FIREWALL TEXNOLOGIYALARINING NAZARIY ASOSLARI

Abdullayev Xushnud Raxmatulla o‘g‘li
Normamatov Xusan Baxodir o‘g‘li
Seytmamatov Sohibjon Muzaffar o‘g‘li
TATU, Kiberxavfsizlik fakulteti talabalari
Saburova Shoxista Shavkat qizi

Annatatsiya: Mazkur maqolada firewall texnologiyalarining nazariy asoslari, ishlash prinsiplari va zamonaviy tarmoq xavfsizligini ta’minlashdagi o‘rni tahlil qilinadi. Tadqiqot davomida firewallning asosiy turlari, arxitekturasi, xavfsizlik siyosatlari hamda trafikni filtrlash mexanizmlari ko‘rib chiqilgan. Shuningdek, firewall sozlamalaridagi muammolar, inson omili bilan bog‘liq xatoliklar va ularni avtomatlashtirish zarurati yoritilgan.
Kalit so‘zlar: Firewall, tarmoq xavfsizligi, paket filtrlash, stateful inspection, NGFW, firewall arxitekturasi, xavfsizlik siyosati, trafik monitoringi, IDS/IPS, avtomatlashtirish, Ansible, Terraform, Python, REST API, kiberxavfsizlik.

Xavfsizlik devori (Firewall) — bu kompyuter tarmog‘ini turli xil tashqi va ichki tahdidlardan himoya qiluvchi maxsus apparat yoki dasturiy vositadir. U asosan ichki (ishonchli) tarmoq bilan tashqi (ishonchsiz) tarmoq, ya’ni internet o‘rtasida “filtr” yoki “himoya devori” sifatida ishlaydi.

Firewallning asosiy vazifasi — tarmoqqa kiruvchi va undan chiquvchi barcha ma’lumot oqimini (trafikni) nazorat qilish, uni oldindan belgilangan xavfsizlik qoidalari asosida tekshirish va faqat ruxsat etilgan ma’lumotlargagina o‘tishga imkon berishdir. Shubhali yoki zararli deb topilgan trafik esa bloklanadi.

Firewall ishlash jarayonida quyidagi mezonlarga e’tibor beradi:

- IP manzillar (qayerdan kelgan va qayerga ketayotgan)
- Port raqamlari (qaysi xizmat ishlatilayotgan)
- Protokollar (TCP, UDP, HTTP, HTTPS va boshqalar)
- Paket tarkibi (ba’zi rivojlangan firewalllarda)

Dastlabki firewall tizimlari juda oddiy bo‘lib, faqat paketlarni filtrlash bilan cheklangan. Ular ma’lumotning faqat tashqi belgilariga qarab qaror qabul qilgan. Ammo bugungi kunda firewall texnologiyasi ancha rivojlangan bo‘lib, u nafaqat paketlarni, balki ularning mazmunini, ulanish holatini va foydalanuvchi xatti-harakatlarini ham tahlil qila oladi.

Firewallni ikki asosiy turga ajratish mumkin:

1. Dasturiy (Software) firewall

Bu turdagi firewall kompyuter yoki serverga dastur sifatida o‘rnatiladi. U faqat o‘sha qurilmani himoya qiladi.

Afzalliklari:

- O‘rnatish oson

- Arzon yoki bepul variantlari mavjud
- Har bir qurilma uchun alohida nazorat

Kamchiliklari:

- Faqat bitta qurilmani himoya qiladi
- Tizim resurslaridan foydalanadi

2. Apparat (Hardware) firewall

Bu alohida qurilma bo‘lib, butun tarmoqni himoya qiladi. Odatda router yoki maxsus xavfsizlik qurilmasi sifatida ishlatiladi.

Afzalliklari:

- Butun tarmoqni himoya qiladi
- Ishlash tezligi yuqori
- Barqaror va ishonchli

Kamchiliklari:

- Qimmatroq
- Sozlash murakkabroq

Firewallning ishlash prinsipi oddiy qilib quyidagicha tushuntiriladi:

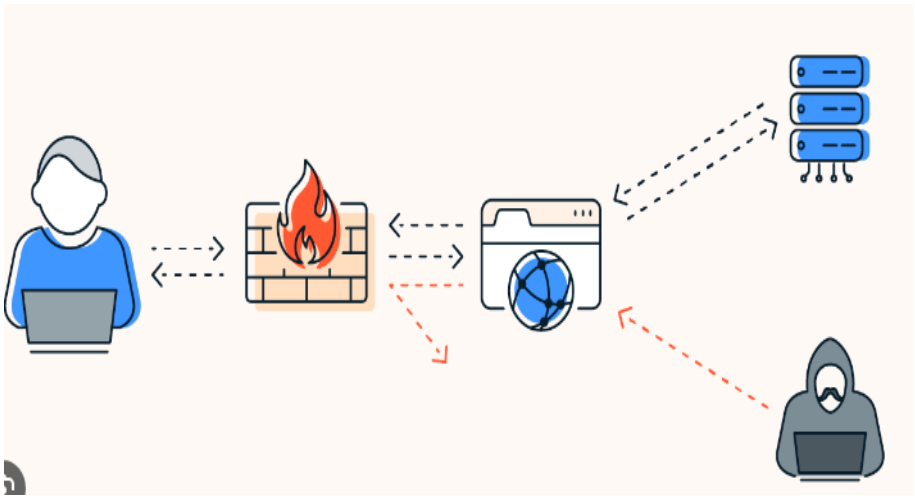
1. Tarmoqqa ma’lumot keladi yoki chiqadi
2. Firewall bu ma’lumotni tekshiradi
3. Belgilangan qoidalar bilan solishtiradi
4. Agar ruxsat bo‘lsa — o‘tkazadi
5. Agar xavfli bo‘lsa — bloklaydi

Shuningdek, firewall xavfsizlik siyosatini amalga oshirishda muhim rol o‘ynaydi. Har bir tashkilot o‘z xavfsizlik talablariga qarab maxsus qoidalar (rules) yaratadi. Masalan:

- Faqat ma’lum IP manzillarga ruxsat berish
- Ba’zi saytlarni bloklash
- Ma’lum portlarni yopish

Zamonaviy firewalllar esa qo‘shimcha imkoniyatlarga ega:

- Deep Packet Inspection (chuqur tahlil)
- VPN qo‘llab-quvvatlash
- IDS/IPS integratsiyasi
- Trafik monitoringi va log yuritish



1.1-rasm. Firewall ishlash tartibi.

1.2. Firewallning asosiy funksiyalari

1. Trafikni filtrlash: Ma’lum IP-manzillar, portlar yoki protokollar asosida ruxsat berish yoki taqiqlash.
2. Tarmoq chegarasini himoyalash: Tashqi tarmoqlardan kiruvchi hujumlarni to‘xtatish.
3. Qo‘shimcha xavfsizlik siyosatini amalga oshirish: Tarmoqdagi foydalanuvchilar uchun kirish cheklovlari.
4. Monitoring va log yuritish: Tizim orqali o‘tgan barcha trafik yozuvini saqlash.

1.3. Firewall turlari

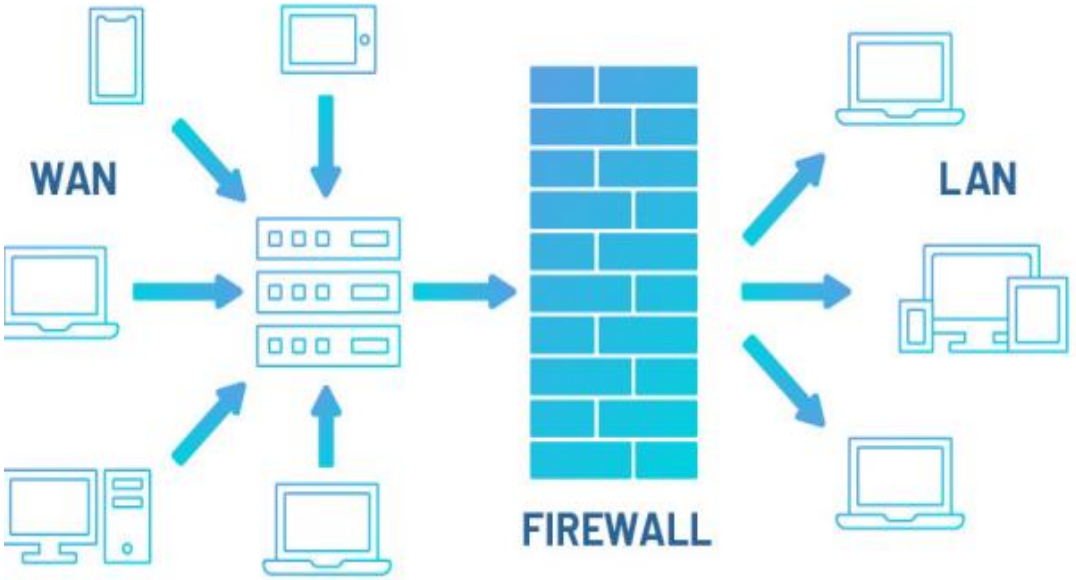
1.1-jadval. Firewall texnologiyalari bir necha avlodlari.

