УДК 004

С.Талмазан, магістр гр. КІ-24М,
Центральноукраїнський національний технічний університет

ДОСЛІДЖЕННЯ ТА ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ПРОТИДІЇ МЕРЕЖЕВИМ DDOS-АТАКАМ

У статті розроблено програмне забезпечення, яке призначено для системи протидії мережевим DDoS-атакам. Метою розробки є дослідження та принципи побудови системи протидії мережевим DDoS-атакам. Об'єктом дослідження є процес протидії мережевим DDoS-атакам. Предметом дослідження є методи протидії мережевим DDoS-атакам. Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення. Результат роботи – програмна реалізація системи протидії мережевим DDoS-атакам. В процесі роботи над програмною моделлю виконано аналіз існуючих апаратних та програмних засобів. В повній мірі описані всі компоненти розробленого програмного забезпечення.

DDoS-атака

Постановка проблеми. Забезпечення захищеності мережі від DDoS-атак вимагає добре структурованої захисної стратегії. Мережа часто містить численні ресурси – веб-сайти, програми та сервіси – не лише для своїх власників, але й для їхніх клієнтів.

Масштабна DDoS-атака, спрямована лише на один із цих ресурсів, може створити величезне навантаження на мережеву інфраструктуру. Різке збільшення незаконного трафіку може перевантажити навіть найпотужніші маршрутизатори, що призведе до перебоїв у роботі та потенційних збоїв.

І це не просто теорія – DDoS-атаки, що досягають сотень гігабіт на секунду, зараз є поширеним явищем. Нещодавно ми навіть зафіксували атаку потужністю 1,5 Тбіт/с.

Зрозуміло, що само по собі обладнання та програмне забезпечення на периферії ледве справляються з такими масованими атаками, що робить хмарні рішення для боротьби з DDoS-атаками необхідністю.

Проблему посилює те, що мережеві оператори зазвичай керують великими пулами IP-адрес, які зловмисники використовують, одночасно запускаючи численні менші DDoS-атаки. Ці атаки низької інтенсивності можуть залишитися непоміченими традиційними засобами захисту, але їхній сукупний вплив на периферійні пристрої може бути серйозним, що призводить до зниження продуктивності, операційної нестабільності або навіть повного виходу з ладу вузла.

Аналіз останніх досліджень і публікацій. При аналізі останніх досліджень і публікацій [1-30] було виявлено певні прогалини у забезпеченні системи протидії мережевим DDoS-АТАКАМ.

Мета й завдання дослідження. Метою роботи є дослідження та принципи побудови системи протидії мережевим DDoS-атакам.

Для досягнення поставленої мети визначена програма дослідження, що складається з наступних завдань:

– Огляд існуючих систем протидії мережевим DDoS-атакам.
– Дослідження системи протидії мережевим DDoS-атакам.
– Програмна реалізація системи протидії мережевим DDoS-атакам.

Об'єктом дослідження є процес протидії мережевим DDoS-атакам.

Предметом дослідження є методи протидії мережевим DDoS-атакам.

Методи дослідження базуються на методах захисту інформації у комп'ютерних мережах, методах математичної статистики, методах розробки програмного забезпечення.

Виклад основного матеріалу. Закрийте невикористовувані порти та приховайте невикористовувані IP-адреси

Ваша мережа повинна виглядати якомога більше схожою на «чорну скриньку» з точки зору зловмисника. Хакери часто шукають вразливості, слабкі місця та незахищені ресурси – іноді навіть ті, які ви могли пропустити під час аудиту – щоб розпочати DDoS-атаки.

Щоб мінімізувати цей ризик, створіть детальний список активних та неактивних мережевих служб і ресурсів. Потім закрийте все, що не використовується, щоб запобігти їхньому використанню зловмисниками.

Ви також захочете ускладнити зловмисникам аналіз вашої мережі. Одна з ефективних стратегій – приховати IP-адреси вашого пірингу від Traceroute, як зовні, так і зсередини. Майте на увазі, що загрози можуть виходити не лише від зовнішніх зловмисників, а й від інсайдерів – це включає ваш власний персонал або співробітників компаній-клієнтів, які розміщують свої ресурси у вашій мережі.

Для адрес, які неможливо приховати, захистіть їх за допомогою списків контролю доступу (ACL). Зверніться до свого постачальника послуг захисту від DDoS, щоб налаштувати це.

Забезпечення належної продуктивності периферійних пристроїв

Одна з найпоширеніших причин, чому мережі страждають від DDoS-атак, – це недостатньо потужні периферійні пристрої – маршрутизатори, брандмауери, балансувальники навантаження та інші компоненти інфраструктури. Ці пристрої можуть добре обробляти звичайний трафік, але навіть відносно невелика DDoS-атака може вивести їх з ладу.

Ми часто стикаємося з брандмауерами Cisco ASA (особливо старішими моделями) та маршрутизаторами MikroTik, які виходять з ладу під час атак. Багато мереж також покладаються на апаратне забезпечення для невеликих офісів або застаріле обладнання, яке колись було ефективним, але тепер нездатним впоратися із сучасними DDoS-загрозами.

Навіть найкращі рішення проти DDoS-атак не можуть відфільтрувати 100% атаки. Якщо лише 1% масштабної атаки (наприклад, 50 Гбіт/с) обійде фільтрацію, це може перевантажити периферійні пристрої в десятки або навіть сотні разів.

