ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ В AZURE»

Виконав студент 6 курсу, групи БСДМ-63
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Фічоряк В. Я.
(прізвище та ініціали)
Керівник Гахов С. О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

ЗМІСТ

Стор.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ …… 10

ВСТУП ……..…… 10

1 **АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** …….. 13

1.1 Дослідження проблеми захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ ……. 13
1.2 Аналіз підходів до захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ …….. 19
1.3 Аналіз існуючих рішень із захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ ……..…..... 25

2 **АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ В AZURE** ……. 33

2.1 Дослідження основних можливостей хмарної платформи Microsoft Azure …….. 33
2.2 Призначення, можливості та функції захисту від атак DDoS Azure ……..…….. 40
2.3 Еталонні архітектури захисту від атак DDoS Azure …….. 45

3 **ТЕХНОЛОГІЯ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ** ……..…….……. 51

3.1 Порядок застосування політики пом’якшення Azure DDoS Protection ……..… 51
3.2 Порядок створення плану захисту від DDoS-атак за допомогою порталу Azure …….. 55
3.3 Рекомендації щодо захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ …… 61

ВИСНОВКИ …….. 68

ПЕРЕЛІК ПОСИЛАНЬ 70

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ (Презентація) 72

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС – операційна система

ПК – персональний комп’ютер

ЦОД – центр обробки даних

ACL – Access Control List

API – Application Programming Interface

APT – Advanced Persistent Threat

AWS – Amazon Web Services

BGP – Border Gateway Protocol

DDoS – Distributed Denial of Service

DNS – Domain Name System

IaaS – Infrastructure as a Service

ICMP – Internet Control Message Protocol

GRE – Generic Routing Encapsulation

MFA – Multi-Factor Authentication

NTP – Network Time Protocol

OSI – Open Systems Interconnection model

TCP – Transmission Control Protocol

UDP – User Datagram Protocol

WAF – Web Application Firewall

ВСТУП

Актуальність дослідження. Сьогодні DDoS атаки хмарних інформаційних ресурсів організацій становлять одну з найбільших проблем забезпечення їх доступності та безпеки. Ця проблема загострюється з погляду на те, що великі організації іноді мають ресурси, необхідні для захисту від DDoS атак, проте, малим підприємствам часто бракує бюджету та кваліфікованого персоналу для протидії цим атакам.

Microsoft Azure є глобальною хмарною платформою для швидкого та безпечного розгортання IT-інфраструктури організації. В листопаді 2021 року Microsoft заявила, що її платформа захисту в Azure пом'якшила масштабну розподілену DDoS атаку зі швидкістю 3,47 терабіт на секунду і швидкістю передачі пакетів 340 мільйонів пакетів за секунду, спрямовану на клієнта Azure з Азії.

Вищесказане визначає актуальність теми даної магістерської роботи, основний зміст якої становлять дослідження технології захисту від DDoS атак на інформаційні ресурси організації в Azure.

Об'єкт дослідження – захист від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ.

Предмет дослідження – технологія захисту від DDoS атак на інформаційні ресурси організації в Azure.

Мета роботи – розробити порядок застосування технології захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ та рекомендації щодо її реалізації.

Наукові завдання:

дослідити сутність проблеми захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ;

проаналізувати підходи до захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ;

проаналізувати існуючі рішення із захисту від DDoS атак на інформаційні

ресурси організації при застосуванні хмарних платформ;

проаналізувати методи та засоби захисту від DDoS атак на інформаційні ресурси організації в Azure;

розкрити порядок реалізації технології захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації, міжнародних стандартів та їх порівняння.

Практичне значення одержаних результатів: запропоновано порядок застосування технології захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ, а також розроблено рекомендації фахівцям з кібербезпеки щодо її реалізації.

Результати магістерської роботи апробовані на Всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ.

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

1.1. Дослідження проблеми захисту від DDOS атак на інформаційні ресурси організації при застосуванні хмарних платформ

Необхідно відмітити, що застосування хмарних технологій в організаціях надають переваги, які включають основні показники, такі як: технічні, адміністративні, ліцензійні. Проте найбільше значення для бізнесу мають насамперед фінансові вигоди. Онлайн-сервіси пропонують простий, гнучкий та недорогий доступ до будь-якого обсягу та асортименту обчислювальних потужностей та додатків, розміщених за межами корпоративної мережі, що гарантує фізичну безпеку та безперервність бізнесу. Замовнику більше не потрібно створювати і підтримувати власну дорогу IT інфраструктуру. Використання хмарних платформ в 2–3 рази дешевше, ніж розробка додатків або утримання традиційної IT інфраструктури, а гнучкість оплати дозволяє точно співвідносити витрати до обсягу реально використаних IT-ресурсів. При цьому забезпечується максимальна надійність та безпека інформаційних ресурсів організації.

Основними перевагами застосування хмарних технологій для бізнесу є:

співробітники більше не прив'язані жорстко до свого офісу, вони можуть працювати зі своїми даними та додатками з будь-якої точки світу, де є доступ до Internet;

замість великих авансових платежів за придбання та встановлення обладнання та ПЗ, компанія здійснює регулярні рівномірні платежі за доступ своїх співробітників до потрібних їм ресурсів, решта лише за фактом їх споживання. Капітальні витрати замінюються на операційні;

усувається необхідність у купівлі, обслуговуванні та постійному оновленні необхідного для роботи ПЗ. Більше того, при зменшенні кількості працівників, які

використовують хмарні послуги, плата за них також зменшується, що неможливо при стандартній купівлі ліцензій на ПЗ;

усувається необхідність придбання та встановлення комп'ютерної техніки для роботи додатків та зберігання інформації, що дозволяє економити як офісні площі, так і кошти на створення та обслуговування серверних кімнат (кондиціювання, безпека доступу, безперебійне енергоживлення тощо);

усувається необхідність у власному штаті системних адміністраторів та техпідтримки, що забезпечує економію на зарплаті та податках;

потрібні сервіси доступні практично миттєво – не потрібно ніяких додаткових робіт з розгортання та конфігурування інформаційних систем, що використовуються;

споживані ресурси можуть практично миттєво масштабуватись на вимогу замовника, залежно від зміни навантажень. У бізнес-процесі нерідкі сплески активності, коли ресурси необхідні лише тимчасово, наприклад, протягом рекламної кампанії. Якщо в подібній ситуації користувачеві потрібно обраховувати більше даних, він може закупити більше ресурсів, а потім відмовитись від додаткових потужностей і навіть скоротити початкові;

для географічно розподілених компаній досягається додаткова економія на комунікаціях та доступ до загальних документів;

непомітна для користувачів міграція на нові версії та нові платформи, замовники завжди працюють з останніми версіями додатків;

підвищена безпека та надійність роботи.

Але навіть одна раптова хакерська атака може нанести суттєвий фінансовий збиток бізнесу, призвести до втрати важливих даних, погіршити репутацію компанії в очах клієнтів. Саме тому потрібен захист організацій від DDoS-атак. DDoS-атака може бути націлена на вичерпання ресурсів IT-системи або зробити неможливим доступ до системи її офіційним власникам та законним користувачам.

DDoS-атака – це вид кібератаки, під час якої зловмисники намагаються порушити роботу веб-сайту, мережі чи інших онлайн-сервісів, перевантажуючи їх

великою кількістю підроблених або небажаних запитів [1].

Зловмисники, які запускають DDoS-атаки, використовують мережі розподілених скомпрометованих пристроїв, щоб порушити роботу системи, націлюючись на один або кілька компонентів, необхідних для встановлення з'єднання з мережевим ресурсом [1].

Найбільш поширені типи DDoS-атак [1]:

об'ємні атаки є одним із найстаріших типів DDoS-атак. Вони використовують великі обсяги трафіку, щоб заповнити пропускну здатність мережі жертви або пропускну здатність між мережею та Інтернетом. Сьогодні найбільші об'ємні атаки вимірюються в терабітах на секунду (тбіт/с), що еквівалентно приблизно 9000 середніх підключень до Інтернету. Наприклад, під час флуд-атаки за протоколом UDP (User Datagram Protocol) зловмисники перевантажують цільовий віддалений сервер, надсилаючи запити програмі, яка прослуховує певний порт. Через те, що сервер перевіряє та відповідає на кожен такий запит, його пропускна здатність швидко закінчується і він стає недоступним;

атаки прикладного рівня (7 рівень моделі OSI) здійснюють на загальнодоступні програми за допомогою великого обсягу підробленого або фіктивного трафіку. Прикладом є HTTP-флуд, який заповнює певний веб-сервер легітимними запитами HTTP GET та HTTP POST. Незважаючи на те, що сервер може мати достатню пропускну здатність, він змушений обробляти велику кількість фіктивних запитів, тому його можливості обробки вичерпуються. Атаки прикладного рівня вимірюються десятками мільйонів запитів на секунду (RPS);

атаки на рівні протоколу: під час атак на рівні протоколу зловмисники використовують уразливості мережевих протоколів, таких як TCP, UDP, ICMP (3 та 4 рівні моделі OSI), щоб вичерпати ресурси системи жертви. Одним із прикладів є SYN-флуд, який надсилає велику кількість запитів на сервер жертви, але залишає відповіді на ці запити без подальших дій, тому так зване «тристороннє рукостискання» (Three-way Handshake) залишається неповним. Коли кількість незавершених з'єднань вичерпує потужність сервера, він стає

недоступним. Атаки на рівні протоколу використовують спеціально створені пакети для досягнення своїх шкідливих цілей та вимірюються в пакетах в секунду (PPS). Під час найбільших зафіксованих атак такого типу кількість пакетів досягала сотень мільйонів.

Наведемо кілька прикладів серйозності DDoS атак на хмарні платформи. Так, Microsoft заявила, що її платформа захисту Azure DDoS пом'якшила масштабну розподілену атаку типу «відмова в обслуговуванні» (DDoS) зі швидкістю 3,47 терабіт на секунду (Тбіт/с) і швидкістю передачі пакетів 340 мільйонів пакетів за секунду (pps), спрямовану на клієнта Azure з Азії в листопаді 2021 року [2].

Після цього в грудні відбулися ще дві великі атаки, також спрямовані на азіатських клієнтів Azure: UDP-атака зі швидкістю 3,25 Тбіт/с на порти 80 і 443 і UDP-флуд зі швидкістю 2,55 Тбіт/с на порт 443 [2].

Це була розподілена атака, яка походила з приблизно 10 000 джерел і з багатьох країн по всьому світу, включаючи Сполучені Штати, Китай, Південну Корею, Росію, Таїланд, Індію, В'єтнам, Іран, Індонезію та Тайвань [2].

15-хвилинна атака використовувала кілька векторів атаки для відбиття UDP на порт 80, зокрема:

простий протокол виявлення служб (SSDP);

спрощений протокол доступу до каталогу (CLDAP) без підключення;

система доменних імен (DNS);

мережевий протокол часу (NTP).

Попередніми рекордними DDoS-атаками, про які повідомлялося у відкритому доступі, були 21,8 мільйона запитів на секунду (rps) на рівні додатків, які вразили російського Інтернет-гіганта Яндекс у серпні, і об'ємний удар 2,3 Тбіт/с, виявлений Amazon Web Services Shield протягом першого кварталу 2020 року [2].

Компанія Google також повідомляла, що в 2017 році Google зменшив DDoS атаку потужністю 2,54 Тбіт/с [2].

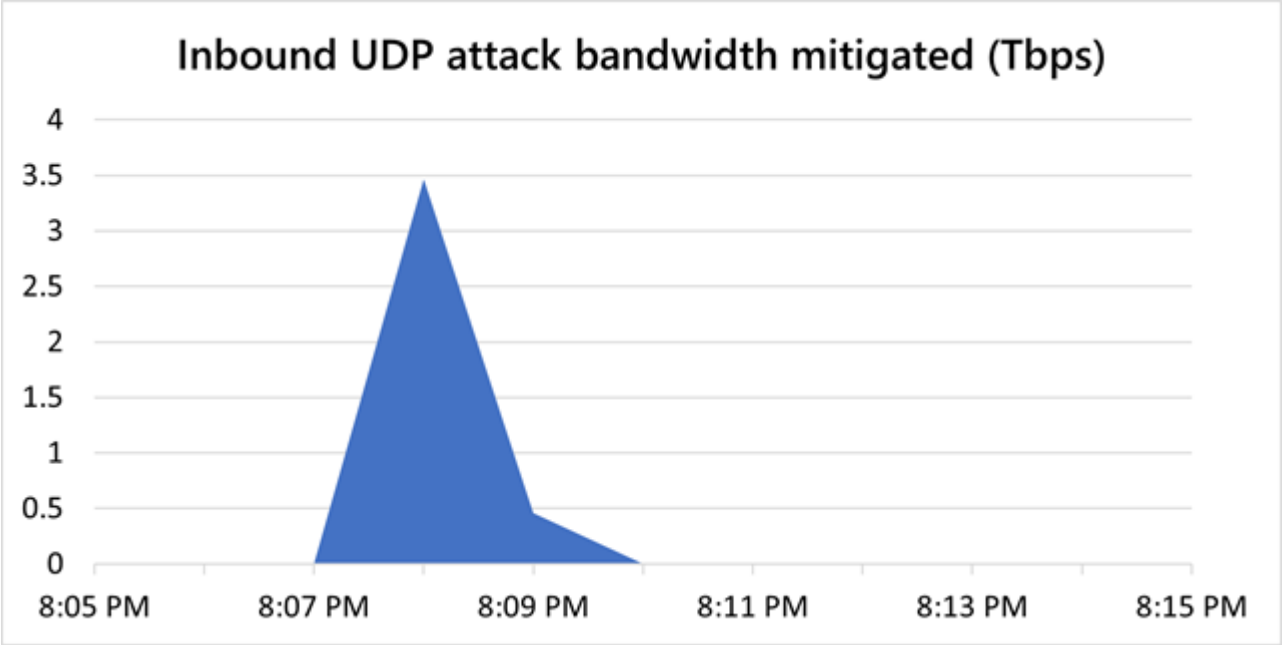

Рис. 1.1. DDoS атака у листопаді 2021 року потужністю 3,47 Тбіт/с [2]

Відмічається, що DDoS атака у листопаді 2021 року зі швидкістю 3,47 Тбіт/с стала найбільшою, з якою Microsoft зіткнулася на сьогоднішній день (і, ймовірно, коли-небудь зареєстрованою), після того, як раніше повідомлялося, що вона пом’якшила ще одну рекордну атаку зі швидкістю 2,4 Тбіт/с, спрямовану на європейського клієнта Azure в кінці серпня 2021 року [2].

У другій половині 2021 року Microsoft спостерігала зростання кількості атак, які тривали більше години, у той час як багатовекторні атаки, такі як рекордна, пом’якшена в листопаді, були поширеними [2].

Ці триваліші DDoS-атаки зазвичай відбуваються як послідовність короткочасних повторюваних пакетних атак, які швидко наростають (за секунди) до терабітних обсягів.

Корпорація Microsoft також захистила клієнтів від нових атак TCP PUSH-ACK (домінуючих у регіоні Східної Азії) під час святкового сезону 2021 року. Було помічено нову техніку маніпулювання параметрами TCP, яку використовували зловмисники для скидання великих корисних даних, завдяки чому в цьому варіанті атаки довжина параметра TCP довша за сам заголовок параметра [2].

Підміна вихідної адреси часто поєднується з відображенням і посиленням

від відкритих Інтернет-серверів, що погано керуються (наприклад, DNS, NTP) для множення об'єму трафіку атаки в 50 або більше разів [5]. Як це працює показано на рис. 1.2. Зловмисник може використовувати один потужний комп'ютер із високошвидкісним Інтернет-з'єднанням або ботнет, що складається з множини скомпрометованих пристроїв, для надсилання запитів на високопродуктивні Інтернет-сервери.

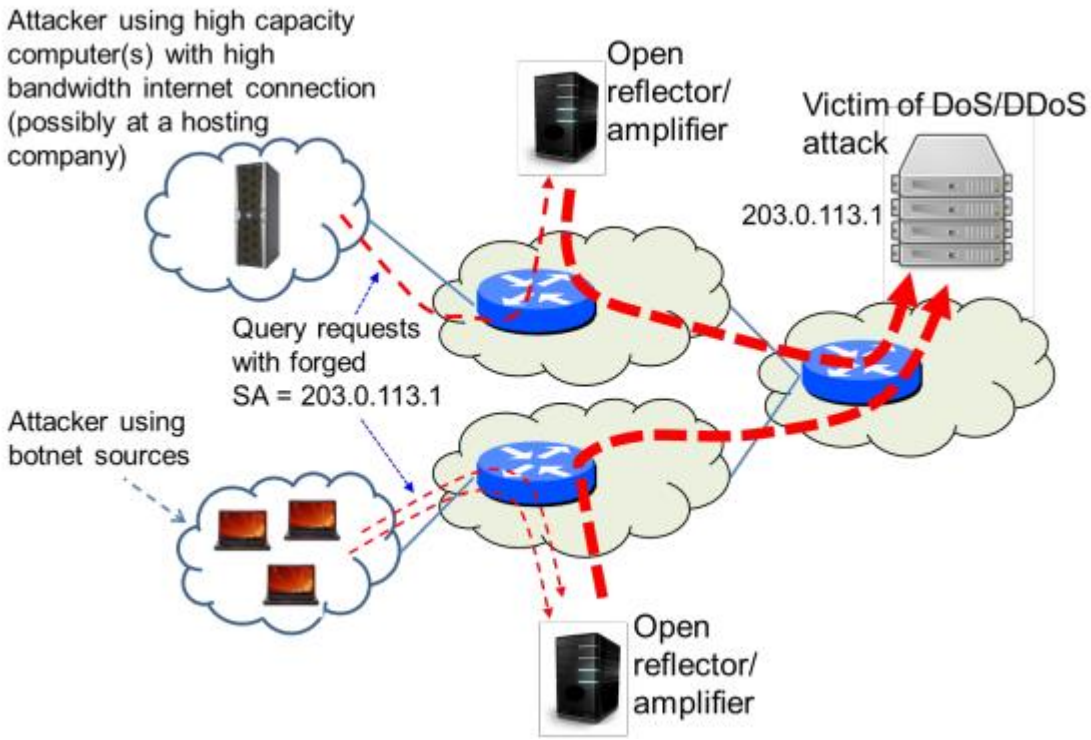

Рис. 1.2. DDoS-атака шляхом підміни IP-адреси джерела, відображення та посилення [5]

Атакуючі системи використовують спуфінг вихідної адреси, який вставляє IP-адресу цілі (203.0.113.1) як вихідну адресу запитів. Для Інтернет-сервісів, що використовують протокол користувацьких дейтаграм (UDP) (наприклад, DNS, NTP), запит і відповідь містяться в одному пакеті, і обмін не вимагає встановлення з'єднання між джерелом та сервером (на відміну від протоколу керування передачею (TCP)) [5].

Відповіді таких відкритих Інтернет-серверів направляються на ціль атаки, оскільки IP-адреса цілі була підроблена як поле вихідної адреси в повідомленнях запиту. Часто відповідь сервера на цільову адресу набагато більша, ніж сам запит,

що посилює ефект DoS-атаки. Такі атаки з відображенням та посиленням можуть призвести до масових DDoS-атаків з обсягами атак у діапазоні сотень Гбіт/с. Обсяги атак можуть значно зрости, якщо атаки масштабу Mirai поєднуються з атаками з посиленням відбиття [5].

