FIREWALL SOZLAMALARINI AVTOMATLASHTIRISH TIZIMINING ARXITEKTURASI VA ALGORITMLARI

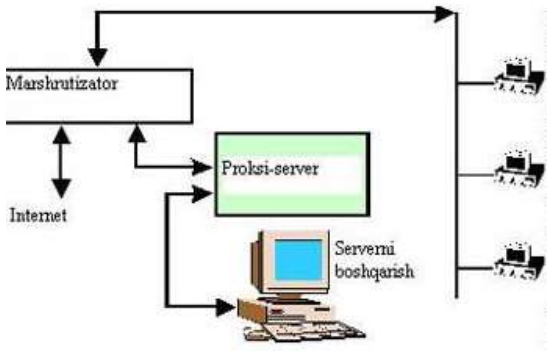
Hafizov Shukrullo Fayzullo o‘g‘li
O‘ktamov Doston Rustam o‘g‘li
Baxtiyorov Murodjon Farxodjon o‘g‘li
O‘razaliyeva Rayxona Qaxramon qizi
Muxammad al – Xorazmiy nomidagi TATU talabalari

Annotatsiya: *Ushbu maqolada firewall sozlamalarini avtomatlashtirish tizimining arxitekturasi va ishlash algoritmlari tahlil qilinadi. Tizim foydalanuvchi tomonidan kiritilgan xavfsizlik siyosatlari asosida firewall konfiguratsiyasini avtomatik ravishda generatsiya qilish, tekshirish va tarmoq qurilmalariga tatbiq etish imkonini beradi. Maqolada avtomatlashtirilgan tizimning modulli arxitekturasi, asosiy komponentlari hamda ularning o‘zaro ishlash mexanizmi yoritilgan. Shuningdek, tizimning ishlash bosqichlari, siyosatlarni tahlil qilish, qoidalarni generatsiya qilish va validatsiya jarayonlari algoritmik nuqtai nazardan ko‘rib chiqilgan.*

Kalit so‘zlar: *Firewall, tarmoq xavfsizligi, avtomatlashtirilgan tizim, xavfsizlik siyosati, konfiguratsiya generatsiyasi, algoritm, tarmoq boshqaruvi, IPTables, pfSense, Ansible, monitoring.*

Firewall sozlamalarini avtomatlashtirish tizimi — bu foydalanuvchi tomonidan kiritilgan xavfsizlik siyosatlari asosida firewall konfiguratsiyasini avtomatik shakllantiruvchi, tekshiruvchi va uni tarmoqqa tatbiq etuvchi dasturiy tizimdir.

Mazkur tizimning asosiy g‘oyasi — qo‘lda bajariladigan ko‘p bosqichli sozlash jarayonini avtomatik algoritmlar orqali optimallashtirish, inson xatosini kamaytirish va tarmoq xavfsizligini yuqori darajada saqlashdan iborat.



1.1-rasm. Firewall sozlamalarini avtomatlashtirish tizimi.

Tizimning asosiy maqsadlari

1. Firewall siyosatini markazlashgan boshqarish — turli tarmoqlarda bir xil xavfsizlik qoidalarini avtomatik tarqatish.

2. Avtomatik konfiguratsiya generatsiyasi — foydalanuvchi kiritgan siyosat asosida to‘g‘ridan-to‘g‘ri ishlaydigan kod (masalan, IPTables, pfSense, Cisco ACL) hosil qilish.

3. Konfiguratsiyani tahlil qilish va tekshirish — qoidalar orasida mos kelmaslik yoki xatolikni aniqlash.

4. Monitoring va loglarni tahlil qilish — avtomatik tahlil va ogohlantirish funksiyasi.

Tizim arxitekturasi

Tizim modulli arxitektura asosida yaratiladi. Har bir modul o‘ziga xos vazifani bajaradi, ammo ular yagona markaziy boshqaruv tizimi orqali bog‘langan. Diagramma tavsifi — “Avtomatlashtirilgan firewall tizimi arxitekturasi”

Diagrammada quyidagi modullar mavjud:

1. User Interface (UI) – Administrator yoki foydalanuvchi siyosatlarni kiritadi (masalan: “192.168.0.0/24 tarmoqdan 80-portga ruxsat berilsin”).

2. Policy Parser – Kiritilgan siyosatni sintaktik tahlil qiladi, noto‘g‘ri formatlarni aniqlaydi.

3. Rule Generator – Tahlildan o‘tgan siyosatlar asosida avtomatik konfiguratsiya faylini (masalan, iptables yoki pf.conf) hosil qiladi.