Avlod	**Tavsif**	**Misollar**
1-avlod	Paket filtrlash (packet filter) asosida ishlaydi	Cisco ACL, IPTables
2-avlod	Holatli tekshiruv (stateful inspection)	pfSense, Fortigate
3-avlod	Ilova darajasida tahlil (application firewall)	Palo Alto, Check Point
4-avlod	NGFW — Next Generation Firewall	Sophos XG, Cisco Firepower

1.4. Firewall arxitekturasi

Firewall tizimi odatda quyidagi asosiy komponentlardan iborat bo‘ladi:

- Policy Engine: Qoidalarni saqlash va tahlil qilish moduli.
- Packet Filter Module: Tarmoq paketlarini qabul qilib, ularni tekshiradi.
- Logging & Monitoring: Har bir qarorni (ruxsat yoki rad etish) yozib boradi.
- User Interface: Administrator uchun boshqaruv paneli.



1.2-rasm. Firewall arxitekturasi.

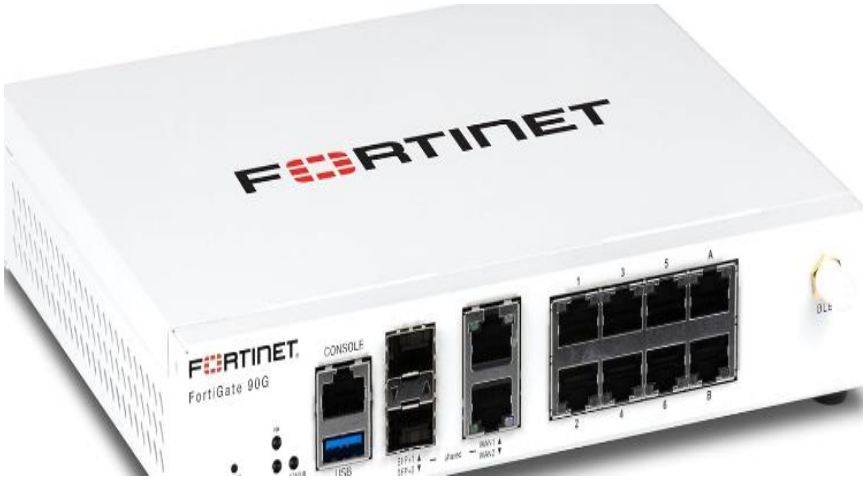
“Firewall arxitekturasi” diagrammasida foydalanuvchi trafik tarmoqdan kirib, paket filtrlash moduliga yo‘naltiriladi. Ushbu modul xavfsizlik siyosatini Policy Engine’dan

oladi va qaror qabul qiladi. Qaror (Allow/Block) natijasida paket yo‘lini davom ettiradi yoki to‘xtatiladi. Har bir operatsiya log fayllarda qayd etiladi.

1.5. Firewall siyosatlari (Policies)

Firewallning ishlash samaradorligi to‘g‘ridan-to‘g‘ri xavfsizlik siyosatiga bog‘liq. Siyosatlar quyidagi mezonlar asosida tuziladi:

- IP manzillar (manba va manzil);
- Port raqamlari;
- Protokollar (TCP, UDP, ICMP va b.);
- Vaqt oralig‘i;
- Tizimdagi foydalanuvchi roli.



1.3-rasm. Firewall siyosatlari.

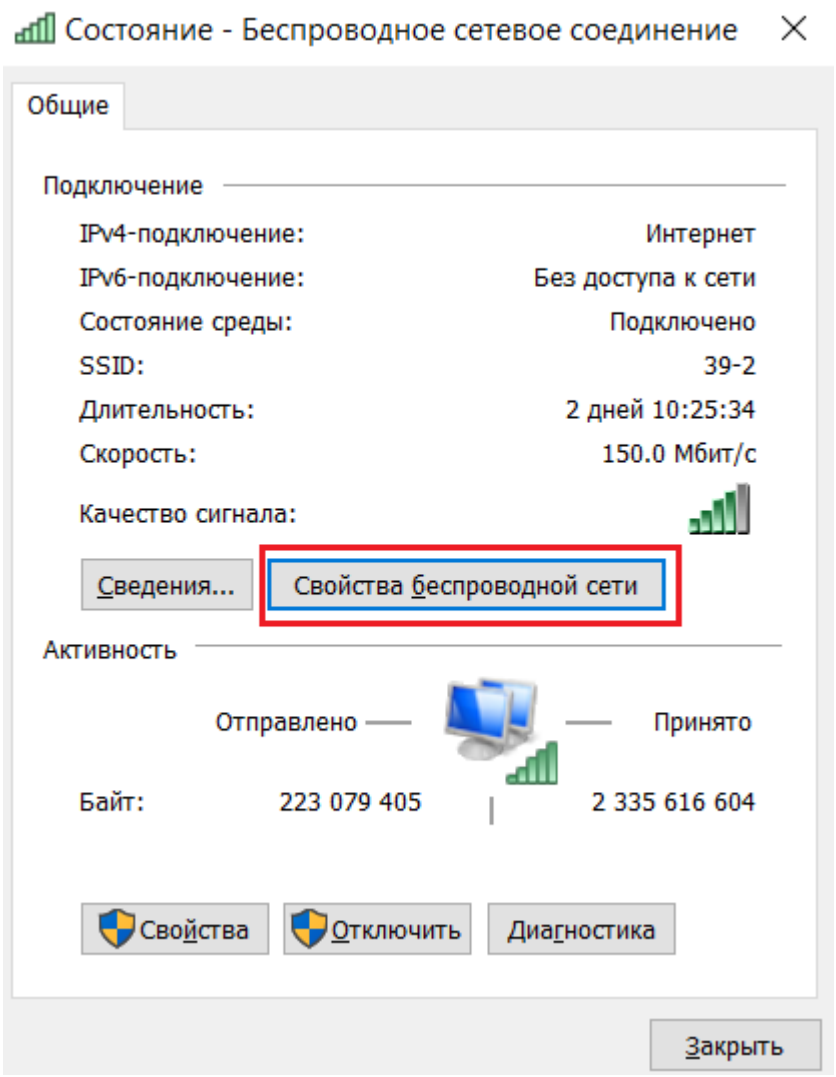
Siyosatlarning noto‘g‘ri o‘rnatilishi tarmoqda xavfsizlik muammosiga olib keladi. Shu sababli siyosatlarni avtomatik tekshirish va yangilash zarur.

1.6. Firewall sozlamalaridagi muammolar

Qo‘lda sozlashda quyidagi kamchiliklar mavjud:

- Inson xatosi (konfiguratsiyada noto‘g‘ri parametr kiritish);
- Sozlamalarning mos kelmasligi (turli tarmoqlar uchun turli formatlar);
- Sozlash vaqtining uzunligi;
- O‘zgarishlarni kuzatishning qiyinligi.

Masalan, yirik korxonalarda yuzlab qoidalarni har hafta yangilash zarur bo‘ladi. Agar bu ish avtomatlashtirilmasa, xavfsizlik siyosatlari izdan chiqishi mumkin.



1.4-rasm. Firewall sozlamalaridagi muammolar

1.7. Firewall avtomatlashtirish zarurati

Avtomatlashtirishning maqsadi — qo‘lda bajariladigan murakkab va xavfli ishlarni avtomatik algoritmlar orqali tez, aniq va xavfsiz bajarishdir. Bu yondashuv quyidagi afzalliklarni beradi:

- Konfiguratsiyani yaratish jarayoni tezlashadi;
- Xatolik ehtimoli kamayadi;
- Tizim xavfsizligi barqaror saqlanadi;
- Qoidalar markazlashgan boshqaruv orqali yangilanadi.

1.5-rasm. Firewall avtomatlashtirish zarurati.

Avtomatlashtirish uchun eng ko‘p qo‘llaniladigan texnologiyalar: Python skriptlari, Ansible, Terraform, va REST API asosidagi boshqaruv tizimlari.

Xulosa

Ushbu bobda firewall texnologiyasining nazariy asoslari, turlari, arxitekturasi va avtomatlashtirish zarurati tahlil qilindi. Keyingi bobda firewall sozlamalarini avtomatlashtirish tizimining konsepsiyasi, ishlash mexanizmi va dasturiy yechimlari yoritiladi.

FOYDALANILGAN ADABIYOTLAR:

1. Stallings W. — *Network Security Essentials*, 6th Edition. Pearson, 2022.
2. Fortinet Technical Documentation — *Firewall Automation Guide*, 2023.
3. Cisco Systems — *Firewall Configuration Best Practices*, Cisco Press, 2021.
4. Tanenbaum A. — *Computer Networks*, 5th Edition. Pearson, 2020.
5. OWASP Foundation — *Security Configuration Automation Protocol (SCAP)*, 2022.
6. Red Hat Ansible Documentation — https://docs.ansible.com
7. Ubuntu Firewall (UFW) Guide — Canonical Docs, 2024.
8. NIST SP 800-41 Rev.1 — *Guidelines on Firewalls and Firewall Policy*, 2022.
9. Python.org — *Python Networking and Automation Libraries*, 2023.