1.2. Аналіз підходів до захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ

Безпека хмарних ресурсів або хмарна безпека – це захист хмарних даних, інфраструктури та додатків від кіберзагроз. Безумовно, частину відповідальності за безпеку бере на себе постачальник послуг. Проте власники компаній та відповідні фахівці повинні знати, як правильно працювати з хмарними сервісами, правильно їх налаштовувати та обслуговувати. Іноді для захисту даних у хмарних сервісах потрібні додаткові ресурси. Наприклад, існують інструменти, які можуть допомогти у запобіганні DDoS-атакам.

Найочевиднішою ознакою DDoS-атаки на організацію є низька продуктивність або відсутність доступу системи чи сервісу. Наприклад, веб-сайт може довго завантажуватись або бути недоступним. Крім цього, таку кібератаку можна ідентифікувати завдяки моніторингу та аналізу мережевого трафіку, які допомагають виявити підроблені або небажані запити, що перевантажують одну або декілька систем компанії. На можливу або вже триваючу DDoS-атаку також можуть вказувати повідомлення від зловмисників, у яких вони вимагають викуп за виключення організації зі списку майбутніх цілей або за припинення поточної атаки.

Необхідно відмітити, що найбільш серйозним та руйнівним видом загроз для бізнесу є DDoS-атака.

DDoS-атака – це метод атаки, при якому хакери націлюються на сервери і перевантажують їх користувальницьким трафіком. Коли сервер не справляється з вхідними запитами, сайт, програма або додаток, розташовані на ньому, відключаються або працюють з низькою продуктивністю.

Наприклад, після початку повномасштабного вторгнення росії в Україну Мінцифри створило добровільну кіберармію, яка здійснює DDoS-атаки на ресурси країни-окупанта. За короткий період IT ARMY of Ukraine поклала сайти російських пропагандистів, органів влади, компаній із держсектора, енергетики, банків, рітейлу, сервіси грошових переказів, бухгалтерської звітності та багато іншого. Все це викликало паніку у місцевого населення [3].

Як уникнути DDoS-атаки? Від DDoS-атак складно захиститися, оскільки вхідний Інтернет-трафік розподілено. Але профілактика – найкращі ліки. Потрібно підготувати бізнес до можливих форс-мажорів, щоб запобігти руйнівному результату.

Топ-5 методів захисту від DDoS-атак [3]:

Упорядкування плану реагування на DDoS-атаки. Щоб лихо не застали вас зненацька, підготуйте план реагування на випадок порушення безпеки, щоб технічні фахівці могли відреагувати якнайшвидше. План повинен містити документацію про те, як підтримувати бізнес-процеси у разі успішної DDoS-атаки, всі необхідні технічні знання та досвід, а також контрольний список систем, щоб переконатися, що вони оснащені передовими засобами виявлення загроз.

Захист IT-інфраструктури за допомогою рішень для запобігання DDoS-атакам. Це можуть бути брандмауери, VPN та інші засоби безпеки для моніторингу дій та виявлення невідповідностей трафіку. Якщо ваша IT-інфраструктура хмарна, або ви використовуєте хмарні сервіси, багато операторів надають ресурси розширеного захисту за додаткову плату. Наприклад, хмарний оператор GigaCloud та телеком-оператор GigaTrans пропонують комплексний захист IT-інфраструктури та каналів передачі даних від можливих загроз.

Здійснення оцінки вразливості мережі. Знайдіть слабкі місця у своїх мережах, перш ніж це зробить хакер. Оцінка вразливостей включає виявлення вразливостей безпеки, щоб ви могли виправити помилки у своїй інфраструктурі та краще підготуватися до DDoS-атаки або до будь-яких кіберрисків в цілому. Хмарний оператор GigaCloud спільно з агентством з кібербезпеки GigaSafe

проводить зовнішнє сканування для пошуку вразливостей та тестування IT-інфраструктури на проникнення.

Визначення попереджувальних ознак DDoS-атаки. Нестабільний зв'язок, низька продуктивність і періодичні збої в роботі сайтів або програм – все це ознаки того, що ваш бізнес може зазнати атаки DDoS-злочинців. Навчіть свою команду розпізнавати ознаки DDoS-атак, щоб усі були готові до попереджувальних сигналів [3].

Використання хмарних технологій. Хмарні оператори, які пропонують високий рівень кібербезпеки, включаючи брандмауери та програмне забезпечення для моніторингу загроз, можуть допомогти захистити ваші IT-системи та мережу від DDoS-злочинців. Хмара також має більшу пропускну здатність, ніж більшість приватних мереж, тому вона, швидше за все, не вийде з ладу, якщо виявиться під тиском посилених DDoS-атак.

Але завжди треба бути готовим до плану «Б», якщо ж DDoS-атаку не вдасться відбити. Наприклад, для відновлення даних GigaCloud пропонує сервіси BaaS (Backup as a Service) для резервного копіювання та DRaaS (Disaster Recovery as a Service) для аварійного відновлення. Вони допомагають зарезервувати, а також відновити дані та послуги у разі форс-мажору [3].

Так, 15 лютого було здійснено кібератаку на українські підприємства, державні структури та їхні сайти. Було атаковано сайти Міністерства оборони України, Збройних Сил України, СБУ, Генпрокуратури, сайт Президента України, сайт застосунку «Дія», Національної поліції, Міністерства закордонних справ, а також банків ПриватБанк, monobank, Ощадбанк [4].

Усі структури, які постраждали від атаки, мають або державне призначення, або стосунок до фінансової системи держави, тому можна зробити висновок, що атака мала політичний чи психологічний характер (залякування).

Такими кібератаками зазвичай займаються APT (Advanced Persistent Threat) – угруповання, багато з яких фінансуються державами і мають значно більші ресурси для атак. Тип кібератаки, який було здійснено, називається DDoS.

Розглянемо механізми DoS/DDoS атаки [4].

Кібератака типу «відмова в обслуговуванні» (DoS) – це спроба заподіяти шкоду компанії або держоргану, зробивши недоступною систему – наприклад, веб-сайт, програму або систему цілком – для звичайних користувачів.

Сама по собі схема нескладна: зазвичай зловмисники генерують велику кількість пакетів або запитів, які зрештою перевантажують роботу цільової системи та тимчасово виводять її з ладу.

Для здійснення атаки типу «розподілена відмова в обслуговуванні» (DDoS або Distributed Denial of Service) зловмисник використовує безліч зламаних або контрольованих джерел (пристроїв).

Найчастіше DDoS-атакам піддаються державні органи, банки, лікарні, фінансові структури або бізнес, що конкурує між собою.

Останнім часом стало популярним використання для DDoS-атак IoT-пристроїв: це розумні чайники, розумні холодильники, системи відеоспостереження тощо. Зазвичай ці пристрої гірше захищені від злому (самому захисту цих пристроїв приділяється менше уваги), їх багато і вони лише продовжують набирати популярності. Самі ж пристрої мають можливість підключення до інтернету.

Розглянемо види DDoS-атак [4].

Для захисту від DDoS-атак є платні послуги, але перш, ніж братися за їхню покупку, необхідно забезпечити захист усередині самого інтернет-сервісу. Для того, щоб ускладнити атаку хакеру на інтернет-ресурс, атакуючий повинен якнайменше знати про структуру вашого сервісу і водночас надати якомога більше інформації тому, хто вас захищає від DDoS-атаки. Це мінімізує наслідки та прискорить відновлення роботи після атаки.

З кожним роком атаки стають потужнішими, дешевшими і дедалі витонченішими, тому один з основних пунктів боротьби з ними зводиться до своєчасного оновлення всього ПЗ в інфраструктурі підприємств. Також варто приділити велику увагу захисту всіх інших вузлів.

Перш ніж роз'яснити, як реалізувати захист від DDoS-атак, варто поговорити про структуру атаки.

Найпоширеніші види DDoS-атак [4]:

HTTP-flood. Цей спосіб є найпоширенішим і найпростішим у реалізації. Якщо коротко, то суть такої атаки – відправлення пакета, на який у відповідь приходить пакет значно більшого розміру.

Атака тяжкими пакетами. За допомогою ботнета атакуючий відправляє на сервер дуже багато складних для обробки пакетів, які унаслідок призводять до перевантаження системи та виведення її з ладу на якийсь час.

DNS-flood. Атака за допомогою більшої кількості запитів із численних IP-адрес. Цей спосіб «добрий» тим, що досить складно виявити нелегітимний трафік.

Зазвичай мета простих DDoS-атак, зокрема, з HTTP-запитами, – порушити роботу веб-сервера, зробити його нездатним обробляти реальні запити користувачів. Якщо на сервер надходить більше запитів, ніж він може обробити, реальні запити ігноруються та іноді сервер виходить з ладу. Для користувачів це означає зниження продуктивності чи збій.

Спочатку атакуючий сканує мережу для пошуку пристроїв для атаки. Найчастіше шукають пристрої з відкритими портами та стандартними паролями доступу, щоб створити мережу ботнетів, тобто мережу заражених пристроїв, які контролюються атакуючим.

Якщо говорити про звичайні атаки, то вони спрямовані на доменне ім'я (DNS) або на HTTP. Але якщо ми говоримо про складніші атаки, що мають тяжкі наслідки, то зазвичай вони здійснюються на знайдені вразливості всередині самої інфраструктури.

Нерідко буває так, що DDoS-атака ставить собі за мету не стільки довести систему до «відмови», скільки «пронести» більш серйозну загрозу всередину системи. Зробити це можна за допомогою перевантаження міжмережевих екранів (IPS/IDS), які забезпечують первинний захист, тобто відстежують активні сесії всередині мережі.

Як захищатися від DDoS-атак? Засоби захисту можна розділити на три типи [4]:

локальні;

хмарні;

гібридні.

Локальні рішення та засоби проти DDoS поділяються на два типи: програмні та апаратні (спеціалізовані мережеві пристрої), і їх можуть встановлювати як клієнти, так і їхні провайдери.

Основні користувачі локальних рішень із захисту від DDoS – великий бізнес, наприклад, дата-центри або оператори зв'язку, які можуть собі дозволити мати власну службу реагування (SOC), здатні впоратися з потужними атаками та пропонують послугу захисту від DDoS своїм клієнтам.

Хмарні рішення реалізують майже той самий функціонал захисту, що і локальні рішення. Крім пакетного захисту, провайдери хмарних сервісів anti-DDoS нерідко пропонують послуги захисту сайтів від атак, що виконуються ботами (зловмисники використовують у них протокол HTTP), а також технічну підтримку та супровід під час DDoS-атаки. Хмарні рішення є оптимальним варіантом для більшості компаній.

Гібридне рішення – це комплект з локального рішення та підписки на хмарний сервіс захисту від DDoS, який автоматично підключається при початку атаки. Гібридний підхід дозволяє усунути обмеження локальних рішень щодо обсягів атак та скористатися перевагами хмарних рішень. Гібридні рішення можна рекомендувати великим підприємствам, які приділяють особливу увагу взаємодії з клієнтами в інтернеті, а також сервіс-провайдерам.

Залежно від того, які саме інтернет-ресурси потрібно захищати, вибирають засоби та сервіси anti-DDoS, що мають той чи той спектр функцій захисту:

Захист від пакетного флуду на основі фільтрації пакетів транспортного та мережевого рівня (L3 та L4). Цього достатньо для захисту мережевих пристроїв;

Захист і від пакетного флуду, і від флуду лише на рівні додатків (L3 – L7). Це необхідно для забезпечення працездатності сайтів, оскільки більшість атак здійснюється саме на рівні L7;

Захист не тільки від флуду на рівні L3 – L7, але й від «інтелектуальних» DDoS-атак з використанням «розумних» ботів, що атакують ті частини веб-

додатків, які володіють найбільшою ресурсоємністю при обробці запитів, що надходять, із застосуванням функцій Web Application Firewall (WAF). Це необхідно для захисту критично важливих інтернет-ресурсів.

Хакери найчастіше здійснюють атаки за допомогою мережі пристроїв (комп'ютерів, ноутбуків, мобільних пристроїв, ПК, серверів), якими вони керують. Кожному боту віддалено надсилаються конкретні інструкції щодо атаки. Якщо метою є мережа чи сервер, кожен бот надсилає запити на IP-адресу сервера. Оскільки кожен бот є законним пристроєм в Інтернеті, трафік від нього виглядає нормально, тому його важко відрізнити від звичайного. Потужність ботнетів постійно зростає.

1.3. Аналіз існуючих рішень із захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ

Forrester у [6] включив 11 постачальників до оцінки рішення для запобігання DDoS-атак: A10 Networks, Akamai Technologies, Alibaba Cloud, Amazon Web Services, Cloudflare, Google, Imperva, Lumen, Microsoft, Neustar і Radware (рис. 1.3).

Ризик DDoS атак є високим як ніколи, тому все більше організацій потребують захисту від DDoS-атак. Щоб зменшити тиск загроз, Akamai пропонує три спеціалізовані рішення для забезпечення комплексного хмарного захисту від DDoS [7].

Для захисту центрів обробки даних та гібридної інфраструктури рішення Prolexic надає хмарні засоби пом'якшення наслідків для всіх портів та протоколів, щоб зупинити DDoS-атаки до того, як вони стануть подіями, що впливають на бізнес.

Prolexic спеціально розроблений для запобігання DDoS-атакам у хмарі до того, як вони досягнуть додатків, центрів обробки даних та інфраструктури з виходом в Інтернет (загальнодоступною або приватною). Мережевий трафік спрямовується одним із двох способів через зміну оголошення маршруту

протоколу прикордонного шлюзу або перенаправлення DNS (запис A або запис CNAME) [7].

Рис. 1.3. The Forrester Wave: Рішення для запобігання DDoS-атак за 1 квартал 2021 року [6]

Prolexic, доступний як послуга «завжди включений» або «на запит», пропонує гнучкі моделі інтеграції, що базуються на потребах бажаного рівня безпеки в гібридних джерелах. Завдяки двадцяти глобальним центрам очищення з високою пропускною здатністю Prolexic може зупиняти атаки ближче до джерела, щоб максимізувати продуктивність для користувачів та підтримувати стійкість до відмов мережі за рахунок хмарного розподілу [7].

Трафік прямує через Anycast через найближчий центр очищення, де Центр

управління операціями безпеки Akamai (SOCC) розгортає запобіжні та/або налаштовані засоби пом'якшення наслідків, призначені для миттєвого припинення атак, забезпечуючи швидкий та точний захист від DDoS-атак. Потім чистий трафік повертається до джерела клієнта через тунелі GRE, з'єднання VLAN рівня 2 та/або внутрішнє зіставлення віртуального IP (VIP) з джерелом.

Варіанти інтеграції з Prolexic [7]:

Prolexic Routed – GRE: не залежить від оператора зв'язку для клієнтів з маршрутизованим IP-простором (IPv4/24 та/або IPv6/48), налаштованим через логічні тунелі GRE для асиметричного повернення чистого трафіку до джерела. Підтримує гібридні розгортання AWS BYOIP;

Prolexic Routed – Connect: призначений для клієнтів із маршрутизованим IP-простором (IPv4/24 та/або IPv6/48), налаштованим через прямі підключення VLAN до джерела з асиметричним поверненням чистого трафіку. Глобальні партнери по платформі включають Equinix Cloud Exchange, GTT Communications, Megaport і AT&T Tao, і в майбутньому їх кількість збільшуватиметься;

Prolexic IP Protect: призначений для клієнтів з менш ніж маршрутизованим IPv4/24 та/або IPv6/48, фрагментованим IP-простором або постачальником хмарного хостингу. Підтримує чистий трафік до джерела через симетричну маршрутизацію.

Ключові можливості Prolexic [7]:

висока потужність захисту: потужність захисту Prolexic від DDoS збільшена з 8,2 Тбіт/с до 10 Тбіт/с, завдяки чому загальна межова пропускна здатність Akamai досягає 200+ Тбіт/с – із планами розширення центрів очищення хмари в нових місцях по всьому світу;

провідна в галузі нуль-секундна угода про рівень обслуговування: Prolexic пом’якшує приблизно 80% атак за допомогою нашої нуль-секундної угоди про рівень обслуговування. Це досягається завдяки тісній співпраці з клієнтами для впровадження проактивних захисних елементів керування, адаптованих до поверхні атаки та профілю ризику клієнта, що відбувається під час процесу перевірки послуги;

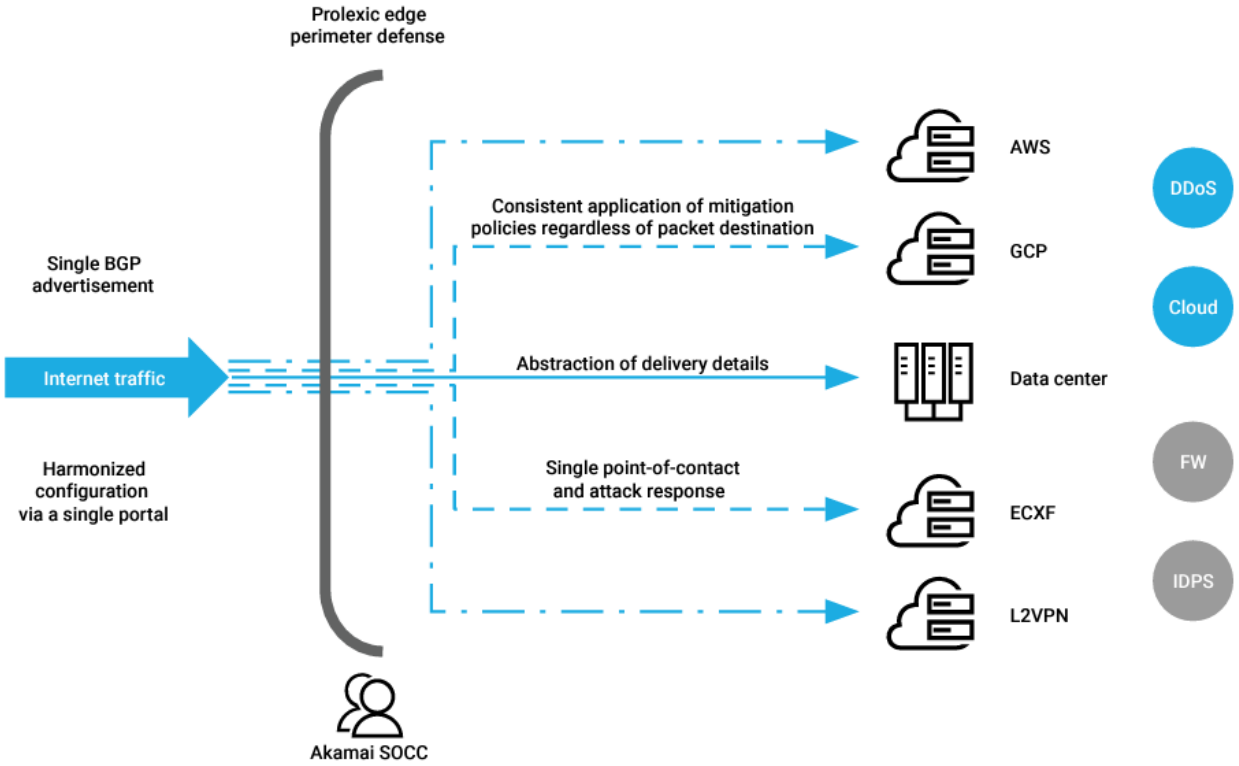

Рис. 1.4. Технологія захисту від DDoS-атак Akamai Prolexic []

стек інтелектуального захисту: пом'якшення контролює динамічне масштабування потужності, щоб зупинити атаки в потоках трафіку IPv4 і IPv6. Обчислювальні ресурси можна динамічно розподіляти для будь-яких елементів керування пом'якшенням, які необхідно збільшити;

широке та всебічне покриття SLA: на додаток до нашої угоди про рівень обслуговування за нуль секунд, Prolexic пропонує 100% доступність платформи, час на пом'якшення, сповіщення про час для попередження, час для відповіді та індивідуальні SLA з часом на пом'якшення на основі конкретних векторів атак;

лазерно-орієнтоване пом'якшення: завдяки створенню обхідних мереж, які пасивно аналізують весь клієнтський трафік, Prolexic може пом'якшувати кожну атаку аж до конкретної /32 IP кінцевої точки, що піддається атаці, без супутнього збитку. Ці дані /32 можна інтегрувати в інформацію про безпеку клієнта та керування подіями, аналітику платіжних систем (для збагачення даних), аналітику, бізнес-аналітику або платформи аналізу загроз за допомогою наших понад 100 API.

