Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Пащенко Тимофія Валерійовича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Підвищення рівня захищеності системи авторизації клієнтів мобільного застосунку Travel Helper*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корченко А.О.			
розділів:				
спеціальний	ст.викл. Мєшков В.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст.викл. Мєшков В.І.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня магістра

студенту *Пащенко Тимофію Валерійовичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Підвищення рівня захищеності системи авторизації клієнтів мобільного застосунку Travel Helper***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22 № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Стан питання. Постановка задачі.	04.09.2022
Розділ 2	Оцінили ризики , виявили модель порушника. Впровадили систему TMS 2800 від компанії Arbor	18.11.2022
Розділ 3	Розрахували економічну цінність та актуальність	03.12.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 16.09.2022 р.

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 101 ст, 28 рис., 13 табл., 2 схеми, 4 додатка, 12 джерел.

Об'єкт дослідження: системи захисту від DDOS-атак Arbor, Huawei, DefensePro.

Мета роботи: впровадити в мережу існуючої організації систему захисту від DDOS-атак на сервери автентифікації клієнтів.

Методи розробки: спостереження, порівняння, впровадження, аналіз, опис.

У першому розділі було проаналізована необхідність систем захисту від DDOS-атак, та їх розвиток в сучасному світі. Проаналізували можливі загрози та їх протидію на декількох системах. Визначили яку проблему вирішуюсь данні системи , провели статистичний та морфологічний аналіз систем захисту.

У спеціальній частині було визначено найкращі системи захисту від DDOS-атак, їх можливості та зручність використання. За мету є впровадження системи для захисту від нападу всіх можливих та критично важливих серверів для мобільної мережі для середньої компанії.

В економічному розділі визначено економічну доцільність розробки та впровадження рекомендацій для проведення ідентифікації інформаційних активів. Проведено розрахунок капітальних (фіксованих) витрат, поточних (експлуатаційних) витрат, загального збитку від атаки на ІТС та загального ефекту від впровадження рекомендацій.

Практичне значення роботи полягає в аналізі системі захисту від DDOS-атак, її покращення та впровадження в систему для блокування та аналізу можливих загроз та їх виявлення зазделегідь. Тестування систем на загрозах в реальному часі.

ІНФОРМАЦІЙНА БЕЗПЕКА, DDOS, АВТОРИЗАЦІЯ ЧЕРЕЗ ТОКЕН, ЦІЛІСНІТЬ, ЗАСОБИ ІНФОРМАЦІЇ, АВТОМАТИЗОВАНІ СИСТЕМИ, МАСИВНІ АТАКИ, СЕРВЕРИ АВТЕНТИФІКАЦІЇ

ABSTRACT

Explanatory note: 101 articles, 28 figures, 13 tables, 2 schemes, 4 appendices, 12 sources.

Object of study: : DDOS-attack protection systems Arbor, Huawei, DefensePro.

Purpose: to introduce into the network of an existing organization a system of protection against DDOS-attacks on client authentication servers.

Development methods: observation, comparison, implementation, analysis, description.

The first section analyzed the need for protection systems against DDOS-attacks, and their development in the modern world. Analyzed possible threats and their counteraction on several systems. Determined what problem is solved by these systems, conducted statistical and morphological analysis of protection systems.

In a special part, the best systems of protection against DDOS-attacks, their capabilities and ease of use were identified. The aim is to implement a system to protect against the attack of all possible and critical servers for a mobile network for a medium-sized company.

The economic section determines the economic feasibility of developing and implementing recommendations for the identification of information assets. The calculation of capital (fixed) costs, current (operating) costs, the total damage from the attack on the ITS and the overall effect of the implementation of the recommendations.

The practical significance of the work is to analyze the system of protection against DDOS-attacks, its improvement and implementation in the system to block and analyze possible threats and their detection in advance. Testing of systems on threats in real time.

INFORMATION SECURITY, DDOS, INTEGRITY, MEDIA, AUTOMATED SYSTEMS, MASSIVE ATTACKS, AUTHENTICATION SERVERS

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС - автоматизована система;

ДСТУ - Державні стандарти України;

ЕОТ - електронно-обчислювальна техніка;

ІТС - Інформаційно-телекомунікаційнасистема;

КМ - комп'ютернамережа;

КС - комп'ютерна система;

МП - модель порушника;

ОБ - офіцер безпеки;

ПК - персональний комп'ютер;

РМ - Робоче місце;

API - Application Programming Interface;

DCC - Digital Command Control;

DDoS - це Distributed Denial of Service,

розподілена відмова в обслуговуванні;

ICMP- Internet Control Message Protocol;

HTTPS - Hyper Text Transfer Protocol Secure;

RUDP Reliable User Datagram Protocol;

SCTP Stream Control Transmission Protocol;

TMS – Transportation Management System;

UDP User Datagram Protocol.

ЗМІСТ

ВСТУП

Сучасне життя суспільства неможливе без постійного застосування інформаційних технологій. Комп'ютерні системи обслуговують банківські системи, контролюють роботу на заводах, стежать за розкладом потягів і літаків. Інформаційна індустрія перетворилась на один із найголовніших секторів світової економіки, що динамічно розвивається та має великі перспективи подальшого росту. Інформаційна діяльність сьогодні стала необхідною умовою ефективної діяльності у всіх сферах життя. Протягом останніх років почались змінюватись тенденції, щодо особливостей, місць та обставин роботи компаній. Увесь бізнес починає переходити на зручні для їх клієнтів «Мобільні Застосунки» аби забезпечити своїх клієнтів зручним сервісом для розвитку того чи іншого бізнесу. Тому потреби в захисті інформації від внутрішніх та зовнішніх загроз стали зростати, популярність та необхідність в системах захисту росте з кожним днем.

Приклад, ситуації, коли певні компанії працюють в одній сфері, створюється конкуренція, яка згодом перетворюється на «нечесну гру» з використанням технологій, яка впливає на працездатність. За допомоги базових знань та доступних ресурсів можна здійснити легку атаку на будь-який сервер за допомоги DDoS-атаки. DDoS - це Distributed Denial of Service, розподілена відмова в обслуговуванні. По суті це хакерська атака, яка перевантажує систему, щоб кінцеві споживачі не могли користуватися сервісом. Атака може бути спрямована на всю IT-інфраструктуру, конкретний сервіс або канал до цього сервісу. Найчастіше під атаки даного типу підпадають онлайн сервіси для розрахунків або банківські застосунки аби нашкодити репутації та завдати шкоди організації. Тому вкрай необхідно вміти підлаштовуватись під події і вміти захистити сервіси для стабільної роботи та збереженням данних клієнтів.

Мета роботи: впровадити систему захисту та протидії (сповіщення) від масових DDoS-атак на сервера для автентифікації клієнтів в мобільному застосунку.

Актуальність роботи зумовлюється тим, що в ній було впроваджено рішення, що до захисту та підтримки особливо важливих серверів мобільного застосунку для організації, а також програмні нововведення які дозволяли б відстежувати підозрілий трафік.

Для досягнення даної мети було поставлено такі завдання:

- встановлення систем захисту від DdoS на віртуальні машини та їх налаштування;
- тестування систем, яке полягає в тому, щоб штучно розробити технічний код для атаки (спаму) на тестові сервера мобільного застосунку з метою тестування системи захисту сервера мобільного застосунку від масивних DDoS-атак та вдосконалити реагування на потенційні загрози збоку підозрілого трафіку та відстежувати його зазделегіть. Для цього можна використовувати процес фільтрації шкідливого трафіку.

Методами дослідження обрано: опрацювання літератури за даною темою, аналіз технічної документації, тестування систем захисту.

Практичне значення результатів роботи випливає з можливості використання створенного доповнення для покращення результатів роботи систем захисту, яке дозволить підвищити показники якості виявлення загроз атак. Таким чином об'єктом дослідження є такі популярні системи захистувід таких компаній, як Arbor та Radware.

Предмет досліджень – здатність систем захисту від DDoS-атак реагувати на злочинний трафік, пов'язаний із атакою на сервера мобільного застосунку.

РОЗДІЛ 1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

У цій главі буде проведене ознайомлення з DDoS-атаками, перераховано їх види та актуальність у наш час. Також проаналізуємо роботу мобільного за стосунку, їх взаємодію із серверами. Проаналізуємо системи захисту від масивних атак та оберемо найдієвішу.

1.1 Розподілена відмова в обслуговуванні

DDoS - це Distributed Denial of Service, розподілена відмова в обслуговуванні. По суті це хакерська атака, яка перевантажує систему, щоб кінцеві споживачі не могли користуватися сервісом. Атака може бути спрямована на всю IT-інфраструктуру, конкретний сервіс або канал до цього сервісу.

Розподілена - означає, що атака виконується одночасно з великої кількості пристроїв, які часто розподілені географічно. Це можуть бути як спеціально підготовлені сервери, так і ботнети із заражених пристроїв. Ботнет - це група пристроїв, на яких запущено скрипти, що виконують потрібний зловмиснику код, у цьому випадку - DDoS-атаку. Найчастіше ботнети збираються з пристроїв, заражених шкідливим ПЗ, і їхні власники навіть не підозрюють про "подвійне життя" своїх гаджетів.

DDoS-атака може бути організована з комерційною метою:

- Отримати викуп - обрушити систему і вимагати гроші за припинення атаки.

- Підставити конкурента. Наприклад, обрушити його сайт напередодні великого свята, щоб клієнти нічого не могли замовити і пішли в інший магазин.

Але бувають і некомерційні причини атак:

- геополітичні;

- просто заради розваги;

- заради "хакерської" практики;

- з "образи" на якийсь сайт, сервіс або бренд.

Незалежно від причини DDoS-атака впливає на кінцеву інфраструктуру і робить сервіс або сайт недоступним. Причини у недоступності можуть бути різні, наприклад:

1.Заповнення мережевого каналу паразитним трафіком: порожніми запитами і пакетами.

2.Утилізація ресурсів: ваш веб-сервер або СУБД виявляється завантажений обробкою непотрібних запитів і не може видати реальним клієнтам потрібну інформацію.

Крім недоступності сервісу є й інші наслідки DDoS-атак:

- Якщо ваші сервери в хмарі, а трафік платний, ви можете понести фінансові витрати.

- Якщо сайт буде недоступний більше двох діб, пошукові боти стануть ранжувати вас нижче. Позиції в пошуковій видачі доведеться відновлювати.

- Навіть після відновлення працездатності сервісу клієнти стануть менше вам довіряти і можуть піти до конкурентів.

- Під атакою елементи IT-інфраструктури можуть поводитися некоректно. Наприклад, видавати користувачеві внутрішню інформацію про СУБД, до якої не вдається підключитися.

1.2 Основні види DDOS атак

Вивчаючи тему кібер-атак, значний акцент слід приділити їхнім видам. Ця інформація допоможе краще розібратися в питанні як захистити свій сайт або мобільний застосунок від ddos атак і визначитися з алгоритмом подальших дій.

DDoS-атаки бувають:

- протокольні;

- прикладні;

- атаки на застосунки.

Розглянули всі види і методи ddos атак детальніше.

Протокольні

DDoS-атака націлена на мережевий рівень. Основна мета - спровокувати перезавантаження табличного простору на екрані з брандмауером у мережі. Її ще називають атакою транспортного рівня. Мережевий флуд заведено вважати найпоширенішим методом цього виду. На різних рівнях запускається безліч запитів, з якими вузол не може впоратися. Звичайно ж, діє правило FIFO, коли опрацювання наступних запитів не починається, поки не закінчиться опрацювання першого. Але під час кібер-нападу кількість запитів настільки зростає, що пристрою бракує ресурсів для того, щоб завершити роботу з вихідним запитом.

Види ddos атак мережевого флуду:

- HTTP-флуд. Вузли забиваються величезною кількістю HTTP-повідомлень. Хост-машина перевантажується службовими запитами.

- SYN-флуд. Вплив виконується на TCP, базовий протокол передачі даних.

- UDP-флуд. Порти забиваються пакетами за протоколом UDP через що перевантажується мережа.

- MAC-флуд. Порти мережевого обладнання завалюються потоком пакетів із різними MAC-адресами.

Прикладні

Атаки на рівні інфраструктури, застосовуються для того, щоб вивести з робочого процесу апаратні ресурси і технології, процесор доводиться до перевантаження. Види:

- Сервер наповнюється лог-файлами завдяки скрипту. Атака спрацює, якщо на сервері не встановлено ліміт.

- Надсилання габаритних пакетів, з якими не справляється процесор.

- Система квотування. Якщо хакер має доступ до CGI, то може написати скрипт для використання частини ресурсів.

- Атака 2-го роду. Помилкове сигналізування, що провокує закриття ресурсу.

Атаки на рівні додатків

Атака використовує упущення в розробці програмного коду, роблячи ПЗ вразливим. Сюди належить Ping of death. Але для атаки великих компаній, де досить складні системи, хакери пишуть експлойт-програму для виявлення вразливості ПЗ і подальшої атаки.

Схематично DDOS-атака виглядає приблизно так: на обраний в якості жертви сервер навалюється величезна кількість помилкових запитів з безлічі комп'ютерів з різних кінців світу. У результаті сервер витрачає всі свої ресурси на обслуговування цих запитів і стає практично недоступним для звичайних користувачів. Цинічність ситуації полягає в тому, що користувачі комп'ютерів, з яких направляються помилкові запити, можуть навіть не підозрювати про те, що їхня машина використовується хакерами. Програми, встановлені зловмисниками на цих комп'ютерах, прийнято називати "зомбі". Відомі безліч шляхів "зомбіювання" комп'ютерів - від проникнення в незахищені мережі до використання програм-троянів. Цей підготовчий етап є для зловмисника найбільш трудомістким.

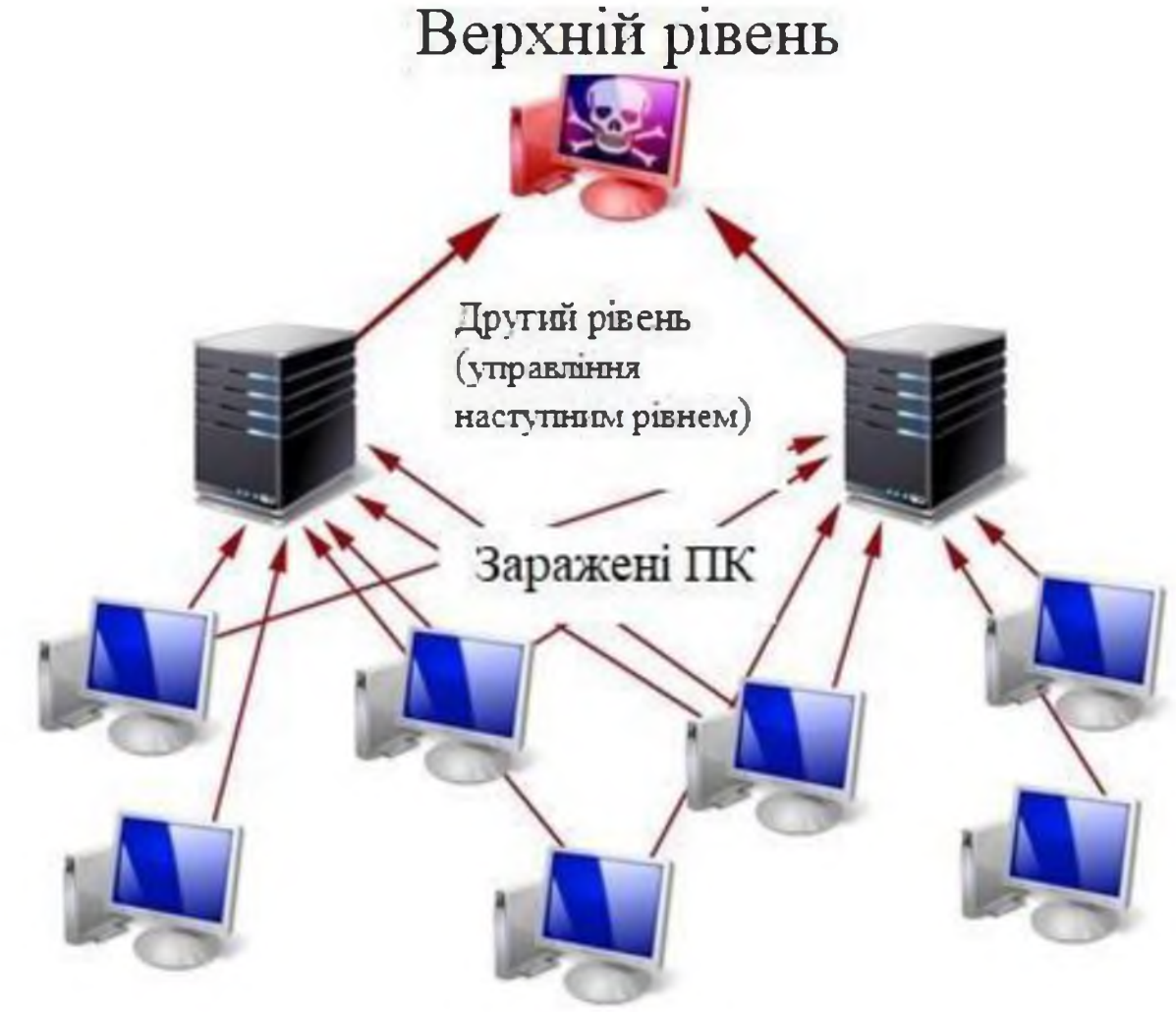


Рисунок 1.1 – Трьохрівнева архітектура для проведення DDOS-атак

Найчастіше зловмисники при проведенні DDOS-атак використовують трьохрівневу архітектуру (рис.1.1), що називають "кластер DDOS". Така ієрархічна структура містить:

- консоль керування (їх може бути декілька), тобто той комп'ютер, з якого зловмисник подає сигнал про початок атаки;

- головні комп'ютери. Це ті машини, які одержують сигнал про атаку з консолі керування й передають його агентам - "зомбі". На одну керуючу консоль залежно від масштабності атаки може доводитися до декількох сотень головних комп'ютерів;

- агенти - безпосередньо самі "зомбі" - комп'ютери, своїми запитами атакуючі вузол-мішень.

Простежити таку структуру у зворотньому напрямку практично неможливо. Як відомо, і комп'ютери-агенти, і головні комп'ютери є також потерпілими в даній ситуації й називаються "скомпрометованими". Така структура робить практично неможливим відстежити адресу вузла, що організував атаку.

Описана статистика зображена на діаграмі - рис. 1.2.

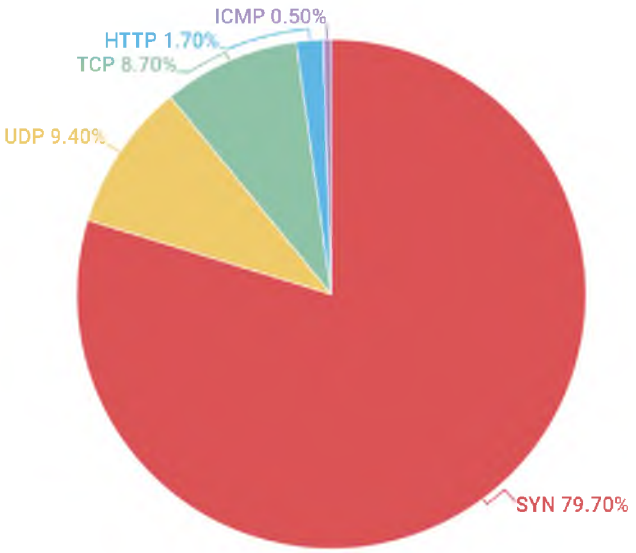


Рисунок 1.2 – Типи DDoS атак за популярністю

Зазвичай мережа зловмисника, з якої відбувається DDoS атака, має три рівні (рис 1.1). Назва такої мережі «кластер DDoS». Верхній рівень кластера складається с декількох комп’ютерів, з яких відбувається початок атаки та надалі іде координація дій інших учасників. Другий рівень – складається з десятків комп'ютери, які вже надають сигнали про атаку на наступний рівень кластера. На третьому рівні — зазвичай DDoS-зловмисники покладаються на ботнети — колекції мережі інфікованих зловмисними програмами, які централізовано контролюються. Ці заражені кінцеві точки, як правило, є комп'ютерами та

серверами, але все частіше є IoT та мобільними пристроями. Зловмисники збирають ці системи шляхом виявлення вразливих систем, якими вони можуть потенційно заразитися за допомогою фішинг-атак, зловмисних атак та інших методів масового зараження. Все частіше зловмисники також орендують цих ботнетів у тих, хто їх побудував.

Залучення до ботнету зазвичай відбувається через встановлення на комп'ютер жертви програму, яка не виявляється користувачем в щоденній роботі. Найчастіше зловмисники здійснюють ці дії через:

- зараження комп'ютера через вразливість (помилки в браузерах, поштовихклієнтів, програмах перегляду документів, зображень, відео);
- незнання або необачність користувачів, коли небезпечна програма маскуєтьсяпід безпечне;
- несанкціонованого доступу до комп'ютера користувача;
- повний перебір пароля (брутфорс) для отримання доступу прав адміністраторамережі, переважно використовується в локальних мережах.

Інша небезпека DDOS полягає в тому, що зловмисникам не потрібно мати якісь спеціальні знання й ресурси. Програми для проведення атак вільно поширюються в мережі. За роки це програмне забезпечення постійно модифікувалося й до теперішнього часу фахівці з інформаційної безпеки виділяють наступні види DDOS-атак:

1. UDP flood - відправлення на адресу системи-мішені безлічі пакетів UDP (User Datagram Protocol). Цей метод використовувався на ранніх атаках і в цей час вважається найменш небезпечним. Програми, що використовують цей тип атаки легко виявляються, тому що при обміні головного контролера й агентів використовуються нешифровані протоколи TCP і UDP.

2. TCP flood - відправлення на адресу мішені безлічі TCP-пакетів, що також приводить до "зв'язування" мережних ресурсів.

3. TCP SYN flood - відправлення великої кількості запитів на ініціалізацію TCP-з'єднань із вузлом-мішенню, якому в результаті доводиться витрачати всі

свої ресурси на те, щоб відслідковувати ці частково відкриті з'єднання. Схема даної атаки показано на рисунку 1.3

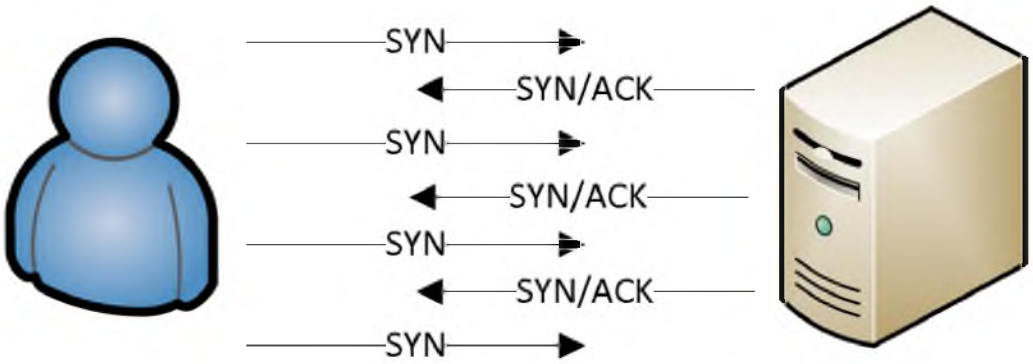


Рисунок 1.3 — SYN-флуд

4. Smurf-атака - ping-запити ICMP (Internet Control Message Protocol) за адресою спрямованого широкомовного розсилання з використанням у пакетах цього запиту фальшивої адреси джерела, яка в результаті виявляється мішенню атаки.

5. ICMP flood - атака, аналогічна Smurf, але без використання розсилання.

Природно, найнебезпечнішими є програми, що використовують одночасно кілька видів описаних атак. Вони одержали назву TFN і TFN2K і вимагають від хакера високого рівня підготовки.