З увімкненою перевіркою стану пакетів (SPI) продуктивність падає ще швидше. У важких випадках пристрої перевантажуються настільки, що не можуть обробляти легітимний трафік або навіть повідомляти про свій стан, що робить усунення несправностей неможливим.

– Визначте слабкі пристрої за допомогою мережевого аудиту та замініть їх на більш продуктивні альтернативи. Без цього навіть найкращий захист від DDoS-атак не запобіжить збоям.

– Розширте пропускну здатність – сильна атака може перевантажити не лише пристрої, але й ваші інтернет-канали. Масштабування існуючої пропускної здатності та додавання резервних каналів допоможе підтримувати стабільність.

Модернізуючи периферійну інфраструктуру та забезпечуючи достатню пропускну здатність, ви можете значно покращити стійкість вашої мережі до DDoS-атак та підтримувати її працездатність навіть під час серйозних атак.

Проведіть стрес-тест

Ви можете оцінити стійкість вашої мережі до DDoS-атак, провівши стрес-тести за допомогою загальнодоступних інструментів, таких як hping3, який входить до складу багатьох дистрибутивів Linux. Ця утиліта дозволяє імітувати різні типи атак з регульованими параметрами. Однак важливо використовувати її обережно, поступово збільшуючи навантаження, щоб уникнути ненавмисних збоїв.

Стрес-тестування також слід регулярно проводити після впровадження захисту від DDoS-атак. Це допомагає оцінити, що відбувається, коли навіть невелика кількість

атакуючого трафіку досягає вашої мережі. Крім того, це дозволяє оцінити швидкість реагування вашого постачальника анти-DDoS-захисту – наскільки швидко вони реагують на атаку, чи надають вони підтримку поза робочим часом і наскільки ефективно вони усувають загрозу.

Читайте також: Чому стрес-тести та інші перевірки захисту від DDoS-атак такі важливі.

Захистіть свої DNS-сервери

У першій половині 2025 року DNS- атаки стали другим за поширеністю типом DDoS-атак, одразу після HTTP-флуду. Це робить захист DNS головним пріоритетом – без нього цілеспрямована атака може спричинити нестабільність, що призведе до проблем з доступністю ресурсів для користувачів.

Якщо ваш DNS-сервер розміщено у вашій мережі, ви можете захистити його за допомогою оголошень BGP, але лише якщо ваш постачальник послуг захисту від DDoS-атак підтримує фільтрацію DNS-атак (не всі вони підтримують!). Якщо ваш постачальник пропонує цю функцію, поділіться з ним адресами своїх DNS-серверів і запросіть налаштовану фільтрацію трафіку для забезпечення стабільної роботи.

Інтегруйте захист від DDoS-атак у свою загальну стратегію безпеки

Захист від DDoS-атак має бути безперешкодно інтегрований у стратегію інформаційної безпеки (ІБ) вашої організації та загальні плани управління кіберризиками. Це не окремий захід – він має працювати синхронно з іншими процесами безпеки, щоб забезпечити комплексний захист від загроз, що постійно змінюються.

Для досягнення цієї мети захист від DDoS-атак має бути тісно узгоджений з:

– Управління вразливостями – виявлення та виправлення слабких місць, перш ніж зловмисники їх скористаються.

– Управління конфігурацією – забезпечення оптимізації налаштувань безпеки для протистояння атакам.

– Реагування на інциденти – наявність чіткого плану виявлення та зменшення DDoS-загроз у режимі реального часу.

– Моніторинг та аудит – безперервна оцінка мережевої активності для виявлення ранніх ознак атаки.

З розвитком DDoS-загроз ваша мережа також повинна адаптуватися:

– Регулярно проводити аудити безпеки та оцінки вразливостей.

– Проаналізуйте минулі атаки, щоб зрозуміти закономірності та запобігти майбутнім загрозам.

– Проведіть стрес-тести, щоб оцінити стійкість вашої мережі під навантаженням.

– Зверніться до свого постачальника анти-DDoS-захисту, щоб проактивно усунути вразливості та покращити конфігурації безпеки.

Постійно вдосконалюючи та узгоджуючи свою стратегію захисту від DDoS-атак із ширшими процесами ІБ, ви забезпечуєте довгострокову стійкість до постійно зростаючої загрози кібератак.

Як запобігти DDoS-атакам у вашій мережі: остаточний контрольний список

1. Проведіть аудит мережі та розробіть стратегію захисту від DDoS-атак.
2. Зберіть ключові мережеві дані для вашого постачальника послуг захисту від DDoS-атак.
3. Закрийте невикористовувані порти та приховайте невикористовувані IP-адреси.
4. Переконайтеся, що периферійні пристрої можуть обробляти DDoS-трафік.
5. Проведіть стрес-тести для оцінки стійкості мережі.
6. Впровадити надійний захист для DNS-серверів.
7. Інтегруйте захист від DDoS-атак у свою загальну стратегію безпеки.

Дотримуючись цих кроків, ви можете захистити свою мережу від DoS-атак і значно зменшити ризик простою через ці загрози.

DDoS-атаки можуть мати шкідливі наслідки для вашої організації, зокрема:

– Фінансові невдачі: Успішна DDoS-атака може призвести до зниження продуктивності, простоїв, втрати доходів та значних витрат на пом'якшення наслідків атаки та відновлення після неї.

– Збої в роботі: DDoS-атаки можуть паралізувати основні операції вашої організації або перешкодити клієнтам у доступі до послуг.

– Шкода репутації: DDoS-атаки можуть потенційно підірвати довіру та лояльність клієнтів, змушуючи їх обирати конкурентів через неможливість доступу до бажаного веб-сайту або сіючи сумніви щодо його надійності.

