- комутатори 7-го рівня;
- інтегрований IDS з мережевим firewall;
- гібридні комутатори.

Крім застосування систем IDS чи мережевих firewall є можливість захисту від цього типу атак на більшості мережевих пристроїв, таких як маршрутизатори, безпровідні пункти доступу, міжмережеві інтерфейси VoIP, тощо шляхом активізації опції операційних систем пристроїв. Їх можливості не такими широкими в порівнянні з вищенаведеними системами, а лише становлять відповідне забезпечення для малих КМ. Нижче можемо побачити приклад міжмережевого інтерфейсу VoIP і маршрутизатора, що запобігають перед атаками DoS/DdoS (рис.1).

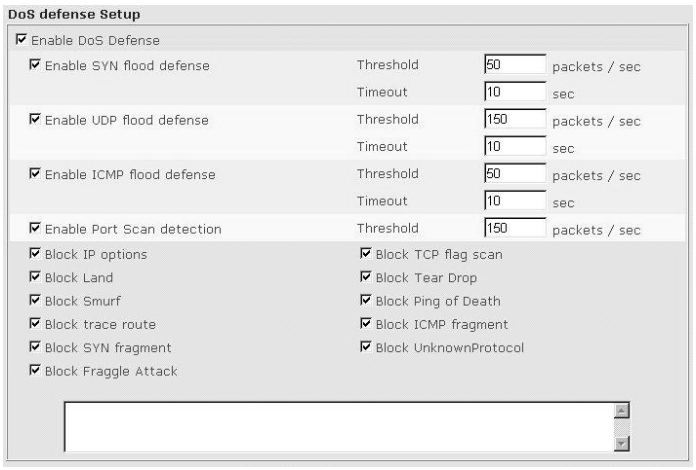

Рисунок 1. – Інтерфейс маршрутизатора при захисті від атак типу DoS/DDoS

Таким чином, в атаках типу DoS/DDoS загалом використовують прогалини існуючих інформаційних систем чи недосконалості специфікації мережевих протоколів. Слід використовувати операційні системи з високим рівнем захисту та безпечне програмне забезпечення, призначене для серверів мережевих послуг.

Список використаних джерел

1. http://www.netfilter.org.
2. http://www.snort.org/.
3. А.В. Уланов, И.В. Котенко Защита от Ddos-атак: механизмы предупреждения, обнаружения, отслеживания источника и противодействия // Защита информации. INSIDE, №1-3,2007.
4. Ганьжа Д. Мосты в локальних сетях // LAN Magazine,2006, №1.

УДК 004.056.5

ПІДВИЩЕННЯ ПРОДУКТИВНОСТІ ПРОТОКОЛУ IPSEC

Шевчук Р.П., Геник Г.Я.
Тернопільський національний економічний університет

І. Постановка проблеми

У сучасних телекомунікаційних системах широко використовуються протоколи захищеної передачі даних, де вирішення задач забезпечення конфіденційності, цілісності та автентичності інформації досягається шляхом криптографічного перетворення даних. Одним із основних криптографічних протоколів є IPSec (Internet Protocol Security) [1].

Зростання швидкості та об’ємів передавання даних, кількості одночасно працюючих захищених мереж приводять до зростання вимог щодо продуктивності оброблення даних згідно з протоколом IPSec. Реалізація оброблення даних згідно з протоколом IPSec базується на сумісному використанні як програмованих, так і спеціалізованих процесорів. Однак, існуючі структури операційних пристроїв процесорів IPSec створюються з недостатнім врахуванням особливостей комп’ютерних мереж, де ці процесори застосовуються. Зокрема, структури операційних пристроїв цих процесорів проектують так, щоб отримати мінімальні затрати обладнання. Часто ця вимога приводить до зменшення

продуктивності оброблення даних. Тенденції розвитку мікроелектроніки свідчать про те, що розробникам надається для проектування значні ресурси обладнання, що дає змогу використовувати всі види просторового і часового паралелізму алгоритмів оброблення даних. На перший план висуваються вимоги з продуктивності оброблення даних, а вимоги мінімізації обладнання відіграють меншу роль. Тому важливою є проблема підвищення продуктивності роботи протоколу IPSec.