Особливостями рішення Imperva DDoS Protection є [8]:

мережа краудсорсінгових знань про нові методи атак. Використовується машинне навчання для забезпечення найсучаснішої, точної та просунутої ступені захисту. Здатність очищення більше 6 Тбит/с може обробляти більше 65 мільярдів атакуючих пакетів в секунду;

Imperva Attack Analytics відстежує атаки в міру їх виникнення. Integrated Attack Analytics корелює DDoS-атаки з іншими векторами атак, що відбуваються паралельно, дозволяючи виявити інші порушення, від яких зазвичай відволікають вашу увагу подібні атаки, наприклад, захоплення облікового запису або фішинг;

гарантований захист з можливостями масштабування. Imperva – єдина компанія, яка надає рішення для постійного моніторингу та запобігання атак будь-якого масштабу та тривалості з гарантією їх виявлення і блокування протягом 3 секунд;

централізоване управління. Є інтеграція з SIEM-рішенням (управління інформацією про безпеку та подіями безпеки), будь-то HP ArcSight, Splunk, McAfee Enterprise Security Manager, IBM QRadar, GrayLog, Sumo Logic або AlienVault USM Anywhere.

Imperva проксує всі веб-запити, щоб блокувати передачу DDoS-атак на сервери клієнта. Imperva виявляє та пом'якшує будь-які типи атак, у тому числі:

CP SYN ACK; TCP FIN; TCP RESET; TCP ACK; TCP ACK PSH; TCP Fragment; UDP; Slowloris; Spoofing; ICMP; IGMP; HTTP Flood; Brute Force; Connection Flood; DNS Flood; NXDomain; Mixed SYN and UDP or ICMP and UDP Flood; Ping of Death; Smurf; Reflected ICMP & UDP; as well as other attacks.

Imperva надає такі DDoS-сервіси [8]:

Website Protection: всі атаки блокуються автоматично. Imperva одночасно захищає сайти від найбільших мережевих атак та найвитонченіших атак. Imperva від DDoS-атак для сайтів маскує реальний IP-адресу вашого сервера та постійно фільтрує вхідний трафік, зупиняючи DDoS-атаки і одночасно пропускаючи на сайт реальних користувачів.

На відміну від інших рішень, багаторівневий підхід не впливає на реальних користувачів навіть при сильній атаці. Imperva гарантує, що ваші відвідувачі та

бізнес ніколи не постраждають від DDoS-атак;

Network Protection: DDoS Protection for Networks доступна як постійна послуга або за запитом, з моніторингом трафіку та підтримкою автоматичного або ручного перемикання.

DDoS Protection for Networks розроблена компанією Imperva для організацій, яким необхідно захистити від DDoS-атак весь діапазон IP-адрес класу C. Це ідеальне рішення для запобігання великомасштабних, об'ємних та складних DDoS-атак, націлених на будь-який тип протоколу обміну даними або мережевої інфраструктури, включаючи HTTP / S, SMTP, FTP, VoIP та інші;

IP Protection: захист Imperva від DDoS-атак для окремих IP-адрес ідеально підходить для організацій, які управляють сайтами та сервісами в хмарі.

Це рішення для захисту додатків, що запускаються на одному хості без контролю всієї мережі. Imperva надає єдине, просте, інтегроване рішення для захисту від DDoS-атак для середовищ, які розміщенні в хмарі;

DNS Protection: захист Imperva від DDoS-атак для DNS-серверів, доступний як постійний сервіс, є рішення на основі проксі, яке захищає DNS-сервери від мережевих DDoS-атак.

Imperva обробляє всі вхідні запити DNS, використовуючи комбінований евристичний аналіз їх репутації та швидкості; він відфільтровує шкідливі пакети, не зачіпаючи реальних відвідувачів. На DNS-сервери пересилаються тільки безпечні запити. Захист Imperva від DDoS-атак для DNS-серверів також блокує спроби використовувати ваші DNS-сервери в якості платформи для запуску DNS-посилених атак на інші сервери [8].

Як показано на рис. 1.5, завдяки багаторівневому підходу до пом’якшення DDoS-атак, здійснюється захист активів організації, де б вони не були, локально чи в хмарі – незалежно від того, розміщено ви в AWS, Microsoft Azure або Google Public Cloud.

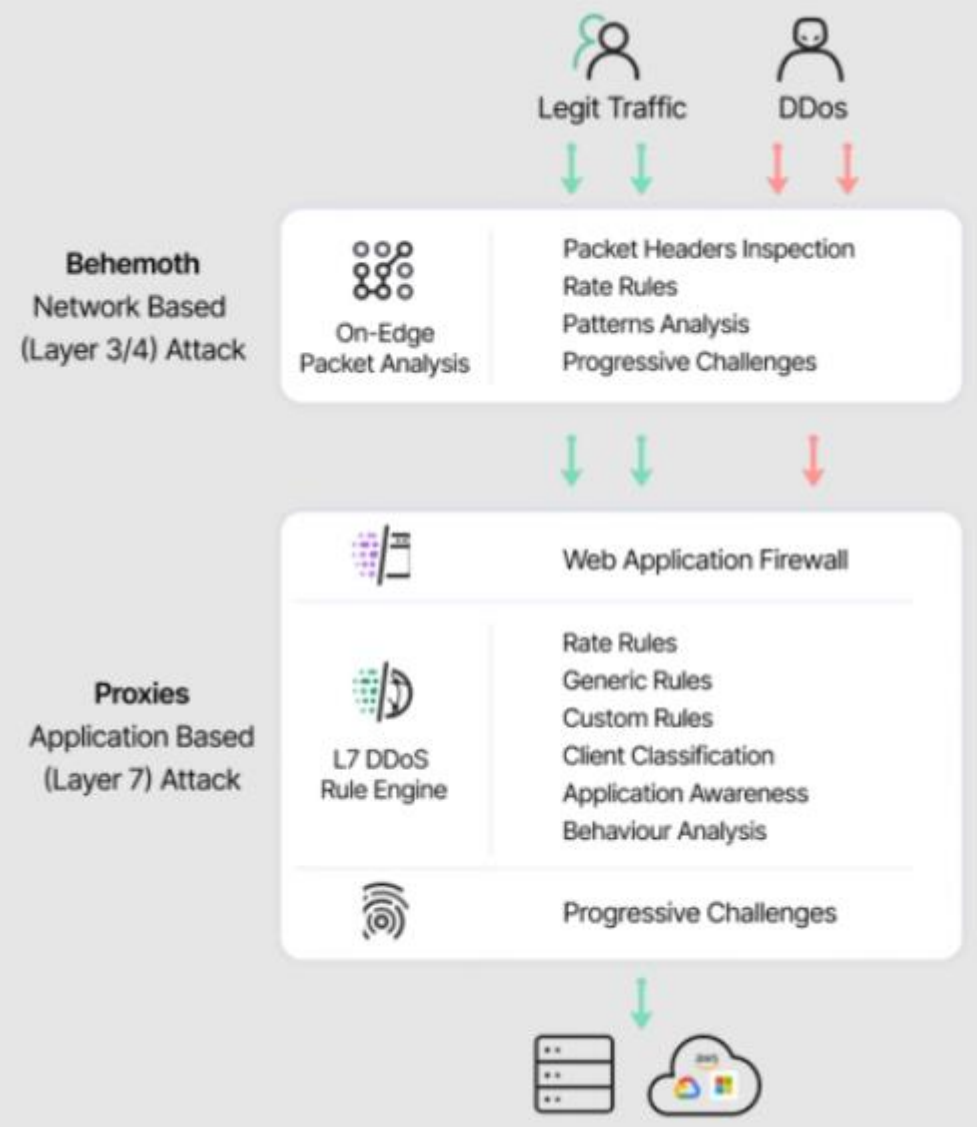

Рис. 1.5. Підхід Imperva до захисту від DDoS-атак [8]

Корпорація Microsoft використовує свої величезні дані про загрози для захисту клієнтів. Корпорація Microsoft використовує аналітичні дані з понад 200 глобальних хмарних і комерційних служб, щоб зібрати величезну кількість даних про загрози DDoS. Логіка така: якщо Microsoft може захистити свій глобальний слід, то вона також зможе захистити клієнтів [9, 10].

Багато організацій, ймовірно, розглядають рішення Microsoft DDoS, оскільки воно вже є частиною хмарної інфраструктури, де вони розміщують програми або служби. Загальна модель постачальника хмарних послуг має захист від DDoS «завжди», і Microsoft не є винятком. Різниця полягає в тому, що Microsoft не є вбудованою, тобто вона може виявити DDoS-атаку, але має подати сигнал своїй технології пом’якшення, щоб ініціювати захист [9, 10].

Microsoft Azure також має широке охоплення відповідності нормативним вимогам і має унікальну інформаційну панель відповідності, яка допомагає, коли телефонують аудитори. Відгуки клієнтів називають легкість налаштування, адаптацію та прозорість цін як сильні сторони служби DDoS від Microsoft. Відгуки клієнтів також вказують на те, що вони віддадуть перевагу захисту рівня 7, який не включає WAF Microsoft. Організаціям, які інвестували багато робочих навантажень в Azure і їм потрібен нечастий захист від DDoS-атак від середніх зловмисників, слід привернути увагу до захисту Microsoft від DDoS-атак [9, 10].

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ В AZURE

2.1. Дослідження основних можливостей хмарної платформи Microsoft Azure

Хмарні обчислення – це термін, що стосується зберігання та доступу до даних через Інтернет. При цьому не зберігається жодних даних на жорсткому диску персонального комп'ютера. У хмарних обчисленнях надається доступ до даних із віддаленого сервера [11].

Microsoft Azure – це платформа хмарних обчислень, яка була запущена корпорацією Microsoft у лютому 2010 року. Це відкрита та гнучка хмарна платформа, яка допомагає розробляти, зберігати дані, розміщувати та керувати послугами. Інструмент Azure розміщує веб-додатки через Інтернет за допомогою центрів обробки даних Microsoft.

В основному в Azure існує три типи хмар: PaaS, SaaS та IaaS (рис. 2.1)

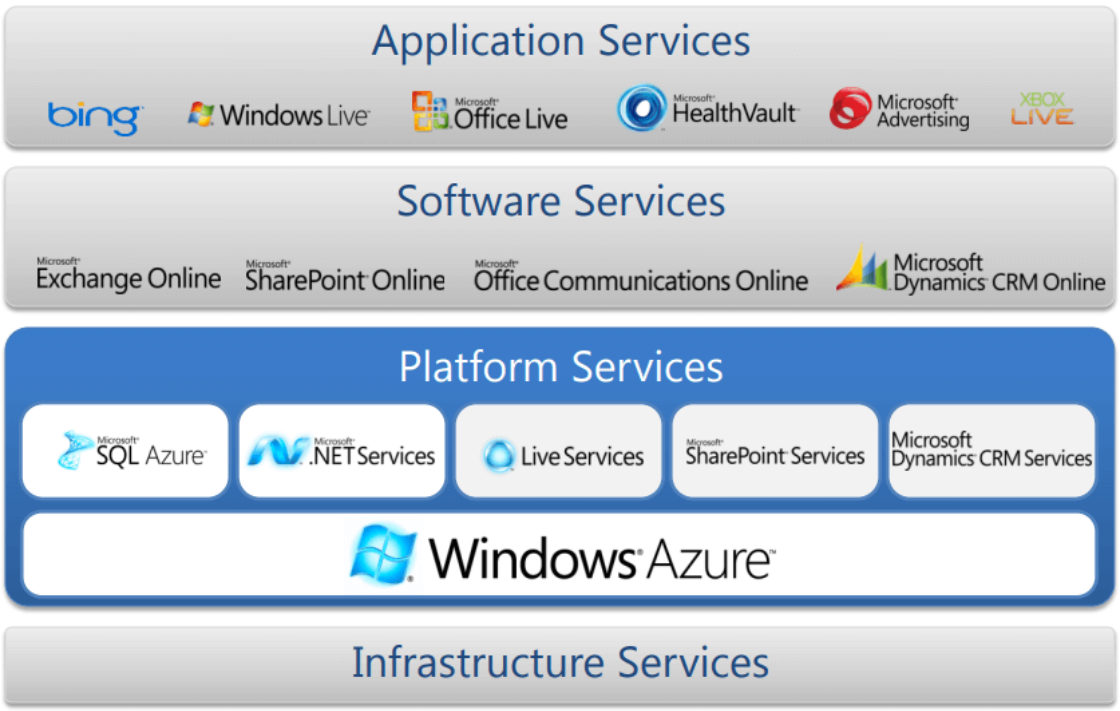

Рис. 2.1. Типи хмар в Microsoft Azure [11]

Інфраструктура як послуга (Infrastructure as a Service, IaaS) – це базовий рівень хмарної платформи. Ця служба Azure використовується IT-адміністраторами для обробки, зберігання, нетворкінгу або будь-яких інших фундаментальних комп'ютерних операцій. Це одна з тем для вивчення Azure, яка дозволяє користувачам запускати довільне програмне забезпечення [11].

Переваги IaaS [11]:

ефективну переносимість часу проектування;

рекомендується для програми, яка потребує повного контролю;

швидкий перехід послуг у хмари.

Очевидна перевага laaS полягає в тому, що вона спрощує налаштування багатьох фізичних або віртуальних машин. Допомагає отримати доступ до центрів обробки даних, контролювати та керувати ними.

Недоліки Iaas [11]:

велика кількість ризиків безпеці через невиправлені сервери;

деякі компанії визначають процеси для тестування та оновлення вразливостей локальних серверів, але це неможливо зробити з Azure.

Платформа як послуга (PaaS) – це обчислювальна платформа, яка включає в себе операційну систему, середовище виконання мови програмування, базу даних або веб-сервіси. Ця служба Azure використовується розробниками та постачальниками додатків.

Як випливає з назви, ця платформа надається клієнту для розробки та розгортання програмного забезпечення. Це одна з основних концепцій Azure, яка дозволяє клієнту зосередитися на розробці додатків замість того, щоб турбуватися про апаратне забезпечення та інфраструктуру. Це сервіс також піклується про операційні системи, мережі та проблеми з серверами.

Перевагами є [11]:

загальна вартість низька, оскільки ресурси розподіляються за вимогою, а сервери автоматично додаються або віднімаються;

Azure менш вразливий, оскільки сервери автоматично перевіряються на наявність усіх відомих проблем безпеки;

весь процес не видно розробнику, тому він не має ризику витоку даних.

Недоліками є [11]:

під час використання служб PaaS можуть виникнути проблеми з переносимістю;

в Azure може бути інше середовище, тому додаток потрібно адаптувати відповідно.

Програмне забезпечення як послуга (SaaS) – це програмне забезпечення, яке централізовано розміщене та кероване. Для всіх клієнтів використовується єдина версія програми. Є можливість масштабувати до кількох екземплярів. Це допомагає забезпечити найкращу продуктивність у всіх місцях. Програмне забезпечення ліцензується через місячну або річну підписку. MS Exchange, Office, Dynamics пропонуються як SaaS [11].

Розглянемо компоненти Azure, які зображено на рис. 2.2.

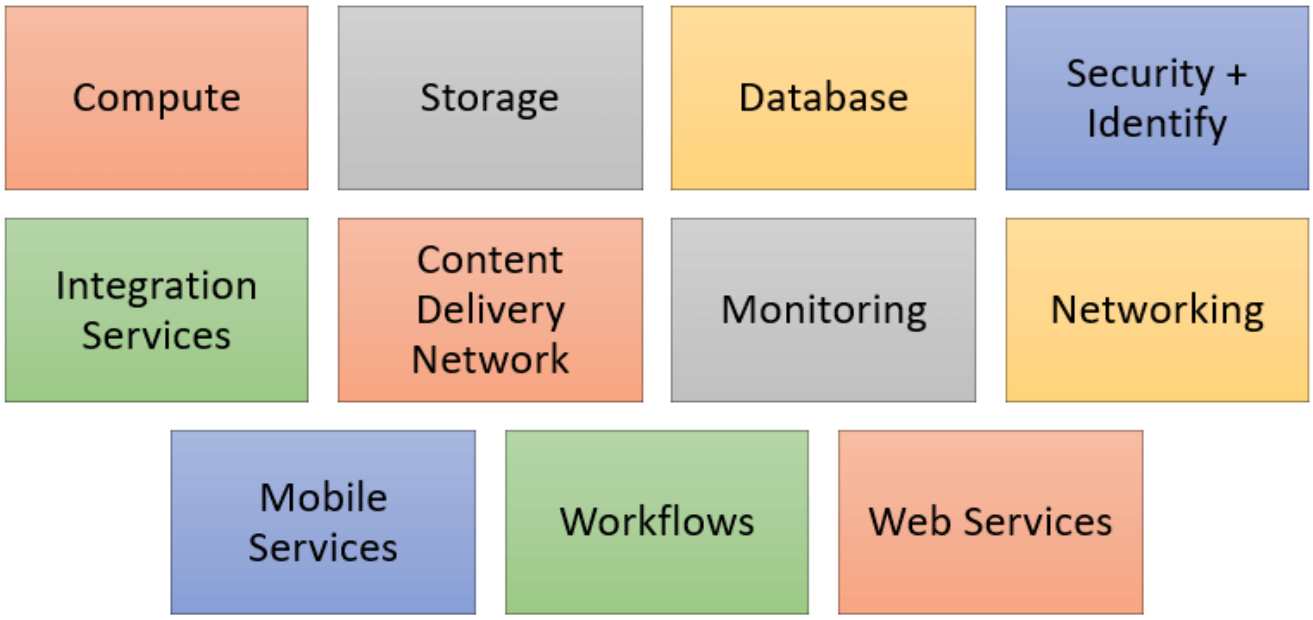

Рис. 2.2. Компоненти платформи Azure [11]

Обчислення (Compute) пропонує такі обчислювальні операції, як розміщення програм, розробка та розгортання на платформі Azure. Він має такі компоненти:

віртуальна машина: дозволяє розгортати будь-яку мову, робоче

навантаження в будь-якій операційній системі;

масштабні набори віртуальних машин: дозволяють створювати тисячі подібних віртуальних машин за лічені хвилини;

служба контейнерів Azure: створює рішення для розміщення контейнерів, оптимізоване для Azure. Ви масштабуєте та впорядковуєте додатки за допомогою Kube, DC/OS, Swarm або Docker;

реєстр контейнерів Azure: ця служба зберігає та керує зображеннями контейнерів у всіх типах розгортань Azure;

функції: забезпечує можливість писати код незалежно від інфраструктури та забезпечення серверів. У ситуації, коли швидкість виклику ваших функцій збільшується;

пакетна обробка: пакетна обробка допомагає масштабувати до десятків, сотень або тисяч віртуальних машин і виконувати комп'ютерні конвеєри;

Service Fabric: спрощує розробку програм на основі мікросервісів і керування життєвим циклом. Він підтримує Java, PHP, Node.js, Python і Ruby.

