ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 5 / UIF:8.2 / MODERNSCIENCE.UZ

TARMOQLARARO EKRANLAR ORQALI KIRUVCHI VA CHIQUVCHI TRAFIKNI BOSHQARISH: ZAMONAVIY YONDASHUVLAR VA AMALIY YECHIMLAR

Ergashev Azizbek Xakimjon o'g'li
University of Management and Future Technologies
Kommunikatsiya va Raqamli Texnologiyalar kafedrasi Magistranti.

https://doi.org/10.5281/zenodo.15405840

Annotatsiya. *Mazkur maqolada tarmoqlararo ekranlar (firewall) orqali tarmoq xavfsizligini ta'minlash, kiruvchi va chiquvchi trafikni nazorat qilish masalalari chuqur tahlil qilinadi. Zamonaviy yondashuvlar, jumladan, davlat asosida va kontekstga yo‘naltirilgan filtrlash, Deep Packet Inspection (DPI), Next-Generation Firewall (NGFW) texnologiyalarining afzalliklari va qo‘llanilishi yoritiladi. Shuningdek, amaliy yechimlar sifatida kiruvchi va chiquvchi trafikni tahlil qilish, siyosatlarni ishlab chiqish va real holatlarda firewall sozlamalari misollar bilan ko‘rsatiladi.*

Kalit so‘zlar: *tarmoqlararo ekran, trafikni boshqarish, xavfsizlik siyosati, NGFW, DPI, kiruvchi va chiquvchi trafik.*

УПРАВЛЕНИЕ ВХОДНЫМ И ИСХОДНЫМ ТРАФИКОМ ЧЕРЕЗ ИНТЕРНЕТ-ЭКРАНЫ: СОВРЕМЕННЫЕ ПОДХОДЫ И ПРАКТИЧЕСКИЕ РЕШЕНИЯ

Аннотация. *В статье подробно анализируются вопросы обеспечения безопасности сети и контроля входящего и исходящего трафика с помощью межсетевых экранов. Будут рассмотрены преимущества и области применения современных подходов, включая фильтрацию на основе состояния и контекста, глубокую проверку пакетов (DPI) и межсетевой экран нового поколения (NGFW). Кроме того, практические решения включают анализ входящего и исходящего трафика, разработку политик и настройку межсетевых экранов в реальных ситуациях с примерами.*

Ключевые слова: *сетевой межсетевой экран, управление трафиком, политика безопасности, NGFW, DPI, входящий и исходящий трафик.*

CONTROLLING INPUT AND OUTPUT TRAFFIC THROUGH INTERNET FIREWALLS: MODERN APPROACHES AND PRACTICAL SOLUTIONS

Abstract. *This article provides an in-depth analysis of the issues of ensuring network security through inter-network firewalls (firewalls), controlling incoming and outgoing traffic.*

The advantages and applications of modern approaches, including state-based and context-oriented filtering, Deep Packet Inspection (DPI), Next-Generation Firewall (NGFW), are discussed. Also, as practical solutions, the analysis of incoming and outgoing traffic, development of policies, and firewall settings in real situations are shown with examples.

Keywords: *inter-network firewall, traffic control, security policy, NGFW, DPI, incoming and outgoing traffic.*

Kirish

Zamonaviy raqamli muhitda axborot texnologiyalarining keskin rivojlanishi bilan bir qatorda, tarmoqlar orqali amalga oshiriladigan axborot almashinuvi hajmi ham keskin ortib bormoqda. Kompaniyalar, davlat idoralari, ta’lim muassasalari va shaxsiy foydalanuvchilar global internet tarmog‘iga ulanib, turli xizmatlardan foydalanmoqda.

Bu esa o‘z navbatida, tarmoq xavfsizligi muammosini birinchi darajali masalaga aylantirmoqda. Ayniqsa, ochiq va yopiq tarmoqlar o‘rtasidagi trafik oqimini tartibga solish, ularni tahlil qilish va xavf-xatarlardan himoya qilish zaruriyati tobora ortmoqda.

Tarmoqlararo ekranlar (firewall) – bu internet va lokal tarmoq o‘rtasida xavfsizlik devori bo‘lib xizmat qiladigan, ma’lumotlar oqimini monitoring qilish va kerakli darajada nazorat ostida ushlab turishga mo‘ljallangan vositadir. Ular nafaqat foydalanuvchilar faoliyatini cheklash, balki tarmoqqa bo‘layotgan tashqi tahdidlarni aniqlash va ularning oldini olishga xizmat qiladi. Har qanday tashkilotda tarmoq xavfsizligi strategiyasining asosi sifatida tarmoqlararo ekranlarning to‘g‘ri sozlanishi va samarali ishlatilishi muhim ahamiyat kasb etadi.