II. Мета роботи

Метою роботи є підвищення продуктивності комп'ютерних засобів захисту інформації в реальному часі на основі оптимізованих програмно-апаратних реалізацій операційних пристроїв шифрування та хешування процесорів, що працюють згідно з протоколом IPSec.

III. Підвищення продуктивності протоколу IPSec

Виділимо основні напрямки підвищення продуктивності протоколу IPSec:

- оптимізація топологічної структури протоколу;
- оптимізація передачі даних та обчислень в межах мережевої взаємодії;
- мінімізація мережевого потоку даних;
- мінімізація часу виконання обчислень базовими алгоритмами протоколу.

Перераховані вище напрямки підвищення продуктивності протоколу IPSec (крім останнього) обмежені в засобах досягнення оптимальних рішень, внаслідок того, що віртуальні-приватні мережі будуються на вже визначеній інфраструктурі. Тому, одним з головних напрямів підвищення продуктивності є мінімізація часу обчислень базових криптографічних алгоритмів IPSec. Використання інших засобів можливе лише при комплексній оптимізації системи, включно з оптимізацією мережевих і апаратних рішень, які відповідають нижнім рівням протоколів взаємодії відкритих систем. Обмеження засобів оптимізації операційних пристроїв криптографічних алгоритмів протоколу IPSec залишає можливість оптимізувати структури операційних пристроїв протоколу IPSec за критеріями часу оброблення пакетів, затратами обладнання, ефективністю використання обладнання, тощо.

Серед цих напрямків оптимізації виділимо оптимізацію структур операційних пристроїв шифрування та хешування процесорів, що працюють згідно з протоколом IPSec, за часовими параметрами. Для мінімізації часових параметрів в математичній моделі протоколу IPSec виділимо [2]:

- структури операційних пристроїв хешування згідно з алгоритмами MD5 та SHA-1;
- структури операційних пристроїв шифрування згідно з алгоритмом DES.
- Додатково виділимо параметри, які визначають область використання протоколу IPSec:
- розмір пакета – визначається топологією мережі та задає кількість буферів N для оброблення;
- сервісні параметри протоколу IPSec – визначають тип сервісу який буде обробляти дані. До сервісних параметрів протоколу IPSec віднесено протоколи AH, ESP та їх комбінацію, транспортний і тунельний режими передачі даних;
- часові параметри алгоритмів шифрування та хешування (час спрацювання регістра, час спрацювання комбінаційної схеми, час спрацювання комутатора) [3].

Алгоритм мінімізації часових параметрів структур операційних простоїв процесора IPSec представимо такою послідовністю етапів:

- Визначається сервіс, який повинен реалізувати процесор IPSec.
- Згідно вибраного сервісу обчислюється час оброблення пакету для кожної структури операційного пристрою процесора.
- Задається умова порівняння часових характеристик масиву сформованих структур з поточною структурою.
- Встановлюються умови визначення оптимальних параметрів структур операційних пристроїв.
- Виконується пошук найкращих параметрів структури операційних пристроїв за встановленими умовами та критеріями.

На кожному етапі задачі мінімізації часових параметрів виконується пошук найкращих параметрів структур операційних пристроїв процесора IPSec за встановленим критерієм.

На основі наведеного алгоритму мінімізації, розроблено програмне забезпечення для знаходження параметрів структури операційного пристрою процесора IPSec з обчисленням її продуктивності (рисунок 1).

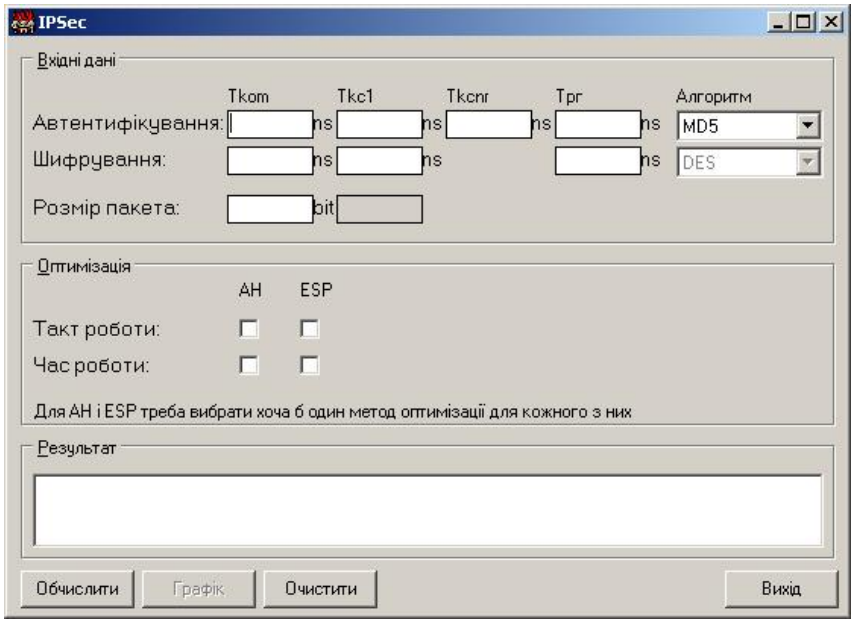

Рисунок 1 – Головне вікно програми пошуку параметрів оптимальної структури операційних пристроїв процесора IPSec

Результатом роботи програми є видача найкращих значень часових характеристик для параметрів структури операційних пристроїв хешування і шифрування. На основі проведених обчислень будуються графіки залежності часу оброблення пакетів даних комп'ютерних мереж від структур операційних пристроїв шифрування та хешування.

Список використаних джерел

1. Шнайер Б. Прикладная криптография, 2-е издание: протоколы, алгоритмы, исходные тексты на языке Си. - Под редакцией П.В. Семьянова. М., Триумф, 2002.
2. Т. Коркішко, Л. Коркішко, Р. Шевчук. Базові структури операційних пристроїв хешування для процесорів підтримки протоколу IPSEC // Комп'ютинг. – 2003. – Том 2. №1. – С. 41-47.
3. Шевчук Р., Манжула В., Адамів О. Оцінка технічних характеристик операційних пристроїв процесорів хешування // Вісник Тернопільського державного технічного університету. – Тернопіль, 2009. № 2. – С. 103 – 108.

УДК 681.511:3

ОЦІНКА СТІЙКОСТІ СТЕГАНОФОНІЧНИХ СИСТЕМ

Шевчук Р.П., Карпова О. В.
Тернопільський національний економічний університет

I. Постановка проблеми

Стеганофонічні системи – це системи в яких приховується факт передачі таємного повідомлення, а саме повідомлення інкапсулюється у стек мережевих протоколів та передається у реальному масштабі часу [1]. Вперше принципи та визначення комп'ютерної стеганофонії були сформовані польськими спеціалістами з Варшавського університету технологій у 2008 році, які запропонували декілька методів приховування даних у трафіку IP-телефонії [1]. Структура та принципи роботи систем комп'ютерної стеганофонії аналогічні до стеганографічних систем, тому часто про ці галузі захисту даних порівнюють між собою.

Аналіз літератури [1] показує, що в стеганофонії чимало проблем поки що знаходяться на початковій стадії свого вирішення. Актуальним є наукове завдання аналізу підходів щодо оцінки стійкості стеганофонічних систем. Вирішення цього завдання дозволить запропонувати методи підвищення стійкості стеганофонічних систем.

II. Мета роботи

Метою дослідження є аналіз підходів щодо оцінки стійкості стеганофонічних систем.