Ministerul Educaţiei, Culturii și Cercetării

Universitatea Tehnică a Moldovei

Faculatea Calculatoare, informatică și microelectronică  
Departamentul Ingineria Software și Automatică



**RAPORT**

Lucrare de Laborator nr.2

Disciplina: Analiza și Specificarea Cerințelor Software

Tema : **Analiza cerințelor**

A efectuat:

st. gr. SI-211 Chirita S.

A verificat:

asist. univ. Tocan A.

Chişinău 2024

Cuprins

[Introducere 1](#_Toc184072304)

[1. Descriere generală 3](#_Toc184072305)

[2. Colectarea cerintelor 5](#_Toc184072306)

[2.1. Cerințe funcționale și nefuncționale 6](#_Toc184072307)

[3. Analiza cerintelor 7](#_Toc184072308)

[3.1 Analiza Cerințelor Funcționale 7](#_Toc184072309)

[3.2 Analiza Cerințelor Nefuncționale 8](#_Toc184072310)

[4. Documentarea cerințelor colectate 10](#_Toc184072311)

[4.1 Descriere generală 10](#_Toc184072312)

[4.2 Cerințe de interfață externă 10](#_Toc184072313)

[4.3 Caracteristica sistemului de gestionare a vânzărilor și a recomandărilor 12](#_Toc184072314)

[4.3.1 Descriere și prioritate 12](#_Toc184072315)

[4.3.2 Acțiune/Rezultat 13](#_Toc184072316)

[4.3.3 Cerințe funcționale 13](#_Toc184072317)

[4.3.4 Cerințe de performanță 14](#_Toc184072318)

[4.3.5 Cerințe de securitate 14](#_Toc184072319)

# Introducere

Proiectul se axează pe dezvoltarea unui sistem integrat pentru interceptarea și analiza traficului de rețea, având ca scop principal monitorizarea și detectarea activităților suspecte, precum și evaluarea performanței rețelelor. Acest sistem va permite utilizatorilor să capteze pachetele de date, să analizeze conținutul acestora și să genereze rapoarte utile pentru luarea deciziilor bazate pe date.

Utilizatorii principali ai sistemului includ administratori de rețea, analiști de securitate cibernetică și specialiști în performanța rețelelor. Sistemul va asigura o interfață intuitivă și funcționalități avansate pentru a facilita monitorizarea traficului în timp real, identificarea amenințărilor și analiza metricilor esențiale ale rețelei.

Un alt obiectiv cheie este automatizarea proceselor de detectare a anomaliilor prin implementarea unor algoritmi bazați pe reguli sau învățare automată. Acești algoritmi vor permite identificarea rapidă a traficului neobișnuit, a potențialelor atacuri de tip DDoS, a accesului neautorizat sau a altor activități malițioase, reducând timpul de răspuns la incidentele de securitate. În plus, sistemul va oferi posibilitatea integrării cu alte soluții de management al rețelelor, precum firewall-uri și sisteme de detecție a intruziunilor (IDS).

Prin implementarea unui mecanism de vizualizare grafică a datelor, utilizatorii vor putea urmări în timp real tendințele traficului de rețea, distribuția protocoalelor utilizate și comportamentul diferitelor noduri din rețea. Acest lucru va permite o mai bună înțelegere a performanței infrastructurii și va facilita luarea de decizii strategice pentru optimizarea acesteia.

În contextul actual, în care volumul de trafic și complexitatea rețelelor cresc exponențial, un astfel de sistem devine esențial pentru a menține securitatea și stabilitatea infrastructurilor IT. Proiectul își propune să adreseze aceste provocări printr-o soluție scalabilă, robustă și ușor de utilizat, care să poată fi adaptată nevoilor specifice ale utilizatorilor finali.

Sistemul nu doar că va contribui la îmbunătățirea securității cibernetice, ci și la eficientizarea managementului rețelei prin reducerea costurilor operaționale și optimizarea utilizării resurselor hardware și software. Astfel, proiectul reprezintă un pas important spre dezvoltarea unor soluții integrate care să răspundă cerințelor moderne de securitate și performanță în domeniul IT.