6. Однією з останніх програм для організації DDOS-атак є Stacheldracht, що дозволяє організовувати всілякі типи атак і лавини широкомовних ping-запитів із шифруванням обміну даними між контролерами й агентами.

У багатьох країнах реалізація DDoS-атаки є злочином, але досить рідко виходить впіймати організаторів, а ще рідше виконавців. В наші дні організацією DDoS атак займаються не одна людина, а добре організовані зловмисна групи. Через їх організаційну та географічну віддаленість, їм вдається вдало протидіяти правоохоронним органам.

1.3 Організація роботи мобільного за стосунку

Стрімкий розвиток мобільних технологій охопив майже всі сфери діяльності людини: соціальну, економічну, політичну, культурну, наукову, освітню та інші. З розвитком технологій, появою мобільних телефонів та мобільного Інтернету робота, комунікація, відпочинок сучасної людини дедалі більше переносяться в онлайн-режим. Можливості сучасних смартфонів не поступаються функціональністю і продуктивністю стаціонарним ПК, а враховуючи сталу тенденцію до розширення мереж точок доступу Wi-Fi, збільшення покриття та фінансову доступність мобільного Інтернету – стає очевидним та обґрунтованим вибір користувачів на користь інтернет-«серфінгу» саме на мобільних пристроях, адже так зручніше і швидше.

Поява мобільних застосунків суттєво вплинула та розширила форми доступу до сервісних послуг, забезпечивши можливість читати книги, комунікувати з колегами, замовляти їжу, купувати речі, оплачувати комунальні послуги, шукати вигідні подорожі в зручний час та в будь-якому місці. Поширення цієї технології торкнулося всіх сфер життя, в тому числі суспільного, зокрема, забезпечення інформаційних та культурних потреб.

Так, наразі державні та місцеві органи влади задля підвищення сервісних та комунікаційних послуг у своїй роботі почали активно створювати мобільні застосунки. Станом на початок 2020 р. успішно функціонують мобільні застосунки Міністерства закордонних справ України, Міністерства внутрішніх справ України, Міністерства екології та природних ресурсів України, Міністерства охорони здоров'я, а також ряду місцевих органів влади та громадських організацій.

Наймаштабнішим державним проектом у рамках цифровізації нині є реалізація концепції «Держава в смартфоні», яка передбачає запуск сайту та застосунку з онлайн-послуг під загальною назвою «Дія». Сервіс об'єднує в єдиному електронному вікні всі послуги, які надає держава громадянам і бізнесу, максимально спрощує і прискорює будь-яку взаємодію громадянина з державою, зробивши максимум процесів електронними та автоматичними. Отже, можна

говорити про наявність в Україні значного прошарку користувачів, які мають як технічні можливості використовувати мобільні технології як комунікаційний зв'язок, так і відповідну інформаційну потребу.

Під мобільним застосунком розуміємо програмне забезпечення, призначене для роботи на смартфонах, планшетах та інших мобільних пристроях. Сьогодні мобільні пристрої реалізуються з уже встановленим набором мобільних застосунків, такими як веб-браузер, поштовий клієнт, календар, застосунок для придбання та прослуховування музики тощо. Є також можливість видалення попередньо встановлених застосунків, які не відповідають потребам власника/користувача. Застосунки, що відразу не встановлені на мобільний пристрій, доступні для завантаження та встановлення через платформи їх розповсюдження, такі платформи називають «магазинами застосунків». Вони почали з'являтися у 2008 р., та зазвичай керуються компанією власником мобільних операційних систем: Apple App Store, Google Play, Windows Phone Store і BlackBerry App World. Проте існують й інші «магазини застосунків», такі як: Cydia, GetJar або F-Droid. Значна кількість мобільних додатків є безкоштовною для встановлення та користування, але є й платні.

Стабільний попит на мобільні пристрої, постійно зростаючий рівень інтернетизації, експонентне збільшення кількості мобільних застосунків та кількості їх завантажень дає підставу зробити висновок про актуальність і перспективність процесу розробки та впровадження такого виду мобільного сервісу в різні сфери життєдіяльності суспільства. Так, за результатами бази даних статистики Statista, яка надає відомості зібрані світовими інститутами дослідження ринку мобільних технологій, оцінки експертів та дані, отримані з економічного сектора і офіційної статистики, станом на 2019 р. користувачі програмного забезпечення Android могли обирати між 2,47 млн застосунків, що зробило Google Play «магазином застосунків» із найбільшою кількістю доступних. Apple App Store став другим за величиною «магазином застосунків» з 1,8 млн доступних пропозицій. Для порівняння: на момент відкриття магазину Apple App Store (2008 р.), користувачам пропонувалося для завантаження всього

500 мобільних застосунків, проте вже за три місяці їх кількість зросла до 3000, а завантаження досягли відмітки в 100 млн. У свою чергу, «магазин застосунків» Google Play в 2009 р. пропонував користувачам всього 2300 мобільних застосунків, проте вже за рік їх кількість зросла до 80 тис., а загальна кількість завантажень досягла 1 млрд. Стабільний ріст завантажень із магазинів застосунків підтверджується і статистичними даними, які представлені в звіті бази даних статистики Statista. У ньому, зокрема, зазначено, що в 2018 р. користувачі мобільних пристроїв завантажили 194 млрд мобільних застосунків на свої підключені пристрої, в порівнянні з 143,7 млрд завантажень застосунків у 2016 р.

Перші мобільні додатки були «вбудованими» (тобто такими, які не можна видалити) в програмне забезпечення телефона та використовувалися для швидкої перевірки електронної пошти, доступу до календаря, контактів, отримання інформації про погоду, але їх активне використання сприяло розширенню призначень і в інших сферах, таких як ігри для мобільних телефонів, GPS, спілкування, перегляд відео та активне користування Інтернетом. Сьогодні функціональність мобільних застосунків є надзвичайно різноманітною: від ігор та сервісів виклику таксі – до офісних програм та фітнес-трекерів.

Фахівці із комп'ютерних технологій розділяють застосунки за способом створення на три категорії: нативні, гібридні та веб-застосунки. Кожна з цих категорій має свої переваги та особливості.

Нативні застосунки – розроблені для конкретної платформи (наприклад, iOS або Android), з урахуванням специфіки цієї платформи та доступом до всіх її ресурсів. До переваг нативних застосунків експерти відносять просте опанування та використання, високу швидкість роботи та стабільність, широку функціональність та легку інтеграцію між собою.

Під гібридним мобільним застосунком фахівці розуміють програмне забезпечення для мобільних пристроїв, що базується на основі WebView мобільної платформи (по суті – ізольований екземпляр браузера). Тобто це – мобільний сайт, розміщений в оболонці нативного застосунку, що надає доступ до нативних функцій смартфону, таких як GPS, камера, здійснення дзвінків тощо.

До переваг гібридних додатків відносять універсальність нижчу вартість розробки, швидший вихід на ринок.

Щодо мобільних веб-застосунків, то фахівці зазначають, що фактично вони не є додатками, адже насправді є сайтом, який адаптований і оптимізований під будь-який смартфон. Для того, щоб скористатися ним, достатньо мати на пристрої браузер та інтернет-з'єднання (завдяки йому відбувається оновлення інформації в цьому виді застосунка), знати потрібну інтернет-адресу. Використовуючи мобільні веб-застосунки, користувач виконує всі ті дії, як і при переході на будь-який веб-сайт, а також отримує можливість «встановити» їх на свій робочий стіл, створивши закладку сторінки веб-сайту.

До переваг веб-застосунків відносять: мультиплатформність простий і швидкий процес розробки, кількість компетентних розробників, відсутність необхідності завантаження з магазину застосунків.

За функціональним призначенням мобільні застосунки класифікують так: рекреаційні – ігри, програвачі аудіо- та відеофайлів, рідери зображень і електронних книг; комунікаційні – відповідають за спілкування користувача по телефону і SMS/MMS, його контакти в електронній пошті, ICQ, соціальних мережах; навігаційні – працюють з системою GPS, електронними картами і географічними координатами; довідкові – словники і енциклопедії, бази даних з можливістю пошуку; прикладні – записні книжки, органайзери, калькулятор, програми для роботи з графікою і текстом тощо.

До факторів, які впливають на позитивну динаміку розвитку зростання ринку мобільних застосунків і викликають інтерес багатьох сучасних компаній/установ експерти відносять:

– зростання числа мобільних пристроїв, у тому числі планшетних комп'ютерів;

– більш доступне спілкування за допомогою мобільних пристроїв;

– розвиток мобільного банкінгу;

– зростання популярності GPS-навігації.

Фахівці агентства інтернет-маркетингу Webbranding розділяють найбільш ефективні за своєю результативністю мобільні застосунки на чотири типи: внутрішньокорпоративні (із закритим типом програми для сторонніх користувачів, розроблені з метою оптимізації бізнес процесів); для брендування і PR (із відкритим типом програми для сторонніх користувачів, розроблені з метою збільшення впізнаваності, підвищення лояльності, інформування про новинки та акції, стимулювання зворотного зв'язку); для новиних та медіа ресурсів (із відкритим типом програми для сторонніх користувачів, розроблені для збільшення лояльності цільової аудиторії, застосунки самі інформують і посилають пуш повідомлення при появі нових матеріалів по темі, стимулюють повторні відвідування); для комерційних ресурсів (із відкритим типом програми для сторонніх користувачів, розроблені з метою збільшення прямих продажів, застосунки самі інформують і посилають пуш повідомлення при появі нових акцій, знижок і т.д., провокуючи повторні продажі).

Для будь-якої інформаційної системи необхіддно мати щонайменше три основні функціональні блоки, це модулі зберігання даних, модулі їх обробки та відповідного інтерфейсу для діалогу з користувачем. Можна реалізувати будь яку з цих частин незважаючи на дві інші частини. Можна навести приклад, що при сталому коду програм, що використовуються для обробки та збереження даних, маємо можливість зміни інтерфейсу з клієнтом таким чином, що одна й та сама інформація, буде відображатися у вигляді інших представленням даних, наприклад у вигляді графіків, у вигляді таблиць або в гістограммах. Не змінюючи програм представлення даних та їх збереження, можна змінювати програми для обробки даних, наприклад змінивши алгоритм роботи програми, наприклад для пошуку тексту. І нарешті, не змінюючи програм представлення і обробки даних, можна змінити програмне забезпечення для зберігання даних, перейшовши, наприклад, на іншу файлову систему.

У класичній архітектурі клієнт-сервер доводиться розподіляти три основні частини програми по двом фізичним модулів. Зазвичай за зберігання даних розташовується на інформаційному сервері, наприклад деякий сервер БД,

інтерфейс з користувачем - на стороні клієнта, а обробку даних розподіляється між клієнтськими і серверними частинами (рисунок 1.4)

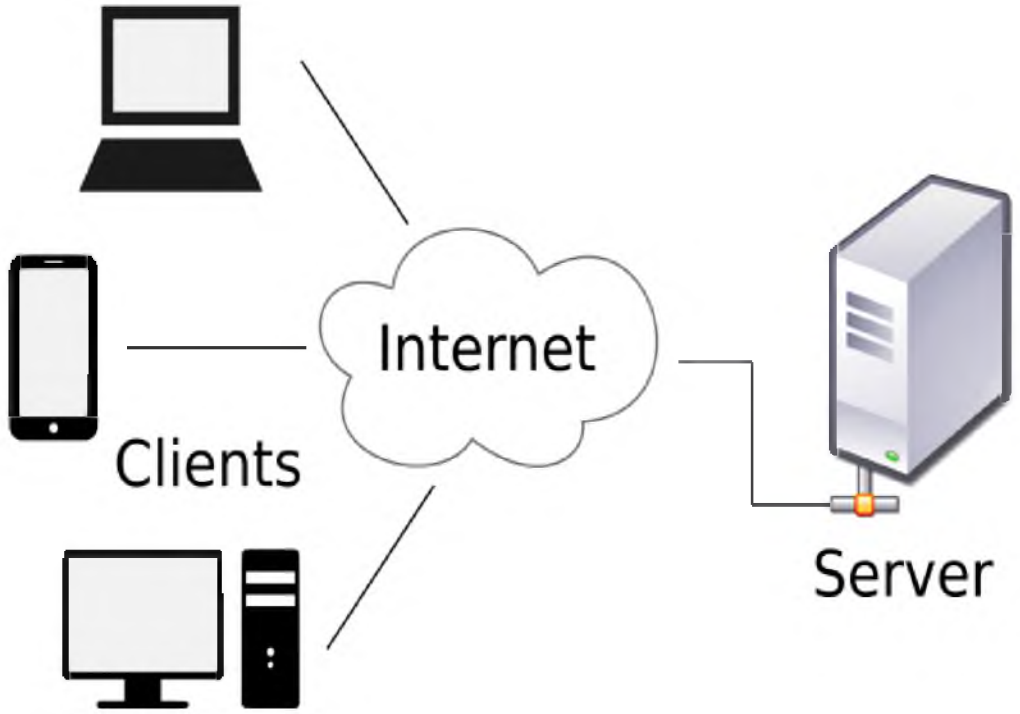


Рисунок. 1.4 Взаємодія клієнт-сервер

Архітектура клієнт-сервер є одним із архітектурних шаблонів програмного забезпечення та є домінуючою концепцією у створенні розподілених мережних застосунків і передбачає взаємодію та обмін даними між ними. Вона передбачає такі основні компоненти:

- набір серверів, які надають інформацію або інші послуги програмам, які звертаються до них;
- набір клієнтів, які використовують сервіси, що надаються серверами;
- мережа, яка забезпечує взаємодію між клієнтами та серверами.

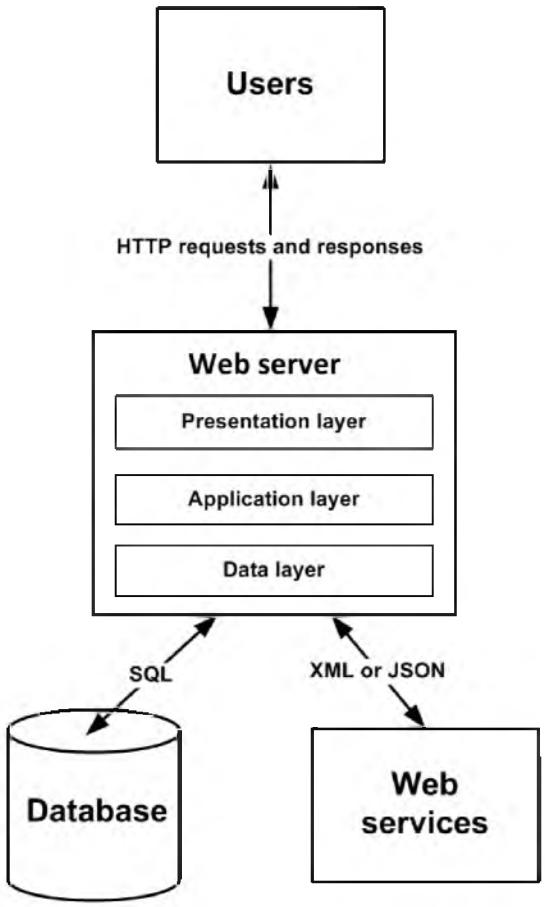


Рис. 1.5 - Компоненти клієнт-серверної архітектури

Архітектура клієнт-сервер визначає загальні принципи роботи та взаємодії вузлів в мережі, де існують сервери, вузли які використовуються для доставки деяких специфічних функцій і клієнти, які споживають ці функції.

Рівень користувальницького інтерфейсу зазвичай реалізується на клієнтських пристроях. На цьому рівні знаходяться програми, з використанням яких, власне користувач може мати змогу комунікувати з додатком. Досить різною може бути складність додатків, які входять до користувальського інтерфейсу.

Найлегший варіант програми, яка входить до користульського інтерфейсу, коли вона не містить нічого окрім дисплея на якому виводиться результат. Такі інтерфейси зазвичай використовуються при роботі з великими серверами. У тому випадку, коли цей сервер може контролювати кожну взаємодію, включаючи роботу клієнта з клавіатурою, а також монітором, але в цьому випадку ми навряд чи зможемо говорити про модель взаємодії клієнт-сервер. Але все ж, у багатьох випадках, термінали клієнтів, можуть виробляти деяку обробку даних, локально,

здійснюючи, наприклад, віддалений друк рядків які друкуються, або надаючи інтерфейси деяких форм, в яких можна зробити маніпуляції, ще до до їх відправлення на сервер.

У багаторівневих інформаційних системах цей рівень взаємодіє з нижнім рівнем інфраструктурних сервісів, наприклад, інтерфейсом до бази даних або файлової системи і вищерозміщеним рівнем сервісів додатки який вже, в свою чергу, взаємодіє з рівнем призначеного длякористувача інтерфейсу (User Interface Layer) або зовнішніми системами.

У фазі бізнес-моделювання та розробки вимог бізнес-логіка може описуватися у вигляді тексту, концептуальних аналітичних моделей предметної області, бізнес-правил, різноманітних алгоритмів, діаграм діяльності, графів і діаграм переходу станів, моделей бізнес-процесів. У фазі аналізу і проектування системи бізнес-логіка втілюється в класах і методах класів, в разі використання об'єктно-орієнтованих мов програмування, або процедур і функцій, в разі застосування процедурних мов.

Рівень інформації даних у моделі клієнт-серверу включає в себе програми, за допомогою який можна обробляти дані в додатках . Своєрідною вимогою для цього рівня є збереження даних. Але, якщо програма не буде працювати, інформація буде збережена у визначеному для неї місці з розрахунком на подальше її користування.

У простішій варіації, рівень даних стане файловою системою, але нерідко для їх реалізації використовується повномасштабна база даних. У макеті клієнт-сервер рівень інформації в основному знаходиться на стороні сервера.Крім простого зберігання інформації рівень даних звичайно відповідає за підтримка цілісності даних для різних додатків. Для бази даних підтримання специфічні метадані додатків, також зберігаються на цьому рівні.

Функції які виконуються в середовищі клієнт-сервер.

Таблиця 1.1- Функціональність між клієнтом та сервером

Клієнт	Сервер
Керує користувальським інтерфейсом	Приймає і оброблює запити до бази даних зі сторони клієнтів
Приймає і перевіряє запити введені користувачем	Перевіряє повноваження користувачів
Генерує запит до бази даних і відправляє його серверу	Виконує запити і відправляє результат клієнту
Відображає отримані дані користувачу	Підтримка системного каталогу Керування відновленням даних
Виконує застосунок	Гарантує цілісніть

Зростання кількості різноманітних застосунків та розширення їх асортименту прямо пов'язане із розв'язанням завдань, що виникають при конкуренції та необхідності підвищення «видимості», функціональності в різних сферах діяльності. З цією метою кожна компанія/установа, як правило, намагається розробити свою власну унікальну пропозицію й у такий спосіб додатково окреслити свої переваги.

До етапів реалізації процесу розробки мобільних застосунків відносять:

– аналіз потреб замовника;

– вибір мобільних платформ (однієї або декількох);

– складання докладного технічного завдання, необхідного в процесі розробки;

– розробка і створення мобільного застосунку;

– альфа і бета-тестування на смартфонах, планшетах тощо;

– упровадження мобільного застосунку та публікація його в магазинах мобільних додатків.

Фахівці зарубіжних бібліотек вже давно активно досліджують ринок мобільних застосунків, а також маркетингові дані задля більш глибокого

розуміння настроїв та потреб користувачів у процесі створення та вдосконалення власних застосунків.

Отже, рівень розвитку технологій у галузі використання мобільних пристроїв і бездротового зв'язку дає змогу ефективно організувати бізнесу соціальні, наукові процеси і досягти позитивних результатів. Маючи у своєму арсеналі велику кількість різноманітних засобів – від персональних ПК до ноутбуків, планшетів, смартфонів та доступом до мережі – інформаційні ресурси та сервіси стали ще доступнішим для будь-якої людини. Крім розширення охоплення цільової аудиторії розробка мобільних застосунків дає можливість бізнесу/установі адаптуватися для роботи з найчастіше використовуваними соціальними мережами, послуговуючись їхніми вбудованими можливостями, доповненими власними маркетинговими напрацюваннями.

1.3.1 Аналіз системи аутентифікації у мобільних застосунках

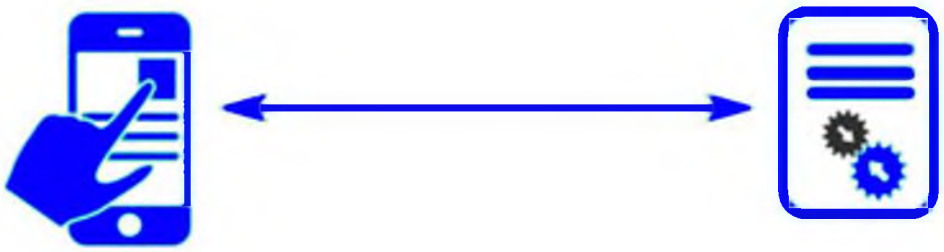
Історично склалося так, що автентифікація в мобільних застосунках не надто відрізняється від автентифікації у веб застосунках. Однак для мобільних додатків є ключові особливості:

Інтерфейс користувача в мобільному застосунку ґрунтується не на стороні сервера, тому будь-які зміни в інтерфейсі (зокрема й нові методи автентифікації) потребують розроблення нової версії застосунку. Це вимагає часу і відволікає від реальної роботи над додатком.

Для веб-застосунків уже багато років успішно застосовують SAML для того, щоб перекласти завдання аутентифікації на інший сервер. Так веб-застосунок може фокусуватися на основному завданні. Інтеграція подібного підходу (редиректи, POST запити) для мобільних застосунків вимагає значного часу і трудомісткої роботи.

Ще одна відмінність у тому, що під час роботи з мобільним застосунком користувач не готовий автентифікуватися щоразу під час запуску застосунку. Оскільки він працює зі свого пристрою, він очікує, що аутентифікувавшись один раз, він залишається залогіненим. Можливо, що і не з повним доступом.

Пропозиція аутентифікації може з'явитися для деяких операцій, наприклад, переказ грошей.



Мобільний додаток

- Логіка програми
- Інтерфейс аутентифікації
- Інтерфейси майбутньої аутентифікації
- Керування сесіями

API

- Логіка програми
- Захист комунікацій
- Аутентифікація
- Майбутні методи аутентифікації
- Керування обліковими даними

Рисунок 1.6 Класичний мобільний додаток

Ключові особливості розробки мобільного застосунку такі:

- Можливість використовувати тих самих користувачів і паролів, як і для веб-застосунків, щоб користувачі не вчили нові паролі або нові методи автентифікації, тобто автентифікація в мобільних застосунках має бути вбудована в поточну автентифікацію.
- Довготривалі сесії з обмеженим доступом. Це можливо з OAuth2
- Перенесення аутентифікації від застосунку, що дає змогу уникнути змін у застосунках під час додавання нових методів аутентифікації
- Паролі додатків не зберігаються локально і не передаються в заголовку HTTP basic
- Можливість закрити доступ до певних застосунків, не впливаючи на інші застосунки та не змушуючи користувачів змінювати паролі

- Додавання багатофакторної автентифікації не повинно призводити до переробки всіх автентифікаційних процесів застосунку
- Необхідність надати мобільному застосунку делегований доступ, але не повний доступ до облікового запису користувача, тобто дозволити обмежений доступ
- Небажано поширювати облікові дані та зберігати їх на мобільних пристроях

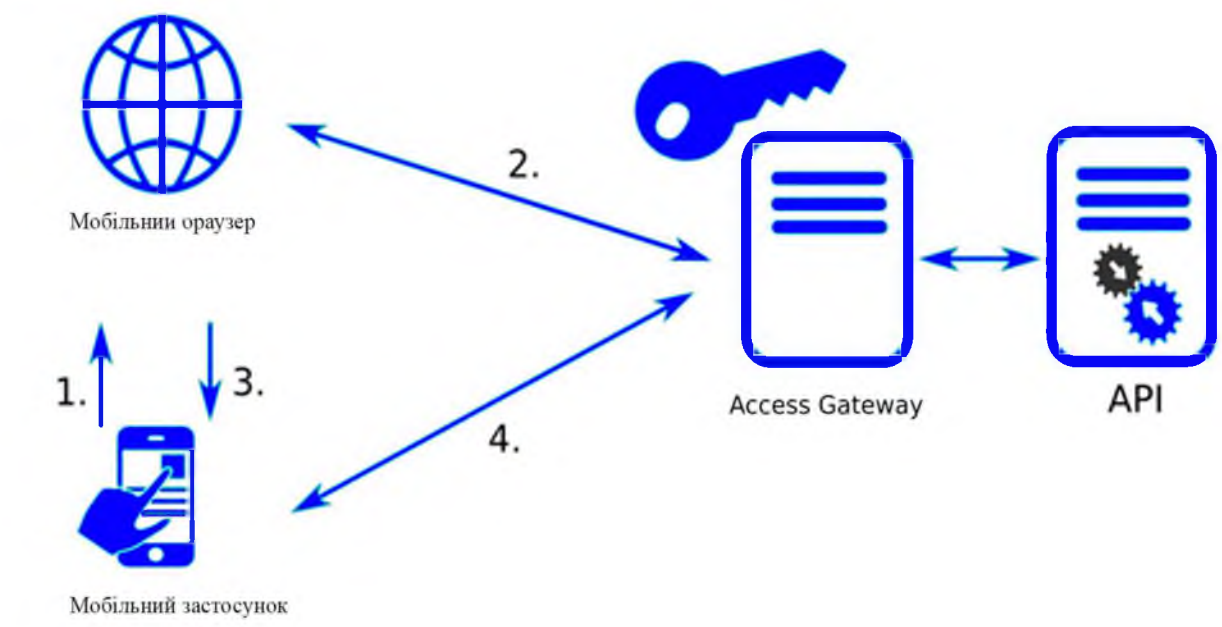


Рисунок 1.7 Схема автентифікації

1. Користувач прямує на Access Gateway (шлюз доступу), який керуватиме аутентифікацією та контролем доступу.