– Підвищені ризики для безпеки системи**:** DDoS-атаки можуть виявити існуючі слабкі місця в корпоративній мережі, які потім можуть бути використані зловмисниками для здійснення додаткових атак або отримання несанкціонованого доступу до системи.

Хоча кінцевою метою DDoS-атаки є зробити онлайн-сервіс недоступним для користувачів, методи, що використовуються для досягнення цієї мети, можуть відрізнятися. Різні типи DDoS-атак спрямовані на різні частини мережі та класифікуються на основі рівнів мережевого з'єднання, які вони використовують. Три основні типи: об'ємна атака, атака протоколу та атака прикладного рівня.

Об'ємні атаки

Найпоширенішим типом DDoS-атаки є волюметрична атака. Цей тип атаки зосереджений на перевантаженні мережі хибними запитами даних та виснаженні пропускної здатності мережі та можливостей обробки, що призводить до відмови в обслуговуванні для законних користувачів. Це часто досягається за допомогою ботнетів. Прикладом волюметричної атаки є посилення системи доменних імен (DNS), яке використовує відкриті DNS-сервери для надсилання багатьох DNS-запитів до цілі, що призводить до перевантаження трафіку. Атака перевантаження протоколу користувацьких дейтаграм (UDP) – це ще один тип волюметричної DDoS-атаки, метою якої є затоплення певного сервера пакетами інтернет-протоколу (IP) за допомогою UDP. Оскільки сервер не може визначити пункт призначення або цільову програму для цих пакетів, він відповідає повідомленнями «пункт призначення недоступний». Цей потік UDP-трафіку може перевантажити сервер, що призведе до перебоїв у обслуговуванні або простоїв.

Атаки на протоколи

Атаки на протоколи – це тип DDoS-атаки, спрямованої на порушення роботи сервісу шляхом використання вразливостей у протоколах, що використовуються для передачі даних. Мета полягає в перевантаженні ресурсів сервера та/або ресурсів мережевого обладнання, такого як брандмауери та балансувальники навантаження. На щастя, цей тип атаки зазвичай має чіткий слід і його легко виявити.

Прикладом протокольної атаки є атака синхронізації (SYN) перевантаженням, коли зловмисник надсилає цілі надмірну кількість запитів на з'єднання протоколу керування передачею (TCP), використовуючи підроблені вихідні IP-адреси. Цільові сервери намагаються виконати ці запити на з'єднання, але замість успішних з'єднань ціль отримує велику кількість запитів на з'єднання. Це перевантаження запитами виснажує ресурси цілі, фактично зв'язуючи систему та перешкоджаючи їй приймати легітимні з'єднання.

Атаки на рівні додатків

Атаки на рівні додатків спрямовані на слабкі місця в додатку. Ці атаки зосереджені переважно на прямому веб-трафіку та їх може бути важко виявити, оскільки машині може бути важко відрізнити їх від звичайного інтернет-трафіку з великим обсягом.

Поширеною формою атаки на рівні додатків є перевантаження через протокол передачі гіпертексту (HTTP), яке нагадує багаторазове оновлення веб-браузера на кількох комп'ютерах одночасно. Ця надмірна кількість HTTP-запитів перевантажує сервер, що призводить до відмови в обслуговуванні.

Прикладом HTTP-флуду є Slowloris, який в першу чергу націлений на веб-сервери. Під час атаки Slowloris зловмисник надсилає HTTP-запити на веб-сервер, але насправді ніколи не завершує їх. Періодично та повільно зловмисник додає додаткові заголовки, щоб продовжувати обробку запиту, так і не завершивши його. Ця стратегія змушує веб-сервер підтримувати відкриті з'єднання для цих частково завершених HTTP-запитів, що зрештою запобігає прийняттю будь-яких нових з'єднань.

Ще одним прикладом атаки на рівні додатків є ін'єкція структурованої мови запитів (SQL). За допомогою цієї форми SQL-ін'єкції зловмисники маніпулюють полями введення на веб-сайті, щоб виконувати шкідливі SQL-запити до бази даних, що споживатиме потужність веб-сервера та бази даних, а також виснажуватиме ресурси сервера.

З мотивації DDoS-атаки

DDoS-атаки можуть бути ініційовані окремими особами, компаніями та навіть державами, кожна з яких має свої власні мотиви. Ось деякі можливі мотиви DDoS-атак:

1. Хактивізм: Хактивісти використовують DDoS-атаки як метод протесту та привернення уваги до своїх соціальних чи політичних проблем. Їхні цілі можуть включати уряди, політиків та великі бізнес-організації.

2. Вимагання: Вимагання стало популярною мотивацією для DDoS-атак, коли зловмисники вимагають викуп від своїх жертв, щоб зупинити DDoS-атаку.

3. Ідеологічні причини: Деякі зловмисники можуть ініціювати DDoS-атаки, керуючись своїми ідеологічними переконаннями. Це може включати осіб, які прагнуть порушити роботу та завдати шкоди компаніям чи організаціям, які вони вважають неетичними.

4. Кібервійна: Кібервійна зазвичай асоціюється з використанням державами DDoS-атаок, що спонсоруються ними, для отримання політичної та військової переваги. Вони спрямовані на руйнування життєво важливих фінансових, медичних та інфраструктурних систем у країнах, на які спрямовані дії. Ці стратегії передбачають залучення добре навчених фахівців з технологій та пов'язані з урядовими військовими або терористичними організаціями. Багато урядів у всьому світі інвестували значні ресурси для здійснення атак, які порушують роботу онлайн- та критично важливої інфраструктури їхніх супротивників.