Сховище (Storage). Azure store – це хмарне рішення для зберігання сучасних додатків. Він розроблений, щоб задовольнити потреби своїх клієнтів щодо масштабованості. Він дозволяє зберігати й обробляти сотні терабайт даних. Він має такі компоненти:

Blob Storage: сховище блобів Azure – це служба, яка зберігає неструктуровані дані в хмарі як об'єкти/блоби. Ви можете зберігати будь-який тип текстових або двійкових даних, як-от документ, мультимедійний файл або інсталятор програми;

Queue Storage (зберігання в черзі): забезпечує хмарний обмін повідомленнями між компонентами додатку. Він забезпечує асинхронний обмін повідомленнями для встановлення зв'язку між компонентами додатку;

File Storage (зберігання файлів): за допомогою сховища файлів Azure ви можете перенести застарілі додатки. Він покладається на спільні файли для Azure швидко та без дорогих перезаписів;

Table Storage (зберігання таблиць): сховище таблиць Azure зберігає

напівструктуровані дані NoSQL у хмарі. Він забезпечує сховище ключів/атрибутів із дизайном без схем.

База даних (Database) – ця категорія включає базу даних як послугу (DBaaS), яка пропонує інструменти SQL і NoSQL. Він також включає такі бази даних, як Azure Cosmos DB і Azure Database для PostgreSQL. Він має такі компоненти:

база даних SQL: це служба реляційної бази даних у хмарі Microsoft на основі лідируючої на ринку системи Microsoft SQL Server;

DocumentDB: це повністю керована служба бази даних NoSQL, створена для швидкої та передбачуваної продуктивності та простоти розробки;

Redis Cache: це безпечне та високорозвинене сховище ключ-значення. Він зберігає такі структури даних, як рядки, хеші, списки тощо.

Мережа доставки контенту (Content Delivery Network): зберігає статичний веб-контент у стратегічно розташованих місцях. Це допоможе вам запропонувати швидкість доставки контенту користувачам. Він має такі компоненти:

VPN-шлюз: надсилає зашифрований трафік через загальнодоступне з’єднання;

Traffic Manager (менеджер трафіку): допомагає контролювати та розподіляти трафік користувачів для таких служб, як WebApps, VM, Azure та хмарних служб у різних центрах обробки даних;

Express Route: допомагає розширити локальні мережі до хмари Microsoft через виділене приватне підключення до Microsoft Azure, Office 365 і CRM Online.

Безпека та ідентифікація служб (Security end Identify sevices): надає можливості для виявлення та реагування на загрози безпеки хмари. Це також допомагає керувати ключами шифрування та іншими конфіденційними ресурсами. Він має такі компоненти:

Key Vault: Azure Key Vault дозволяє захищати криптографічні ключі та допомагає створювати секрети, які використовуються хмарними додатками та службами;

Azure Active Directory і служба керування ідентифікацією включає

багатофакторну автентифікацію, реєстрацію пристрою тощо;

Azure AD B2C – це хмарне рішення для керування ідентифікацією для веб- та мобільних додатків, орієнтованих на споживача. Це дозволяє масштабувати сотні мільйонів ідентифікацій споживачів.

Служби корпоративної інтеграції (Enterprise Integration Services):

Service Bus: Service Bus – це служба доставки інформації, яка працює в системі зв'язку третьої сторони;

SQL Server Stretch Database: ця послуга допомагає безпечно та прозоро переносити будь-які холодні дані в хмару Microsoft Azure;

доменні служби Azure AD: пропонують керовані служби домену, такі як приєднання до домену, групова політика, LDAP тощо. Ця автентифікація сумісна з Windows Server Active Directory;

багатофакторна автентифікація Azure (MFA) – це двоетапна перевірка. Це допомагає отримати доступ до даних і програм, а також пропонує простий процес входу.

Послуги моніторингу та управління (Monitoring end Management Services): служби дозволяють легко керувати розгортанням Azure.

Менеджер ресурсів Azure полегшує керування та візуалізацію ресурсів у вашій програмі. Ви навіть можете контролювати, хто з вашої організації може діяти на ресурсах.

Автоматизація (Microsoft Azure Automation) – це спосіб автоматизувати ручні, довгострокові, безпомилкові та постійно повторювані завдання. Ці завдання зазвичай виконуються в хмарному та корпоративному середовищі.

Мережа Azure (Networking):

віртуальна мережа – ізоляція та сегментація мережі. Він пропонує фільтр і маршрутизацію мережевого трафіку;

балансувальник навантаження забезпечує високу доступність і мережеву продуктивність будь-якої програми. Інформація про баланс навантаження Інтернет-трафік на віртуальні машини;

шлюз додатків: спеціальний віртуальний пристрій, який пропонує

контролер доставки додатків (ADC) як послугу;

служба хостингу Azure DNS пропонує розпізнавання імен за допомогою інфраструктури Microsoft Azure.

Веб-сервіси та мобільні послуги [11]:

веб-додатки дозволяють створювати та розміщувати веб-сайти мовою програмування на ваш вибір без необхідності керувати їх інфраструктурою;

служба мобільних додатків пропонує користувачам широкомасштабовану глобально доступну платформу розробки мобільних додатків;

додатки API спрощують розробку, розміщення та використання API у хмарі та локально;

Logic Apps допомагає спростити та реалізувати масштабовані інтеграції.

Робочі процеси в хмарі (Workflows): візуальний конструктор для створення та автоматизації вашого процесу у вигляді серії кроків, відомих як робочий процес.

Центри сповіщень Azure пропонують простий у використанні, багатоплатформний, масштабований механізм надсилання.

Центри подій (Azure Event Hubs) – це платформа потокового передавання даних, яка може керувати мільйонами подій за секунду. Дані, надіслані до центру подій, можна трансформувати та зберігати за допомогою будь-яких адаптерів пакетування/зберігання, які пропонують аналітичні пропозиції в реальному часі.

Пошук Azure – це рішення хмарного пошуку як послуги, яке пропонує керування сервером та інфраструктурою. Він пропонує готовий до використання сервіс, який можна заповнити своїми даними. Це можна використовувати для додавання пошуку до вашої веб-програми чи мобільної програми.

Міграція: інструменти міграції допомагають організації оцінити витрати на міграцію робочого навантаження. Це також допомагає виконувати міграцію робочих навантажень із ваших локальних центрів обробки даних у хмару Azure.

2.2. Призначення, можливості та функції захисту від атак DDoS Azure

Розподілені атаки типу "відмова в обслуговуванні" (DDoS) – це одна з найбільших загроз доступності та безпеки, з якою стикаються клієнти, які переміщають свої додатки в хмару. Метою DDoS-атаки є вичерпання ресурсів програми, щоб вона стала недоступною для звичайних користувачів. Атаку DDoS можна направити будь-яку кінцеву точку, публічно доступну через Інтернет.

Захист від атак DDoS Azure (рис. 2.3) у поєднанні з рекомендаціями щодо проектування додатків надає розширені функції захисту від атак DDoS. Вона автоматично налаштовується для захисту конкретних ресурсів Azure у віртуальній мережі. Захист простий у використанні для будь-якої нової або наявної віртуальної мережі та не потребує змін додатків чи ресурсів [12].

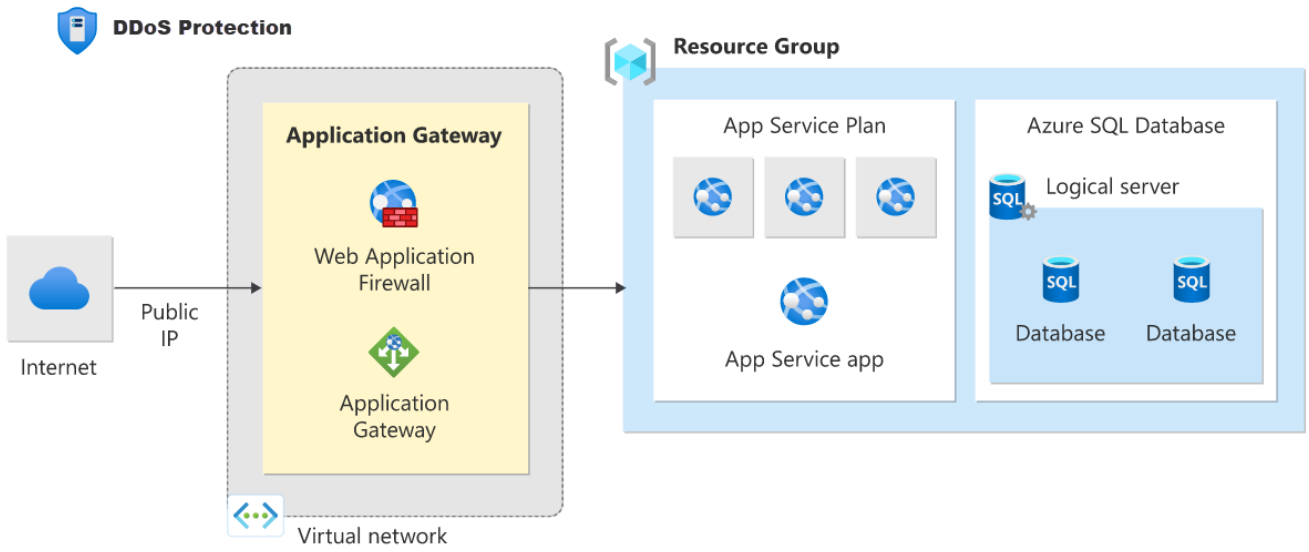

Рис. 2.3. Архітектура сервісу захисту від атак DDoS Azure [12]

Розглянемо основні переваги сервісу захисту від атак DDoS Azure [12].

Постійний моніторинг трафіку: трафік додатку цілодобово та щодня перевіряється на наявність ознак DDoS-атак. Сервіс захисту від атак DDoS Azure миттєво та автоматично усуває атаку після її виявлення.

Адаптивне налаштування в режимі реального часу: система інтелектуального профілювання трафіку вивчає трафік корпоративного додатку з

часом і вибирає та оновлює профіль, який найкраще підходить для вашої служби. Цей профіль коригується зі зміною трафіку з часом.

Телеметрія, моніторинг та попередження сервісу захисту від атак DDoS Azure: захист від атак DDoS Azure застосовує три автоматично налаштовані політики усунення ризиків (TCP SYN, TCP і UDP) для кожної загальнодоступної IP-адреси захищеного ресурсу у віртуальній мережі з увімкненим DDoS. Порогові значення політики настроюються автоматично через профіль мережевого трафіку на основі машинного навчання. Усунення атак DDoS виконується для атакованої IP-адреси, лише якщо перевищено граничні значення політики.

Швидке реагування сервісу захисту від атак DDoS Azure: під час активної атаки клієнти сервісу захисту від атак DDoS Azure мають доступ до команди швидкого реагування DDoS (DRR), яка може допомогти у розслідуванні атак під час атаки та аналізу після атаки.

Сервіс захисту від атак DDoS Azure надається у двох доступних номерах SKU: захист IP-адрес DDoS та захист від атак DDoS [12].

Спрощена конфігурація негайно захищає всі ресурси у віртуальній мережі відразу після активації захисту від атак DDoS. Користувач не потребує жодних дій або налаштувань. Аналогічно спрощена конфігурація негайно захищає ресурс загальнодоступної IP-адреси при включенні захисту IP-адрес від атак DDoS.

Забезпечення багаторівневого захисту: при розгортанні з брандмауером веб-застосунку (WAF) сервіс захисту від атак DDoS Azure захищає як на мережному рівні (рівень 3 і 4, запропонований службою захисту від атак DDoS Azure), так і на рівні додатків (рівень 7, запропонований WAF). Пропозиції WAF включають цінову категорію WAF шлюзу додатків Azure та пропозиції брандмауера веб-додатків сторонніх виробників, які доступні в Azure Marketplace.

Забезпечення широкого діапазону атак, що усуваються: захист від усіх векторів атак на рівнях 3 та 4 для боротьби з найвідомішими атаками DDoS із використанням усіх можливостей глобальної мережі.

Забезпечення аналітики атак: під час атаки вам будуть надсилатися докладні звіти з п'ятихвилинними інтервалами, а після її завершення ви отримаєте повне

зведення. Виконуйте потокову передачу журналів потоків усунення ризиків у Microsoft Sentinel або в автономну систему керування інформаційною безпекою та подіями безпеки (SIEM), щоб забезпечити під час атаки моніторинг майже в реальному часі. У Azure Monitor доступні узагальнені метрики кожної атаки.

Є можливість налаштувати оповіщення на початку, в кінці та протягом атаки, використовуючи вбудовані метрики атаки. Оповіщення інтегруються в операційне програмне забезпечення, наприклад Microsoft Azure Monitor, Splunk, служба сховища Azure, програми для роботи з електронною поштою та портал Azure.

Необхідно відмітити, що захист від атак DDoS Azure призначений для служб, розгорнутих у віртуальній мережі. Для інших служб застосовується захист від атак DDoS на рівні стандартної інфраструктури, що забезпечує захист від поширених атак мережевого рівня.

Розглянемо типи атак, які пом’якшує Azure DDoS Protection [12]. Azure DDoS Protection може пом’якшити наступні типи атак:

Об’ємні атаки: ці атаки заповнюють мережевий рівень значною кількістю, здавалося б, законного трафіку. Вони включають UDP-флуд, ампліфікаційний флуд та інші флуди підроблених пакетів. Захист від DDoS пом’якшує ці потенційні багатогігабайтні атаки, автоматично поглинаючи та очищаючи їх за допомогою масштабу глобальної мережі Azure.

Атаки на протокол: ці атаки роблять ціль недоступною, використовуючи слабкі місця в стеку протоколів рівня 3 і 4. Вони включають атаки SYN flood, атаки відображення та інші атаки на протоколи. Захист від DDoS пом’якшує ці атаки, розрізняючи зловмисний і законний трафік, взаємодіючи з клієнтом і блокуючи зловмисний трафік.

Атаки рівня ресурсів (додатків): ці атаки спрямовані на пакети веб-додатків, щоб порушити передачу даних між хостами. Вони включають порушення протоколу HTTP, впровадження SQL, міжсайтовий сценарій та інші атаки рівня 7. Використовуйте брандмауер веб-програм, наприклад брандмауер веб-програм Azure Application Gateway, а також захист від DDoS, щоб

забезпечити захист від цих атак. На Azure Marketplace також доступні сторонні брандмауери веб-додатків.

Azure DDoS Protection захищає ресурси у віртуальній мережі, включаючи публічні IP-адреси, пов'язані з віртуальними машинами, балансувальниками навантаження та шлюзами додатків. У поєднанні з брандмауером веб-додатки Application Gateway або стороннім брандмауером веб-додатків, розгорнутим у віртуальній мережі з загальнодоступною IP-адресою, Azure DDoS Protection може забезпечити повну здатність пом'якшення рівня 3–7.

Розглянемо функції Azure DDoS Protection [12].

По-перше, це постійний моніторинг трафіку. Azure DDoS Protection відстежує фактичне використання трафіку та постійно порівнює його з пороговими значеннями, визначеними в політиці DDoS. При перевищенні порогового трафіку автоматично запускається захист від DDoS. Коли трафік повертається нижче порогових значень, пом'якшення припиняється.

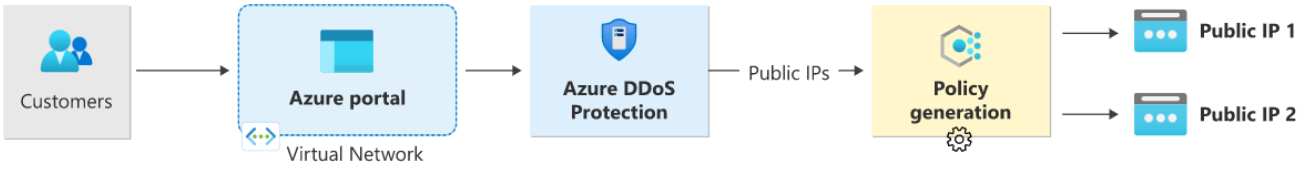

Рис. 2.4. Схема моніторингу трафіку Azure DDoS Protection [12]

Під час пом'якшення трафік, який надсилається до захищеного ресурсу, перенаправляється службою захисту від DDoS-атак і виконується кілька перевірок, наприклад:

переконайтеся, що пакети відповідають специфікаціям Інтернету та не мають неправильного формату;

взаємодійте з клієнтом, щоб визначити, чи є трафік потенційно підробленим пакетом (наприклад, SYN Auth або SYN Cookie або скинувши пакет для повторної передачі джерелом);

пакети з обмеженням швидкості, якщо неможливо застосувати інший метод примусового контролю.

Azure DDoS Protection відкидає трафік атак і пересилає трафік, що залишився, за призначенням. Протягом кількох хвилин після виявлення атаки ви отримаєте сповіщення за допомогою показників Azure Monitor. Налаштувавши журнал телеметрії захисту від DDoS, ви можете записати журнали в доступні параметри для майбутнього аналізу. Дані показників у Azure Monitor for DDoS Protection зберігаються протягом 30 днів.

Розглянемо як здійснюється адаптивне налаштування в реальному часі (рис. 2.5) [12].

Складність атак (наприклад, багатовекторні атаки DDoS) і поведінка орендарів, що залежать від програми, вимагають індивідуальної політики захисту для кожного клієнта. Служба досягає цього, використовуючи дві статистичні дані:

Автоматичне вивчення шаблонів трафіку для кожного клієнта (для кожного публічного IP) для рівня 3 і 4.

Зведення до мінімуму помилкових спрацьовувань, враховуючи, що масштаб Azure дозволяє поглинати значну кількість трафіку.