2. Користувач аутентифікується і запитує права на доступ до API.

3. Користувачеві повертається токен.

4. Застосунок використовує токен для доступу до API

На процесах автентифікації та авторизації заснований поділ прав доступу, без якого не обходиться жоден більш-менш серйозний застосунок. Ідентифікація - процес визначення, що за людина перед нами. Аутентифікація - процес

підтвердження, що ця людина саме та, за кого себе видає. Авторизація - процес ухвалення рішення про те, що саме цій аутентифікованій персоні дозволяється робити. Тобто, це три різних, послідовних і взаємно замінних поняття. Ідентифікацію часто мають на увазі в складі аутентифікації. Під час аутентифікації ми переконуємося, що людина, яка до нас прийшла, має докази, які підтверджують особу.

Існують певні способи аутентифікації:

При використанні HTTP-протоколу найпростіший спосіб аутентифікації - Basic access authentication. В принципі цей протокол застарів і вже рідко використовується в інтернеті, особливо в незахищених з'єднаннях, але ще зберігається у внутрішньокорпоративних системах, просто тому що деякі з них створені досить давно.

HTTP Basic Authentication

Першим, що при зверненні до захищеного ресурсу сервер видасть користувачеві, який не має доступу, буде помилка 401 Unauthorized. При цьому відповідь також містить інформацію про тип аутентифікації (в нашому випадку - Basic), який він може приймати, і контекст, в рамках якого ця аутентифікація діє (Realm). Користувач вводить логін і пароль, вони упаковуються в Base64 і відправляються на сервер для перевірки. Тут існують різні небезпеки. Найпоширеніша - загроза man-in-the-middle attack, або атаки посередника, в ході якої при використанні незахищеного з'єднання облікові дані можуть перехопити зловмисники в момент передачі від клієнта до сервера або назад.

HTTP Digest Authentication

Наступним етапом розвитку технології стала трохи більш складна система HTTP digest authentication, яка виключає передачу облікових даних у відкритому вигляді - тут для перевірки використовується MD5-хеш з деякими домішками, що дозволяє уникнути підбору логіна і пароля. Звичайно, цей алгоритм виглядає більш надійним, але і він схильний до цілого ряду не найскладніших атак.

Forms Authentication

Пізніше з'явився процес Forms authentication, при якому аутентифікація відбувається на більш високому рівні моделі абстракції. HTTP-сервер при цьому не повідомляє про помилку доступу, а просто перенаправляє нерозпізнаних користувачів на іншу сторінку. Зазвичай на цій сторінці відображаються поля для введення логіна і пароля, після заповнення яких формується *POST-запит* з даними і через захищений канал направляється на сервер. Серверна сторона в свою чергу повертає користувачеві токен або ідентифікатор сесії, який зберігається в Cookies і надалі використовується для доступу до захищеного ресурсу.

Token Authentication

Наступне покоління способів аутентифікації представляє Token Based Authentication, який зазвичай застосовується при побудові систем Single sign-on (SSO). При його використанні запитуваний сервіс делегує функцію перевірки достовірності відомостей про користувача іншому сервісу. Т. е. Провайдер послуг довіряє видачу необхідних для доступу токенов власне токен-провайдеру (Identity provider). Це те, що ми бачимо, наприклад, входячи в додатки через акаунти в соціальних мережах. Поза IT найпростішої аналогією цього процесу можна назвати використання загальногромадянського паспорта. Офіційний документ якраз є виданими вам токеном - всі державні служби за замовчуванням довіряє відділу поліції, який його вручив, і вважає паспорт достатнім для вашої аутентифікації протягом усього терміну дії при збереженні його цілісності.

В мобільному застосунку розглянуто спосіб Token Authentication. Детально схема отримання дозволу зображено на схема 1.1 та 1.2 нижче.

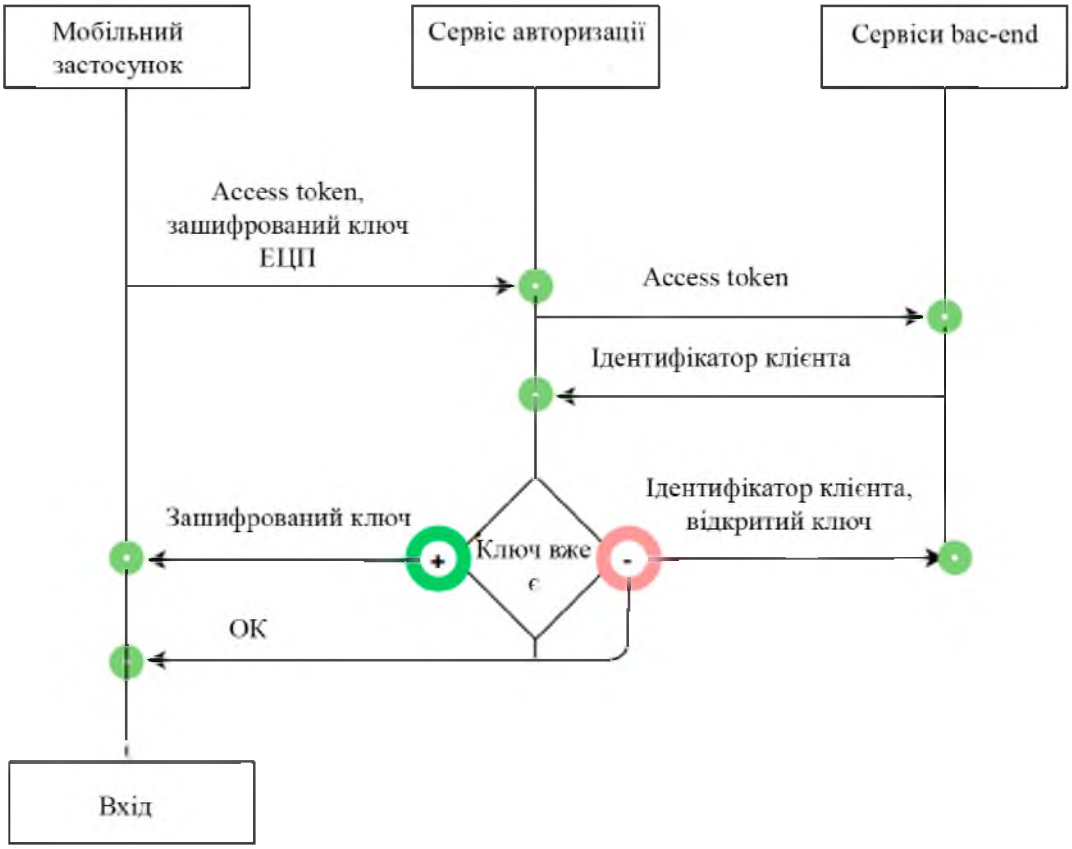


Схема. 1.1 Схема генерації ключа

Схема першого етапу для авторизації в мобільному за стосунку на рисунку 1.1

Перед взаємодією клієнт:

1) встановлює PIN під час реєстрації

2) генерує 2 ключові пари, одна основна, інша backup (необхідна лише для відновлення ключа в разіутери PINa)

3) створює дві заяви на видачу сертифіката, для основного ключа самопідписану, для backup ключа самопідписану і додатково підписану основним ключом (для юридичного зв'язку основного з backup)

4) основний ключ зашифровується на PIN-коді та зберігається в додатку

5) зашифровану основну ключову пару і backup разом із заявками передають на сервер.

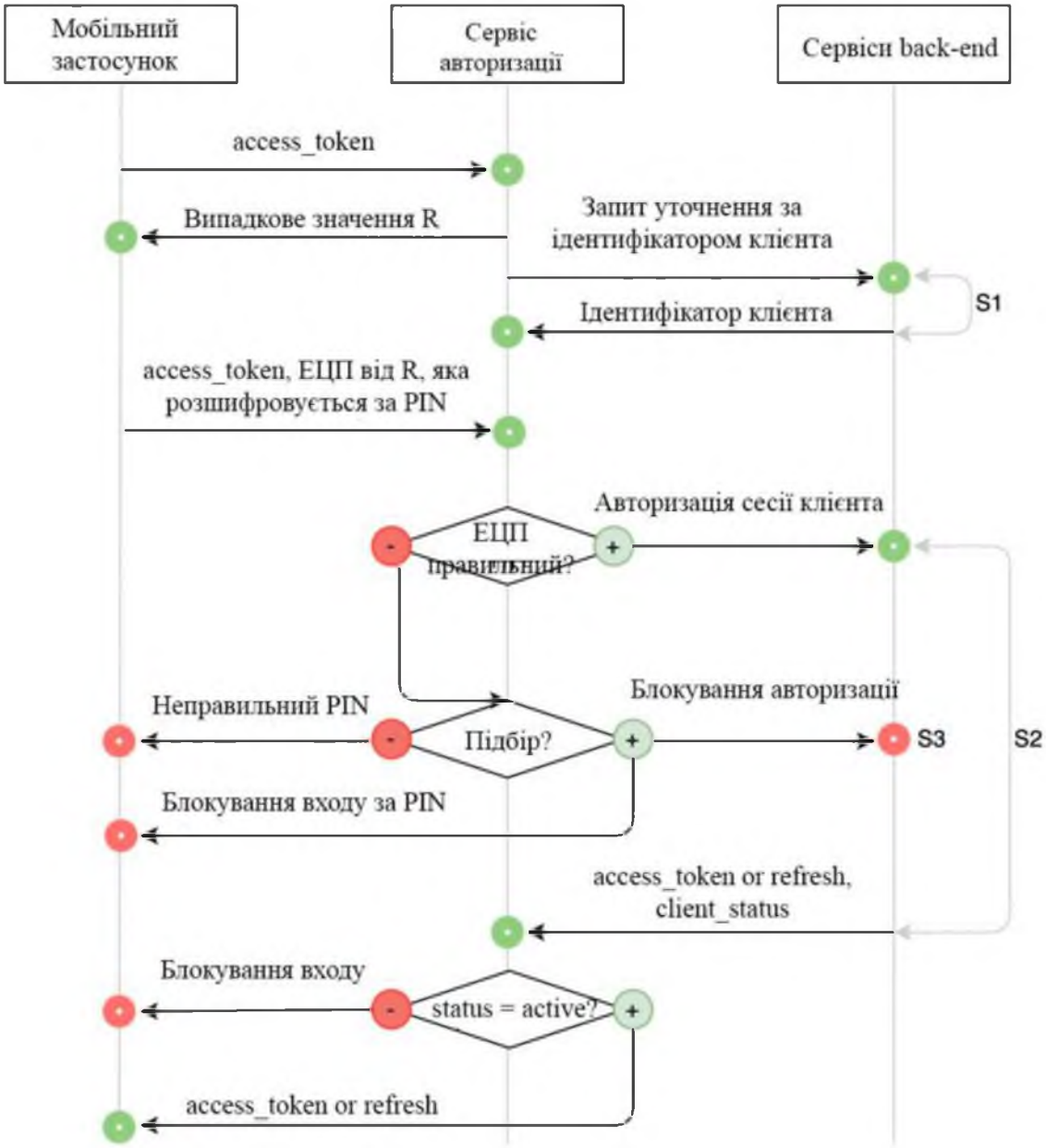


Схема. 1.2 Схема автентифікації

Одразу після генерації ключа за стосунок переходить на етап отримання токену для авторизації, схематично послідовність зображена на схемі 1.2 , на якій клієнт успішно авторизовується у мобільному за стосунку зі сформованим для нього токеном.

Автентифікація на основі токенів спрощує процес аутентифікації для вже відомих користувачів. Для початку роботи користувач надсилає запит до сервера,

вказавши ім'я користувача та пароль. Потім сервер підтверджує їх на підставі значень, зареєстрованих у його базі даних ідентифікаційної інформації. Якщо ідентифікаційні дані підтверджено, сервер повертає токен аутентифікації (який теж зберігається в базі даних).

Коли той самий користувач надалі надсилає запити на доступ до захищених ресурсів, ці запити можна авторизувати за допомогою токена аутентифікації замість імені користувача і пароля. Сервер звіряє токен із зареєстрованим у базі даних токеном і надає доступ. Аутентифікацію можна реалізувати на основі різних типів токенів, наприклад, OAuth і JSON Web Tokens (JWT).

Усі токени безпечним чином зберігають ідентифікаційну інформацію та дані користувача. Токен також може підтвердити, що дані вірні та їх не модифікували - важлива вимога безпеки з урахуванням безлічі сучасних законів про конфіденційність. Також вони значно підвищують зручність роботи для користувача, оскільки дозволяють користувачам виконувати вхід без необхідності запам'ятовування паролів.

Аутентифікація на основі токенів зазвичай складається з чотирьох етапів:

1. Початковий запит - користувач запитує доступ до захищеного ресурсу. Спочатку користувач повинен ідентифікувати себе способом, що не вимагає токена, наприклад, за допомогою імені користувача або пароля.

2. Верифікація - автентифікація визначає, що ідентифікаційні дані користувача вірні, і перевіряє, які повноваження він має в запитаній системі.

3. Токени - система випускає токен і передає його користувачеві. У разі апаратного токена це передбачає фізичну передачу токенів користувачеві. У разі програмних токенів це відбувається у фоновому режимі, поки фонові процеси користувача обмінюються даними із сервером.

4. Збереження - токен утримується користувачем, або фізично, або в браузері/мобільному телефоні. Це дозволяє йому виконувати аутентифікацію без зазначення ідентифікаційних даних.

Кіберзлочини стають дедалі витонченішими, тому постачальники сервісів із віддаленим управлінням повинні безперервно оновлювати методики та політики

безпеки. Останнім часом зросла кількість атак, націлених на ідентифікаційні дані за допомогою таких способів, як фішинг, брутфорс і атаки за словником. Це означає, що аутентифікація більше не може використовувати тільки паролі.

Аутентифікація на основі токенів у поєднанні з додатковими техніками аутентифікації може створити складніший бар'єр, щоб перешкодити розумним хакерам використовувати вкрадені паролі. Токени можна отримувати лише з унікального пристрою, який їх створив (наприклад, смартфона або брелока), завдяки чому вони стають сьогодні високоефективною методикою авторизації.

Хоча платформи токенів аутентифікації зробили великий прогрес, загроза частково зберігається. Токени, що зберігаються в мобільних пристроях, легко використовувати, але вони можуть виявитися доступними через уразливості пристрою. Якщо токени надсилаються текстовим повідомленням, їх можна легко перехопити під час передачі. Також існує загроза багаторазових запитів на формування токенів під час DDOS-атак, яка негативно впливає на працездатність застосунку або навіть виводить його з ладу, таким чином не даючи легітимним користувачам авторизуватись в ньому.

1.4 Захисту серверів від DDOS-атак

Для порівняння систем захисту від DDoS-атак ознайомились з класифікаціями DDoS-атак. Найчастіше застосовуваний спосіб класифікації атак - за рівнем OSI, на якому вони здійснювалися. Перелічимо найпоширеніші види атак:

Мережевий рівень (L3): DDoS-атаки цього рівня "працюють" за протоколами IP, DVMRP, ICMP, IGMP, PIM-SM, IPsec, IPX, RIP, DDP, OSPF, OSPF. Цілями атак є насамперед мережеві пристрої - комутатори (свічі) і маршрутизатори (роутери).

Транспортний рівень (L4): вплив здійснюється за протоколами TCP і UDP, а також за підпротоколами DCCP, RUDP, SCTP, UDP Lite. Цілями атак цього рівня зазвичай стають сервери і деякі інтернет-сервіси, наприклад ігрові.

Рівень додатків (L7): атака здійснюється на рівні протоколів додатків. Найчастіше зловмисники використовують HTTP, HTTPS і DNS. Атаки цього рівня націлені як на популярні мережеві сервіси, так і на різноманітні вебсайти та веб-застосунки.

Ще один поширений спосіб класифікації - за способом впливу: використання вразливостей протоколів: вони дають змогу домагатися відмови в обслуговуванні шляхом впливу на атакований ресурс некоректними запитами, унаслідок чого жертва "йде в ступор", намагаючись їх обробити; переповнення трафіку потужним потоком запитів, який жертва не в змозі "перетравити"; вплив на слабкі місця в архітектурі та логіці роботи додатків, здатний сильно порушити працездатність підключеного до Інтернету програмного комплексу, особливо якщо він має слабкий рівень захищеності.

Способи захисту від DDoS-атак

Перш ніж братися за використання сервісів захисту від DDoS-атак, слід подбати про підвищення ступеня захищеності інтернет-сервісу - його здатності ефективно відбивати атаки з мінімальними витратами ресурсів. В іншому разі, щоб убезпечити інтернет-сервіс від впливів, доведеться витратити дуже багато сил і засобів. Якщо гранично коротко, то для підвищення захищеності потрібно:

- надати якомога менше інформації атакуючому;
- надати якомога більше інформації DDoS-захиснику;
- забезпечити зрозумілі можливості фільтрації атаки;
- забезпечити надійність сервісу під атакою.

Можливості захисту від DDoS-атак можна і потрібно передбачати в інтернет-ресурсі ще на стадії проектування його архітектури: гарне проектування дасть змогу підвищити доступність ресурсу і знизити витрати на його захист від атак.

Що стосується засобів захисту, то їх можна розділити на локальні (on-premise), хмарні та гібридні. Рішення on-premise і засоби anti-DDoS бувають як програмні, так і апаратні (спеціалізовані мережеві пристрої), і їх можуть

встановлювати як самі клієнти, так і їхні провайдери. Основні користувачі локальних рішень anti-DDoS - великі оператори зв'язку (хмарні та інтернет-провайдери) і дата-центри, які можуть собі дозволити мати власну службу реагування, здатні впоратися з потужними (у сотні гігабіт) атаками і пропонують послугу anti-DDoS своїм клієнтам.

Хмарні рішення реалізують практично той самий функціонал захисту, що й рішення on-premise. Крім пакетного захисту, провайдери хмарних сервісів anti-DDoS нерідко пропонують послуги захисту сайтів від атак, які здійснюють боти (зловмисники використовують у них протокол HTTP), а також технічну підтримку і супровід під час DDoS-атаки. Хмарні рішення видаються оптимальним варіантом для більшості компаній.

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

захист від пакетного флуду на основі фільтрації пакетів транспортного і мережевого рівня (L3 і L4) - цього достатньо для захисту мережевих пристроїв;

захист і від пакетного флуду, і від флуду на рівні додатків (L3 - L7) - це необхідно, зокрема, для забезпечення працездатності сайтів, оскільки більшість атак на них здійснюється саме на рівні L7;

захист не тільки від флуду на рівні L3 - L7, а й від "інтелектуальних" DDoS-атак із використанням "розумних" ботів, що атакують ті частини веб-застосунків, які мають найбільшу ресурсоємність під час опрацювання запитів, що надходять, із застосуванням функцій Web Application Firewall (WAF) - це необхідно для захисту критично важливих інтернет-ресурсів.

За форматом підключення розрізняють симетричний і асиметричний DDoS-захист. Перший варіант передбачає встановлення фільтра в симетричному режимі: через фільтр завжди проходить і вхідний, і вихідний трафік сервера, що захищається (або службова інформація про цей трафік). Асиметричні алгоритми аналізують тільки вхідний трафік. Як правило, симетричні засоби захисту ефективніші, але вартість володіння ними вища, до того ж затримка сигналу більша. Асиметричні засоби часто складніші, але, оскільки вони не аналізують

вихідний трафік, повна фільтрація деяких атак в асиметричному режимі не забезпечується.

1.4.1 Порівняння систем захисту

Було обрано декілька система захисту проти DDOS-атак від таких компаній, як Arbor Networks, Huawei та Radware.

Перша система розглянута це *DefensePro: DDoS Protection and Attack Mitigation.*

1)DefensePro є частиною рішення для захисту від атак Radware і являє собою відзначений нагородами пристрій для захисту периметра від атак в режимі реального часу, який захищає організації від нових мережевих загроз і загроз для додатків. DefensePro захищає інфраструктуру від простою мережі та додатків, використання вразливостей додатків, поширення шкідливого програмного забезпечення, мережевих аномалій, крадіжки інформації та інших типів атак.

DefensePro допомагає організаціям виграти безперервну битву за безпеку проти атак на доступність, виявляючи і пом'якшуючи відомі і "нульові" DoS/DDoS-атаки в режимі реального часу. Він захищає від інших загроз безпеки, які зазвичай не виявляються традиційними інструментами захисту від DDoS-атак, таких як флуд-атаки на основі SSL, атаки на сторінки входу в систему і атаки через CDN.

Рішення DefensePro від Radware забезпечує захист з найкоротшим часом усунення наслідків атак і найширшим покриттям атак. Radware пропонує гібридне рішення, що поєднує локальні та хмарні засоби захисту в єдиному інтегрованому рішенні, призначеному для оптимального блокування декількох векторів атак, що відбуваються паралельно.

Рис 1.7 – DefensePro системи захисту

Цінність для бізнесу:

Підтримуйте безперервність бізнес-процесів (COOP), навіть коли мережа піддається атаці

- Повний захист додатків центру обробки даних від нових мережевих загроз

- Підтримуйте продуктивність мережі навіть в умовах мережевих атак з високим рівнем PPS

- Підтримуйте відмінний час відгуку користувачів навіть в умовах атаки

Краще рішення для захисту центрів обробки даних в одному корпусі

- DefensePro поєднує в собі систему запобігання вторгнень (IPS), аналіз мережевої поведінки (NBA), захист від атак типу "відмова в обслуговуванні" (DoS) і DefenseSSL

- Отримайте найбільш точне виявлення і запобігання атакам без блокування легітимного трафіку користувачів

Зниження сукупної вартості володіння (TCO) системою безпеки

- Безліч інструментів безпеки в одному корпусі

- Єдиний додаток для управління декількома пристроями DefensePro в різних центрах обробки даних

- Повний захист інвестицій і продовження терміну служби платформи з можливістю масштабування оновлення ліцензії по мірі зростання, що забезпечує найкращий захист інвестицій з точки зору ROI і капітальних вкладень

2) Система Arbor TMS, рішення Arbor для захисту від DDoS-атак об'єднує в собі мережеву розвідку і виявлення аномалій з управлінням загрозами операторського класу, щоб допомогти виявити і зупинити об'ємні DDoS-атаки, виснаження стану TCP і DDoS-атаки на рівні додатків.