5. Конкуренція в бізнесі: DDoS-атаки все частіше використовуються як стратегічний інструмент для конкурентних підприємств. Основною метою застосування такої тактики є завдання фінансової та репутаційної шкоди конкуруючим компаніям з метою порушення їхніх послуг для отримання конкурентної переваги на ринку. Ці атаки можуть приймати різні форми, починаючи від запобігання участі конкурента в онлайн-заходах і закінчуючи повним порушенням їхньої онлайн-операцій на тривалий час.

6. Помста: Деякі особи або групи, які відчувають розчарування через уявну несправедливість, можуть розпочинати DDoS-атаки як помсту проти особи чи організації.

Як виявити DDoS-атаку?

Виявлення DDoS-атаки передбачає розпізнавання ознак, які можуть свідчити про те, що ваша мережа піддається атаці. Наступні ознаки можуть потенційно вказувати на DDoS-атаку:

– Раптове та неочікуване зростання веб-трафіку з певного місця або IP-адреси

o У більшості випадків ці запити на підключення неможливо виконати, оскільки справжнє джерело IP-пакетів приховане.

– Повільна або нестабільна робота мережі, наприклад, затримка завантаження веб-сайту

o Це трапляється, коли зловмисник перевантажує сервер надмірним обсягом запитів, що призводить до помітного уповільнення роботи системи.

– Незрозумілі повідомлення про помилки сервера, тайм-аути або неможливість доступу до вашого веб-сайту

- Це трапляється, коли зловмисник завантажує ваш сервер великою кількістю запитів, що призводить до його перевантаження та виникнення помилки 503 "Служба недоступна", яка зазвичай пов'язана зі збоями в роботі сервісу. Зазвичай це вирішується самостійно, коли вхідний трафік зменшується. Однак, якщо проблема не зникає, це може свідчити про серйознішу проблему, таку як DDoS-атака.

– Працівники скаржаться на повільне з'єднання

- Це особливо актуально, якщо вони використовують те саме мережеве з’єднання, що й ваш вебсайт. У такому випадку це свідчить про те, що продуктивність мережі може бути порушена та пов’язана з DDoS-атакою.

– Зниження продуктивності інших служб, що використовують ту саму мережу

- Часто це відбувається через те, що запити зловмисника перевищують доступну пропускну здатність мережі, що призводить до уповільнення або перебоїв в роботі інших служб.

– Сповіщення від постачальника інтернет-послуг (ISP), постачальника хмарних послуг (CSP) або іншого постачальника послуг

5 стратегій пом'якшення наслідків DDoS-атак

Основною проблемою у запобіганні DDoS-атаці є розрізнення легітимного трафіку та шкідливого трафіку. Проблема виникає через безліч різних типів DDoS-атак в Інтернеті. Ці атаки можуть набувати різних форм, починаючи від атак з одного джерела до складних атак з кількох джерел.

Складні DDoS-атаки можуть використовувати кілька шляхів для перевантаження цілі, одночасно використовуючи різні методи для перенаправлення зусиль щодо пом'якшення наслідків між цими різними маршрутами. Прикладом є одночасне націлювання на кілька рівнів стеку протоколів, наприклад, поєднання атаки посилення DNS з HTTP-флудом. Загалом, чим складніша атака, тим важче відрізнити трафік атаки від легітимного трафіку.

Зловмисники прагнуть залишатися непоміченими, щоб перешкоджати зусиллям щодо пом'якшення наслідків. Щоб ефективно протидіяти цим складним DDoS-атакам, слід впровадити багаторівневе захисне рішення для боротьби з різноманітними маршрутами атак. Ваше рішення має бути розроблене з урахуванням масштабованості, інтегрованого резервування, а також мати можливість моніторити трафік і ефективно керувати вразливостями.

Навчайте своїх співробітників

Навчання ваших співробітників є важливою частиною загальної стратегії кібербезпеки. DDoS-ботнет – це тактика, яку використовують зловмисники для компрометації мережі пристроїв шляхом дистанційного маніпулювання ними, щоб затопити ціль величезним обсягом трафіку. Зловмисники можуть використовувати пристрої нічого не підозрюючих співробітників як частину цього ботнету. Вкрай важливо навчити своїх співробітників, щоб вони розуміли, як захистити свої пристрої від такого використання.

Працівники можуть значно зменшити ризик стати учасником ботнету, дотримуючись наступних запобіжних заходів та впроваджуючи рекомендації, описані у відповідних інструкціях, зазначених нижче.

– Забезпечте регулярне оновлення ваших пристроїв та програмного забезпечення.

– Використовуйте багатофакторну автентифікацію для захисту своїх облікових записів.

– Будьте пильними щодо підозрілих електронних листів та їхніх вкладень.

– Використовуйте надійне рішення для захисту своїх пристроїв від шкідливих програм.

– Використовуйте надійну віртуальну приватну мережу (VPN).

– Резервне копіювання ваших пристроїв та інформації.