# 

# Descriere generală

Proiectul **„Sistem integrat pentru interceptarea și analiza traficului de rețea”** își propune să dezvolte o soluție software capabilă să monitorizeze traficul dintr-o rețea în timp real, să analizeze datele colectate și să genereze rapoarte detaliate, contribuind astfel la o mai bună înțelegere a performanței rețelei și la îmbunătățirea securității acesteia. Sistemul va oferi o gamă largă de funcționalități esențiale pentru organizațiile moderne care doresc să-și optimizeze infrastructura IT și să răspundă rapid la amenințările de securitate cibernetică.

Proiectul vizează dezvoltarea unui sistem robust și scalabil, care să răspundă cerințelor variate ale utilizatorilor. Acesta va permite colectarea și prelucrarea pachetelor de date din rețea, utilizând tehnologii avansate pentru analiza protocoalelor și identificarea anomaliilor. În contextul amenințărilor cibernetice tot mai sofisticate și al creșterii exponențiale a traficului de date, un astfel de sistem devine o necesitate pentru organizațiile care doresc să-și protejeze datele și să asigure funcționarea eficientă a rețelelor.

Sistemul va fi utilizat de administratori de rețea, analiști de securitate și manageri IT, fiecare având acces la funcționalități adaptate nevoilor lor specifice. Administratorii de rețea vor putea monitoriza traficul în timp real, identificând rapid problemele care afectează performanța. Analiștii de securitate vor folosi sistemul pentru detectarea și investigarea activităților suspecte, prevenind potențiale incidente cibernetice. Managerii IT vor avea acces la rapoarte sumare care le permit să evalueze performanța generală a rețelei și să ia decizii strategice pentru optimizarea acesteia.

Un element central al proiectului îl reprezintă componenta de analiză a traficului. Sistemul va fi capabil să decodeze pachetele de date, să extragă informații relevante despre protocoale și să identifice traficul anormal. Aceasta include detectarea atacurilor de tip DDoS, a încercărilor de acces neautorizat sau a altor activități malițioase. În plus, algoritmii utilizați vor putea învăța și adapta în timp, îmbunătățind continuu acuratețea analizei și reducând alarmele false.

Pe lângă securitate, sistemul se concentrează pe optimizarea performanței rețelei. Prin analiza detaliată a traficului, utilizatorii vor putea identifica punctele de congestie, vor înțelege tiparele de utilizare și vor lua măsuri pentru a îmbunătăți viteza și fiabilitatea conexiunilor. Integrarea cu alte soluții, cum ar fi firewall-uri sau sisteme de detecție a intruziunilor (IDS), va permite crearea unei infrastructuri IT mai robuste și mai bine protejate.

Soluția va include și un sistem avansat de raportare, care va permite utilizatorilor să genereze rapoarte personalizate în funcție de nevoile lor. Aceste rapoarte vor putea fi utilizate pentru a demonstra conformitatea cu reglementările, pentru a evalua performanța rețelei sau pentru a lua decizii informate cu privire la investițiile viitoare în infrastructură.

În ceea ce privește designul, sistemul va fi construit pe o arhitectură modulară, care să permită extinderea și personalizarea funcționalităților în funcție de cerințele utilizatorilor. Acesta va fi compatibil cu protocoalele și standardele de rețea existente, asigurând astfel o integrare ușoară în infrastructurile IT deja implementate. De asemenea, sistemul va include o interfață intuitivă, care să permită utilizatorilor să navigheze și să acceseze rapid informațiile relevante.

Un alt aspect important al proiectului este asigurarea confidențialității datelor. Sistemul va respecta reglementările legale în vigoare și va implementa mecanisme de securitate avansate pentru protejarea informațiilor colectate. Aceste măsuri includ criptarea datelor în timpul transmisiei, autentificarea utilizatorilor și gestionarea atentă a accesului la informații.

# Colectarea cerintelor

Colectarea cerințelor este un pas esențial în dezvoltarea unui sistem integrat pentru interceptarea și analiza traficului de rețea, având în vedere complexitatea interacțiunii dintre componentele tehnice și utilizatorii acestuia. Procesul urmărește să identifice și să definească clar obiectivele și funcționalitățile sistemului, garantând astfel că produsul final satisface nevoile utilizatorilor și cerințele organizaționale. O colectare corectă a cerințelor permite dezvoltatorilor să creeze o soluție funcțională, scalabilă și eficientă, care să îndeplinească atât cerințele tehnice, cât și cele operaționale.

