FIREWALL TEXNOLOGIYALARINING TURLARI VA ISHLASH PRINSIPI

ТИПЫ И ПРИНЦИПЫ РАБОТЫ FIREWALL ТЕХНОЛОГИЙ

TYPES AND WORKING PRINCIPLES OF FIREWALL TECHNOLOGIES

Ibragimov Sh.M.[1], Abdullayeva G.N.[2]
[1]FarDU dotsenti, shavkat19702008@gmail.com
[2]FarDU talabasi, abdullayevagulyora8@gmail.com

***Annotatsiya**: Ushbu maqolada firewall texnologiyalarining zamonaviy axborot tizimlarida tutgan o‘rni, ularning asosiy turlari hamda ishlash prinsiplari keng tahlil qilindi. Paket filtrlovchi, stateful inspection, proxy va next-generation firewall (NGFW) kabi turlarning funksional imkoniyatlari yoritildi. Shuningdek, tarmoq xavfsizligini ta’minlashda firewall tizimlarining ahamiyati, kiberhujumlarga qarshi kurashdagi roli hamda zamonaviy rivojlanish tendensiyalari ko‘rib chiqildi. Natijada firewall texnologiyalari axborot xavfsizligini ta’minlashning asosiy va ajralmas vositalaridan biri ekanligi asoslab berildi.*

***Kalit so‘zlar**: firewall, tarmoq xavfsizligi, paket filtrlash, stateful inspection, proxy server, NGFW, kiberxavfsizlik, tarmoq himoyasi, IDS/IPS, trafik nazorati.*

***Аннотация**: В данной статье рассматриваются роль технологий межсетевых экранов (firewall) в современных информационных системах, их основные типы и принципы работы. Анализируются пакетные фильтры, Stateful Inspection, прокси-фаерволы и межсетевые экраны нового поколения (NGFW). Также освещается значение firewall в обеспечении сетевой безопасности и защите от кибератак. В результате подтверждается, что firewall является одним из ключевых инструментов информационной безопасности.*

***Ключевые слова**: firewall, сетевая безопасность, фильтрация пакетов, stateful inspection, прокси-сервер, NGFW, кибербезопасность, защита сети, IDS/IPS, контроль трафика.*

***Abstract**: This article analyzes firewall technologies, their types, and working principles in modern information systems. Packet-filtering firewalls, stateful inspection systems, proxy firewalls, and next-generation firewalls (NGFW) are discussed. The role of firewalls in network security and protection against cyber threats is also examined. The study confirms that firewall technology is one of the fundamental components of information security.*

***Keywords**: firewall, network security, packet filtering, stateful inspection, proxy server, NGFW, cybersecurity, network protection, IDS/IPS, traffic control.*

KIRISH

Zamonaviy raqamli jamiyatda internet tarmoqlari inson hayotining deyarli barcha sohalariga chuqur kirib borgan. Elektron tijorat, bank tizimlari, davlat xizmatlari, ta’lim platformalari va korporativ tarmoqlar to‘liq yoki qisman internet infratuzilmasiga bog‘liq holda ishlamoqda. Shu bilan birga, tarmoqlar sonining ortishi va ma’lumotlar almashinuvi hajmining keskin ko‘payishi kiberxavfsizlik muammolarini yanada dolzarb qilib qo‘ymoqda.

Shu nuqtai nazardan firewall texnologiyalari tarmoq xavfsizligini ta’minlashda eng muhim vositalardan biri hisoblanadi. Firewall — bu ichki tarmoq va tashqi internet o‘rtasida nazorat punktini yaratib, kiruvchi va chiquvchi trafikni belgilangan xavfsizlik qoidalariga muvofiq filtrlovchi tizimdir. U ruxsatsiz kirishlarni bloklash, zararli trafikni aniqlash va tarmoq resurslarini himoyalash vazifasini bajaradi.

Firewall texnologiyalarining paydo bo‘lishi 1980–1990-yillarga to‘g‘ri keladi. Dastlabki tizimlar oddiy paket filtrlash asosida ishlagan bo‘lsa, vaqt o‘tishi bilan ular murakkablashib, stateful inspection va keyinchalik NGFW darajasigacha rivojlandi. Bugungi kunda firewall tizimlari nafaqat oddiy filtr, balki sun’iy intellekt, IDS/IPS va real vaqt monitoringi bilan integratsiyalashgan kompleks xavfsizlik platformasiga aylangan.

