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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню бакалавра

студента *Тофана Віктора Валерійовича*

академічної групи *125-16-2*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка кластерної системи захисту WEB-серверів від DDoS-атак*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи	д.т.н., проф. Корнієнко В.І			
розділів:				
спеціальний	ст. викл. Саксонов Г.М			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Лізунова Т.Л.			

Дніпро
2020

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня бакалавра

студенту ***Тофану Віктору Валерійовичу*** **академічної групи** ***125-16-2***
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка кластерної системи захисту WEB-серверів від DDoS-атак***

затверджену наказом ректора НТУ «Дніпровська політехніка» від _____ № ____

Розділ	Зміст	Термін виконання
Розділ 1	Проаналізувати загрози, що створюється атаками типу DDoS їх наслідки, методи захисту від атак типу DDoS, а також апаратно-програмне рішення CISCO.	29.03.2020
Розділ 2	Розробити концепцію систем захисту, аналіз існуючих DDoS-атак, розробив схему вирішення завдання комплексного захисту від різних типів DDoS атак, а також створення blacklist-а та Фільтрація пошукових роботів.	24.05.2020
Розділ 3	Розрахувати поточні витрат, капітальні витрат, виконати оцінку можливого збитку, та аналіз показників економічної ефективності системи інформаційної безпеки.	14.06.2020

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

Дата видачі: 08.01.2020р.

Дата подання до екзаменаційної комісії: 15.06.2020р.

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

РЕФЕРАТ

Пояснювальна записка: __с., __рис., __таблиць, __додатків, __джерел;

Мета роботи: Розробка кластерної системи захисту WEB-серверів від DDoS-атак. У першій частині розглянуті загрози, що створюється атаками типу DDoS, методи захисту: маршрутизація в «чорні діри», міжмережеві екрани та системи IDS. Розглянута проблема забезпечення доступності web-ресурсів.

У спеціальній частині проаналізовані існуючі DDoS-атаки та концепція реалізації систем захисту. Запропонована схема вирішення завдання комплексного захисту від різних типів DDoS атак високої інтенсивності та модулювання її у програмному середовищі.

Виконано обґрунтування та вибір обладнання, запропоновані рекомендації щодо налаштування системи захисту.

В економічному розділі виконано аналіз економічної ефективності Web-серверів та її розрахунок.

Практичне значення роботи полягає в підвищенні рівня захисту WEB-серверів від атак типу DDoS.

ЗАХИСТ WEB-СЕРВЕРА, DDoS, КЛАСТЕР, БЕЗПЕКА, МІЖМЕРЕЖЕВІ ЕКРАН, МАРШРУТИЗАТОР, АТАКА, ТРАФІК.

РЕФЕРАТ

Пояснительная записка: __с., __ рис., __таблиц, __приложений, __ источников.

Цель работы: Разработка кластерной системы защиты WEB-серверов от DDoS-атак

В первой части рассмотренные угрозы, которые создаются атаками типа DDoS, методы защиты: маршрутизация в «черные дыры», межсетевые экраны и системы IDS. Рассмотрена проблема обеспечения доступности web-ресурсов.

В специальной части проанализированы существующие DDoS-атаки и концепция реализации систем защиты. Предложена схема решения задания комплексной защиты от разных типов DDoS атак высокой интенсивности и моделирование её в программной среде.

Выполнено обоснование и выбор оборудования, предложены рекомендации по настройке системы защиты.

В экономическом разделе выполнен анализ экономической эффективности Web-серверов и ее расчет

Практическое значение работы заключается в повышении уровня защиты WEB-серверов от атак типа DDoS.

ЗАЩИТА WEB-СЕРВЕРА, DDoS, КЛАСТЕР, БЕЗОПАСНОСТЬ, МЕЖСЕТЕВОЙ ЭКРАН, МАРШРУТИЗАТОР, АТАКА, ТРАФИК

ABSTRACT

Explanatory note: __ p., __ fig., __ tab., __ additions, __ sources.

The purpose of the graduation project: Development of a cluster system for protecting WEB servers from DDoS attacks.

In the first part, the threats that are attacks such as DDoS, methods of protection: routing to the "black hole", firewalls and system IDS. The problem of ensuring the availability of web-resources.

A special part of the analysis of existing DDoS-attacks and the implementation of the concept of protection systems. A scheme for solving the task of comprehensive protection from different types of DDoS attacks, high intensity and modeling it in the software environment.

Completed study and selection of equipment, offered advice on setting up the protection system.

The economic section analyzes the economic efficiency of Web-servers and its calculation.

The practical significance of the work is to improve the protection of WEB servers from attacks such as DDoS.

PROTECTION OF WEB-PAGES, DDoS, CLUSTER, SECURITY, FIREWALL, ROUTER, ATTACK, TRAFFIC.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АС	-	автоматизована система;
ІТ	-	інформаційні технології;
ІТС	-	інформаційно-телекомунікаційна система;
КС	-	комп'ютерна мережа (або система);
НД ТЗІ	-	нормативний документ технічного захисту інформації;
НСД	-	несанкціонований доступ;
ОС	-	операційна система;
ПЗ	-	програмне забезпечення;
ПК	-	персональний комп’ютер;
ТЗ	-	технічне завдання;
ТЗІ	-	технічний захист інформації.

ЗМІСТ

ВСТУП

Атаки з розподіленою відмовою в обслуговуванні (DDoS) – це реальна і зростаюча загроза, з якою стикаються компанії у всьому світі. Ці атаки, невразливі для найпопулярніших на сьогоднішній день інструментів виявлення, здатні швидко виснажити ресурси компанії, вибраної як жертва. Збитки обчислюватимуться тисячами, якщо не мільйонами доларів недоотриманого прибутку і не наданих послуг. Використовуючи нові рішення, спеціально створені для виявлення атак DDoS і боротьби з ними, компанії отримають гарантію спокійної стійкої роботи.

На відміну від атак доступу, які проникають по периметру систем захисту з метою крадіжки інформації, атаки DDoS паралізують Інтернет-системи, наповнюючи сервери, мережеві канали зв'язку і мережеві пристрої (маршрутизатори, міжмережеві екрани і так далі) фальсифікованим трафіком. Спочатку атаки DDoS були знаряддям хакерів, шантажистів і кібертерористів. Атаки DDoS, які нескладно націлити на обмежені ресурси захисту, орієнтовані не лише на конкретні web-сайти або сервери на кордоні мережі. Ці атаки націлені на мережу як таку. На перших етапах розвитку ці атаки були націлені безпосередньо на мережеву інфраструктуру, наприклад, акумулюючи або на центральні маршрутизатори і комутатори, або на сервери систем доменних імен (DNS) в мережах провайдерів. Були потужні атаки DDoS, яка торкнулася серверів DNS, найважливіші системи, що служили “картою” практично для всіх Інтернет-комунікацій.

Зростаюча залежність від ресурсів Інтернет приводить до того, що фінансові і інші наслідки успішних атак DDoS болісно ударяють по провайдерах послуг, компаніях і урядових відомствах. Нові, потужніші інструменти DDoS створюють загрозу ще більш руйнівних атак найближчим часом.

Оскільки DDoS відносяться до тих атак, захиститися від яких найважче, перед всіма компаніями, які залежать від мережі Інтернет, стає

складне завдання - застосовувати проти цих атак дієві і ефективні заходи. Мережеві пристрої і традиційні технології захисту периметру, зокрема, міжмережеві екрани і системи виявлення вторгнень (IDS), хоча і служать важливими складовими стратегії безпеки в цілому, не забезпечують повномасштабний захист від DDoS. Для захисту від сьогоднішніх нападів DDoS, націлених на ресурси Інтернет, потрібна спеціально розроблена архітектура, в якій, зокрема, має бути передбачена можливість виявляти і усувати усе більш складні, витончені і невразливі атаки.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Загрози, що створюється атаками типу DDoS

У атаці DDoS беруть участь сотні або навіть тисячі «зомбі»-ПК, які нападають на один цільовий об'єкт. Цими «зомбі»-ПК ненавмисно стають мільйони незахищених комп'ютерів, які виходять в Інтернет через широкосмугові постійно-активні з'єднання. Підсаджуючи на ці комп'ютери «сплячі» коди, зловмисники дістають можливість швидко створити цілі легіони «зомбі», яким досить лише дати команду на запуск атаки DDoS. Якщо в атаці бере участь чимала кількість «зомбі»-ПК, її масштаби можуть бути колосальними.

1.2 Наслідки атаки DDoS

Успішна атака DDoS викликає найрізноманітніші наслідки: істотно погіршується швидкодія сайтів, що викликає обґрунтовану незадоволеність клієнтів і інших користувачів. Порушуються зобов'язання по договорах обслуговування (Service-level agreements, SLA) і доводиться повертати чималі гроші за ненадані послуги. Недотримані прибутки, падіння продуктивності, зростання витрат на IT, судові витрати - збитки поширюються і зростають. Цифри приголомшуючі. За оцінкою Forrester, IDC, і прогнозам Yankee Group збитки від 24-годинного перерви в роботі для крупної компанії у сфері електронної комерції наближаються до US$30 млн. За даними компанії McAfee, що займається розробкою антивірусного програмного забезпечення, щорічно світова економіка втрачає $ 600 млрд через кіберзлочинців. Ця цифра включає і збиток від DDoS.

GitHub 28 лютого 2018р піддався найпотужнішою DDoS-атаці в історії інтернету, трафік якої на піку досягав 1,35 терабіт в секунду.

Очевидно, що компанії повинні захистити себе від цих руйнівних атак, забезпечивши надійний захист різних уразливих ланок.

Об’єми DDoS-атак кожен рік зростають. Вони стають більш потужними. Раніше вимірювався у мегабайтах, потім в гігабайтах, а зараз в терабайтах.

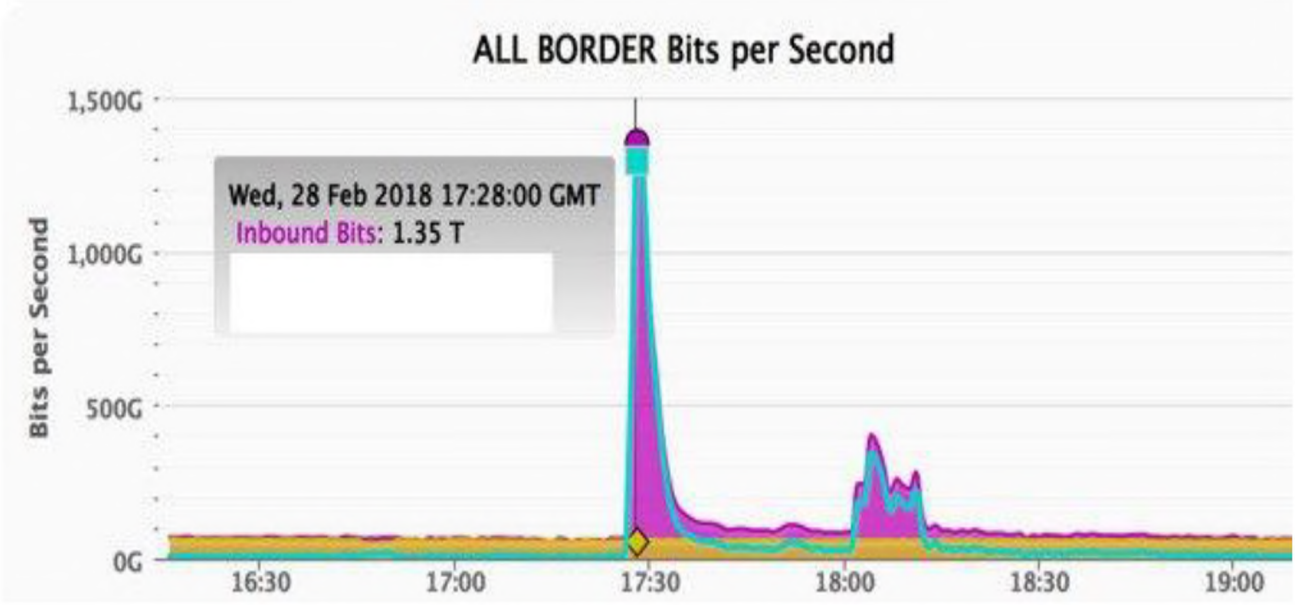

Рисунок 1.1 – Графік трафіку під час атаки

Атака типу DDoS використовує Інтернет-протоколи і дуже вигідну для хакерів можливість доставки пакетів даних через інтернет практично з будь-якого джерела на будь-яку без виключень адресу.

Фактично саме поведінку пакетів визначає суть атаки DDoS: або застосовується величезна кількість пакетів, які переповнюють мережеві пристрої і сервери, або використовуються умисне неповні пакети, які швидко виснажують ресурси сервера. Атакам DDoS дуже складно запобігти, оскільки «зловмисні» пакети невідмітні від «благонадійних», і виявити загрозу непросто: типове зіставлення «сигнатур», що виконується системами IDS, тут не діє. У багатьох атаках даного типа також застосовуються підроблені початкові IP-адреса. Це ускладнює ідентифікацію джерела за допомогою інструментів моніторингу, які діють на базі аномалій і контролюють появу нетипово великих об'ємів трафіку з конкретних джерел.

1.3 Різновиди атак

1.3.1 Атаки із заповненням смуги пропускання.

Ці атаки DDoS виснажують ресурси мережевої смуги пропускання або мережевого устаткування, наповнюючи смугу і/або устаткування великою кількістю пакетів. Вибрані як жертва маршрутизатори, сервери і міжмережеві екрани, кожен з яких має лише обмежені ресурси обробки, під дією атаки можуть стати недоступні для обробки коректних транзакцій або вийти зі строю під великим навантаженням. Найпоширеніша форма атаки із заповненням смуги пропускання - це лавинна атака з відправкою пакетів, при якій велика кількість зовні благонадійних пакетів протоколу TCP, протоколу призначених для користувача датаграм (UDP) або протоколу управління повідомленнями в мережі Інтернет (ICMP), прямує в конкретну ціль. Для того, щоб ще більше ускладнити виявлення такої атаки, зловмисник змінює початкову адресу, тобто імітує IP-адрес, з якого, ймовірно, вчинив запит, щоб зробити ідентифікацію неможливою.

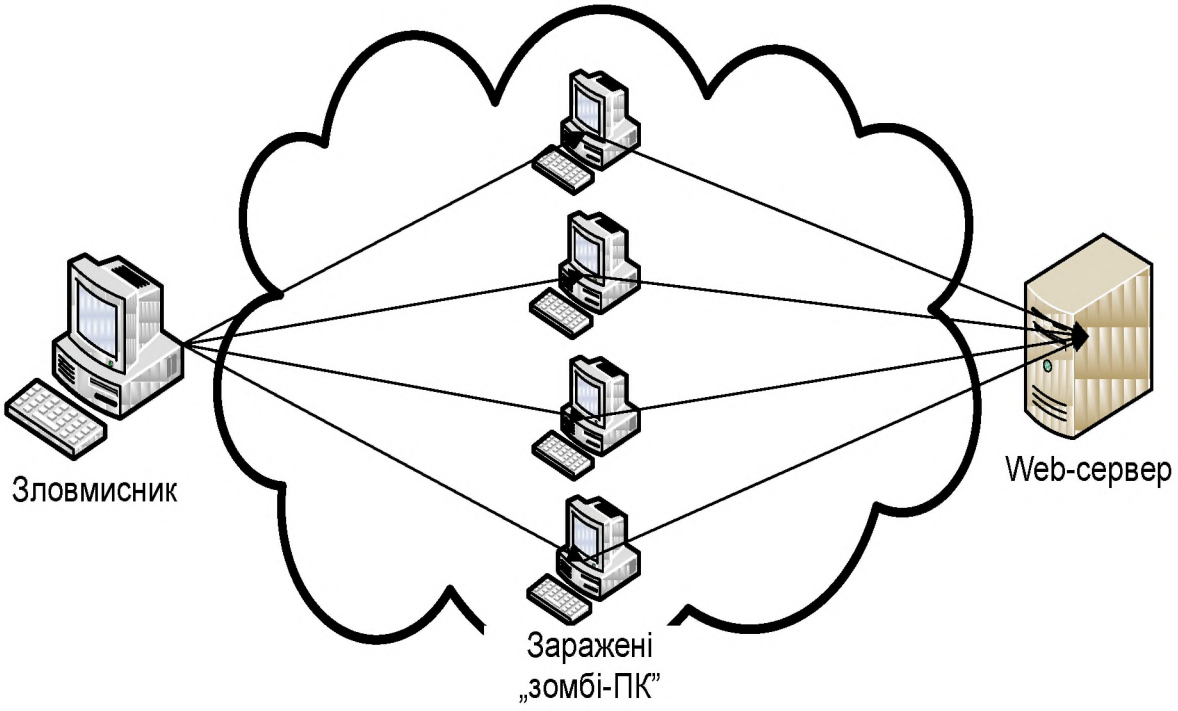

Рисунок 1.2 – Типова схема реалізації DDoS атак

1.3.2 Атаки на додатки

В цих атаках DDoS хакери експлуатують очікувану поведінку протоколів, зокрема, TCP і HTTP. Вони захоплюють обчислювальні ресурси, не даючи їм можливості обробляти транзакції і запити. Приклад атак на додатки: це атаки з напіввідкритими з'єднаннями HTTP і з помилковими з'єднаннями HTTP.