Sistemul va deservi diverse categorii de utilizatori, inclusiv administratori de rețea, analiști de securitate și manageri IT. Fiecare categorie are nevoi specifice care trebuie luate în considerare. De exemplu, administratorii de rețea vor necesita acces la funcționalități pentru monitorizarea traficului în timp real, în timp ce analiștii de securitate vor avea nevoie de instrumente avansate pentru detectarea anomaliilor și generarea rapoartelor detaliate. Prin definirea clară a acestor cerințe, echipa de dezvoltare poate asigura funcționalități personalizate și intuitive pentru fiecare tip de utilizator.

Colectarea cerințelor este esențială și pentru stabilirea funcționalităților legate de analiza traficului. Sistemul trebuie să fie capabil să intercepteze pachete de date din rețea, să analizeze conținutul acestora și să genereze alerte în cazul detectării unor activități suspecte. Pentru a realiza acest lucru, sunt necesare cerințe detaliate privind protocoalele acceptate, volumul de trafic ce poate fi procesat simultan și integrarea cu alte soluții de securitate. Acest proces contribuie la clarificarea nevoilor tehnice și la definirea standardelor de performanță.

În plus, colectarea cerințelor asigură că toate fluxurile de informații sunt gestionate eficient și securizat. Într-un context în care traficul de rețea poate conține date sensibile, este vital ca sistemul să respecte reglementările legale și să implementeze măsuri robuste de protecție a datelor. Acest aspect este crucial pentru prevenirea breșelor de securitate și pentru asigurarea conformității cu normele privind protecția informațiilor.

Un alt aspect important al colectării cerințelor este definirea clară a obiectivelor legate de performanță. Sistemul trebuie să fie capabil să gestioneze volume mari de date, mai ales în perioade de activitate intensă, cum ar fi atacuri de tip DDoS sau monitorizarea rețelelor cu trafic ridicat. Stabilirea unor standarde clare de performanță ajută la proiectarea unui sistem care să răspundă rapid și precis cerințelor utilizatorilor.

Prin colectarea adecvată a cerințelor, se asigură crearea unui sistem care răspunde nevoilor organizaționale și utilizatorilor, contribuind la creșterea securității cibernetice, optimizarea infrastructurii IT și îmbunătățirea procesului decizional. Această etapă reprezintă fundația pentru proiectarea și dezvoltarea unei soluții robuste, scalabile și eficiente.

## 2.1. Cerințe funcționale și nefuncționale

Obiectivele propuse pentru dezvoltarea sistemului includ atât cerințe funcționale, care definesc ce trebuie să facă sistemul, cât și cerințe nefuncționale, care asigură un standard ridicat de performanță, securitate și scalabilitate.

**Cerințe funcționale identificate:**

* Sistemul va intercepta și captura pachete de date din rețea utilizând protocoale standard precum TCP, UDP, HTTP și DNS.
* Va analiza conținutul pachetelor pentru a identifica tiparele de trafic, protocoalele utilizate și comportamentele anormale.
* Sistemul va genera alerte automate în cazul detectării unor anomalii sau amenințări, cum ar fi atacuri de tip DDoS, acces neautorizat sau tentative de exfiltrare de date.
* Utilizatorii vor putea genera rapoarte detaliate despre traficul de rețea, incluzând distribuția protocoalelor, sursele traficului și activitățile suspecte.
* Sistemul va oferi o interfață grafică pentru monitorizarea traficului în timp real, incluzând vizualizări grafice ale volumului de trafic și indicatorilor de performanță.
* Va include funcționalități de filtrare și căutare pentru a permite utilizatorilor să analizeze segmente specifice de trafic.
* Integrarea cu alte sisteme de securitate, cum ar fi firewall-uri și IDS/IPS, pentru a extinde capabilitățile de protecție.

**Cerințe nefuncționale identificate:**

* Sistemul va asigura protecția datelor colectate prin mecanisme de criptare în timpul transmisiei și stocării.
* Va fi proiectat pentru a procesa volume mari de trafic în timp real, garantând un timp de răspuns sub 2 secunde pentru majoritatea cerințelor de analiză.
* Sistemul va avea o arhitectură modulară, permițând extinderea facilă a funcționalităților și adaptarea la cerințele în schimbare.
* Disponibilitatea sistemului va fi ridicată, cu măsuri de redundanță și backup pentru a asigura continuitatea operațiunilor în cazul unor defecțiuni.
* Sistemul va fi compatibil cu platforme și tehnologii externe, precum baze de date și API-uri, pentru integrarea facilă în infrastructurile IT existente.
* Interfața utilizatorului va fi intuitivă și prietenoasă, reducând timpul necesar instruirii utilizatorilor și creând o experiență plăcută.

