УДК 004.7

Жеребцов Д.В., здобувач,
Кухар А.А., здобувач,
Сергійко В.М., здобувач,
Рудюк Б.М., асистент
Державний університет «Житомирська політехніка»

РОЛЬ FIREWALL В СУЧАСНИХ МЕРЕЖАХ

Firewall (міжмережевий екран) від початків Інтернету є ключовим інструментом кібербезпеки, формуючи бар'єр між внутрішньою довіреною мережею та зовнішніми загрозами. Він контролює та фільтрує трафік відповідно до визначених правил безпеки, дозволяючи проходити лише легітимним даним. Сьогодні міжмережевий екран залишається першою лінією оборони проти кібератак як у традиційних, так і в сучасних мережах, захищаючи внутрішні системи від несанкціонованого доступу ззовні. Така система захисту є глобально визнаною і застосовується всюди – від персональних мереж до корпоративних центрів обробки даних і публічних мереж Wi-Fi.

Функціонально міжмережевий екран виконує фільтрацію та моніторинг мережевого трафіку, блокуючи небезпечні або неприпустимі з'єднання і пропускаючи лише дозволені пакети даних. Він може бути реалізований як апаратний пристрій на межі мережі або як програмне забезпечення на сервері чи кінцевому пристрої. Залежно від середовища використання розрізняють мережеві та хостові екрани. Перші працюють на виділеному обладнанні та захищають цілі сегменти мережі, тоді як другі встановлюються безпосередньо на комп'ютерах або серверах, у тому числі хмарних і контролюють трафік окремого вузла

Сучасний глобальний контекст мережевої безпеки ставить перед міжмережними екранами нові завдання. Попри появу додаткових засобів безпеки, міжмережні екрани продовжують еволюціонувати, щоб відповідати загрозам і умовам сьогодення.

Масовий перехід на хмарні сервіси змінив звичну модель безпеки та побудови корпоративних мереж. Критично важливі застосунки та дані тепер розміщені у публічних хмарах, а компанії використовують мультимодельні середовища. У результаті трафік все менше проходить через одну точку контролю, і потребується захист одразу в кількох периметрах. Сучасні міжмережеві екрани відповідають на цей виклик шляхом віртуалізації: з'явилися хмарні міжмережеві екрани, які можна розгортати в хмарній інфраструктурі, а також концепція Firewall-as-a-

Service, що дозволяє централізовано керувати політиками безпеки у хмарному середовищі.

Зростання кількості IoT-пристроїв формує новий фронт кібератак. Ці пристрої, часто зі слабким захистом, генерують великі обсяги даних і працюють у режимі постійного зв'язку, підвищуючи ризик компрометації. Тому мережеві екрани критично необхідні для їхньої безпеки. Сучасні екрани мають бути проактивними. Їхнє використання разом із сегментацією мережі дозволяє ізолювати небезпечний трафік та мінімізувати вплив потенційних атак.

Перехід до віддаленої роботи та концепції BYOD (Bring Your Own Device) призвів до того, що багато співробітників і пристроїв тепер знаходяться поза межами корпоративної мережі. Це кидає виклик традиційним підходам безпеки, адже потрібно захищати доступ до внутрішніх ресурсів із зовнішніх мереж. Новітні рішення дають змогу розширити периметр безпеки на будь-яке місце розташування користувача. Зокрема, модель Firewall-as-a-Service дозволяє охопити всіх авторизованих користувачів незалежно від їхнього місця перебування, часто у поєднанні з VPN, тим самим забезпечуючи захист віддалених офісів і працівників. Такий підхід підтримує концепцію нульової довіри, коли кожне з’єднання перевіряється, а міжмережевий екран виконує роль центрального пункту контролю політик доступу навіть поза межами фізичної офісної мережі.

Незважаючи на швидку еволюцію IT-інфраструктури, міжмережеві екрани продовжує відігравати провідну роль у захисті персональних, корпоративних і публічних мереж. Водночас, сучасні міжмережні екрани значно розширили свої можливості: вони поєднують функції глибокої інспекції пакетів, виявлення вторгнень, веб-фільтрації та інших сервісів, аби протидіяти передовим загрозам.

Отже, міжмережеві екрани продовжують бути ключовим елементом кібербезпеки, адаптуючись до глобальних викликів і залишаючись ефективним інструментом захисту для мереж користувачів у сучасну епоху.

Список використаних джерел:

1. Raja Waseem Anwar, Tariq Abdullah and Flavio Pastore. Multidisciplinary Digital Publishing Institute. Firewall Best Practices for Securing Smart Healthcare Environment. 2021. https://doi.org/10.3390/app11199183

2. Cisco. The Future of the Firewall White Paper. 2019. URL: https://www.cisco.com/c/en/us/products/collateral/security/firewalls/ngfw-futureoffirewalling-wp.html