Hozirgi vaqtda kiberhujumlarning murakkablashgani, zararli dasturiy vositalarning diversifikatsiyalashgani va foydalanuvchi xatti-harakatlarining oldindan aytib bo‘lmasligi, tarmoq xavfsizligiga bo‘lgan talablarni ham sezilarli darajada oshirmoqda. Endilikda oddiy paket filtrlash tizimlari yetarli emas – ular o‘rnini zamonaviy, intellektual yondashuvlar egallamoqda.

Ayniqsa, Next-Generation Firewall (NGFW), Deep Packet Inspection (DPI), mashinali o‘rganish (Machine Learning) asosida ishlovchi tizimlar bugungi kunda yuqori samaradorlik ko‘rsatmoqda.

Mazkur maqolada aynan kiruvchi va chiquvchi trafikni zamonaviy tarmoqlararo ekranlar orqali boshqarish masalalari yoritiladi. Unga qo‘llanilayotgan texnologiyalar, siyosat ishlab chiqish uslublari, real amaliyotdagi yechimlar va xavfsizlikni ta’minlashdagi dolzarb yondashuvlar atroflicha tahlil qilinadi. Maqola nafaqat nazariy asoslarni, balki axborot xavfsizligini ta’minlashga doir amaliy tajriba va qo‘llanmalarning integratsiyasini ham o‘z ichiga oladi.

Tarmoqlararo ekranlar (firewall) haqida umumiy tushuncha

Tarmoqlararo ekranlar (firewall) – bu kompyuter tarmoqlarida xavfsizlikni ta’minlashga mo‘ljallangan dasturiy yoki apparat vositasi bo‘lib, ular tarmoqlararo (masalan, internet va lokal tarmoq o‘rtasida) axborot oqimini nazorat qiladi, ruxsat etilgan yoki taqiqlangan trafikni ajratib beradi hamda tashkilotning xavfsizlik siyosatiga mos holda qarorlar qabul qiladi.

Asosiy maqsad – xavfli yoki nomaqbul trafikni aniqlash, uning kirishiga yo‘l qo‘ymaslik hamda tarmoqdagi muhim resurslarni himoya qilishdan iborat. Firewalllar “signalizatsiya tizimi” rolini bajaradi: ular orqali har bir kiruvchi yoki chiquvchi paket kuzatilib, aniq qoidalarga asosan tahlil qilinadi va tegishli choralar ko‘riladi.

Tarmoqlararo ekranlarning vazifalari quyidagilardan iborat:

1. **Trafikni filtrlash** – ma’lum IP-manzillar, portlar, protokollar asosida ma’lumot paketlarini o‘tkazish yoki bloklash.
2. **Tarmoq chegaralarini himoyalash** – tashqi manbalardan bo‘ladigan hujumlar (DDoS, port scanning, spoofing) oldini olish.
3. **Xavfsizlik siyosatini amalga oshirish** – tashkilot siyosatida belgilangan qoidalarga muvofiq trafik oqimini boshqarish.
4. **Foydalanuvchilar faoliyatini nazorat qilish** – kim qayerga ulanmoqda, qanday kontentga kiryapti va nimalar yubormoqda, shu kabi harakatlarni monitoring qilish.
5. **Tarmoq hodisalarini loglash (log management)** – barcha trafik holatlarini yozib borish va ularni tahlil qilish imkonini yaratish.

Firewall'larning asosiy turlari va ishlash prinsiplari

Firewall texnologiyalari rivojlanib borishi bilan turli avlodlarga mansub ekranlar shakllandi. Ular orasida eng keng tarqalgan turlar quyidagilar:

1. Packet Filtering Firewall (Paket asosida filtrlovchi)

Bu eng oddiy tarmoq ekranidir. U ma'lumot paketining IP manzili, port raqami va protokoliga qarab qaror qabul qiladi. U paketlarning ichki mazmunini tahlil qilmaydi, faqat sarlavha (header) bilan ishlaydi.

Afzalliklari: Soddaligi, tez ishlashi.

Kamchiliklari: Murakkab tahdidlarni aniqlay olmaydi.

2. Stateful Inspection Firewall (Holatga asoslangan)

Bu turdagi firewall har bir aloqaning holatini kuzatib boradi (ya'ni, sessiyalarni tahlil qiladi). Paketlar faqat mavjud va ruxsat berilgan sessiyalarga tegishli bo'lsa, o'tkaziladi.

Afzalliklari: Dinamik nazorat, xavfsizroq.

Kamchiliklari: Resurs talab qiladi, murakkab konfiguratsiya.

3. Application-Level Firewall (Ilova darajasidagi)

Ushbu turdagi firewalllar ilovalar (masalan, HTTP, FTP, DNS) darajasida ish yuritadi.

Ular orqali aniq bir protokol doirasida ruxsat etilgan harakatlargina bajariladi.

Afzalliklari: Ilova asosida nazorat qilish imkoniyati.

Kamchiliklari: Sezilarli darajada tizim resursini talab qiladi.

4. Next-Generation Firewall (NGFW)

Bu keyingi avlod tarmoqlararo ekrani bo'lib, ilova identifikatsiyasi, foydalanuvchi identifikatsiyasi, kiruvchi trafikni tahlil qilish, zararli dasturiy ta'minotni aniqlash (malware detection) kabi ko'plab funksiyalarni o'z ichiga oladi. Shuningdek, ular Deep Packet Inspection (DPI) texnologiyasidan foydalanadi.

Afzalliklari: Kengaytirilgan xavfsizlik, chuqur tahlil, AI va ML integratsiyasi.

Kamchiliklari: Yuqori narx, murakkab texnik sozlamalar.

5. Web Application Firewall (WAF)

WAF – bu asosan veb-ilovalarni himoya qilishga mo'ljallangan maxsus ekran bo'lib, XSS, SQL injection, Cookie hijacking kabi hujumlarni aniqlaydi va bloklaydi.

Afzalliklari: Veb-xavfsizlikni kuchaytiradi.

Kamchiliklari: Faqat veb-ilovalar uchun mos.

Firewall'larning apparat va dasturiy shakllari

- **Apparatli (hardware) firewall** – bu maxsus qurilmalarda ishlaydigan, yuqori tezlikda ishlashga mo'ljallangan himoya vositalaridir. Ular yirik tashkilotlarda, ma'lumot markazlarida keng qo'llaniladi.
- **Dasturiy (software) firewall** – bu operatsion tizimga o'rnatiladigan yoki virtual muhitda ishlaydigan vositalar bo'lib, kichik tarmoqlarda, kompyuterlar yoki serverlarda keng tarqalgan.

Firewall'larning real tarmoqlardagi roli

Zamonaviy IT-infratuzilmada firewall'lar nafaqat chegara himoyachisi, balki:

- **Xavfsizlik siyosatini amalga oshiruvchi boshqaruv markazi**,
- **Xavf tahlilchisi**,
- **Trafik ma'lumotlarini yig'uvchi monitoring vositasi**,

- **Tizimdagi nojo‘ya harakatlarni aniqlovchi himoyachi** sifatida ishlaydi.

Firewall’larning to‘g‘ri konfiguratsiyasi, doimiy yangilanishi va log-fayllarning kuzatuvi ularning samaradorligini ta’minlovchi asosiy omillardir.

Zamonaviy yondashuvlar

1. Kontekstga asoslangan filtrlash (Context-aware filtering)

Bu yondashuvda nafaqat IP-manzil va portlar, balki foydalanuvchi shaxsiyati, joylashuvi, vaqt, ishlatilayotgan qurilma va ilovaning o‘zi hisobga olinadi. Bu esa xavfsizlik siyosatini yanada moslashuvchan qilishga yordam beradi.

2. Deep Packet Inspection (DPI)

DPI texnologiyasi paketlarning faqat sarlavhasini emas, balki butun tarkibini tahlil qilib, zararli dasturlarni aniqlash imkonini beradi. DPI orqali quyidagilar nazorat qilinadi:

- Ilova protokollari (HTTPS, FTP, VoIP);
- Fayl turlari;
- Shifrlangan trafik;
- Tarmoqdagi anomaliyalar.

3. NGFW – Keyingi avlod tarmoqlararo ekranlari

NGFW – bu an’anaviy tarmoqlararo ekranlarning imkoniyatlarini kengaytiruvchi texnologiya bo‘lib, quyidagi funksiyalarga ega:

- Ilovalarni identifikatsiyalash;
- Foydalanuvchi identifikatsiyasi;
- VPN tahlili;
- Integratsiyalashgan xavf tahlili va SIEM tizimlariga ulanish.

4. AI va Machine Learning asosidagi xavfsizlik

Yaqinda firewall tizimlariga sun’iy intellekt va mashinali o‘rganish algoritmlari joriy etilmoqda. Bu orqali ular mustaqil ravishda:

- Xavfli trafikni aniqlaydi;
- O‘zini moslashtiradi;
- Yangi tahdidlarni oldindan bashorat qiladi.

Kiruvchi va chiquvchi trafikni boshqarish amaliyoti

Kiruvchi trafikni boshqarish:

- IP Whitelisting – faqat ruxsat etilgan manzillarni qo‘yib yuborish;
- Port-based filtering – zarur portlargina ochiq bo‘lishi;
- IDS/IPS tizimlari integratsiyasi – tarmoqdagi tahdidlarni aniqlash va bloklash.

Chiquvchi trafikni boshqarish:

- URL Filtering – zararli yoki noxush kontentga chiqishni cheklash;
- Bandwidth Management – tarmoq o‘tkazuvchanligini maqbullashtirish;
- Ilova asosida boshqaruv – foydalanuvchi ma’lumotlarni qaysi ilova orqali yuborayotganini nazorat qilish.

Firewall siyosatlarini ishlab chiqish bosqichlari

1. **Tarmoq infratuzilmasini tahlil qilish.**
2. **Xavfsizlik talablari asosida siyosat tuzish.**
3. **Qoida ketma-ketligini aniq belgilash.**

4. **Qoidalarning real vaqtda sinovdan o‘tkazilishi.**
5. **Doimiy monitoring va loglar orqali tahlil.**

Xulosa

Tarmoqlararo ekranlar (firewall) bugungi kunda raqamli xavfsizlik tizimining ajralmas qismi hisoblanadi. Ular nafaqat axborot resurslarini tashqi tahdidlardan himoya qilish, balki tarmoq ichidagi harakatlarni ham nazorat qilish, kiruvchi va chiquvchi trafikni tahlil qilish, ma’lumotlar oqimini optimallashtirishda muhim rol o‘ynaydi. Zamonaviy xavflarning murakkablashuvi, tarmoqlardagi qurilmalarning ko‘payishi, mobil va bulut texnologiyalarining kengayib borishi firewall texnologiyalarining ham rivojlanishini taqozo etmoqda.

Next-Generation Firewall (NGFW), Deep Packet Inspection (DPI), sun’iy intellekt (AI) va mashinali o‘rganish (ML) asosida ishlovchi tarmoq xavfsizlik yechimlari bugungi kunda nafaqat xavfli trafikni aniqlash, balki uni oldindan prognozlash imkonini ham bermoqda. Shu bilan birga, samarali xavfsizlik siyosatini ishlab chiqish, uni doimiy ravishda yangilab borish, tarmoq faoliyatini monitoring qilish va foydalanuvchilar harakatlarini tahlil qilish orqali tarmoq xavfsizligi maksimal darajaga yetkazilishi mumkin.

Maqolada keltirilgan nazariy asoslar, amaliy yondashuvlar va texnologik vositalar har qanday tashkilot yoki IT mutaxassisi uchun tarmoqlararo ekranlarni to‘g‘ri tanlash, ularni samarali sozlash va xavfsizlik siyosatini amalga oshirishda muhim ko‘rsatkich bo‘lib xizmat qiladi. Yaqin kelajakda firewall texnologiyalarining avtomatlashtirilgan, aqlli va kontekstga asoslangan variantlari axborot xavfsizligini ta’minlashda markaziy o‘ringa ega bo‘lishi shubhasiz.

REFERENCES

1. **Stallings, W.** *Network Security Essentials: Applications and Standards*. Pearson Education, 2020.
2. **Chapple, M. & Seidl, D.** *CompTIA Security+ Study Guide Exam SY0-601*. Wiley, 2021.
3. **Zwicky, E.D., Cooper, S., Chapman, D.B.** *Building Internet Firewalls*. O'Reilly Media, 2000.
4. **Scarfone, K., & Hoffman, P.** *Guidelines on Firewalls and Firewall Policy* (NIST SP 800-41 Rev.1). National Institute of Standards and Technology, 2009.
5. **Cisco Systems.** *Cisco ASA Series Firewall Fundamentals*. Cisco Press, 2017.
6. **Gibson, D.** *Managing Risk in Information Systems*. Jones & Bartlett Learning, 2015.
7. **Alomari, E., Manickam, S., Gupta, B. B.** "A Review of the Limitations of Signature-Based Intrusion Detection Systems". *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 2016.
8. **Check Point Software Technologies Ltd.** *Firewall Best Practices Guide*. https://www.checkpoint.com
9. **Palo Alto Networks.** *Next-Generation Firewall Capabilities Overview*. https://www.paloaltonetworks.com
10. **Fortinet Inc.** *FortiGate NGFW Technical Guide*. https://www.fortinet.com