Мережеві екрани: що новенького

«Хмарно-нативні» мережеві екрани входять у моду, але й «залізні» платформи продовжують щороку оновлюватися.

Термін «мережевий екран наступного покоління» (NGFW) з'явився більш ніж десять років тому і за цей час втратив свою «наступність». Змінилися й підходи до захисту корпоративних ресурсів через віддалену роботу, зокрема й з-за кордону, та міграцію цих ресурсів до хмар. Окрім того, з'явилися або набули поширення численні інші інструменти кіберзахисту. Мережевий екран залишається важливим елементом архітектури безпеки, але теж зазнає змін, зокрема виробники пропонують рішення як для локального використання, так і для захисту в хмарі або й навіть мережевий екран як сервіс (FWaaS).

Слід сказати, що аналітики, та й почасти самі виробники потроху відходять від терміну «мережевий екран наступного покоління». Адже від появи цього терміну минуло вже понад два десятиліття. Gartner, який його і вигадав, тепер у своїх дослідженнях використовує просто назву «мережевий екран» (Network Firewall), деінде можна зустріти терміни «корпоративний екран» (Enterprise Firewall) або «захисний екран» (Secure Firewall).

«Магічний квадрант» Gartner

Різні організації періодично проводять оцінювання і порівняння брендів мережевих екранів. Мабуть, найвідоміша з них – це Gartner зі своїм дослідженням Magic Quadrant for Network Firewalls, найсвіжіше було оприлюднене у грудні минулого року.

За визначенням Gartner, мережевий екран повинен мати низку ключових можливостей. Список включає мережеві функції, зокрема підтримку таблиць маршрутизації і перетворення статичних мережевих адрес; інспекцію трафіку зз урахуванням стану з'єднань (stateful inspection); виявлення та дослідження загроз, у тому числі запобігання вторгненням (IPS) і аналіз зловмисного ПО; фільтрацію веб-трафіку; потужні можливості ведення журналів і генерування звітів. Додатково мережевий екран може підтримувати функції захисту IoT-пристроїв, пісочниці, захист операційних технологій (OT) і DNS, доступу з нульовою довірою (ZTNA), а також SD-WAN.

Gartner зазначає, що ринок мережевих екранів залишається одним з найбільших ринків рішень у галузі кібербезпеки і еволюціонує разом з загальним безпековим ринком. Зокрема, поширення гібридних середовищ спричинило появу нових моделей впровадження мережевих екранів. Це хмарні (cloud-native), FWaaS («мережевий екран як послуга», тобто багатофункціональний шлюз, який надається як хмарний сервіс, зокрема для захисту невеликих офісів та мобільних користувачів), а також гібридні платформи типу Mesh, які забезпечують контроль трафіку в багатьох територіально рознесених точках, але з централізованим управлінням через хмару.

Gartner прогнозує, що до 2026 року 60% організацій будуть використовувати більш ніж одну модель впровадження мережевого екрану, що стимулюватиме поширення гібридних моделей. Окрім того, понад 30% мережевих екранів у філіях компаній будуть за моделлю FWaaS (проти 10% у 2022-му).

Інтерес до моделі безпеки з нульовою довірою (Zero Trust) спонукає замовників до вибору рішень від єдиного виробника, який може надати усі рішення для створення архітектури ZTNA, щоб їм не доводилось використовувати продукти різних вендорів. При цьому замовники, обираючи виробника, розраховують на тісну інтеграцію з іншими продуктами, функції яких також закриваються мережевим екраном.

Gartner відносить до квадранту лідерів компанії Fortinet, Palo Alto Networks і Check Point Software Technologies. Четвірку претендентів склали Cisco, Juniper, Huawei і, що цікаво, Alibaba Cloud. Нагадаємо: Gartner оцінює виробників за наборами критеріїв «виконавча спроможність» (функціональні можливості продукту і його підтримка, ціноутворення, гнучкість ринкової стратегії тощо) і «повнота візії» (розуміння потреб ринку, стратегія маркетингу, географічне охоплення тощо).