Реалізація маршрутизації чорних дір

Чорні діри – це контрзахід для пом'якшення DDoS-атаки шляхом відкидання вхідного трафіку, спрямованого на певну IP-адресу. За допомогою вашого інтернет-провайдера ваш мережевий адміністратор може встановити маршрут чорної діри, який спрямовує весь мережевий трафік на нульовий маршрут. Однак, якщо фільтрація чорних дір не має конкретних критеріїв обмеження, вона може направляти як легітимний, так і шкідливий мережевий трафік у чорну діру, назавжди видаляючи його з мережі. Маршрутизація чорних дір DDoS далеко не ідеальна, оскільки вона по суті досягає мети зловмисника, яка полягає в тому, щоб зробити мережу недоступною та потенційно спричинити втрати для бізнесу. Отже, її слід розглядати як крайній засіб, коли альтернативні методи пом'якшення виявляються неефективними. Незважаючи на свій потенціал допомогти зловмиснику досягти своїх цілей, маршрутизація чорних дір все ще може служити цінній меті, коли ціллю атаки є менший сайт у більшій мережі. У таких ситуаціях перенаправлення трафіку з цільового сайту за допомогою чорних дір може ефективно захистити більшу мережу від негативних наслідків атаки.

Впровадження обмеження швидкості

Обмеження швидкості – це ще один метод зменшення DDoS-атак, який передбачає встановлення обмежень на кількість запитів, які сервер може прийняти до певної IP-адреси протягом певного періоду часу. Це обмежить мережевий трафік і допоможе запобігти перевантаженню системних ресурсів з боку зловмисників. Впровадження обмеження швидкості – це хороший спосіб гарантувати, що законні користувачі все ще можуть отримати доступ до системних ресурсів, не перешкоджаючи загальній продуктивності програми. Хоча цей підхід сам по собі може не забезпечити повного захисту від складних DDoS-атак, він може служити цінним компонентом більш комплексної стратегії зменшення DDoS-атак.

Встановлення брандмауера веб-застосунку

Брандмауер веб-застосунків(WAF) – це захисний інструмент, який використовується для зменшення DDoS-атак на рівні додатків. Він служить зворотним проксі-сервером і створює щит між Інтернетом і вашими додатками. Він допомагає експертам з безпеки виявляти будь-який шкідливий трафік, який намагається порушити роботу ваших сервісів. WAF дозволяє вам контролювати вхідний трафік, дозволяючи або забороняючи доступ на основі попередньо визначеного набору правил безпеки. Ви можете почати з базового набору правил і налаштовувати їх у міру виявлення підозрілих закономірностей, пов’язаних з DDoS-атаками.

Забезпечити постійний моніторинг мережевого трафіку

Безперервний моніторинг (CM) та аналіз мережевого трафіку в режимі реального часу пропонують кілька переваг для виявлення та зменшення потенційних DDoS-атак. Впровадження виявлення вторгненьСистеми виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS) для постійного моніторингу мережевого трафіку ефективні у розпізнаванні та блокуванні підозрілих моделей трафіку, пов'язаних з DDoS-атаками. Використання цих інструментів аналізу трафіку дозволяє раннє виявлення DDoS-атаок, що дозволяє швидко реагувати до ескалації атак. Моніторинг допомагає створити базовий рівень нормальної активності в мережі або комп'ютерних системах. Цей базовий рівень повинен охоплювати як дні із середнім, так і з високим трафіком. Він також допомагає зрозуміти нормальну мережеву активність та моделі трафіку, що полегшує розрізнення легітимного та шкідливого трафіку та виявлення незвичайної або підозрілої активності. Цілодобовий моніторинг також дозволить виявити майбутню атаку навіть у неробочий час та вихідні.

Реалізація розповсюдження мережі anycast

Одноадресна маршрутизація, що широко використовується в мережевому зв'язку завдяки своїй простоті та універсальності, обслуговує різні програми, такі як перегляд веб-сторінок, електронна пошта та передача файлів. В моделі одноадресної розсилки кожен мережевий вузолабо пристрою призначається унікальна IP-адреса, що забезпечує прямий та

ефективний зв'язок по мережі. Однак, незважаючи на свою простоту, одноадресний зв'язок не є стійким до DDoS-атак. Оскільки трафік спрямовується безпосередньо до певного центру обробки даних, DDoS-атака може перевантажити це місце або навколишню інфраструктуру надмірним трафіком. Такий сплеск може призвести до відмови в обслуговуванні, що ускладнить виконання законних запитів. На відміну від одноадресної маршрутизації, мережеве поширення Anycast є більш стійким завдяки своїм унікальним характеристикам маршрутизації та адресації. Anycast розподіляє вхідний трафік по мережі серверів, розподілених у різних місцях, використовуючи одну й ту саму IP-адресу. Цей метод розширює покриття мережі, запобігаючи перевантаженню будь-якого місця шкідливими запитами. Коли на адресу надсилається надзвичайно великий обсяг трафіку, наприклад, під час DDoS-атаки, трафік автоматично перенаправляється до найближчого доступного місця в мережі, тим самим мінімізуючи вплив на основну інфраструктуру.

Маршрутизація Anycast підвищує стійкість мережі, роблячи атаки більш керованими та зменшуючи їхній потенціал для збоїв, тим самим забезпечуючи безперебійну доступність послуг. Широко розповсюджена конфігурація мережі ускладнює для зловмисників виконання DDoS-атаки, оскільки це вимагає значних ресурсів для ефективного надсилання шкідливого трафіку через ботнет.

Проведіть оцінку ризиків

Оцінка ризиків дозволить вам оцінити вразливість вашої організації до DDoS-атак. Вам слід регулярно проводити оцінки ризиків та аудити вашої мережевої інфраструктури, щоб виявити вразливості. Хоча повністю запобігти DDoS-атаці неможливо, повне розуміння апаратних та програмних активів вашої організації, включаючи їхні сильні та слабкі сторони, має вирішальне значення для забезпечення належного захисту. Визначення найбільш вразливих зон у вашій мережі є важливим для визначення найефективнішої стратегії пом'якшення впливу DDoS-атаки.