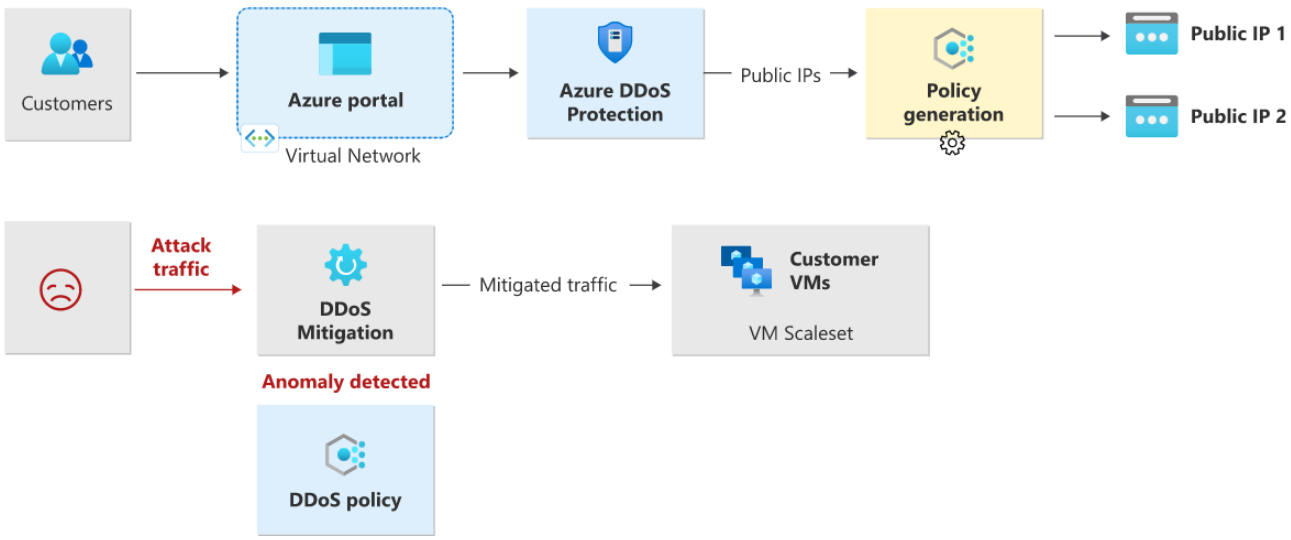

Рис. 2.5 Схема захисту трафіку Azure DDoS Protection [12]

Телеметрія захисту від DDoS, моніторинг і сповіщення

Azure DDoS Protection надає повну телеметрію через Azure Monitor. Ви можете налаштувати сповіщення для будь-якої метрики Azure Monitor, яку

використовує захист від DDoS. Ви можете інтегрувати ведення журналів із Splunk (концентраторами подій Azure), журналами Azure Monitor і Azure Storage для розширеного аналізу через інтерфейс діагностики Azure Monitor.

2.3. Еталонні архітектури захисту від атак DDoS Azure

Сервіс захисту від атак DDoS Azure розроблено для служб, які розгортаються у віртуальній мережі. Розглянемо еталонні архітектури відповідно до сценаріїв застосування [13].

Розглянемо робочі навантаження віртуальної машини (Windows/Linux).

Додаток працює на віртуальних машинах із балансуванням навантаження: ця еталонна архітектура демонструє набір перевірених практик для запуску кількох віртуальних машин Windows у масштабованому наборі із балансувальником навантаження для покращення доступності та масштабованості. Цю архітектуру можна використовувати для будь-якого робочого навантаження без збереження стану, наприклад веб-сервера.

У цій архітектурі робоче навантаження розподіляється між кількома примірниками віртуальної машини. Існує єдина загальнодоступна IP-адреса, а Інтернет-трафік розподіляється на віртуальну машину через балансувальник навантаження.

Балансувальник навантаження розподіляє вхідні Інтернет-запити до примірників віртуальної машини. Набори масштабування віртуальної машини дозволяють масштабувати кількість віртуальних машин вручну чи автоматично на основі попередньо визначених правил. Це важливо, якщо ресурс піддається DDoS-атаці.

Архітектура віртуальної машини DDoS Network Protection показано на рис. 2.6.

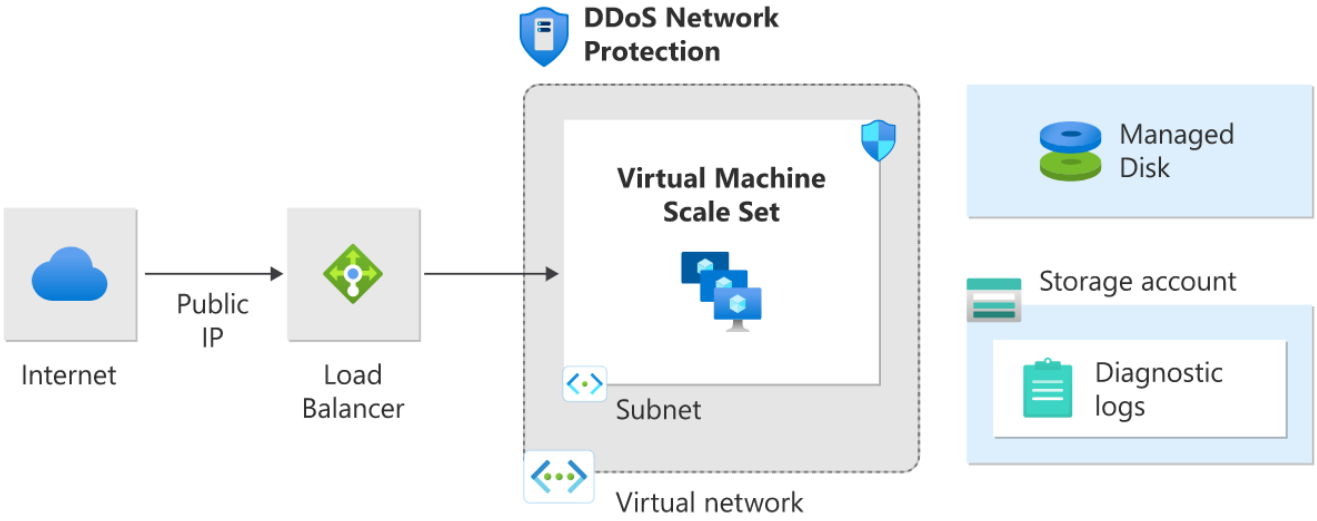

Рис. 2.6. Архітектура віртуальної машини DDoS Network Protection [13]

Захист мережі від DDoS увімкнено у віртуальній мережі балансувальника навантаження Azure (Інтернет), з яким пов'язано загальнодоступну IP-адресу (рис. 2.7).

Архітектура віртуальної машини DDoS IP Protection показано на рис. 2.5.

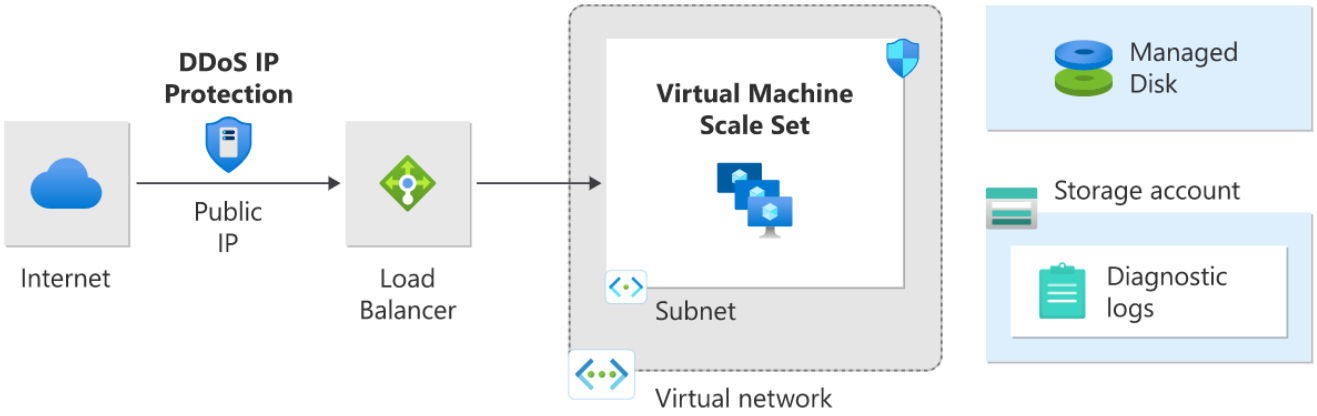

Рис. 2.7. Архітектура віртуальної машини DDoS IP Protection [13]

IP-захист від DDoS увімкнено на зовнішній загальнодоступній IP-адресі загальнодоступного балансувальника навантаження.

Розглянемо випадок коли додаток працює на Windows N-рівня.

Існує багато способів реалізації N-рівневої архітектури. На наступних схемах показано типовий трирівневий веб-додаток. Веб- та бізнес-рівні використовують віртуальні машини із збалансованим навантаженням.

Архітектура захисту мережі DDoS N-рівневої архітектури Windows показано на рис. 2.8.

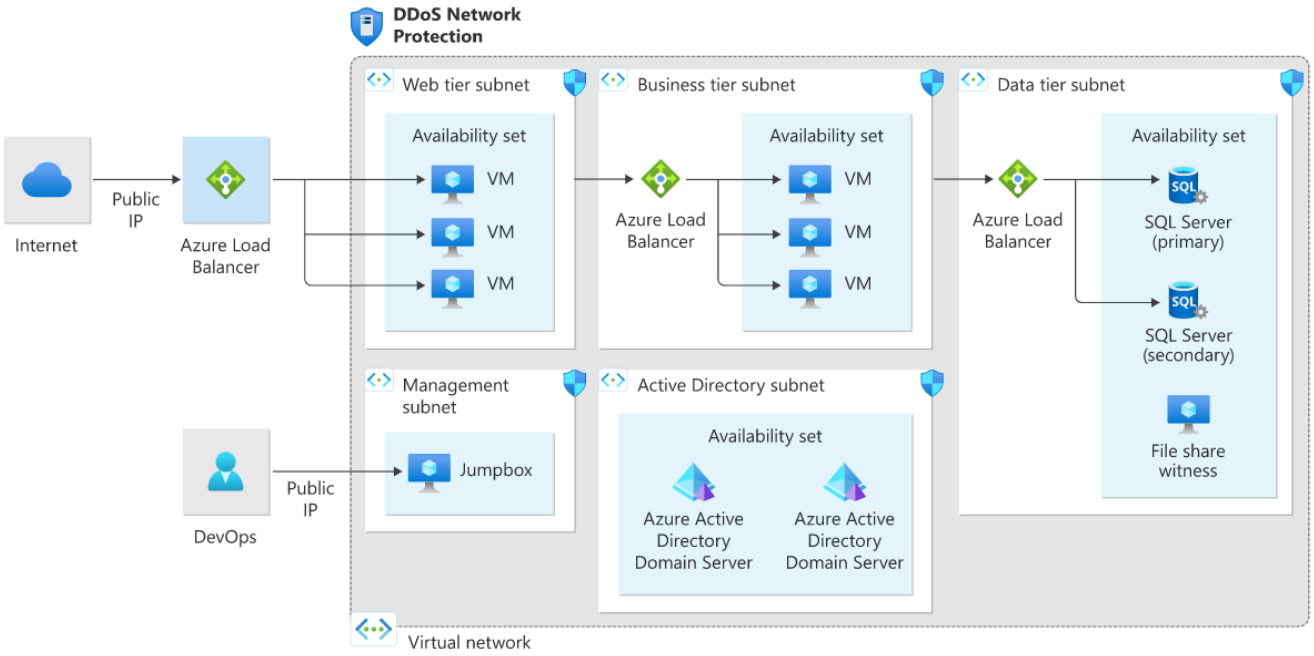

Рис. 2.8. Архітектура захисту мережі DDoS N-рівневої архітектури Windows [13]

На цій схемі (рис. 2.8) архітектури захист мережі DDoS увімкнено у віртуальній мережі. Усі загальнодоступні IP-адреси у віртуальній мережі отримують захист від DDoS для рівня 3 і 4. Для захисту рівня 7 розгортається Application Gateway у SKU WAF.

Розглянемо IP-захист від DDoS N-рівневої архітектури Windows.

На цій схемі архітектури (рис. 2.9) захист IP від DDoS увімкнено на загальнодоступній IP-адресі.

Сценарії, коли одна віртуальна машина працює за публічною IP-адресою, не підтримуються. Пом’якшення DDoS може не розпочатися миттєво, коли виявлено DDoS-атаку. У результаті розгортання окремої віртуальної машини, яке не можна масштабувати, у таких випадках вийде з ладу.

Розглянемо коли веб-додаток як PaaS.

Ця еталонна архітектура показує запуск додатку Azure App Service в одному регіоні. Ця архітектура демонструє набір перевірених практик для веб-додатку, який використовує службу додатків Azure і базу даних SQL Azure. Регіон очікування налаштовано для сценаріїв відновлення після відмови.

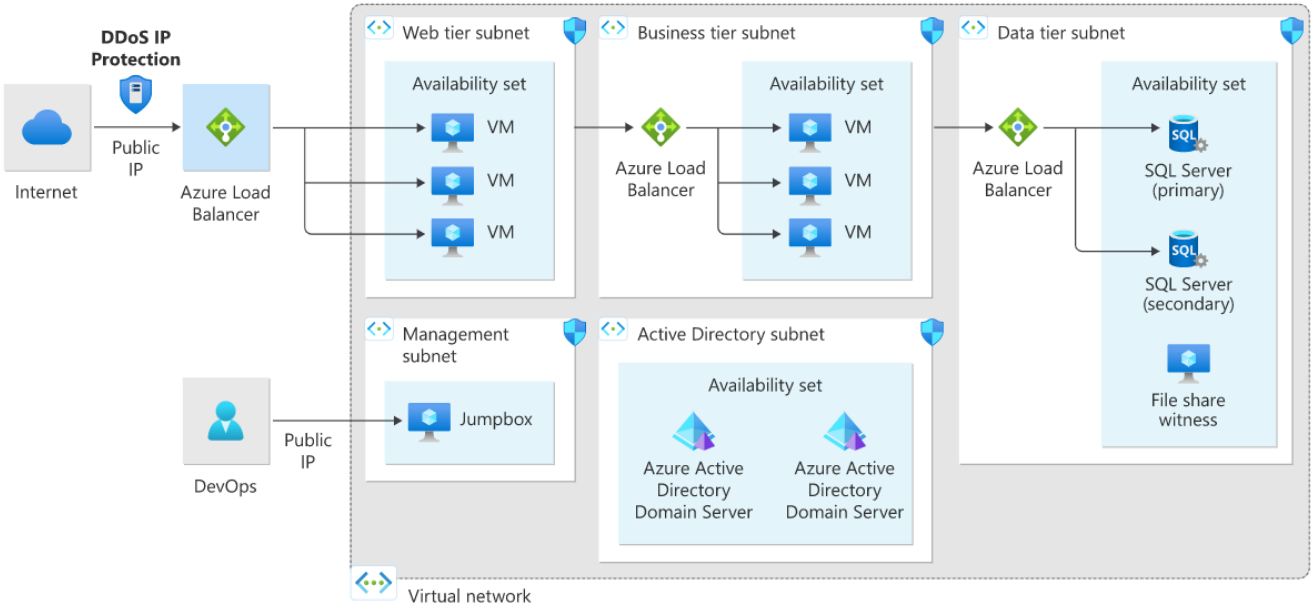

Рис. 2.9. Архітектура IP-захисту від DDoS N-рівневої архітектури Windows [13]

Диспетчер трафіку Azure направляє вхідні запити до шлюзу додатків в одному з регіонів. Під час звичайної роботи він направляє запити до шлюзу додатків в активній області. Якщо цей регіон стає недоступним, диспетчер трафіку переключається на шлюз додатків у резервному регіоні.

Весь трафік з Інтернету, призначений до веб-додатку, спрямовується на загальнодоступну IP-адресу шлюзу додатків за допомогою диспетчера трафіку. У цьому сценарії сама служба додатків (веб-додаток) не має прямого зовнішнього доступу та захищена шлюзом додатків.

Рекомендується налаштувати WAF SKU шлюзу додатків (режим запобігання), щоб захистити від атак рівня 7 (http/https/WebSocket). Крім того, веб-додатки налаштовані на прийом лише трафіку з IP-адреси шлюзу додатків.

Захист мережі DDoS з архітектурою веб-додатків PaaS показано на рис. 2.10.

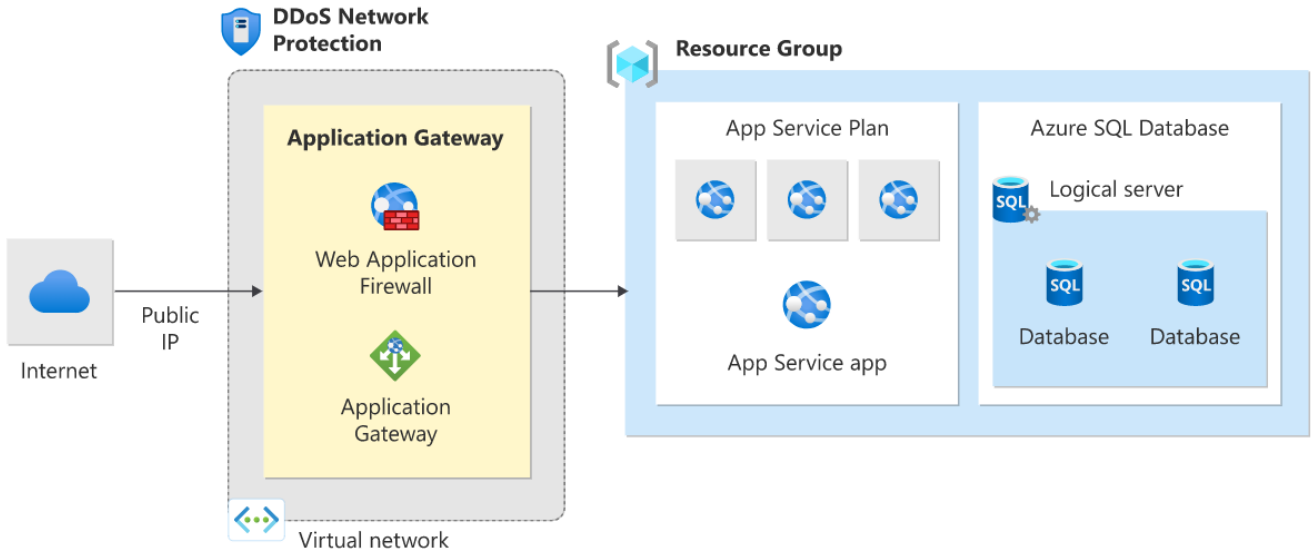

Рис. 2.10. Захист мережі DDoS з архітектурою веб-додатків PaaS [13]

На цій схемі архітектури (рис. 2.10) захист мережі від DDoS увімкнено у віртуальній мережі шлюзу веб-додатку.

Розглянемо IP-захист від DDoS з архітектурою веб-додатків PaaS

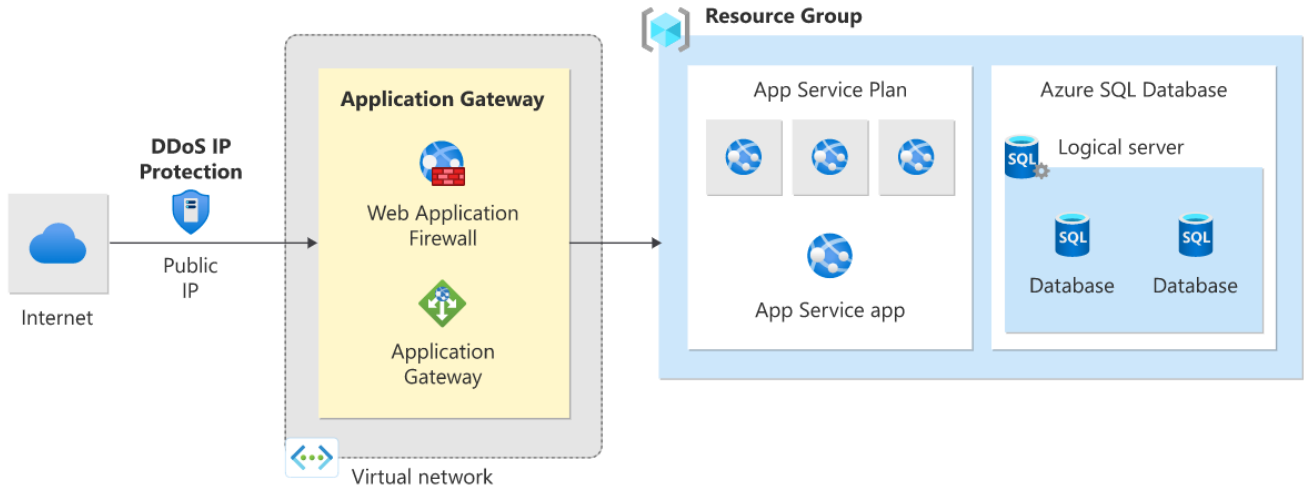

Рис. 2.11. IP-захист від DDoS з архітектурою веб-додатків PaaS [13]

На цій схемі архітектури (рис. 2.11) захист IP від DDoS увімкнено для загальнодоступної IP-адреси, пов’язаної зі шлюзом веб-додатку.