Aceste cerințe stabilesc o bază solidă pentru proiectarea și dezvoltarea sistemului, garantând atât funcționalitatea esențială, cât și un nivel înalt de performanță și fiabilitate.

# Analiza cerintelor

## 3.1 Analiza Cerințelor Funcționale

Cerințele funcționale sunt esențiale pentru sistemele de interceptare și analiză a traficului de rețea pentru a asigura colectarea, organizarea și interpretarea datelor de rețea, oferind utilizatorilor informații clare și utile privind activitatea rețelei și posibilele amenințări.

Sistemul va colecta automat pachetele de trafic din rețeaua monitorizată, provenind de la surse multiple, precum routere, servere, dispozitive de terminal, și aplicații. Această centralizare automată a datelor va permite analiza eficientă a fluxurilor de trafic în timp real și pe perioade istorice. Sistemul va include tehnologii de stocare de date scalabile (ex. PostgreSQL pentru stocarea de jurnale de trafic sau baze de date NoSQL pentru date nestructurate), și API-uri de integrare cu echipamentele de rețea și aplicațiile de monitorizare existente.

**Generarea automată de rapoarte**

Sistemul va permite generarea automată de rapoarte detaliate care vor oferi informații despre traficul de rețea, identificând tiparele de utilizare, fluxurile de trafic suspecte și performanțele rețelei. Aceste rapoarte vor prezenta date legate de pachetele de date capturate, analiza bandelor de frecvență, starea conexiunilor și vor permite utilizatorilor să detecteze anomalii în trafic, cum ar fi atacuri DDoS sau comunicări neautorizate. Rapoartele vor putea fi generate pentru perioade personalizabile (zi, săptămână, lună).

**Interfață grafică interactivă**

Pentru a vizualiza datele în timp real și pentru a urmări evoluțiile traficului de rețea, sistemul va include o interfață grafică interactivă. Aceasta va oferi utilizatorilor posibilitatea de a urmări fluxurile de trafic în timp real, de a vizualiza statistici privind utilizarea lățimii de bandă, și de a detecta traficul suspect. Interfața poate fi construită folosind tehnologii frontend moderne, cum ar fi **Angular** sau **React**, și va fi optimizată pentru diverse dispozitive (desktop, mobil, tabletă), astfel încât utilizatorii să poată monitoriza traficul de oriunde.

**Notificări automate**

În cazul în care sistemul detectează modificări semnificative în trafic, cum ar fi creșteri neobișnuite ale volumului de date sau tentative de acces neautorizat, sistemul va trimite notificări automate utilizatorilor. Aceste notificări vor include detalii despre sursa și destinația pachetelor suspecte, timpul în care a avut loc activitatea, și recomandări pentru măsuri de intervenție.

**Analiza comportamentului de rețea**

Sistemul va include un modul de analiză a comportamentului de rețea, care va studia tiparele de trafic și va ajuta la identificarea comportamentului anormal, ce poate indica un atac sau o vulnerabilitate. În acest context, vor fi oferite sugestii automate pentru optimizarea rețelei și măsuri de protecție suplimentare. De asemenea, se vor include rapoarte pe categorii de rețea pentru a ajuta administratorii să facă ajustări strategice.

**Gestionarea utilizatorilor și a accesului**

În funcție de roluri (administrator de rețea, analist de securitate, manager de infrastructură), sistemul va permite gestionarea accesului la diferite funcționalități. Acest lucru va asigura că numai utilizatorii autorizați au acces la date sensibile, precum datele de trafic criptate sau parametrii rețelei critici. Sistemul va implementa autentificare multi-factor și politici de control al accesului bazate pe roluri (RBAC).

**Accesibilitate și compatibilitate**

Sistemul va putea fi accesat de pe o gamă largă de dispozitive, inclusiv servere, terminale și echipamente mobile, facilitând monitorizarea continuă a rețelei. Arhitectura sistemului va fi compatibilă cu diverse platforme și va permite integrarea cu diverse echipamente hardware și aplicații de gestionare a rețelei.

