

Мережевий захист засобами синтаксичного аналізу трафіку

Студент: Медведєв Володимир Євгенович

Керівник: Медведєва Валентина Миколаївна

Мережевий захист засобами синтаксичного аналізу трафіку

Мета: розробка засобів підвищення ефективності мережевого захисту за допомогою застосування методу синтаксичного аналізу трафіку

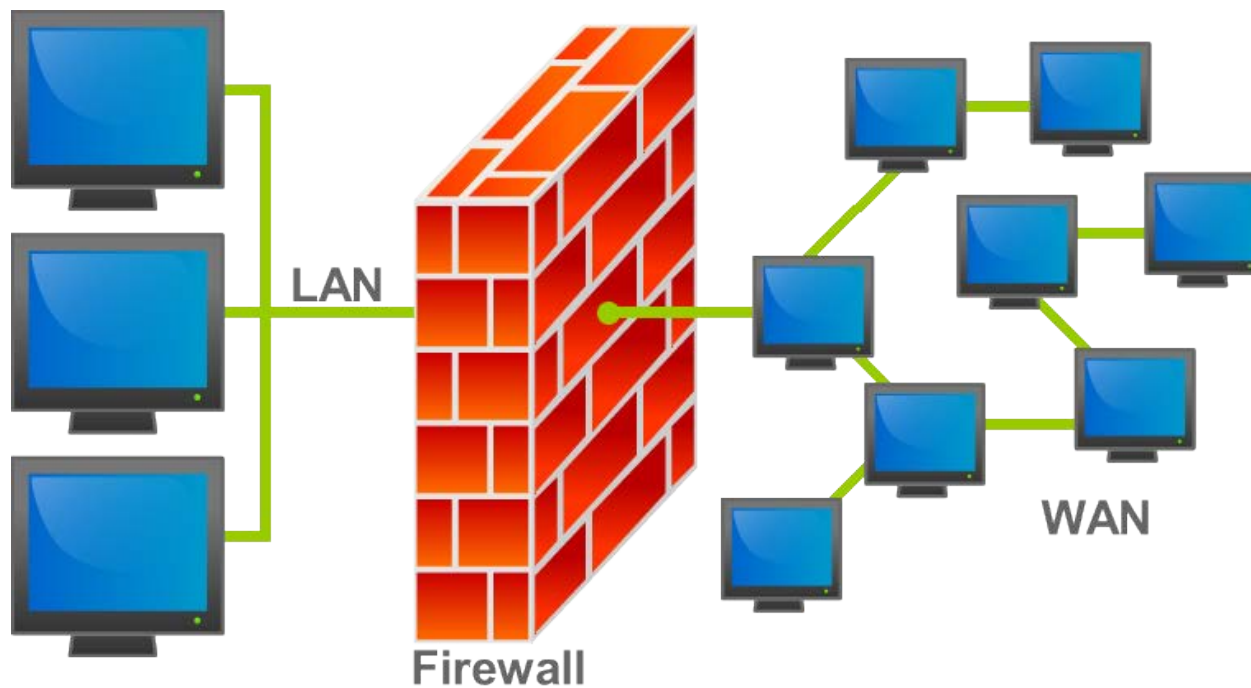
Задачі:

- дослідити засоби мережевого захисту;
- розробити алгоритм синтаксичного аналізу трафіку на основі опису взаємодії протоколів;
- розробити програмний засіб, що реалізує синтаксичний аналіз трафіку.

Об'єктом дослідження є програмне забезпечення мережевого захисту інформації.

Предметом дослідження є програмне забезпечення мережевого захисту засобами синтаксичного аналізу трафіку.