Зловмисники, що застосовують атаки типа DDoS, все ширше використовують витончені прийоми спуфинга і найважливіші протоколи (замість проколів другорядної важливості, які можна заблокувати), завдяки чому атаки DDoS стають ще більш невловимими і руйнівними. Ці атаки, в яких застосовуються коректні дозволені прикладні протоколи і сервіси, дуже важко ідентифікувати і усунути. Вживані заходи фільтрації пакетів або обмеження продуктивності обробки лише спрощують завдання хакера: вони приводять до відключення всіх ресурсів і відмови від обслуговування легітимних користувачів.

1.4 Методи захисту від атак типу DDoS

Незалежно від типу атаки DDoS, ті прийоми боротьби з ними, які застосовуються сьогодні, не забезпечують необхідне усунення загрози і надійну безперервну роботу. Деякі найбільш поширені у відповідь заходи боротьби з атаками DDoS, наприклад, маршрутизація в «чорні діри» і фільтрація на маршрутизаторах, не оптимізовані для боротьби з сьогоднішніми атаками, які стають все більш і більш витонченими. У системах IDS є ряд відмінних ресурсів виявлення атак, проте вони не можуть усунути наслідків атак. Міжмережеві екрани забезпечують захист на рудиментарному рівні, але, подібно до «чорних дір» і фільтрації на маршрутизаторах, вони не призначені для захисту від досконаліших атак, які стають поширеними на сьогоднішній день. Інші стратегії, наприклад, ресурсозабезпечення з резервуванням, не забезпечують достатній захист від атак, масштаби яких постійно зростають, оскільки така стратегія запобігання атакам DDoS виявляється дуже дорогою.

1.4.1 Маршрутизація в «чорні діри»

Процес маршрутизації в «чорні діри» застосовується провайдером послуг для блокування всього трафіку, адресованого на цільовий об'єкт, в як можна ранішній точці. «Знятий з маршруту» трафік маршрутизуеться в «чорну діру» для захисту мережі провайдера і інших його клієнтів. Маршрутизацію в «чорні діри» не можна назвати вдалим рішенням, оскільки разом із зловмисним трафіком атаки відбраковуються і благонадійні пакети. Жертви повністю позбавляються свого трафіку, і хакер святкує перемогу.

Маршрутизатори, на яких застосовуються списки контролю доступу (ACL) для фільтрації «небажаного» трафіку, забезпечують деякий захист від атак DDoS. Дійсно, списки ACL можуть захистити від простих і відомих атак DDoS, наприклад, від ICMP-атак, фільтрація другорядних, невживаних протоколів.

Проте на сьогоднішній день в атаках DDoS, як правило, використовуються коректні протоколи, що діють, які необхідні для присутності в мережі Інтернет, і тому фільтрація протоколів стає менш ефективним засобом захисту. Маршрутизатори також можуть блокувати зони з некоректними IP-адресами, проте зловмисники, щоб їх не виявили, зазвичай підроблюють коректні IP-адреса. В цілому, хоча списки ACL на маршрутизаторах служать першою лінією оборони від базових атак, вони не оптимізовані для захисту від наступних складних атак DDoS:

- SYN, SYN-ACK, FIN і інші лавинні атаки. Списки ACL не можуть

заблокувати атаку SYN з довільним вибором об'єктів спуфінга або атаки ACK і RST на 80-й порт web-сервера, при яких підроблені IP-адреса джерела постійно міняються, оскільки для цього потрібно було б уручну відстежити і ідентифікувати кожне підроблене джерело, а це завдання практично нездійсниме. Єдиний можливий варіант тут полягає в тому, щоб заблокувати весь сервер, а саме в цьому і полягає завдання хакера;

- Proxy. Оскільки списки ACL не можуть відрізнити один від одного «благонадійні» і «зловмисні» SYN, що поступають з одного початкового IP або Proxy, то, намагаючись зупинити сфокусовану атаку із спуфінгом, вони вимушені, за визначенням, блокувати весь трафік клієнтів жертви, що поступає з визначеного початкового IP або Proxy (модуля доступу);

- DNS або протокол прикордонного шлюзу (Border Gateway Protocol, BGP). Коли запускаються атаки з довільним вибором об'єктів спуфінга на сервер DNS або на маршрутизатор BGP, списки ACL, як і у випадку з лавинними атаками SYN, не можуть відстежити швидко змінний об'єм трафіку з довільно вибраними об'єктами спуфінга. Окрім цього, списки ACL не в змозі відрізнити підроблені адреси від коректних;

- Атаки на рівні додатків (клієнтські). Хоча списки ACL теоретично можуть блокувати клієнтські атаки, наприклад, атаки з помилковими з'єднаннями HTTP і з напіввідкритими з'єднаннями HTTP (за умови, що є можливість точно ідентифікувати джерело атаки і конкретні не підроблені джерела), користувачам потрібно буде конфігурувати сотні, а в деяких випадках і тисячі списків ACL для кожної потенційної жертви;

Ще одна стратегія запобігання атакам DDoS на базі маршрутизаторів - вживання одно направленої перевірки передачі по зворотному шляху (Unicast Reverse Path Forwarding, uRPF) для зупинки атак із спуфінгом на зовнішній стороні - як правило, виявляється неефективною в боротьбі з сьогоднішніми атаками DDoS, оскільки основоположний принцип uRPF полягає в тому, щоб блокувати витікаючий трафік, якщо IP-адрес не відноситься до підмережі. Проте, оскільки зловмисники можуть імітувати IP-адреса з тієї ж підмережі, за якою вони ховаються, вони здатні без зусиль обійти цей заслін. Окрім цього, для того, щоб uRPF була дійсно ефективною, її необхідно упровадити перед кожним потенційним джерелом атаки, а реалізувати таку схему на практиці непросто, і навіть практично неможливо.

1.4.2 Міжмережеві екрани

Хоча міжмережеві екрани грають виключно важливу роль в системі безпеки будь-якої компанії, вони не створені саме як інструмент запобігання атакам DDoS. Фактично, у міжмережевих екранів є ряд початкових властивостей, які не дозволяють їм забезпечити повний захист від найвитонченіших сучасних атак DDoS.

Перш за все, йдеться про місця розташування. Міжмережеві екрани знаходяться в дуже віддаленому від розташованого нижче оператора зв'язку на шляху дотримання даних, і це не забезпечує достатній захист каналу доступу, який тягнеться від провайдера до граничного маршрутизатора на периферії корпоративної системи, із-за чого ці компоненти стають уразливою мішенню для атак DDoS. Фактично, оскільки міжмережеві екрани вбудовуються по лінійній схемі, вони часто стають мішенню зловмисників, які намагаються виснажити ресурси обробки сеансів, щоб викликати збій.

Друга проблема - це відсутність механізму виявлення аномалій. Міжмережеві екрани насамперед призначені для контролю доступу в приватні мережі, і вони відмінно справляються з цим завданням. Один з шляхів виконання цього завдання - вистежування сеансів, які ініційовані зсередини (на «чистій» стороні) і адресовані на зовнішній сервіс, і подальший прийом лише особливих відгуків від очікуваних джерел на («брудній») зовнішній стороні. Проте така схема не діє стосовно таких сервісів як Веб, DNS, і до інших сервісів, які мають бути відкриті для спільного доступу, щоб була забезпечена можливість приймати запити. У подібних випадках міжмережеві екрани виконують операцію, яка називається «Відкриттям каналу»: вони пропускають трафік HTTP на IP-адрес web-сервера. Хоча такий підхід і забезпечує деякий захист, оскільки дозволені лише певні протоколи, що адресуються на певні адреси, він не дуже ефективний в боротьбі з атаками DDoS, оскільки хакери можуть без зусиль скористатися «дозволеним» протоколом (в даному випадку HTTP) для перенесення трафіку атаки. Відсутність можливостей для виявлення

аномалій означає, що міжмережеві екрани не можуть розпізнати ситуацію, в якій носієм атаки служать коректні дозволені протоколи.

Третя причина, по якій міжмережеві екрани не можуть забезпечити повнофункціональний захист від атак DDoS, - це відсутність ресурсів боротьби із спуфінгом. Якщо виявлена атака DDoS, міжмережеві екрани можуть заблокувати конкретний потік трафіку, пов'язаний з атакою, але не можуть застосувати міри антиспуфинга на попакетній основі, щоб відокремити хороший, «благонадійний» трафік від поганого, а саме ця операція важлива для захисту від атак, в яких використовується великий об'єм підроблених IP-адресов.

1.4.3 Системи IDS

Хоча системи IDS відмінно можуть виявляти атаки на рівні додатків, у них є і слабка сторона: вони не можуть виявити атаку DDoS, в якій використовуються коректні пакети, а на сьогоднішній день в більшості атак використовуються саме коректні пакети. Хоча в системах IDS передбачені певні механізми, що діють на базі аномалій, які необхідні для виявлення даних атак, потрібне їх масштабне підстроювання уручну, і вони не ідентифікують конкретні потоки трафіку атак.

Інша потенційна проблема систем IDS для захисту від атак DDoS полягає в тому, що вони лише виявляють атаку, але не роблять жодних дій для усунення її наслідків. У рішеннях на базі IDS можуть бути рекомендовані фільтри для маршрутизаторів і міжмережеві екрани, але, як вже було сказано вище, не забезпечується повною мірою ефективне усунення сучасних витончених атак DDoS. Якщо застосовуються системи IDS, необхідне доповнююче рішення по усуненню атаки, яке забезпечило б вищий рівень ідентифікації конкретних потоків трафіку атаки з негайною реалізацією у відповідь заходів.

Загалом, системи IDS - це оптимальний інструмент виявлення атак на рівні додатків на основі сигнатур. Оскільки складні атаки DDoS виявляються по аномальній поведінці на 3-му і 4-му рівнях, сучасна технологія IDS не пристосована для виявлення і усунення атак DDoS.

1.4.4 Реакція на атаки DDoS, що ініціюється в ручний спосіб

Перша реакція жертви на атаку DDoS, як правило, полягає в тому, що він просить найближчого попереднього провайдера послуг з'єднання (це може бути провайдер Інтернет-послуг (ISP), провайдер послуг хостингу або магістральний) спробувати ідентифікувати джерело. Якщо адреси підроблені, цей процес може виявитися довгим і важким, і для його реалізації буде необхідно об'єднати зусилля багатьох провайдерів. Хоча джерело, можливо, і буде ідентифіковане, блокування цього джерела виллється в блокування всього трафіку - і поганого, і хорошого.

Фахівці компаній можуть використовувати для протидії атакам DDoS різні стратегії, зокрема, вживання резервних ресурсів, тобто закупівлю резервної смуги пропускання або резервних мережевих пристроїв, які допоможуть впоратися з будь-яким піковим зростанням попиту. Такий підхід не відрізняється високою рентабельністю, особливо через те, що необхідно вводити резервні мережеві інтерфейси і пристрої. І, незалежно від первинного ефекту, для того, щоб здолати ці додаткові потужності хакерам знадобиться лише збільшити масштаби атаки.

1.4.5 Апаратно-програмне рішення CISCO

Cisco Systems пропонує повнофункціональне рішення по захисту від атак DDoS, засноване на принципах виявлення, переорієнтації, верифікації і пересилки, вживання яких гарантує повний захист. Якщо атака DDoS запущена

проти об'єкту, який знаходиться під захистом вирішення Cisco, діють наступні механізми:

- Виявлення атаки DDoS.
- Перевідправка інформаційного трафіку, адресованого цільовому об'єкту, на пристрої Cisco для обробки.
- Аналіз і фільтрація з відділенням потоків «поганого» трафіку від потоків «хорошого» трафіку. При цьому зловмисний трафік не погіршує швидкодія, і забезпечено виконання легітимних транзакцій.
- Пересилка «хорошого» трафіку забезпечує стійку безперервну роботу.

Рішення Cisco забезпечує повнофункціональний захист від атак DDoS всіх видів, включаючи абсолютно нові різновиди. Активні ресурси усунення дозволяють швидко виявити атаку і відокремити зловмисний трафік від легітимного. Тому вирішення Cisco забезпечує оперативну реакцію на атаки DDoS, швидкість якої вимірюється секундами, а не годинами. Вирішення Cisco можна легко розвернути поряд з важливими маршрутизаторами і комутаторами, його можна масштабувати, завдяки чому усуваються будь-які точки можливого збою і не погіршується швидкодія і надійність існуючих мережевих компонентів. У комплексному вирішенні Cisco дві найважливіші складові - Cisco Traffic Anomaly Detector (TAD) XT і Cisco Guard XT - спільна робота яких забезпечує повнофункціональний захист від атак DDoS практично в будь-якій середі.

Cisco Traffic Anomaly Detector XT - Діючи як система раннього запобігання, Cisco TAD XT виконує поглиблений аналіз навіть найскладніших атак DDoS. Cisco TAD XT веде пасивний моніторинг мережевого трафіку і виявляє будь-які відхилення від «нормальної» або базової поведінки, які вказують на атаку DDoS. Якщо ідентифікована атака, Cisco TAD XT посилає запобігання в Cisco Guard XT і видає докладні звіти і специфічні сигнали тривоги для оперативної реакції на загрозу. Наприклад, Cisco TAD XT може виявити, що інтенсивність пакетів UDP, що поступають з одного IP-источника,

виходить за задані рамки, навіть в тому випадку, якщо сукупні порогові значення не перевищені.

Cisco Guard XT - Cisco Guard XT - це наріжний камінь комплексного вирішення Cisco по захисту від атак DDoS. Це високопродуктивний пристрій для усунення атак DDoS, що розгортається на вищестоящому відрізку маршруту трафіку, в центрі обробки даних ISP або на зовнішньому периметрі крупної компанії, для захисту ресурсів мережі і центру обробки даних. Коли Cisco Guard XT отримує повідомлення про атаку на цільовий об'єкт (від Cisco TAD XT або від іншого захисного пристрою моніторингу, наприклад, від детектора вторгнень або від міжмережевого екрану), трафік, що адресується об'єкту, що атакується, пересилається на пов'язаний з ним модуль (або модулі) Cisco Guard. Потім трафік піддається скрупульозному п'ятиступінчастому аналізу і фільтрації для видалення всього зловмисного трафіку і безперешкодного пропуску «хороших» пакетів. Cisco Guard XT розташовується поряд з маршрутизатором або комутатором в окремому мережевому інтерфейсі, завдяки чому забезпечується захист, що відповідає конкретним потребам і що не впливає на трафік даних інших систем. Залежно від місця розташування, Cisco Guard XT може одночасно забезпечити захист декількох потенційних жертв атаки, в числі яких можуть бути маршрутизатори, web-серверы, DNS-серверы, пропускна спроможність LAN і WAN.

