Периметр щезає, а NGFW — ні

Попри деякі твердження, мережевий екран не вмер, але його роль потроху змінюється.

Мережеві екрани наступного покоління (NGFW) поєднують у собі цілу низку функцій захисту: антивірус, пісочниця, запобігання вторгненням, веб-фільтрація, перевірка шифрованого трафіка тощо. Попри назву, ці системи давно досягли зрілості, і подекуди можна почути, що вони невдовзі вимруть, звільнивши місце для більш актуальних рішень. Проте NGFW продовжують розвиватися, всотуючи такі технології та концепції, як машинне навчання, SASE і Zero Trust. Пандемія коронавірусу ще більш посилила тренд на використання хмарних рішень і моделі FWaaS.

«СіБ» розбирався, як змінились технології за останні два роки і що нового з'явилося в арсеналі виробників у 2020-му.

Останні тести NSS Labs

Компанія NSS Labs, яка впродовж багатьох років проводила тестування рішень кіберзахисту, торік несподівано припинила свою діяльність, пославшись на негативний вплив пандемії. Востаннє результати групового тестування NGFW були оприлюднені влітку 2019 року. Рішення від різних виробників оцінювалися за критеріями ефективності захисту і сукупної вартості володіння в розрахунку на 1 Мбіт/с трафіка, який захищається.

З-поміж 12 продуктів, що брали участь у випробуваннях, 10 було названо «рекомендованими». При цьому найвищу ефективність показало рішення ***Palo Alto Networks*** (97,9%), яке, втім, виявилося і найдорожчим. Найдешевшим же виявилося рішення ***Huawei***.

У своїх висновках NSS Labs відзначала, що NGFW здебільшого використовуються для захисту кінцевих користувачів (а не дата-центрів). Окрім того, деякі підприємства використовують шлюзи для внутрішньої сегментації мереж. Важливо, що у Web 3.0 трафік різних програм прямує через порти, які досі були зарезервовані лише для однієї функції (наприклад, HTTP), і тому на додачу до контролю портів і адрес призначення потрібен аналіз трафіка на рівні застосунків.

Компанія вказала, що з 2007 року спостерігається суттєве зростання кількості атак, які починаються на стороні користувача (наприклад, як результат відвідання інфікованих веб-сайтів). Такі атаки традиційно вважалися зоною відповідальності антивірусних продуктів, але, оскільки NGFW найчастіше використовуються для захисту робочих станцій, шлюзи повинні забезпечувати комплексний захист від таких атак. При цьому дослідження показало, що більшість компаній змушені підтримувати розмаїтий набір клієнтських застосунків, а IT-відділи часто не в змозі відслідкувати, які саме програми працюють на робочих станціях. Оскільки через це точно налаштувати NGFW на захист конкретних застосунків неможливо, зазвичай краще підтримувати повний набір сигнатур.

NSS Labs вказала, що при виявленні нових вразливостей виробники намагаються якнайшвидше їх закрити. Проте надто поквапні спроби можуть призводити до появи сигнатур, які є неточними, неефективними і спричиняють хибну тривогу. У той же час, всупереч загальним переконанням, найбільший ризик не завжди становлять ті вразливості, про які повідомляється в останніх патчах, оскільки давніше зловмисне ПО продовжує циркулювати і становити загрозу. При цьому буває, що виробники видаляють старі сигнатури, щоб збільшити пропускну здатність продукту, це теж може призводити до нерівномірного закриття старих вразливостей.

Також NSS Labs звернула увагу на технології ухилення від механізмів виявлення і блокування атак. Результативність захисту може бути оманливою, якщо не враховувати ухилення, і чим більше класів ухилень пропущено, тим менш ефективним є захист. Наприклад, краще, коли пропущені усі техніки з однієї категорії методів ухилення (скажімо, у трафіку FTP), аніж по одній техніці з кожної категорії, оскільки це збільшує поверхню атаки. При цьому найбільше знижують ефективність захисту техніки обходу, що працюють на нижніх рівнях OSI, оскільки вони потенційно зачіпають більшу кількість вразливостей.