«Хвиля» Forrester

Компанія Forrester оцінює виробників за трьома групами критеріїв: поточна пропозиція (технічні параметри і можливості продукту), стратегія (план розвитку і його виконання, супутні продукти, модель постачання тощо) і ринкова присутність (дохід, динаміка продажів та база встановлених пристроїв). «Хвиля» являє собою фрагменти концентричних кілець у куті квадрата, де вертикальна вісь відповідає силі поточної пропозиції, горизонтальна – стратегії, а компанії відображаються у вигляді кругів, розмір яких відповідає ринковій присутності. Внутрішнє кільце зарезервоване для лідерів ринку, за ним розташовуються «сильні гравці» (Strong Performers), а ще далі дві категорії компаній, назви яких перекладемо як «ближні претенденти» і «дальші претенденти» (Contenders і Challengers).

Отже, у дослідженні Forrester Wave: Enterprise Firewalls. Q4 2022, яке було опубліковане у жовтні минулого року, до лідерів віднесено знову-таки Palo Alto, Fortinet і Check Point Software Technologies. Сильними гравцями названо Cisco, Juniper Networks, Sophos, і на межі – SonicWall. Barracuda Networks, Watchguard і Forcepoint зараховано до ближніх претендентів.

Forrester зазначає, що Palo Alto винайшла NGFW і першою запропонувала хмарні мережеві екрани на платформах AWS та Google Cloud, має одну з найкращих функціональностей дешифрування TLS, а один з опитаних покупців заявив, що «пристрій працює за чотирьох [конкурентів]», водночас замовники нарікають на високу вартість підписок. Fortinet бере співвідношенням «ціна/якість», API-центричністю, що допомогло збудувати потужну партнерську екосистему, і активною техпідтримкою. Check Point зосередився на технологіях запобігання загрозам, щоб його продукти могли захищати бізнеси, які не мають центрів управління кібербезпекою (SOC) та відповідних фахівців. Користувачі хвалять гарну підтримку, інтуїтивно зрозумілий інтерфейс і нову послугу FWaaS.

Серед трендів Forrester відзначає надання виробниками послуг клієнтам, таких як SOCaaS (центр управління кібербезпекою як послуга), виявлення та знешкодження загроз.

«Кібер-рейтинг»

Неприбуткова організація CyberRatings.org продовжує справу, започатковану колись NSS Labs. У квітні вона оприлюднила результати дослідження мережевих екранів за критеріями ефективності захисту і сукупної власності володіння. Враховувались, зокрема, такі характеристики, як запобігання використанню вразливостей і обходів

захисту, рівень хибно-позитивних сповіщень, дешифрування TLS/SSL, пропускна здатність і стабільність роботи при високому завантаженні.

З восьми протестованих рішень шість потрапили до області «рекомендованих». Найвищу ефективність захисту продемонстрував мережевий екран Juniper SRX4600, який зумів заблокувати 1723 з 1724 атак через вразливості, що відповідає показнику у 99,94%. Проте це рішення виявилось і доволі дорогим. Мережевий екран FortiGate 600F від Fortinet заблокував 99,88% атак, Forcepoint 2205 і Versa Networks CSG5000 – 99,48%, але при цьому останній має найнижчу вартість захисту в обрахунку на 1 Мбіт/с: $2,55. Рішення Fortinent і Versa, які на діаграмі розташувались дуже близько одне до одного, можна вважати переможцями цих перегонів. Загалом рейтинг рекомендованих отримали 6 продуктів, ефективність яких виявилась у діапазоні 94,05%–99,94%.

У висновках CyberRating зауважує, що наразі 80% веб-трафіку шифрується, але при цьому у мережевих екранах дешифрування не ввімкнено за умовчанням, тож якщо екран не налаштований відповідним чином, атак через HTTPS він просто не побачить. А при увімкненому дешифруванні пропускна здатність пристрою суттєво падає – під час тестів середня швидкість була на рівні 65–86,5% від незашифрованого трафіку.

Також у багатьох мережевих екранах не увімкнено за умовчанням протидію обходам захисту, а у деяких знайшлися прогалини, які «викликають стурбованість». Якщо мережевий екран блокує відомий експлойт, атакуючій стороні простіше вигадати техніку обходу, ніж шукати нову вразливість. Дослідники виявили, що для багатьох поширених вразливостей існує по кілька правил і сигнатур, з яких деякі ефективніші за інші. Це свідчить про намагання посіхом закрити не дуже зрозумілу вразливість, що призводить до появи неефективних сигнатур або таких, які спричиняють хибні спрацювання.