Вирішення нового покоління Cisco Guard XT, що забезпечує захист від атак DDoS, засноване на унікальній архітектурі процесу мульти-верификации, що патентується (Multiverification Process, MVP). Ця архітектура інтегрує різні методи верифікації, аналізу і у відповідь дій, щоб ідентифікувати і відокремлювати зловмисний трафік від благонадійного трафіку.

Цей процес санації складається з п'яти модулів або етапів:

- Фільтрація - В цей модуль включені статичні і динамічні фільтри DDoS. Статичні фільтри, які блокують другорядний трафік, не пропускаючи його до жертви, що атакується, можуть бути конфігуровані користувачем. Cisco поставляє ці фільтри із заздалегідь заданими параметрами, що діють за

умовчанням. Динамічні фільтри вводяться в дію іншими модулями на базі спостережуваної поведінки і докладного аналізу потоків трафіку. При цьому в реальному часі формуються оновлення, які підвищують рівень верифікації, вживаної до підозрілих потоків, або блокують джерела і потоки, які за результатами верифікації визнані зловмисними.

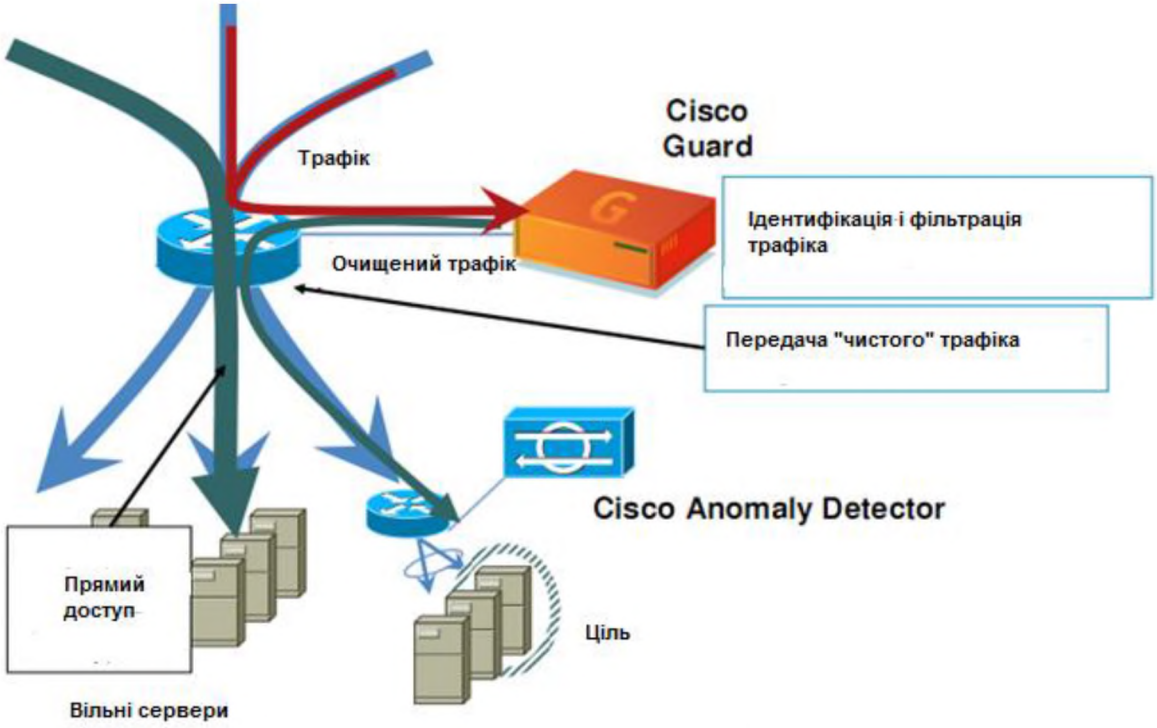

Рисунок 1.3 – Рішення Cisco AntiDDOS

- Активна верифікація - Цей модуль перевіряє на спуфинг всі пакети, що поступають в систему. У Cisco Guard XT застосований цілий ряд унікальних механізмів аутентифікації джерел, які не дозволяють підробленим пакетам дістатися до жертви атаки, що патентуються. Окрім цього, в модулі активної верифікації є ряд механізмів, які допомагають правильно ідентифікувати благонадійний трафік і фактично усувають ризик знищення коректних пакетів.

- Розпізнавання аномалій - Цей модуль виконує моніторинг всього трафіку, який не був зупинений модулями фільтрації і активної верифікації, і зіставляє цей трафік з базовою поведінкою, зафіксованою протягом певного періоду часу. Ведеться контроль за відхиленнями, які вказують на джерело появи зловмисних пакетів. Базовий принцип, на якому заснована робота цього

модуля, такий: закономірності поведінки трафіку, що поступає від джерела, в якому розташувався «таємничий лиходій», істотно відрізняються від закономірностей поведінки благонадійних джерел в режимі нормальної роботи. Цей принцип застосовується для ідентифікації джерела і типа атаки, а також для формування рекомендацій по блокуванню трафіку або проведенню детальнішого аналізу підозрілої інформації.

- Аналіз протоколів - В цьому модулі обробляються ті потоки, які були визнані підозрілими на етапі розпізнавання аномалій. Завдання полягає в ідентифікації атак, пов'язаних з конкретними додатками, наприклад, атак з помилковими з'єднаннями HTTP. Потім виявляються будь-які транзакції по протоколу, в яких є аномалії поведінки, зокрема, неповні транзакції або помилки.

- Нормування - В цьому модулі закладені інші у відповідь заходи. Він не допускає, щоб потоки з аномаліями поведінки наповнювали цільовий об'єкт під час докладнішого моніторингу. Цей модуль формує трафік по кожному конкретному потоку, застосовуючи штрафні санкції до джерел, які споживають надмірний об'єм ресурсів (наприклад, по смузі пропускання або кількості з'єднань) впродовж дуже тривалого періоду.

Поважно відзначити, що в періоди між атаками Cisco Guard XT знаходиться в режимі «навчання», виконує пасивний моніторинг закономірностей поведінки трафіку і потоків, адресованих різним ресурсам, що захищаються. Цим шляхом Cisco Guard XT вивчає нормальну поведінку і формує базовий профіль. Пізніше ця інформація використовується для підстроювання правил політики в цілях розпізнавання і фільтрації відомих і невідомих, таких, що ніколи не зустрічалися раніше атак, при роботі мережі в режимі реального часу.

Безумовно це один з досконаліших продуктів захисту від атак, але дуже дорогий, і застосування його в багатьох випадках не є виправданим.

1.5 Проблема забезпечення доступності web-серверів

В будь-якої компанії, яка працює в онлайновій середі, є ряд причин - економічних і інших - вкладати засоби в захист від атак DDoS. Крупні компанії, урядові відомства і провайдери послуг повинні захищати елементи своєї інфраструктури (web-серверы, сервери DNS, сервери електронної пошти і конференцій, міжмережеві екрани, комутатори і маршрутизатори), щоб забезпечити стійку безперервну роботу і ефективніше використовувати технічний персонал.

Безумовно, впровадження повнофункціонального захисту від атак DDoS пов'язане з певними витратами. Проте прибутковість інвестицій (ROI) у впровадження такої програми захисту незаперечна.

- Електронна комерція. Витрати на захист сайтів електронної комерції від атак DDoS можуть окупитися за лічений години, якщо зіставити їх з розміром потенційних збитків, зв'язаних з атакою DDoS. Об'єми транзакцій на сайті електронної комерції, середня прибутковість однієї транзакції, доходи від реклами, нематеріальні активи, наприклад, репутація торгівельної марки і юридичні зобов'язання, а також трудовитрати технічного персоналу, необхідні для відновлення атакованого сайту, - всі ці чинники необхідно враховувати, оцінюючи фінансові аспекти будь-яких простоїв, що виникають унаслідок атаки DDoS. Слід додати те, що впровадження захисту від атак DDoS, можливо, дозволить перейти на менш дорогі широкосмугові канали зв'язку, і показники ROI стануть ще значнішими.

- Провайдери послуг. Для провайдерів послуг підтримка працездатності власної мережі грає колосальну роль як чинник ROI. Якщо інфраструктура провайдера (маршрутизатори, DNS і інші об'єкти) піддається атаці, виникає збій всіх послуг, що надаються клієнтам, тобто порушення зобов'язань по договорах про обслуговування. Витрати на захист від атак DDoS - це страхування від катастрофічних наслідків, масштаб яких може бути на декілька порядків вище, як в аспекті доходів, так і в аспекті негативної реакції клієнтів.

Проте прагнення захистити себе від збитків - це не єдиний стимул до впровадження повнофункціонального рішення по захисту від атак DDoS для провайдерів послуг хостингу, транзиту і сервісних послуг. Таким користувачам можна запропонувати захист від атак DDoS як коштовний додатковий сервіс, який генерує нові потоки доходів і приносить вигідні конкурентні переваги.

Атаки DDoS набирають силу, і необхідний новий підхід, який дозволить не лише виявляти усе більш витончені і добре замасковані погрози, але і усувати наслідки атаки, забезпечуючи стабільну безперервну роботу компаній і доступність ресурсів.

1.6 Постановка задачі

Зробивши аналіз загроз, створюваних атаками DDoS, та оглянувши методи боротьби з ними, був зроблений висновок, що потрібно створювати повнофункціональну систему захисту від DDoS-атак. Для цього в дипломному проекті були поставлені наступні задачі:

- проаналізувати типи DDoS-атак
- оглянути концепцію реалізацій системи захисту
- запропонувати схему захисту
- змоделювати запропоновану схему
- розробити рекомендації що до вибору обладнання та настройки системи
- визначити та встановити відповідність умов схеми нормам охорони праці;
- розрахувати економічну ефективність впровадженої схеми

1.7 Висновки розділу

Масштаби і руйнівна сила атак DDoS продовжують зростати, оскільки застосовуються усе більш потужні і досяжні інструменти атаки, в мережі

Інтернет багато уразливих точок, і зростає «Інтернет-залежність» компаній. Оскільки збиток від таких атак збільшується, провайдери, компанії і урядові відомства повинні застосовувати у відповідь заходи для захисту своїх інвестицій, доходів і послуг.

З урахуванням особливостей надання доступу до інформації WEB-сторінки, типових характеристик середовищ функціонування та особливостей технологічних процесів оброблення інформації, зазначених у розділі 6, визначаються наступні мінімально необхідні рівні послуг безпеки для забезпечення захисту інформації від загроз:

- за умови, коли WEB-сервер і робочі станції розміщуються на території установи-власника WEB-сторінки або на території оператора (технологія Т1), мінімально необхідний функціональний профіль визначається:

КА-2, ЦА-1, ЦО-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1;

- за умови, коли WEB-сервер розміщується у оператора, а робочі станції – на території власника WEB-сторінки, взаємодія яких з WEB-сервером здійснюється з використанням мереж передачі даних (технологія Т2), мінімально необхідний функціональний профіль визначається:

КА-2, КВ-1, ЦА-1, ЦО-1, ЦВ-1, ДВ-1, ДР-1, НР-2, НИ-2, НК-1, НО-1,НЦ-1, НТ-1, НВ-1.

Встановлені цим НД ТЗІ вимоги є обов'язковими для виконання державними органами, Збройними Силами України, іншими військовими формуваннями, утвореними відповідно до законів України, та органами місцевого самоврядування, а також підприємствами, установами та організаціями (далі - установи) усіх форм власності під час захисту інформації, що є власністю держави, на WEB-сторінках.

Для захисту інших видів інформації власники WEB-сторінок користуються цим НД ТЗІ на власний розсуд.

Для бізнесу потрібне вирішення нового типа, яке доповнило б існуючі рішення по забезпеченню безпеки, зокрема, міжмережеві екрани і системи IDS, і могло не лише виявляти найвитонченіші атаки DDoS, але і блокувати усе

більш витончений і важко вловимий трафік атак без збитку для благонадійних транзакцій. При такому підході потрібна досконаліша, ніж в рішеннях, що існують на сьогоднішній день, перевірка і аналіз трафіку атаки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Аналіз існуючих DDoS-атак

Розподілені атаки на відмову за способом реалізації і об'єкту дії можна поділити на два класи:

– поглинання ресурсів мережі;

– поглинання ресурсів вузла.

Поглинання ресурсів мережі полягає в пересилці великої кількості пакетів в мережу жертви. Вони зменшують її пропускну здатність для законних користувачів. Існує декілька видів таких атак:

– UDP/ICMP flood полягає в пересилці значної кількості великих(фрагментованих) пакетів по протоколам UDP/ICMP;

– Smurf/Fraggle полягає у пересилці пакетів UDP/ICMP ECHO на широкий діапазон адрес з сфальшованою IP адресою. При цьому на адресу жертви приходить велика кількість пакетів-відповідей.

Поглинання ресурсів вузла полягає в пересилці трудоємних або некоректних запитів жертві. До цього вида відносяться наступні атаки:

– TCP SYN - свідоме переривання процесу встановлення з'єднання і створення великої кількості напіввідкритих TCP/IP з'єднань (оскільки це число обмежене, то вузол перестає приймати запити на з'єднання);

– Land - пересилка пакету TCP SYN з однаковими адресами одержувача і джерела та портами (при посилці таких пакетів вузол з Windows NT зависає);

– Ping of Death - посилка пакету «ping» дуже великої довжини, який ОС не може обробити;

– Пересилка некоректних пакетів при обробці яких на вузлі можуть виникнути помилки;

– Пересилка трудоємних запитів для завантаження вузла.

Необхідно проаналізувати, найбільш важливі з точки зору побудови системи захисту, які достатньо повно характеризують атаку на відмову.

Тип атаки. Проаналізуємо атаки двох типів: просту (коли атака йде з однієї машини) та розподілену (коли використовуються машини-агенти).

Напрям атаки - визначає конкретну частину інфраструктури мережі, яка зазнає атаки. Виділимо дві частини: ресурси мережі (тобто пропускних каналів) та ресурси цілі (тобто ресурси конкретного комп'ютера) [4].

Схема атаки - визначає план здійснення атаки, тобто доставки атакуючим зловмисного трафіка жертві. Може бути прямою (пересилка трафіка з одного або багатьох машин), віддзеркаленою (пересилка трафіка через третіх осіб) або прихованою (зловмисний трафік ховається в «законному») [6].

Спосіб атаки - визначає які вразливості використовуються при здійсненні атаки. Виділимо такі способи атаки: спрямована, яка використовує недоліки конкретних прикладних програмних систем, служб, протоколів, поглинаюча, яка намагається завантажити всі ресурси системи або мережі, експлойтна, яка використовує вразливості програмних систем [7].

У роботі [8] авторами описана класифікація існуючих типів атак у розрізі цих аспектів.

Системи, що підлягають захисту

Для успішного функціонування системи захисту від атак на відмову надзвичайно важливо виділити множину припущень про систему, яка підлягає захисту. Очевидно, що захист систем різного типу має бути побудований на основі різних принципів, що ґрунтуються на типових характеристиках, класах атак, що спрямовані проти систем даного типу, вимог до функціонування системи захисту. Як правило, ці припущення стосуються нормальної роботи системи, що підлягає захисту. Виділення таких емпіричних характеристик суттєво полегшує виявлення атаки при умові збереження їх відповідності реальному стану системи.

Існує також декілька базових припущень, які використовуються в усіх системах захисту. Перше з них полягає в тому, що атаки взаємопов'язані з незвичним використанням системи і тому їх дія суттєво відрізняється від типової роботи. Тобто вважається, що атаки супроводжуються аномальною

поведінкою системи, яку легко можна відрізнити від звичайної. У роботі [9] здійснена спроба узагальнити і описати існуючі припущення, на основі яких функціонує більшість систем виявлення. Можна виділити декілька ключових припущень, які лягли в основу багатьох систем виявлення, це:

– користувачі створюють приблизно однакову кількість трафіку [10];

– кількість пакетів в одиницю часу (загально або тільки по окремим протоколам) при звичайній роботі представляє собою статистично однорідну послідовність (тобто його характеристики залишаються сталими протягом часу) [11, 12];

– кількість постійних, легітимних користувачів протягом достатньо довгого періоду часу залишається сталою або поступово змінюється [10, 13];

– при атаці на відмову відбувається суттєва зміна статистичних характеристик роботи системи [14].