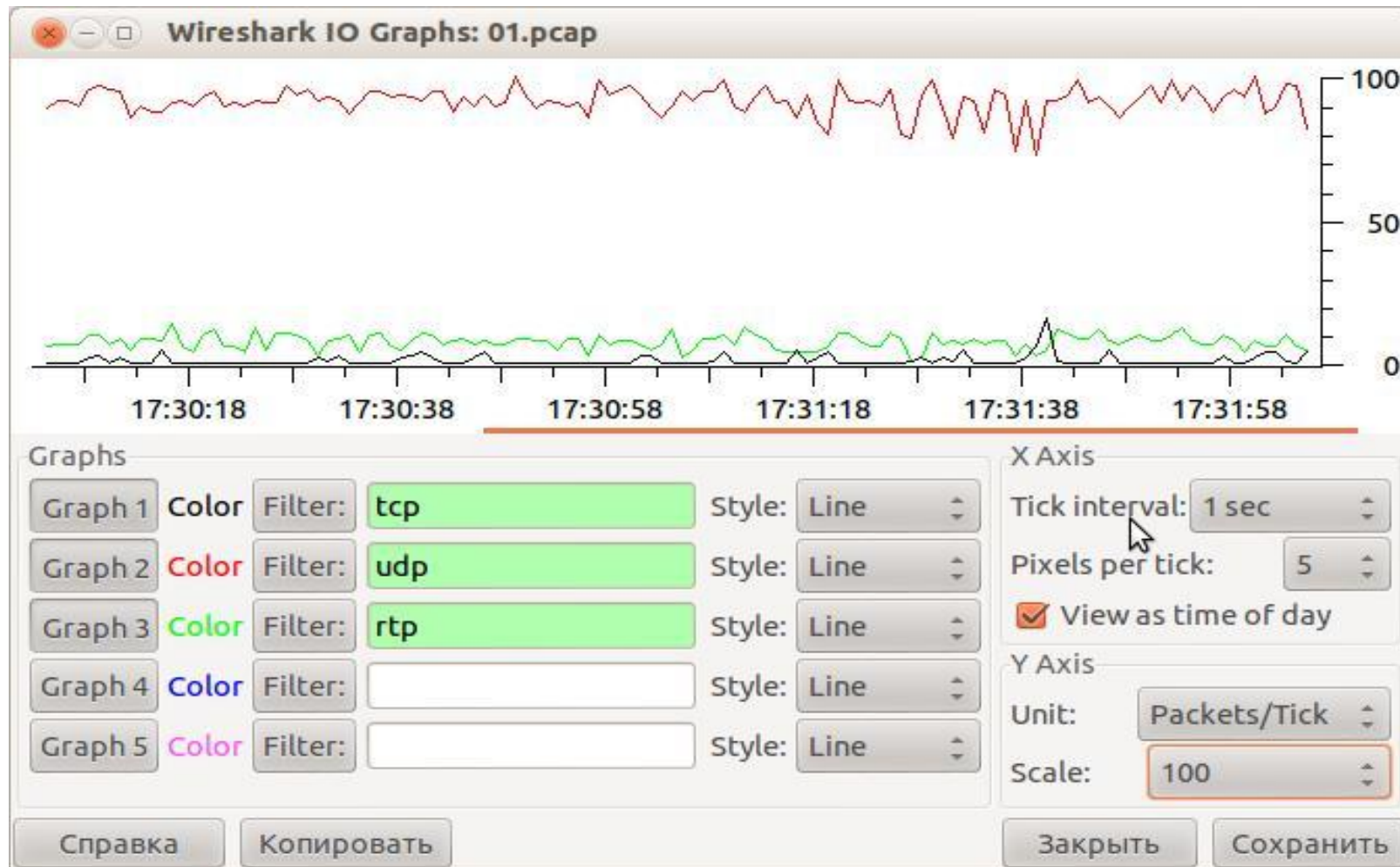
Мережевий екран



WAN (*Wide Area Network*) - глобальна мережа