Впродовж 2022 року CyberRatings проводив ще одне дослідження, перше у своєму роді, а саме – порівняльні тести хмарних мережевих екранів. Організація знову-таки випробувала продукти восьми виробників, з яких п'ять (Check Point, Forcepoint, Fortinet, Juniper і Versa) отримали найвищий рейтинг. Тести проходили на платформі AWS і включали 977 тестових експлойтів та 35 технік обходу. Оцінки ефективності захисту виявилися в межах 27–100%, при цьому рівень блокування експлойтів був у межах 88,3–100%, а щодо технік обходу, то тут усі продукти показали стовідсоткову опірність.

CyberRatings зазначає, що виробники систем безпеки звикли контролювати платформи, на яких ті працюють, але у хмарі вони цього контролю не мають. Тож мусять пристосовуватись до роботи в новому середовищі, а на цьому шляху можуть бути труднощі. «Безпека – це ваша проблема, а не *Amazon*, – прокоментував президент CyberRating Вікрам Фатак. – Якщо ви переносите дані зі свого ЦОД до хмари, розробіть план, як їх захистити. І якщо вам у дата-центрі потрібен мережевий екран, то, ймовірно, він знадобиться і в хмарному середовищі».

Таблиця 1. Основні виробники мережевих екранів та їхні українські партнери у 2023 році

Виробник	Країна	Дистриб'ютори	Партнери	Статус
Check Point	Ізраїль	MUK	IT Specialist	Elite
			Svit IT	4 Stars
			ITBiz, Сембер Трейд	3 Stars
			18 компаній	2 Stars
Cisco (категорія «Безпека»)	США	ERC, MUK, Мегатрейд	17 компаній	Gold Integrator
			10 компаній	Premier Integrator
			5 компаній	Select Integrator
Fortinet	США	ERC, MUK	LAN Systems	Expert Partner
			IT Specialist, Netwave, PF Service, Smart Net	Advanced Partner
			21 компанія	Select
Juniper Networks	США	MUK	Interklast	—
Palo Alto Networks	США	MUK, БАКОТЕК	RMRF Services	PSDP (професійні послуги)
			8 компаній	Innovator/Reseller
Sophos	Великобританія	Abitek Distribution	4 компанії	—
Watchguard	США	БАКОТЕК	—	—

Світовий ринок NGFW зростає

Що стосується суто ринкових показників, то агенція Mordor Intelligence прогнозує, що протягом 2020-х років світовий ринок NGFW зростатиме в середньому по 12% на рік. Однією з ключових причин є дедалі більше поширення «Інтернету речей». Окрім того, після гучних кібератак уряди країн виділяють кошти на посилення кібербезпеки. Головним стримуючим фактором є відносно висока вартість цих систем, які можуть собі дозволити тільки великі компанії, на додачу малий бізнес консервативний і тримається за свої застарілі технології.

Цікаво, що лідерів світового ринку Mordor Intelligence перелічує в такому порядку: 1) Juniper; 2) Palo Alto; 3) Dell; 4) Huawei; Fortinet.

В **табл. 1** наведені ключові виробники мережевих екранів, які присутні на українському ринку, а також їхні дистриб'ютори та ключові партнери. Інформацію про партнерів та їхні статуси взято з офіційних сайтів виробників.

Мережеві екрани в металі і в хмарі

Хоча аналітики стверджують про неминуче переселення мережевих екранів до хмари слідом за даними користувачів, апаратні пристрої нікуди не поділися, як і локальна модель розгортання (On-Prem).