Розглянемо архітектуру мережі Hub-and-Spoke з Azure Firewall і Azure Bastion.

Ця еталонна архітектура детально описує топологію концентратора та

спілкування з брандмауером Azure всередині концентратора як DMZ для сценаріїв, які потребують централізованого контролю над аспектами безпеки. Брандмауер Azure – це керований брандмауер як служба, який розміщено у власній підмережі. Azure Bastion розгорнуто та розміщено у власній підмережі.

Є два спілкування, які підключені до концентратора за допомогою однорангового зв'язку VNet, і немає зв'язку між спілами. Якщо потрібне з'єднання «звуковий зв'язок», то потрібно створити маршрути для перенаправлення трафіку з однієї спілки на брандмауер, який потім зможе спрямувати його на іншу спільну мережу. Усі публічні IP-адреси, які знаходяться всередині концентратора, захищені захистом від DDoS. У цьому сценарії брандмауер у концентраторі допомагає контролювати вхідний трафік з Інтернету, тоді як публічна IP-адреса брандмауера захищена. Azure DDoS Protection також захищає публічну IP-адресу бастіону.

Захист від DDoS-атак розроблений для служб, які розгортаються у віртуальній мережі.

Розглянемо мережу hub-and-spoke захисту від DDoS (рис. 2.12).

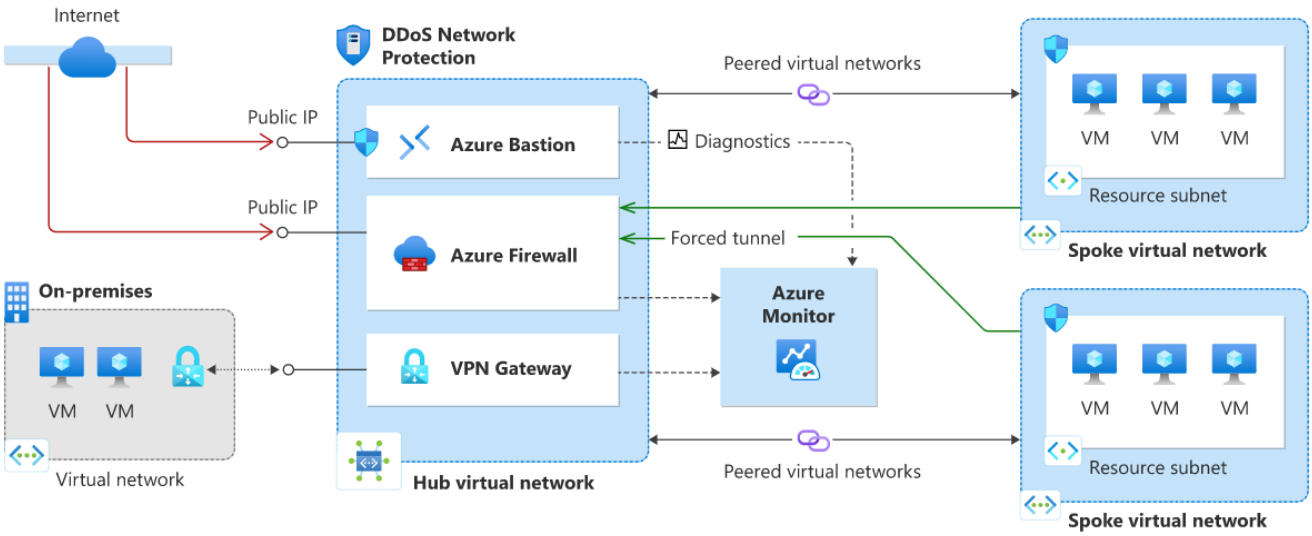

Рис. 2.12. Мережа hub-and-spoke захисту від DDoS [13]

На цій схемі архітектури (рис. 2.12) мережевий захист Azure DDoS увімкнено у віртуальній мережі концентратора.

Розгянемо DDoS-захист IP-мережі (рис. 2.13).

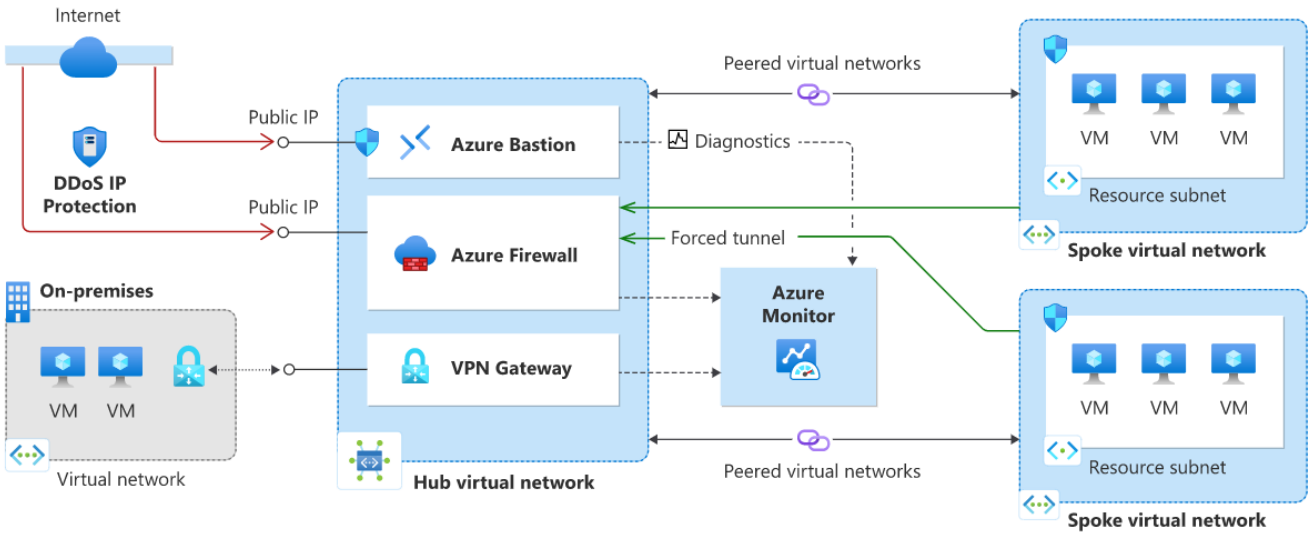

Рис. 2.13. Архітектура DDoS-захисту IP-мережі [13]

На цій схемі (рис. 2.13) архітектура IP-захист Azure DDoS увімкнено для загальнодоступної IP-адреси.

Azure DDoS Protection захищає публічні IP-адреси ресурсу Azure. Захист інфраструктури DDoS, який не потребує налаштування та ввімкнено за умовчанням, захищає лише базову інфраструктуру платформи Azure (наприклад, Azure DNS).

3 ТЕХНОЛОГІЯ ЗАХИСТУ ВІД DDOS АТАК НА ІНФОРМАЦІЙНІ РЕСУРСИ ОРГАНІЗАЦІЇ ПРИ ЗАСТОСУВАННІ ХМАРНИХ ПЛАТФОРМ

3.1. Порядок застосування політики пом'якшення Azure DDoS Protection

Розглянемо політики пом'якшення Azure DDoS Protection.

На порталі Azure виберіть Монітор > Показники. На панелі «Метрики» (рис. 3.1) виберіть групу ресурсів, виберіть тип ресурсу «Загальнодоступна IP-адреса» та виберіть свою публічну IP-адресу Azure. Показники DDoS відображаються на панелі доступних показників.

Захист від DDoS застосовує три автоматично налаштовані політики пом'якшення (TCP SYN, TCP і UDP) для кожної загальнодоступної IP-адреси захищеного ресурсу у віртуальній мережі, у якій увімкнено DDoS. Ви можете переглянути порогові значення політики, вибравши метрику Вхідні пакети для ініціювання пом'якшення DDoS.

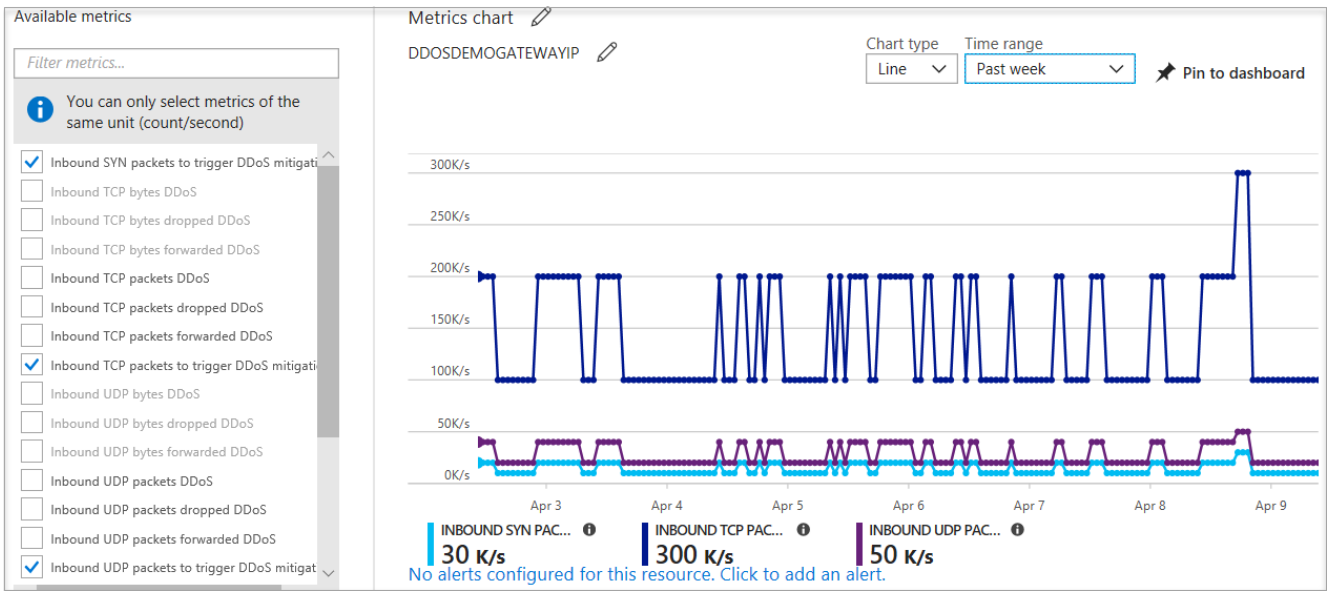

Рис. 3.1. Інтерфейс сервісу Azure DDoS Protection [12]

Порогові значення політики налаштовуються автоматично за допомогою

профілювання мережевого трафіку на основі машинного навчання. Пом'якшення DDoS відбувається для IP-адреси, що піддається атаці, лише коли перевищено порогове значення політики.

Метрика для IP-адреси під DDoS-атакою (рис. 3.2).

Якщо загальнодоступна IP-адреса піддається атаці, значення метрики Під DDoS-атакою чи ні змінюється на 1, оскільки захист від DDoS-атак виконує пом'якшення трафіку атаки.

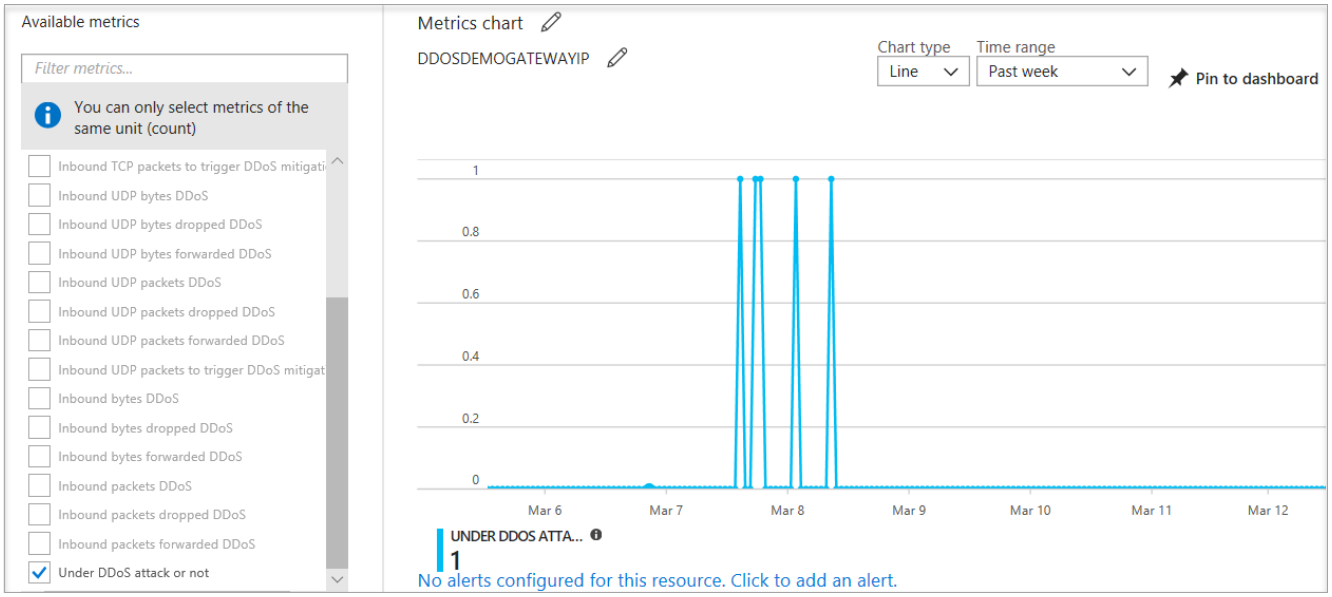

Рис. 3.2. Метрика для IP-адреси під DDoS-атакою [12]

Ми рекомендуємо налаштувати сповіщення для цього показника. Потім ви отримаєте сповіщення, коли на вашій загальнодоступній IP-адресі буде виконано активне пом'якшення DDoS.

Брандмауер веб-додатків для атак на ресурси. Що стосується атак на ресурси на прикладному рівні, вам слід налаштувати брандмауер веб-додатків (WAF), щоб захистити веб-додатки. WAF перевіряє вхідний веб-трафік, щоб заблокувати впровадження SQL, міжсайтовий сценарій, DDoS та інші атаки рівня 7. Azure надає WAF як функцію Application Gateway для централізованого захисту ваших веб-програм від поширених експлойтів і вразливостей. Є інші пропозиції WAF, доступні від партнерів Azure, які можуть бути більш придатними для ваших потреб через Azure Marketplace [12].

Навіть брандмауери веб-додатків сприйнятливі до атак обсягу та виснаження стану. Ми настійно рекомендуємо ввімкнути захист від DDoS-атак у віртуальній мережі WAF, щоб захистити від об’ємних і протокольних атак.

Планування захисту має вирішальне значення.

Планування та підготовка мають вирішальне значення, щоб зрозуміти, як працюватиме система під час DDoS-атаки. Розробка плану реагування на інциденти є частиною цих зусиль.

Якщо у вас є захист від DDoS-атак, переконайтеся, що його ввімкнено у віртуальній мережі кінцевих точок, що виходять в Інтернет. Налаштування сповіщень про DDoS допомагає постійно стежити за будь-якими потенційними атаками на вашу інфраструктуру.

Незалежно відстежуйте свої програми. Зрозумійте звичайну поведінку програми. Будьте готові діяти, якщо під час DDoS-атаки програма поводиться не так, як очікувалося.

Розглянемо як створити стійкі до DDoS атак сервіси на Azure.

Треба створити дизайн для безпеки. Для цього необхідно переконатися, що безпека є пріоритетом протягом усього життєвого циклу додатку, від розробки та впровадження до розгортання та експлуатації. Додатки можуть мати помилки, які дозволяють відносно невеликій кількості запитів використовувати надмірну кількість ресурсів, що призводить до збою служби.

Щоб захистити службу, що працює в Microsoft Azure, необхідно розуміти архітектуру своєї програми та зосередитися на п’яти стовпах якості програмного забезпечення. Необхідно знати типові обсяги трафіку, модель підключення між додатком та іншими додатками, а також кінцеві точки служби, доступні для загальнодоступного Інтернету.

Найважливіше переконатися, що додаток є достатньо стійким, щоб впоратися з відмовою в обслуговуванні, яка спрямована на додаток. Безпека та конфіденційність вбудовані в платформу Azure, починаючи з життєвого циклу розробки безпеки (SDL). SDL забезпечує безпеку на кожному етапі розробки та забезпечує безперервне оновлення Azure для ще більшої безпеки.

Необхідно втілювати дизайн для масштабованості.

Масштабованість – це те, наскільки добре система справляється зі збільшеним навантаженням. Створюйте свої додатки так, щоб вони масштабувалися горизонтально, щоб задовольнити попит на підвищене навантаження, зокрема у випадку DDoS-атаки. Якщо ваш додаток залежить від одного екземпляра служби, це створює єдину точку збою. Надання кількох екземплярів робить вашу систему більш стійкою та масштабованою.

Для Azure App Service виберіть план App Service, який пропонує кілька екземплярів. Для хмарних служб Azure налаштуйте кожну зі своїх ролей на використання кількох екземплярів . Для віртуальних машин Azure переконайтеся, що архітектура вашої віртуальної машини (VM) містить більше однієї віртуальної машини та що кожна віртуальна машина входить до набору доступності . Ми рекомендуємо використовувати набори масштабування віртуальної машини для можливостей автоматичного масштабування.

Ідея глибокого захисту полягає в управлінні ризиком за допомогою різноманітних захисних стратегій. Розташування засобів захисту безпеки в програмі зменшує ймовірність успішної атаки. Ми рекомендуємо вам реалізовувати безпечні проекти для своїх програм, використовуючи вбудовані можливості платформи Azure.

Наприклад, ризик атаки зростає зі збільшенням розміру (площі поверхні) програми. Ви можете зменшити площу поверхні, використовуючи список схвалення, щоб закрити відкритий простір IP-адрес і порти прослуховування, які не потрібні на балансувальниках навантаження (балансувальник навантаження Azure і шлюз програм Azure). Групи безпеки мережі (NSG) є ще одним способом зменшити поверхню атаки. Ви можете використовувати службові теги та групи безпеки програми, щоб мінімізувати складність створення правил безпеки та налаштування безпеки мережі, як природне розширення структури програми.

По можливості слід розгортати служби Azure у віртуальній мережі . Ця практика дозволяє ресурсам служби спілкуватися через приватні IP-адреси. Трафік служби Azure із віртуальної мережі за умовчанням використовує

загальнодоступні IP-адреси як вихідні IP-адреси. Використання кінцевих точок служби перемикатиме трафік служби на використання приватних адрес віртуальної мережі як вихідних IP-адрес, коли вони отримують доступ до служби Azure із віртуальної мережі.