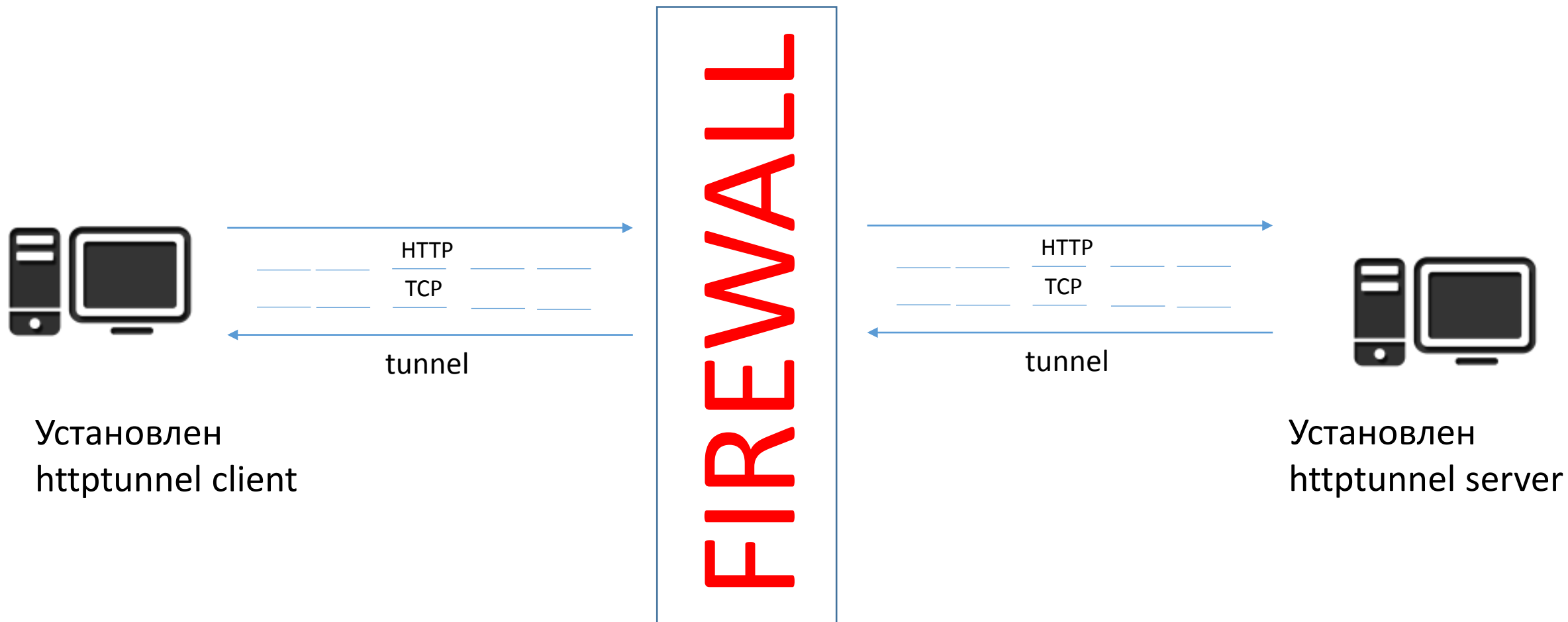
LAN (*Local Area Network*) - локальна комп'ютерна мережа

Статистичні методи виявлення зовнішнього втручання



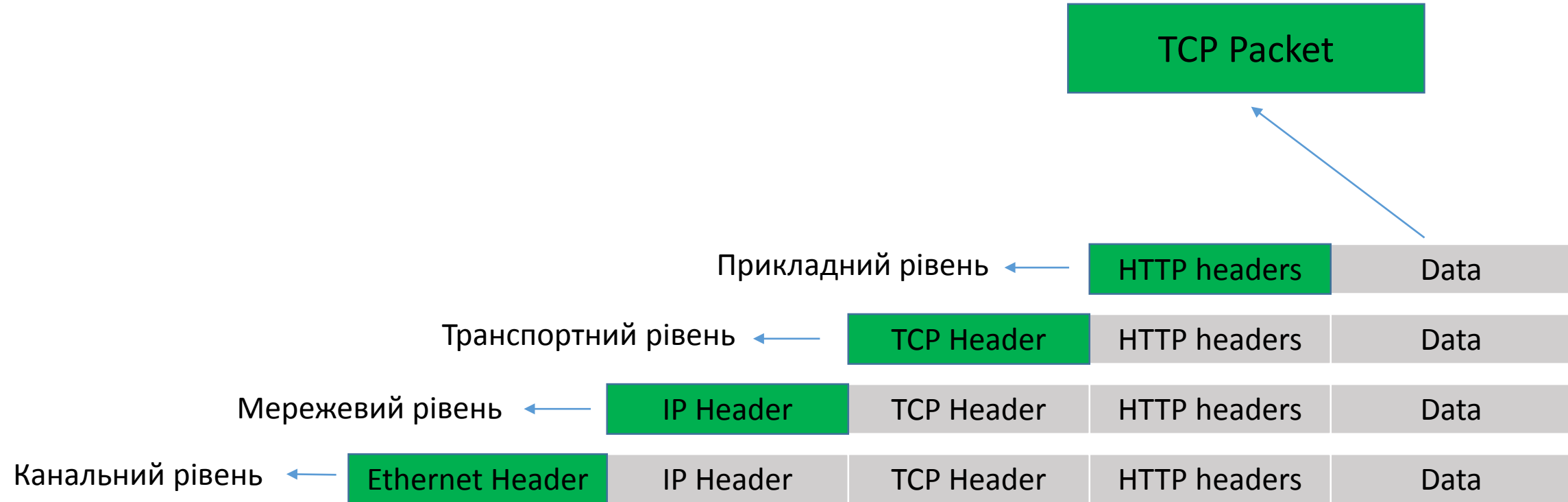
Wireshark, графік

Організація тунелів

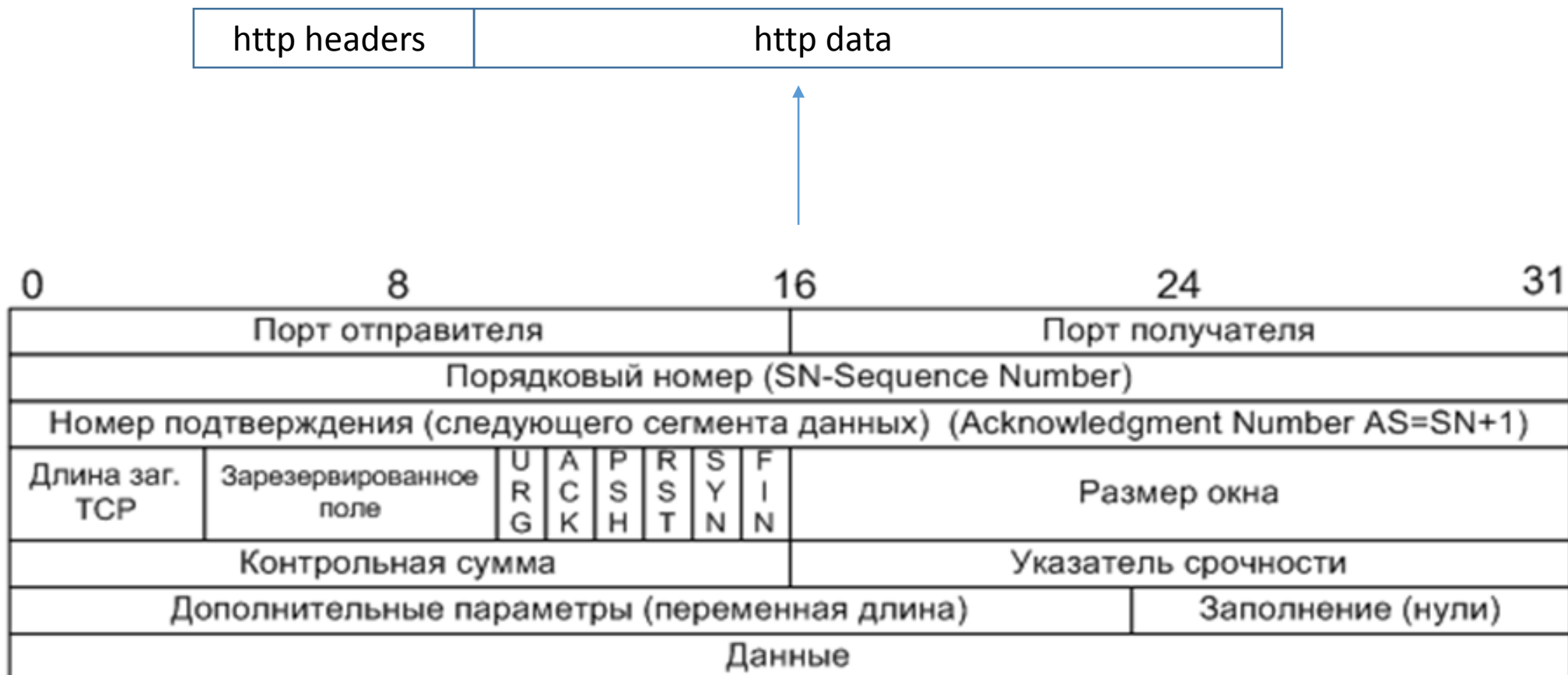


Інкапсуляція протоколів

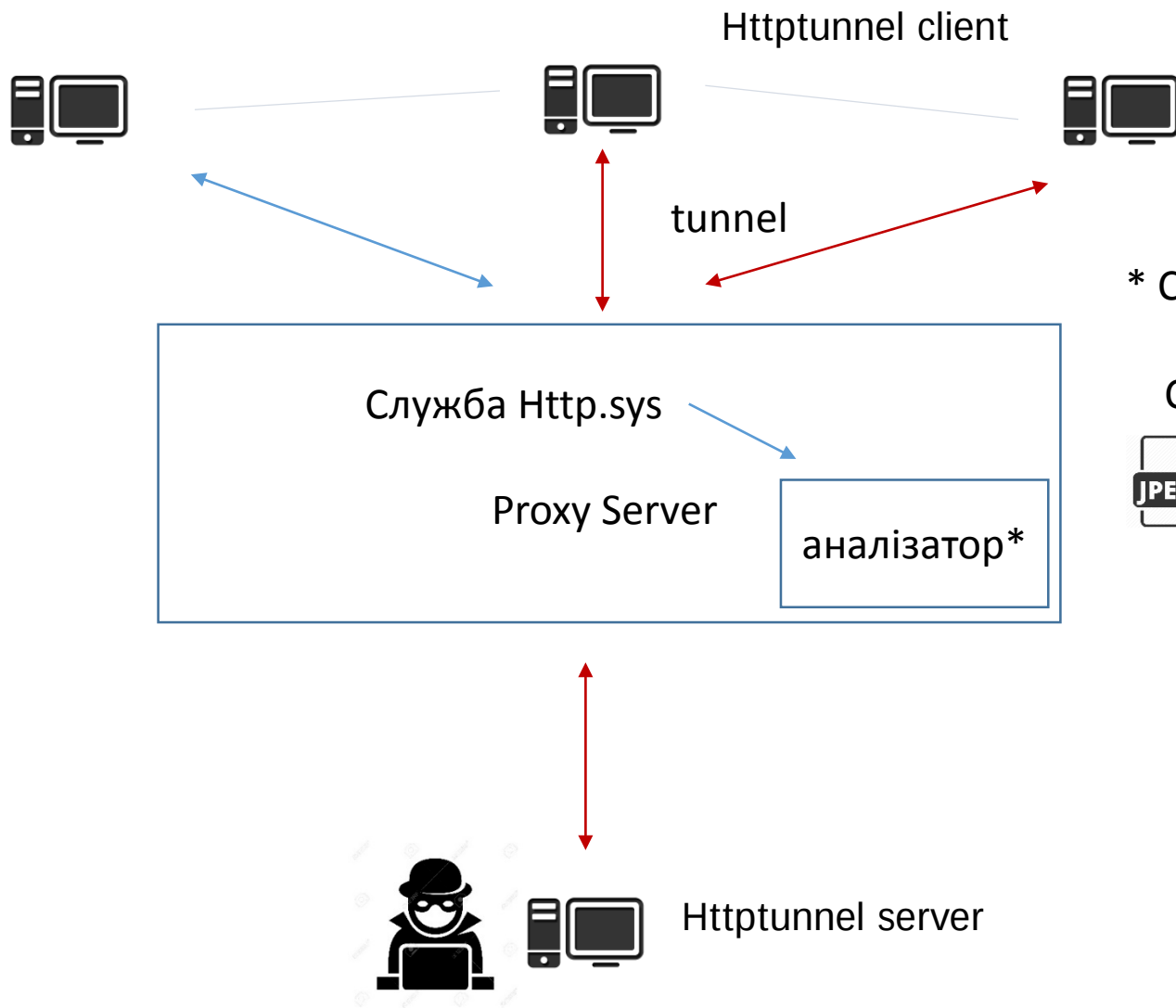
(тунелювання)



Фрагмент ТСП



Синтаксичний аналізатор трафіку

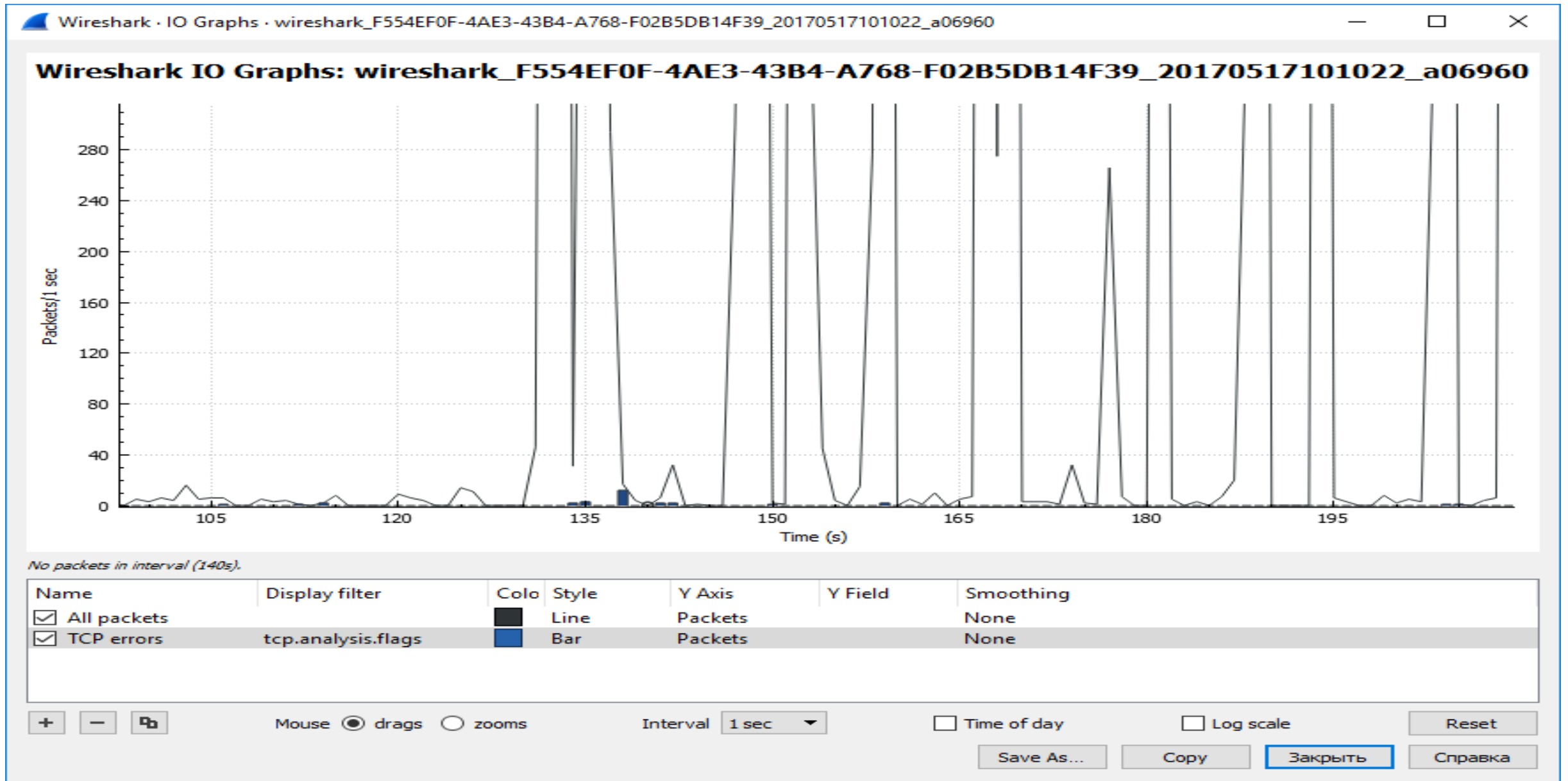


* Синтаксична перевірка формату
протоколу

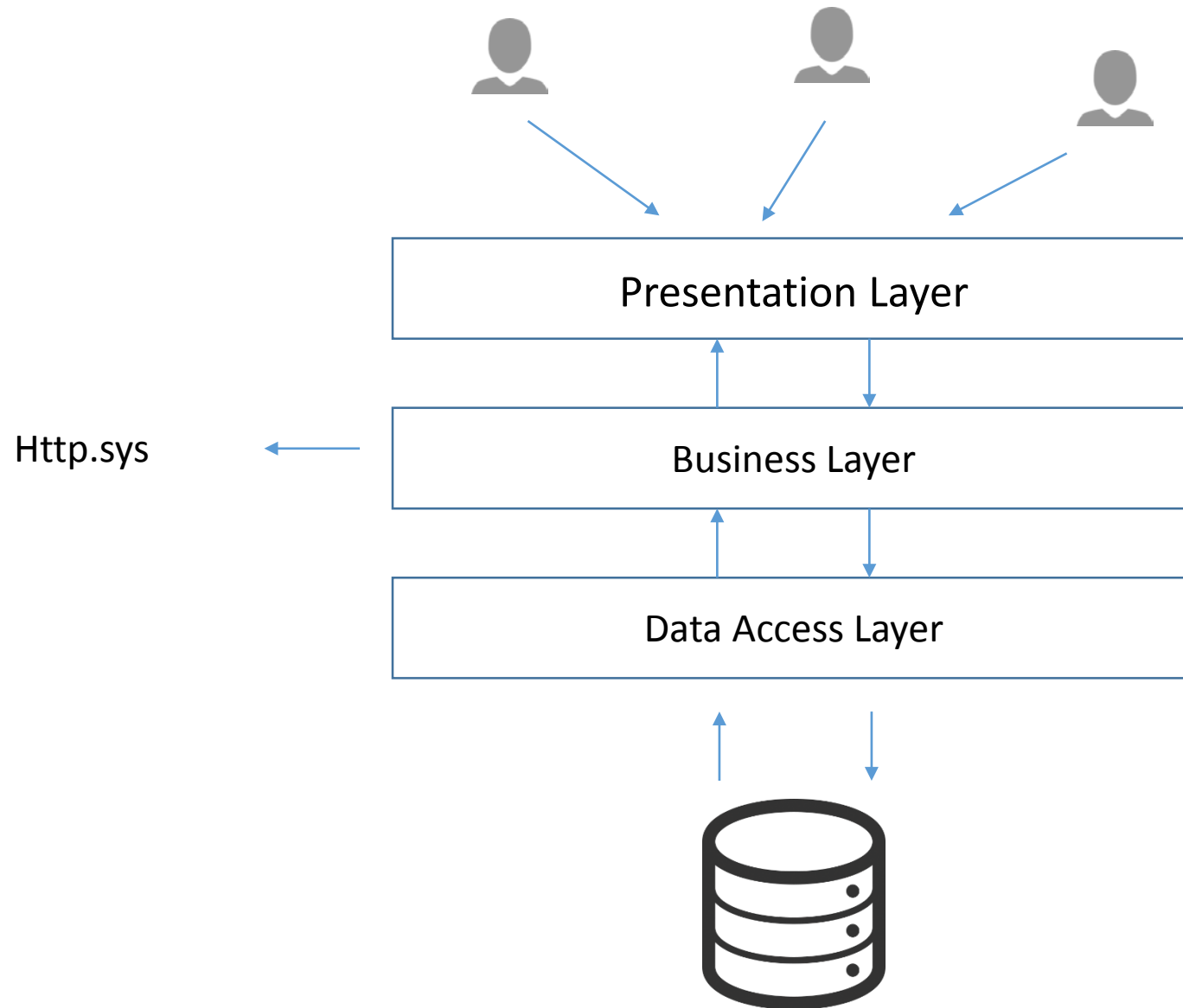
Семантична перевірка даних



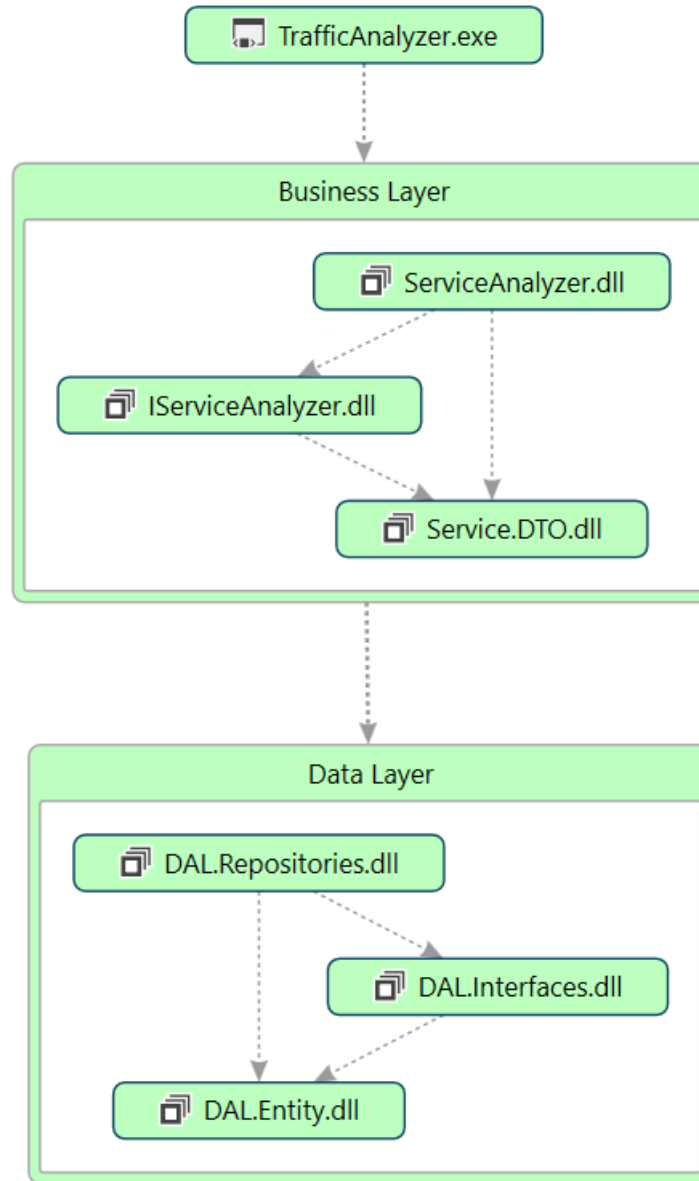
Статичний аналіз мережі при тунелюванні



Архітектура системи



Компоненти системи



Результат виявлення тунелювання

☐ filter Filter Start Stop Clear All ShowBlock							
Source_IP	Source_PORT	Destination_IP	Destination_PORT	TYPE	TIME	TotalLength	
192.168.0.103	64373	216.58.209.46	443	Http	23:51:03	836	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	67	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	104	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	862	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	56	
