuje radna površina gdje su izlistan board-ovi koji u sebi sadrže card-ove. Pored toga moguće je pozvati akciju brisanja ili izmjene izlistanih entiteta. Pored toga može se uočiti forma uz pomoć koje je moguće kreirati novi board.



Slika 5. Dialog za pregled izmjenu board-a

Na slici 5 je prikaz otvorenog board-a. U dialogu je moguće preimenovati board, dodavati nove liste za card-ove, brisati ih ili im mijenjati imena. Takođe je omogućeno dodavanje novih card-ova, preimenovanje postojećih ili njihovo prebacivanje iz jedne u drugu listu.

Dugme u elipsi 1 omogućava odustajanje od napravljenih izmjena, dok dugme u elipsi 2 omogućava njihovo čuvanje. Sve napravljene izmjene se prenose na integrisani Trello servis.

5. AWS I BEZBIJEDNOST UPOTREBOM FIREWALL-A

5.1. AWS i njegove osnove

Amazon Web Services (AWS) je sveobuhvatna platforma za cloud computing koju pruža Amazon. AWS nudi širok spektar usluga za računarstvo, skladištenje, baze podataka, analitiku, razvoj aplikacija, mašinsko učenje i još mnogo toga. Omogućava kompanijama i razvojnim timovima brzu skalabilnost i integraciju resursa bez potrebe za održavanjem fizičke infrastrukture.

Ključne komponente AWS-a uključuju:

- EC2 (Elastic Compute Cloud),
- S3 (Simple Storage Service,
- RDS (Relational Database Service),
- Lambda,
- VPC (Virtual Private Cloud),
- DynamoDB,
- IAM (Identity and Access Management).

AWS omogućava organizacijama da povećaju IT infrastrukturu smanjujući troškove i poboljšavajući agilnost, pružajući pouzdanu i stabilnu platformu za razvoj i skaliranje aplikacija.

5.2. Virtual Private Cloud

Virtual Private Cloud (VPC) je AWS usluga koja omogućava kreiranje izolovanog dijela AWS oblaka za pokretanje AWS resursa, poput EC2 instanci. VPC pruža kontrolu nad virtualnim mrežnim okruženjem [6].

Ključne karakteristike VPC-a uključuju:

Izolovani mrežni prostor, konfigurisanje mreže, kontrola pristupa i integracija s lokalnom mrežom.

VPC je osnova za arhitekturu u AWS oblaku, omogućavajući prilagođavanje mrežnog okruženja na osnovu specifikacijskih i bezbijednosnih zahtjeva aplikacije.

5.3. Bezbijednosne grupe

Bezbjednosne grupe u AWS-u služe kao firewall za kontrolu saobraćaja do AWS resursa, kao što su EC2 instance. Ove grupe regulišu koji saobraćaj može pristupiti i koji može napustiti ove resurse. Kada se bezbjednosna grupa poveže sa EC2 instancom, ona upravlja ulaznim i izlaznim saobraćajem za tu instancu. VPC takođe posjeduje podrazumijevanu bezbjednosnu grupu [7].

Bezbjednosna grupa se može dodijeliti samo resursima unutar istog VPC-a, a jedan resurs može imati više grupa. Grupa je stateful, što znači da ako instanca inicira zahtev, odgovor može proći bez obzira na ulazna pravila.

Bezbjednosne grupe ne ograničavaju saobraćaj ka i od Amazon DNS-a, Amazon DHCP-a, EC2 i ECS metadata, ovjera Windows licenci i servisa za sinhronizaciju vremena. Postoje ograničenja u broju grupa unutar VPC-a, broju pravila po grupi i broju grupa na mrežnom interfejsu. Preporučuje se da samo određeni IAM korisnici mogu mijenjati grupe. Treba ograničiti pristup preko specifičnih TCP portova i izbjegavati korištenje velikog broja portova u grupi radi smanjenja rizika od napada.

5.4. Access Controll Lists

Mrežna kontrola pristupa (ACL) omogućava ili odbija određeni ulazni ili izlazni saobraćaj na nivou podsistema. U VPC-u se može koristiti podrazumijevana mrežna ACL ili se može kreirati prilagođena mrežna ACL koja sadrži pravila slična onima u bezbjednosnim grupama.