За результатами тестування найвищий відсоток блокування атак (99%) показали продукти ***Fortinet*** і ***Versa***

Таблиця 1. Основні виробники систем NGFW та їхні українські партнери у 2020 році

Виробник	Штаб-квартира	Представництво в Україні	Дистриб'ютори	Партнери	
				Назва компанії	Статус
Check Point	Ізраїль	+	МУК	IT Specialist, Svit IT	Check Point Star Partner **** (найвищий)
				Infosafe, Intergrity Vision	Check Point Star Partner ***
				20 компаній	Check Point Star Partner **
Cisco	США	+	ERC, Мегатрейд, МУК	11 компаній	Gold
				10 компаній	Premier
				9 компаній	Select
Forcepoint	США	-		IBM, ISSP, Intrasystems	
Fortinet	США	+	МУК, ERC	LAN Systems, Netwave, PF Service, Смарт Нет	Advanced
				11 компаній	Select
Juniper	США		RRC, МУК	Interclast, Intrasystems	-
Palo Alto	США	-	БАКОТЕК, МУК	49 компаній	Innovator
Watchguard	США	-	БАКОТЕК	-	-

Networks, тоді як рішення ***Palo Alto*** і ***WatchGuard*** продемонстрували стовідсоткове розпізнавання технік обходу. Пізніше рішення ***Forcepoint*** було протестовано з новою версією ПО, і воно показало рівень блокування 99,4% при стовідсотковому виявленні ухилень.

Оцінки Gartner і Forrester

Gartner свій останній «магічний квадрант» мережевих шлюзів оприлюднив у листопаді минулого року. До лідерів віднесені ***Palo Alto Networks***, ***Fortinet*** і ***Check Point***, до претендентів — ***Cisco***, ***Juniper Networks*** і ***Huawei***, візіонерами названі ***Forcepoint*** і ***Sophos***.

У своєму аналізі Gartner зазначає, що з початком пандемії COVID-19 і переведенням співробітників на віддалену роботу підприємства зіткнулися з необхідністю модернізації інфраструктури, що, зокрема, справило позитивний вплив і на ринок мережевих екранів. Стрибкоподібне зростання вхідного трафіка, що надходив через VPN, змусило дата-центри закупити більш потужне обладнання. Водночас прискорилося впровадження моделі «екран як послуга» (FWaaS), що забезпечує швидке підключення і налаштування доступу з дому; окрім того, замовники активно обирають хмарні безпекові рішення. Ще одним трендом став перехід до концепції мережевого доступу з нульовою довірою (Zero Trust Network Access).

Агенція підкреслює, що економічна рецесія змусила великі компанії укрупнювати філії і переводити ресурси у хмару, а також консолідувати парк обладнання, закуповуючи різні системи захисту в одного виробника. Загалом Gartner прогнозує, що до 2024 року 30% філій компаній користуватимуться послугою FWaaS (порівняно з 5% у 2020 році), а також що 2024 року 25% витрат на мережеві екрани входитимуть до більш всеохопних контрактів на закупівлю «платформ» безпеки відповідно до корпоративних ліцензійних угод (також порівняно з торішніми 5%).

Компанія ***Forrester*** оцінює виробників мережевих екранів за 34 критеріями, які групуються у 3 загальні категорії: нинішня пропозиція (технічні характеристики пристроїв і інтеграція з суміжними рішеннями безпеки), стратегія (дорожня карта, зокрема, у тому, що стосується впровадження концепції Zero Trust) і присутність на ринку (дохід і кількість корпоративних клієнтів з понад 5000 працівників). Згідно з торішнім звітом Forrester Wave: Enterprise Firewalls, за першими двома групами критеріїв до лідерів віднесені Palo Alto і Cisco, до «сильних гравців» — Check Point, Fortinet, Huawei, Forcepoint і Sophos. При цьому за ринковою присутністю лідирують Cisco, Palo Alto і Fortinet, дещо меншу мають Check Point і Huawei.

Мережеві екрани на українському ринку

Основні виробники NGFW, а також їхні місцеві дистриб'ютори і партнери представлені в **табл. 1.** Ключовими гравцями, як і власне у світі, є Palo Alto, Cisco, Check Point і Fortinet.