192.168.0.103	64373	216.58.209.46	443	Http	23:51:03	69	
192.168.0.103	64373	216.58.209.46	443	Http	23:51:03	167	
192.168.0.103	64373	216.58.209.46	443	Http	23:51:03	1021	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	61	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	80	
216.58.209.46	443	192.168.0.103	443	Http	23:51:03	437	

Source_IP	Source_PORT	Destination_IP	Destination_PORT	TYPE	TIME	TotalLength	
192.168.0.103	52112	157.140.2.32	80	Tcp	23:50:31	662	
192.168.0.103	52120	173.194.222.95	443	Tcp	23:50:43	557	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:46	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:46	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:47	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:47	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:48	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:48	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:49	201	
192.168.0.103	56111	239.255.255.250	1900	Tcp	23:50:49	201	
192.168.0.103	52123	172.217.20.172	443	Tcp	23:50:52	247	

Порівняння з існуючими рішеннями

Назва	Розпізнає тунелювання	Розпізнає тунелювання при високих навантаженнях	Легке впровадження	Висока вартість
Firewall				
Stalker Traffic Analyst				
Синтаксичний аналіз				

Висновок

В процесі магістерської роботи були досліджені:

- засоби мережевого захисту;
- засоби обходу мережевого захисту.

та розроблені:

- алгоритм синтаксичного аналізу трафіку на основі опису протоколів;
- програмний засіб мережевого захисту за допомогою синтаксичного аналізу трафіку.

Дякую за увагу