Jedna ACL se može povezati s više podsistema, ali jedan podsistem može imati samo jednu ACL. Sve ACL liste sastoje se od numerisanih pravila od 1 do 32766, koja se primjenjuju redom. Nova pravila je preporučljivo numerisati s velikim razmacima. Mrežne ACL nisu stateful, što znači da ne pamte prethodne zahtjeve – ako je ulazni saobraćaj dozvoljen, izlazni nije dozvoljen automatski. Mrežne ACL ne mogu blokirati DNS zahtjeve ka ili od Route 53 Resolver-a, niti saobraćaj ka IMDS. Takođe, ne filtriraju saobraćaj od: Amazon EC2 metadata, DHCP, Amazon ECS task metadata, aktivacija Windows licenci, Amazon servisa za sinhronizaciju vremena, i rezervisanih IP adresa podrazumijevanog VPC rutera [8].

5.5. AWS Network Firewall

AWS Network Firewall (ANF) korisnicima nudi deep packet inspection (DPI), mogućnost detekcije aplikativnih protokola, filtriranje domena i sistem za sprječavanje upada (IPS). ANF pruža stateful i stateless mehanizme za upravljanje pravilima saobraćaja unutar VPC-a, omogućavajući inspekciju saobraćaja u svim pravcima sa podrškom za hiljade pravila. Korisnici mogu usmjeriti dolazni saobraćaj ka ANF krajnjoj tački, sa ANF smještenim u namjenskoj podmreži unutar VPC-a. ANF koristi AWS Gateway Load Balancer za raspoređivanje opterećenja i ulazno rutiranje VPC-a radi sveobuhvatne kontrole saobraćaja.

Podržani modeli primjene uključuju: Distribuirani model, Centralizovani model i Kombinovani model, a modeli se razlikuju od raspoređivanja u VPC [9].

6. ZAKLJUČAK

Tokom izrade ovog rada, istražena su i implementirana tehnološka rješenja za efikasno i sigurno upravljanje digitalnim resursima i aplikacijama. Razvijena aplikacija za upravljanje zadacima koristi AWS infrastrukturu za skalabilnost i pouzdanost, omogućavajući integraciju s eksternim servisima kao što je Trello.

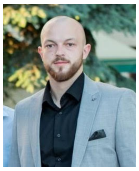
Poseban akcenat stavljen je na bezbjednosne aspekte. Kao virtualni firewall-i, Security Groups omogućile su precizno definisanje ulaznih i izlaznih pravila, kritično za siguran i pouzdan prenos podataka. Ovaj bezbjednosni sloj kontroliše pristup EC2 instancama, minimizirajući rizike od neovlašćenog pristupa i ugrožavanja podataka.

Konfiguracija Security Groups bila je fokusirana na dozvoljavanje samo neophodnih protokola i portova, održavajući visoku bezbjednost bez ugrožavanja funkcionalnosti aplikacije. Tako je omogućen siguran prenos podataka između komponenti aplikacije i eksternih servisa. Dodatno, korištenje Security Groups omogućilo je primjenu promjena u bezbjednosnim pravilima u realnom vremenu bez prekida rada sistema. Rad demonstrira snagu AWS inovacija u razvoju aplikacija, ističući skalabilnost i integraciju kao čvrstu osnovu za razvoj sigurnih i robusnih aplikacija u oblaku. Očekuje se da će buduća istraživanja nastaviti unapređivanje bezbjednosnih i funkcionalnih aspekata razvoja u cloud computingu, doprinoseći boljoj zaštiti podataka i digitalnih resursa.

7. LITERATURA

[1] Walter Goralski, *The illustrated network: how TCP/IP works in modern network*
[2] Macfarlane, Richard; Buchanan, William, Ekonomou, Elias; Uthmani, Omari; Fan, Lu; Lo, Owen (2012). *Formal security policy implementations in network firewalls*
[3] Gartner, *Gartner Magic Quadrant for Cloud Infrastructure and Platform Services*
[4] NPM, *Nodemailer Download Statistics*
[5] AWS Documentation, *AWS services by Category*
[6] AWS Documentation, *Amazon VPC*
[7] AWS Documentation, Security Groups
[8] AWS Documentation, *Network ACL*
[9] AWS Documentation, *AWS Network Firewall*

Kratka biografija:



Nebojša Gordić rođen je u Sokocu, BiH 1999. god. Diplomski rad na Fakultetu tehničkih nauka iz oblasti Elektrotehnike i računarstva – Izazovi u vizuelizaciji pozicija i stanja malih elektrana odbranio je 2022.god. kontakt: nebojsagordic@gmail.com