У табл. 2 наведені основні параметри деяких мережевих екранів чотирьох виробників: найпростішої і найпотужнішої моделей, а також певного середнього пристрою, що його тестувала NSS Labs (або близького, оскільки відтоді минуло вже два роки, і подекуди лінійки суттєво оновилися). У таблиці вказані величини продуктивності в трьох режимах: звичайного фаєрвола (деякі виробники вказують значення при увімкненій функції розпізнавання застосунків), 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. В цифрах, що їх надають компанії, трафік вимірюється по-різному. Наприклад, Palo Alto дає два значення продуктивності: для 64K HTTP і для змішаного трафіка різних додатків, обидва значення наведені в таблиці (три нижні рядки) через скісну риску.

Далі поглянемо, що нового з'явилось у виробників NGFW.

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

Модель	Продуктивність у режимі мережевого екрану	Продуктивність у режимі NGFW (мережевий екран, контроль застосунків і IPS)	Продуктивність у режимі захисту від загроз (Threat Prevention)	Кількість одночасних сеансів	Кількість нових сеансів на секунду
Check Point Quantum Spark 1530	1 Гбіт/с	600 Мбіт/с	340 Мбіт/с	10,5 тис.	500 тис.
Check Point Quantum 6600	18 Гбіт/с	6,2 Гбіт/с	3,7 Гбіт/с	116 тис.	8 млн
Check Point Quantum 28600 Hyperscale	145 Гбіт/с	51,5 Гбіт/с	30 Гбіт/с	590 млн	49 млн
Cisco ASA 5506+FTD	250 Мбіт/с (з App-ID)	125 Мбіт/с	н/д	50 тис.	3 тис.
Cisco Firepower 9300 з 3 модулями SM-56 і образом ASA	235 Гбіт/с	н/д	н/д	195 млн	4,75 млн
Fortinet FortiGate 30E	950 Мбіт/с	200 Мбіт/с	150 Мбіт/с	900 тис.	15 тис.
Fortinet FortiGate 500E	36 Гбіт/с	5 Гбіт/с	4,7 Гбіт/с	8 млн	300 тис.
Fortinet FortiGate 7121F	1,89 Тбіт/с	550 Гбіт/с	520 Гбіт/с	1 млрд	9 млн
Palo Alto PA-220	575 / 540 Мбіт/с (з App-ID)	н/д	275 / 320 Мбіт/с	640 тис.	4,3 тис.
Palo Alto Networks PA-5220	16 / 18 Гбит/с (с App-ID)	н/д	8,2 / 10 Гбит/с	4 млн	150
Palo Alto PA-7080	644 / 700 Гбіт/с (з App-ID)	н/д	342 / 430 Гбіт/с	416 млн	4 млн

«Квантовий» захист Check Point

Родина мережевих екранів («шлюзів безпеки») ізраїльської компанії Check Point входить до архітектури безпеки Infinity, яка також включає в себе пісочниці SandBlast, пристрої захисту від DDoS-атак DDoS Protector і систему оркестрування Quantum Maestro для кластеризації NGFW. Самі мережеві екрани складають оновлену родину Quantum Security Gateways, яку було представлено рік тому. Мережеві екрани (за визначенням Check Point) призначені для захисту від «кібератак п'ятого покоління», тобто складних багатовекторних атак типу WannaCry і NotPetya, у яких використовуються високорозвинені зловмисні програми.

Функціональність мережевих екранів включає функцію перевірки у хмарній пісочниці SandBlast Threat Emulation, яка, за твердженням виробника, виявляє зловмисне ПО на етапі експлойту (використання вразливості) ще до того, як воно встигне застосувати технології ухилення для обману пісочниці. Інший інструмент, SandBlast Threat Extraction, вилучає з файлів потенційно вразливі елементи і надає користувачам вже знешкоджений контент.