Також неявно припускається, що:

– атаки на відмову є аномальним використанням системи;

– атаки на відмову є рідкісною, надзвичайною ситуацією;

– аномалії шкодять функціонуванню системи;

– визначення аномальної поведінки не залежить від мережі. (аномалії є універсальними, або залежать тільки від протоколу взаємодії);

– адміністратори можуть адекватно інтерпретувати аномальні явища, що виникають при функціонуванні мережі.

Виділяють наступні типи систем, що можуть бути ціллю атаки:

– окремий сервіс;

– окремий вузол (поштовий або файловий сервер);

– мережа;

– ad-hoc мережа (динамічна мережа);

– інфраструктура мережі Інтернет.

Для кожної з них система захисту має враховувати окремі припущення і бути налаштована на різні типи атак. Зупинимось коротко на кожному з цих типів.

Окремий сервіс. Кожен вузол мережі забезпечує роботу декількох сервісів, кожний з яких, як правило, пов'язаний з окремою прикладною програмою. Атака може бути спрямована на особливості або вразливості реалізації такого сервісу. Це може заблокувати доступ користувачів до сервісу, хоча робота всього комп'ютера не буде зупинена. Атаки такого типу складно виявляти оскільки зміни в роботі всієї системи можуть бути незначними.

Окремий вузол. Атаки на вузол спрямовані на механізми, що забезпечують його зв'язок з мережею. Це можуть бути атаки, пов'язані з TCP/IP, UDP або іншими протоколами мережі. При такій атаці часто змінюються статистичні характеристики трафіка. Також часто виконується припущення про приблизно однакову кількість трафіка кожного користувача.

Мережа. Атаки, що спрямовані на мережу намагаються заповнити її пропускну здатність фальшивими пакетами. В разі успіху весь зв'язок користувачів з системою, яку атакують буде перерваний. При нормальній роботі мережі статистичні характеристики трафіка змінюються повільно, кількість користувачів часто залишається сталою (це залежить від природи послуг, що надаються). Тому для виявлення атак існують досить розвинені методи. Більш складною задачею є відділення атакуючих пакетів від пакетів користувачів. Для повного її розв'язання потрібне широке запровадження системи маркування пакетів, що дозволить протидіяти спуфінгу IP адрес.

Ad hoc мережа. Ці мережі набули поширення порівняно недавно. Як правило, це безпровідні мережі, що дозволяють підключитись користувачам з будь-якого місця. Вони характеризуються високою динамічністю трафіка і кількості користувачів. Одним з прикладів можуть слугувати пірингові мережі, що набули широкої популярності і використовуються для розповсюдження музики, фільмів або програм мережами. Атаки на такі мережі (або з

використанням таких мереж) мають ряд особливостей і досить складні для виявлення.

Інфраструктура мережі Інтернет. Атаки на інфраструктуру намагаються вивести з ладу сервіси і компоненти, функціонування яких критичне для роботи мережі Інтернет. У разі успішності такої атаки наслідки можуть бути катастрофічні для всієї мережі. На сьогоднішній момент DNS сервери добре забезпечені додатковими ресурсами і можуть протистояти практично будь-якій атаці, однак спроби нападу регулярно відбуваються з року в рік.

2.2 Концепція систем захисту

2.2.1 Загальна концепція побудови та реалізації системи захисту

Розвиток систем захисту від атак на відмову відбувався у відповідь на існуючі загрози. Спочатку це були прості індикатори, що фіксували, наприклад, кількість байт в секунду або кількість відкритих з'єднань. З появою більш складних типів атак відповідно ускладнювали механізми захисту. При цьому відбувалось залучення математичних моделей з області статистики, нейронних мереж, імітаційного моделювання та інших.

Сучасні системи виявлення атак – це системи прийняття рішення в умовах невизначеності інформації, динамічних змін середовища та можливих загроз. Для визначення аномальних явищ у таких системах використовуються складні математичні алгоритми та спеціально побудовані бази знань. Однак існуючі системи захисту через вищезазначені причини не можуть забезпечити достатній рівень виявлення і протидії атакам на відмову.

Для ефективної протидії атакам на відмову в сучасних мережах система захисту має задовольняти таким вимогам:

– Адаптивність. Вимоги до безпеки в організаціях можуть бути різними або змінюватися з часом. Тому при зміні параметрів та настройок системи її функціональність має змінюватись відповідно.

– Гнучкість. Мережа, за якою ведеться спостереження, може змінюватися протягом часу. Це може бути спричинене появою додаткових можливостей або ресурсів. Отже, система захисту повинна мати можливість змінювати свою функціональність без перезапуску - в режимі он-лайн. Агентні системи можуть забезпечити необхідну гнучкість шляхом встановлення цілей для кожного агента. При змінах відбувається зміна цілей, що не призводить до перезапуску.

– Навчання. Фундаментальна характеристика, що дозволяє виявляти нові атаки. З огляду атак видно, що сценарії атак постійно змінюються, знаходять нові вразливості або схеми здійснення. Пропонується здійснювати навчання двома способами. Перший полягає в заданні адміністратором нових цілей для інтелектуальних агентів. Іншим способом є самонавчання агентів, та використання методів інтелектуальної обробки інформації (видобування знань, статистичних моделей, нейронних мереж тощо).

– Розподільність. Одною з властивостей мережі є взаємо зв'язаність її компонентів. Для успішної роботи потрібна чітка взаємодія всіх складових елементів (маршрутизаторів, файлових серверів, окремих комп'ютерів). Нападнику достатньо здійснити атаку проти однієї з цих ланок, щоб вся мережа або її частина стала враженою. Наприклад, він може завантажити мережу фальшивими ICMP запитами від імені третіх осіб. Або спрямувати атаку проти провайдера, що надає Інтернет послуги. Тому система виявлення атаки, побудована на базі кінцевого комп'ютера може виявитись неефективною. Більш результативним уявляється проведення розподіленого моніторингу з різних точок мережі.

– Автономність. Для спрощення задачі виявлення атак необхідно виконати розподілення обчислювальних задач за різними вузлами. При цьому значно скоротиться час реагування, але слід також створити систему обміну інформацією, яка б дозволила доповнювати виміри вузла даними з інших місць. Інший аспект, пов'язаний з автономністю - це функція делегування. Динаміка процесів в комп'ютерних мережах часто вимагає у відповідь на початок атаки

негайне застосування змін у настройках безпеки. Наприклад, чим раніше будуть увімкнені фільтри виявлених фальшованих адрес, тим менша буде потужність атаки. Тому делегування елементам системи виявлення певних функцій адміністрування системи дозволить значно скоротити час реакції та загальну ефективність системи захисту.

Базою для створення такої системи пропонується технологія інтелектуальних агентів, що використовують методи статистичного аналізу та теорії ігор. Підхід інтелектуальних систем для розв'язання складних проблем, зокрема, в області керування комп'ютерними мережами описаний і обґрунтований в багатьох роботах, наприклад, [23, 24]. Багато агентні системи являються більш мобільними, крім того вони мають додаткові особливості, такі як, наприклад, розподіленість, можливість працювати в умовах непередбачуваних змін як мережі так і зловмисної діяльності, виявлення і документування значимих подій, навчання, аналіз зібраної інформації, планування дій, автономність, адаптивність.

2.2.2 Архітектура систем захисту від DDoS-атак

Як уже зазначалось, існуючі системи виявлення принципово можна розділити на системи виявлення аномалій і системи виявлення особливостей. Основний недолік систем виявлення особливостей полягає у тому, що вони розроблені для виявлення конкретних типів атак (як правило найбільш небезпечних на час створення системи). При появі нових атак або зміні характеристик трафіка задачу виявлення необхідно фактично розв'язувати заново. Системи виявлення аномалій (в силу складності моделювання нормального Інтернет трафіка) використовують різні припущення про функціонування системи, таких як, наприклад, статистична однорідність трафіка. При цьому групи комп'ютерних систем, для яких ці припущення мають місце або умови їх виконання не обговорюються. В результаті незначні

зміни в структурі трафіка або послуг, що надаються можуть призвести до необхідності нового навчання алгоритму виявлення.

Одним з можливих розв'язків такої ситуації є використання до побудови системи захисту від атак на відмову комплексного підходу, що включає в себе моніторинг функціонування системи, збереження історії транзакцій, ведення спеціального сховища для інтелектуального аналізу активності нападників та їх дій, прийняття рішення щодо вибору стратегії протидії. Пропонується будувати систему захисту на основі наступних елементів:

– агенти стеження;

– агенти попередньої обробки і зберігання;

– сховище для зберігання інформації про транзакції, що описують функціонування системи;

– сховище з аналітичними компонентами для виявлення загроз та ознак здійснення зловмисної активності;

– агенти протидії атакам.

Важливим елементом побудови такої системи є визначення відповідного математичного забезпечення для кожного етапу роботи:

– Стеження за трафіком. Перехват пакетів з метою оцінки завантаження, складу трафіка, активності користувачів. Для здійснення цієї задачі необхідно розробити алгоритми визначення кількості і частоти перехоплення пакетів в залежності від завантаження каналу й інших параметрів. Якщо пакети будуть перехоплюватися занадто часто це може призвести до вповільнення трафіку. Якщо ж пакети будуть перехоплюватися через певні постійні проміжки часу це може створити «сліпі зони», про які не буде відомостей.

– Попередня обробка захоплених пакетів, оцінка найбільш небезпечних загроз, збереження інформації у сховищі. Оскільки на цьому етапі необхідна швидка оцінка з мінімальними затратами ресурсів, доцільно використовувати прості й адаптивні порогові значення або (за необхідності) послідовний CUSUM (перевірка процесу на відхільність) .

– Аналіз даних при завантаженні у сховище, виявлення атак, оцінка загроз. Після запису інформації в сховище можна провести комплексну оцінку й обчислити можливі загрози. Для цього доцільно використовувати вищеописані багатоканальні алгоритми CUSUM та сковзне середнє.

– Фоновий аналіз даних для встановлення спроб сканування, атак погіршення якості, пульсуючих атак. Здійснюється постійно або за розкладом. Оскільки ці атаки представляють меншу загрозу, то є час для більш детального їх аналізу. Використовуються методи Data Mining, системи інтелектуальних правил, нейронні мережі тощо.

– Прийняття рішення про виявлення атаки. При перевищенні певних порогових значень на одному з попередніх етапів формується признак про можливу загрозу атаки. В цьому випадку має бути створена експертна система, яка б могла оцінити рівень загрози та прийняти рішення про здійснення атаки.

– Оцінка загрози, вибір моделі, її верифікація, пошук стратегії. Виявлення атаки відразу ставить питання про визначення протидії. У залежності від типу і навіть особливостей конкретної атаки така протидія може значно змінюватися. Тобто можна говорити про «стратегію» протидії. У залежності від умов якості протидії, наприклад, якість обслуговування зареєстрованих користувачів, буде змінюватися стратегія. База можливих стратегій має утворюватися за результатами аналітичного моделювання взаємодії між нападниками та агентами захисту. Дослідження аналітичних моделей дозволяє вивчити ефективність протидії та можливі наслідки. Ігрова постановка тут випливає з самої природи конфліктної взаємодії нападника та системи захисту, а основна величина, на яку впливають гравці - завантаженість системи. Це може бути загальна завантаженість або завантаженість окремих, критичних для роботи системи, вузлів (процесора, оперативної пам'яті, каналів мережі).

Для формування стратегії протидії необхідно спочатку оцінити параметри динамічної моделі, в рамках якої відбувається протиборство. В цей процес входить:

– Визначення типу динаміки;

– Оцінка кількості і потужності нападників;

– Оцінка рівня загрози;

– Визначення можливої протидії та прогнозування наслідків;

– Застосування протидії та порівняння наслідників з передбаченням.

Після застосування стратегії захисту система має оцінювати ефективність стратегії, вимірюючи загрозу. Якщо атака продовжується, необхідно переглянути стратегію.

Повнофункціональний захист від атак DDoS будується на принципах:

– Усунення, а не лише придушення;

– Точне розмежування благонадійного трафіку і зловмисного трафіку, яке дозволяє не лише виявити присутність атаки, але і забезпечити стійку роботу без переривання ділової активності;

– Особливі функціональні характеристики і архітектура, що розгортається на попередньому відрізку маршруту трафіку для захисту всіх уразливих точок.

Оборонні характеристики системи захисту від атак DDoS збудовані на цих принципах:

– Миттєвий відгук на атаки DDoS із застосуванням вбудованих механізмів виявлення і блокування, навіть в разі атаки із спуфингом, коли відбувається безперервна зміна ідентифікаційних параметрів і профілів хакерів;

– Повніші ресурси верифікації в порівнянні з ресурсами, що існують на сьогоднішній день, статичних фільтрів маршрутизаторів і сигнатур IDS;

– Розпізнавання аномалій на базі поведінки дозволяє виявляти зовні коректні пакети, які відправлені із злим наміром, для переповнювання сервісних ресурсів;

– Ідентифікація і блокування конкретних підроблених пакетів для захисту благонадійних коректних трансакцій;

– Механізми, призначені для обробки великомасштабних атак DDoS без збитку для захищених ресурсів;

– Розгортання, відповідно до потреб для захисту мережі під час атак без виникнення збоїв, і додаткових витрат на лінійно-вбудовуванні рішення.

– Обробка (з вбудованою інтелектуальною логікою) лише забруднених потоків трафіку, що забезпечує максимальну надійність і мінімальні витрати на масштабування;

– Усунення залежності від ресурсів мережевих пристроїв і від конфігураційних змін;

– Вживання стандартних протоколів для всіх комунікацій допомагає забезпечити максимальну взаємодію і надійність.

2.3 Схема вирішення завдання комплексного захисту від різних типів DDoS атак високої інтенсивності

Проаналізуємо найбільш універсальну схему захисту. Схема ґрунтується на відділенні системи захисту (фронтенда) від сервера додатків (бэкенда).

Основні види атак типу DDoS, від яких захищає запропонована схема:

– атака, направлена на переповнювання ресурсів каналу в інтернет;

– атака, направлена на перевищення максимальної кількості одночасних з'єднань сервера (SYN флуд);

– атака, направлена на вичерпання процесорних потужностей сервера (частий запит сторінок - HTTP флуд).

Рішення повинне забезпечувати захист від кожного типа атаки.