Проводячи оцінку ризиків, ви:

– Визначте критично важливі активи вашої організації та їх важливість для забезпечення безперервної роботи.

– Аналізуйте та оцінюйте потенційні загрози, що стосуються діяльності вашої організації.

– Визначте вразливості мережі вашої організації, включаючи слабкі місця, які можуть використовувати зловмисники, та оцініть вплив і ймовірність DDoS-атаки на основі історичних даних, розвідки загроз та галузевих тенденцій.

– Визначте різні шляхи, які зловмисники можуть використовувати для ініціювання DDoS-атаки, включаючи такі методи, як UDP-флуд, SYN-флуд або HTTP-флуд.

– Розставте пріоритети між виявленими ризиками, враховуючи такі фактори, як ймовірність здійснення атаки, потенційні наслідки атаки та ймовірність як виявлення, так і пом'якшення наслідків атаки.

Розробка плану реагування на DDoS-атаку

Для ефективної підготовки до DDoS-атаки вкрай важливо мати добре структурований план реагування. Цей план повинен містити чіткі кроки, які допоможуть виявити, пом'якшити та відновитися після атаки. Ваш план також має бути спрямований на мінімізацію впливу на вашу організацію та забезпечення безперебійного або мінімального простою у вашій бізнес-операції.

У рамках цього плану слід враховувати такі компоненти:

– Чітко окресліть та задокументуйте ролі та обов'язки всіх членів команди, які реагуватимуть на DDoS-атаку, включаючи внутрішніх зацікавлених сторін, керівників організації та мережевих адміністраторів, а також будь-яких залучених постачальників послуг.

– Розробіть вичерпний контрольний список, який визначає процеси та дії, необхідні під час DDoS-атаки. Вкажіть необхідні інструменти та ресурси, які будуть потрібні, та визначте осіб, з якими потрібно зв’язатися.

– Розробіть надійний план комунікації, який окреслює заздалегідь визначений ланцюжок зв'язку, якого слід дотримуватися у разі DDoS-атаки.

– Регулярно проводите навчання з реагування на інциденти та переконайтеся, що ваш план реагування на DDoS-атаки є невід'ємною частиною загальної стратегії аварійного відновлення та плану забезпечення безперервності бізнесу вашої організації.

Зверніться до постачальника послуг захисту від DDoS-атак

Якщо ваша організація має обмежені ресурси для управління кібербезпекою, ви можете розглянути можливість співпраці зі сторонніми організаціями для посилення захисту від кіберзагроз. Вони можуть пропонувати різні послуги захисту, включаючи очищення DDoS-трафіку, яке може допомогти захистити ваш інтернет-трафік від DDoS-атаки. Очищення DDoS-трафіку передбачає фільтрацію вхідного трафіку для виявлення та видалення шкідливих даних, дозволяючи лише легітимному трафіку потрапляти до цільової мережі. Це дозволить вам підтримувати онлайн-присутність під час атак, не втрачаючи зв'язку.

Більшість інтернет-провайдерів та постачальників послуг зв'язку пропонують певний рівень захисту від DDoS-атак. Вам слід дізнатися про захисні заходи, які вони надають, та переглянути угоду про надання послуг, щоб визначити будь-які потенційні обмеження їхнього покриття.

Використання хмарних рішень для запобігання DDoS-атак також може запропонувати багато переваг. До них належать спеціалізований персонал, який забезпечує швидший час реагування у разі атаки, та висока пропускна здатність мережі, що робить їх більш стійкими до DDoS-атак на основі обсягів. Ці рішення також можуть забезпечувати автоматичні варіанти реплікації або резервного копіювання, що дозволяє вам запускати свої сервіси, не перериваючи роботу користувачів.

Якщо вам потрібне ще надійніше рішення для захисту від DDoS-атак, зверніться до постачальника керованих послуг (MSP), щоб дослідити рішення, адаптовані до потреб вашої організації для захисту від DDoS-атак. Ці служби вміють активно моніторити ваш мережевий трафік, виявляти будь-які ознаки атаки, визначати її походження та вживати заходів для перенаправлення шкідливого трафіку з вашої мережі.

Звернення до постачальника керованих послуг (MSP) для захисту від DDoS-атак пропонує численні переваги. MSP, що спеціалізуються на кібербезпеці, надають досвід, передові технології та цілодобовий моніторинг для раннього виявлення загроз. Вони швидко реагують на атаки та масштабують послуги відповідно до потреб мережі. MSP постійно оновлюють системи, щоб випереджати нові загрози, забезпечуючи стратегічний та ефективний підхід до захисту онлайн-сервісів. Довіривши захист від DDoS-атак постачальнику керованих послуг (MSP), ваша внутрішня IT-команда може зосередитися на основних бізнес-операціях, а не постійно моніторити та реагувати на потенційні кіберзагрози.