Ми часто бачимо, як локальні ресурси клієнтів піддаються атакам разом із їхніми ресурсами в Azure. Якщо ви підключаєте локальне середовище до Azure, ми рекомендуємо звести до мінімуму доступ локальних ресурсів до загальнодоступного Інтернету. Ви можете використовувати масштаб і розширені можливості захисту від DDoS Azure, розгорнувши в Azure свої відомі загальнодоступні об’єкти. Оскільки ці загальнодоступні об’єкти часто є ціллю DDoS-атак, розміщення їх у Azure зменшує вплив на ваші локальні ресурси.

3.2. Порядок створення плану захисту від DDoS-атак за допомогою порталу Azure

План захисту від DDoS-атак визначає набір віртуальних мереж, у яких увімкнено захист мережі від DDoS-атак, для всіх підписок. Ви можете налаштувати один план захисту від DDoS для вашої організації та зв’язати віртуальні мережі з кількох підписок в рамках одного клієнта Azure AD до того самого плану [14].

Порядок створення плану захисту від DDoS атак.

1. Виберіть *Створити ресурс* у верхньому лівому куті порталу Azure.

2. Знайдіть термін DDoS. Коли план захисту від DDoS з’явиться в результатах пошуку, виберіть його.

3. Виберіть *Створити*.

4. Введіть або виберіть наведені нижче значення:

Підписка Виберіть свою підписку.

Група ресурсів Виберіть *Створити новий* і введіть *MyResourceGroup*.

Ім'я Введіть *MyDdosProtectionPlan*.

Регіон Введіть *Схід США*.

5. Виберіть *Переглянути + створити*, а потім *Створити*.

Хоча ресурси плану захисту від DDoS-атак мають бути пов’язані з регіоном, користувачі можуть увімкнути захист від DDoS-атак у віртуальних мережах у різних регіонах і в кількох підписках під одним клієнтом Azure Active Directory.

Порядок увімкнення захисту від DDoS для нової віртуальної мережі.

1. Виберіть *Створити ресурс* у верхньому лівому куті порталу Azure.

2. Виберіть *Мережа*, а потім виберіть *Віртуальна мережа*.

3. Введіть або виберіть наведені нижче значення:

Підписка Виберіть свою підписку.

Група ресурсів Виберіть *Використовувати наявні*, а потім виберіть *MyResourceGroup.*

Ім'я Введіть *MyVnet.*

Регіон Введіть *Схід США*.

4. Виберіть *Далі*: IP-адреси та введіть наступні значення:

Адресний простір IPv4 Введіть *10.1.0.0/16.*

Назва підмережі У розділі *Назва підмережі* виберіть *Додати підмережу* та введіть *mySubnet.*

Діапазон адрес підмережі Введіть *10.1.0.0/24*.

5. Виберіть *Додати*.

6. Виберіть *Далі: Безпека*.

7. Виберіть *Увімкнути* на *DDoS Network Protection*.

8. Виберіть *MyDdosProtectionPlan* на панелі плану захисту від DDoS. Вибраний вами план може мати ту саму або іншу підписку, що й віртуальна мережа, але обидві підписки мають бути пов’язані з одним клієнтом Azure Active Directory.

9. Виберіть *Переглянути + створити*, а потім *Створити*.

Ви не можете перемістити віртуальну мережу до іншої групи ресурсів або підписки, якщо для віртуальної мережі ввімкнено стандарт DDoS. Якщо вам потрібно перемістити віртуальну мережу з увімкненим стандартом DDoS,

спочатку вимкніть стандарт DDoS, перемістіть віртуальну мережу, а потім увімкніть стандарт DDoS. Після переміщення автоматично налаштовані порогові значення політики для всіх захищених публічних IP-адрес у віртуальній мережі скидаються.

Порядок увімкнення від DDoS атак для існуючої віртуальної мережі:

1. Створіть план захисту від DDoS, виконавши дії, описані в Створення плану захисту від DDoS, якщо у вас немає плану захисту від DDoS.

2. Введіть ім’я віртуальної мережі, для якої потрібно ввімкнути захист мережі DDoS, у полі *Пошук ресурсів*, служб і документів у верхній частині порталу Azure. Коли назва віртуальної мережі з’явиться в результатах пошуку, виберіть її.

3. Виберіть *захист від DDoS* у розділі *Налаштування*.

4. Виберіть *Увімкнути*. У розділі *План захисту від DDoS* виберіть наявний план захисту від DDoS або план, створений на кроці 1, а потім натисніть *Зберегти*. Вибраний вами план може мати ту саму або іншу підписку, що й віртуальна мережа, але обидві підписки мають бути пов’язані з одним клієнтом Azure Active Directory.

Ви також можете ввімкнути план захисту від DDoS для існуючої віртуальної мережі з плану захисту від DDoS, а не з віртуальної мережі:

1. Знайдіть *Плани захисту від DDoS* у полі пошуку ресурсів, служб і документів у верхній частині порталу Azure. Коли плани захисту від DDoS з’являться в результатах пошуку, виберіть їх.

2. Виберіть потрібний план захисту від DDoS, який потрібно ввімкнути для вашої віртуальної мережі.

3. Виберіть *Захищені ресурси* в розділі *Налаштування*.

Натисніть *Додати* та виберіть потрібну підписку, групу ресурсів і назву віртуальної мережі. Знову натисніть *Додати*.

У розділі Захищені ресурси (рис. 3.3) ви можете переглянути свої захищені віртуальні мережі та публічні IP-адреси або додати більше віртуальних мереж до свого плану захисту від DDoS.

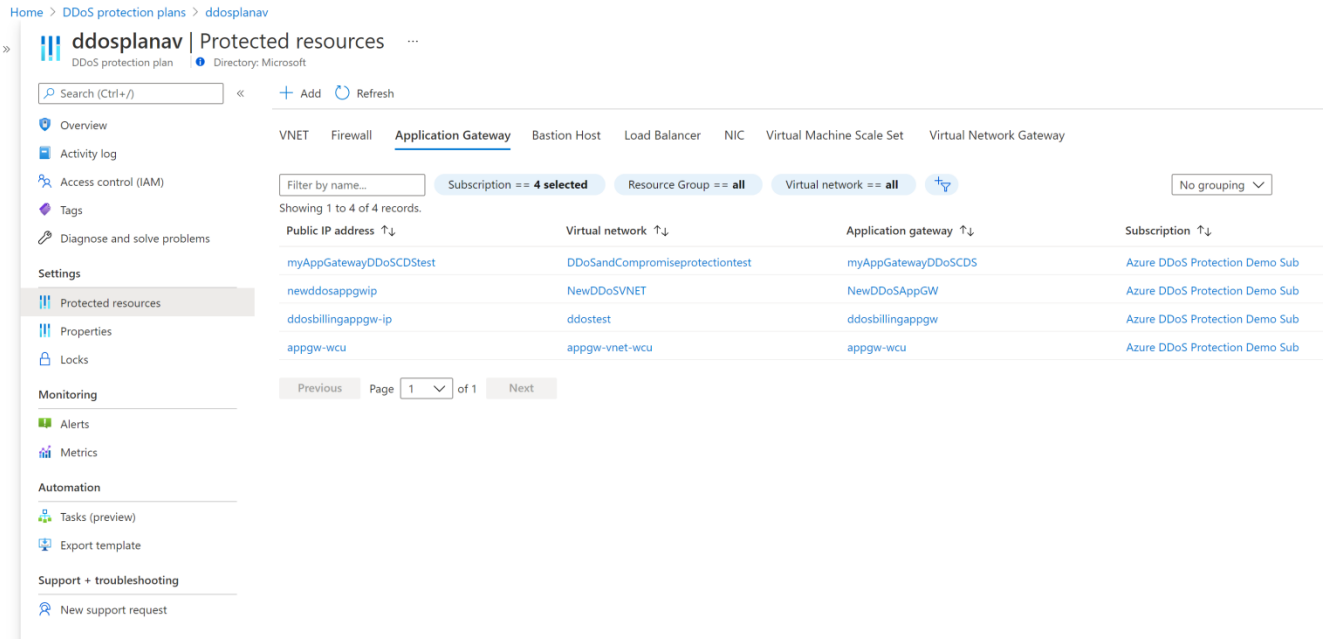

Рис. 3.3. Розділ Захищені ресурси

Побачити показники плану захисту від DDoS можна на відповідній вкладці, яка показано на рис. 3.4.

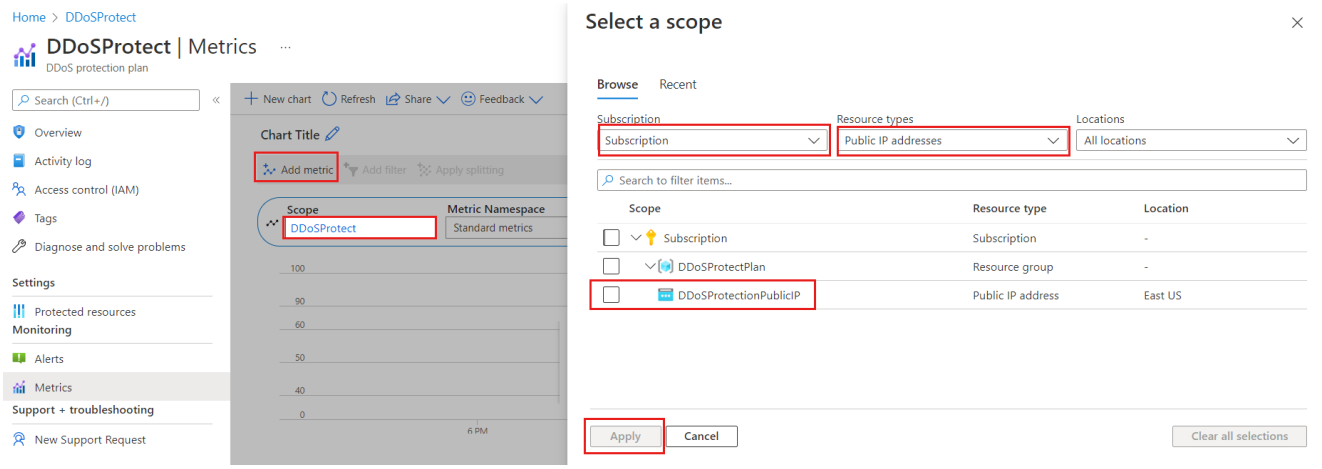

Рис. 3.4. Розділ Показники плану захисту від DDoS

Azure DDoS Protection застосовує три автоматично налаштовані політики пом’якшення (TCP SYN, TCP і UDP) для кожної публічної IP-адреси захищеного ресурсу у віртуальній мережі, у якій увімкнено захист від DDoS. Ви можете переглянути порогові значення політики, вибравши вхідні TCP-пакети для ініціювання пом’якшення DDoS-атак і вхідні пакети UDP для ініціювання

показників пом’якшення DDoS-атак із типом агрегації «Макс», як показано на рис. 3.5.

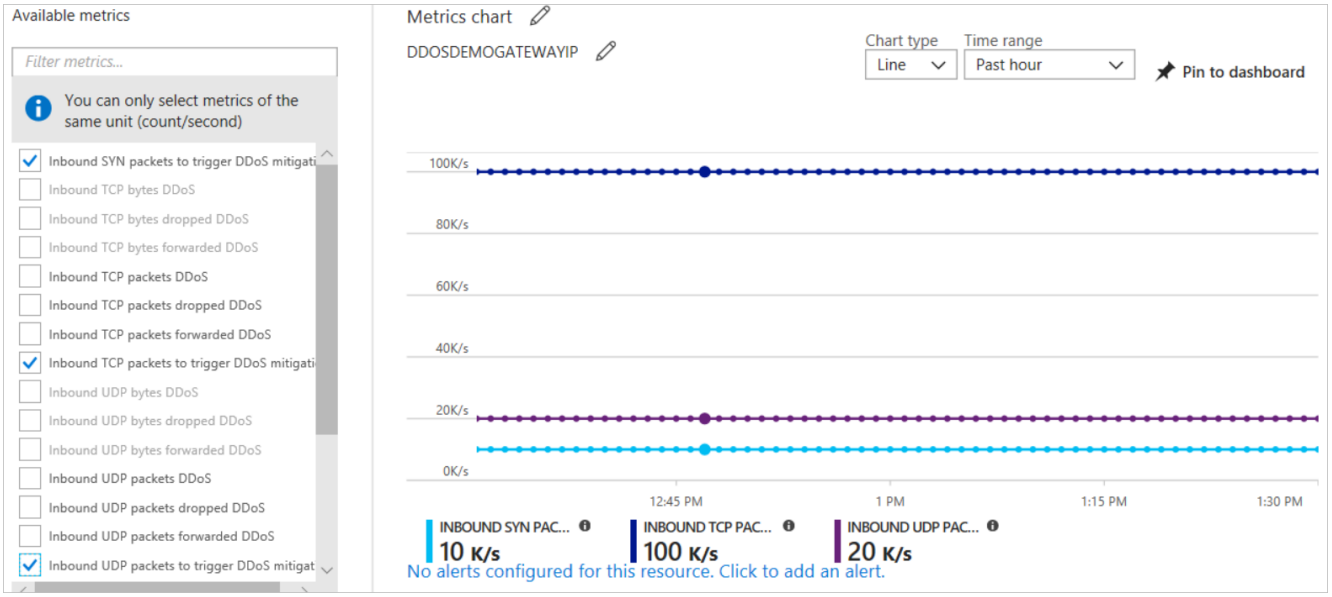

Рис. 3.5. Розділ політики запобігання DDoS

Хорошою практикою є перевірка припущень щодо того, як служби реагуватимуть на атаку, проводячи періодичне моделювання.

Ми можемо налаштувати тестову DDoS атаку за такими даними, які показано в таблиці 3.1.

Таблиця 3.1

Значення налаштувань тестової DDoS атаки

Налаштування	**Значення**
Цільова IP-адреса	Введіть одну зі своїх загальнодоступних IP-адрес, які ви хочете перевірити.
Номер порту	Введіть *443* .
Профіль DDoS	Серед можливих значень: `DNS Flood`, `NTPv2 Flood`, `SSDP Flood`, `TCP SYN Flood`, `UDP 64B Flood`, `UDP 128B Flood`, `UDP 256B Flood`, `UDP 512B Flood`, `UDP 1024B Flood`, `UDP 1514B Flood`, `UDP Fragmentation`, `UDP Memcached`.
Розмір тесту	Можливі значення включають `100K pps, 50 Mbps and 4 source IPs`, `200K pps, 100 Mbps and 8 source IPs`, `400K pps, 200Mbps and 16 source IPs`, `800K pps, 400 Mbps and 32 source IPs`.
Тривалість тесту	Можливі значення включають `10 Minutes`, `15 Minutes`, `20 Minutes`, `25 Minutes`, `30 Minutes`.

Під час тестування необхідно переконайтеся, що наші служби чи додатки продовжують функціонувати належним чином і немає перешкод у роботі користувача. Визначте прогалини з точки зору технології та процесу та включіть їх у стратегію реагування на DDoS. Рекомендується виконувати такі тести в робочих середовищах або в непікові години, щоб мінімізувати вплив на робоче середовище.

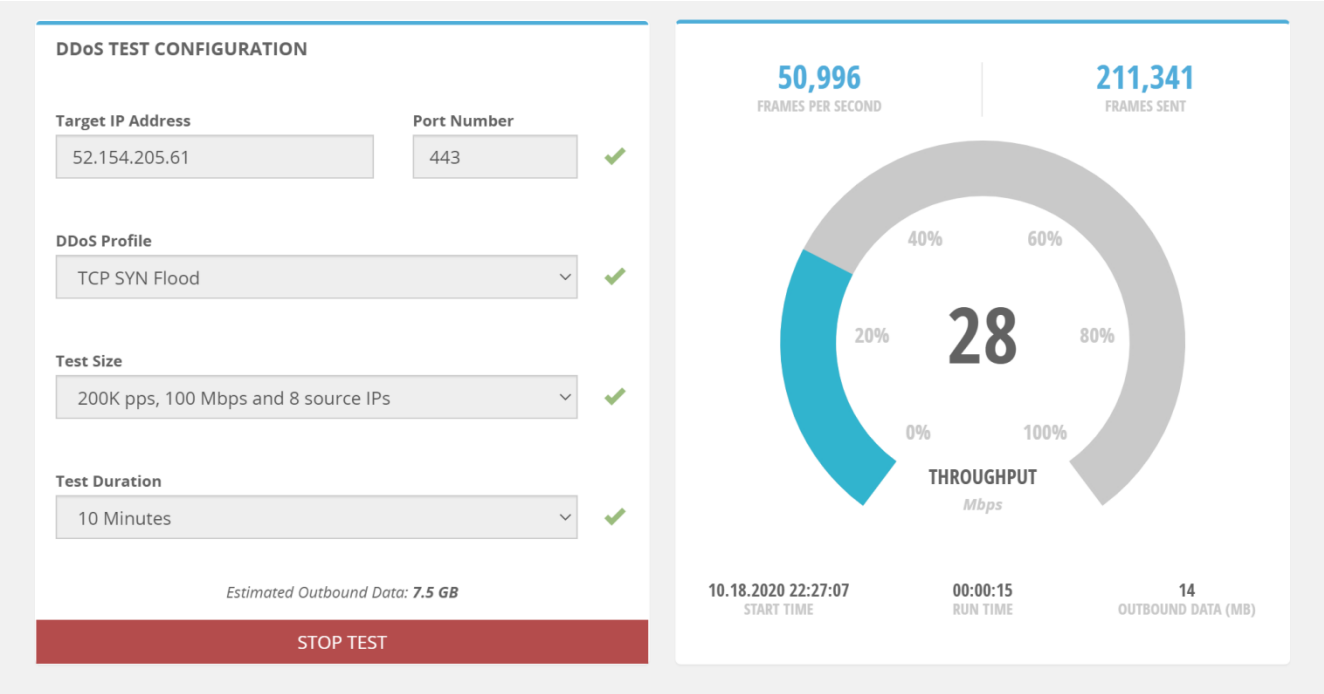

Рис. 3.6. Інтерфейс налаштування тестової DDoS атаки

Тестування DDoS атаки необхідно для:

перевірки, як Azure DDoS Protection допомагає захистити корпоративні ресурси Azure від атак DDoS;

оптимізації процесу реагування на інцидент під час DDoS-атаки;

задокументування відповідності захисту від DDoS;

навчання команди мережевої безпеки.

3.3. Рекомендації щодо захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ

Термін «пом’якшення DDoS» стосується процесу успішного захисту цілі від розподіленої атаки на відмову в обслуговуванні [15].

Типовий процес пом’якшення наслідків DDoS-атаки можна загалом визначити чотирма етапами, які показано на рис. 3.7 [15].