Мережеві пристрої Arbor TMS забезпечують життєво важливий компонент рішення Arbor, що очищає трафік. Arbor TMS може бути розгорнутий в лінію для забезпечення "завжди включеного" захисту. На відміну від інших продуктів, він також підтримує архітектуру пом'якшення наслідків, яка називається "перенаправлення/реінжекція". У цьому режимі тільки потік трафіку, що несе DDoS-атаку, перенаправляється на Arbor TMS за допомогою оновлень маршрутизації, що випускаються рішенням Arbor. Arbor TMS видаляє з цього потоку тільки зловмисний трафік, а легітимний трафік перенаправляє за призначенням.

Це дуже вигідно для постачальників послуг, великих підприємств і великих хостингових/хмарних провайдерів. Це дозволяє єдиній, централізовано розташованій системі Arbor TMS захищати кілька каналів зв'язку і кілька центрів обробки даних. Це призводить до набагато більш ефективного використання засобів пом'якшення наслідків і повністю ненав'язливого захисту. Вбудовані пристрої повинні постійно перевіряти весь трафік на каналах, які вони контролюють. Arbor TMS повинен перевіряти тільки той трафік, який перенаправляється на нього у відповідь на атаку на конкретну ціль.

Arbor TMS поставляється з різними платформами і можливостями пом'якшення наслідків атак, включаючи 2U пристрої (500 Мбіт/с-400 Гбіт/с), шасі 6U (10-100 Гбіт/с), Cisco ASR

9000 Router (10-60 Гбіт/с) та віртуальні гіпервізори з підтримкою KVM та VMware (1- 40 Гбіт/с).

Рис 1.8 – Arbor системи захисту

3)Рішення Huawei Next Generation (NG) Anti-DDoS виконує абстрактне моделювання та побудову системи репутації на мережевому трафіку з більш ніж 60 вимірів, використовуючи технології аналітики Big Data. У порівнянні з традиційними механізмами захисту від DDoS в галузі, рішення Huawei NG Anti-DDoS забезпечує більш точний і комплексний захист від DDoS-атак.

Функціональні можливості:

Anti-Large-DDoS: захист від DDoS-атак з великим трафіком

- Багатоядерна, розподілена апаратна архітектура та інтелектуальний механізм захисту на основі великих даних Intelligent Defense Engine1 забезпечують Т-бітну продуктивність захисту.

- Миттєва реакція на атаку протягом декількох секунд захищає доступність каналу зв'язку.

Anti-App-DDoS: Захист від DDoS-атак на додатки

- Виконує весь збір трафіку та 3-7-шаровий пакетний аналіз, створює моделі трафіку з більш ніж 60 вимірів, забезпечує найбільш точне та всебічне виявлення атак.

- Тонка система репутації, що складається з репутації на основі поведінки локального сеансу, репутації на основі поведінки доступу до сервісу, репутації на основі географічного розташування та хмарної репутації ботнету, точно захищає від різноманітних легких, повільних DDoS-атак на рівні додатків, що запускаються ботнетами.

- Повномасштабний захист від понад 100 атак гарантує безперервну роботу ключових сервісних систем, що охоплюють корпоративні веб-додатки та послуги DNS, DHCP і VoIP.

Anti-Mobile-DDoS: Захист від мобільних DDoS-атак

- Динамічне оновлення в режимі реального часу 20 000 "відбитків пальців" та фільтрація трафіку за базою даних мобільних бот-мереж ефективно захищають від DDoS-атак, що здійснюються бот-мереж та мобільних терміналів і гарантує санкціонований доступ до мобільних шлюзів.

- Захищає доступність мобільних сервісів передачі даних, таких як мобільні платежі, мобільні магазини, мобільні соціальні мережі та мобільні ігри.

Anti-Outbound-DDoS: Захист від вхідних та вихідних DDoS-атак

- Блокування найактивніших у світі зомбі, троянських коней та черв'яків, що контролюють трафік.

- Блокування трафіку C&C DNS-запитів.

- Запобігає DDoS-атакам в джерелі.

Managed-Anti-DDoS: Керована служба захисту від DDoS-атак

- Забезпечує автоматичні і ручні політики захисту на основі зон (VIP)/сервісів і повні методи захисту.

- Незалежні статистичні звіти на основі VIP/сервісу та розсилка електронною поштою спрощують управління захистом.

- Підвищує прихильність VIP-користувачів до послуг за рахунок надання функцій самообслуговування на основі порталу для VIP-користувачів.

- Підтримує великомасштабні операції, наприклад, 10 000 VIP-персон/сервісів, і захищає 10 000 IP-адрес кожного VIP-персони/сервісу одночасно.

Рис 1.9 - Huawei системи захисту

1.5 Діяльність та опис за стосунку

Ефективність систем захисту від DDOS-атак будемо перевіряти на основі мобільного застосунку «Travel Helper», який за останні роки набирає все більшу популярність. Компанія займається розробкою мобільного застосунку для допомоги мандрівникам. Клієти, користуючись мобільним за стосунком мають змогу у будь-який час та у будь-якій країні знайти інформацію за місцевістю, одразу забронювати готель та знайти місця для відпочинку та прийому їжі. Наразі вже нараховується більше 1млн онлайн клієнтів. Тому постає питання, щодо забезпечення стабільної роботи застосунку, безперервної роботи для збереження

та підтримки репутації. Робота офіційна, тому кожний працівник ознайомився та підписав «положення про конфіденційну інформацію та комерційну таємницю».

1.6 Висновки

Неможливо не помітити, що світ поступово підходить до етапу прямої залежності від інформаційних технологій та онлайн доступу до Мережі. Всесвітня "коронакриза" посилила інтерес споживачів до інтернет-торгівлі, дистанційного навчання, онлайн-комунікацій та розважальних ресурсів. Як наслідок, на тлі неухильного зростання кількості DDoS-атак стався їх різкий сплеск. Власники сервісів і ресурсів змушені подвоїти свою увагу до їхнього захисту від впливів зловмисників і "заряджених" ними ботів.

Електронна пошта, SIP-дзвінки, спілкування і безперервне перебування онлайн, проведення платежів або переказів, інтернет-покупки - вже давно доступні з телефонів і планшетів. Саме зараз загроза зупинки безлічі сервісів є актуальною для зловмисників. Тому використання засобів захисту від DDoS-атак стає таким самим актуальним засобом захисту мережі, як брандмауер, система виявлення/запобігання вторгненням або управління уніфікованими загрозами.

У момент проведення DDoS-атаки заражені хости з будь-якої точки світу перевантажують апаратні або програмні ресурси жертви (сервер, мережевий пристрій, мережу), чим викликають відмову в обслуговуванні легітимних клієнтів. Тим самим перериваючи роботу online-сервісів, інформаційних порталів, електронних платежів.

Вести бізнес онлайн і бути при цьому стовідсотково спокійним вкрай важко. Інтернет-ресурси мають великі ризики піддатися хакерським нападам. Важливо своєчасно мінімізувати ймовірність такої небезпеки.

РОДІЛ 2 СПЕЦІАЛЬНА ЧАСТИНА

У цьому розділі розділі розглянемо потенційні загрози, виявимо та оцінемо порушника, інсталюємо систему систему захисту від масивних DDOS-атак на сервер автентифікаціїї мобільного застосунку «Travel Helper» для інформаційної безпеки даних та безперебійної роботи, розглянемо користь даних систем та їх актуальністьу сучасному світі.

2.1 Оцінювання ризиків

Для середовища ІТС, необхідно визначити всі можливі потенційні загрози. Походження загроз може бути випадковим і навмисним.

Випадкове походження обумовлюється спонтанними і не залежними від волі людей обставинами, що виникають в ІТС в процесі її функціонування. Найбільш відомими випадковими загрозами є стихійні лиха, відмови, збої, помилки та побічні впливи.

Сутність цих загроз (окрім стихійних лих, сутність яких незрозуміла):

–відмова – порушення працездатності системи, що призводить до неможливості виконання нею основних своїх функцій;

– збій – тимчасове порушення працездатності системи, наслідком чого може бути неправильне виконання у цей момент своїх функцій;

–помилка – неправильне виконання системою своїх функцій, що відбувається внаслідок її специфічного стану;

Навмисне походження загроз обумовлюється зловмисними діями співробітників. Передумови появи таких загроз можуть бути об'єктивними та суб'єктивними.

Об'єктивні передумови можуть бути спричинені кількісною або якісною недостатністю елементів системи тощо.

До суб'єктивних передумов відносяться різновиди людської діяльності: розвідка (хакери конкурентів), злочинні дії, неякісна робота персоналу ІТС. В даному випадку джерело загрози – хакери, які навмисно можуть завдати шкоди

серверам мобільного за стосунку. Спираючись на обране джерело загроз, визначаємо кількість загроз, потенційно можливих у сучасних ІТС. При цьому врахуємо не лише всі відомі загрози, але й ті загрози, що раніше не виявлялися, але потенційно можуть виникнути. В даному випадку акцентується увага на зовнішніх загрозах.

Модель загроз визначає:

– перелік можливих типів загроз, класифікований за результатом впливу на інформацію, тобто на порушення яких її властивостей вони спрямовані (конфіденційності, цілісності або доступності інформації);

– перелік можливих способів реалізації загроз певного типу (способів атак) відносно різних інформаційних об’єктів ІТС у різному стані класифікований, наприклад, за такими ознаками, як компонент обчислювальної системи ІТС або програмний засіб, уразливості яких експлуатуються порушником, причини виникнення відповідної уразливості тощо.

Загрози для інформації, що обробляється в ІТС, залежать від характеристик ОС, апаратного складу, програмних засобів, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу.

Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Визначені основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно ІТС і повинні враховуватись у моделі загроз, наприклад:

– зміна умов фізичного середовища (стихійні лиха і аварії,пожежа або інші випадкові події);

– збої та відмови у роботі технічних або програмних засобів ІТС;

– наслідки помилок під час проектування та розробки компонентів ІТС (технічних засобів, технології обробки інформації, ПЗ, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) ІТС під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

Випадкові загрози суб'єктивної природи – це помилкові дії персоналу по неуважності, недбалості, незнанню тощо, але без навмисного наміру.46

До них відносяться:

– дії, що призводять до відмови ІТС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм тощо);

– ненавмисне пошкодження носіїв інформації;

– неправомірна зміна режимів роботи ІТС, ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації або виведення з ладу серверві обслуговування);

– неумисне зараження ПЗ комп'ютерними вірусами;

– невиконання вимог до організаційних заходів захисту чинних в ІТС розпорядчих документів;

– помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

– будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

– неправомірне впровадження та використання заборонених політикою безпеки ПЗ (наприклад, навчальні та ігрові програми, системне і прикладне забезпечення тощо);

– наслідки некомпетентного застосування засобів захисту тощо.

Навмисні загрози суб'єктивної природи – це дії порушника, спрямовані на проникнення в систему та одержання можливості НСД до її ресурсів або дезорганізацію роботи ІТС та виведення її з ладу.

До них відносяться:

– порушення фізичної цілісності ІТС (окремих компонентів, пристроїв, обладнання, носіїв інформації);

– порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІТС (електроживлення, заземлення, охоронної сигналізації, кондиціонування тощо.);

– порушення режимів функціонування ІТС (обладнання і ПЗ);

– впровадження та використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки;

– використання (шантаж, підкуп тощо) з корисливою метою персоналу ІТС;

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);

– несанкціоноване копіювання носіїв інформації;

– читання залишкової інформації з оперативної пам'яті ЕОТ, зовнішніх накопичувачів;

– одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача; – неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо; Для кожної з загроз необхідно визначити її спрямованість, джерело, механізм реалізації та можливі наслідки.

По-перше, на порушення яких властивостей інформації або ІТС загроза спрямована:

– конфіденційності – несанкціоноване ознайомлення з інформацією;

– цілісності – несанкціонована модифікація (спотворення, фальсифікація, викривлення) інформації;

– доступності – порушення можливості використання ІТС або оброблюваної інформації (відмова в обслуговуванні користувача);

По-друге, джерела виникнення загрози (які суб'єкти ІТС або суб'єкти, зовнішні по відношенню до неї, можуть ініціювати загрозу):

– персонал і користувачі;

– технічні засоби;

– моделі, алгоритми, програми;

– технологія функціонування;

– зовнішнє середовище.

«Модель загроз» сформавана у вигляді системи таблиць (№2.1) , визначенням порушень властивостей інформації та ІТС.

Таблиця 2.1 – Загрози для ІТС

	Потенційні загрози для ІТС	Ризики для ІТС		
		К	Ц	Д
Загрози природних явищ(місто)				
1.1	Пожежа, затоплення	-	-	+
1.2	Втрата електроживлення	-	-	+
1.3	Втрата / пошкодження комунікаційних каналів	-	-	+
1.4	Перенавантаження системи	+	+	+
1.5	Збої та відмови обчислювальної техніки, програмного забезпечення	+	+	+
Порушення нормального режиму роботи				
2.1	Зараження серверу авторизації вірусами	+	+	+
2.2	Пошкодження носіїв інформації для відновлення працездності серверів автентифікації	-	-	+
2.3	Доступ до серверів мобільного застосунку сторонніх осіб	+	+	+
2.4	Впровадження та доступ до системи агентів інших компаній до центра керування або до приміщення, де зберігаються ТЗ.	+	+	+
Помилки співробітників				
3.2	Встановлення сторонніх програм , що не є необхідними для виконання обов'язків	-	+	+
3.3	Помилки DevOps при опрацьовування серверів авторизації	+	-	+
3.4	Порушення технології обробки, введення та експлуатації технічних засобів	+	+	+

Зробимо аналіз загроз з урахуванням 3-х рівнів ризиків і збитків за 5-ти бальною шкалою. Отримаємо «Модель загроз з визначенням рівня ризиків і збитків» у вигляді 3-х таблиць в системі таблиць 2.2 (загрози конфіденційності, цілісності, доступності).

- Великий – якщо реалізація загрози надає великих збитків (5 бали);

- Середній – якщо реалізація загрози надає помірних збитків (3 бали);
- Низький – якщо реалізація загрози надає незначних збитків (1 бал).

Таблиця 2.2 - Модель загроз з визначенням рівня ризиків і збитків

	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Загроза конфіденційності				
К.1	Викрадення ТЗ з метою несанкціоновагого ознайомлення сторонніх осіб	3	4	7
К.1	Передавання співробітниками технічних засобів та конфіденційної інформації стороннім особам	2	3	5
К.3	Агенти конкуруючих компаній, які змогли отримати доступ до приміщення із серверами організації	5	5	10
Загроза цілісності				
Ц.1	Навмисна модифікація або створення штучної загрози інформації персоналом ІТС засобами на жорсткому диску або зовнішніх носіях	3	3	6
Ц.2	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація ІзОД (інформація з обмеженим доступом)	3	3	6
Ц.3	Безпосередній доступ до інформації сторонніми особами	1	3	4
Загроза доступності				
Д.1	Помилки співробітників ІТС, які призвели до знищення технічних засобів (серверів авторизації) або доступів до них	5	5	10
Д.2	Помилки системного ПЗ ІТС, які призвели до некороектної роботи або доступів до них	4	5	9

Д.3	Некоректне налагодження засобів захисту, яке призвело до втрати доступу до інформації	4	4	8

Таблиця 2.3 – Загальний рівень ризиків

№	Види загроз	1	2	3	Сума загроз
1	Конфіденційності	7	5	10	22
2	Цілісності	6	6	4	16
3	Доступності	10	9	8	27

Порушення цілісності технічних систем максимально впливає на бізнес компанії, адже основне джерело доходу є мобільний застосунок. Саме через відсутність систем безпеки є велика вірогідність нападу зовнішніх чинників і тому дуже важливо зазделегіть запропонувати рішення щодо захисту серверів мобільного за стосунку,а особливо приділити увагу серверу автентифікації, оскільки клієнти не зможуть навіть увійти у мобільний застосунок. Саме ці проблеми розглядаються, а також аналізуються для впровадження системи захисту від найпопулярнішого виду загроз, DDOS.

2.2 Модель порушника

Порушниками називають осіб, які реалізують загрози. Порушник – фізична особа (у загальному випадку не обов'язково користувач системи), яка здійснює порушення політики безпеки системи. Існують терміни «порушник» та «зловмисник». Останній термін підкреслює умисність порушення, тоді як у загальному випадку порушник може здійснювати порушення неумисно (наприклад, через необережність або недостатню обізнаність).
В першу чергу розглянемо модель порушника –абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час і місце дії тощо. В нашому випадку порушник розглядається, як особа, яка має технічні знання інформаційних систем,

доступ до мобільного застосунку, як клієнт, і мету виведення з ладу системи автентифікації для авторизації.

Метою порушника можуть бути:

– заради забави вкласти сервери мобільного застосунку;

– отримання конфіденційної інформації для конкуруючих компанії;

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами;

– нанесення збитків компанії шляхом виведення з ладу систем для забезпечення коректної роботи мобільного застосунку.

Існує три типи засобів отримання інформації: людина, апаратура, програма. В нашому випадку ми розглядаємо загрози з боку програми – ботнет хакерів робить масивну автентифікацію у мобільному застосунку через заміну пакетів одночасно, чим саме впливає на коректне відпрацювання серверу автентифікації мобільного застосунку.

В компанії на проекті «Travel Helper» працюють 2 DevOps , 1 адміністратор системний, 3 Back-end розробника, 2 Front-end, 2 бізнес-аналітика та 1 продуктовий менеджер і директор. Кожен працівник має свої «ролі» в компанії та займається окремими видами діяльності. Сервера мобільного за стосунку знаходяться в Києві в окремому приміщенні, облаштованному системами вентиляції та однієї броньованою дверею з біометричним замком та 8-значним додатковим паролем. Доступ та паролі з відбитками пальця до кімнати мають лише DevOps та директор.

Модель порушників можна відобразити на таблицях №2.1.1-2.1.6

Для побудови моделі використовуються усі можливі категорії, ознаки та характеристики порушників для більш точного їх аналізу, причому рівень загрози кожної з них оцінюється за 5-бальною шкалою.

Таблиця 2.1 - Модель порушника

Таблиця 1. Категорії порушників , визначених у моделі		
Позначення	Визначення категорії	Рівень загроз (1-5)
Внутрішні по відношенню до ІТС		
ВП1	Технічний персонал, який обслуговує приміщення (електрики,прибиральниці тощо)	3
ВП2	Персонал , який обслуговує технічні засоби ІТС (DevOps)	3
ВП3	Користувачі ІТС (розробники)	1
ВП4	Співробітники служби безпеки установи та керівники різних рівнів	4
Зовнішні по відношенню до ІТС		
ЗП1	Відвідувачі	1
ЗП2	Представники комунальних організацій (енерго-,тепло-,водопостачання тощо)	2
ЗП3	Користувачі звичайні	4
ЗП4	Хакери конкурентів	5

Таблиця 2.2 - Модель порушника

Таблиця 2. Специфікація МП за мотивами		
Позначення	Мотив порушення	Рівень загроз (1-5)
М1	Безвідповідальність	1
М2	Самоствердження	4
М3	Корисливий інтерес	3
М4	Професійний обов'язок (ЗП4)	5

Таблиця 2.3 - Модель порушника

Таблиця 3. Специфікація МП за рівнем кваліфікації та обізнаності щодо ІТС		
Позначення	Основні кваліфікаційні ознаки порушника	Рівень загроз (1-5)
К1	Володіє низьким рівнем знань, але вміє працювати з технічними засобами	2

Продовження таблиці 2.3 - Модель порушника

К2	Володіє середнім рівнем знань та практичними навичками роботи з технічними засобами ІТС та їх обслуговування	3
К3	Володіє високим рівнем знань у галузі програмування та ЕОТ	4
К4	Повністю ознайомлений зі структурою , функціями та механізмами дії організації.	5

Таблиця 2.4 - Модель порушника

Таблиця 4. Специфікація МП за показником можливостей використання засобів та методів подолання системи захисту		
Позначення	Характеристика можливостей порушника	Рівень загроз (1-5)
З1	Може лише підслуховувати розмови у приміщеннях та підглядати у документацію по роботі із серверами авторизації на робочих місцях	1
З2	Використовує пасивні технічні засоби перехвату без модифікацій інформації та компонентів ІТС	1
З3	Використовує лише штатні засоби та недоліки системи захисту для її подолання, а також компактні носії інформації, які можуть бути приховано пронесені крізь охорону	4
З4	Використовує технічні засоби активного впливу з метою модифікації інформації та компонентів ІТС, дезорганізації систем обробки данних в мережі.	5

Таблиця 2.5 - Модель порушника

Таблиця 5. Специфікація МП за часом дії		
Позначення	Характеристика часу дії порушника	Рівень загроз (1-5)
Ч1	Під час повної бездіяльності ІТС	1
Ч2	Під час призупинки компонентів ІТС з метою технічного обслуговування	4
Ч3	Під час функціонування ІТС (або компонентів системи)	2
Ч4	Під час функціонування ІТС, так і під час призупинки компонентів системи	3

Таблиця 2.6 - Модель порушника

Таблиця 6. Специфікація МП за місцем дії		
Позначення	Характеристика місця дії порушника	Рівень загроз (1-5)
Д1	Усередині приміщень, але без доступу до засобів ІТС	1
Д2	З робочих місць працевників	1
Д3	З доступом у зону зберігання баз даних , серверів, архівів тощо	5
Д4	З доступом у зону керування засобами забезпечення безпеки та обслуговування ІТС	5

Після аналізу МП у таблиці, є можливість звезти у загальну таблицю №2.8 мінімальні загрози з причини безвідповідального ставлення до виконання своєї роботи та посадових обов’язків.

Таблиця 2.8 - Модель внутрішнього порушника політики безпеки інформації

Категорія порушн-ика (ВД)	Мотив порушення	Можлив-ості щодо подалання захисту	Можлив-ості за часом дії	Можлив-ості за місцем дії	Рівень обізнаності щодо ІТС	Сума загроз
DevOps	М3	З4	Ч4	Д3	К4	21
Хакери	М4+(ЗП4)	З4	Ч4	Д1	К3	23
Адміністратор	М2	З3	Ч3	Д1	К2	14
Розробники	М1	З1	Ч3	Д2	К2	8
Менеджер	М1	З1	Ч1	Д2	К1	6
Бізнес-аналітик	М1	З2	Ч2	Д2	К2	10

З фінальної таблиці ми бачимо , що найбільша загроза по відношенню до проблеми захисту, становлять хакери да DevOps компанії, які працюють у напрямку оброблення та data обчислень. У випадку з DevOps, робота даних осіб повинна бути більш контрольованою, тому що вона є потенційним порушником безпеки інформації, а хакери (агенти конкурентів) є основним порушником.

2.3 Профіль захищеності

Обраний профіль згідно НД-ТЗІ-2.5-005-99 (https://tzi.ua/assets/files/НД-ТЗІ-2.5-005-99.pdf):

Стандартні функціональні профілі захищеності в КС, що входять до складу АС класу 3, з підвищеними вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

КД (Довірча конфіденційність) – 2: Частково реалізовано

Ця послуга дозволяє користувачу керувати потоками інформації від захищених об'єктів, що належать його домену, до інших користувачів. Рівні даної

послуги ранжируються на підставі повноти захисту і вибірковості керування.

В організації встановлено розмежування доступу до окремих частин мобільного застосунку, доступ до серверної мають лише директор та DevOps-и. Потрібно розділити сервери на окремі приміщення, та надати доступ конкретному DevOps його зону відповідальності.