До сімейства Quantum Security Gateways входять мережеві екрани на будь-який смак і масштаб. Наприклад, серія Quantum Spark 1500 для малих і віддалених офісів містить 4 моделі з пропускною здатністю 340–660 Мбіт/с у режимі Threat Prevention, мають 6 або 10 портів GE, підтримують Wi-Fi, деякі також можна підключити по DSL або LTE. Для використання у промислових середовищах розроблено стійкий до вібрацій, екстремальних температур (від -40 до +75 °C) і електромагнітних впливів пристрій Quantum Rugged 1570R, який має 8 LAN-портів GE і може комплектуватися модемом Wi-Fi або 3G/4G. У верхній частині спектру перебувають нові платформи 26000 і 28000 (**рис. 1**) для великих дата-центрів і телекомунікаційних операторів, вони забезпечують відповідно 24 і 30 Гбіт/с у режимі Threat Prevention і мають високу щільність портів: від 66×1 GE до 16×100/25 GE.

Рис. 1. Check Point Quantum 28600

Цікавою особливістю рішення Check Point є можливість об'єднання мережевих екранів у великі кластери за допомогою системи оркестрування Maestro. В екстремальному варіанті 52 пристрої Quantum 28000 утворюють кластер із загальною пропускною здатністю 1,5 Тбіт/с в режимі Threat Prevention, при цьому можна почати з невеликої конфігурації, а потім за потреби додавати або відключати пристрої. Оркестратор дозволяє створювати захищені групи, кожну з яких система управління бачить як єдиний віртуальний шлюз, і динамічно перерозподіляти обчислювальні ресурси всередині цих груп або між ними.

Check Point також надає послуги FWaaS, зокрема, пропонуючи використовувати хмарний шлюз безпеки спільно з SD-WAN: завдяки цьому оптимізація розподілу трафіка в SD-WAN не обмежуватиметься необхідністю пропускати його через централізований апаратний шлюз.

Чотири серії Cisco

Cisco має в своєму арсеналі одразу декілька родин мережевих екранів. Насамперед це лінійки Firepower, які різняться продуктивністю і можливостями: від СМБ і філій до мереж інтернет-провайдерів і великих дата-центрів. Ці лінійки впродовж останніх двох років дещо оновились: так, «середня» серія 4100 поповнилась чотирма моделями з продуктивністю у режимі NGFW 12,5–45 Гбіт/с. Також три нові моделі з'явились у найпотужнішій серії 9300. Остання побудована за модульним принципом (є можливість додавання до 3 елементів розширення), а з іншого боку, на апаратній платформі можна створювати виокремлені логічні мережеві екрани.

Окрім того, у Cisco є серія мережевих екранів ASA-5500 у складі 6 пристроїв, які можуть працювати як під управлінням власного ПО, так і з образом Firepower Threat Defence (FTD), сфери їх застосування — від домашнього або віддаленого офісу до границі мережі інтернет-провайдера. Зазначимо, що пристрої Firepower, зі свого боку, також можуть працювати з образом ASA.

Cisco Meraki — це рішення для організації і централізованого управління SD-WAN, до якого входять апаратні і віртуальні пристрої MX різного призначення: від малих офісів до великих філій і кампусів. Серед іншого, у цих пристроях реалізовані різні функції мережевого екрану: контроль і класифікація трафіка на рівні застосунків, запобігання вторгненням, автоматичне розпізнавання клієнтських пристроїв та їх адміністрування.

Нарешті, у Cisco є рішення для промислових об'єктів — ISA3000. Ці пристрої сертифіковані для використання у середовищах зі складними умовами експлуатації (електростанції, нафтогазовий сектор, гірнича галузь тощо).

ASA і Firepower мають віртуалізовані версії, які називаються відповідно ASAv і Threat Defence Virtual, вони можуть працювати як у приватних, так і публічних хмарах і підтримують різні хмарні платформи (KVM, AWS, Azure та ін.). FWaaS-рішення (Cloud-delovered firewall, CDFW) є частиною хмарного сервісу кібербезпеки Cisco Umbrella.

Fortinet: гонитва за продуктивністю

Мережеві екрани Fortinet пропонуються як елемент архітектури кібербезпеки Security Fabric. Вона об'єднує різні системи захисту Fortinet (це пісочниця FortiSandbox, рішення для захисту робочих станцій, контролю доступу тощо), а також інтегрується з партнерськими і хмарними платформами через програмні інтерфейси Fabric Connectors. Управління мережами і кінцевими точками здійснюється з єдиної консолі.