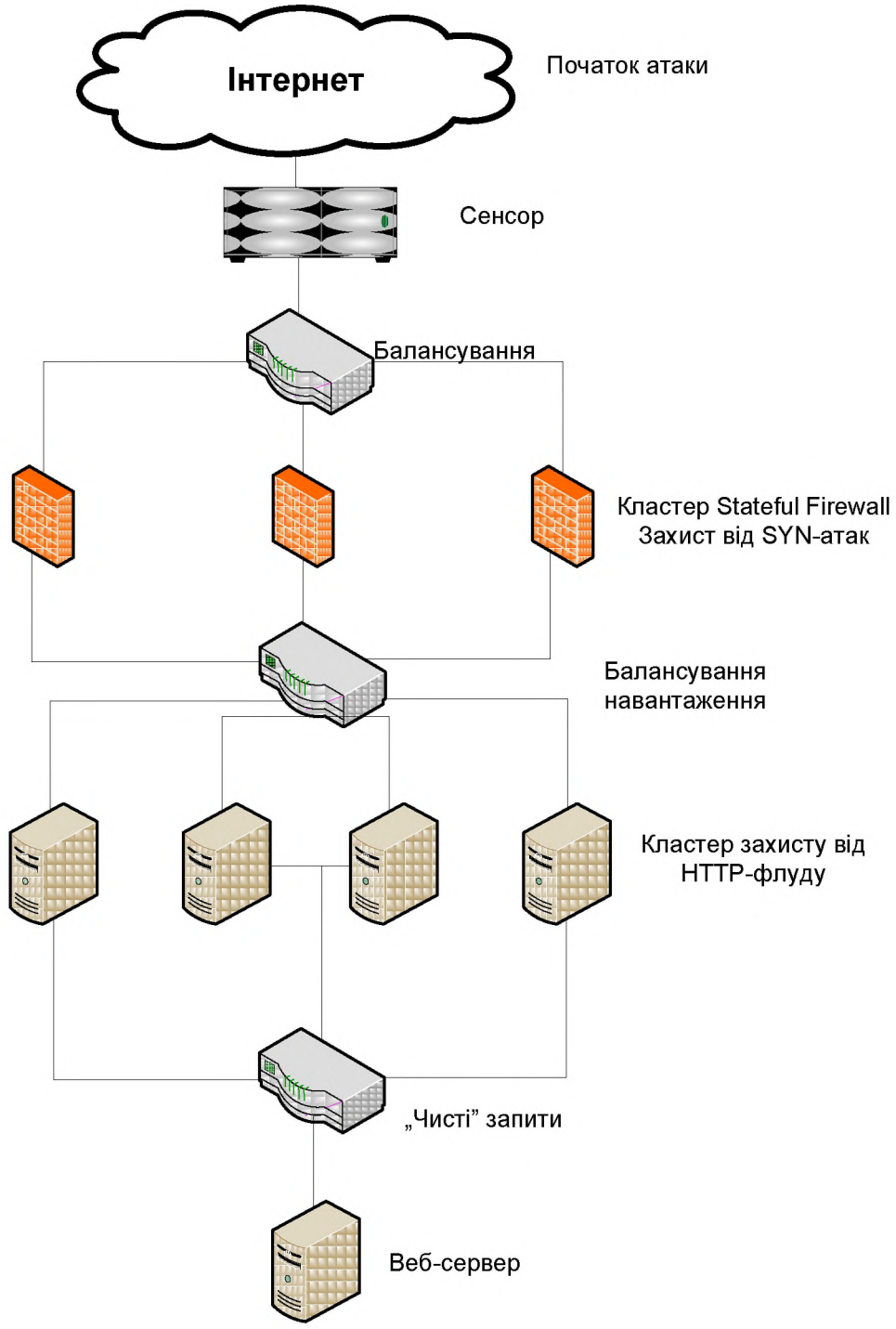

Рисунок 2.1 – Розроблена схема кластерного захисту

2.3.1 Мережевий флуд

На сьогоднішній день найбільш ефективним засобом боротьби із звичайним мережевим флудом є підвищення пропускної спроможності каналу зв'язку. Каналу в 10Gbps досить для захисту від більшості атак цього типа.

Для того, щоб зайвий раз не навантажувати устаткування під час такої атаки, відсіваємо зайві пакети на наші адреси. Наприклад, сервіс, що захищається нами, працює на 80-му порту TCP. У такому разі пакети з destination port відмінним від 80 можна сміливо фільтрувати.

Додатково, необхідно мати резервний канал канал, шириною не менш ніж 1Gbps.

2.3.2 SYN-флуд

Найбільш ефективною схемою захисту від SYN флуда є використання statefull міжмережевих екранів (SFFW).

Залежно від передбачуваної потужності атаки підбирається потрібна кількість міжмережевих екранів. На маршрутизаторі, що стоїть на вході нашого захисту, створюється маршрут мережі (на схемі це 2.1.1.0/24), що захищається нами, з next-hop адресою кожного SFFW.

Кожен SFFW має статичний маршрут мережі 1.1.1.0 на наступний маршрутизатор. На ньому балансується навантаження між нодами останнього рівня захисту, що являють собою сервера з UNIX системою.

В даному випадку зручно використовувати протокол динамічної маршрутизації BGP (при виході зі строю однієї ноды, навантаження автоматично розподілиться між робочими нодами). Таким чином, кожен сервер анонсує маршрутизатору маршрут до мережі 1.1.1.0 з next-hop self.

2.3.3 HTTP-флуд

Пакети, що дійшли до даного рівня захисту, потрапляють на реверс-

proxy. Це має бути proxy-сервер, здатний відрізнити бота від справжнього клієнта. Наприклад, nginx з аналізатором логів, кількості одночасних з'єднань з однієї адреси.

На proxy-серверах набудовується policy based routing як показано в прикладі. Це позбавить запити на бэкенд від вторинного проходження через statefull firewall.

Адреса, на яку приходять запити від фронтенда, повинна відрізнятися від адреси, через яку здійснюється управління сервером. В разі засвічування management адреси (наприклад, прикладною програмою), завжди можна викинути management адресу в «чорну діру» і це не вплине на роботу додатка.

При вирішуванні реальних задач захисту, звичайно немає необхідності у використанні такої кількості маршрутизаторів як показано на схемі. Замість цього раціональніше використовувати один пристрій як маршрутизатор з декількома таблицями маршрутизації (VRF, routing instances) або декількома логічними маршрутами.

Апаратні stateful між мережеві екрани також можна виключити з даної схеми, а замість них на proxy-серверах використовувати PF в режимі SYN Proxy (PF в цьому режимі показує якнайкращу продуктивність на рідній OPENBSD, в разі використання ОС Linux краще взагалі відмовитися від PF, і просто виконати налаштування sysctl потрібним чином). Проте, кількість серверів в цьому випадку доведеться збільшити.

2.3.4 Пошта

Вхідну пошту найвигідніше направити на MX сервера глобальних провайдерів послуг (наприклад, google.com) можливість атак яких дуже невисока, а потім забирати за допомогою fetchmail назад на сервер. DNS теж краще всього тримати на сервісах крупних реєстраторів, що надають досить відмово стійкі кластера як NS для куплених доменів.

Технологія BGP вибрана з тієї причини, що коли один з proxy стане недоступним, на нього перестануть поступати запити. BGP в даному випадку використовується лише усередині кластера і може бути побудований на сірих адресах і сірих ASN.

Проксі не можна поставити просто за міжмережевим екраном, оскільки він зазвичай не уміє балансувати (за допомогою Per Packet Load Balancing), необхідний для балансування. Грубо кажучи, на всіх серверах є одна і та ж адреса, саме на цю адресу і направлений домен, що атакується, а якщо не використовувати балансування, то можуть рватися TCP сесії (та і розділення запитів буде нерівномірним).

Балансування потрібне лише для того, щоб рівномірно розподілити запити proxy, оскільки при серйозній атаці навіть найпотужніший сервер не впорається.

Один 8-ядерний Xeon 55-ої серії тримає, в середньому, 30 000 GET запитів в секунду.

Також використовується сенсор

2.4 Перевірка ефективності пропонованої схеми

При побудові системи захисту від DDoS-атак важливо попередньо протестувати поведінку системи захисту при проведенні масованих розподільних атак.

На цьому етапі необхідно:

- побудувати модель;
- провести тестування моделі;
- проаналізувати результати.

В якості середовища для модулювання був обран програмний пакет Opnet Modeler 14.0 edu.

Opnet Modeler – програмний пакет для проектування та симулювання локальних та глобальних мереж, комп'ютерних систем та розподілених мереж. Він використовується провідними компаніями та світовими виробниками мережевого обладнання при розробці мережевих пристроїв та технології .

Для оцінки запропонованого рішення необхідно виконати наступні етапи:

- побудувати модель;

- змоделювати найбільш вірогідні типи DDoS атак;
- проаналізувати отримані результати;
- зробити висновок про ефективність запропонованої схеми.

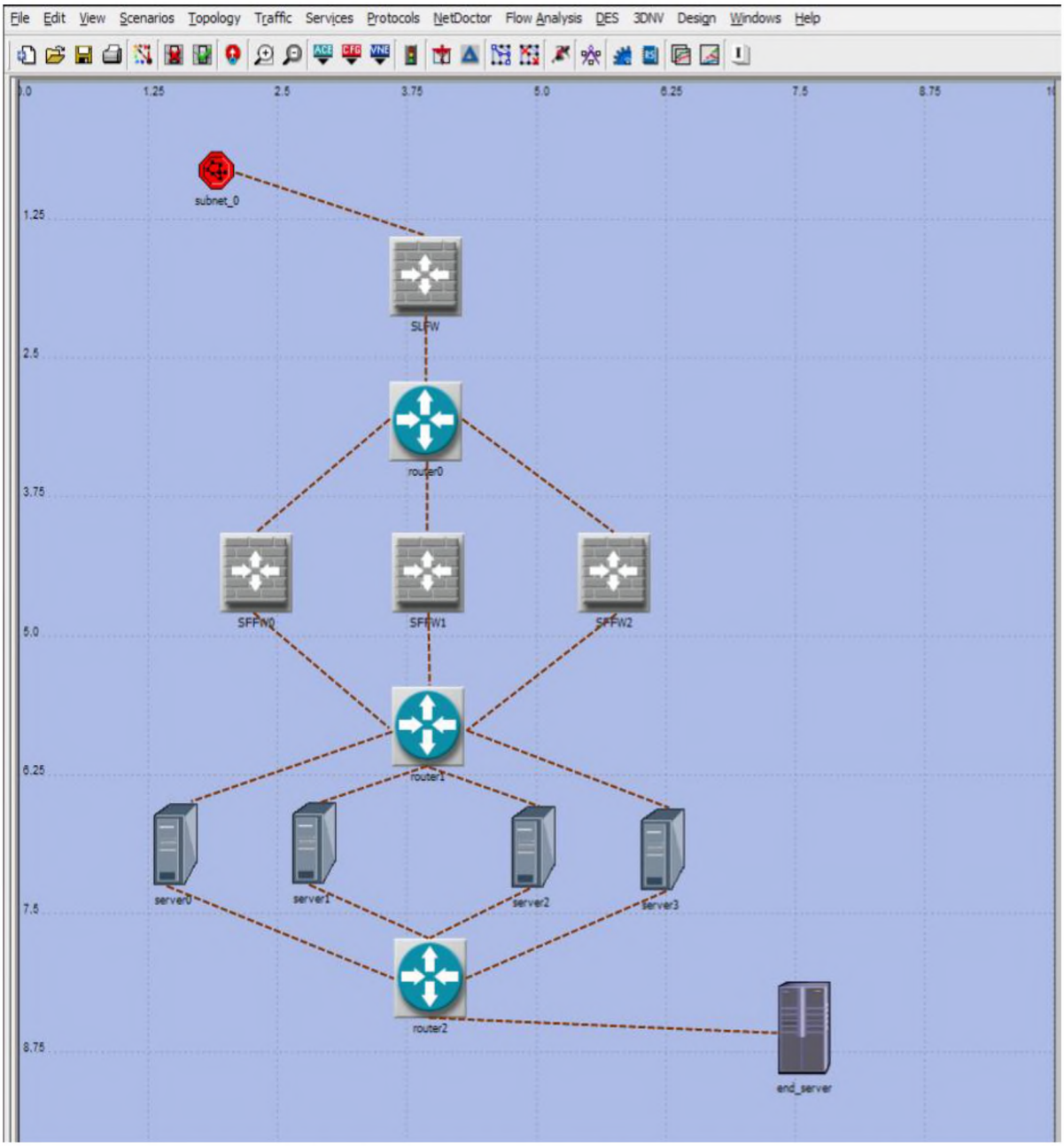

Рисунок 2.2 – Змодельована кластерна схема захисту

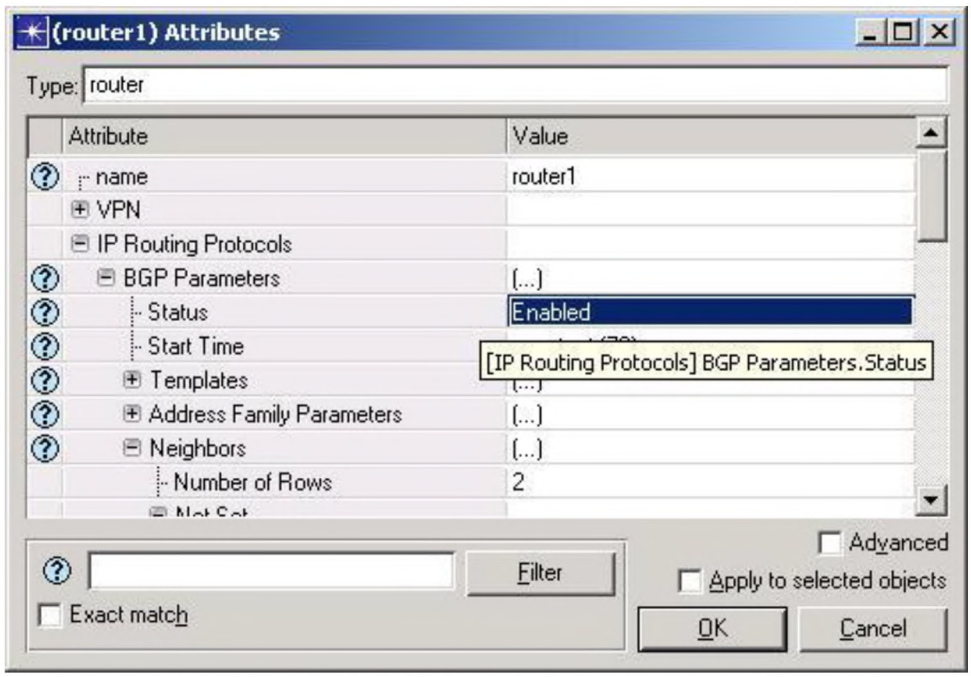

Рисунок 2.3 – Налаштування BGP маршрутизації

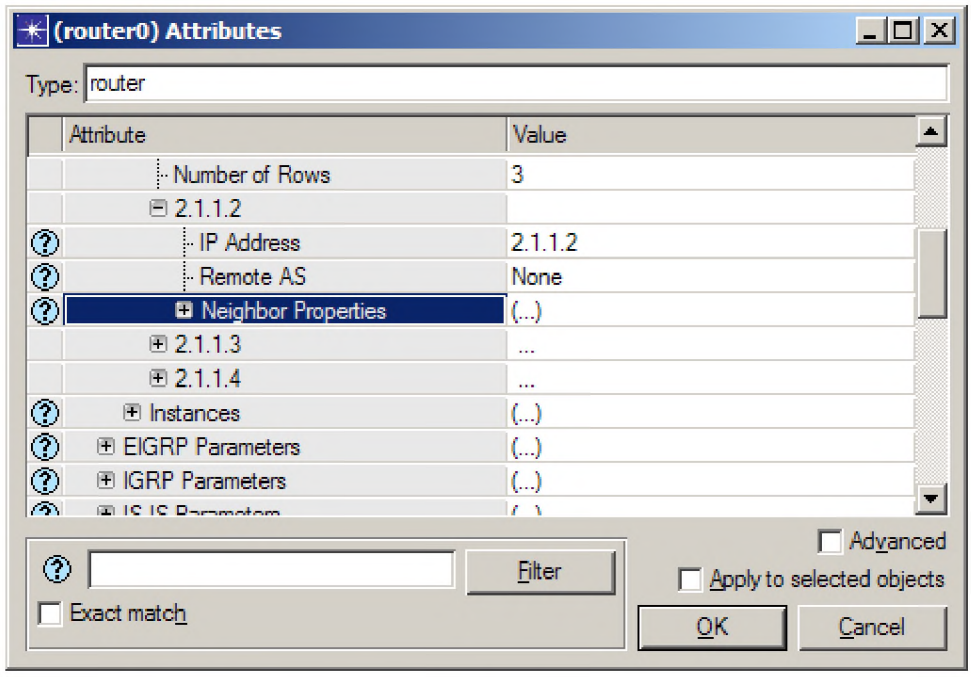

Рисунок 2.4 – Налаштування маршруту мережі на кластер SFFW

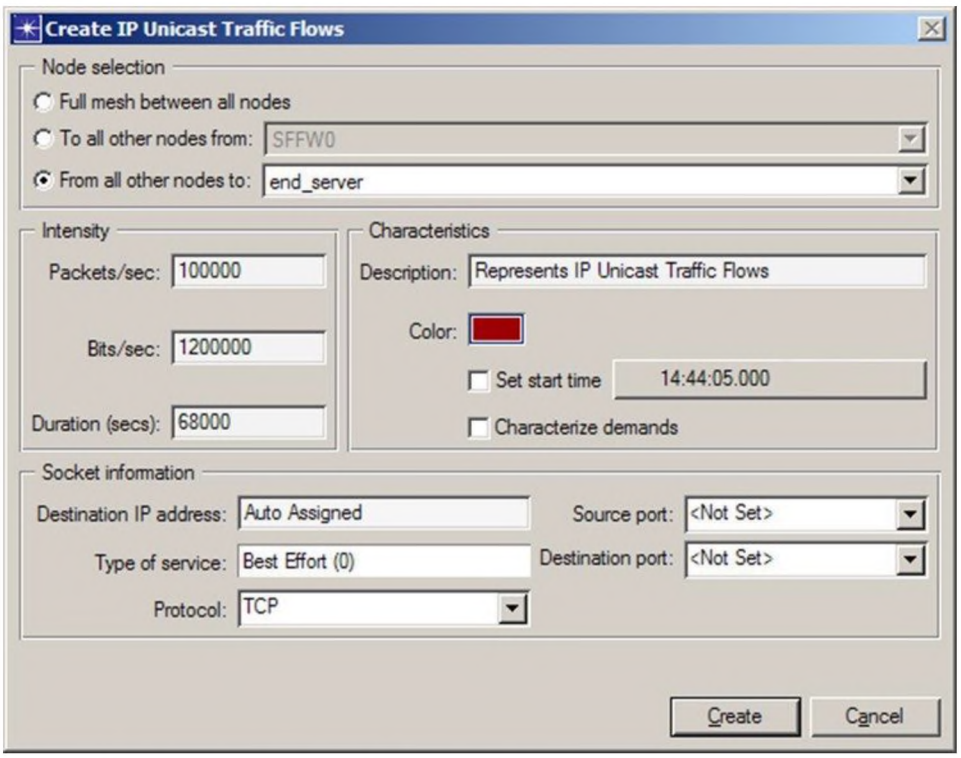

Рисунок 2.5 – Імітування зловмисного трафіку

Тест трафіка складається з:

- Звичайного TCP -150 загальний потік 800 Мбит/с;
- Звичайного UDP - 50 загальний потік 150 Мбит/с;
- Атаковий UDP – потік 400 Мбит/с.