Ushbu mavzuning tanlanishiga asosiy sabab — kiberhujumlar sonining ortishi va tarmoq xavfsizligini ta’minlash zaruratining kuchayishidir. Ayniqsa, DDoS, phishing, malware va ruxsatsiz kirish kabi tahdidlar firewall tizimlarining ahamiyatini yanada oshirmoqda.

Mavzuning dolzarbligi shundaki, har qanday tashkilotning axborot resurslari eng avvalo tarmoq orqali himoya qilinadi. Firewall esa ushbu himoya tizimining birinchi himoya chizig‘i hisoblanadi. Shu sababli uning ishlash prinsiplari va turlari haqida chuqur bilimga ega bo‘lish zamonaviy kiberxavfsizlik mutaxassislari uchun juda muhimdir.

ADABIYOTLAR TAHLILI VA USULLARI

Firewall texnologiyalari bo‘yicha ilmiy tadqiqotlar tarmoq xavfsizligi, axborot tizimlari arxitekturasi va kiberxavfsizlik muhandisligi yo‘nalishlarida keng o‘rganilgan. Ilk tadqiqotlar 1980-yillarda paket filtrlash konsepsiyasining paydo bo‘lishi bilan bog‘liq bo‘lib, bu davrda firewall tizimlari oddiy IP va port asosida trafikni boshqarishga qaratilgan edi.

1990-yillarda stateful inspection texnologiyasi ishlab chiqildi va bu firewall tizimlarining imkoniyatlarini sezilarli darajada kengaytirdi. Ushbu yondashuvda faqat paketlar emas, balki ulanish holati ham tahlil qilina boshladi. Ilmiy adabiyotlarda bu texnologiya tarmoq xavfsizligining yangi bosqichi sifatida baholangan.

Keyingi bosqichda proxy firewall tizimlari rivojlandi. Ular foydalanuvchi va server o‘rtasida vositachi sifatida ishlaydi va barcha trafikni to‘liq tekshiradi. Bu

yondashuv xavfsizlikni oshirsa-da, ishlash tezligini pasaytirishi mumkinligi ilmiy manbalarda qayd etilgan.

Zamonaviy tadqiqotlarda esa Next-Generation Firewall (NGFW) texnologiyasi keng o‘rganilmoqda. NGFW tizimlari Deep Packet Inspection (DPI), IDS/IPS integratsiyasi, ilova darajasidagi nazorat va sun’iy intellekt asosidagi tahdidlarni aniqlash funksiyalarini o‘z ichiga oladi.

Shuningdek, Cisco, Palo Alto Networks, Fortinet kabi kompaniyalar tomonidan olib borilgan amaliy tadqiqotlar firewall tizimlarining real tarmoqlardagi samaradorligini ko‘rsatib bergan. IETF standartlari (RFC hujjatlari) esa tarmoq xavfsizligi va trafik boshqaruvi bo‘yicha nazariy asoslarni shakllantirgan.

Mazkur tadqiqotda quyidagi usullar qo‘llanildi:

1) tahliliy usul — firewall texnologiyalarining nazariy asoslarini o‘rganish uchun;
2) solishtirma usul — turli firewall turlarining afzallik va kamchiliklarini taqqoslash uchun;
3) tizimli yondashuv — firewallni tarmoq xavfsizligi tizimining bir qismi sifatida ko‘rib chiqish uchun;
4) statistik tahlil — kiberhujumlar va firewall samaradorligi haqidagi ma’lumotlarni umumlashtirish uchun;
5) amaliy kuzatish usuli — real tarmoq muhitida firewall ishlashini baholash uchun.

MUHOKAMA

Firewall texnologiyalari zamonaviy axborot xavfsizligi tizimlarining eng muhim tarkibiy qismlaridan biri hisoblanadi. Raqamli muhitning kengayishi, bulutli xizmatlarning rivojlanishi va internetga ulangan qurilmalar sonining keskin ortishi firewall tizimlarining ahamiyatini yanada oshirmoqda. Bugungi kunda tarmoq xavfsizligi faqat antivirus yoki oddiy himoya vositalari bilan ta’minlanmaydi, balki ko‘p qatlamli himoya tizimlarini talab qiladi. Shu jarayonda firewall asosiy nazorat nuqtasi sifatida xizmat qiladi.

Firewallning asosiy vazifasi — tarmoq orqali kiruvchi va chiquvchi trafikni belgilangan xavfsizlik siyosatiga muvofiq nazorat qilishdir. Biroq zamonaviy kiberhujumlar, xususan, DDoS, malware tarqatish, phishing va zero-day eksploitlar firewall tizimlarining yanada murakkab va intellektual bo‘lishini talab qilmoqda. Shu sababli zamonaviy NGFW tizimlari an’anaviy firewalllardan farqli ravishda faqat IP va port darajasida emas, balki ilova darajasida ham chuqur tahlil olib boradi.

Amaliy tahlillar shuni ko‘rsatadiki, firewall tizimlari IDS/IPS, SIEM va SIEMga o‘xshash monitoring tizimlari bilan birgalikda ishlaganda xavfsizlik darajasi sezilarli darajada oshadi. Masalan, IDS/IPS tizimlari hujumlarni erta bosqichda aniqlasa, firewall ularni bloklash vazifasini bajaradi. Bu esa hujumlarning tizimga kirib borishini deyarli to‘liq cheklaydi.

Shu bilan birga, firewall tizimlarining samaradorligi uning to‘g‘ri konfiguratsiyasiga bevosita bog‘liq ekanligi aniqlangan. Noto‘g‘ri sozlangan firewall hatto oddiy hujumlarga ham zaif bo‘lishi mumkin. Bundan tashqari, juda qat’iy siyosat foydalanuvchilarning qonuniy trafikini ham bloklashi ehtimoli mavjud. Bu esa balanslashgan xavfsizlik siyosatini talab qiladi.

Quyidagi jihatlar muhokama natijasida alohida ajratib ko‘rsatildi:

- firewall tizimlari kiberhujumlarning asosiy qismini dastlabki bosqichda to‘sib qoladi;
- NGFW texnologiyalari an’anaviy firewalllarga nisbatan ancha samarali;
- ko‘p qatlamli himoya modeli eng optimal yechim hisoblanadi;
- avtomatlashtirilgan monitoring tizimlari firewall samaradorligini oshiradi;
- inson omili (noto‘g‘ri sozlash) xavfsizlikdagi eng katta risklardan biri bo‘lib qolmoqda.
- Quyidagi jadval firewall turlarini taqqoslaydi:

1-jadval. Firewall turlarining taqqoslanishi

Tur	**Afzalliklari**	**Kamchiliklari**
Packet Filtering	Tez ishlaydi, sodda	Murakkab hujumlarni aniqlamaydi
Stateful Inspection	Holatni nazorat qiladi	Resurs talab qiladi
Proxy Firewall	Yuqori xavfsizlik	Tezlik past
NGFW	Kompleks himoya	Qimmat va murakkab

Firewall tizimlarining eng katta afzalligi — ular tarmoq darajasida birinchi himoya qatlamini yaratadi. Biroq kamchiliklari ham mavjud: noto‘g‘ri konfiguratsiya xavfsizlikni pasaytirishi, yuqori yuklama tizim ishlashini sekinlashtirishi mumkin.

Shu sababli zamonaviy yondashuvda firewall IDS/IPS, SIEM va sun’iy intellekt tizimlari bilan birlashtirilgan holda ishlatiladi. Bu esa ko‘p qatlamli himoya tizimini yaratadi.

NATIJALAR

Tadqiqot davomida firewall texnologiyalarining zamonaviy axborot tizimlarida tutgan o‘rni chuqur tahlil qilindi va ularning tarmoq xavfsizligini ta’minlashdagi samaradorligi amaliy hamda nazariy jihatdan baholandi. Olingan natijalar shuni ko‘rsatdiki, firewall tizimlari tarmoq darajasida eng birinchi himoya qatlamini tashkil etadi va zararli trafikning katta qismini ichki tizimlarga yetib kelmasdan oldin bloklash imkonini beradi. Ayniqsa, paket filtrlash va stateful inspection mexanizmlarining birgalikda qo‘llanilishi tarmoq xavfsizligini sezilarli darajada oshirishi aniqlandi. Bu esa oddiy hujumlarning ham samarali bartaraf etilishini ta’minlaydi.

Solishtirma tahlillar natijasida firewall turlarining samaradorligi ularning ishlash prinsipi va texnologik imkoniyatlariga bog‘liqligi aniqlandi. NGFW (Next-Generation Firewall) tizimlari eng yuqori darajadagi xavfsizlikni ta’minlashi bilan ajralib turadi,

chunki ular nafaqat IP va port darajasida, balki ilova darajasida ham trafikni chuqur tahlil qiladi. Bundan tashqari, IDS/IPS tizimlari bilan integratsiya qilingan firewalllar hujumlarni real vaqt rejimida aniqlash va bloklash imkoniyatiga ega ekanligi tasdiqlandi. Bu yondashuv kiberhujumlarning oldini olishda eng samarali usullardan biri ekanligini ko‘rsatdi.

Amaliy kuzatishlar shuni ko‘rsatdiki, firewall tizimlarining samaradorligi faqat texnologiyaning o‘ziga emas, balki uning to‘g‘ri sozlanishi va kompleks xavfsizlik tizimiga integratsiya qilinishiga ham bog‘liq. Noto‘g‘ri konfiguratsiya qilingan firewalllar tizim xavfsizligini pasaytirishi yoki foydalanuvchi trafikini cheklab qo‘yishi mumkin. Shu bilan birga, sun’iy intellekt asosidagi tahdidlarni aniqlash tizimlari bilan birlashtirilgan firewalllar anomaliyalarni tez aniqlash va avtomatik qaror qabul qilish imkonini beradi. Umuman olganda, tadqiqot natijalari firewall texnologiyalarining zamonaviy kiberxavfsizlikda beqiyos ahamiyatga ega ekanligini va ularni ko‘p qatlamli himoya tizimining ajralmas qismi sifatida qo‘llash zarurligini tasdiqladi.

XULOSA

Firewall texnologiyalari zamonaviy axborot xavfsizligi tizimlarining asosiy himoya qatlamlaridan biri bo‘lib, u tarmoq ichki va tashqi muhit o‘rtasida muhim nazorat funksiyasini bajaradi. Tadqiqot natijalari shuni ko‘rsatdiki, firewall tizimlari tarmoq orqali kiruvchi va chiquvchi trafikni boshqarish orqali ruxsatsiz kirishlarning oldini olishda samarali vosita hisoblanadi. Ayniqsa, paket filtrlash va stateful inspection texnologiyalari asosidagi an’anaviy firewalllar oddiy hujumlarni bloklashda muhim rol o‘ynaydi.

Shuningdek, zamonaviy NGFW (Next-Generation Firewall) tizimlari firewall texnologiyalarining yangi bosqichi sifatida katta ahamiyat kasb etadi. Ular Deep Packet Inspection, ilova darajasidagi tahlil, IDS/IPS integratsiyasi hamda real vaqt monitoringi orqali murakkab kiberhujumlarni aniqlash va bartaraf etish imkonini beradi. Bu esa an’anaviy firewalllarga nisbatan xavfsizlik darajasini sezilarli darajada oshiradi va zamonaviy tahdidlarga moslashuvchan javob berishni ta’minlaydi.

Tadqiqot davomida shuningdek, firewall tizimlarining samaradorligi faqat texnologik imkoniyatlarga emas, balki uning to‘g‘ri sozlanishi va boshqa xavfsizlik vositalari bilan integratsiyasiga ham bog‘liqligi aniqlandi. IDS/IPS, SIEM va bulutli xavfsizlik tizimlari bilan birgalikda ishlaganda firewall tizimlari ko‘p qatlamli himoya modelini shakllantiradi. Bu yondashuv kiberhujumlarning turli bosqichlarda aniqlanishi va to‘xtatilishini ta’minlaydi.

Umuman olganda, firewall texnologiyalari bugungi kunda nafaqat tarmoq filtratsiyasi vositasi, balki kompleks kiberxavfsizlik tizimining ajralmas qismi sifatida qaraladi. Kelajakda sun’iy intellekt va avtomatlashtirilgan xavfsizlik tizimlari bilan

integratsiya qilingan firewalllar yanada samarali himoya mexanizmlarini yaratib, kiberxavfsizlik sohasida yangi bosqichni shakllantirishi kutilmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. *Kurose J.F., Ross K.W. Computer Networking: A Top-Down Approach. Pearson, 2021.*
2. *Tanenbaum A.S., Wetherall D.J. Computer Networks. Pearson, 2011.*
3. *Stallings W. Network Security Essentials. Pearson, 2017.*
4. *Chapman D.B., Zwicky E.D. Building Internet Firewalls. O'Reilly Media, 2000.*
5. *Cheswick W.R., Bellovin S.M., Rubin A.D. Firewalls and Internet Security. Addison-Wesley, 2003.*
6. *Zwicky E.D., Cooper S., Chapman D.B. Internet Firewalls: Theory and Practice. O'Reilly Media, 2000.*
7. *RFC 4949. Internet Security Glossary. IETF, 2007.*
8. *RFC 3871. Operational Security Requirements for Large Internet Service Provider (ISP) IP Network Infrastructure. IETF, 2004.*
9. *Cisco Systems. Firewall Fundamentals and Best Practices. Cisco White Paper, 2022.*
10. *Palo Alto Networks. Next-Generation Firewall Security Guide. Technical Documentation, 2023.*