## 3.2 Analiza Cerințelor Nefuncționale

Sistemul integrat pentru interceptarea și analiza traficului de rețea va include mecanisme avansate de securitate, cum ar fi autentificarea și autorizarea utilizatorilor, pentru a proteja datele sensibile și a preveni accesul neautorizat. Comunicarea între componentele sistemului va fi criptată prin protocoale de securitate precum SSL/TLS, asigurând confidențialitatea și integritatea datelor pe parcursul transferului. Acest lucru este esențial pentru protejarea informațiilor sensibile, cum ar fi datele despre traficul de rețea și configurațiile echipamentelor de rețea.

În ceea ce privește performanța, sistemul va trebui să fie capabil să proceseze volume mari de date în timp real. Acesta va utiliza soluții avansate de procesare și stocare a datelor, cum ar fi baze de date optimizate și arhitecturi scalabile, pentru a analiza fluxurile de trafic fără a afecta viteza de reacție. Implementarea unor soluții de caching și utilizarea arhitecturii microserviciilor vor contribui la reducerea întârzierilor și la asigurarea unui răspuns rapid în fața cerințelor de analiză și interceptare a traficului.

Sistemul va fi proiectat astfel încât să asigure disponibilitate ridicată și continuitatea operațiunilor. Măsuri de redundanță și backup vor fi implementate pentru a proteja datele critice și a asigura restaurarea rapidă a serviciilor în caz de defecțiuni sau erori semnificative. Astfel, sistemul va fi capabil să facă față unor întreruperi sau pierderi de date, minimizând impactul asupra operațiunilor de monitorizare și analiză a traficului.

Pentru a răspunde cerințelor în continuă schimbare ale rețelelor moderne, sistemul va fi scalabil, utilizând tehnologii precum Docker și Kubernetes pentru a adăuga noi resurse și a ajusta capacitatea procesării în mod dinamic. Acesta va permite extinderea rapidă a infrastructurii fără a compromite performanța, garantând o scalabilitate care să țină pasul cu creșterea constantă a volumului de trafic de rețea.

Sistemul va fi integrabil cu diverse soluții externe de securitate și monitorizare a rețelei, cum ar fi platformele de management al traficului sau soluțiile de analiză a comportamentului rețelei, pentru a îmbunătăți procesul de interceptare și detectare a anomaliilor. Integrarea cu aceste platforme va asigura o colectare mai eficientă a datelor și o analiză mai rapidă a evenimentelor de securitate.

În ceea ce privește interfața utilizatorului, aceasta va fi simplă și intuitivă, permițând monitorizarea și analiza traficului de rețea într-un mod eficient. Designul va fi centrat pe utilizator, astfel încât acesta să poată naviga ușor prin diferitele opțiuni și funcționalități ale sistemului, iar informațiile vor fi prezentate într-un mod clar și accesibil. Indiferent de dispozitivul utilizat, interfața va asigura o experiență de utilizator uniformă pe toate platformele.

# Documentarea cerințelor colectate

## 4.1 Descriere generală

Sistemul **„Sistem integrat pentru interceptarea și analiza traficului de rețea”** este conceput pentru a sprijini organizațiile în monitorizarea, analiza și raportarea traficului de rețea într-un mod eficient și scalabil. Acesta oferă funcționalități avansate pentru capturarea pachetelor de date, analiza comportamentului rețelei și identificarea activităților suspecte sau a anomaliilor. Scopul principal al sistemului este să crească securitatea și performanța rețelelor prin furnizarea de informații detaliate și relevante pentru utilizatorii săi.

Sistemul permite monitorizarea în timp real a traficului de rețea și generarea de rapoarte detaliate privind activitatea rețelei. Utilizatorii pot analiza istoricul traficului, pot identifica tendințele de utilizare și pot detecta evenimente neobișnuite. Aceste informații permit utilizatorilor să ia decizii informate, să optimizeze infrastructura rețelei și să răspundă prompt la potențiale amenințări de securitate.

Experiența de utilizare a sistemului este esențială pentru eficiența sa. Interfața grafică a fost proiectată pentru a fi intuitivă și accesibilă, fiind compatibilă atât cu dispozitive desktop, cât și cu dispozitive mobile. Utilizatorii, indiferent de nivelul lor de expertiză tehnică, vor putea accesa rapid informațiile relevante, ceea ce contribuie la crearea unei experiențe de utilizare simplă și eficientă, fără necesitatea unei pregătiri extinse.