Пропорція нормального TCP і UDP в Інтернеті типово складає вісім чи дев’ять к одному. Усі п’ять потоків атак UDP мають однакові адреси призначення, порт, розмір пакету.

Ефективність захисту від DDoS-атак зазвичай описується трьома основними параметрами:

- Потужність атаки (зазвичай в Мбіт /с), яку здатна витримати система;
- Точність дій системи при виявленні та відбитті атаки;
- Вірогідність і кількість помилкових спрацьовувань;

Залежно від поєднання цих параметрів і формуються ціна і якість послуг із захисту від DDoS атак.

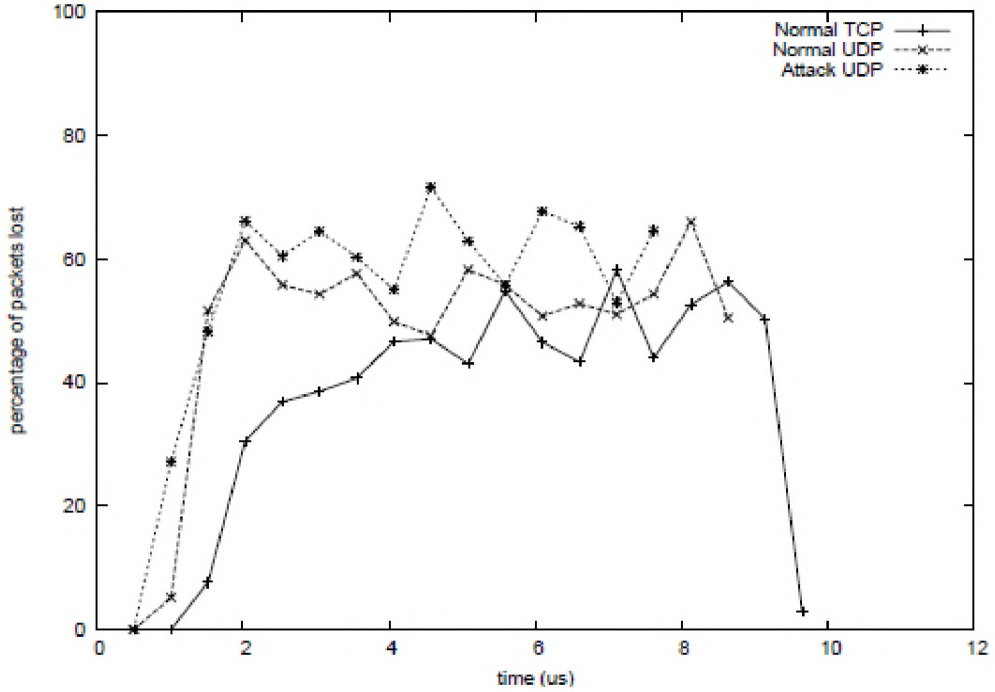

Рисунок 2.6 – Результат моделювання без кластерного захисту

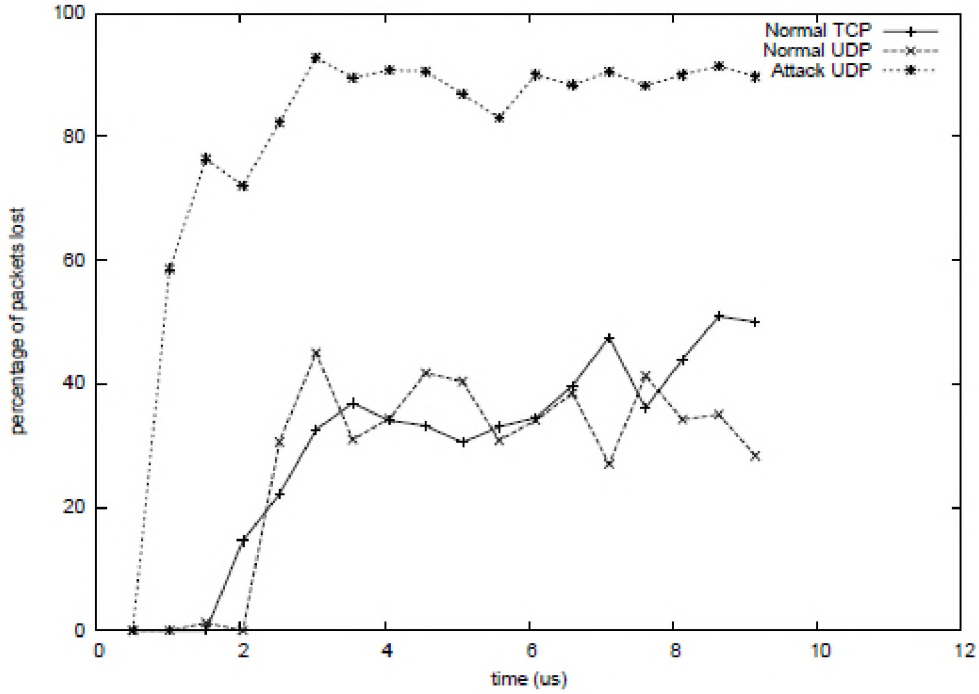

Рисунок 2.7 – Результат моделювання з кластерним захистом

Проаналізувавши отримані результати, можна сказати, що застосування кластерної системи захисту дозволяє відбити більшість зловмисного трафіку,

завдяки цьому можна зробити висновок, що використання цієї системи захисту виправдано.

2.5. Обґрунтування та вибір обладнання.

2.5.1 Сервери

Більш доцільним у більшості випадків є використання сучасних серверів формату 1U, які в більшості своїй є універсальними машинами для різних конфігурацій, починаючи від web-сервера-хостингу і закінчуючи HPC і суперкомп'ютерами. Завдяки використанню 2.5-дюймових вінчестерів і сучасних материнських плат, 1U сервери економлять місце в стійках при практично тих же самих можливостях розширення і тієї ж гнучкості адміністрування і рівні надійності HP ProLiant DL360 G6 і Proliant DL360 G6. Порівняльні характеристики наведемо у таблиці 2.1

Таблиця 2.1 – Параметри HP ProLiant DL360 G6 і Proliant DL360 G6

Сервер	HP ProLiant DL360 G6	Proliant DL360 G6
Висота	1U	1U
Об'єм оперативної пам'яті	192 GB	72 GB
Тип процесору	Intel Xeon X5670	Intel Xeon X5660
Блоки живлення	2	2
RAID-контролер	HP Smart array B110i SATA	HP Smart Array P410i+ Cache 256 MB
Комплектація	4 корзини в комплекте	4 корзини в комплекте
Частота процесора	2.93 GHz	2.83 GHz
Кількість ядер процесора	6	6
Кількість процесорів	2	2
Тип оперативної пам'яті	DDR3	DDR3
Сертифікат Intel Cluster Ready	Так	Так

Сервер від HP підтримує більший об'єм пам'яті, має слот PCI Express 16x, але чомусь поступається Proliant по кількості мережевих портів. Proliant має більше конфігурацій установки жорстких дисків.

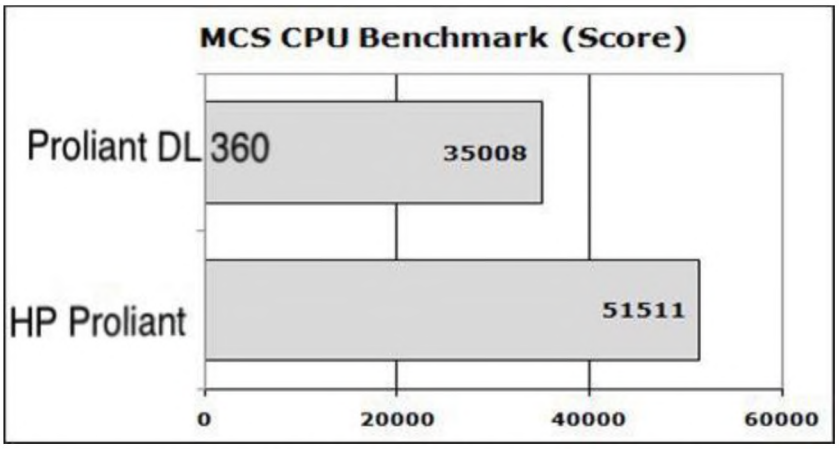

Рисунок 2.8 – Тест швидкодії HP ProLiant DL360 G6 і Proliant DL360 G6

За результатами порівняння обираємо рішення від HP для побудови кластера.

2.5.2 Маршрутизатор і міжмережевий екран

У схемі захисту використовується маршрутизатори серії Cisco 7600.

Ці маршрутизатори мають властивість DoS attack prevention (Профілкатика DDoS-атак), яка забезпечує додаткову захищеність від атак.

У якості міжмережевого екрану використовується продукт Juniper серії SRX. Ця серія має великий вибір моделей, що дозволяє обрати міжмережевий екран потрібної потужності залежно від конфігурації системи.

2.5.3 Конфігурації системи

Залежно від фінансових можливостей підприємства та потужності Web-ресурсу пропонується три варіанта конфігурації системи:

- В мінімальному варіанті можливо виключити деяке обладнання та спростити кількість серверів до трьох. В якості між мережевого екрану обрати

Juniper SRX240. На серверах використовувати Packet Filter в режимі SYN Proxy.

- В оптимальній конфігурації у якості маршрутизатора підійде пристрій Cisco 7606-S Chassis, та в якості міжмережевого екрану Juniper SRX650. Кластер proxy-серверів зробити з 3 серверів.

- В максимальній кофігурації потрібно встановити чотири сервера та залучити до конфігурації маршрутизатор CISCO 7613 .Кластер міжмережевих екранів включатиме три пристрою Juniper SRX650.

Також у якості сенсора використовується пристрії Cisco IPS 4270.

2.6. Рекомендації налаштування системи

2.6.1 Налаштування ядра

Сервер буде здатний витримувати не менше підключень від ботнету, ніж канал до сервера зможе пропустити.

Боротьба з Http DDoS проводиться на виділеному сервері, максимальна можлива потужність стримування DDoS атаки обмежується фізичними можливостями сервера і пропускною спроможністю каналу.

Інформаційний ресурс буде правильно індексуватися пошуковими машинами під час атаки, що дозволить зберегти позиції у видачі пошукових систем. Особливо актуально для сайтів з великими SEO бюджетами.

На час атаки доведеться відмовитися від деяких сервісів вашого сайту – наприклад системи пошуку. Ефективність досягається максимізацією коефіцієнта масштабованості системи. Забезпечується швидке нарощування апаратних ресурсів при збільшенні потужності атаки.

Конфігурація серверів в кластері:

Xeon 2.5GHz / 4Gb RAM / SAS,

З параметрами за замовчуванням ОС Debian та інші ОС не в змозі підтримувати величезну кількість сполук створюванних ботнет. Необхідно внести зміни в налаштування ядра, щоб зміцнити стек TCP/IP.

Лістінг зміцненої конфігурації для ОС Debian ядро вище 2.6.4:

net.ipv4.conf.all.accept_redirects = 0

net.ipv4.conf.eth0.accept_redirects = 0

net.ipv4.conf.default.accept_redirects = 0

net.core.rmem_max = 996777216

net.core.wmem_max = 996777216

net.ipv4.tcp_rmem = 4096 87 380 4194304

net.ipv4.tcp_mem = 786432 1048576 996777216

net.ipv4.tcp_wmem = 4096 87 380 4194304

net.ipv4.tcp_max_orphans = 2255360

net.core.netdev_max_backlog = 10000

net.ipv4.tcp_fin_timeout = 10

net.ipv4.tcp_keepalive_intvl = 15

net.ipv4.tcp_max_syn_backlog = 2048

net.ipv4.tcp_synack_retries = 1

kernel.msgmnb = 65536

kernel.msgmax = 65536

kernel.shmmax = 494967295

kernel.shmall = 268435456

net.core.somaxconn = 16096

Значення параметрів наведено у таблиці 2.1.

Таблиця 2.2 – Параметри налаштувань файлу sysctl.conf

Функція	Призначення
net.ipv4.conf.default.forwarding = 1	Необхідно дозволити ядру операційної системи здійснювати кидок трафіку з одного інтерфейсу на інший.
fs.file-max = 64000	Максимальне значення відкритих файлів.

Продовження таблиці 2.2

Функція	Призначення
net.ipv4.conf.all.rp_filter = 1	Цей параметр повідомляє ядру про необхідність фільтрації пакетів по їх вихідних адресах
kernel.sysrq = 0	Відключається комбінація клавіш sysrq, яка використовується при збою системи.
net.ipv4.conf.default.rp_filter = 1	Фільтр зворотного шляху, захист від спуфінга (підмін адрес)
net.ipv4.conf.all.accept_source_route = 0	Маршрутизація від джерела (source routing) дозволяє відправнику визначити шлях, по якому пакет повинен пройти по мережі Internet, щоб досягти пункту призначення.
net.ipv4.tcp_syncookies = 1	Дозволяє / забороняє передачу так званих syncookies у разі переповнення черги SYN-пакетів для заданого сокета
net.ipv4.ip_default_ttl = 64	Встановлює значення по замовчуванню для величини Time To Live вихідних пакетів.
net.ipv4.ip_dynaddr = 0	Змінна використовується для вирішення деяких проблем, пов'язаних з динамічною адресацією.
net.ipv4.ip_local_port_range = 32768 61000	Містить два цілих числа, які визначають діапазон локальних портів, які використовуються у клієнтських з'єднаннях.
net.ipv4.ip_nonlocal_bind = 0	Встановлення цієї змінної дозволяє окремим локальним процесам виступати від імені зовнішньої IP адреси.