Що стосується власне мережевих екранів, то вони виготовляються на основі фірмових процесорів безпеки, остання версія яких називаються NP7. Fortinet може запропонувати чималий вибір NGFW, від початкового рівня до серії 7000 для великих підприємств і провайдерів. Зокрема, для розподілених офісів компанія пропонує мережеві екрани з вбудованою функціональністю SD-WAN, що зменшує складність управління системою і підвищує продуктивність.

При цьому компанія постійно поповнює лінійки новими пристроями. Наприклад, торік з'явилася серія (у складі двох моделей) FortiGate 4400F для гіпермасштабованих ЦОД, їхня максимальна пропускна здатність у режимі Threat Prevention становить 75 Гбіт/с. У березні вже нинішнього року Fortinet випустила нову надпотужну серію FortiGate 7121F (**рис. 2**), ці пристрої на велетенському шасі розміром 16U мають пропускну здатність 520 Гбіт/с у режимі Threat Protection (лише як мережевий екран — 1,89 Тбіт/с).

Рік тому Fortinet придбав американську компанію OPAQ Networks — постачальника послуг безпечного периферійного доступу SASE (це відносно нова концепція, яка розроблена з метою доступу до корпоративних ресурсів в умовах розмиття периметру і загалом включає в себе FWaaS як один з компонентів). Важливою подією вже 2021 року став вихід версії 7.0 операційної системи FortiOS, яка лежить в основі архітектури Security Fabric. Серед основних нововведень — підтримка доступу з нульовою довірою (ZTNA), що передбачає перевірку усіх користувачів і застосунків у мережі, підтримка SASE, фільтрація відео для посилення безпеки під час роботи з дому.

Рис. 2. Fortinet FortiGate 7121F

Palo Alto і машинне навчання

Palo Alto Networks є одним із законодавців мод у царині NGFW. У 2007 році компанія, власне, представила перший «мережевий екран нового покоління». Рішення Palo Alto побудовані на архітектурі Single Pass, яка забезпечує перевірку трафіка на різні види загроз в один прохід. Аналіз невідомих загроз здійснюється у хмарній пісочниці WildFire.

Торік компанія представила «нову парадигму» NGFW з технологією машинного навчання «в ядрі». Нові можливості були впроваджені як частина операційної системи PAN-OS 10.0 і стали відповіддю на розширення корпоративних мереж, що тепер включають в себе гібридні хмари, IoT і домашні офіси, а також на автоматичну еволюцію кібератак. Як зазначалося у повідомленні Palo Alto, зловмисники також використовують машинне навчання для автоматичного видозмінення атак, а тому сигнатури все гірше й гірше дозволяють запобігати таким загрозам. На стороні захисту моделі машинного навчання досі використовувались лише для аналізу постфактум, проте у шлюзах Palo Alto вони працюють у реальному часі в лінійному режимі (in-line) і дозволяють виявляти раніше невідомі атаки.

Також машинне навчання радикально скорочує час, необхідний на вироблення сигнатури; за словами виконавчого директора PAN Лі Клерича, він становить близько 5 мс. При цьому NGFW на базі машинного навчання миттєво захищатиме від

95% відомих файлових і веб-загроз. Важливим застосуванням технології є інтегрований захист пристроїв IoT: NGFW забезпечує їх повну видимість (у тому числі може розпізнавати раніше невідомі пристрої), виявляє аномалії і вразливості. Окрім того, штучний інтелект збирає і обробляє великі обсяги телеметрії і рекомендує найбільш відповідні політики безпеки. Все це разом усуває потребу у спеціалізованих мережевих сенсорах, скорочує кількість людських помилок і загалом вивільняє час персоналу.

У березні вже нинішнього року Palo Alto оголосила про запровадження Zero Trust, представивши низку нових функцій: зокрема, інтегрований брокер захисту доступу до хмарних сервісів (CASB), систему ідентифікації користувачів Cloud Identity Engine, а також вдосконалені сервіси URL-фільтрації і захисту DNS, що має уможливити безпечний доступ до даних і програм.