Sistemul va funcționa continuu, asigurând o disponibilitate ridicată, 24/7. Timpul maxim de nefuncționare planificat nu va depăși o oră pe lună, iar în cazul unei defecțiuni, recuperarea va fi efectuată în cel mult 30 de minute, prevenind pierderile de date și asigurând continuitatea operațiunilor critice. Acest nivel de disponibilitate este esențial pentru monitorizarea eficientă și analiza traficului de rețea.

Scalabilitatea este o caracteristică de bază a sistemului, permițându-i să gestioneze volume mari de trafic și un număr tot mai mare de utilizatori fără a compromite performanța. Arhitectura modulară a sistemului va permite extinderea funcționalităților în funcție de cerințele organizațiilor și de creșterea infrastructurii rețelei.

Sistemul este structurat în două componente principale:

* **Sistemul de interceptare și analiză a traficului de rețea** – va capta pachetele de date din rețea, va analiza traficul pentru a identifica anomaliile și va genera rapoarte și alerte personalizate.
* **Sistemul de gestionare a datelor colectate** – se va ocupa de stocarea și procesarea sigură a datelor, asigurând acces rapid și securizat la informații istorice și curente.

Aceste componente colaborează pentru a oferi o soluție completă și robustă, adaptată nevoilor specifice ale utilizatorilor și cerințelor din domeniul securității rețelelor.

## 4.2 Cerințe de interfață externă

Pentru a facilita interacțiunea eficientă dintre utilizatori, componente hardware și software, **sistemul integrat pentru interceptarea și analiza traficului de rețea** va include o serie de interfețe externe esențiale. Aceste interfețe sunt fundamentale pentru a asigura comunicarea fluidă între toate modulele sistemului și pentru a permite utilizatorilor să acceseze și să utilizeze funcționalitățile oferite.

Interfața utilizatorului va fi proiectată pentru a permite acces facil și eficient la funcționalitățile sistemului. Interfața grafică va include pagini dedicate pentru autentificare, vizualizarea traficului în timp real, analiza detaliată a pachetelor și gestionarea alertelor. Secțiunea de autentificare va asigura acces diferențiat pe baza rolurilor utilizatorilor, cum ar fi administratori de rețea, analiști de securitate sau manageri IT.

Utilizatorii vor beneficia de o experiență consistentă și optimizată atât pe dispozitive desktop, cât și pe dispozitive mobile, permițând accesul de oriunde și oricând. Interfața va fi proiectată pentru a prezenta informații complexe într-un mod vizual atractiv, incluzând grafice, diagrame și rapoarte detaliate pentru monitorizarea traficului și identificarea anomaliilor.

Sistemul nu necesită hardware specializat, fiind conceput pentru a rula pe infrastructuri comune, compatibile cu servere Linux. Capturarea pachetelor va fi realizată prin integrarea cu plăci de rețea standard, utilizând librării precum **libpcap** sau **WinPcap**. Acest lucru asigură o compatibilitate largă și permite implementarea sistemului pe echipamente convenționale fără necesitatea achiziționării de hardware suplimentar.

Pentru stocarea și gestionarea datelor colectate, sistemul va utiliza o bază de date relațională, precum **PostgreSQL**, capabilă să gestioneze volume mari de informații despre pachete, utilizatori și evenimente detectate. Această bază de date va fi integrată direct cu partea de analiză și raportare, asigurând acces rapid și securizat la date istorice și curente.

Comunicarea dintre interfața client și server va fi realizată prin intermediul API-urilor REST, care oferă un mod standardizat și scalabil de transfer al datelor. Aceste API-uri vor permite interacțiunea cu serverul pentru colectarea datelor, configurarea alertelor și generarea de rapoarte. Protocolul **HTTP/HTTPS** va fi utilizat pentru transmiterea datelor, asigurând securitatea informațiilor sensibile prin criptare în cazul conexiunilor HTTPS.

Pe partea de comunicație, sistemul va suporta protocoale precum **SNMP**, pentru monitorizarea dispozitivelor de rețea, și **NetFlow**, pentru colectarea de date statistice despre traficul din rețea. Aceste protocoale vor permite o integrare ușoară cu infrastructura IT existentă, oferind informații detaliate despre performanța rețelei și comportamentul utilizatorilor.

Prin integrarea coerentă a acestor interfețe hardware și software, sistemul va asigura o funcționare optimă și o experiență sigură și eficientă pentru utilizatori. Această combinație de interfețe va permite utilizatorilor să monitorizeze și să analizeze traficul rețelei într-un mod detaliat și accesibil, contribuind la o mai bună înțelegere și gestionare a infrastructurii IT.

## 4.3 Caracteristica sistemului de gestionare a vânzărilor și a recomandărilor

### 4.3.1 Descriere și prioritate

Scopul sistemului de gestionare a vânzărilor și a recomandărilor este de a colecta, analiza și furniza informații esențiale despre traficul de rețea interceptat și analizat, pentru a oferi recomandări privind îmbunătățirea securității și performanței rețelei. Acesta va ajuta echipele IT și administratorii de rețea să identifice vulnerabilitățile și anomaliile, sugerând acțiuni pentru optimizarea infrastructurii de rețea și a politicii de securitate.

Sistemul va permite monitorizarea în timp real a traficului de rețea, analizând fluxurile de date pentru a detecta activități suspecte sau comportamente neobișnuite. În baza acestor analize, sistemul va genera recomandări pentru îmbunătățirea performanței rețelei și securizarea acesteia, precum și pentru prevenirea atacurilor cibernetice. Aceste recomandări vor fi personalizate în funcție de comportamentul specific al rețelei și de modelele identificate.

Principalele funcționalități ale sistemului includ:

* **Colectarea și analiza traficului**: Sistemul va monitoriza fluxurile de date în timp real și va analiza pachetele de date pentru a detecta anomalii sau activități suspecte, cum ar fi tentative de atac DDoS, malware sau acces neautorizat.
* **Generarea de recomandări**: Pe baza datelor colectate, sistemul va oferi recomandări pentru îmbunătățirea securității și performanței rețelei, cum ar fi ajustarea setărilor de firewall, implementarea de filtre mai stricte sau actualizarea protocoalelor de securitate.
* **Notificări în timp real**: Sistemul va trimite notificări și alerte imediat ce o anomalie este detectată, permițând echipei IT să intervină rapid și să ia măsuri corective.
* **Vizualizarea datelor și rapoarte**: Interfața va permite generarea de rapoarte detaliate, vizualizând analizele traficului și recomandările de îmbunătățire, într-o manieră ușor de înțeles și accesibilă pentru utilizatori cu diferite niveluri de expertiză.

Securitatea este un aspect crucial al acestui sistem. Datele colectate vor fi procesate și stocate în mod securizat, utilizând criptarea pentru a preveni accesul neautorizat și pentru a asigura confidențialitatea informațiilor sensibile. Sistemul va fi capabil să gestioneze volume mari de date fără a afecta performanța, asigurându-se că analiza în timp real a traficului nu va întârzia procesarea.

Scalabilitatea este esențială pentru ca sistemul să poată răspunde nevoilor în continuă schimbare ale pieței. Acesta trebuie să fie capabil să proceseze date de la o gamă largă de dispozitive și servere, fără a compromite viteza de răspuns sau acuratețea analizei.

Principalele priorități ale sistemului includ:

* **Accesibilitatea și interfața ușor de utilizat**: Interfața va fi intuitivă și va oferi acces rapid la datele și recomandările esențiale.
* **Furnizarea de informații actualizate și relevante**: Sistemul va asigura că analizele și recomandările sunt generate pe baza celor mai recente date de trafic.
* **Eficiența în gestionarea volumelor mari de date**: Sistemul va fi optimizat pentru a gestiona eficient atât datele mici, cât și volumele mari de trafic, fără a afecta performanța.