У **табл. 2** наведені основні параметри деяких мережевих екранів чотирьох виробників: найпростішої і найпотужнішої моделей, а також тієї, яка проходила тестування у лабораторії CyberRatings (Palo Alto у лютому цього року оголосила про завершення продажів серії PA-3200, до якої належала модель зі списку тестування, тому замість неї долучено модель з іншої серії, PA-3410). У таблиці вказані величини продуктивності в чотирьох режимах: звичайного фаєрвола (деякі виробники вказують значення при увімкненій функції розпізнавання трафіку застосунків), IPS, власне NGFW (мережевий екран, контроль застосунків і IPS) і повного запобігання загрозам (Threat Prevention), куди також входять додаткові функції, такі як розширений аналіз шкідливого ПО у пісочниці, протидія шпигунським програмам і т.д. Дані узято з сайтів виробників.

Цифри, можливо, не є цілковито зіставними, бо компанії по-різному вимірюють пропускну здатність, а також загалом є дуже багато інших важливих параметрів (наприклад, затримка, пропускна здатність при увімкненому дешифруванні, яка буде меншою, кількість підтримуваних правил тощо), проте вони дають уявлення про продуктивність цих пристроїв і про те, як вона змінюється при збільшенні числа завдань.

Лінійки мережевих екранів продовжують розвиватися. Взимку минулого року ***Check Point*** представив, за власним твердженням, серію найшвидших у світі фаєрволів – Quantum Lightspeed (один з них, до речі, потім тестували в лабораторії CyberRatings). Оскільки мережевий трафік у світі подвоюється щотрироки, зазначав у своєму блозі виробник, великі корпорації мусять якось забезпечити захист трафіку на тій самій швидкості, з якою він передається в мережі. Check Point долучив до розробки нової лінійки компанію NVIDIA, чия мережева карта ConnectX узяла на себе інспекцію трафіку з урахуванням стану з'єднань (stateful inspection). Лінійка Lightspeed складається з чотирьох моделей, які мають максимальну пропускну здатність від 250 до 800 Гбіт/с і можуть масштабуватися до

Таблиця 2. Параметри деяких апаратних мережевих екранів Check Point, Cisco, Fortinet і Palo Alto

Модель	Продуктивність у режимі мережевого екрану	Продуктивність у режимі IPS	Продуктивність у режимі NGFW	Продуктивність у режимі Threat Prevention	Кількість одночасних сесій	Кількість нових сесій на секунду	Формфактор
Check Point Quantum Spark 1500 Pro	2000 Мбіт/с[1]	670 Мбіт/с	600 Мбіт/с	440 Мбіт/с	1 млн	10 тис.	Desktop
Check Point Quantum QLS250 Lightspeed	250 Гбіт/с	79,8 Гбіт/с	53,2 Гбіт/с	16,65 Гбіт/с	32 млн	430,8 тис.	2U
Check Point Quantum 28600 Hyperscale	193 Гбіт/с	52,5 Гбіт/с	51,5 Гбіт/с	30 Гбіт/с	49 млн	590 тис.	2U Масштабування до 8 груп по 31 пристрою
Cisco Firepower 1010 FTD	890 Мбіт/с[2]	900 Мбіт/с	880 Мбіт/с	н/д	100 тис.	6 тис.	1U
Cisco Firepower 2130 FTD	10 Гбіт/с	5,4 Гбіт/с	5,4 Гбіт/с	н/д	2 млн	30 тис.	1U
Cisco 3×SM-56 FTD	235 Гбіт/с	190 Гбіт/с	190 Гбіт/с	н/д	60 млн	1 млн	3U
Fortinet Fortigate FG-40	5/5/5 Гбіт/с[3]	1 Гбіт/с	800 Мбіт/с	600 Мбіт/с	700 тис.	35 тис.	Desktop
Fortinet FortiGate FG-600F	139/137,5/70 Гбіт/с	14 Гбіт/с	11,5 Гбіт/с	10,5 Гбіт/с	8 млн	550 тис.	1U
Fortinet FortiGate 7122F	1,89/1,88,1,129 Тбіт/с	675 Гбіт/с	550 Гбіт/с	520 Гбіт/с	1 млрд	9 млн	16U
Palo Alto P-410[4]	1,59/1,1 Гбіт/с[5]	н/д	н/д	0,6/0,68 Гбіт/с	64 тис.	12 тис.	Desktop
Palo Alto P3410	14,1/11 Гбіт/с	н/д	н/д	5,1/5,6 Гбіт/с	14 млн	145 тис.	1U
Palo Alto PA-7080	567/595 Гбіт/с	н/д	н/д	292,4/312,8 Гбіт/с	416 млн	6 млн	19U