Мережеві екрани Palo Alto доступні у різноманітних форм-факторах. Насамперед це, звісно, апаратні рішення, починаючи від PA-220 (для філій територіально розподілених компаній, магазинів і середнього бізнесу) і до потужних систем серії 7000, призначених для ЦОД, великих підприємств і телеком-операторів. Нещодавно (власне, у травні цього року) було представлено ще деякі новинки. Серія PA-400 розрахована на ті ж застосування, що PA-220, і пропонується як альтернатива Fortinet. В серію входять 4 моделі з пропускною здатністю до 2,4 Гбіт/с у режимі Threat Prevention, вони виконані у безвентиляторному корпусі з резервованим блоком живлення і загалом оптимізовані для роботи з мінімальним обслуговуванням.

Іншою новинкою стала платформа PA-5450 (**рис. 3**), призначена для гіпермасштабованих дата-центрів, крайових застосувань і сегментації кампусних мереж. Платформа є модульною, і її можна нарощувати залежно від потреб. Пропускна здатність у режимі Threat Prevention для одного модуля становить 31 Гбіт/с, у повній конфігурації — 125 Гбіт/с, що вчетверо більше, ніж у пристрою попереднього покоління PA-5260.

Рис. 3. Palo-Alto PA-5450

Віртуальні мережеві екрани Palo Alto представлені п'ятьма варіантами конфігурації, що мають пропускну здатність від 200 Мбіт/с до 16 Гбіт/с у режимі мережевого екрану з розпізнаванням застосунків. Вони можуть бути розгорнуті у різноманітних публічних хмарних сервісах і на базі різних гіпервізорів. Рік тому, одночасно з машинним навчанням, Palo Alto представила контейнеризовану систему CN для середовищ оркестрування застосунків Kubernetes, вона може працювати як локально, так і у публічних хмарах і безсерверних службах Kubernetes від Google, Microsoft, Amazon та ін.

Нарешті, Palo Alto надає послуги FWaaS в рамках комплексного рішення хмарного захисту Prisma Access.

Мережеві екрани в умовах нульової довіри

Про смерть NGFW почали говорити мало не з часу їх появи, і проблеми були загалом ті самі: розмиття периметру через хмари, домашні офіси і загалом мобільність працівників. Так звана смерть мережевого екрана, писав два роки тому віце-президент кібербезпекової фірми FireMon Тім Вудс, очікувалася через концепцію BYOD. Зростання числа віддалених працівників у поєднанні зі стрімким перетворенням мобільного телефона на портативний робочий інструмент призвели до того, що «рів навколо замку» втратив сенс. Проте відповіддю стала не відмова від мережевих екранів — навпаки, їх стало ще більше, вони скрізь: в ЦОД, у хмарі і на робочому столі. NGFW тепер використовуються для сегментації мереж на менші зони контролю, а самі вони доповнюються функціями керування доступом.

Перефразовуючи Марка Твена, Forrester зазначає, що смерть периметрового захисту досі не настала, незважаючи на численні заяви про протилежне. «*Хранитель цього периметру, мережевий екран, не лише не застарів, — йдеться у звіті агенції, — але й став фундаментальною платформою для таких функцій мережевого захисту, як детонація зловмисного коду, сигнатурний аналіз контенту і реагування на загрози*». Проте нинішня пандемія, ймовірно, становить найбільшу загрозу, оскільки програми мігрували у хмари, а співробітники працюють удома і, згідно з дослідженням Forrester, половина з них сподіваються там залишатися і після закінчення локдаунів.

Відповідно Forrester рекомендує обирати рішення, які підтримують модель Zero Trust (насамперед мережевий доступ з нульовою довірою), дозволяють керувати з однієї й тієї самої панелі управління як апаратними рішеннями, так і тими, що працюють у хмарі, а також містять компонент для захисту кінцевих точок або можуть інтегруватися з провідними рішеннями у цій царині (що досі не було сильною стороною NGFW).

Справді, виробники один за одним оголошують про запровадження Zero Trust, проте це стосується не лише мережевого екрану, а й комплексного захисту. Виробники відходять від чистого мережевого екрану і намагаються інтегрувати, зокрема, функції SD-WAN і контролю доступу до хмарних сервісів.

У новій парадигмі не можна довіряти жодному пристрою лише тому, що він знаходиться всередині периметру. Мережевий екран стане точкою, де здійснюватиметься контроль, фільтрація і забезпечення виконання політик доступу.

Василь ТКАЧЕНКО, **СиБ**