### 4.3.2 Acțiune/Rezultat

**4.3 Tabel - Acțiune/Rezultat sistemului de gestionare a vânzărilor și a recomandărilor**

|  |  |
| --- | --- |
| **Acțiune** | **Rezultat** |
| Utilizatorul selectează tipul de analiză dorit (trafic, protocoale, atacuri) | Sistemul afișează informațiile relevante corespunzătoare tipului de analiză selectat. |
| Utilizatorul introduce parametrii pentru analiza traficului (IP sursă/destinație, porturi, tip de protocol) | Sistemul validează datele introduse și oferă feedback imediat dacă informațiile sunt incomplete sau incorecte. |
| Utilizatorul confirmă inițierea analizei | Sistemul începe procesul de capturare și analiza traficului de rețea și oferă un raport detaliat al sesiunilor de trafic monitorizate. |
| Sistemul detectează anomalii în traficul de rețea (ex: atacuri DDoS, tentative de phishing, malware) | Utilizatorul primește o alertă în timp real despre activitățile suspecte sau potențial dăunătoare. |
| Sistemul trimite notificări automate despre anomaliile detectate (ex: trafic excesiv, acces neautorizat) | Utilizatorul este informat imediat despre posibilele riscuri de securitate, permițând intervenția rapidă. |
| Utilizatorul poate accesa istoricul analizei traficului | Sistemul oferă un raport detaliat al traficului monitorizat anterior, cu informații despre evenimentele și atacurile detectate, facilitând analiza ulterioară a tendințelor de securitat |

### 4.3.3 Cerințe funcționale

Este necesar ca sistemul de interceptare și analiza traficului de rețea să îndeplinească următoarele criterii funcționale:

* Utilizatorii pot configura parametrii de capturare a traficului, cum ar fi IP-uri sursă/destinație, porturi și protocoale.
* Utilizatorii vor putea analiza traficul în timp real și vor putea vizualiza statistici detaliate despre pachetele de date.
* În cazul în care se detectează activități suspecte (ex: atacuri DDoS, acces neautorizat), sistemul va trimite notificări utilizatorilor.
* Sistemul va permite utilizatorilor să vizualizeze istoricul sesiunilor de trafic și al alertelor anterioare pentru o analiză ulterioară.
* Interfața va fi accesibilă atât de pe desktop, cât și de pe dispozitive mobile, pentru a permite utilizatorilor să monitorizeze rețeaua de oriunde.
* Sistemul va oferi opțiuni de filtrare și sortare a traficului, astfel încât utilizatorii să poată extrage rapid informațiile necesare.
* Designul interfeței va fi simplu, intuitiv și ușor de utilizat, pentru a facilita utilizarea de către persoanele cu diferite nivele de experiență.

Aceste cerințe vor contribui la o gestionare eficientă a traficului de rețea și vor asigura monitorizarea proactivă a posibilelor amenințări.

### 4.3.4 Cerințe de performanță

Pentru a asigura performanța optimă a sistemului de interceptare și analiza traficului de rețea, acesta trebuie să îndeplinească următoarele cerințe de performanță:

* Răspunsul sistemului la acțiunea utilizatorului (ex: inițierea unei analize de trafic, vizualizarea unui raport) trebuie să fie de cel mult două secunde.
* Sistemul trebuie să poată gestiona simultan monitorizarea unui număr mare de sesiuni de trafic de rețea, fără a afecta performanța sau viteza analizei.
* În cazul unui atac sau a unei defecțiuni semnificative în rețea, sistemul trebuie să poată detecta și alerta utilizatorii imediat, iar timpii de recuperare a sistemului nu trebuie să depășească 30 de minute.
* Performanța sistemului trebuie să rămână constantă pe măsură ce volumul de trafic și numărul de utilizatori crește.

Aceste cerințe sunt esențiale pentru asigurarea unui sistem de monitorizare a traficului rapid și fiabil, capabil să răspundă prompt în fața amenințărilor.

### 4.3.5 Cerințe de securitate

Pentru a asigura protecția datelor și a infrastructurii rețelei, se vor implementa următoarele cerințe de securitate:

* Datele capturate din rețea vor fi verificate înainte de a fi stocate sau procesate, pentru a preveni erorile și pentru a asigura acuratețea acestora.
* Conexiunea între client și server va fi criptată folosind protocoale de securitate moderne (ex: TLS), pentru a proteja datele în timpul transmiterii și pentru a preveni accesul neautorizat.
* Datele capturate și stocate vor fi păstrate într-un mediu securizat pe servere care respectă cele mai bune practici de securitate cibernetică.
* Accesul la datele sensibile va fi restricționat prin autentificare multi-factor și va fi monitorizat constant pentru a preveni accesul neautorizat.
* Sistemul va include măsuri de prevenire a atacurilor interne (ex: prin politici de acces bazate pe roluri) și va permite auditarea completă a activităților utilizatorilor pentru a asigura integritatea datelor.

Aceste cerințe vor asigura protecția și integritatea datelor analizate și vor oferi utilizatorilor încredere în securitatea sistemului.