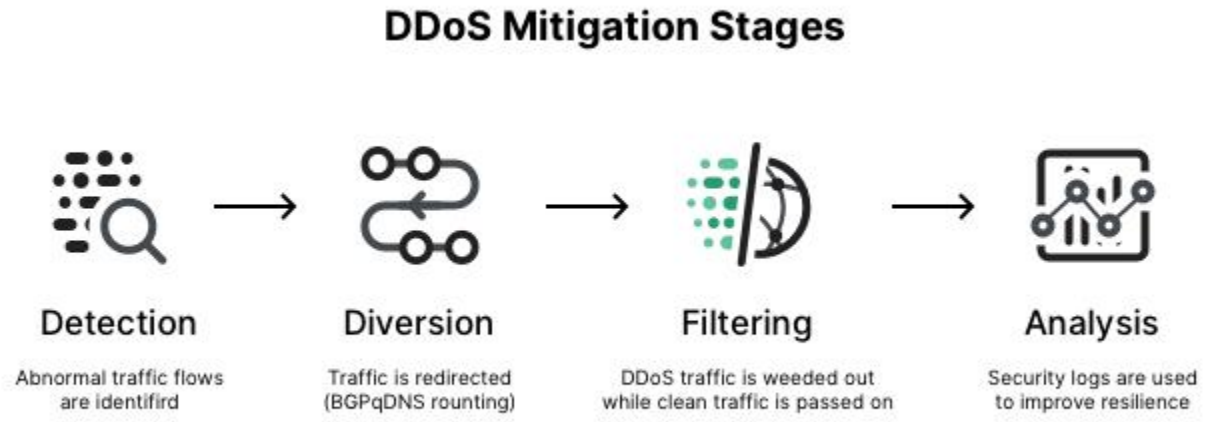

Рис. 3.7. Типовий процес пом’якшення наслідків DDoS-атаки [15]

Виявлення – ідентифікація відхилень потоку трафіку, які можуть сигналізувати про накопичення DDoS-атаки. Ефективність вимірюється здатністю розпізнати атаку якомога раніше, при цьому миттєве виявлення є кінцевою метою.

Перенаправлення – трафік перенаправляється від цільового маршруту за допомогою маршрутизації DNS (система доменних імен) або BGP (протокол прикордонного шлюзу), і приймається рішення, фільтрувати його чи взагалі відкидати. DNS-маршрутизація завжди ввімкнена, тому вона може швидко реагувати на атаки та ефективна проти атак як на прикладному, так і на мережевому рівнях. Маршрутизація BGP є постійною або на вимогу.

Фільтрація – DDoS-трафік відсіюється, як правило, шляхом виявлення шаблонів, які миттєво розрізняють законний трафік (тобто люди, виклики API та

роботи пошукових систем) і зловмисних відвідувачів. Швидкість реагування – це функція здатності блокувати атаку, не заважаючи роботі користувачів. Мета полягає в тому, щоб рішення було повністю прозорим для відвідувачів сайту.

Аналіз – системні журнали та аналітика можуть допомогти зібрати інформацію про атаку як для ідентифікації порушника(ів), так і для покращення майбутньої стійкості. Ведення журналу – це застарілий підхід, який може надавати статистичні дані, але не в реальному часі та може вимагати детального аналізу вручну. Розширені методи аналітики безпеки можуть запропонувати точне бачення трафіку атак і миттєве розуміння деталей атаки.

Вибір постачальника пом'якшення наслідків DDoS-атаки є найважливішим моментом. Є кілька інших ключових аспектів, які ви повинні враховувати, обираючи постачальника пом'якшення наслідків DDoS-атаки. До них належать:

ємність мереж. Пропускна здатність мережі залишається чудовим способом порівняльного аналізу служби пом'якшення DDoS. Він відображає загальну масштабованість, доступну вам під час атаки.

Наприклад, мережа зі швидкістю 1 Тбіт/с (терабіт на секунду) теоретично може блокувати до такого ж обсягу трафіку атак за вирахуванням пропускної здатності, необхідної для підтримки її регулярних операцій.

Більшість хмарних служб пом'якшення надають мережеву пропускну здатність із кількома Тбіт/с, що значно перевищує те, що будь-якому окремому клієнту може знадобитися. З іншого боку, локальні пристрої пом'якшення DDoS обмежені за замовчуванням – як розміром мережевого каналу організації, так і потужністю внутрішнього обладнання.

Ключові характеристики:

доступна пропускна здатність – вимірюється в Гбіт/с або Тбіт/с, доступна для захисту від атаки. Атака, яка перевищує пропускну здатність вашого постачальника DDoS, вразить ваші сервери;

модель розгортання – хмарне або локальне рішення. Хмарні рішення є еластично масштабованими та можуть захистити від масових DDoS-атак.

обробна потужність. Окрім пропускної спроможності, слід також звернути

увагу на можливості обробки вашого рішення пом’якшення. Вони представлені швидкістю пересилання, виміряною в Mpps (мільйонах пакетів за секунду).

Сьогодні нерідко атаки досягають піку понад 50 Mpps, а деякі досягають 200-300 Mpps і більше. Напад, який перевищить обчислювальну потужність вашого постачальника пом’якшення, порушить його захист, тому вам слід запитати про таке обмеження заздалегідь.

Ключові характеристики:

швидкість пересилання – вимірюється в Mpps. Атака, яка перевищує швидкість пересилання вашого постачальника DDoS, вразить ваші сервери.

техніка пересилання – маршрутизація DNS або BGP. DNS-маршрутизація завжди ввімкнена та може захистити від атак як на прикладному, так і на мережевому рівнях. Маршрутизація BGP може захистити практично від будь-яких атак і може бути постійно включеною або активуватися на вимогу.

затримка. Важливо розуміти, що в якийсь момент законний трафік до вашого веб-сайту або додатка проходитиме через мережу постачальника DDoS:

якщо служби DDoS працюють на вимогу, трафік перемикається на постачальника DDoS, коли відбувається атака;

якщо DDoS-послуги постійно включені (що має значні переваги), весь ваш трафік буде проходити через сервери провайдера.

З’єднання між центром обробки даних і постачальником DDoS має бути дуже ефективним, інакше це може призвести до високої затримки для ваших користувачів. Ви повинні оцінити:

які географічні точки присутності (PoP) пропонує постачальник DDoS і наскільки близько вони до ваших центрів обробки даних;

чи пропонує ваш постачальник DDoS-атак PoPs, де розташована ваша основна клієнтська база;

чи пропонує постачальник DDoS найсучасніші методи маршрутизації для забезпечення оптимального підключення до вашого центру обробки даних і користувачів.

Перший пункт є найважливішим – розглянемо, наприклад, компанію в Індії,

яка працює зі службою DDoS, яка має PoP лише в Європі. Кожен запит користувача повинен буде відправлятися до європейського PoP, звідти до центру обробки даних в Індії, назад до європейського центру обробки даних і назад до користувача.

Це станеться, навіть якщо користувач фактично перебуває в Європі. Якщо користувач, як і компанія в нашому прикладі, знаходиться в Індії чи іншому непідтримуваному місці, затримка збільшується в рази.

Два варіанти:

завжди ввімкнено – завжди переходить до постачальника захисту від DDoS;

на вимогу – при нападі.

час для пом'якшення. Після виявлення атаки критично важливий час для пом’якшення. Більшість нападів можуть знищити ціль за лічені хвилини, а процес відновлення може тривати години. Негативний вплив такого простою потенційно може відчути ваша організація на тижні та місяці вперед.

Забезпечуючи попереджувальне виявлення, завжди ввімкнені рішення мають тут явну перевагу. Вони пропонують майже миттєве пом’якшення, часто захищаючи організації від першого залпу під час будь-якого нападу. Шукайте рішення, яке може відповісти на атаку за лічені секунди.

Але не всі постійно включені рішення пропонують такий рівень відгуку. Ось чому під час оцінки постачальника засобів захисту від DDoS, на додаток до тестування під час випробування служби, запит про час до пом’якшення має бути у вашому контрольному списку.

пом'якшення мережевого рівня. DDoS-атаки мережевого рівня мають об’ємний характер – вони покладаються на дуже великий трафік, який може завдати більшої шкоди вашій інфраструктурі. Постачальники DDoS-атак використовують кілька методів для запобігання мережевим атакам. Усі ці методи мають на меті відокремити законний трафік від зловмисного , позбутися зловмисних пакетів, дозволяючи законним пакетам досягти місця призначення.

Перевірте, які методи підтримуються вашим постачальником захисту від DDoS:

нульова маршрутизація – нульова маршрутизація (так відома як blackholing) спрямовує весь трафік на неіснуючу IP-адресу. Його недоліком є те, що він, ймовірно, спричинить високий відсоток хибних спрацьовувань – утилізацію як зловмисних, так і законних відвідувачів;

sinkholing – цей метод відволікає зловмисний трафік від його цілі, зазвичай використовуючи список відомих зловмисних IP-адрес для ідентифікації трафіку DDoS. Хоча не такий невибірковий, як нульова маршрутизація, синкхолінг все ще схильний до помилкових спрацьовувань, оскільки IP-адреси ботнету також можуть використовувати законні користувачі. Крім того, синкхолінг неефективний проти IP-спуфінгу – типової риси атак на мережевому рівні;

очищення – вдосконалення довільного синкхолінгу, очищення маршрутів усього вхідного трафіку через службу безпеки. Шкідливі мережеві пакети ідентифікуються на основі їхнього вмісту заголовка, розміру, типу, точки походження тощо. Завдання полягає в тому, щоб виконати очищення з вбудованою швидкістю, не викликаючи затримок або іншим чином не впливаючи на законних користувачів;

маскування IP -адреси – цей метод запобігає DDoS-атакам прямо на IP-адресу, приховуючи IP-адресу вихідного сервера;

захист прикладного рівня. DDoS-атаки прикладного рівня (рівень OSI 7) є набагато більш прихованими, ніж аналоги мережевого рівня, зазвичай імітуючи законний трафік користувачів, щоб уникнути заходів безпеки. Щоб зупинити їх, ваше рішення має мати можливість профілювати вхідний трафік HTTP/S, розрізняючи DDoS-ботів і законних відвідувачів.

Ключові риси:

кілька методів перевірки для виявлення легітимного трафіку – служба має перевіряти IP-адресу та номер автономної системи (ASN), забезпечувати перехресну перевірку вмісту заголовка HTTP/S і перевіряти моделі поведінки, щоб побачити, чи є кожен сеанс законним сеансом користувача чи частиною DDoS-атака;

численні виклики – багато служб безпеки використовують виклики, щоб

перевірити, чи є трафік зловмисним чи легітимним, наприклад перевіряючи кожен запит на його здатність аналізувати JavaScript і зберігати файли cookie. Переконайтеся, що служба не використовує надмірно CAPTCHA, «затримку сторінок» та інші методи фільтрації, які можуть дратувати законних відвідувачів і зашкодити взаємодії з веб-сайтом;

захист вторинних активів. Ваша мережева інфраструктура, ймовірно, складається з кількох серверів та інших IT-активів. Це можуть бути веб-сервери, DNS-сервери, сервери електронної пошти, FTP-сервери та платформи бек-офісу CRM або ERP. У сценарії DDoS-атаки вони також можуть стати мішенню зловмисника, спричиняючи простої або іншим чином паралізуючи ваш бізнес.

Оцініть ризик усієї мережевої інфраструктури та визначте, які компоненти потрібно захистити. Принаймні майте на увазі, що ваша служба DNS є однією з найпоширеніших цілей атак і єдиною точкою збою.

Ключові риси:

захист сервера імен DNS – захист від затоплення DNS та інших методів DDoS, спрямованих на збій або порушення роботи серверів імен DNS;

захист програм – захист поширених додатків, таких як електронна пошта, FTP, CRM, ERP;

захист індивідуальних IP. Традиційно хмарні служби захисту від DDoS могли захищати лише цілі діапазони IP-адрес. Було важко поширити цей захист на конкретні хмарні середовища та активи, аж до рівня окремих IP-адрес.

Розширені служби DDoS пропонують захист для окремих IP-адрес, дозволяючи зареєструвати загальнодоступну IP-адресу або доменне ім’я, додати службу DDoS до конфігурації DNS і ввімкнути негайний захист цієї конкретної IP-адреси.

технічна підтримка. Навіть якщо ваша служба DDoS повністю автоматизована, що є кращим, оскільки вона дозволяє швидко реагувати на атаку, переконайтеся, що ваш провайдер пропонує професійні послуги підтримки. Коли відбувається атака, вам може знадобитися поговорити зі своїм провайдером, щоб зрозуміти, що відбувається, і вирішити критичні проблеми, які впливають на ваш

законний трафік.

Переконайтеся, що у вашій службі пом’якшення DDoS працює Центр безпеки (SOC) із фахівцями з безпеки, доступними для виклику 24x7x365 для екстреної допомоги.

Треба мати на увазі, що різноманітний спектр технологій, послуг і постачальників становить ринок захисту від DDoS. Спеціалізовані компанії, які спеціалізуються на безпеці, пропонують більш просунуті рішення, як правило, з експертами, присвяченими постійним дослідженням безпеки та цілодобовому моніторингу нових векторів атак. Універсали, такі як Інтернет-провайдери та хостинг-провайдери, пропонують базові рішення пом’якшення як «доповнення» до своїх основних послуг з метою підвищення їх цінності для існуючих клієнтів.

Послуги з пом’якшення, які пропонують спеціалісти широкого профілю, можуть бути достатніми для невеликих простих атак. Але якщо ваші онлайн-додатки є важливими для повсякденних бізнес-операцій, спеціалізований постачальник захисту від DDoS є найкращим і найменш ризикованим вибором для вашої організації.

У той же час, вибираючи постачальника засобів безпеки, ви повинні враховувати їхні додаткові пропозиції безпеки. Крім пом’якшення DDoS-атак, досвідчений постачальник запропонує інші рішення безпеки, такі як безпека додатків, даних і захист мережі. Надавайте перевагу продукту DDoS, який інтегровано з додатковими функціями безпеки, надаючи вашій організації всебічне рішення безпеки.

ВИСНОВКИ

В роботі проведено дослідження проблеми захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ як складової частини забезпечення кібербезпеки її інформаційних ресурсів.

Microsoft Azure – це платформа хмарних обчислень, яка допомагає розробляти, зберігати дані, розміщувати та керувати послугами. Інструмент Azure розміщує веб-додатки через Інтернет за допомогою центрів обробки даних Microsoft. Тому, Microsoft Azure широко застосовується у сучасних організаціях.

Проаналізовано існуючі технології захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ. Досліджено методи та засоби захисту від DDoS атак на інформаційні ресурси організації в Azure.

Встановлено, що захист від атак DDoS Azure у поєднанні з рекомендаціями щодо проектування додатків надає розширені функції захисту від атак DDoS. Захист від атак DDoS Azure автоматично налаштовується для захисту конкретних ресурсів Azure у віртуальній мережі.

Сервіс захисту від атак DDoS Azure розроблено для служб, які розгортаються у віртуальній мережі. В роботі розглянуто різні еталонні архітектури відповідно до сценаріїв застосування.

Для того, щоб захистити сервіс в Microsoft Azure, необхідно розуміти архітектуру даного додатку та зосередитися на п’яти стовпах якості програмного забезпечення. Необхідно знати типові обсяги трафіку, модель підключення між додатком та іншими додатками, а також кінцеві точки служби, доступні для загальнодоступного Інтернету.

У роботі розглянуто порядок застосування політики пом’якшення Azure DDoS Protection. Від правильного налаштування системи захисту залежить ефективність протидії DDoS-атакам.

У роботі розглянуто порядок створення плану захисту від DDoS-атак за допомогою порталу Azure. Планування та підготовка мають вирішальне значення,

щоб зрозуміти, як працюватиме система під час DDoS-атаки. Розробка плану реагування на інциденти є частиною цих зусиль.

Розроблено рекомендації фахівцям з кібербезпеки щодо захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ.

Таким чином, правильна реалізація технології захисту від DDoS атак на інформаційні ресурси організації при застосуванні хмарних платформ має забезпечити ефективний захист корпоративних даних та кібербезпеку інформаційної системи організації.

ПЕРЕЛІК ПОСИЛАНЬ

1. Розподілена атака на відмову в обслуговуванні (DDoS). [Електронний ресурс] – Режим доступу: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/distributed-denial-of-service/.

2. Sergiu Gatlan. Microsoft mitigates largest DDoS attack 'ever reported in history'. January 27, 2022. [Електронний ресурс] – Режим доступу: https://www.bleepingcomputer.com/news/security/microsoft-mitigates-largest-ddos-attack-ever-reported-in-history/.

3. Що таке кібербезпека і як бізнесу захиститися від DDOS-атак. GigaCloud. [Електронний ресурс] – Режим доступу: https://gigacloud.ua/blog/navchannja/scho-take-kiberbezpeka-i-jak-biznesu-zahistitisja-vid-ddos-atak.

4. Микита Захаров. З технічного боку. Як компаніям захиститися від DDoS-атак: пояснюють кіберексперти. [Електронний ресурс] – Режим доступу: https://forbes.ua/company/s-tekhnicheskoy-storony-kak-kompaniyam-zashchititsya-ot-ddos-atak-obyasnyayut-kibereksperty-17022022-3733.

5. Kotikalapudi Sriram, Doug Montgomery. Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation. NIST Special Publication 800-189. – 81 pp. https://doi.org/10.6028/NIST.SP.800-189.

6. David Holmes with Joseph Blankenship, Alexis Bouffard, Peggy Dostie. The Forrester Wave™: DDoS Mitigation Solutions, Q1 2021. The 11 Providers That Matter Most And How They Stack Up. WAVE REPORT. March 3, 2021. https://reprints2.forrester.com/#/assets/2/596/RES159092/report.

7. Akamai Product Brief. Prolexic. Defend internet-facing infrastructure against DDoS attacks. [Електронний ресурс] – Режим доступу: https://www.akamai.com/resources/product-brief/prolexic-routed-product-brief.

8. Заблокуємо атаку будь-якого масштабу за три секунди – DDoS protection. [Електронний ресурс] – Режим доступу:

https://softprom.com/ua/vendor/imperva/product/imperva-ddos-protection.

9. Sergiu Gatlan. Microsoft announces enterprise DDoS protection for SMBs. October 19, 2022. [Електронний ресурс] – Режим доступу: https://www.bleepingcomputer.com/news/microsoft/microsoft-announces-enterprise-ddos-protection-for-smbs/

10. Amir Dahan. Enterprise-grade DDoS protection for SMBs now available in preview. 19 October, 2022. [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-gb/blog/enterprisegrade-ddos-protection-for-smbs-now-available-in-preview/

11. Richard Peterson. Microsoft Azure Tutorial for Beginners: Learn Basics in 1 Day. Updated October 15, 2022. [Електронний ресурс] – Режим доступу: https://www.guru99.com/microsoft-azure-tutorial.html

12. Azure DDoS Protection documentation. Learn how the Azure DDoS Protection, when combined with application design best practices, provides defense against DDoS attacks. [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/ddos-protection/

13. Azure DDoS Protection reference architectures [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/ddos-protection/ddos-protection-reference-architectures

14. Quickstart: Create and configure Azure DDoS Network Protection using the Azure portal [Електронний ресурс] – Режим доступу: https://learn.microsoft.com/en-gb/azure/ddos-protection/manage-ddos-protection

15. DDoS Mitigation: The Definitive Buyer’s Guide. Imperva. [Електронний ресурс] – Режим доступу: https://www.imperva.com/learn/ddos/ddos-mitigation-services/

16. Фічоряк В. Я. Технологія захисту від DDoS атак на інформаційні ресурси організації в AZURE. Всеукраїнська наукова конференція «Актуальні проблеми кібербезпеки». Державний Університет Телекомунікацій. 27 жовтня 2022. Тези доповідей. С. 41-46. [Електронний ресурс] – Режим доступу: https://dut.edu.ua/uploads/p_2121_20358827.pdf

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

(Презентація)