Продовження таблиці 2.2

	Призначення
net.ipv4.ipfrag_low_thresh = 196608	Задає максимальний обсяг пам'яті, що виділяється під чергу фрагментованих пакетів.
net.ipv4.ipfrag_time = 30	Ця мінлива визначає максимальний час «зберігання» фрагментів у секундах
net.ipv4.inet_peer_gc_maxtime = 120	inet_peer_gc_maxtime визначає частоту «збирання сміття» при незначному обсязі даних.
net.ipv4.inet_peer_gc_mintime = 10	inet_peer_gc_maxtime визначає частоту «збирання сміття» при незначному обсязі даних
net.ipv4.inet_peer_maxttl = 600	Це максимальний час зберігання записів.
net.ipv4.inet_peer_minttl = 120	Визначає мінімальний час зберігання даних в «inet peer storage».
net.ipv4.inet_peer_threshold = 65664	Визначає мінімальний час зберігання даних в «inet peer storage».

2.6.2 Створення blacklist-а

Другою проблемою є величезна кількість з'єднань процесів PHP і БД, що повністю «з'їдають» ресурси пам'яті і процесора, так що значення load average перевищує 100 пунктів.

Необхідно відсікти паразитні з'єднання

Багато адміністраторів використовують метод пошуку пошукових роботів командою netstat. У процесі застосування даного методу є кілька істотних недоліків:

1. Створення blacklist-а займає багато часу, що не дозволяє нам часто оновлювати blacklist.

2. Ефективна робота пошукових роботів можлива тільки при зупиненому Web-сервері. У цей час сайт не доступний для клієнтів і з'являється загроза неправильної індексації сайту пошуковими системами.

3. У blacklist можуть потрапити IP пошукових роботів, що неприпустимо продемонструвавши неефективність цього методу, пропоновано новий метод пошуку та блокування пошукових роботів який повинен:

1. забезпечити постійну стабільну роботу Web-сервера (сайту)

2. гарантувати найменшу ймовірність появи у blacklist пошукових роботів.

Був проведен наступний експеримент:

Сервер Xeon 2.5GHz / 4Gb RAM / SAS під DoS запитами GET / HTTP/1.1.

Експеримент А. Web-сервер (в даному випадку nginx) зупинено

Вхідний трафік 6085.2 kbits / sec

Вихідний трафік 5342.1 kbits / sec

Експеримент Б. Nginx віддає порожній HTML (return 444;)

Вхідний трафік 56 Мбіт / с

Вихідний трафік 54 Мбіт / с

Експеримент В. Nginx віддає HTML розміром близько 2 Кб - це сторінка з невеликим повідомленням на кшталт «приносимо свої вибачення за перебої в роботі сайту»

Вхідний трафік 57 Мбіт / с

Вихідний трафік 353 Мбіт / с

На основі проведеного експерименту можна зробити наступні висновки:

а) Можна повністю відмовитися від фільтрації при наявності достатньої ємності каналу і відсутністю співвідношень вхідний / вихідний трафік. Сайт буде доступний клієнтам ціною величезного зловмисного трафіку.Легковажне рішення повністю відмовитися від фільтрації. Зловмисники можуть збільшити потужність DoS, так що припине роботу гігабітний канал.

б) При блокуванні абсолютно всіх пошукових роботів, зловмисний трафік від ботнету складе всього лише 5 Мбіт / с. Заблокувати всіх пошукових

роботів також неможливо, на це буде потрібно занадто багато ресурсів. Крім того, висока ймовірність блокування пошукових роботів.

Також необхідно звернути увагу на те, що вихідний трафік у останньому випадку перевищив 100 Мбіт/с. Значить, сервер підключений до порта 100 Мбіт/с стане важко доступний shh-протокол при повному завантаженню каналу. Щоб уникнути подібної неприємності, я рекомендую налаштувати віддачу порожнього HTML або return 444 в nginx до завершення налаштування фільтрації пошукових роботів.

Було зроблено припущення, що хороші клієнти роблять не більше 2х одночасних запитів до головної сторінці сайту. Можно вважати, що клієнти відкрили більш 3х одночасних з'єднань атакуючими ботами та блокуємо їх IP адреса на міжмережевий екран.

Припущення було підтверджене експериментально. На основі аналізу логу http запитів за добу з 120 000 IP адрес, тільки з 19ті IP було зроблено більше 2х одночасних запитів.

Для реалізації пошуку «пошукових» роботів створена спеціальну обробку запитів

request: «GET / HTTP/1.1» в nginx.

error_log / var / log / nginx / error.log;

<...>

location = / (

limit_conn one 3;

root / home / www /site.com;

)

IP адреси з яких було відкрито понад 3х одночасних підключень будуть записані в error.log з повідомленням limiting connections by zone. На основі логу помилок будується blacklist ip атакуючого ботнету.

Налаштування Nginx (файл nginx.conf):

user www-data www-data;

worker_processes 10;

```
error_log /var/log/nginx/error.log;
pid /var/run/nginx.pid;
events {
worker_connections 1024;
}
http
 {
include /etc/nginx/mime.types;
default_type application/octet-stream;
access_log /var/log/nginx/access.log;
sendfile on;
keepalive_timeout 5;
tcp_nodelay on;
gzip on;
limit_req_zone $binary_remote_addr zone=antiddosphp:10m rate=1r/s;
limit_req_zone $binary_remote_addr zone=antiddos:10m rate=10r/s;
include /etc/nginx /*;
}
server {
root /home/www-data/site.com;
listen 80;
server_name site.com;
access_log off;

location /
{
index index.php index.html index.htm;
limit_req zone=antiddos burst=10;
}
location ~ \.php$
```

```
{
fastcgi_pass unix:/tmp/php-fpm.sock;
fastcgi_index index.php;
include fastcgi_params;
fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
fastcgi_read_timeout 1800;
fastcgi_param SERVER_NAME $http_host;
fastcgi_ignore_client_abort on;
limit_req zone=antiddosphp burst=2;
}
}
```

2.6.3 Фільтрація пошукових роботів в IPtables

IPtables не придатні для фільтрації великої кількості адрес. При кількості ланцюжків більших ніж 2К IPtables процес ksoftirqd починає споживати 100% CPU, що призводить до позамежної завантаженні сервера. Проблема вирішується установкою ipset або зменшенням кількість правил в iptables.

У даному випадку установка ipset була відкладена на випадок крайньої необхідності. У сервера не було вбудованого KVM і перезібрати ядро було ризиковано.

Приступимо до створення blacklist-а.Блокування тільки самих агресивних ботів, щоб не перевантажувати IPtables.

```
# Пошук ботів
cat / var / log / nginx / error.log | grep "limiting connections by zone" | grep "request: \" GET / HTTP/1.1 "| awk '(print $ 12)' | awk-F", "'(print $
1) '| sort | uniq-c | sort-nr> / tmp / botnet.blacklist
# Очищення скрипт блокування
cat / dev / null> / tmp / iptables_ban.sh
# Створення DROP правила для 50 найагресивніших ботів
```

awk '(print "iptables-A INPUT-p tcp - dport 80-s" $ 2 "-j DROP")' botnet.blacklist | head-n 50>> / tmp / iptables_ban.sh

Завантаження blacklist

bash / tmp / iptables_ban.sh

Ротація логу

cat / dev / null> / home / www / nginx_log / error.log

[! -F / var / run / nginx.pid] | | kill-USR1 `cat / var / run / nginx.pid`

Додавання скрипт в крон з частотою кілька хвилин. Частоту підбиране дослідним шляхом і становить раз на 5 хвилин.

* / 5 * * * * / root / script / ban.sh

У результаті iptables буде поповнюватися новими роботами.

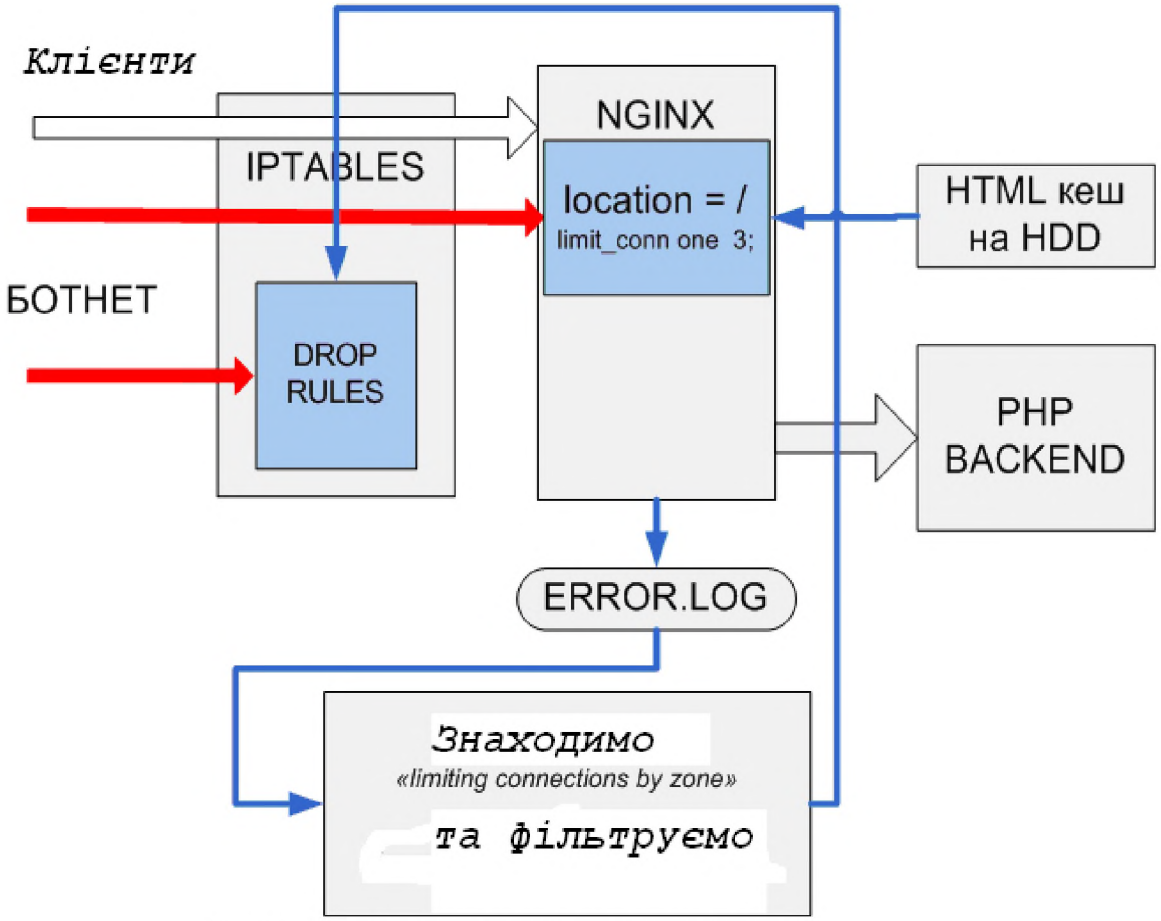

Рисунок 2.9 – Схема фільтрації трафіка

Схема фільтрації наведена на рис. 2.4.

Запропонований метод забезпечує стабільний доступ клієнтів до інформаційних ресурсів сайту. Правильна індексація в ПС була підтверджена тим, що сайт зберіг свої позиції у видачі. Завантаження сервера не виходила за розумні межі la невеликі 6-7 пунктів. Вихідний трафік з сервера не перевищував 100 Мбіт/с. Для відбиття атаки більшої ніж 7К, ботнету цілком достатньо можливостей IPtables. Повний лістинг розробленої системи захисту по IP наведено у додатку Д.

Для захисту від ботів, що не мають референів, доцільно використати наступну конфігурацію:

```
set $add 1;
 location /index.php {
 limit_except GET POST {
 deny all;
 }
 set $ban "";
 if ($http_referer = "" ) {set $ban $ban$add;}
 if ($request_method = POST) {set $ban $ban$add;}
 if ($query_string = "action=login" ){set $ban $ban$add;}
 if ($ban = 111 ) {
 access_log /var/log/nginx/ban IP;
 return 404;
 }
 proxy_pass http://127.0.0.1:8000;# backend
 }
```

2.6.4 Захист від надлишкових з'єднань за географічною ознакою

Для зупинення атак типу DDOS вкрай важливо захистити сервер від відвідувачів з небажаних країн. Причини такого захисту є безліч - скорочення

спаму і можливих платформ для проведення атак, вирівнювання співвідношень або розподілення навантаження в кластері за географічною ознакою.

Наприклад, іноді необхідно заблокувати CN повністю, на UA віддавати повний канал, а на інші країни - в два рази менше.

Зрозуміло, забивати повністю всі підмережі уручну незручно, та й вони часто міняються. Найефективніше - це використати можливості geoip ядра. Якщо на серверах встановлено ОС Debian:

```
apt-get install linux-source-2.6.18
tar xjf /usr/src/linux-source-2.6.18.tar.bz2 -C /usr/src/
apt-get source iptables
wget people.netfilter.org/peejix/patchlets/geoip.tar.gz
wget ftp.netfilter.org/pub/patch-o-matic-ng/snapshot/patch-o-matic-ng-20070414.tar.bz2
tar xjf patch-o-matic-ng-20070414.tar.bz2
tar xzf geoip.tar.gz -C patch-o-matic-ng-20070414/patchlets/
```

Для підготовки треба завантажити безкоштовну базу, хоча краще взяти платний варіант - він точніше. У будь-якому випадку підготовка бази буде йти за допомогою csv2bin, який треба зібрати:

```
wget people.netfilter.org/peejix/geoip/tools/csv2bin-20041103.tar.gz
tar xzf csv2bin-20041103.tar.gz
cd csv2bin/
make
wget www.maxmind.com/download/geoip/database/GeoIPCountryCSV.zip
unzip GeoIPCountryCSV.zip
./csv2bin ../GeoIPCountryWhois.csv
mkdir /var/geoip
mv geoipdb. * /var/geoip/
```

Можна використати mod_geoip так:

iptables -A INPUT -p tcp --dport 80 -m geoip --src-cc CN -j REJECT

Відкидаємо трафік с CN та змінюємо смугу з допомогою міжмережевого екрану.

Висновки розділу

На основі проведеного аналізу існуючих класів атак типу «відмова в обслуговуванні», а також заходів і засобів, що використовуються для боротьби, була розроблена система кластерного захисту Web-серверів від розподілених атак, що дозволяє мінімізувати ймовірність відмови забезпечуваних сервісів. Ефективність запропонованої схеми була доведена за допомогою програмного моделювання DDoS-атак в пакеті OPnet. Результат моделювання показав, що запропонована система кластерного захисту дозволяє активно протидіяти розподіленим атакам.

Так само були запропоновані рекомендації з налаштування, що дозволяють підвищити відмовостійкість системи, а також здійснено вибір необхідного обладнання.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Метою економічного розділу є аналіз економічної ефективності Web-серверів. Для цього необхідно здійснити розрахунок:

– капітальних витрат на придбання і налагодження складових системи інформаційної безпеки або витрат, що пов'язані з виготовленням апаратури, приладів, програмного забезпечення;

– річних експлуатаційних витрат на утримання і обслуговування об'єкта проектування;

– річного економічного ефекту;

– показників економічної ефективності розробки та впровадження розробки Web-серверів від DDoS-атак

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 Web-серверів.

Визначення трудомісткості розробки Web-серверів.

Трудомісткість розробки Web-серверів визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації (за умови роботи одного спеціаліста з інформаційної безпеки):

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

де $t_{тз}$ – тривалість складання технічного завдання на розробку Web-серверів;

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

t_a – 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 Web- серверів, тривалість операцій складає наступні величини: $t_{тз}$=20 годин, $t_в$=35 годин, $t_{вз}$=19 годин, $t_{озб}$=12 годин, $t_{овр}$=10 годин, $t_д$=6 годин.

Отже, t=20+35+19+12+10+6= 102 годин,

Розрахунок витрат на створення Web-серверів

Витрати на розробку Web-серверів 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.

$$К_{рп} = З_{зп} + З_{мч}\ .$$

$$К_{рп} = З_{зп} + З_{мч} = 21420 + 1015{,}92 = 22435{,}92 \text{ грн.}$$

$$З_{зп} = t\ З_{пр} = 102*210 = 21420 \text{ грн.}$$

де t – загальна тривалість розробки Web- серверів, годин;

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

Вартість машинного часу для розробки Web- серверів на ПК визначається за формулою:

$$З_{мч} = t*С_{мч} = 102*9{,}96 = 1015{,}92 \text{ грн.}$$

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

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

Вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = 1 \cdot 5 \cdot 1{,}64 + \frac{9350 \cdot 0{,}3}{1920} + \frac{5800 \cdot 0{,}1}{1920} = 9{,}96 \text{ грн.}$$

Відповідно до розроблених рекомендації щодо застосування розробки Web-серверів на підприємстві планується використання AKAMAI та Cloudflare, які вже встановлені на підприємстві.