КО (Повторне використання) – 1: Не Реалізовано

Ця послуга дозволяє забезпечити коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ (Конфіденційність при обміні) – 1: Не реалізовано

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

ЦД (Цілісність Довірча) – 1: Реалізовано

Ця послуга дозволяє користувачу керувати потоками інформації від інших користувачів до захищених об'єктів, що належать його домену. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування. Користувач може надати права на доступ до об’єктів, які обробляє користувач. (На поширені об’єкти будуть накладені права звичайного користувача, що дозволить мати доступ до них без підвищених атрибутів доступу)

ЦО – 1- Відкат: Не реалізовано

Ця послуга забезпечує можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану. Рівні даної послуги ран жируються на підставі множини операцій, для яких забезпечується відкат.

ЦВ (Цілісність при обміні) – 1: Не реалізовано

Ця послуга дозволяє забезпечити захист об'єктів від несанкціонованої модифікації інформації, що міститься в них, під час їх експорту/імпорту через

незахищене середовище. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування.

Цілісність забезпечується за допомогою системних засобів операційної системи, що звіряє повноту переданої інформації за допомогою хеш-функції sha256.

ДР (Використання ресурсів) – 1: Не реалізовано

Ця послуга дозволяє користувачам керувати використанням послуг і ресурсів. Рівні даної послуги ран жируються на підставі повноти захисту і вибірковості керування доступністю послуг КС.

Користувачі не мають обмеження до використання ресурсів, що пропонує мобільний застосунок, проте доступу до самих файлів вони не мають.

ДВ (Стійкість до відмов) – 1: Не реалізовано

Ця послуга забезпечує повернення КС у відомий захищений стан після відмови або переривання обслуговування. Рівні даної послуги ранжируються на підставі міри автоматизації процесу відновлення.

НР (Реєстрація) – 2: Частково реалізовано

Реєстрація дозволяє контролювати небезпечні для КС дії. Рівні даної послуги ран жируються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

Повинно бути реалізовано за допомогою вбудованого системного журналу подій і знаходитись під контролем відповідального адміністратора.

НИ (Ідентифікація і автентифікація) – 2: Реалізовано

Ідентифікація і автентифікація дозволяють КЗЗ визначити і перевірити особистість користувача, що намагається одержати доступ до КС. Рівні даної послуги ран жируються залежно від числа задіяних механізмів автентифікації. Реалізовано за допомогою облікових записів користувачів. Щодо доступу до кімнати з фізичними серверами, двері мають біометричний сканер та пароль, які знають та мають лише директор та DevOps.

НК (Достовірний канал) – 1: Не реалізовано

Ця послуга дозволяє гарантувати користувачу можливість безпосередньої взаємодії з КЗЗ. Рівні даної послуги ран жируються залежно від гнучкості надання можливості КЗЗ або користувачу ініціювати захищений обмін.

НО (Розподіл обов-язків) – 2: Частково реалізовано

Ця послуга дозволяє зменшити потенційні збитки від навмисних або помилкових дій користувача і обмежити авторитарність керування. Рівні даної послуги ран жируються на підставі вибірковості керування можливостями користувачів і адміністраторів.

Один користувач не може нашкодити роботі системи мобільного за стосунку, проте якщо він буде робити по 1млн запитів на мобільний за стосунок, оброблювальна система данних не витримає. Треба впровадити систему фільтрації та блокування запитів на певні сервера для коректної та безперервної роботи мобільного застосунку.

НЦ (Цілісність КЗЗ) – 2: Частково реалізовано

Ця послуга визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НТ (Самотестування) – 2: Частково реалізовано

Самотестування дозволяє КЗЗ перевірити і на підставі цього гарантувати правильність функціонування і цілісність певної множини функцій КС. Рівні даної послуги ран жируються на підставі можливості виконання тестів у процесі запуску або штатної роботи.

Система має можливість до самотестування лише системних файлів, а не користувальних.

НВ (Автентифікація при обміні) – 1: Не реалізовано

Ця послуга дозволяє одному КЗЗ ідентифікувати інший КЗЗ (встановити і перевірити його ідентичність) і забезпечити іншому КЗЗ можливість ідентифікувати перший, перш ніж почати взаємодію. Рівні даної послуги ран жируються на підставі повноти реалізації.

2.4 Впровадження ситеми захисту в мережу мобільного застосунку

На основі вже існуючого мобільного за стосунку інсталюємо систему TMS 2800 Arbor від компанії Arbor Networks.

Рисунок 2.1 – Апаратні засоби захисту від DDOS – атак компанії Arbor

Продукт APS від Arbor Networks забезпечує перевірений on-premise захист від DDoS-атак для критично важливих глобальних корпоративних та урядових мереж. Завдяки розширеним можливостям детектування та відбиття атак DDoS, а також автоматичним оновленням безпеки, які надає група інженерів з безпеки та реагування на загрози (ASERT), APS забезпечує відбиття DDoS як від відомих загроз, так і від загроз, які щойно з'явилися. Завдяки APS організація може підтримувати безперервність бізнесу - незалежно від типу атак.

Рішення Arbor дозволяє провайдерам послуг та хостинг-провайдерам/хмарним провайдерам надавати своїм клієнтам послуги захисту від DDoS-атак. Індивідуальний доступ до порталу, API та делеговане управління надають постачальникам керованих послуг (MSP) гнучкість та контроль для адаптації послуг до потреб своїх клієнтів. Arbor є беззаперечним лідером у сфері

керованого захисту від DDoS-атак. Це рішення, яке обирає переважна більшість провідних провайдерів керованих DDoS-сервісів.

Центри обробки даних та загальнодоступні мережі є численними цілями для DDoS-атак. Ці цілі включають пристрої інфраструктури (наприклад, маршрутизатори, комутатори і балансувальники навантаження), системи доменних імен (DNS), пропускну здатність і ключові додатки, такі як веб, електронна комерція, голос і відео. Навіть пристрої безпеки, такі як брандмауери і системи запобігання вторгнень, є об'єктами атак. Рішення Arbor надає найбільш повний і адаптивний набір можливостей виявлення загроз в галузі, призначений для захисту різноманітних ресурсів від складних, змішаних атак. Ці можливості включають виявлення статистичних аномалій, виявлення аномалій протоколу, зіставлення відбитків пальців і виявлення аномалій за профілем. Наше рішення постійно навчається і адаптується в режимі реального часу, попереджаючи операторів про атаки, а також про незвичайні зміни попиту і рівня обслуговування.

Ключовим фактором для ефективного усунення наслідків атаки є здатність ідентифікувати та блокувати атакуючий трафік, дозволяючи не атакуючий трафік проходити до місця призначення. Масштабні DDoS-атаки впливають не тільки на передбачувану жертву, але і на інших клієнтів, які можуть використовувати ті ж загальні мережевого сервісу. Щоб зменшити цей супутній збиток, провайдери послуг і хостинг-провайдери часто відключають весь трафік, призначений для сайту жертви, таким чином завершуючи DDoS-атаку. Незалежно від того, чи є це атака великого обсягу, призначена для вичерпання пропускної здатності, або цілеспрямована атака, спрямована на виведення з ладу веб-сайту, в деяких випадках Arbor TMS може ізолювати і видалити атакуючий трафік, не впливаючи на інших користувачів, всього за кілька секунд. Методи включають в себе виявлення і внесення в чорний список зловмисних хостів, пом'якшення наслідків на основі IP-адреси, фільтрацію на основі аномалій протоколу, видалення деформованих пакетів і обмеження швидкості, для плавного управління нешкідливими сплесками попиту.

Пом'якшення наслідків можуть бути автоматизованими або ініційованими оператором, а контрзаходи можуть бути об'єднані для протистояти змішаним атакам.

Arbor SP масштабується на фізичні та віртуальні екземпляри для забезпечення комплексного виявлення DDoS-атак у всій мережі постачальника послуг, від межі клієнта до межі пірингу, межі центру обробки даних (або хмарної межі) до мобільної межі, включаючи магістральну мережу між ними.

Завдяки такій безпрецедентній видимості робочі процеси Arbor SP забезпечують швидке ефективне пом'якшення наслідків будь-якої DDoS-атаки за допомогою Arbor TMS або Cisco ASR 9000 vDDoS-захисту. Пом'якшення наслідків на основі контрзаходів масштабується до 400 Гбіт/с на TMS HD1000 і до 8 Тбіт/с в розгортанні. Внесення в чорний список розблоковує додатковий рівень захисту перед будь-якими контрзаходами.

Arbor TMS спрощує і впорядковує операції, надаючи можливість переглядати і управляти до восьми терабіт пропускної здатності з єдиної точки управління. Це дає можливість запобігати численним великомасштабним атакам і створювати комплексні звіти, які підсумовують процес пом'якшення наслідків для клієнтів та/або керівництва.

Для порівняння характеристик систем захисту, було обрано декілька актуальних апаратних засобів від компанії Arbor.

Таблиця 2.9 - Arbor TMS DDoS Defense Специфікації

Одночасні сесії	Кількість сеансів не обмежена
Режими розгортання	Inline Active, Inline Monitoring, SPAN port, Diversion/Reinjection
Блокування дій	Блокування джерела/призупинення джерела; блокування на пакет; комбінація блокування на основі джерела, заголовка та швидкості; автоматичне блокування джерела/призначення BGP Flowspec

Продовження таблиці 2.9 - Arbor TMS DDoS Defense Специфікації

Захист від атак	Reflection Amplification Flood-атаки (TCP, UDP, ICMP, DNS, mDNS, Memcached, SSDP, NTP, NetBIOS, RIPv1, rpcbind, SNMP, SQL RS, Chargen, L2TP, Microsoft SQL Resolution Service); Фрагментаційні атаки (Teardrop, Targa3, Jolt2, Nestea); Атаки на стек TCP (SYN, FIN, RST, ACK, SYN-ACK, URG-PSH, інші комбінації прапорів TCP, повільні TCP-атаки); Атаки на додатки (HTTP GET/POST Floods, повільні HTTP-атаки, SIP Invite Floods, DNS-атаки, атаки на протокол HTTPS); SSL/ TLS-атаки (Malformed SSL Floods, SSL Renegotiation, SSL Session Floods); Отруєння кешу DNS; Атаки на уразливості; Атаки на виснаження ресурсів (Slowloris, Pyloris, LOIC і т.д.).); Flash Crowd Protection; Атаки на ігрові протоколи	
Протидія DDoS-атакам	**Тільки об'ємні контрзаходи**	**Повний набір контрзаходів**
	Недійсні пакети, списки IP-адрес, чорно-білий фільтр, фільтрація заголовків пакетів, списки фільтрів місцезнаходження, виявлення зомбі, захист від віддзеркалення/підсилення UDP, захист від флуду на одне з'єднання, підроблений TCP SYN флуд, аутентифікація TCP SYN, обмеження TCP з'єднань, скидання з'єднань, фільтр регулярних виразів, шейпінг, визначення IP-адреси, вбудований фільтр, "чорні списки", базове налаштування протоколів	HTTP-аутентифікація, HTTP-фільтр, неправильний, HTTP-обмеження, HTTP-списки, обмеження швидкості, HTTP/URL Regular I expression, DNS-аутентифікація, DNS неправильний, DNS-обмеження, DNS-обмеження швидкості, DNS Regular expression, SIP неправильний, SIP-обмеження запитів, SSL-узгодження, ATLAS Intelligence Feed (AIF) TCP

Розглянуто для порівння найбільш актуальні системи захисту від компанії Arbor

Arbor TMS 2600, 2800, 5000, and HD1000 специфікації

Таблиця 2.10 Характеристики систем захисту від Arbor

	Arbor TMS 2600	**Arbor TMS 2800**	**Arbor TMS 5000**	**Arbor TMS HD1000**
Пропускна спроможність і зниження рівня шуму 2600 і 2800 серії – це ліцензія на програмне забезпечення.	Licenses for 1 Gbps, 2 Gbps, 5 Gbps, 10 Gbps (add-on to 20 Gbps) all up to 15 Mpps	Licenses for 10 Gbps, 20 Gbps, 30 Gbps, 40 Gbps, allup to 30 Mpps	**1 x APMe:** Up to 25 Gbps, 10 Mpps **2 x APMe:** Up to 50 Gbps, 20 Mpps **3 x APMe:** Up to 75 Gbps, 30 Mpps **4 x APMe:** Up to 100 Gbps, 40 Mpps	До восьми модулів обробки пакетів (PPM); кожен PPM додає 50 Гбіт/с (25 Мбіт/с) пропускної здатності, Максимально 400 Гбіт/с, 198 Мбіт/с
Вимоги до електроживлення	Резервні джерела живлення змінного струму: 100-240 В змінного струму, 50/60 Гц, 12/6 А макс.; постійного струму: від -40 до -72 Постійний струм, 28/14 А макс.	Резервні джерела живлення змінного струму: 100-240 В змінного струму, 50/60 Гц, 12/6 А макс.; постійного струму: від -40 до -72 Постійний струм, 28/14 А макс.	Резервні чотирифазні джерела живлення змінного струму: 100-120 В змінного струму / 200-240 В змінного струму, 50-60 Гц, 15А; постійного струму: -48/-60 В постійного струму, 90А макс	AC: Два резервних джерела живлення по 1500 Вт; 100-240 В змінного струму, 15-10 А, 50-60 Гц (x2); DC: Два резервних джерела живлення по 1500 Вт; від -48 до -60 В постійного струму, 44 А (x2)
Потреба в електроенергії та теплі	325 Вт (макс.), 280 Вт (номінальна): @ 280 Вт, 955 BTU/год	325 Вт (макс.), 280 Вт (номінальна): @ 280 Вт, 955 BTU/год	1xAPMe: 1090 Вт (макс.), @ 610 Вт (ном.) 2081 BTU/год 2x APMe: 1125 Вт макс., @ 800 Вт ном. 2730 BTU/год 3 x APMe: 1440 Вт макс, @ 980 Вт ном. 3344 BTU/год 4 x APMe: 1595 Вт макс, @ 1160 Вт ном. 3958 BTU/год	1)MM,(5)вентиляторів, (2) QSFP+,(4) QSFP28; (x1) PPM: @ 327 Вт, 1116 BTU/год; (x4) PPM: @ 569 Вт, 1940 BTU/год; (x8) PPM: @ 932 Вт, 3180 BTU/год

Продовження таблиці 2.10 Характеристики систем захисту від Arbor

Розміри	**Шасі**: висота стійки 2U **Вага**: 36.95 фунтів (17.76 кг) **Висота**: 3.45 дюйма (8.76 см) **Ширина**:17.14 дюйма (43.53 см) **Глибина**:20 дюймів (50,8 см)	**Шасі**: висота стійки 2U **Вага**: 36.95 фунтів (17.76 кг) **Висота**: 3.45 дюйма (8.76 см) **Ширина**:17.14 дюйма (43.53 см) **Глибина**: 20 дюймів (50,8 см)	**Шасі**: висота стійки 6U **Вага** З змінним струмом: 77,15 фунта (34,99 кг); З постійним струмом: 58,52 фунта (26,54 кг); Додайте 6 фунтів (2,72 кг) на лезо APM-E **Висота**: 10.463 дюйма (265.76 мм) **Ширина**: 19.00 дюйма (482.6 мм) **Глибина**:18,19 дюйма (462,00 мм) з ручками	**Шасі**: висота стійки 2U **Вага**: 45,2 фунта (20,5 кг) з 1 PPM, додайте 1,6 фунта (.73 кг) на PPM (до восьми) **Висота**:3,5дюйма (88,1 мм) **Ширина**:17,6 дюйма (449 мм) **Глибина**:21дюйм (50,8 мм)
Мережеві інтерфейси	4x10G (SFP+) + 8x1G (SFP) ports	8 x 10 GigE (SFP+ for SR orLR or mixed fiber)	32 x 10 GigE (QSFP+ з розгалужувальними кабелями, SR4 або 4LR); 8 x 40 GigE (QSFP+ SR4 або LR4); 4 x 100 GigE (QSFP28 SR4 або LR4)	4x100G + 8x10G = від одного до чотирьох 100 GbE QSFP28 (LR) оптичних трансиверів + Один або два оптичних трансивера 4 x 10 GbE QSFP+ (SR або LR Lite) з одним розгалужувальним кабелем 4 x 10 GbE на кожному трансивері 16x10G = від одного до восьми оптичних трансиверів 10 GbE SFP+ (SR або LR) + один або два 4 x 10 GbE QSFP+ (SR або LR Lite) оптичні трансивери з одним розгалужувальним кабелем 4 x 10 GbE на кожному трансивері

Продовження таблиці 2.10 Характеристики систем захисту від Arbor

Сховище	2x150GB SSD диски, RAID 1	2x240GB SSD диски, RAID 1	2x128GB SSD диски, RAID 1	2x480GB SSD диски, RAID 1
Екологічні покажчики	Робоча температура: від 41° до 104°F (від 5° до 40°C) Відносна вологість (робоча): від 5 до 85% без конденсації	Робоча температура: від 41° до 104°F (від 5° до 40°C) Відносна вологість (робоча): від 5 до 85%, (неробоча) 95% при температурі від 73° до 104°F (від 23° до 40°C)	Робоча температура: від 23° до 104°F (від -5° до 40°C) Відносна вологість (робоча): від 5% до 85% без конденсації	Робоча температура: 39,2° до 104°F (-5° до 40°C)
Регуляторна діяльність	UL60950-1/CSA 60950-1 (США/Канада); EN60950-1 (Європа); IE60950 (міжнародний), сертифікат CB & Звіт, включаючи всі міжнародні відхилення; GS Сертифікат (Німеччина); EAC-R Схвалення (Україна); CE – низька иректива низької напруги 73/23/EEE (Європа); BSMI CNS 13436 (Тайвань); KCC (Південна Корея); Директива RoHS 2002/95/EC (Європа)	UL 60950-1 2nd edition/ CSA C22.2 № 60950-1-07 2-е видання, низька напруга Директива 2006/95/EC, Безпека Директива 2001/95/EC, CB Сертифікат та звіт відповідно до IEC60950-1, 2-е видання та всі міжнародні відхилення, FCC 47CFR, частини 15, перевірено Обмеження класу A, клас ICES-003 A Limit, Директива з електромагнітної сумісності, 2004/108/EC, EN55022, EN55024, EN61000-4-2, EN61000-4-3, EN61000-4-4, EN61000-4-5, EN61000-4-6, EN61000-4-8, EN61000-4-11, EN61000-3-2,	RoHS 6/6, IEC/EN/UL 60950-1, FCC Частина 15, підрозділ B, клас A, ETSI EN 300 386, UL Mark, CE Mark	RoHS 6/6, IEC/EN/UL CSA 60950-1, FCC Part 15 Підрозділ B, клас A, EN 55022, EN55024, ETSI EN 300 386, cCSAus Mark, CE Mark, KN22, KN24, RCM Mark, KCC Mark, EAC Mark, BIS, CCC Mark (на розгляді).

		EN61000-3-3, ITE класу A VCCI (CISPR 22, Class A Limit), BSMI Схвалення, CNS 13438, Клас A і CNS13436 Безпека, схвалення KCC, схвалення Gost Схвалення, CISPR 22, клас A Обмеження, CISPR 24 Імунітет, Директива RoHS (переглянута)2011/65/EU		
Ціна	103 000грн	105 000 грн	190 000 грн	290 000 грн

Найбільш доречною для мобільного застосунку “Travel Helper” буде система **Arbor TMS 2800** для захисту серверу автентифікації. Ситема **Arbor TMS 2800** відповідає запитам стосовно відстежуваня трафіку в системі,його аналізу та обмеження (рисунок 2.3)

Рисунок 2.2 Основні функції

Arbor Network APS – ефективний технологічний і програмний продукт, що забезпечує безпеку корпоративних мереж від DDoS-атак.

Відрізняючись простотою інтеграції в систему, пристрій Arbor APS надає негайну захист від більшості мережевих загроз. Апаратні настройки налаштовуються без труднощів і не потребують тривалого вивчення. Забезпечення захисту від DDoS-атак відбувається в автоматичному режимі, без активної діяльності з боку системного адміністратора. Разом з тим, завдяки чіткій візуалізації загроз, у адміністратора є можливість швидкої зміни налаштувань і регуляції процесу в разі потреби.

Перейдемо до інсталювання системи захисту від DDOS-атак. Розглянуто схему доступу до мобільного застосунку до впровадження системи захисту. Наразі кожен користувач може увійти у мобільний застосунок, провівши

авторизацію та реєстрацію в додатку. Кожен користувач формує свій токен для користування додатком, завдяки Token Authentication (схема 1.2 та 1.2), який програмно встановлюється на етапі проектування back-end логіки авторизації. Отже на кожного користувача, який авторизовується у мобільному застосунку, відправляються запити до серверу для формування та зберігання токену. На рисунку 2.11 зображено лінійно логіку запитів до серверу на одного клієнта.

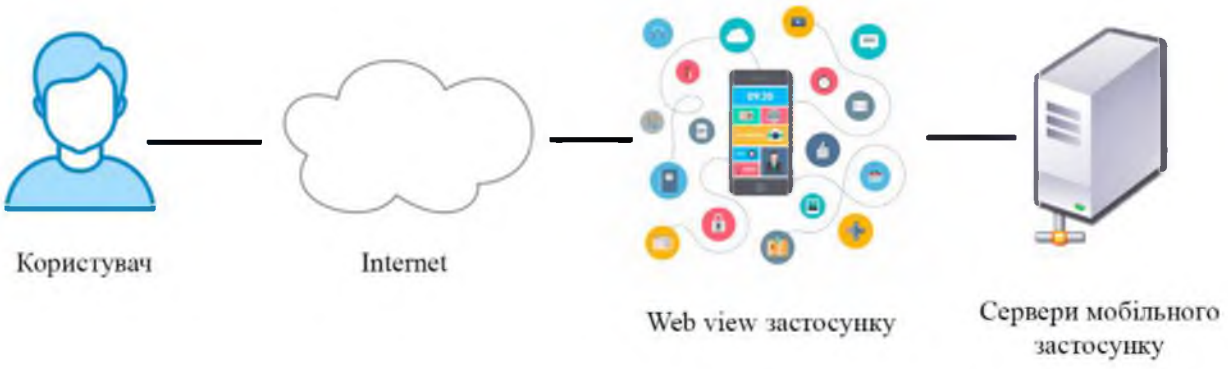


Рисунок 2.11 Початкова схема зв'язку клінт-сервер мобільного застосунку

Коли багато запитів одночасно йде на сервер, може статись перенавантаження (Рисунок 2.12), саме штучні одночасні запити на сервер, це DDoS, розподілена відмова в обслуговуванні. По суті це хакерська атака, яка перевантажує систему, щоб кінцеві споживачі не могли користуватися сервісом. Атака може бути спрямована на всю IT-інфраструктуру, конкретний сервіс або канал до цього сервісу. В даному випадку розглянуто атаку на сервер автентифікації мобільного застосунку, через який клієнти отримуюит авторизований токен та доступ у додаток.