4. Validator Module – Yaratilgan qoidalarni tarmoq topologiyasi bilan solishtiradi, to‘qnashuvlarni aniqlaydi.

5. Deployment Module – Sozlamalarni mos tarmoq qurilmalariga yuboradi (SSH, API yoki Ansible orqali).

6. Logging & Monitor – Jarayonni kuzatadi, natijalarni log faylga yozadi.

1.1-jadval. Tizim komponentlari tahlili

Modul nomi	Asosiy funksiyasi	Amalga oshiriladigan texnologiya
UI (Interfeys)	Siyosatlarni kiritish va tahrirlash	Web interfeys (Flask / Django)
Policy Parser	Siyosatni tahlil qilish	Python skript, YAML format
Rule Generator	Firewall konfiguratsiyasini yaratish	Python, Ansible Jinja2 templating
Validator	Xatoliklarni aniqlash	Regex, tarmoq topologiya modeli
Deployer	Sozlamalarni yuborish	SSH, REST API, Ansible Playbook

Modul nomi	Asosiy funksiyasi	Amalga oshiriladigan texnologiya
Logger	Natijalarni saqlash	JSON log fayllar, syslog integratsiyasi

Ishlash prinsipi. Avtomatlashtirilgan tizim quyidagi bosqichlarda ishlaydi:

1. Ma’lumotlarni kiritish: Administrator web-interfeys orqali xavfsizlik siyosatini kiritadi.

2. Sintaksis tahlili: Policy Parser kiritilgan siyosatni tahlil qiladi (IP manzil, port, protokol to‘g‘riligini tekshiradi).

3. Qoidalar generatsiyasi: Rule Generator siyosat asosida avtomatik tarzda konfiguratsiya faylini yaratadi.

4. Validatsiya: Yaratilgan fayl Firewall’ning joriy qoidalari bilan solishtiriladi, to‘qnashuv aniqlansa, tizim xabar beradi.

5. Qo‘llash (Deploy): Sozlamalar avtomatik ravishda serverga yuboriladi.

6. Monitoring: Har bir amal log faylga yoziladi, tizim administratorni natijalar bilan tanishtiradi.

1.2-rasm. Avtomatlashtirilgan tizimning ishlash prinspi.

Algoritm tavsifi

Tizimning ishlash algoritmini quyidagi psevdokod orqali ifodalash mumkin:

```
pgsql

Algorithm FirewallAutoConfig
Input: PolicyList
Output: Firewall_Config_File

Begin
    For each policy in PolicyList do
        If ValidateSyntax(policy) == True then
            rule ← GenerateRule(policy)
            Append rule to Config_File
        Else
            LogError(policy, "Invalid policy syntax")
        End If
    End For

    If ValidateConfig(Config_File) == True then
        DeployConfig(Config_File)
        Log("Deployment successful")
    Else
        Log("Configuration validation failed")
    End If
End
```

Bu algoritmda har bir siyosat (policy) avval sintaktik jihatdan tekshiriladi. Agar xatolik topilmasa, undan konfiguratsion qoida yaratiladi. Keyin barcha qoidalar birlashtirilib, yakuniy fayl hosil qilinadi va serverga yuboriladi.

XULOSA

Xulosa qilib aytganda, firewall sozlamalarini avtomatlashtirish tizimi zamonaviy tarmoq xavfsizligini boshqarishda muhim ahamiyatga ega. Ushbu tizim yordamida xavfsizlik siyosatlarini markazlashgan tarzda boshqarish, konfiguratsiya qoidalarini avtomatik generatsiya qilish hamda ularni tarmoq qurilmalariga tezkor tatbiq etish imkoniyati yaratiladi. Tizimning modulli arxitekturasi har bir funksional komponentni alohida boshqarish va rivojlantirish imkonini beradi. Avtomatlashtirilgan algoritmlar yordamida firewall qoidalaridagi xatoliklar aniqlanadi va inson omili bilan bog‘liq kamchiliklar kamaytiriladi. Natijada tarmoq xavfsizligi darajasi oshadi, tizimni boshqarish jarayoni esa yanada samarali va ishonchli bo‘ladi.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings W. Network Security Essentials: Applications and Standards. Pearson Education, 2017.
2. Kurose J., Ross K. Computer Networking: A Top-Down Approach. Pearson, 2021.
3. Tanenbaum A., Wetherall D. Computer Networks. Pearson, 2019.
4. Cheswick W., Bellovin S., Rubin A. Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley, 2014.

5. Behl B., Behl K. Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2017.
6. Netfilter Project. IPTables Documentation. https://netfilter.org
7. pfSense Documentation. https://docs.netgate.com