Таким чином, капітальні (фіксовані) витрати на створення Web- серверів:

$$К = К_{рп} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н} = 22435{,}92 \text{ грн.}$$

де $К_{рп}$ – вартість розробки Web- серверів 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:

$$С = С_в + С_к + С_{ак}\ ,\quad грн.$$

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:

$$С_к = С_н + С_а + С_з + С_{ел} + С_о + С_{тос},\ грн.$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів визначаються ($С_н = 12000$ грн.).

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

$$С_з = З_{осн} + З_{дод},\ грн.$$

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 17000 грн. Додаткова заробітна плата – 10% від основної заробітної плати. Виконання роботи щодо налаштувань Web- серверів потребує залучення спеціаліста інформаційної безпеки на 0,25 ставки. Отже,

$$С_з = (17000*12 + 17000*12*0,1)*0,25 = 56100\ грн.$$

Ставка ЄСВ для всіх категорій платників складає 22%.

$$С_{єв} = 56100\ *0,22 = 12342\ грн.$$

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е, \text{ грн.},$$

де Р – встановлена потужність апаратури інформаційної безпеки, (Р=1 кВт);

$F_р$ – річний фонд робочого часу системи інформаційної безпеки ($F_р$ = 1920 год.);

$Ц_е$ – тариф на електроенергію, ($Ц_е$ = 1,64 грн./кВт за годину).

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

$$С_{ел} = 1*1920*1,64 = 3148,8 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки визначаються у відсотках від вартості капітальних витрат - 1% (Стос = 22435,92 *0,01=224,36 грн).

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

$$С_к = 12000+56100+12342+3148,8+224,36 = 83815,16 \text{ грн.}$$

Таким чином, річні поточні витрати на функціонування системи інформаційної безпеки складають 83815,16 грн.

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, 5 години;

$t_в$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 3 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.), 9500 грн./міс.;

$З_с$ – заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 10000 грн./міс.;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особи;

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

О – обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 1700000 тис. 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, 32.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U = П_п + П_в + V,$$

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:

$$П_П = \frac{\sum Зс}{F} \cdot t_п = \frac{1000 \cdot 12}{176} \cdot 5 = 3409{,}09 \quad \text{грн},$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

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

$$П_в = П_{ви} + П_{пв} + П_{зч},$$

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 $t_{ви}$:

$$П_{ви} = \frac{\sum Зс}{F} \cdot t_{ви} = \frac{1000 \cdot 12}{176} \cdot 6 = 4090{,}91 \text{ грн.}$$

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

$$П_{пв} = \frac{\sum Зо}{F} \cdot t_в = \frac{9500 \cdot 1}{176} \cdot 3 = 161{,}93 \text{ грн.}$$

Витрати на заміни встаткування або запасних частин можуть скласти 3700 грн.

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$П_в = 4090{,}91 + 161{,}93 + 3700 = 7952{,}84 \text{ грн.}$$

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

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

$$V = \frac{1700000}{2080} \cdot (5 + 3 + 6) = 11442{,}31 \text{ грн.}$$

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.

$$U = 3409{,}09 + 7952{,}84 + 11442{,}31 = 22804{,}24 \text{ грн.}$$

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

$$B = \sum_i \sum_n U = \sum_1 \sum_{32} 22804{,}24 = 729735{,}68 \text{ грн.}$$

3.2.2 Загальний ефект від впровадження системи інформаційної безпеки

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

$$E = B \cdot R - C \text{ грн.},$$

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

R – вірогідність успішної реалізації атаки на сегмент мережі, частки одиниці (60%);

C – щорічні витрати на експлуатацію системи інформаційної безпеки.

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

$$E = 729735{,}68 * 0{,}6 - 83815{,}16 = 354026{,}25 \text{ грн.}$$

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:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці,}$$

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

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

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{354026,25}{22435,92} = 15,78, \quad \text{частки одиниці,}$$

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

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

де $N_{деп}$ – річна депозитна ставка в 2020р., (15,5%);

$N_{інф}$ – річний рівень інфляції в 2019р., (3,54%).

Розрахункове значення коефіцієнта повернення інвестицій:

$$15,78 > (15,5 - 3,54)/100 = 15,78 > 0,1196.$$

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

$$T_O = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{15,78} = 0,06 \text{ років, } \approx 1 \text{ місяць.}$$

3.4 Висновок

Розробка Web-серверів на підприємстві є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 15,78 грн./грн., що означає отримання 15,78 грн. економічного ефекту на кожну гривню капітальних вкладень на розробку Web-серверів. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів. Термін окупності при цьому складатиме 0,06 років (біля 1 місяця). Капітальні витрати складають 22435,92 грн.

ВИСНОВКИ

DDoS як стихійне лихо і уникнути шкоди неможливо.

З кожним роком зростає кількість, обсяги і досконалість розподілених атак.

У більшості випадків DDoS є зброєю конкурентної боротьби в мережі. Клієнти практично миттєво здатні перейти до ваших конкурентів, якщо ваш ресурс буде працювати зі сбоями.

Використовуючи удосконалені рішення, створені для боротьби з актами, компанії отримають гарантію безперервної роботі Web-сервісів.

Результати аналізу існуючих методів боротьби з атаками дають можливість стверджувати про їх недосконалість і про необхідність створення сучасних систем протидії цим типам загроз.

Проаналізувавши всі види існуючих атак і концепцій боротьби з ними була запропонована схема розв'язання проблеми, яка за допомогою ретельних налаштувань і правильного вибору обладнання, надає ефективну протидію існуючим загрозам.

Результати моделювання системи довели здатність системи протистояти масованим атакам.

Запропонована кластерна система захисту від атак цього типу дозволяє мінімізувати збитки та вільно нарощувати міцність захисту за необхідності для забезпечення високої доступності інформаційних ресурсів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Закон України “Про інформацію”.

2. Закон України “Про державну таємницю”.

3. Закон України “Про захист інформації в інформаційно-телекомунікаційних системах”.

4. Указ Президента України від 04.05.2008 р. підстава 333\2008 “Про затвердження Положення про технічний захист інформації в Україні”.

5. Наказ N 76 від 24.12.2005 Департаменту спеціальних телекомунікаційних систем та захисту інформації служби безпеки України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах»

6. НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

7. НД ТЗІ 2.5-010-03 Вимоги до захисту інформації WEB-сторінки від несанкціонованого доступу.

8. НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу.

9. Xiang Y., Zhou W., Chowdhury A.Survey of Active and Passive Defence Mechanisms against DDoS Attacks. Technical Report, TR C04/02,

10. School of Information Technology, Deakin University, Australia, March 2009.

11. Specht S. and Lee Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures // Proceedings of the 17th International

Conference on Parallel and Distributed Computing Systems, 2012 International Workshop on Security in Parallel and Distributed Systems,

12. Уланов А. В., Котенко И. В. Защита от DDoS-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. - 2007, INSIDE, № 1-3.

13. Mircovic J., Dietrich S., Dietrich D., Reiher P.Internet Denial of Service: Attack and Defense // Mechanisms. Prentice Hall, Engle Wood liffs, NJ.

14. Rocky K., Chang CD efending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial // IEEE Communications Magazine, 2008 October, - P. 42 - 51.

15. Ігнатенко О.П. Виявлення низькочастотних атак на відмову на основі історичних даних // Комп'ютерні науки та інформаційні технології, - Львів: 2008, - № 1.

16. Jansen W. A. Intrusion detection with mobile agents // Computer communications. -. - 25. - P. 1392 - 1401.

17. Agent-Based Network Intrusion Detection System // In Intelligent Agent Technology. IEEE

18. Computer Society. Los Alamitos, California. - 2007. - P. 528 - 531.

19. Семёнов Ю.А. Задачи государственной службы Украины по вопросам технической защиты информации.- “Безопасность информации”, №1, 1995. С. 6-9.

20. Методичні вказівки з курсу «Проектування та застосування систем ТЗІ на об’єктах інформаційної діяльності».

21. Норткатт С. и др. Анализ типовых нарушений безопасности в сетях. — Киев: Издательство "Вильямс".

22. Державна служба спеціального зв'язку та захисту інформації України (Електрон. ресурс) / Спосіб доступу: URL: http://www.dstszi.gov.ua/. – Загол. з екрана.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	17	
6	А4	2 Розділ	33	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	
14	А4	Додаток Д	5	

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

16 Додаток Д.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК

на кваліфікаційну роботу бакалавра на тему:
Розробка кластерної системи захисту WEB-серверів від DDoS-атак
Тофана Віктора Валерійовича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на __ сторінках та містить __ рисунків, __ таблиць, __ джерел та __ додатків.

Мета роботи: розробка кластерної системи захисту WEB-серверів від DDoS-атак. У першій частині розглянуті загрози, що створюється атаками типу DDoS, методи захисту: маршрутизація в «чорні діри», міжмережеві екрани та системи IDS. Розглянута проблема забезпечення доступності web-ресурсів.

У спеціальній частині проаналізовані існуючі DDoS-атаки та концепція реалізації систем захисту. Запропонована схема вирішення завдання комплексного захисту від різних типів DDoS атак високої інтенсивності та модулювання її у програмному середовищі.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник

```
##### CONFIG #####
PROGDIR="/usr/local/ddos"
PROG="/usr/local/ddos/ddos.sh"
IGNORE_IP_LIST="/usr/local/ddos/ignore.ip.list"
CRON="/etc/cron.d/ddos.cron"
APF="/etc/apf/apf"
IPT="/sbin/iptables"

##### frequency in minutes for running the script
##### Caution: Every time this setting is changed, run the script with --cron
#####          option so that the new frequency takes effect
FREQ=1

##### How many connections define a bad IP? Indicate that below.
NO_OF_CONNECTIONS=150

##### APF_BAN=1 (Make sure your APF version is atleast 0.96)
##### APF_BAN=0 (Uses iptables for banning ips instead of APF)
APF_BAN=1

##### KILL=0 (Bad IPs are'nt banned, good for interactive execution of
script)
##### KILL=1 (Recommended setting)
KILL=1

##### An email is sent to the following address when an IP is banned.
##### Blank would suppress sending of mails
EMAIL_TO="root"

##### Number of seconds the banned ip should remain in blacklist.
BAN_PERIOD=600


#!/bin/sh
###############################################################
#####
# DDoS ZAHYST #
```

```
        ###################################################################
#####
        load_conf()
        {
                CONF="/usr/local/ddos/ddos.conf"
                if [ -f "$CONF" ] && [ ! "$CONF" ==         "" ]; then
                        source $CONF
                else
                        head
                        echo "\$CONF not found."
                        exit 1
                fi
        }

        head()
        {
        }

        showhelp()
        {
                head
                echo 'Usage: ddos.sh [OPTIONS] [N]'
                echo 'N : number of tcp/udp      connections (default 150)'
                echo 'OPTIONS:'
                echo '-h | --help: Show     this help screen'
                echo '-c | --cron: Create cron job to run this script regularly (default 1
mins)'
                echo '-k | --kill: Block the offending ip making more than N
connections'
        }

        unbanip()
        {
                UNBAN_SCRIPT=`mktemp /tmp/unban.XXXXXXXX`
                TMP_FILE=`mktemp /tmp/unban.XXXXXXXX`
                UNBAN_IP_LIST=`mktemp /tmp/unban.XXXXXXXX`
                echo '#!/bin/sh' > $UNBAN_SCRIPT
                echo "sleep $BAN_PERIOD" >> $UNBAN_SCRIPT
                if [ $APF_BAN -eq 1 ]; then
```

```
                while read line; do
                        echo "$APF -u $line" >> $UNBAN_SCRIPT
                        echo $line >> $UNBAN_IP_LIST
                done < $BANNED_IP_LIST
        else
                while read line; do
                        echo "$IPT -D INPUT -s $line -j DROP" >>
$UNBAN_SCRIPT
                        echo $line >> $UNBAN_IP_LIST
                done < $BANNED_IP_LIST
        fi
        echo "grep -v --file=$UNBAN_IP_LIST $IGNORE_IP_LIST >
$TMP_FILE" >> $UNBAN_SCRIPT
        echo "mv $TMP_FILE $IGNORE_IP_LIST" >> $UNBAN_SCRIPT
        echo "rm -f $UNBAN_SCRIPT" >> $UNBAN_SCRIPT
        echo "rm -f $UNBAN_IP_LIST" >> $UNBAN_SCRIPT
        echo "rm -f $TMP_FILE" >> $UNBAN_SCRIPT
        . $UNBAN_SCRIPT &
}

add_to_cron()
{
        rm -f $CRON
        sleep 1
        service crond restart
        sleep 1
        echo "SHELL=/bin/sh" > $CRON
        if [ $FREQ -le 2 ]; then
                echo "0-59/$FREQ * * * * root /usr/local/ddos/ddos.sh
>/dev/null 2>&1" >> $CRON
        else
                let "START_MINUTE = $RANDOM % ($FREQ - 1)"
                let "START_MINUTE = $START_MINUTE + 1"
                let "END_MINUTE = 60 - $FREQ + $START_MINUTE"
                echo "$START_MINUTE-$END_MINUTE/$FREQ * * * *
root /usr/local/ddos/ddos.sh >/dev/null 2>&1" >> $CRON
        fi
        service crond restart
}
```

```
load_conf
while [ $1 ]; do
        case $1 in
                '-h' | '--help' | '?' )
                        showhelp
                        exit
                        ;;
                '--cron' | '-c' )
                        add_to_cron
                        exit
                        ;;
                '--kill' | '-k' )
                        KILL=1
                        ;;
                 *[0-9]* )
                        NO_OF_CONNECTIONS=$1
                        ;;
                * )
                        showhelp
                        exit
                        ;;
        esac
        shift
done

TMP_PREFIX='/tmp/ddos'
TMP_FILE="mktemp $TMP_PREFIX.XXXXXXXX"
BANNED_IP_MAIL=`$TMP_FILE`
BANNED_IP_LIST=`$TMP_FILE`
echo "Banned the following ip addresses on `date`" > $BANNED_IP_MAIL
echo >>      $BANNED_IP_MAIL
BAD_IP_LIST=`$TMP_FILE`
netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr >
$BAD_IP_LIST
cat $BAD_IP_LIST
if [ $KILL -eq 1 ]; then
        IP_BAN_NOW=0
```

```
                while read line; do
                        CURR_LINE_CONN=$(echo $line | cut -d" " -f1)
                        CURR_LINE_IP=$(echo $line | cut -d" " -f2)
                        if [ $CURR_LINE_CONN -lt $NO_OF_CONNECTIONS ];
then
                                break
                        fi
                        IGNORE_BAN=`grep -c $CURR_LINE_IP
$IGNORE_IP_LIST`
                        if [ $IGNORE_BAN -ge 1 ]; then
                                continue
                        fi
                        IP_BAN_NOW=1
                        echo "$CURR_LINE_IP with $CURR_LINE_CONN
connections" >> $BANNED_IP_MAIL
                        echo $CURR_LINE_IP >> $BANNED_IP_LIST
                        echo $CURR_LINE_IP >> $IGNORE_IP_LIST
                        if [ $APF_BAN -eq 1 ]; then
                                $APF -d $CURR_LINE_IP
                        else
                                $IPT -I INPUT -s $CURR_LINE_IP -j DROP
                        fi
                done < $BAD_IP_LIST
                if [ $IP_BAN_NOW -eq 1 ]; then
                        dt=`date`
                        if [ $EMAIL_TO != "" ]; then
                                cat $BANNED_IP_MAIL | mail -s "IP addresses banned
on $dt" $EMAIL_TO
                        fi
                        unbanip
                fi
        fi
        rm -f $TMP_PREFIX.*
```