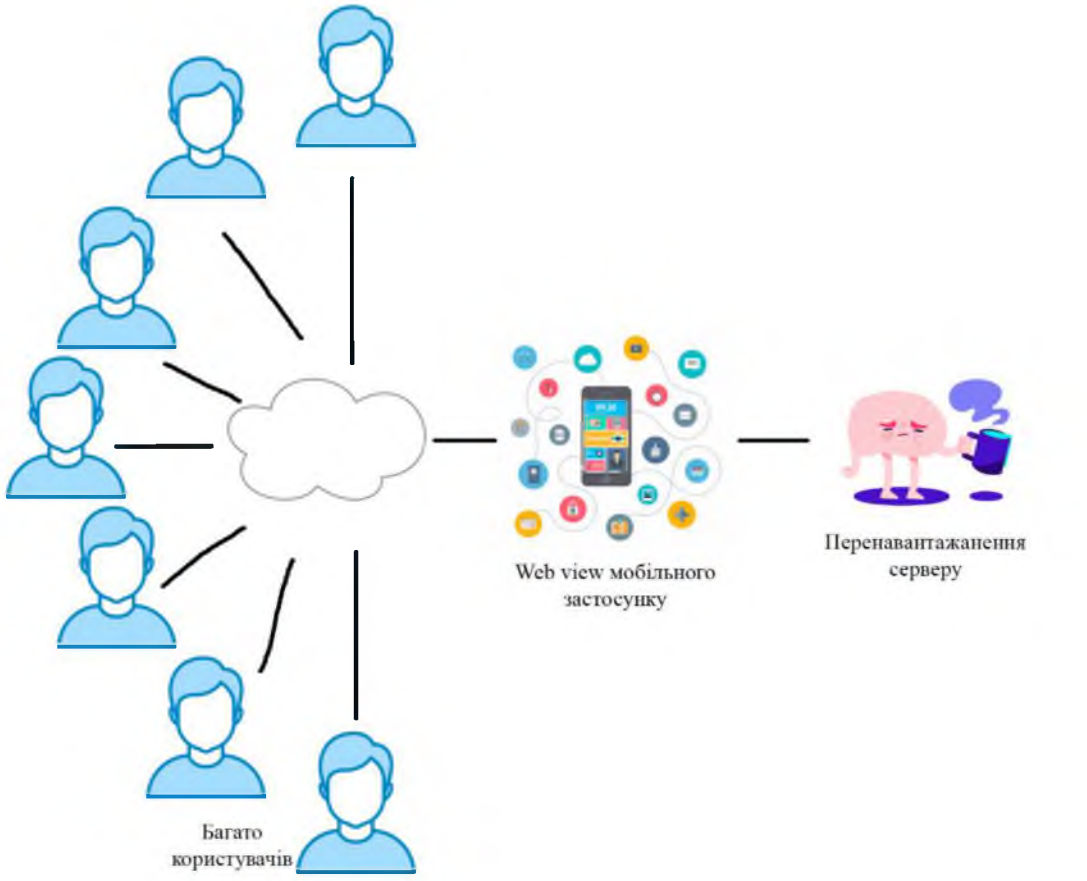


Рисунок 2.12 Перенавантаження серверу

Саме для контролю трафіку від перенавантаження було впроваджено систему Arbor TMS 2800. Однією з ключових переваг цього рішення є можливість його використання у вигляді віртуальної машини, що розміщується в стандартному кластері серверів. Це важливо, оскільки специфіка бізнесу інтернет-сервіс провайдерів така, що вони прагнуть скоротити число точок відмови при передачі трафіку. А в Arbor його аналіз виконується тільки на базі зібраних на маршрутизаторах мета-даних без необхідності безпосереднього перенаправлення трафіку. При цьому платформа дозволяє відсікти до 95% DDoS-атак на базових налаштуваннях. Інтеграцію і налаштування платформи Arbor виконуємо схематично на рисунку 2.13. Швидкість спрацьовування системи Arbor при появі DDoS-атаки становить від 1 секунди, при середньому значенні 10-15 секунд. Її виявлення відбувається шляхом аналізу BGP / Flow / SNMP. Це активує автоматичне перенаправлення трафіку на систему очищення Arbor TMS (Threat Mitigation System), після якої легітимний трафік відправляється до одержувача.

При цьому є можливість блокування атак рівнів L3 / L4 на самих маршрутизаторах провайдера з використанням протоколу BGP FlowSpec. Це дозволяє відсікти об'ємну атаку на кордоні мережі, без перевантаження систем DPI. Подібне рішення просто незамінне для операторів, у яких загальний потік може досягати сотен гігабіт на секунду, і з ним однозначно не впорається DPI-рішення з продуктивністю навіть в десятки гігабіт на секунду. Взагалі, можливість масштабування ресурсів Arbor TMS дозволяє будувати успішну бізнес-модель, пропонуючи ряду клієнтів смугу пропускання цього сервісу, з тим розрахунком, що DDoS-атаки не будуть негативно впливати на всіх їх одночасно.

Перевагою Arbor TMS є також здатність з хірургічною точністю виділяти з потоку, який проходить через систему очистки, корисний трафік, що дозволяє не переривати надання сервісів клієнта оператора.

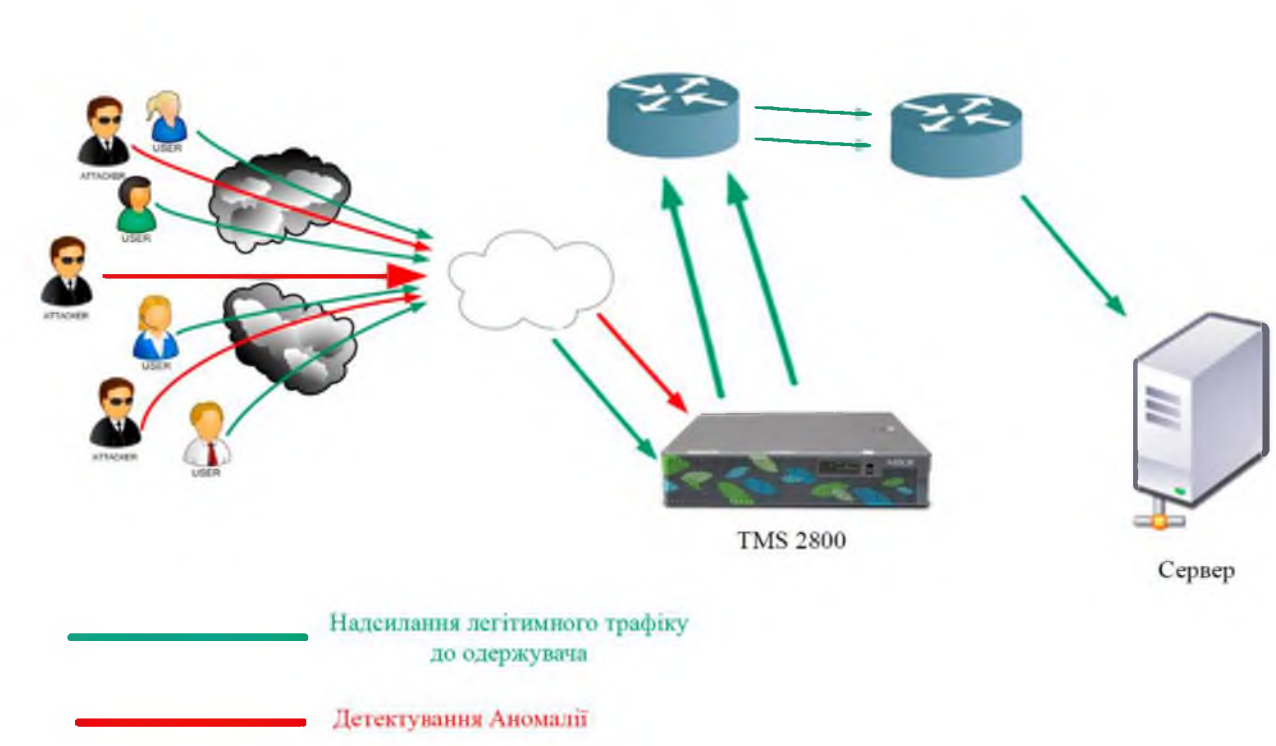


Рисунок 2.13 Інстальована система захисту

Функціональність платформи Arbor передбачає не тільки визначення установок за замовчуванням, але і тонкий підбір параметрів під кожне конкретне підключене до сервіс-провайдера підприємство. В результаті можна повністю

убезпечити операційну діяльність клієнта від зловмисного впливу DDoS-атак практично будь-якого рівня складності.

Отже було зазначенно основні налаштування системи TMS 2800 та інтегровано у мережу мобільного застосунку.

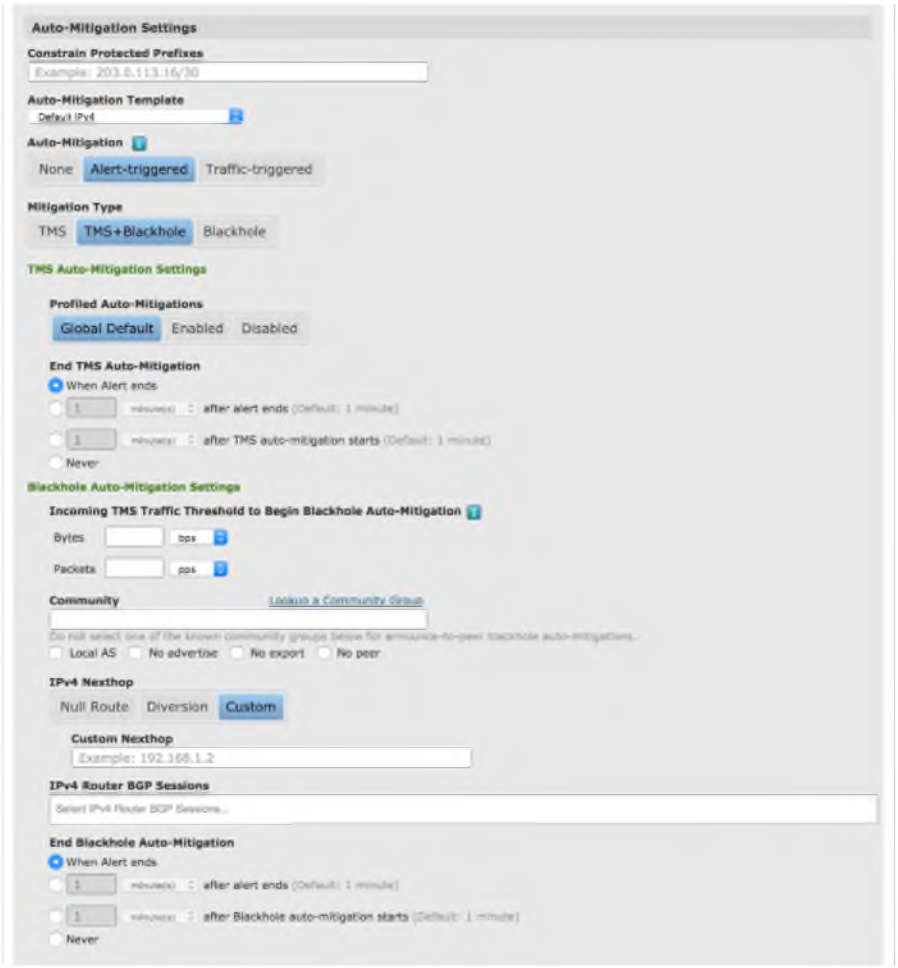


Рисунок 2.14 Blackhole Auto-Mitigation

- TMS

- Попередження про хост запускає пом'якшення наслідків TMS

- Чорна діра

- Сповіщення хоста запускає пом'якшення чорної діри

- TMS+Чорна діра

- Пом'якшення наслідків TMS
- Трафік TMS запускає пом'якшення чорної діри

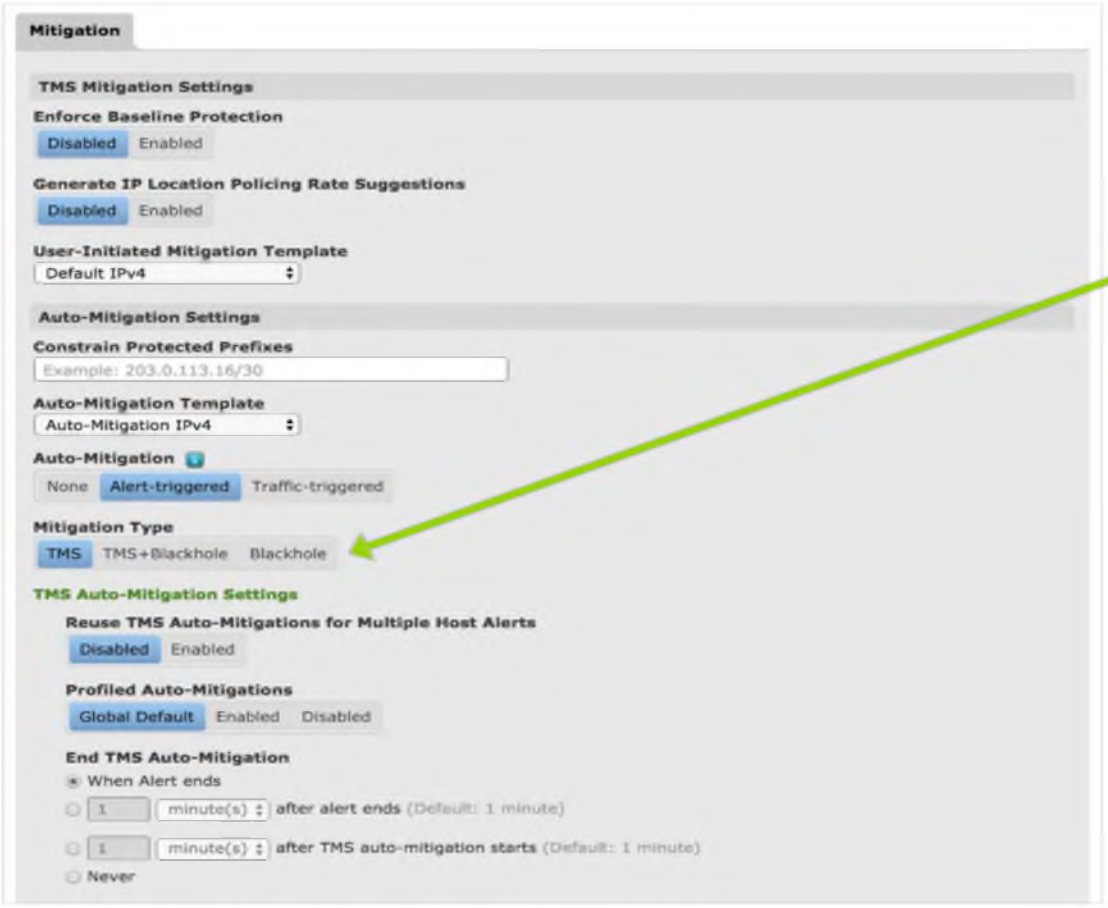


Рисунок 2.15 Налаштування захисту від чорних дір

- Засоби захисту від чорних дір Arbor SP призначені для захисту від TMS-атак, щоб обробляти атаки до того, як загальний трафік загрожує перевищити норму:

- Пропускна здатність TMS сайту замовника

- Пропускна здатність висхідної / низхідної лінії зв'язку сайту замовника

- Arbor SP також підтримує пом'якшення наслідків чорних дір як захист для клієнтів без TMS

- Не хірургічне втручання

- Виводить ціль атаки в автономний режим

- Arbor пропонує використовувати TMS

Рисунок 2.16 Налаштування TMS

- Нова опція повторного використання автоматичного заспокоєння для декількох оповіщень про виявлення хостів

- Налаштовується для кожного керованого об'єкта

- Доступно лише для автоініціювання TMS за тривогою

- Не доступно для автоматичних сповіщень TMS+Blackhole

- Зменшує кількість автоматичних сповіщень TMS, коли багато хостів піддаються одночасній атаці