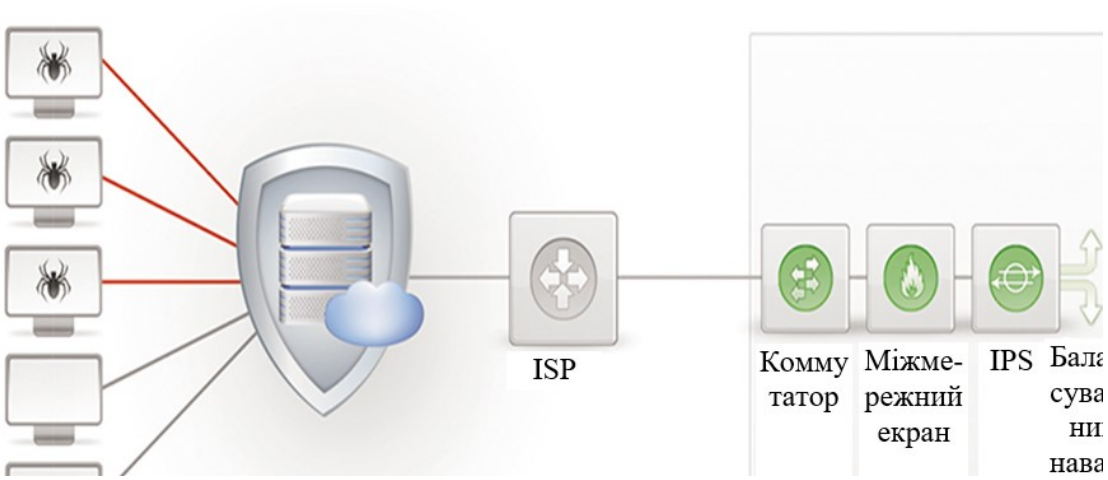

Рисунок 1 – Структурна схема системи

Висновки. У статті наведені теоретичне узагальнення й рішення наукового завдання дослідження методів протидії мережевим DDoS-атакам. Рішення даного завдання полягало у вирішенні наступних задач:

– Був проведений огляд існуючих систем протидії мережевим DDoS-атакам.

– Досліджена система протидії мережевим DDoS-атакам.

– На основі отриманих результатів досліджень створена програмна реалізація системи протидії мережевим DDoS-атакам.

Розроблені алгоритми дозволяють успішно вирішувати завдання протидії мережевим DDoS-атакам. Проведено аналіз предметної галузі в ході якого були виявлені об'єкти, взаємодія яких носить істотний характер для функціональної діяльності предметної галузі, і їхні основні характеристики; побудована алгоритм і вибраний середовище розробки.

Список літератури

1. Smirnov, O., Neskorodieva, T., Fedorov, E., Rudakov, K., Neskorodieva, A. «Method Detection Audit Data Anomalies on Basis Restricted Cauchy Machine» CEUR Workshop Proceedings, Volume 3187, 2022,
2. Smirnov O.A., Al-Oraiqat A.M., Ulichev O.S., Meleshko Ye.V., Al-Rawashdeh H.S., Polishchuk L.I. «Modeling strategies for information influence dissemination in social networks». Journal of Ambient Intelligence and Humanized Computing Volume 13, Issue 5. Springer, Cham. 2022, pp. 2463-2477.
3. Смірнова Т.В., Гнатюк С.О., Сидоренко В.М., Юдін О.Ю., Сидоренко С.Ю., «Модель визначення критичності галузевих інформаційно-телекомунікаційних систем». Проблеми інформатизації та управління, № 2(70). 2022. С. 28-37.
4. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Смірнов С.А., Поліщук Л.І., «Дослідження стійкості до диференціального криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 3(69). С. 93-98.
5. Смірнов О.А., Смірнова Т.В., Якименко Н.М., Поліщук Л.І., Смірнов С.А. «Дослідження статистичної стійкості та швидкісних характеристик запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Вісник Хмельницького національного університету. Серія: «Технічні науки», № 2 (307). С. 46-52. 2022.
6. Смірнов О.А., Смірнова Т.В., Константинова Л.В., Смірнов С.А., Якименко Н.М., «Дослідження стійкості до лінійного криптоаналізу запропонованої функції гешування удосконаленого модуля криптографічного захисту в інформаційно-комунікаційних системах» Системи управління, навігації та зв'язку, 2022, № 1(67). С. 84-89.
7. Smirnov O., Kuznetsov A., Zhora V., Onikiychuk A., Pieshkova O. «Hiding Messages in Audio Files Using Direct Spread Spectrum». 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2021, Cracow, Poland, 22-25 September 2021. P. 414-418
8. Smirnov O., Kuznetsov A., Lokotkova I., Kuznetsova T., Florov S., Lebid O. «Using Orthogonal Signals to Hide Information in Images». 4 IEEE International Conference on Advanced Information and Communication Technologies (AICT) - 2021, Lviv, Ukraine, September 21-25, 2021. P. 255-260.
9. Smirnov O., Kuznetsov A., Girzheva O., Kiian A., Nakisko O., Kuznetsova T. «Advanced Code-Based Electronic Digital Signature Scheme». 2020 IEEE International Conference on Problems of Infocommunications Science and Technology, PIC S and T 2020, Kharkiv, 6 October 2020-9 October 2020, P. 358-362.

10. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova K. «Data hiding scheme based on spread sequence addressing». CEUR Workshop Proceedings Volume 2805, 2020, Pages 44-58.
11. Smirnov, O., Kuznetsov, A., Potii, O., Poluyanenko, N., Stelnyk, I., Mialkovsky, D. «Combining and filtering functions in the framework of nonlinear-feedback shift register». International Journal of Computing; 2020, Volume 19, Issue 2 – Research Institute for Intelligent Computer Systems – 2020. – P. 247-256.
12. Smirnov O., Kuznetsov A., Kiian A., Kuznetsova T. «Non-binary constant weight coding technique». CEUR Workshop Proceedings. Volume 2740, 2020, Pages 102-114.
13. Smirnov O., Alimseitova Zh., Adranova A., Akhmetov B., Lakhno V., Zhilkishbayeva G. «Models and algorithms for ensuring functional stability and cybersecurity of virtual cloud resources». Journal of theoretical and applied information technology Vol.98. No 21, 2020, P. 3334-3346.
14. Smirnov O., Kuznetsov A., Arischenko A., Chepurko I., Onikiychuk A., Kuznetsova T. «Pseudorandom sequences for spread spectrum image steganography». CEUR Workshop Proceedings Volume 2654, 2020, Pages 122-131.
15. Smirnov O., Kuznetsov A., Kovalchuk D., Kuznetsova T. «New technique for data hiding in cover images using adaptively generated pseudorandom sequences». CEUR Workshop Proceedings Volume 2654, 2020, Pages 1-14.
16. Smirnov O., Lutsenko M., Kuznetsov A., Kiian A., Kuznetsova T., «Biometric cryptosystems: overview, state-of-the-art and perspective directions». Lecture Notes in Networks and Systems, vol 152. Springer, Cham. 2021, pp 66-84.
17. Smirnov O., Kuznetsov A., Onikiychuk A., Makushenko T., Anisimova O., Arischenko A. «Adaptive pseudo-random sequence generation for spread spectrum image steganography». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 161-165.
18. Smirnov O., Kuznetsov A., Kiian A., Babenko V., Perevozova I.,Chepurko I. «New Approach to the Implementation of Post-Quantum Digital Signature Scheme». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 166-171.
19. Smirnov O., Kuznetsov A., Kiian A., Cherep A., Kanabekova M., Chepurko I. «Testing of code-based pseudorandom number generators for post-quantum application». 2020 IEEE 11th International Conference on Dependable Systems, Services and Technologies (DESSERT), Ukraine, Kyiv, May 14-18. 2020. P. 172-177.
20. Smirnov O., Kuznetsov A., Pushkar'ov A., Serhiienko R., Babenko V., Kuznetsova T., «Representation of Cascade Codes in the Frequency Domain». In: Radivilova T., Ageyev D., Kryvinska N. (eds) Data-Centric Business and Applications. Lecture Notes on Data Engineering and Communications Technologies, vol 48. Springer, Cham. 2021. pp 557-587.
21. Smirnov, O., Markovets, O. Vovk, N., Turchyn, Y., «Model of informational support for social network administrators' content creation». CEUR Workshop Proceedings Volume 2616, 2020, Pages 125-136.
22. Smirnov, O., Shekhanin, K., Kuznetsov, A., Krasnobayev, V. «Detecting Hidden Information in FAT». International Journal of Computer Network and Information Security (IJCNIS). Vol. 12, No. 3, 2020. PP.33-43.
23. Smirnov, O., Kuznetsov, A., Gorbacheva, L., Babenko, V., «Hiding data in images using a pseudo-random sequence», CEUR Workshop Proceedings Volume 2608, 2020, Pages 646-660.
24. Smirnov, O., Kuznetsov, A., Kolovanova, I., Kuznetsova, T., «Noise immunity of the algebraic geometric codes». International Journal of Computing; 2019, Volume 18, Issue 4 – Research Institute for Intelligent Computer Systems – 2019. – P. 393-407.
25. Smirnov, O., Kuznetsov, A., Reshetniak, O., Ivko, N., Katkova, T., Kuznetsova, T., «Generators of Pseudorandom Sequence with Multilevel Function of Correlation». 2019 IEEE International Scientific-Practical Conference Problems of Infocommunications, Science and Technology (PIC S&T), Kyiv, Ukraine, 8 – 11 October 2019 . P.517-522.
26. Smirnov, O., Ulichev, O., Meleshko, Y., Khokh, V., Goncharenko, I. «Method of Choosing Objects for Informational Influence in Social Networks during Information Campaign Based on the Analytic Hierarchy Process». CEUR Workshop Proceedings, Vol 2588, P. 215-227, 2019.
27. Smirnov, O., Krasnobayev, V., Yanko, A., Kuznetsova, T. «Methods of nulling numbers in the system of residual classes». CEUR Workshop Proceedings, Vol 2588, P. 90-106, 2019.
28. Smirnov, O., Kuznetsov, A., Kiian, A., Gorbenko, Y., Cherep, O., Bexhter L. «Code-based Pseudorandom Generator for the Post-Quantum Period», 2019 IEEE International Conference on Advanced Trends in Information Theory (IEEE ATIT 2019). 18.12.19-20.12.19 Kyiv Ukraine. P. 204 – 209.
29. Smirnov, O., Kuznetsov, A., Nariezhnii, O., Stelnyk, S., Kokhanovska, T., Kuznetsova T., «Side Channel Attack on a Quantum Random Number Generator», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18 -21 September 2019. P.713-718.
30. Smirnov, O., Kuznetsov, A., Kiian, A., Pushkar'ov, A., Mialkovskyi, D., Kuznetsova, T., «Code-Based Schemes for Post-Quantum Digital Signatures», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P. 707-712.
31. Smirnov, O., Kuznetsov, A., Stefanovych, O., Gorbenko, Y., Krasnobaev, V., Kuznetsova K. «Information Hiding Using 3D-Printing Technology», 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, IDAACS 2019; Metz; France; 18-21 September 2019. P.701-706.