[1] У Check Point 1518 байт, UDP

[2] У Cisco режим мережевого екрану з видимістю і контролем трафіку застосунків (AVC), 1024 байти

[3] У Fortinet 1518/512/64 байт, UDP

[4] У всіх рішеннях Palo Alto 64 КБ, HTTP/ змішаний трафік застосунків

[5] У Palo Alto режим мережевого екрану з визначенням трафіку застосунків(App-ID)

Рис. 1. Одна з моделей Check Point Quantum Lightspeed

Рис. 2. FortiGate FG4000F

3 Тбіт/с. Окрім того, забезпечується надмала затримка на рівні 3 мкс (**рис. 1**).

Fortinet, теж не пасучи задніх, у серпні 2022 року представив «найшвидший у світі компактний мережевий екран» FortiGate FG4000F для гіпермасштабних дата-центрів та 5G (**рис. 2**). Серія складається з двох моделей, які мають на боту 16 мережевих процесорів Fortinet NP7. Заявлена максимальна пропускна здатність у режимі «голого» фаєрвола на рівні 2,4 Тбіт/с, у режимі захисту від загроз – 70 Гбіт/с, SSL-інспекції – 55 Гбіт/с. Пристрої мають порти 400G, що забезпечує швидкий і захищений інтерконет між дата-центрами.

Цілий пакет новинок було представлено ще раніше, у травні 2022 року. Це шлюзи FortiGate FG600 з підтримкою стратегії «нульової довіри» для кампусних мереж, їх створено для підприємств, які повертають працівників до офісів, але прагнуть підтримувати і персонал з гібридним режимом роботи. Для малих офісів та філій випущено шлюзи FortiGate 70F, які перетворюють WAN у SD-WAN. А лінійка для дата-центрів FortiGate 3700F відрізняється наднизькою затримкою на рівні 2 мкс і має інтегровану політику ZTNA.

Ще з новинок у листопаді було анонсовано серію FortiGate 1000, яка, за твердженням виробника, потребує на 83% менше потужності в обрахунку на 1 Гбіт/с пропускної здатності, аніж в середньому по галузі. Також система охолодження споживає на 15% менше в одиницях теплової потужності на годину.

Palo Alto продовжує заміщення свого асортименту мережевими екранами «четвертого покоління». Наприкінці минулого року компанія вивела на ринок одразу кілька новинок. По-перше, це високопродуктивна платформа PA-5440, яка має пропускну здатність у режимі Threat Prevention до 61,5 Гбіт/с. Пристрій призначений для великих кампусних мереж і дата-центрів, де архітектура Zero Trust вимагає повної фільтрації трафіку на прикладному рівні.

Рис. 3. NGFW 4 покоління Palo Alto PA1420

Нова серія PA-1400 складається з двох моделей: PA1410 і PA-1420 (**рис. 3**), які мають пропускну здатність в режимі екрану з контролем застосунків відповідно 6,8 і 9,5 Гбіт/с. Ця серія розрахована на великі філії і мережі підприємств з невеликою територією. А пристрої PA-445 і PA-415 призначені для СМБ і територіально рознесених підприємств. Усі представлені мережеві екрани працюють з новою операційною системою PAN-OS 11.0 Nova і з машинним навчанням. За твердженням виробника, вміють зупиняти атаки через вразливості нульового дня «з нульовим часом».

Що стосується хмарних продуктів, то у травні цього року Check Point представив інтеграцію свого хмарного мережевого екрану CloudGuard з NaaS-сервісом Microsoft Azure Virtual WAN, що має доповнити власні безпекові механізми Azure і забезпечити багатошаровий захист у хмарних середовищах. Приблизно тоді ж для користувачів Azure став доступний хмарний сервіс Palo Alto Cloud NGFW. Ще з весни минулого року сервіс віртуальних NGFW працює на платформі AWS. Fortinet запустив хмарний сервіс FortiGate CNF на платформі AWS у листопаді 2022-го. Зрештою, хочемо того чи ні, а все переходить у хмару.