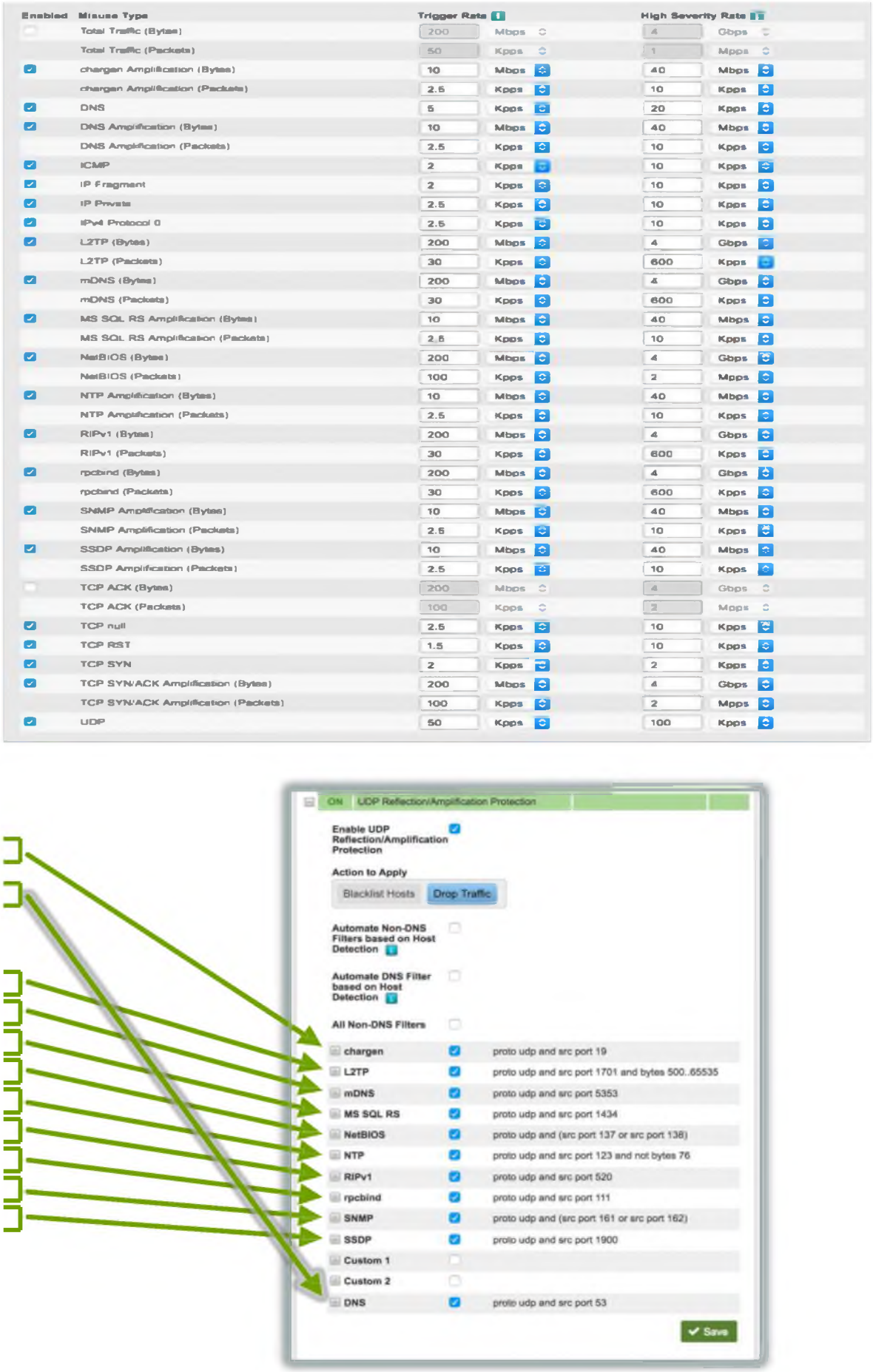


Рисунок 2.17 Автоматизація очищення підвищенних атак

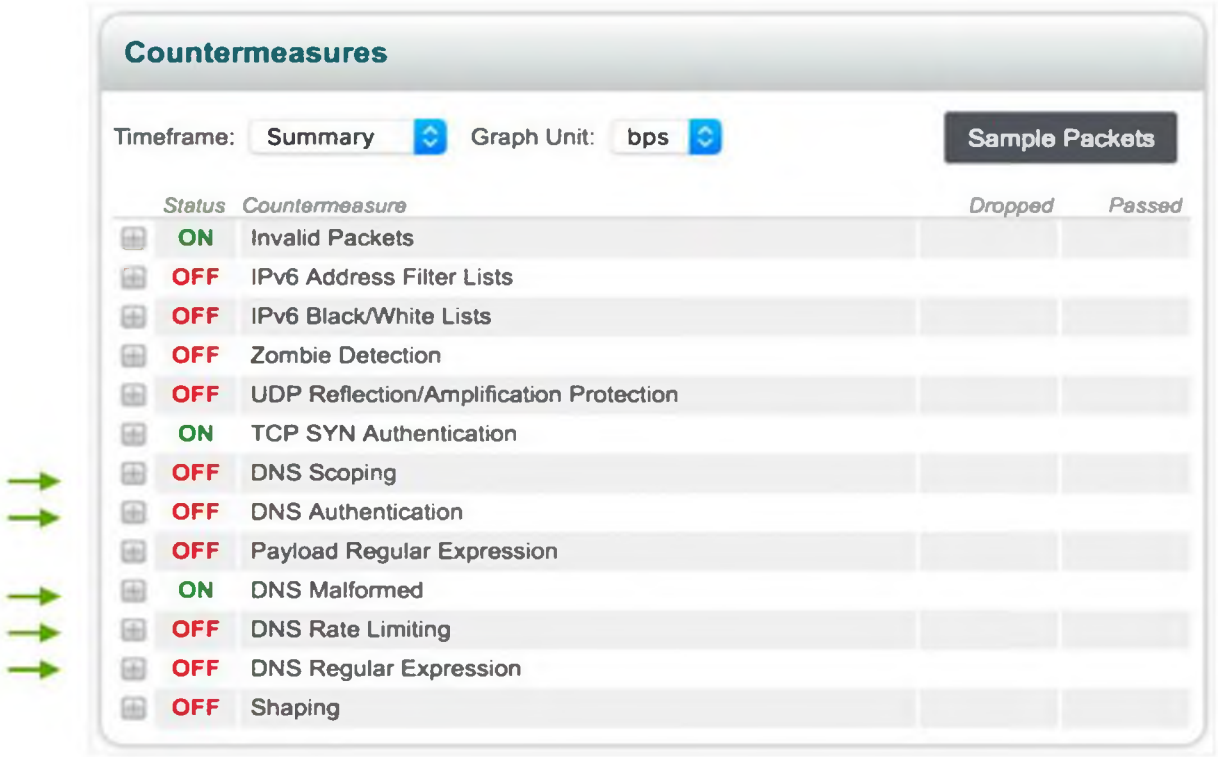


Рисунок 2.18 DNS IPv6 лічильники

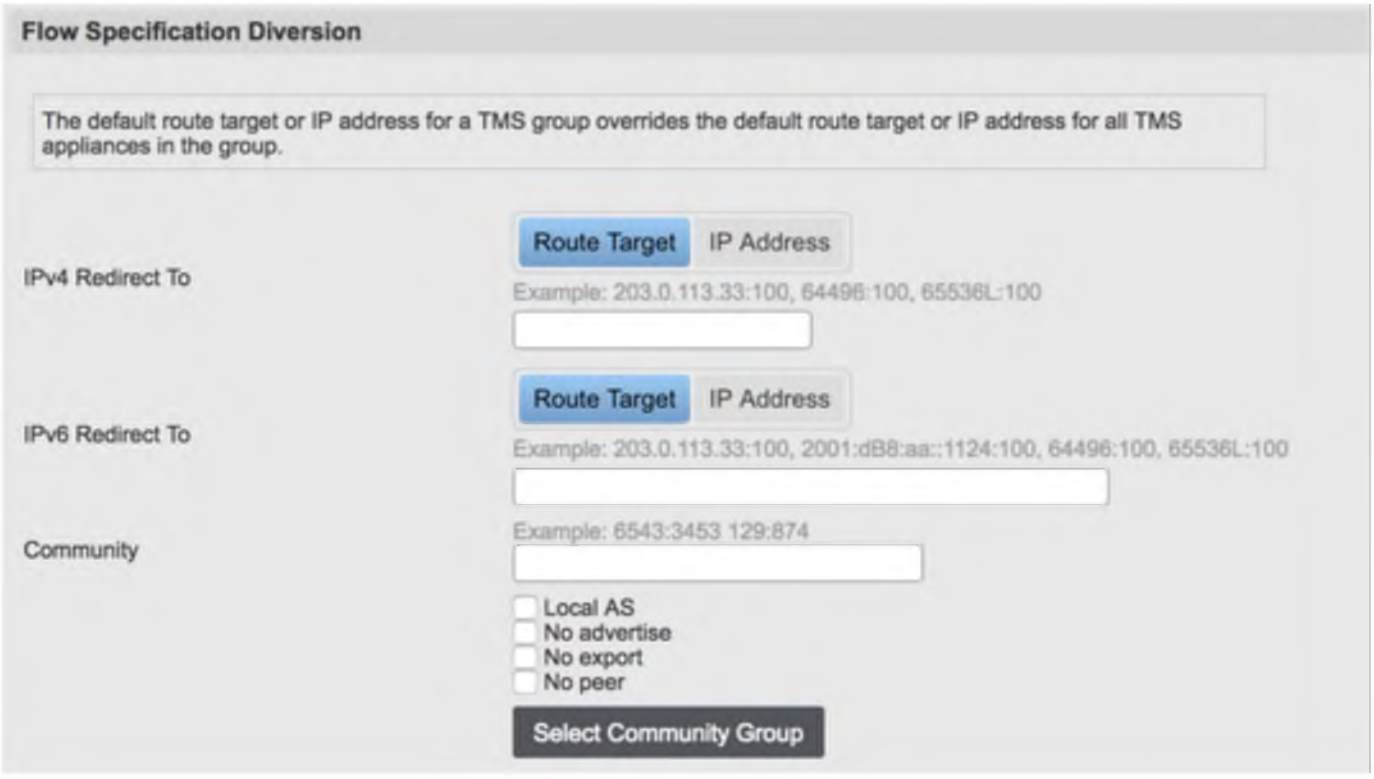


Рисунок 2.19 Redirect IPv4/IPv6 за допомогою FlowSpec

- Пом'якшення TMS IPv4/IPv6 підтримують перенаправлення потоку на TMS

- Тільки при перенаправленні через пірінгові оголошення SP

- Перенаправлення трафіку на цільовий маршрут або IPv4/IPv6-адресу

- Функціональний паритет з перенаправленням IPv4 flowspec на TMS

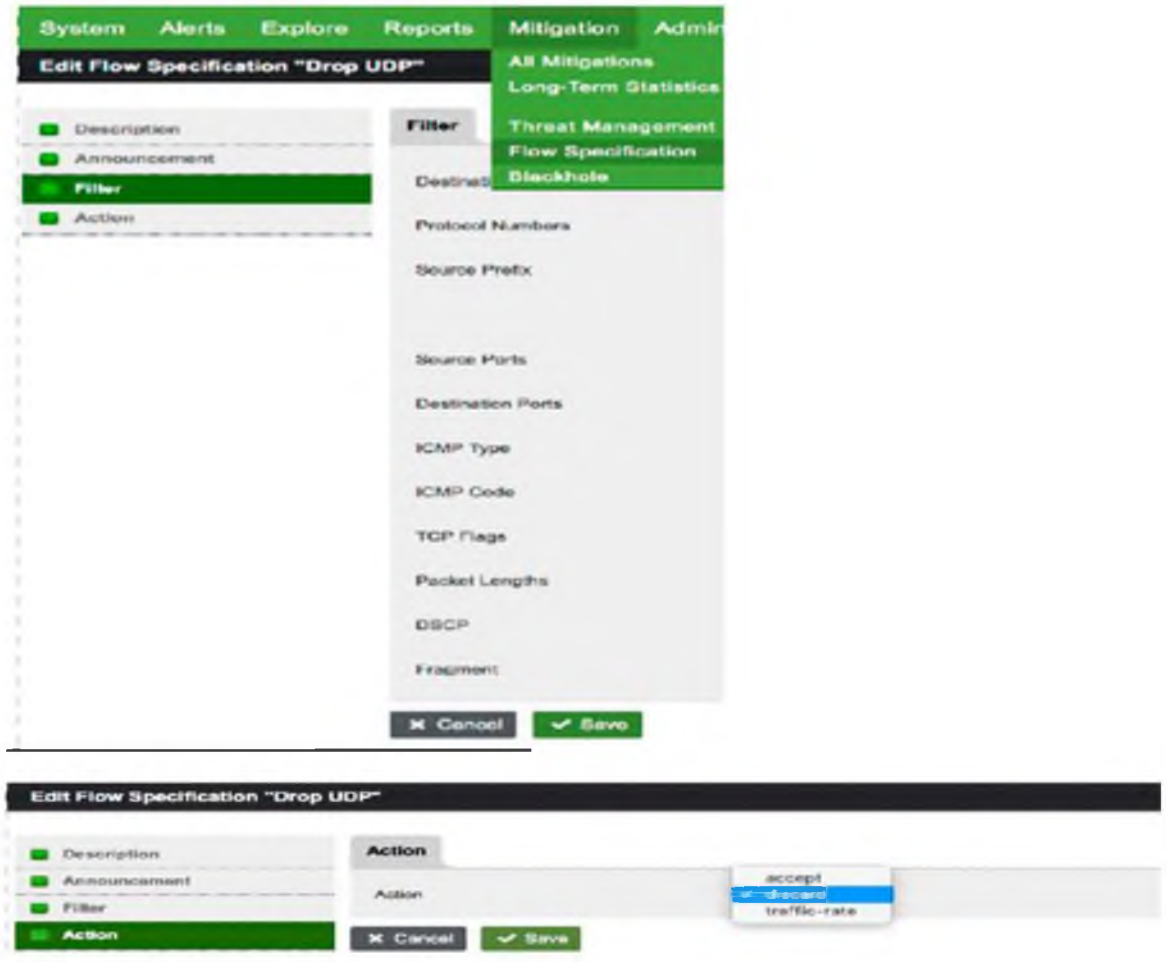


Рисунок 2.20 Вивантаження FlowSpec

- Робить маршрутизатор частиною системи MITIGATION

- Вивантажує фільтри FlowSpec на маршрутизатор

- Блокує масовий трафік

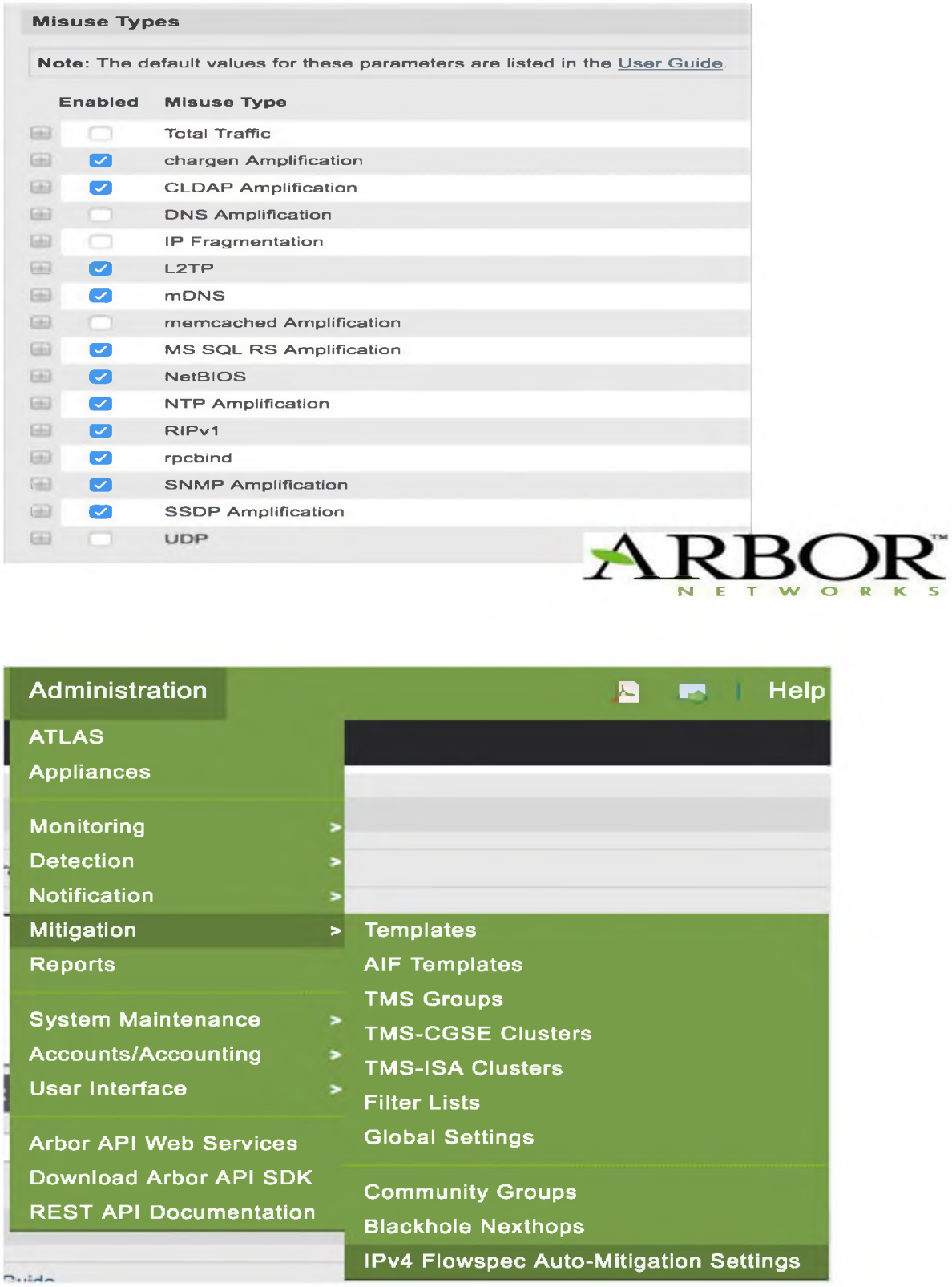
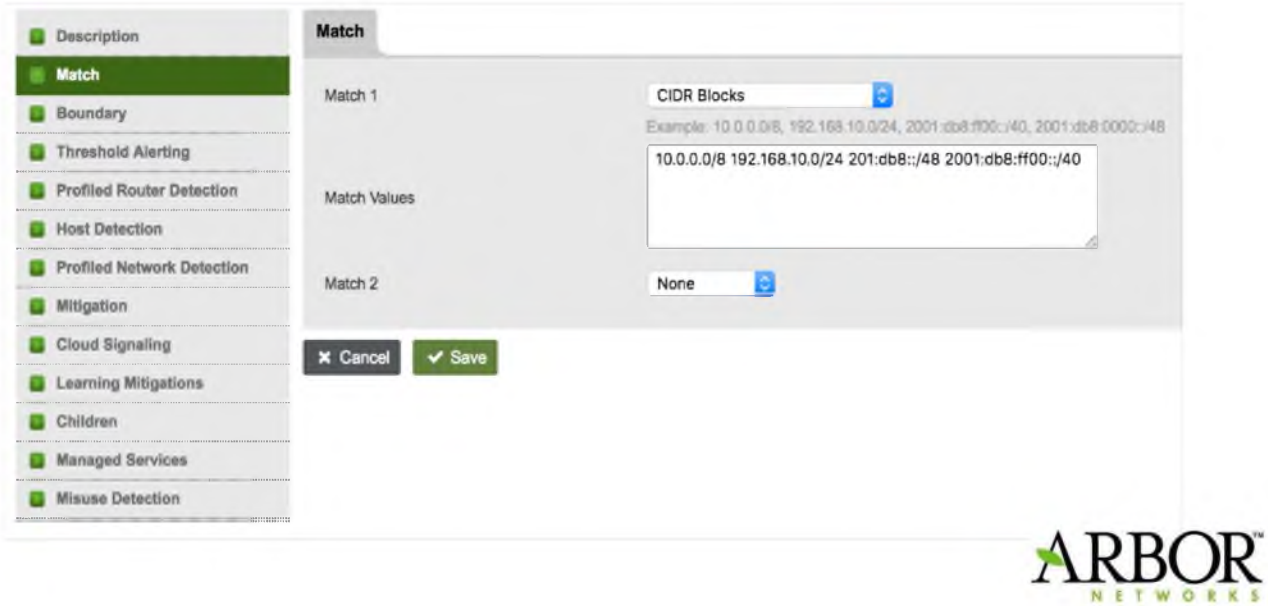


Рисунок 2.21 Автоматизація FlowSpec



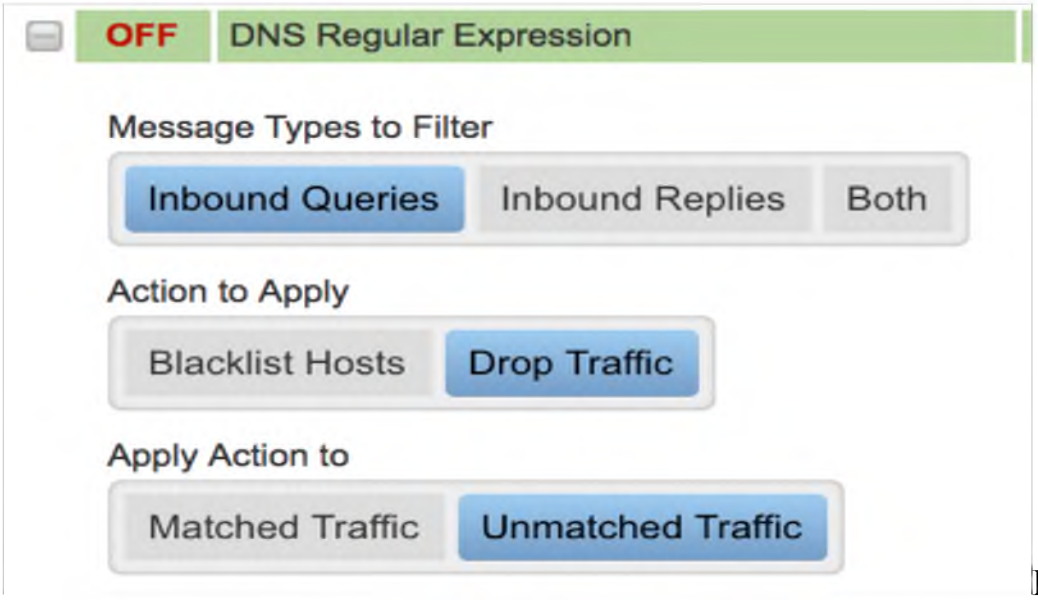


Рисунок 2.22 IPv4/IPv6 комбіновані МО

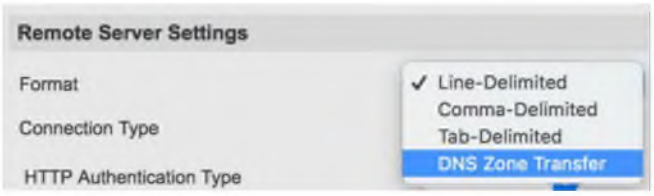


Рисунок 2.23 Захист авторитативних DNS серверів

- SP виконує Zone Transfer і створює/оновлює DNS whitelist, який застосовується в mitigation.

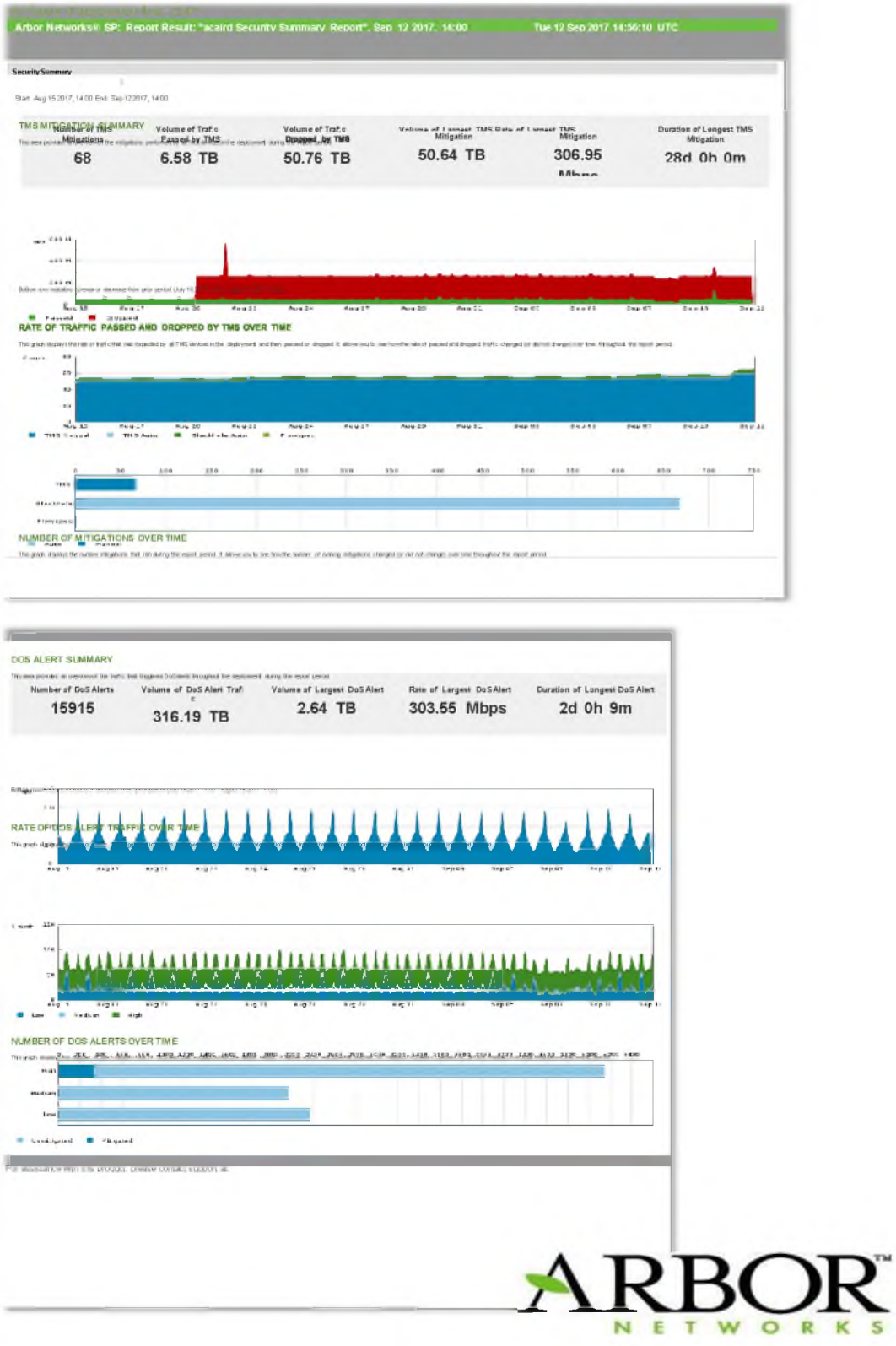


Рисунок 2.24 Виконавчі звіти

Рисунок 2.25 Atlas Global DDoS Report

- Atlas Global DDoS Report
- Глобальний стан світу DDoS за останній місяць
- Створюється ASERT
- Дані з ATLAS

Отже після інтегрування та налаштування системи ми отримали захист від мобільних DDoS-атак.

- Динамічне оновлення в режимі реального часу 20 000 "відбитків пальців" та фільтрація трафіку за базою даних мобільних бот-мереж ефективно захищають від DDoS-атак, що здійснюються бот-мереж та мобільних терміналів і гарантує санкціонований доступ до мобільних шлюзів.

- Захистили доступність мобільних сервісів передачі даних, таких як авторизацію та маємо можливість встановити захист на ішні мережеві носії.

2.5 Аналіз змін у мережі

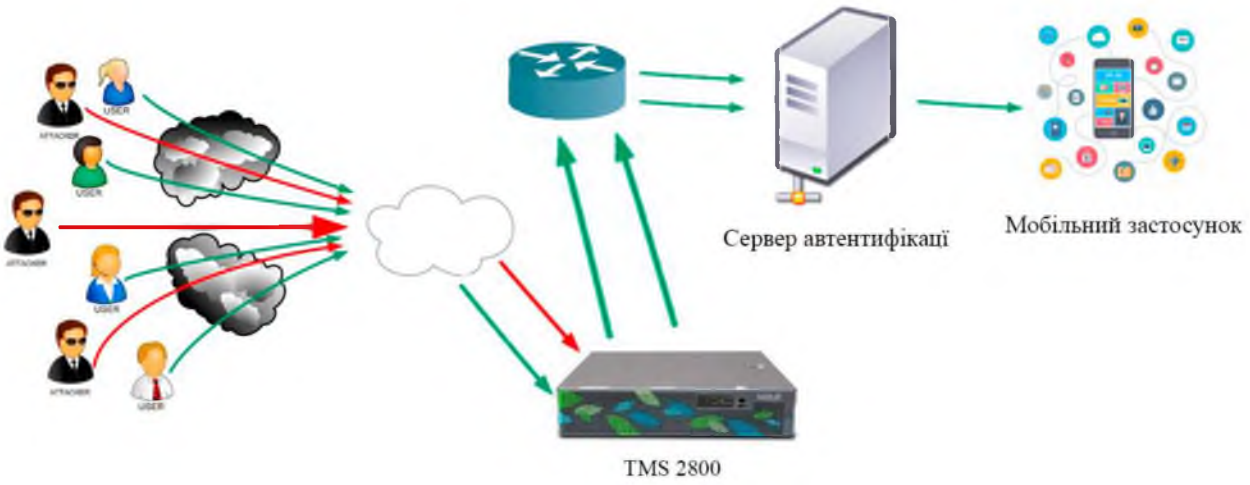


Рисунок 2.26 Мережа мобільного застосунку із захистом серверу автентифікації

Після інсталяції системи в мережу з правильним налаштуванням , ми отримуємо захисту від мережевих атак методом низки фільтрів, під'єднаних до інтернет-каналу з великою пропускною здатністю. Фільтри діють таким чином, що послідовно аналізують трафік, що проходить, виявляючи нестандартну мережеву активність і помилки. До числа аналізованих шаблонів нестандартного трафіку входять усі відомі на сьогоднішній день методи атак, зокрема ті, що реалізуються і за допомогою розподілених бот-мереж. Найефективніші фільтри реалізовуються спеціалізованими апаратними засобами, опис яких представлено нижче. NETSCOUT Arbor - це комплексна система, що забезпечує безпеку найвимогливіших і найскладніших мереж від DDoS атак та інших сучасних просунутих загроз. Рішення Arbor надають всебічний набір продуктів і послуг із захисту від DDoS-атак для хостинг-провайдерів і операторів зв'язку. Продукти Arbor легко масштабуються і мають гнучку модель ліцензування, що дає змогу закрити потреби будь-якої сучасної організації, яка експлуатує віртуальні, хмарні ресурси або власні центри обробки даних.

Рішення Arbor для захисту від DDoS-атак засновані на передових технологіях. NETSCOUT пропонує повний набір повністю інтегрованих продуктів і послуг для захисту від DDoS-атак у хмарних і локальних системах. Якість Arbor підкріплено безперервним і глобальним вивченням сучасних типів загроз.

Компоненти Arbor:

- Arbor Sightline з Insight - забезпечує інтелектуальне уявлення про мережевий трафік для операторів. Розуміння того, звідки йде трафік, Sightline з Insight забезпечує більш точне проєктування трафіку, планування мережі та аналіз пірингу - все це допомагає знизити витрати й оптимізувати послуги.

- Arbor Threat Mitigation System (TMS) - система запобігання загрозам TMS працює спільно з рішенням Arbor Sightline, яке забезпечує видимість і виявлення загроз. Система Arbor Threat Mitigation (TMS) хірургічним шляхом видаляє трафік DDoS-атак з атакованих мереж, не перериваючи роботу ключових мережевих служб.

- Arbor Cloud DDoS Protection Services - поєднує локальний захист від DDoS з хмарними службами очищення трафіку, які тісно інтегровані за допомогою автоматичного хмарного аналізатора. Цей багаторівневий, гібридний підхід є перевіреною передовою практикою в галузі та є єдиним способом зниження сучасного повного спектра загроз DDoS як для постачальників послуг, так і для підприємств.

- ATLAS Intelligence Feed Service (AIF) для NETSCOUT TMS - надає користувачам політики та заходи для протидії атакам як частини розширеної загрози або DDoS-атаки. AIF є службою групи розробки та реагування безпеки ATLAS (ASERT) і була розроблена спеціально для великих мереж, щоб максимально якісно застосувати дослідницькі технології NETSCOUT.

- ATLAS Intelligence Feed (AIF) для захисту Arbor Edge - TLAS Intelligence Feed (AIF) дає користувачам змогу застосовувати політики та контрзаходи для протидії атакам у рамках розширеної загрози або DDoS-атаки. Надана інформація

дає змогу мережевим і операційним командам забезпечувати доступність новітніх засобів захисту від загроз і захищати корпоративне середовище.

- Arbor Availability Protection System (APS) - система забезпечення доступності (APS) забезпечує локальний захист від DDoS-атак від загроз доступності, як-от DDoS-атаки на рівні застосунків, перш ніж вони вплинуть на доступність вашої мережі та служби.

Таким чином на основі звітів , можна зробити висновок а також зробити аналіз загроз з урахуванням системи Arbor TMS 2800.

Проведемо аналіз загроз з урахуванням 3-х рівнів ризиків і збитків за 5-ти бальною шкалою після інсталяції системи Arbor TMS та внесемо у таблицю №2.9

- Великий – якщо реалізація загрози надає великих збитків (5 бали);
- Середній – якщо реалізація загрози надає помірних збитків (3 бали);
- Низький – якщо реалізація загрози надає незначних збитків (1 бал).

Таблиця 2.11 - Модель загроз з визначенням рівня ризиків і збитків після інсталяції системи Arbor TMS

	Механізм реалізації	Рівень		Сума загроз
		ризиків	збитків	
Загроза конфіденційності				
К.1	Викрадення технічних засобів з метою несанкціоновагого ознайомлення сторонніх осіб	1	3	4
К.1	Отримання данних із серверів напряму, шляхом sql ін'єкцій.	1	1	2
К.3	Агенти конкуруючих компаній, які роблять ддос атаку з цілью виведення з ладу серверів з подальшою метою викрадення інформації	1	1	2
Загроза цілісності				
Ц.1	Навмисна модифікація або створення перешкод персоналом ІТС	3	3	6

Продовження таблиці 2.11 - Модель загроз з визначенням рівня ризиків і збитків після інсталяції системи Arbor TMS

Ц.2	Прояви помилок системного ПЗ, в наслідок яких стала можливою модифікація ІзОД(інформація з обмеженим доступом)	1	3	4
Ц.3	Безпосередній доступ до місця із налаштовуваними ТЗ сторонніми особами	3	1	4
Загроза доступності				
Д.1	Помилки співробітників ІТС, які призвели до некоректної роботи ТЗ	1	1	2
Д.2	Помилки системного ПЗ ІТС, які призвели до знищення інформації або доступу до неї	3	5	8
Д.3	Некоректне налагодження засобів захисту, яке призвело до втрати доступу до інформації	1	3	4

Таблиця 2.12 – Загальний рівень ризиків після інсталяції DLP системи DeviceLock

№	Види загроз	1	2	3	Сума загроз
1	Конфіденційності	4	2	2	8
2	Цілісності	6	4	4	14
3	Доступності	2	8	4	14

Отже с фінальної Таблиці №2.10 бачимо , що після впровадження системи Arbor TMS покращили показники КД , КВ , ЦО, ЦВ, ДР, НР, НК, НО, НЦ згідно з НД ТЗІ-2.5-005—99 та знизили рівень загроз для конфіденційності, цілісності та доступності.

КД - встановили обмеження та налагодили керування потоків інформації, розділяючи реальний трафік від бот-систем. Також розділяючи ТЗ зберігання

інформації забезпечили коректність повторного використання розділюваних об'єктів, гарантуючи, що в разі, якщо розділюваний об'єкт виділяється новому користувачу або процесу, то він не містить інформації, яка залишилась від попереднього користувача або процесу.

КВ – реалізовано і система дозволяє забезпечити захист об'єктів від несанкціонованого ознайомлення з інформацією.

ЦО – система дає можливість відмінити операцію або послідовність операцій і повернути (відкатити) захищений об'єкт до попереднього стану.

ЦВ - Цілісність забезпечується за допомогою алгоритмів системи TMS, що дозволяє забезпечити захист об'єктів від несанкціонованої модифікації та ознайомлення з інформацією.

ДР - Користувачі мають обмеження до використання ресурсів, а також системи відстежую трафік запитів та показує у статистиці ATLAS.

НР - система дозволяє контролювати небезпечні для КС дії. TMS 2800 дає можливість аналізу даних журналів реєстрації і спроможності вияву потенційних порушень.

НК – система може відслідковувати взаємодії з КЗЗ

НЦ – система дає змогу серверам захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

НО – система дозволяє зменшити потенційні збитки від навмисних або помилкових дій співробітників і обмежити авторитарність керування. Навіть якщо розробник або DevOps припуститься помилки у керуванні системами, TMS 2800 одразу відповість помилкою та виведе на екран сигнал про порушення роботи будь-якої із систем.

Ключові функції , які тепер викнуються через систему Arbor TMS 2800 в компанії:

- Нові типи Host Detection такі як, TCP ACK, TCP SYN/ACK, L2TP, mDNS, NetBIOS, RIPv1, rpcbind C-LDAP, memcached.
- Захист від DDoS-атак Always On, In-Line Захист від об'ємних DDoS-атак, DDoS-атак з вичерпанням ресурсу, DDoS-атак на рівні додатків.

- Тематична фільтрація.
- Захист вхідного та вихідного трафіку. Зупиняє вхідні DDoS-атаки та вихідну шкідливу активність зі скомпрометованих внутрішніх хостів.
- Інтелектуально автоматизована хмарна сигналізація. При необхідності надсилайте сигнал в хмару Arbor Cloud (або провайдеру), щоб зупинити великі атаки, які можуть перевантажити ваш
- Вбудована перевірка SSL. Зупиняє DDoS-атаки, приховані в зашифрованому трафіку.Захист від локального адміністратора.
- Підтримка IPV6 Виявлення та зупинка атак як на IPv4, так і на IPv6..
- ATLAS Intelligence Feed. Захист, який постійно оновлюється останніми даними про глобальні загрози від команди інженерів з безпеки та реагування (ASERT) компанії Arbor.
- Підтримка віртуальних і гібридних хмарних середовищ. vAPS - це віртуальна версія пристрою APS, яка може працювати у вашому приватному віртуальному середовищі або в Amazon Web Services (AWS), забезпечуючи уніфікований захист вашого гібридно-хмарного середовища..
- Керована послуга APS (mAPS). Arbor Networks для управління локальними продуктами Arbor APS та оптимізації захисту від DDoS-атак.

Портфоліо рішень Arbor Networks для захисту від DDoS-атак бореться з цими передовими загрозами, надаючи вам повний огляд мережевої активності для швидкого усунення та блокування на рівні експертів.

APS допомагає захистити безперервність та доступність бізнесу від зростаючої кількості DDoS-атак та інших сучасних загроз. Він забезпечує найсучасніші та найскладніші у світі засоби виявлення та усунення наслідків атак

Локальний, постійно діючий захист від атак на рівні додатків технологію в простій в розгортанні платформі, призначеній для автоматичної нейтралізації атак IPv4 і IPv6 до того, як вони вплинуть на критичні додатки і сервіси.

Завдяки ATLAS® Intelligence Feed, оновлення в режимі реального часу, що містять оперативну інформацію про DDoS-атаки та сучасні загрози, можуть

допомогти запобігти впливу атак на ваші мережі та сервіси. Такими можливостями є

- DDoS захист від активних бот-мереж
- DDoS захист від активних DDoS-кампаній на основі репутації IP-адреси
- Розширений сервіс веб-сканера
- Відстеження GeoIP
- Репутація домену та IP для блокування загроз

Arbor APS підвищує загальний рівень захисту, використовуючи Cloud Signaling™ для інтелектуального та автоматичного підключення локального захисту до хмарних DDoS-сервісів. За допомогою Cloud Signaling APS автоматично попереджає постачальників послуг, таких як ваш інтернет-провайдер або Arbor Cloud SM, коли великі атаки загрожують доступності. Це дозволяє швидше нейтралізувати атаки.

2.6 Висновки

Для вирішення проблем масивних атак на мобільний за стосунок, а саме на сервер автентифікації збоку хакерів(конкурентів) впровадили систему захисту від компанії Arbor, а саме комплексну систему TMS 2800. Рішення Arbor об'єднує в собі мережеву аналітику і виявлення аномалій з управлінням загрозами операторського класу, щоб допомогти виявити і зупинити об'ємні DDoS-атаки, виснаження стану TCP і DDoS-атаки на рівні додатків. Мережеві пристрої Arbor TMS забезпечують життєво важливий компонент рішення Arbor, що очищає трафік. Arbor TMS може бути розгорнутий в лінію для забезпечення "завжди включеного" захисту. На відміну від інших продуктів, він також підтримує архітектуру пом'якшення наслідків, яка називається "перенаправлення/реінжекція". У цьому режимі тільки потік трафіку, що несе DDoS-атаку, перенаправляється на Arbor TMS за допомогою оновлень маршрутизації, що випускаються рішенням Arbor. Arbor TMS видаляє з цього потоку тільки зловмисний трафік, а легітимний трафік перенаправляє за призначенням.

Це дозволяє єдиній, централізовано розташованій системі Arbor TMS захищати кілька каналів зв'язку і кілька центрів обробки даних. Це призводить до набагато більш ефективного використання засобів пом'якшення наслідків і повністю ненав'язливого захисту. Вбудовані пристрої повинні постійно перевіряти весь трафік на каналах, які вони контролюють. Arbor TMS повинен перевіряти тільки той трафік, який перенаправляється на нього у відповідь на атаку на конкретну ціль.

РОЗДІЛ 3 ЕКОНОМІЧНИЙ РОЗДІЛ

Успішність, як і ефективність будь-кого бізнесу, безпосередньо залежить від збереження і цілісності конфіденційних даних та безперебійної роботи. Збиток від успішної DDoS-атаки насамперед полягає у фінансових і репутаційних витратах: недоотриманому прибутку, розриві контрактів і відтоку користувачів, численних скаргах і рекламаціях клієнтів, хвилі негативу в ЗМІ та соціальних мережах і, як наслідок, падінні популярності інтернет-ресурсу та його власника.

Нерідко DDoS-напад використовується як прикриття для основного шкідливого впливу під час цілеспрямованих атак: тоді як фахівці з інформаційної безпеки концентруються на відбитті DDoS і відновленні працездатності систем, зловмисники посилюють головний вектор атаки - наприклад, зламують сервіс, викрадають конфіденційні дані або встановлюють шкідливі коди.

Для запобігання таких атак та збереження ТС у стабільному стані та працездатності впроваджуються спеціальні системи захисту від DDoS-атак. Тому метою економічного розділу є здійснення відповідних розрахунків, які дозволять встановити економічного ефекту від впровадження та налагодження комплексів засобів захисту серверу мобільного застосунку в мережі.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

До капітальних витрат належать витрати на розробку політики безпеки інформації, які визначаються виходячи з трудомісткості розробки політики безпеки інформації.

Визначення трудомісткості розробки політики безпеки інформації

Трудомісткість розробки політики безпеки інформації визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і

закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

$$t = t_{тз} + t_{в} + t_{а} + t_{вз} + t_{озб} + t_{овр} + t_{д}, \text{ годин,} \quad (3.1)$$

де $t_{тз}$ – тривалість складання технічного завдання на розробку політики безпеки інформації;

$t_{в}$ – тривалість розробки концепції безпеки інформації у організації;

$t_{а}$ – тривалість процесу аналізу ризиків;

$t_{вз}$ – тривалість визначення вимог до заходів, методів та засобів захисту;

$t_{озб}$ – тривалість вибору основних рішень з забезпечення безпеки інформації;

$t_{овр}$ – тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організації;

$t_{д}$ – тривалість документального оформлення політики безпеки.

Визначено, що відповідно до етапів розробки політики безпеки інформації, тривалість операцій склала наступні величини:

$t_{тз}$=24 годин, $t_{в}$=20 годин, $t_{тз}$=40 годин, $t_{вз}$=54 годин, $t_{озб}$=6 годин, $t_{овр}$=6 годин, $t_{д}$=6 годин.

Отже, t=24+20+40+54+6+6+36= 186 годин,

Розрахунок витрат на створення політики безпеки інформації Витрати на розробку політики безпеки інформації Крп складаються з витрат на заробітну плату спеціаліста з інформаційної безпеки Ззп і вартості витрат машинного часу, що необхідний для розробки політики безпеки інформації Змч.

$$К_{рп} = З_{зп} + З_{мч}. \quad (3.2)$$

$$К_{рп} = З_{зп} + З_{мч} = 24000 + 1110,42 = 25110,42 \text{грн.}$$

$$З_{зп} = t\, З_{пр} = 186 * 129 = 24000 \text{ грн.}$$

де t – загальна тривалість розробки політики безпеки, годин;

Зіб – средньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями, грн/годину.

Вартість машинного часу для розробки політики безпеки інформації на ПК визначається за формулою:

$$З_{мч} = t*C_{мч} = 186*5,97 = 1110,42 грн.$$

де $t_д$ – трудомісткість підготовки документації на ПК, годин;

$C_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 0,9 \cdot 3 \cdot 1,64 + \frac{3800 \cdot 0,4}{1920} + \frac{7200 \cdot 0,2}{1920} = 5,97 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо впровадження фаєрволу до мережі мобільного застосунку «Travel Helper», а також рекомендацій та інструкції по безпосередній роботі з інсталяціює вказаного у інструкціях до системи безпеки

Для впровадження DLP системи обрано DeviceLock програмний комплекс, вартість якого складає 105 468 грн. Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають 20% відсотків від первісної вартості програмного забезпечення, тобто 21 000 грн. Також планується придбання додаткових модулей для системи , вартість яких складає 1500грн.

Таким чином, капітальні (фіксовані) витрати на створення політики інформаційної безпеки підприємства складають:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} =$$
$$= 25110,42 + 105\,468 + 1500 + 21000 = 153\,078 грн.$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу,

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки.

3.1.1 Розрахунок поточних витрат

Річні поточні витрати на функціонування системи інформаційної безпеки складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad грн. \qquad (3.3)$$

де $С_{в}$ - вартість відновлення й модернізації системи ($С_{в} = 0$);

$С_{к}$ - витрати на керування системою в цілому;

$С_{ак}$ - витрати, викликані активністю користувачів системи інформаційної безпеки ($С_{ак} = 0$ грн.).

Витрати на керування системою інформаційної безпеки ($С_{к}$) складають:

$$С_{к} = С_{н} + С_{а} + С_{з} + С_{ел} + С_{о} + С_{тос}, \text{ грн.} \qquad (3.4)$$

Витрати на донавчання персоналу (DevOps) визначаються ($С_{н} = 7000$ грн.).

Річні амортизаційні відрахування за обслуговування та додаткову підтримку збоку розробників складає 5000 грн із корисним строком використання 2 роки, за прямолінійним методом нарахування амортизації складуть:

$С_{а} = 5000 / 2 = 2500$ грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}, \text{ грн.} \quad (3.5)$$

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

Основна заробітна плата одного спеціаліста з інформаційної безпеки на місяць складає 8000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Отже,

$$С_з = 8000*12 + 8000*12*0,1= 105600\text{грн.}$$

Ставка ЄСВ для всіх категорій платників з 01.01.2021 р. складає 22%.

$$С_{єв} = 8000*0,22 = 1760 \text{ грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_{ел}$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.}, \quad (3.6)$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=2,3 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 8760 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,68 грн./кВт за годину).

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року:

$С_{ел}$ = 2,3*8760*1,68 = 33 848,64 7418,88 грн.

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос =153 078*0,01=1530.78 грн).

Витрати на керування системою інформаційної безпеки ($С_к$) визначаються:

$$С_к = 7000+2500+105600\text{грн} +1760 +33\ 848,64 + 1530.78 = 152\ 239.42\text{грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 152 239.42грн.

3.2 Оцінка можливого збитку від атаки на вузол або сегмент мережі

3.2.1 Оцінка величини збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

$t_п$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки, 4 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, 6 годин;

$З_о$ – заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 6000 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 8000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 2 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 15 осіб.;

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1млн. грн. у рік;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих сегментів корпоративної мережі, 1;

N – середнє число атак на рік, 50.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить, а також наслідки від втреченої інформації:

$$U = П_п + П_в + V, \quad (3.7)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_П = \frac{\sum Зо}{F} \cdot t_п = \frac{6000 \cdot 9}{165} \cdot 4 = 1309{,}09 \quad \text{грн},$$

де F – місячний фонд робочого часу.

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.8)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн.;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum Зо}{F} \cdot t_{ви} = \frac{6000 \cdot 9}{165} \cdot 6 = 1963{,}63 \text{ грн.}$$

Витрати на відновлення сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{8000 \cdot 1}{165} \cdot 2 = 96{,}96 \text{ грн.}$$

$П_в$ = 1963,63 + 96,96 = 2060,60 грн.

Втрати від зниження очікуваного обсягу прибутків за час простою атакованого вузла або втраченої інформації із средньогодинного обсягу прибутку і сумарного часу простою сегмента корпоративної мережі:

$$V = \frac{O}{Fг} \cdot (t_П + t_В + t_{ВИ})$$

$$V = \frac{1000000}{2080} \cdot (4 + 2 + 6) = 5769{,}23 \text{грн.}$$

де $F_г$ – річний фонд часу роботи філії (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 год.

U =1309,09+ 2060,60 + 5769,23 = 9138,92 грн.

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$B = \sum_i \sum_n U = \sum_1 \sum_{50} 9138{,}92 = 456946 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної:

$$E = B \cdot R - C \text{ грн.,} \qquad (3.9)$$

де B – загальний збиток від атаки у разі перехоплення інформації, тис. грн.;

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (35%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки:

E = 456 946*0,35 – 129 111,98= 30 819,12 грн.

3.3 Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження системи інформаційної безпеки:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,} \qquad (3.10)$$

де E – загальний ефект від впровадження системи інформаційної безпеки грн.;

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{30819,12}{153\,078} = 0.20, \quad \text{частки одиниці,}$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

$$\text{ROSI} > (N_{\text{деп}} - N_{\text{інф}})/100),$$

де $N_{\text{деп}}$ – річна депозитна ставка, (18 %);

$N_{\text{інф}}$ – річний рівень інфляції, (11%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$0,41 > (18 – 11)/100 = 0,2 > 0,07.$$

Термін окупності капітальних інвестицій T_o показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження системи інформаційної безпеки:

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{0,2} = 1.2 \text{,років.}$$

3.4 Висновок

Розробка системи захисту від витоку конфіденційної інформації в комп'ютерній мережі «TravelTeam» є економічно доцільним, оскільки капітальні та експлуатаційні витрати будуть меншими за можливий відвернений збиток. Капітальні витрати складають 153 078 грн., експлуатаційні – 129 111,98грн. Величина річного економічного ефекту складає 30 819,12 грн. Коефіцієнт повернення інвестицій ROSI складає 0,201 грн./грн.

З розрахунків , видно , що впровадження Arbor TMS 2800 системи та його експлуатація , є коштовним в матеріальному плані ресурсі , але необхідним.

ВИСНОВОК

DDOS-атаку дуже складно виявити й запобігти, оскільки "шкідливі" пакети не відрізняються від "легітимних". Мережеві пристрої й традиційні технічні рішення для забезпечення безпеки мережевого периметру, такі як міжмережеві екрани й системи виявлення вторгнень (IDS), є важливими компонентами загальної стратегії мережевої безпеки, однак самі ці пристрої не забезпечують повного захисту від DDOS-атак. Міжмережеві екрани дозволяють або забороняють проходження мережевого трафіку на підставі аналізу різних полів мережевих пакетів. Але DDOS-атака може бути успішно реалізована в рамках дозволених міжмережевим екраном потоків трафіка. Оскільки трафік DDOS-атаки – це звичайні мережеві пакети, кожен з яких окремо собою атаку не представляє, то система IDS не виявить таку атаку. У деяких випадках, при проведенні таких атак використовується підміна IP-адрес джерела, через що стає неможливою ідентифікація шкідливого трафіку від конкретного джерела.

Для боротьби з DDOS-атаками необхідно використовувати комбіновані рішення: на рівні сервера, на рівні сервісів сервера, на рівні мережі, на рівні провайдера, на рівні апаратури, на рівні адміністраторів сервера.

У цій роботі було ознайомлення із такими системами захисту, розібрано основні функції систем Arbor TMS 2800, а також проаналізовано методи аналізу потоків даних. Було обрано та описано 3 найбільш актуальні бренди, які займаються захистом від данних атак для малого та середнього бізнесу , а остаточний вибір був зроблений на користь Arbor TMS 2800. Система була обрана, тому що виконує всі основні функції захисту, які були поставлені в кваліфікаційній роботі та є доцільною з економічної точки зору.

Основною метою було поставлено встановлення моделі загроз та опис потенційного порушника в мережі компанії для аналізу можливих витоків інформації. На основі аналізу інстальована Arbor TMS 2800 система з основними налаштування для корпоративної мережі на сервер для автентифікації клієнтів. Програмний комплекс Arbor TMS 2800 це технічне і програмне рішення для

детального і глибокого мережевого моніторингу, метою якого є виявлення та аналіз загроз.

З економічної точки зору , система є дуже вигідною , за підрахунками може окупити себе майже за 1.2 роки. Оскільки компанія буде активно розвиватись, питання безперебійної роботи є дуже актуальним. Все більше компаній розуміють, що захищатися від DDOS-атак важливо. І краще робити це за допомогою спеціалізованих рішень, які відмінно справляються з таким завданням, запобігаючи фінансові, репутаційні та інші види втрат.

ПЕРЕЛІК ПОСИЛАНЬ

1. SysAdmin Online-Безопасность, SysAdmin Online-Безопасность. Кібребезпека [Електронний ресурс] / SysAdmin Online-Безопасность – Режим доступу до ресурсу: http://sysadminonline.ru/100-zaschita-ot-ddos/

2. unihost. Кібребезпека [Електронний ресурс] / unihost – Режим доступу до ресурсу: https://unihost.com/blog/ru/ddos/..

3.Режим доступу до ресурсу: https://machoster.eu/ddos-protection.html?gclid=EAIaIQobChMInKKe5ev2gIVHQB7Ch0Mnw2LEAAYAiAAEgLNp_D_BwE.

4. Программная Анти-DDOS защита. Недорогой способ отражения большинства DDOS атак // Офіційна сторінка програмного забезпечення ANTIDDOS. – unihost. Кібребезпека [Електронний ресурс] / unihost – Режим доступу до ресурсу: http://antiddos.com.ua.

5. megazakaz. Сайт для купівлі обладнання [Електронний ресурс] / megazakaz – Режим доступу до ресурсу: https://megazakaz.com/ebay/product/373606480804.

6. nashi-resheniy. ddos-ptotection [Електронний ресурс] / nashi-resheniy – Режим доступу до ресурсу: http://allta.com.ua/nashi-resheniya/informacionnaya-bezopasnost/ddos-ptotection.

7. omnilink. sistema-zashhity [Електронний ресурс] / omnilink – Режим доступу до ресурсу: https://omnilink.ua/ru/sistema-zashhity-ot-ddos-atak-arbor-sp-tms/.

8. anti-malware. Кібербезпека [Електронний ресурс] / anti-malware – Режим доступу до ресурсу: https://www.anti-malware/practice/methods/How-to-protect-from-DDoS-correctly#part11.

9. studref. Кібербезпека [Електронний ресурс] / studref – Режим доступу до ресурсу: https://studref.com/319749/zhurnalistika/opyt_vzaimodeystviya_polzovateley_informatsionnyh_sistem#854.10. machoster. Налаштування системи [Електронний ресурс] / machoster – Режим доступу до ресурсу: https://machoster.eu/ddos-

protection.html?gclid=EAIaIQobChMInKKe5ev2-gIVHQB7Ch0Mnw2LEAAYAiAAEgLNp_D_BwE

11. Налаштування системи [Електронний ресурс] / machoster – Режим доступу до ресурсу: https://stormwall.pro/knowledge-base/termin/ddos-protection.

12. radappliances. Джерело [Електронний ресурс] / radappliances – Режим доступу до ресурсу: https://www.radappliances.com.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	1	
4	А4	Вступ	1	
5	А4	1 Розділ	34	
6	А4	2 Розділ	44	
7	А4	3 Розділ	9	
8	А4	Висновки	1	
9	А4	Перелік посилань	1	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx