

Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

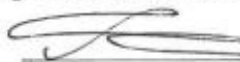
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи бакалавра
на тему: «Підсистема моніторингу подій безпеки
мережевої інфраструктури організації
на базі протоколів сімейства NetFlow»

Виконав студент 3-го курсу групи КБК-19-1
спеціальності 125 «Кібербезпека»

 Рабчинський М.О.

Керівник доцент кафедри КІ та КБ, к.т.н., доцент

 Россінський Ю.М.

Рецензент професор кафедри КІ та КБ, д.т.н., доцент

 Воротніков В.В.

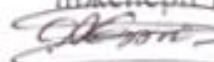
Житомир – 2022

Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки
Спеціальність 125 «Кібербезпека»
Освітня програма «Кібербезпека»

ЗАТВЕРДЖУЮ

Завідувач

кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко
1 березня 2022 р.

ЗАВДАННЯ

на випускну кваліфікаційну роботу бакалавра

Студент: Рабчинський Микита Олегович

Тема роботи: «Підсистема моніторингу подій безпеки мережевої інфраструктури організації на базі протоколів сімейства NetFlow»

затверджена Наказом університету від 1 березня 2022 р. № 128/с

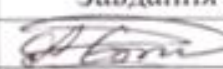
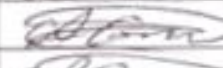
Термін здачі студентом закінченої роботи 10 червня 2022 р.

Вихідні дані роботи (зазначається предмет і об'єкт дослідження):
топологія тестової мережі; проект підсистеми моніторингу подій.

Обладнання та програмне забезпечення:

1. GNS3;
2. Oracle VM VirtualBox;

Консультанти з випускної кваліфікаційної роботи із зазначенням розділів, що їх стосуються

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Єфіменко А.А.	 1.03.2022	 1.03.2022
2	Єфіменко А.А.	 1.03.2022	 1.03.2022
3	Єфіменко А.А.	 1.03.2022	 1.03.2022

Студент
Керівник



Рабчинський М.О.
Росієнський Ю.М.

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	1 березня	
2	Створення плану виконання роботи	13 березня	
3	Огляд та аналіз теоретичного матеріалу	27 березня	
4	Проектування топології тестової мережі	3 квітня	
5	Створення віртуальної моделі мережі	12 квітня	
6	Налаштування підсистеми моніторингу	26 травня	
7	Проведення тестування підсистеми моніторингу	29 травня	
8	Оформлення пояснювальної записки	21 червня	

Студент



Рабчинський М.О.

Керівник



Росенський Ю.М.

АНОТАЦІЯ

Обсяг пояснювальної записки становить 53 сторінок, дипломна робота містить 3 розділи, кількість рисунків – 20, кількість таблиць – 5, кількість найменувань у списку використаних джерел – 30.

Метою даної кваліфікаційної роботи є використання протоколів сімейства NetFlow для створення підсистеми, що зможе працювати у будь-якій мережі, і за допомогою якої буде можливо аналізувати мережевий трафік та виявляти «аномалії».

У першому розділі наведено теоретичні відомості щодо систем перехоплення й аналізу трафіку й відомості про відменності роботи різних протоколів сімейства NetFlow. У другому розділі виконано проектування тестової мережі для подальшого розгортання підсистеми, а також визначено порядок налагодження роботи відповідних протоколів. В останньому розділі проведено налаштування пристроїв мережі й представлено результати тестування роботи підсистеми аналізу трафіку.

Ключові слова: МЕРЕЖА, МОНІТОРИНГ, NETFLOW.

					КІК.КР.Б - 125 - 26 - ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розроб.		Рабчинський М.О.		20.06.19	Підсистема моніторингу подій безпеки мережевої інфраструктури організації на базі протоколів сімейства NetFlow	Лист	Арк.
Керівник		Россицький Ю.М.		20.06.19			4
Реценз.		Воротніков В.В.		20.06.19			50
Н. контр.		Россицький Ю.М.		20.06.19		ФІКТ, Гр. КБК-19-1	
Затверд.		Сфіменко А.А.		20.06.19			

ANNOTATION

The volume of the explanatory note is 53 pages, the thesis contains 3 sections, the number of figures – 20, the number of tables – 5, the number of names in the list of sources used – 30.

The purpose of this qualification is to use the NetFlow family of protocols to create a subsystem that can run on any network, and through which it will be possible to analyze network traffic and detect "anomalies".

The first section provides theoretical information on traffic interception and analysis systems and information on the differences in the performance of different protocols of the NetFlow family. In the second section the design of the test network for further deployment of the subsystem is performed, and also the order of adjustment of work of the corresponding protocols is defined. In the last section, the network devices are configured and the results of testing the operation of the traffic analysis sub-system are presented.

Keywords: NETWORK, MONITORING, NETFLOW.

		<i>Рабчинський М.О.</i>			<i>КІК.КР.Б - 125 - 26 - ПЗ</i>	<i>Арк.</i>
		<i>Росієнський Ю.М.</i>				
<i>Змн.</i>	<i>Арк.</i>	<i>№ докум.</i>	<i>Підпис</i>	<i>Дата</i>		<i>5</i>

ЗМІСТ

ВСТУП	9
РОЗДІЛ 1 ОГЛЯД ТЕОРЕТИЧНИХ ВІДОМОСТЕЙ ЩОДО ЗДІЙСНЕННЯ АНАЛІЗУ ТРАФІКУ	10
1.1 NTA або системи аналізу трафіку	10
1.2 Світовий ринок network traffic analysis.....	12
1.2.1 Awake Security Platform	12
1.2.2 Darktrace Enterprise Immune System	13
1.2.3 Positive Technologies Network Attack Discovery	14
1.2.4 Cisco Stealthwatch	15
1.3 Опис протоколу моніторингу трафіку netflow.....	17
1.3.1 Переваги і недоліки	18
1.3.2 Склад системи обробки інформації, зібраної за допомогою NetFlow	19
1.4 Опис протоколів сімейства netflow	20
1.4.1 Netflow V5	20
1.4.2 Netflow V9	20
1.4.3 Flexible Netflow	21
1.4.4 NSEL	21
1.4.5 IPFIX	22
1.4.6 Jflow, Netstream.....	23
1.4.7 sFlow	23
1.5 Огляд існуючих flow аналізаторів	25
1.5.1 PRTG Network Monitor.....	25
1.5.2 Scrutinizer	26
1.5.3 nProbe and ntopng.....	27
1.5.4 Solarwinds NetFlow Traffic Analyzer	28
1.6 Постановка технічного завдання.....	30
РОЗДІЛ 2 ПРОЕКТУВАННЯ ТЕСТОВОЇ МЕРЕЖІ Й ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ.....	31

2.1	Проектування загальної топології мережі для реалізації підсистеми моніторингу подій.....	31
2.2	Опис локальних мереж.....	32
2.3	Проектування системи моніторингу подій	34
2.4	Розробка схеми адресації мережі	35
РОЗДІЛ 3 НАЛАГОДЖЕННЯ ПРИСТРОЇВ МЕРЕЖІ Й ПРОВЕДЕННЯ		
	ТЕСТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ	38
3.1	Налагодження пристроїв мережі.....	38
3.2	Налагодження підсистеми моніторингу подій	43
3.3	Тестування системи моніторингу подій.....	45
ВИСНОВКИ.....		48
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ		49
ДОДАТКИ.....		52

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				7
Змн.	Арк.	№ докум.	Підпис	Дата		

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

NTA (Network Traffic Analysis) – Системи аналізу трафіку;

SOC (Security Operations Center) – Центр забезпечення безпеки;

SIEM (Security Information And Event Management) – управління інформацією про безпеку й управління подіями безпеки;

APT (Advanced Persistent Threat) – Постійна серйозна загроза;

EDR (Endpoint Detection & Response) – Виявлення кінцевих точок та реагування на них;

LDAP (Lightweight Directory Access Protocol) – Легковажний протокол доступу до каталогів;

IPFIX (IP Flow Information Export) – Експорт інформації по IP потоку;

DSCP (Differentiated Services Code Point) – Точка коду диференційованих послуг;

BGP (Border Gateway Protocol) – Протокол граничного шлюзу;

CoS/ToS (Type of Service) – Тип обслуговування;

QoS (Quality of Service) – Якість обслуговування, технологія надання різним класам трафіку різних пріоритетів в обслуговуванні;

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				8
Змн.	Арк.	№ докум.	Підпис	Дата		

ВСТУП

Актуальність теми. Домашня або корпоративна мережа може почати збоїти отже під час здійснення адміністрування комп'ютерних мереж може з'явитися потреба у виявленні певних проблем з мережею: проблеми з передачею файлів, загальні затримки мережі, конфліктність адрес тощо. У таких випадках необхідні програмний аналіз та виправлення несправностей. Одним з засобів виявлення несправностей є аналіз трафіку на певних вузлах мережі.

Метою кваліфікаційної роботи є використання протоколів сімейства Net-Flow для створення підсистеми, що зможе працювати у будь-якій мережі, і за допомогою якої буде можливо аналізувати мережевий трафік та виявляти «аномалії».

Визначена мета обумовлює наступні завдання:

- Створення прикладу мережі для проведення розгортання підсистеми.
- Проектування й розгортання системи аналізу трафіку.
- Виконання перехоплення трафіку для проведення тестування підсистеми.

Об'єктом дослідження є процес забезпечення надійності роботи мереж й підвищення швидкості реагування на негативні події в мережі.

Предметом дослідження є аналіз трафіку, що проходить крізь мережу підприємства.

У процесі виконання кваліфікаційної роботи було розроблено проект тестової мережі, а також підсистему моніторингу подій з використанням сенсорів та віддаленого аналізатору.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				9
Змн.	Арк.	№ докум.	Підпис	Дата		

РОЗДІЛ 1 ОГЛЯД ТЕОРЕТИЧНИХ ВІДОМОСТЕЙ ЩОДО ЗДІЙСНЕННЯ АНАЛІЗУ ТРАФІКУ

1.1 NTA або системи аналізу трафіку

Історично інспекцією трафіку займаються системи виявлення вторгнень (Intrusion Detection Systems, IDS). Однак вони функціонують лише в режимі реального часу, тому за їх допомогою неможливо побачити атаки в минулому, просто підвантаживши нові сигнатури загроз та індикатори компрометації. Крім того, IDS-рішення зазвичай не застосовуються для виявлення небезпечної та підозрілої активності у внутрішньомережевих інформаційних потоках. У тих випадках, коли вони все ж таки використовуються для аналізу внутрішнього трафіку (переважно – за допомогою сигнатурних методів), у «сліпій зоні» залишаються приховані канали передачі даних, переміщення зловмисника по мережі та його закріплення в ній, несанкціонований доступ до мережевих сервісів (у в тому числі - за допомогою легітимних інструментів) та всілякі нові техніки атакуючих.

Крім того, просто виявити проблему недостатньо. Необхідне оперативне розслідування інциденту та ефективне реагування. Зловмисники можуть діяти та закріплюватися в інфраструктурі жертви дуже швидко, тому важливо скоротити час між виявленням атаки та відгуком на неї.

Системи класу Network Traffic Analysis (NTA) призначені для перехоплення та аналізу мережного трафіку, а також для виявлення складних та цільових атак. З їхньою допомогою можна проводити ретроспективне вивчення мережевих подій, виявляти та розслідувати дії зловмисників, реагувати на інциденти. NTA можуть бути відмінним джерелом даних для оперативних центрів інформаційної безпеки (SOC).

Це нова категорія систем мережевої безпеки, які не тільки служать джерелами даних для центрів моніторингу (SOC), але й забезпечують потужні можливості ретроспективного пошуку, розслідування інцидентів, централізованої протидії шкідливій активності.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		10

Рішення класу NTA відстежують трафік та комунікації всередині корпоративної мережі та застосовують різні техніки (поведінковий аналіз, машинне навчання) для того, щоб швидко виявити, проаналізувати та обробити загрози, які інакше залишалися б прихованими. NTA може застосовуватися в мережах будь-якого масштабу, так само як і будь-якої архітектури: локальної, хмарної, гібридної.

Інтеграція з EDR- та SIEM-рішеннями забезпечує безшовну кореляцію даних. У такій схемі NTA відповідає за видимість інформації, що передається по мережі, EDR постачає відповідні відомості від кінцевих точок, а SIEM агрегує журнали подій.

Основні функції NTA-рішень:

- аналіз трафіку як на периметрі мережі, так і всередині інфраструктури;
- виявлення атак за допомогою комбінації технологій виявлення;
- допомога у розслідуванні інцидентів.

Як правило, типова архітектура NTA-рішень включає:

- мережевий сенсор, який збирає трафік;
- сервери централізованого керування;
- консоль моніторингу (дашборд).

Використання NTA дозволить:

- підвищити ефективність обробки складних інцидентів за рахунок додаткової видимості кінцевих точок, можливості проактивного пошуку загроз та наочного подання інформації про виявлені події у мережі;
- збагатити базу SOC попередньо обробленими релевантними даними для зіставлення з журналами, що надходять з інших джерел, для ефективного розслідування;
- значно скоротити кількість годин, що витрачаються аналітиками на завдання, пов'язані з перевіркою даних від робочих місць та серверів, а також із реагуванням на інциденти.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		11

Деякі рішення NTA поєднують можливості пошуку проблем безпеки з автоматизованими завданнями щодо реагування на ризики та пом'якшення наслідків інцидентів. Інструменти цього типу постійно шукають у мережі підозрілі чи шкідливі дані. Якщо в результаті сканування вдалося виявити щось, то NTA діагностує проблему, щоб визначити, в чому саме полягає загроза безпеці. Виходячи з цього діагнозу, продукт розгортає автоматизовані завдання, щоб допомогти нейтралізувати проблему, одночасно оповіщаючи відділ ІБ або SOC про неї.

Мета автоматизованих завдань – спробувати вирішити ситуацію без участі людини. Це скорочує час між пошуком та зняттям проблеми безпеки, дозволяючи команді фахівців вирішувати інші важливі питання.

1.2 Світовий ринок network traffic analysis

Network Traffic Analysis – це відносно новий ринковий сегмент, на який з 2016 року входять багато вендорів. У 2019 році компанія Gartner проводила дослідження рішень класу Network Traffic Analysis. Результати зосереджені у звіті "Market Guide for Network Traffic Analysis", згідно з яким на світовому ринку можна виділити наступних рішення.

1.2.1 Awake Security Platform

Платформа Awake Security розроблена компанією Awake (Саннівейл, Каліфорнія, США). Рішення використовує комбінацію контрольованого та неконтрольованого машинного навчання та інших аналітичних методів для виявлення підозрілого трафіку. Платформа може бути розгорнута за принципом "все-в-одному" (сенсор та аналітика в одному блоці) або розподіленим способом, де сенсор та аналітичний центр розділені. Сенсор може функціонувати як фізичний або віртуальний пристрій у локальних та промислових мережах, а також у хмарі для захисту робочих навантажень Amazon Web Services (AWS), Microsoft Azure та Google Cloud Platform (GCP).

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		12

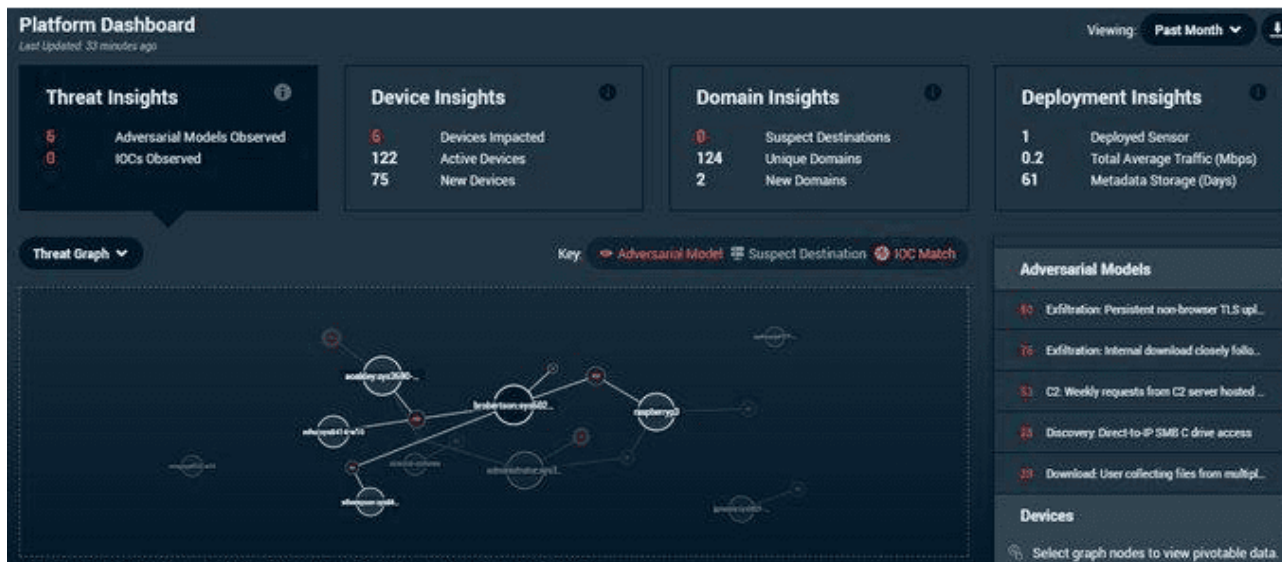


Рисунок 1.1 – Консоль моніторингу в Awake Security Platform

Awake використовує машинне навчання для пошуку загроз у зашифрованих даних без необхідності декодування. При цьому Awake не забезпечує розшифровку трафіку SSL/TLS.

Використовуваний підхід Awake Security полягає у взаємодії з рішеннями з оркестрації (Splunk Adaptive Response, Demisto тощо) або захист кінцевих точок (Carbon Black) для виконання карантину або запуску програм відновлення. Наприклад, клієнти використовують ці механізми, щоб блокувати домени та IP-адреси у брандмауері або проксі-сервері та переводити пристрої в автономний режим.

1.2.2 Darktrace Enterprise Immune System

Платформа Enterprise Immune System розроблена британською ІБ-компанією Darktrace зі штаб-квартирою в Кембриджі, Великобританія та Сан-Франциско, США.

Enterprise Immune System вміє спостерігати за мережевою активністю користувачів та пристроїв, у режимі реального часу, виявляючи аномалії на основі поведінкового аналізу. За заявою виробника, його розробка здатна виявляти інсайдерську активність, автоматизовані атаки та інші невідомі загрози. Рішення існує у вигляді фізичного пристрою або віртуальної машини.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		13

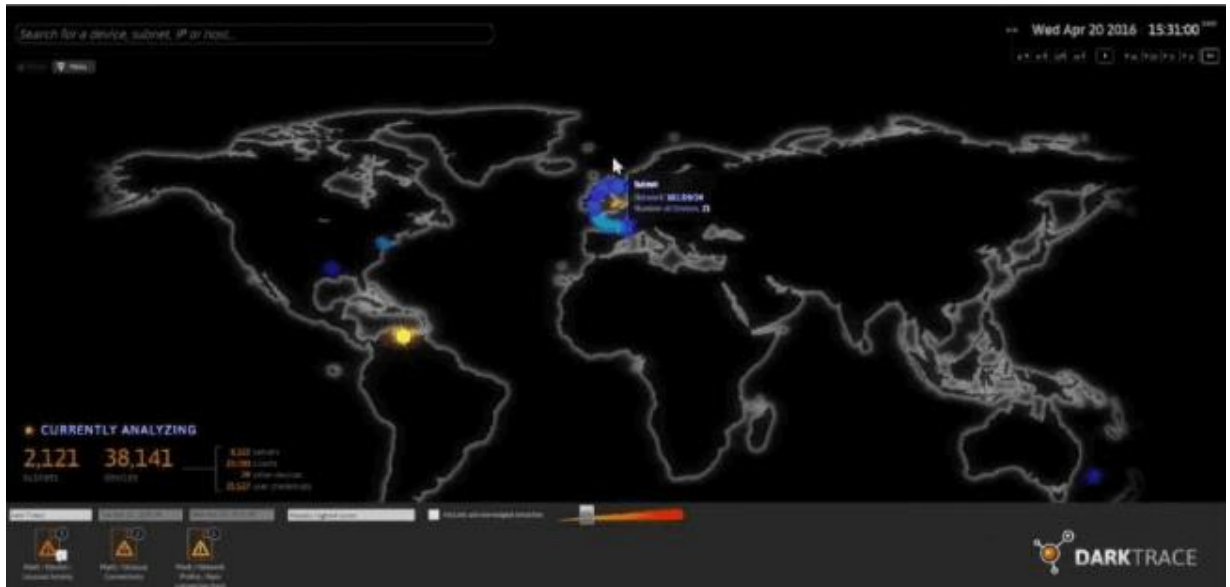


Рисунок 1.2 – Консоль оператора в Darktrace Enterprise Immune System

Enterprise Immune System вміє не тільки контролювати весь трафік, але й диференціювати активність, відокремлюючи небезпечні процеси від нормальних операцій, здійснення яких вимагає виробнича діяльність. Оскільки швидкість інсайдерської атаки може наростати швидко, платформа здатна автоматично блокувати загрозу.

1.2.3 Positive Technologies Network Attack Discovery

Рішення PT Network Attack Discovery створено компанією Positive Technologies, що спеціалізується на розробці ПЗ та наданні сервісів в області кібербезпеки, і є системою глибокого аналізу мережевого трафіку (NTA) для виявлення атак на периметрі мережі і всередині неї.

PT Network Attack Discovery аналізує потоки даних на периметрі та в інфраструктурі, виявляє активність зловмисників навіть у зашифрованому трафіку та допомагає у розслідуваннях. Також продукт здатний виявити порушення регламентів ІБ, порівняти події з техніками та тактиками зловмисників за матрицею MITRE ATT&CK, допомогти при вибудовуванні процесу Threat Hunting (проактивного пошуку загроз).

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				14
Змн.	Арк.	№ докум.	Підпис	Дата		

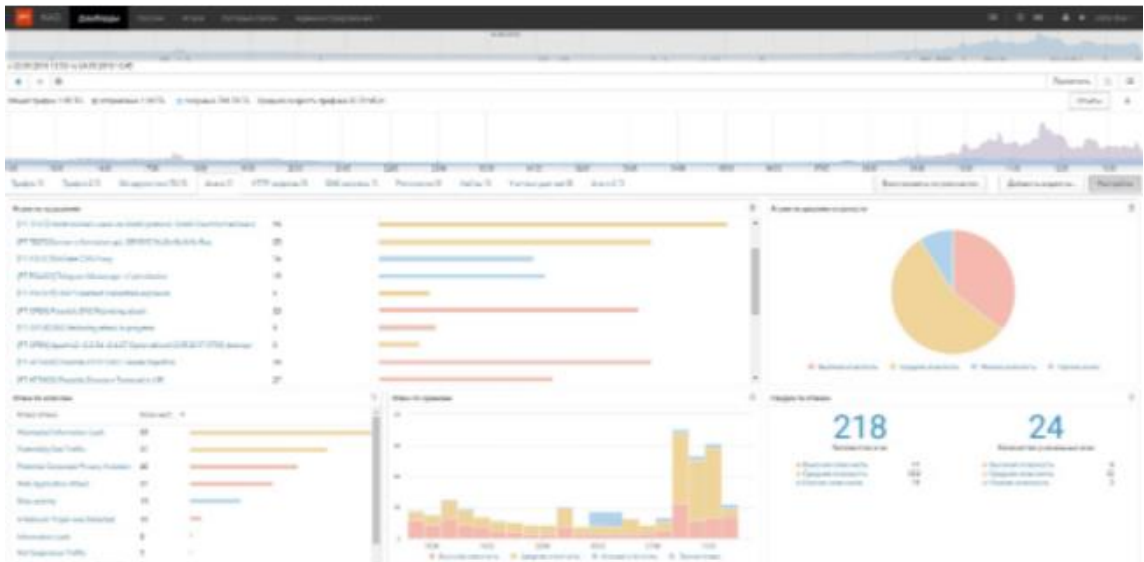


Рисунок 1.3 – Консоль моніторингу у PT Network Attack Discovery

На даний момент у базі знань PT NAD – понад 5 000 правил детектування та 20 000 індикаторів компрометації. Нові правила та індикатори двічі на тиждень надходять від фахівців експертного центру безпеки Positive Technologies (PT Expert Security Center).

Продукт виявляє горизонтальне переміщення злоумисника всередині периметра, активність шкідливих програм, спроби приховати дії від засобів захисту, експлуатацію вразливостей та використання хакерського інструментарію.

1.2.4 Cisco Stealthwatch

Американська компанія Cisco Systems розробила рішення Stealthwatch для аналізу трафіку з метою виявлення загроз та реагування на них. Cisco Stealthwatch – це засіб моніторингу ІБ в мережі, який базується на зборі телеметричних даних з різних пристроїв: міжмережевих екранів, маршрутизаторів, комутаторів, серверів з віртуальними машинами, кінцевих точок.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				15
Змн.	Арк.	№ докум.	Підпис	Дата		



Рисунок 1.4 – Консоль моніторингу у Cisco Stealthwatch

Основні функції цієї системи:

- Збір та аналіз трафіку NetFlow з пристроїв будь-яких виробників, у тому числі з тих, що не підтримують цей протокол;
- Виявлення в реальному часі як зовнішніх, так і внутрішніх загроз мережі;
- Можливість аналізувати та виявляти аномальний вміст трафіку, у тому числі шифрованого;
- Прискорення реагування на інциденти та проведення технічної експертизи;
- Спрощення сегментації мережі під час інтеграції з платформою Cisco Identity Services Engine;
- Інтеграція як із продуктами Cisco (ISE, TrustSec), так і із зовнішніми системами (Active Directory, проксі-сервери);
- Виявлення порушення внутрішніх політик мережевої безпеки;
- Можливість виявлення несанкціонованої мережевої активності;
- Використання багаторівневого машинного навчання виявлення нових видів загроз;
- Виявлення розповсюдження шкідливого коду.

Архітектура рішення включає компоненти Stealthwatch Management Console та Flow Collector. Доступні також додаткові елементи: Flow Sensor та UDP Director.

Як основний протокол збору даних про телеметрію рішення Cisco Stealthwatch використовує NetFlow/IPFIX. Розширену інформацію про контекст безпеки надають хмарні служби виробника, що містять бази даних IP/URL-репутацій, та окреме рішення Cisco ISE.

Cisco Stealthwatch також дозволяє контролювати хмарні середовища та мобільні пристрої. Продукт відстежує кожен хост і користувача, записує всі дії в мережі (у тому числі – бачить мережевий трафік на рівні сигнатур додатків), відстежує відхилення від «нормальної» поведінки, забезпечує зберігання цих даних і здатний робити вибірки з них, включаючи аналіз підозрілої активності. Рішення містить понад сто різних алгоритмів виявлення аномалій та поведінки, що дозволяє йому попереджати адміністраторів ІБ про будь-які зміни. Також Cisco Stealthwatch можна використовувати як інструмент постійного аудиту працездатності традиційних захисних засобів або для розслідування шляхів розповсюдження шкідливого коду та векторів атаки.

1.3 Опис протоколу моніторингу трафіку netflow

NetFlow – це протокол, розроблений компанією Cisco Systems, також відомий як стандарт IPFIX – компонент Cisco IOS. Протокол NetFlow працює на IP-пристроях (маршрутизаторах, комутаторах 3-го рівня) та надає статистику IP-трафіку. Ряд виробників упровадили цей стандарт (напр., Juniper випустила аналогічне рішення під назвою jFlow). Інші компанії (напр., HP, Foundry та Extreme) використовують технологію контролю потоку даних sFlow.

Система візуалізує не тільки параметри TCP/IP на 3-му та 4-му рівні (IP-адреса джерела, цільова IP-адреса, протокол, порт), але й додаткові атрибути трафіку (Type of Service, DSCP, ідентифікатор джерела та цільові області) автономних систем у протоколі BGP) та додаткову інформацію про маршрутизацію

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		17

та трафік – наступна транзитна ділянка, вхідні та вихідні інтерфейси, мережна адреса джерела та цільова мережна адреса.

Незважаючи на свою назву, NetFlow охоплює значний обсяг даних та є багатим джерелом інформації, що оновлюється в режимі реального часу; ця інформація доступна у будь-який час і містить багато відомостей про трафік мережі.

1.3.1 Переваги і недоліки

Технологія NetFlow дозволяє виявляти проблеми, вузькі місця в мережі, перевіряти налаштування класів трафіку (CoS/ToS), визначати надісланий трафік та програми, а також дозволяє прив'язати його до певного користувача в певний період. Більше того, NetFlow як технологія, інтегрована в Cisco IOS, не вимагає використання додаткових пристроїв або придбання ліцензій. Більшість платформ Cisco, починаючи з маршрутизаторів Cisco ISR, сумісні з NetFlow.

Головна перевага NetFlow у тому, що при грамотному використанні можна створити відносно недорогою та просту систему моніторингу мережевого трафіку. Єдині витрати будуть пов'язані з придбанням програми візуалізації даних.

Крім того, за допомогою NetFlow можна моніторити будь-який канал мережі. Оскільки налаштування NetFlow на маршрутизаторі виконується на програмному рівні, можна вибірково активувати його моніторингові пристрої, а також інші критичні пристрої (напр. на концентраторі, на маршрутизаторі, який забезпечує підключення до Інтернету або у місцях, де виникають проблеми в мережі).

Більше того, NetFlow – це відкритий протокол, тому він підтримує ряд сторонніх програм для моніторингу мережі в режимі реального часу, створення звітів та зіставлення користувачів у мережі. Зазвичай програми розробляються під індивідуального клієнта та конкретні вимоги.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		18

Однак, без відповідних інструментів для обробки даних NetFlow не особливо корисний. Його користь та роль в управлінні продуктивністю мережі залежать від способу отримання даних ІТ-фахівцями. Враховуючи обсяг доступної інформації, немає сенсу аналізувати дані з погляду їх потоку окремо взятого елемента мережі. Для повноцінного використання протоколу NetFlow необхідно зібрати зовнішню базу даних та забезпечити інтуїтивний інтерфейс, що дозволить знайти інформацію, яка нас цікавить, та аномальну активність мережі, а також допоможе розпланувати розширення мережевої інфраструктури.

Переваги використання системи на основі NetFlow:

- Підвищена безпека мережі – моніторинг мережної активності є одним із ключових елементів забезпечення безпеки. За допомогою інтерфейсу систем візуалізації можна виконувати сканування портів, виявляти DoS-атаки та перемикання між IP-адресами.
- Можливість повного відображення мережного трафіку та його джерела дозволяє виявляти незаконні дії та уникнути великих штрафів (напр., за використання неліцензійного ПЗ).
- Планування розвитку мережі – визначення моделей трафіку та адаптація до ширини каналу до того, як мережа досягне максимальної пропускної спроможності.
- Прискорене вирішення проблем (напр., за допомогою оптимізації налаштувань QoS для правильної пріорітизації важливих програм, що забезпечує більш швидку відповідь).

1.3.2 Склад системи обробки інформації, зібраної за допомогою NetFlow Агент NetFlow

Агент NetFlow збирає дані про трафік, що проходить через мережеві пристрої та відправляє їх у центральне сховище (так званий колектор). Фактично, будь-який маршрутизатор Cisco, на якому встановлено програмне забезпечення IOS (починаючи з версії 12.3T і вище, NetFlow доступний у функціоналі SP Services), можна використовувати як агент. Комутатори Catalyst 6500 також

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		19

підтримують протокол NetFlow, а в комутаторі Catalyst 4500 він вбудований як додаткова функція.

Колектор NetFlow

Колектор NetFlow отримує інформацію від агентів. Враховуючи великий обсяг даних, колектор зазвичай фільтрує, агрегує та видаляє дані перед поміщенням їх у базу.

Модуль візуалізації

Модуль візуалізації використовується для представлення даних, що зібрані в колекторі NetFlow. Він підтримує ряд функцій, таких як забезпечення мережевого планування, зіставлення користувачів або моніторинг трафіку.

1.4 Опис протоколів сімейства netflow

Спочатку Cisco розробляв протокол для своїх рішень. Інші виробники наслідували такий підхід і створили більш-менш схожі формати даних flow.

1.4.1 Netflow V5

Першою широко використовуваною версією був протокол NetFlow v5, який став доступним у 2006 році. Він досі є найпоширенішим, і підтримується рядом роутерів. Тим не менш, він уже не відповідає вимогам точного flow-моніторингу, і він не підтримує IPv6 трафік, адресу MAC, VLAN та інші розширення.

Формат пакетів NetFlow v5 є фіксованим, завжди однаковим, і його легко розшифрувати. Усі потоки враховуються, коли вони надходять на інтерфейс (тобто inBound). Про вихідний трафік повідомляється за допомогою потоків inBound з інших інтерфейсів. Через це зазвичай рекомендується ввімкнути NetFlow v5 на всіх інтерфейсах пристрою, інакше використання вихідних даних на деяких інтерфейсах може бути заниженим.

1.4.2 Netflow V9

NetFlow v9 отримав кілька додатків. Найважливіший з них – підтримка шаблонів, яка дозволяє здійснювати експорт flow, що настраюється, і забезпечує те, що NetFlow може бути адаптований для підтримки нових протоколів.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		20

Інші доробки пов'язані з появою підтримки IPv6, Virtual Local Area Networks (VLANs) та Multiprotocol Label Switching (MPLS) та інших функцій. NetFlow v9 використовується в більшості сучасних роутерів та комутаторів Cisco. NetFlow v9 набирає все більшої популярності на ринку, хоча й повільно.

1.4.3 Flexible Netflow

Cisco продовжує працювати над технологією NetFlow. Наступне покоління отримує назву Flexible NetFlow і незабаром має розширення NetFlow v9. Все, що може експортувати NetFlow, стає налаштованим під вимоги користувача, що дозволяє клієнтам експортувати практично будь-які дані, які проходять через роутер.

Flexible NetFlow (FnF) – технологія моніторингу IP-потоків наступного покоління, розроблена компанією Cisco. Тут запроваджуються дві нові концепції моніторингу потоків. По-перше, допускається використання шаблонів, а по-друге, користувач має можливість «заглянути» в пакети досить глибоко і вибрати для моніторингу поля, що цікавлять його. Як правило, NetFlow відстежує в IP-потоці такі поля: IP-адреси, порти, протоколи, прапори TCP. Flexible NetFlow дозволяє вибирати із заголовка IP майже всі поля, всі типи прапорів TCP та іншу інформацію, у тому числі теги VLAN та URL.

Аналізуючи цю інформацію, більшість систем безпеки шукають аномалії чи зміни у мережевому поведінці виявлення інцидентів. Flexible NetFlow дозволяє відстежувати широкий спектр IP-інформації, включаючи всі поля заголовка IPv4 або IPv6, а також індивідуальні прапори TCP. Експортувати можна навіть розділи пакета, а в інформацію, що відстежується, включати як ключові поля (використовувані для створення потоку), так і не ключові (збираються з потоком). При необхідності, на додаток до кешу NetFlow для виявлення вразливостей у системі безпеки (виявлення аномалій), користувач може створити інший, щоб сфокусуватися на конкретній проблемі.

1.4.4 NSEL

NSEL (NetFlow Security Event Logging) дозволяє експортувати інформацію брандмауера із сімейства пристроїв Cisco ASA, що забезпечують захист

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		21

мережі. Він використовує протокол NetFlow, але запитує іншу інтерпретацію та має інші випадки застосування: мета NSEL – це відстеження подій та журналів міжмережевого екрану через NetFlow.

Таким чином, коли ви налаштовуєте ASA для експорту NetFlow, ви вибираєте, які події хочете відстежувати за допомогою колектора NetFlow. Наразі існує три типи подій для моніторингу:

- Flow Create;
- Flow Denied;
- Flow Teardown.

На відміну від кожного маршрутизатора, що експортує NetFlow v9; під час моніторингу типів подій для вашого ASA існує кілька унікальних шаблонів, які можна експортувати для цієї події. Наприклад, за допомогою події FLOW CREATE є чотири можливі шаблони, які можна експортувати. Два шаблони пов'язані з використанням адрес IPv4. Два пов'язані з IPv6.

1.4.5 IPFIX

Опис протоколу IPFIX (Internet Export Flow Information eXport) було опубліковано комітетом IETF у 2008 році. IPFIX є похідним від NetFlow v9 і має бути універсальним протоколом для експорту інформації про flow-потoki з мережевих пристроїв в колектор або NMS (систему управління мережею).

IPFIX – це стандарт на основі NetFlow, що розглядає потік як будь-яке число пакетів, що спостерігаються в певному інтервалі часу і мають ряд загальних властивостей (наприклад, той самий відправник, той самий протокол). IPFIX дозволяє надсилаючому пристрої включати в повідомлення визначені типи даних, які може задати за допомогою спеціальних шаблонів. Крім того, він передбачає примусову доставку: кожен відправник періодично надсилає налаштованим приймаючим пристроям повідомлення IPFIX без будь-якого запиту з боку одержувача. Як протокол транспортного рівня переважно використовувати Stream Control Transmission Protocol (SCTP), але можливі також Transmission Control Protocol (TCP) і User Datagram Protocol (UDP).

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		22

В наш час деякі пристрої Cisco підтримують лише традиційний NetFlow протокол, тоді як інші підтримують Flexible NetFlow або відразу обидва протоколи.

1.4.6 Jflow, Netstream

Обидва протоколи базуються на оригінальному стандарті Cisco NetFlow. jFlow було розроблено компанією Juniper Networks, NetStream – компанією Huawei.

JFlow – це програмна мережева технологія, яка полегшує моніторинг і запис пакетів даних, що перетікають між налаштованими пристроями, зокрема маршрутизаторами та комутаторами.

JFlow налаштовується за замовчуванням у маршрутизаторах і комутаторах, розроблених мережами Juniper. Він записує всю мережеву активність через увімкнений порт і зберігає статистичну інформацію про використання мережі, яку можна отримати через його програмний інтерфейс.

JFlow – це в першу чергу технологія вибірки потоків даних, створена за допомогою набору класів Java. JFlow працює як NetFlow і SFlow, розроблені Cisco і HP відповідно. Хоча JFlow в основному використовується як метод запису потоку, він також забезпечує аналіз мережі та виявлення аномалій шляхом збереження та порівняння тенденцій потоків мережевих даних.

JFlow працює шляхом моніторингу кожного пакета, який протікає всередині мережі. Якщо вхідний пакет не зареєстровано в таблиці маршрутизатора, JFlow записує цей екземпляр і відкидає всі, які вже мають екземпляри таблиці маршрутизації. Дані, зібрані JFlow, зберігаються в серії кешів, кожен з яких надає різний набір інформації, що стосується мережевого потоку.

1.4.7 sFlow

Стандарт sFlow, що називається також вибіркою потоків, підтримується на різних платформах. Він є засобом для експорту усічених пакетів, а також лічильників інтерфейсу. Послідовний розвиток sFlow уможливив отримання ним статусу галузевого стандарту для експорту пакетів на рівні 2. Поточною версією sFlow є версія 5.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		23

sFlow – це технологія вибіркового захоплення пакетів. З усього трафіку через інтерфейс вибирається один з n пакетів (де n - частота вибірки), перші x байт (128 байт для sFlow v5) захопленого пакета копіюються та експортуються в пакети UDP, які називають дейтаграмами sFlow. Перші x байт – це дані заголовка, необхідні відновлення інформації про трафік. Однак оскільки sFlow орієнтований на пакети, деякі IP-потoki можуть пропускатися. Коли пакети захоплюються для аналізу, вони завжди представляють усі IP-потoki (діалоги), які проходять через інтерфейс. В результаті IP-потoki, пакети яких не зібрані, не враховуються, що створює прогалини у картині діалогів у мережі.

Система sFlow складається з декількох пристроїв, що реалізують вибірки двох типів: випадкову вибірку пакетів та вибірку лічильників на основі часу. Вибіркова інформація про пакети/операції та лічильники, звана відповідно зразками потоків та зразками лічильників, пересилається у вигляді дейтаграми sFlow на центральний сервер з необхідним програмним забезпеченням, де проводиться її аналіз та формуються звіти про мережевий трафік. Такий сервер називається колектором sFlow.

sFlow довільно відбирає мережеві пакети та передає ці зразки зовнішньому колектору sFlow, який функціонує як станція моніторингу фактичного використання різних програм та статистичного аналізу характеру використання мережі. Для вирішення цих завдань методи рівномірно розподіленої вибірки, такі як sFlow, вважаються досить точними та надійними навіть при використанні сервісів із високою пропускнуою здатністю.

NetFlow і sFlow мають важливі відмінності. У NetFlow облік трафіку, що проходить через мережу, може виконуватися як для всіх транзакцій (повний NetFlow), так і для вибіркового їх числа (вибірковий NetFlow), у той час як sFlow є «виключно вибірковою» технологією, в якій комутатор або маршрутизатор випадковим чином відбирає зразки фіксованої довжини одного з N пакетів.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		24

1.5 Огляд існуючих flow аналізаторів

Flow аналізатори та колектори – це дуже корисний інструментарій для моніторингу та аналізу даних мережевого трафіку, який допоможе вам виявити можливі проблеми ще до того, як вони стануть реальною загрозою. Аналізатори NetFlow дозволять вам визначити ті машини та пристрої, які негативно впливають на пропускну здатність вашої мережі, знайти вузькі місця у вашій системі, а також зрештою підвищити загальну ефективність функціонування вашої мережі.

Інформація, яку збирає з IP-трафіку NetFlow, включає:

- IP-адреса джерела;
- IP-адреса призначення;
- порт джерела для UDP та TCP;
- порт призначення для UDP та TCP;
- тип та код повідомлення для ICMP;
- номер інтернет-протоколу транспортного рівня, інкапсульованого у протоколі IP;
- тип обслуговування (Type of Service, ToS);
- мережевий інтерфейс.

Збираючи та аналізуючи цю інформацію, ви можете багато дізнатися про функціонування вашої мережі, а також використовувати її для різних цілей, включаючи моніторинг пропускну здатності, усунення несправностей у роботі мережі та виявлення аномалій.

1.5.1 PRTG Network Monitor

PRTG Network Monitor – це універсальне програмне рішення для моніторингу мережі, яке включає моніторинг продуктивності, відстеження обмежень пропускну здатності, спостереження за роботою серверів, центральних процесорів, додатків, веб-сайтів, хмарних служб та багато іншого. Стандартне встановлення спочатку надає вам всі необхідні інструменти для моніторингу всього трафіку у вашій мережі. PRTG Network Monitor може використовувати

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		25

для аналізу різні версії стандарту NetFlow (v5 і v9), відкритий універсальний стандарт IPFIX, а також інші технології обліку мережевого трафіку, такі як sFlow та J-Flow.

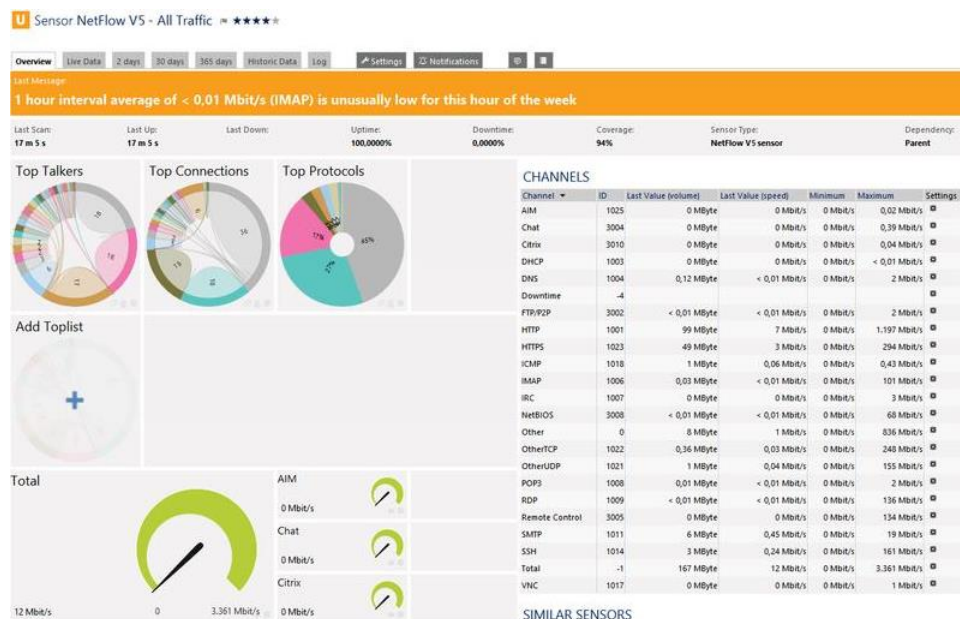


Рисунок 1.5 – Вікно аналізатора PRTG Network Monitor

Однією з можливостей застосування моніторингу NetFlow, доступною в PRTG Network Monitor, є аналіз пропускної здатності. Звіти візуалізуються у вигляді рейтингових списків, що дозволяють відстежувати дані за різними категоріями, що налаштовуються, що значно спростить вам завдання. Наприклад, ви можете відстежувати і відразу порівнювати отримані результати окремо для різних IP-адрес, для підключень, для протоколів, для додатків і т. д. Це дуже корисно при усуненні несправностей у роботі мережі.

1.5.2 Scrutinizer

Програмне рішення Scrutinizer це набагато більше, ніж просто аналізатор NetFlow. Програма є повноцінною системою реагування на інциденти, яка може використовуватися як для аналізу мережевого трафіку, так і для отримання звітів про інциденти безпеки. Scrutinizer може збирати та аналізувати дані з різних типів потоків, використовуючи NetFlow, J-Flow, NetStream та IPFIX. Іншими словами, це рішення буде повноцінно працювати з різними пристроями від різних постачальників.

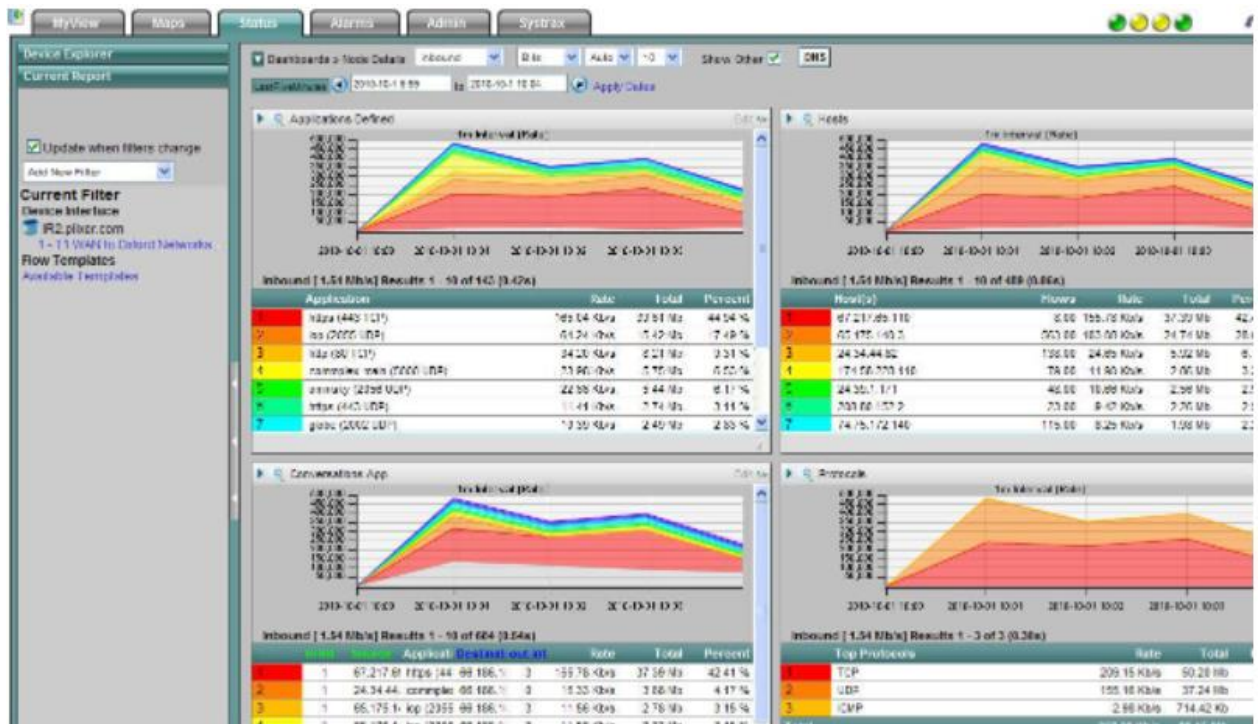


Рисунок 1.6 – Вікно аналізатора Scrutinizer

Scrutinizer забезпечує видимість як у фізичному середовищі, так і віртуальному. Він також має швидку та просунуту функціональність щодо формування звітності, підтримує можливості колективної роботи та має можливості масштабування, оскільки побудований на принципах розподіленої архітектури.

1.5.3 nProbe and ntopng

Рішення ntopng — це веб-інструмент із відкритим вихідним кодом для моніторингу та аналізу мережного трафіку. Програма була написана для використання на мобільних пристроях під керуванням будь-якої з найпопулярніших платформ: Unix, MacOS та Windows. Через зашифрований інтерфейс надходять дані про передані пакети.

ntop

Home ▾

Flows

Hosts ▾

Admin ▾

Search Host

Active Flows



10 ▾



Info	Application	L4 Proto	Client	Server	Duration	Breakdown	Bytes
Info	Unknown	TCP	216.34.181.57:22	192.168.1.92:58356	23 sec	Server	1.12 MB
Info	Unknown	TCP	192.12.193.5:2222	192.168.1.92:61086	23 sec	Client Server	86.78 KB
Info	SSL	TCP	192.168.1.92:58641	72.233.2.58:443	3 sec	Client Server	9.79 KB
Info	Unknown	TCP	66.155.11.238:443	192.168.1.92:58607	5 sec	Client Server	8.83 KB
Info	Google	TCP	192.168.1.92:58638	173.194.35.4:443	1 sec	Client Server	2.34 KB
Info	Google	TCP	192.168.1.92:58636	173.194.35.4:443	2 sec	Client Server	2.15 KB
Info	Google	TCP	192.168.1.92:58409	173.194.35.6:443	2 sec	Client Server	633
Info	Unknown	TCP	2.225.48.185:22515	192.168.1.92:60969	14 sec	Client Server	612
Info	DropBox	UDP	192.168.1.92:17500	Broadcast:17500	1 sec	Client	516
Info	DropBox	UDP	192.168.1.92:17500	192.168.1.255:17500	1 sec	Client	516

Showing 1 to 10 of 55 rows

← First

Prev

1

2

3

4

5

Next

Last →

Рисунок 1.7 – Вікно аналізатора ntopng

Програма ntopng може підключатися до nProbe, який є колектором NetFlow/IPFIX. У цьому тандемі ролі розподілені так: nProbe збирає дані про потоки і відправляє цю інформацію в ntopng, який, у свою чергу, аналізує її і представляє у зручному для сприйняття вигляді.

1.5.4 Solarwinds NetFlow Traffic Analyzer

NetFlow Traffic Analyzer (NTA) виробництва компанії Solarwinds – це програмний інструмент для аналізу мережевого трафіку та моніторингу пропускної спроможності, який підтримує роботу з різними протоколами, включаючи: NetFlow, J-Flow, sFlow, IPFIX та NetStream.

Рішення Solarwinds NTA дозволить зрозуміти, як використовується пропускна спроможність мережі. Наприклад, ви можете дізнатися, яка IP-адреса або програма має максимальні обсяги споживання ресурсів пропускної спроможності в певний момент часу. Також ви зможете використовувати шаблони для аналізу трафіку, тим самим значно розширивши свої можливості щодо детального мережевого аналізу.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		28

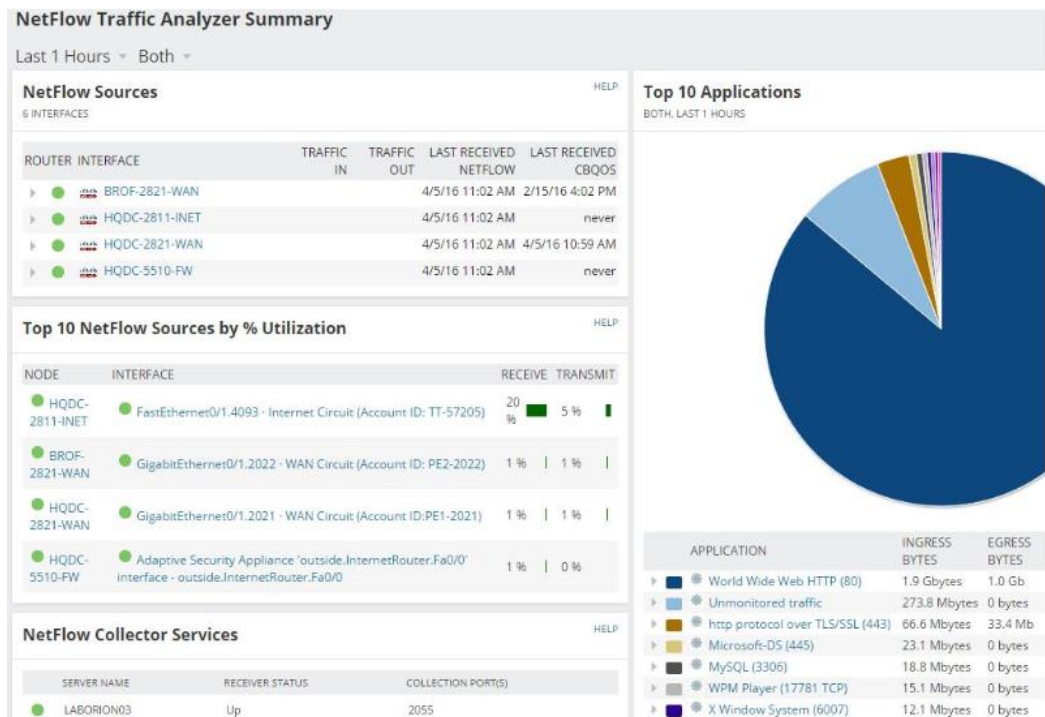


Рисунок 1.8 – Вікно аналізатора Solarwinds NetFlow Traffic Analyzer

NetFlow Traffic Analyzer збирає дані трафіку, погоджує їх з форматами, що використовуються, і демонструє отриману інформацію користувачеві через веб-інтерфейс для моніторингу мережевого трафіку. Ви можете аналізувати мережевий трафік за конкретний період: хвилину, годину, день або місяць.

Solarwinds NTA дозволить зрозуміти, чи політики QoS працюють так, як це було заплановано. Тобто, якщо ваш бізнес залежить від VoIP, електронної комерції або інших хмарних програм, моніторинг NetFlow допоможе підтвердити, що пріоритетний трафік проходить безперешкодно через мережу.

1.6 Постановка технічного завдання

Необхідно створити проект мережі з використанням трьохрівневої організації. Рівень ядра повинен складатися з декількох маршрутизаторів. На маршрутизаторах рівня розподілу повинні бути налаштовані сенсори NetFlow. Для NetFlow колекторів має бути виділена окрема підмережа.

Висновки з розділу:

У розділі було визначено поняття систем аналізу трафіку, тобто системи NTA призначені для перехоплення потоків даних та виявлення ознак складних цільових атак. Таким чином, протоколи сімейства NetFlow відносяться до NTA-систем. Далі було описано принцип роботи і основні відмінності протоколу NetFlow й протоколів, що відносяться до тєї ж категорії, а саме протоколів: NSEL, IPFIX, й sFlow. Наприкінці було проведено огляд існуючих програмних рішень для здійснення аналізу зібраної інформації про трафік. Отже існує достатня кількість додатків від «легкого» ntopng, що може бути використаний на мобільних пристроях, до Scrutinizer, що є повноцінною системою реагування на інциденти.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		30

РОЗДІЛ 2 ПРОЕКТУВАННЯ ТЕСТОВОЇ МЕРЕЖІ Й ПІДСИСТЕМИ МОНІТОРИНГУ ПОДІЙ

2.1 Проектування загальної топології мережі для реалізації підсистеми моніторингу подій

Для реалізації підсистеми моніторингу подій необхідно спочатку створити тестову мережу. В якості тестової мережі була створена мережа з трьохрівневою організацією, що складається з рівня ядра, розподілу й доступу (рисунок 2.1).

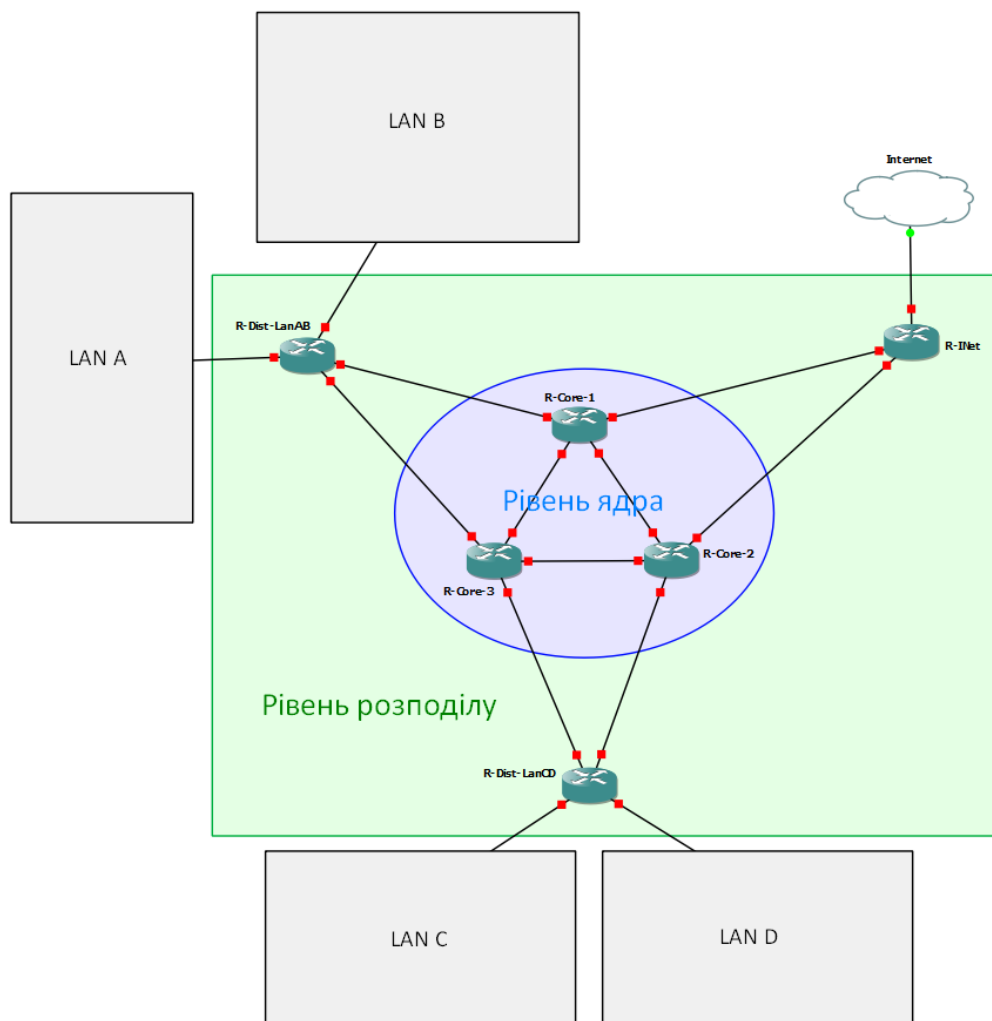


Рисунок 2.1 – Топологія тестової мережі

Рівень ядра являє собою 3 маршрутизатори, що з'єднані між собою за допомогою послідовних кабелів з використанням технології GigabitEthernet.

Інші 3 маршрутизатори складають рівень розподілу, з'єднуючи рівень ядра й локальні мережі. Маршрутизатори рівня розподілу використовують технологію GigabitEthernet для підключення до маршрутизаторів рівня ядра.

Рівень доступу складається з 4-х локальних мереж, пристрої яких з'єднані між собою з використанням технології FastEthernet.

2.2 Опис локальних мереж

Тестова мережа має чотири локальні мережі, що є достатнім для демонстрації роботи підсистеми аналізу подій. Таким чином передбачається, що у локальних мережах «LAN C» й «LAN D»(рисунок 2.2) знаходяться офісні робочі станції.

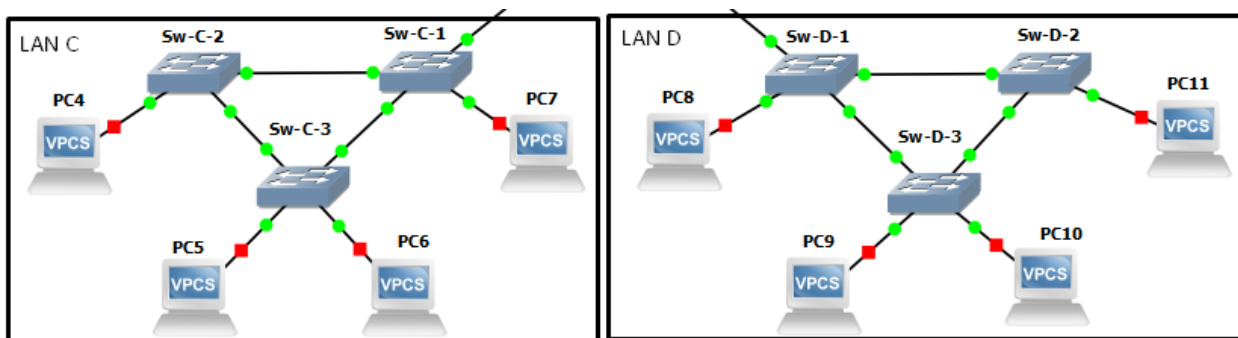


Рисунок 2.2 – Локальні мережі «LAN C» й «LAN D»

До комутаторів Sw-C-1, Sw-C-2, Sw-C-3 та Sw-D-1, Sw-D-2, Sw-D-3 підключено 4 ПК відповідно, що у сумі дає 8 кінцевих користувачів, але на комутаторах в теорії доступні ще 61 вільних порти на кожную підмережу, для підключення додаткових користувачів. З'єднання ПК з комутаторами повинно бути виконане за допомогою виті пари технології FastEthernet, а з'єднання між комутатором й маршрутизатором за допомогою технології GigabitEthernet.

Локальна мережа «LAN A»(рисунок 2.3) містить декілька робочих станцій й серверів.

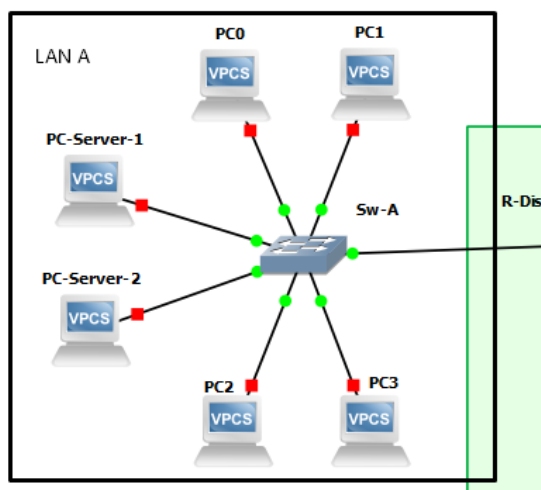


Рисунок 2.3 – Локальна мережа «LAN А»

До комутатора Sw-A підключено 4 кінцевих користувача й 2 сервери. На комутаторі Sw-A доступні ще 19 вільних порти для підключення додаткових користувачів. З'єднання ПК з комутатором повинно бути виконане за допомогою виті пари технології FastEthernet, а між комутатором й маршрутизатором за допомогою технології GigabitEthernet.

У локальній мережі «LAN В»(рисунок 2.4) розташовано декілька колекторів NetFlow.

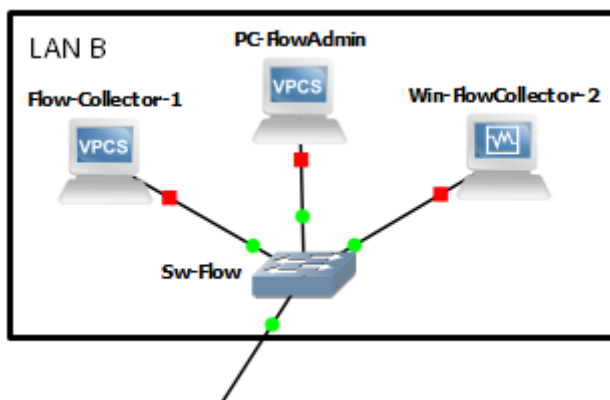


Рисунок 2.4 – Локальна мережа «LAN В»

До комутатора Sw-Flow підключено 3 кінцевих користувача. На комутаторі Sw- Flow доступні ще 21 вільних порти для підключення додаткових користувачів. З'єднання ПК з комутатором повинно бути виконане за допомогою виті пари технології FastEthernet, а між комутатором й маршрутизатором за допомогою технології GigabitEthernet.

2.3 Проектування системи моніторингу подій

Підсистема складається з трьох компонентів: сенсор, колектор і аналізатор. За допомогою сенсора буде проводитись захоплення інформації про проходження трафіку, після чого зібрана інформація буде відсилатись до колектора. У нашому випадку сенсори NetFlow буде налагоджено на маршрутизаторах рівня розподілу(рисунок 2.5).

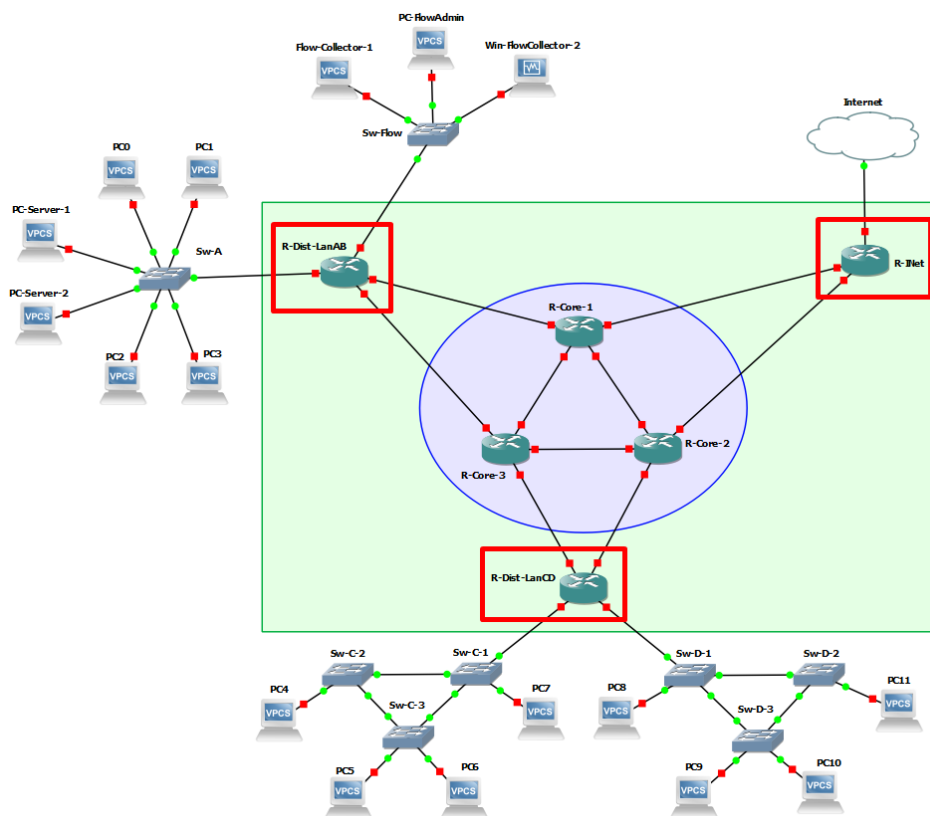
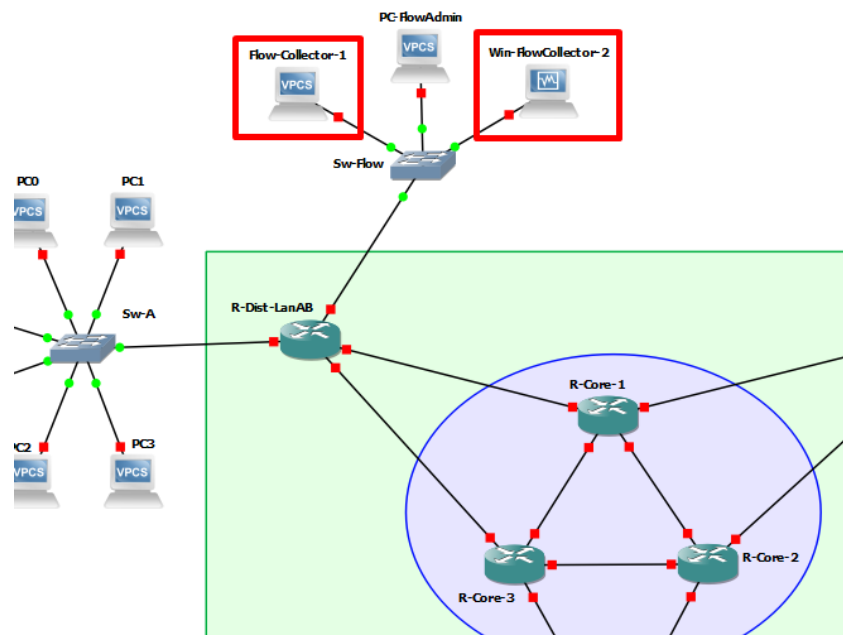


Рисунок 2.5 – Розташування сенсорів NetFlow

На маршрутизаторі R-Dist-LanAB буде використано протокол NetFlow v5, а на маршрутизаторах R-Dist-LanCD й R-INet протокол NetFlow v9.

Інформація, зібрана з сенсорів передається до колекторів(рисунок 2.6), що в нашому випадку виконують й роль аналізаторів.



2.4 Розробка схеми адресації мережі

Для спроектованої віще мережі було виконано розрахунок адрес й створено схему адресації. Результат розрахунку адрес для підмереж LAN А – LAN Д представлено у таблицях 2.1 – 2.4.

Таблиця 2.1 – Схема адресації LAN А

Призначення	ІР-адреса
Адреса мережі	192.191.1.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.191.1.1
Максимальна адреса	192.191.1.253
Широкомовна адреса	192.191.1.254
Шлюз по замовчуванню	192.191.1.253
Діапазон адрес комутаторів	192.191.1.250-192.191.1.252
Діапазон використаних адрес	192.191.1.1-192.191.1.6
Діапазон вільних адрес	192.191.1.7-192.191.1.249

Таблиця 2.2 – Схема адресації LAN В

Призначення	ІР-адреса
Адреса мережі	192.191.2.0
Маска мережі	255.255.255.0/24

Інвертована маска	0.0.0.255
Мінімальна адреса	192.191.2.1
Максимальна адреса	192.191.2.253
Широкомовна адреса	192.191.2.254
Шлюз по замовчуванню	192.191.2.253
Діапазон адрес комутаторів	192.191.2.250-192.191.2.252
Діапазон використаних адрес	192.191.2.1-192.191.2.3
Діапазон вільних адрес	192.191.2.4-192.191.2.249

Таблиця 2.3 – Схема адресації LAN C

Призначення	ІР-адреса
Адреса мережі	192.191.3.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.191.3.1
Максимальна адреса	192.191.3.253
Широкомовна адреса	192.191.3.254
Шлюз по замовчуванню	192.191.3.253
Діапазон адрес комутаторів	192.191.3.250-192.191.3.252
Діапазон використаних адрес	192.191.3.1-192.191.3.4
Діапазон вільних адрес	192.191.3.5-192.191.3.249

Таблиця 2.4 – Схема адресації LAN D

Призначення	ІР-адреса
Адреса мережі	192.191.4.0
Маска мережі	255.255.255.0/24
Інвертована маска	0.0.0.255
Мінімальна адреса	192.191.4.1
Максимальна адреса	192.191.4.253
Широкомовна адреса	192.191.4.254
Шлюз по замовчуванню	192.191.4.253
Діапазон адрес комутаторів	192.191.4.250-192.191.4.252
Діапазон використаних адрес	192.191.4.1-192.191.4.4
Діапазон вільних адрес	192.191.4.5-192.191.4.249

Схема адресації для мереж між маршрутизаторами, а саме С-А, С-В, С-С й D-1, D-2, D-3, D-4, D-5, D-6, наведена у таблиці 2.5.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		36

Таблиця 2.5 – Адресація мереж між маршрутизаторами

Мережа	Адреса мережі	Маска мережі
C-A	192.191.10.0	255.255.255.252/30
C-B	192.191.10.4	255.255.255.252/30
C-C	192.191.10.8	255.255.255.252/30
D-1	192.191.20.0	255.255.255.252/30
D-2	192.191.20.4	255.255.255.252/30
D-3	192.191.20.8	255.255.255.252/30
D-4	192.191.20.12	255.255.255.252/30
D-5	192.191.20.16	255.255.255.252/30
D-6	192.191.20.20	255.255.255.252/30

Висновки з розділу:

У другому розділі було визначено топологію й виконано проектування тестової мережі. Отже мережа має трьохрівневу організацію, а на рівні доступу має чотири локальні мережі. Було визначено розташування сенсорів й колекторів/аналізаторів NetFlow, розташування сенсорів на маршрутизаторах рівня розподілу дозволить в аналізувати значну частину трафіку, що проходить крізь мережу. Також було проведено розрахунок адрес мережі й складено схему адресації.

РОЗДІЛ 3 НАЛАГОДЖЕННЯ ПРИСТРОЇВ МЕРЕЖІ Й ПРОВЕДЕННЯ ТЕСТУВАННЯ ПІДСИСТЕМИ МОНІТОРИНГУ

3.1 Налаштування пристроїв мережі

Спочатку було проведено налаштування маршрутизаторів рівня ядра: R-Core-1, R-Core-2 й R-Core-3.

Налаштування R-Core-1:

```
hostname R-Core-1
```

```
interface GigabitEthernet2/0
```

```
ip address 192.191.10.1 255.255.255.252
```

```
ip nat inside
```

```
interface GigabitEthernet3/0
```

```
ip address 192.191.10.5 255.255.255.252
```

```
ip nat inside
```

```
interface GigabitEthernet0/0
```

```
ip address 192.191.20.21 255.255.255.252
```

```
ip nat inside
```

```
interface GigabitEthernet1/0
```

```
ip address 192.191.20.1 255.255.255.252
```

```
ip nat outside
```

```
ip route 0.0.0.0 0.0.0.0 192.191.20.1
```

```
ip domain-lookup
```

```
ip name-server 8.8.8.8
```

```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

```
access-list 1 permit any
```

```
router rip
```

```
version 2
```

```
network 192.191.10.0
```

```
network 192.191.10.8
```

```
network 192.191.20.20
```

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		38

network 192.191.20.1

Налагодження R-Core-2:

hostname R-Core-2

interface GigabitEthernet2/0

ip address 192.191.10.6 255.255.255.252

ip nat inside

interface GigabitEthernet3/0

ip address 192.191.10.9 255.255.255.252

ip nat inside

interface GigabitEthernet0/0

ip address 192.191.20.5 255.255.255.252

ip nat outside

interface GigabitEthernet1/0

ip address 192.191.20.9 255.255.255.252

ip nat inside

ip route 0.0.0.0 0.0.0.0 192.191.20.5

ip domain-lookup

ip name-server 8.8.8.8

ip nat inside source list 1 interface GigabitEthernet0/0 overload

access-list 1 permit any

router rip

version 2

network 192.191.10.4

network 192.191.10.8

network 192.191.20.4

network 192.191.20.8

Налагодження R-Core-3:

hostname R-Core-3

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		39

```

interface GigabitEthernet2/0
ip address 192.191.10.2 255.255.255.252
ip nat outside
interface GigabitEthernet3/0
ip address 192.191.10.10 255.255.255.252
ip nat inside
interface GigabitEthernet0/0
ip address 192.191.20.17 255.255.255.252
ip nat inside
interface GigabitEthernet1/0
ip address 192.191.20.13 255.255.255.252
ip nat inside
ip route 0.0.0.0 0.0.0.0 192.191.10.1
ip domain-lookup
ip name-server 8.8.8.8
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit any
router rip
version 2
network 192.191.10.0
network 192.191.10.8
network 192.191.20.16
network 192.191.20.12

```

Далі було проведено налаштування маршрутизаторів рівня розподілу: R-Dist-LanAB, R-Dist-LanCD, R-INet.

Налагодження R-Dist-LanAB:

```

hostname R-Dist-LanAB
interface GigabitEthernet2/0
ip address 192.191.20.22 255.255.255.252

```

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		40

```

ip nat outside
interface GigabitEthernet3/0
ip address 192.191.20.18 255.255.255.252
interface FastEthernet0/0
ip address 192.191.1.253 255.255.255.0
ip nat inside
interface FastEthernet1/0
ip address 192.191.2.253 255.255.255.0
ip nat inside
ip route 0.0.0.0 0.0.0.0 192.191.20.21
ip domain-lookup
ip name-server 8.8.8.8
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit any
router rip
version 2
network 192.191.20.20
network 192.191.20.16
network 192.191.1.0
network 192.191.2.0

```

Налагодження R-Dist-LanCD:

```

hostname R-Dist-LanCD
interface GigabitEthernet1/0
ip address 192.191.20.14 255.255.255.252
interface GigabitEthernet2/0
ip address 192.191.20.10 255.255.255.252
ip nat outside
interface FastEthernet0/0
ip address 192.191.3.253 255.255.255.0

```

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		41

```

ip nat inside
interface FastEthernet3/0
ip address 192.191.4.253 255.255.255.0
ip nat inside
ip route 0.0.0.0 0.0.0.0 192.191.20.9
ip domain-lookup
ip name-server 8.8.8.8
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit any
router rip
version 2
network 192.191.20.12
network 192.191.20.8
network 192.191.3.0
network 192.191.4.0

```

Налагодження R-INet:

```

hostname R-INet
interface GigabitEthernet0/0
ip address dhcp
ip nat outside
interface GigabitEthernet1/0
ip address 192.191.20.2 255.255.255.252
ip nat inside
interface GigabitEthernet2/0
ip address 192.191.20.6 255.255.255.252
ip nat inside
exit
ip nat inside source list 1 interface GigabitEthernet0/0 overload
access-list 1 permit any

```

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієвський Ю.М.				42
Змн.	Арк.	№ докум.	Підпис	Дата		

3.2 Налаштування підсистеми моніторингу подій

Виконання налаштування протоколу NetFlow версії 5 на маршрутизаторі R-Dist-Lan-AB:

```
ip flow-export destination 192.191.2.2 9997
ip flow-export destination 192.191.2.3 9997
ip flow-export version 5
ip flow-cache timeout active 1
ip flow-cache timeout inactive 20
interface FastEthernet0/0
ip flow egress
ip flow ingress
interface FastEthernet1/0
ip flow egress
ip flow ingress
```

Виконання налаштування протоколу NetFlow версії 9 на маршрутизаторі R-Dist-Lan-CD:

```
ip flow-export destination 192.191.2.2 9997
ip flow-export destination 192.191.2.3 9997
ip flow-export version 9
ip flow-cache timeout active 1
ip flow-cache timeout inactive 20
interface FastEthernet0/0
ip flow egress
ip flow ingress
interface FastEthernet3/0
ip flow egress
ip flow ingress
```

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		43

Виконання налаштування протоколу NetFlow версії 9 на маршрутизаторі R-INet:

ip flow-export destination 192.191.2.2 9997

ip flow-export destination 192.191.2.3 9997

ip flow-export version 9

ip flow-cache timeout active 1

ip flow-cache timeout inactive 30

interface GigabitEthernet0/0

ip flow egress

ip flow ingress

Після проведення налаштування сенсорів потрібно налаштувати колектор/аналізатор. В якості аналізатора було обрано «PRTG Network Monitor». Спочатку було створено групу сенсорів NetFlow й додано до неї маршрутизатори в якості пристроїв, що показано на рисунку 3.1.

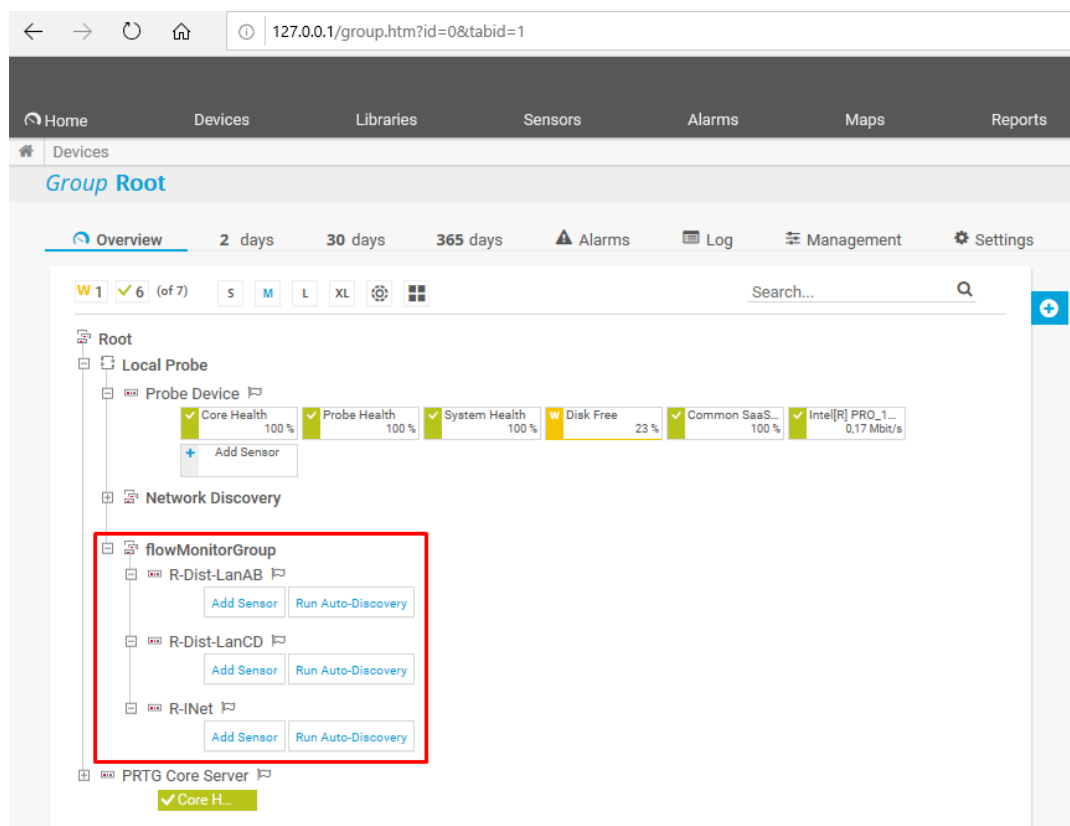


Рисунок 3.1 – Налаштована група й пристрої в «PRTG Network Monitor»

Після створення групи й додання моделей маршрутизаторів потрібно провести налаштування сенсорів на кожному з пристроїв(рисунок 3.2).

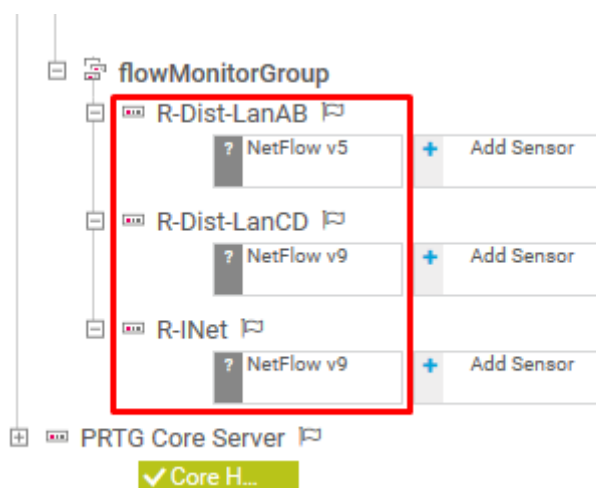


Рисунок 3.2 – Налаштовані NetFlow сенсори в «PRTG Network Monitor»

Таким чином інформація про трафік, що проходить крізь маршрутизатори R-Dist-LanAB, R-Dist-LanCD й R-INet буде спочатку надіслана до колектора, а потім аналізатор PRTG Network Monitor, що дає змогу відобразити різноманітну інформацію, закладену в повідомленнях NetFlow.

3.3 Тестування системи моніторингу подій

Для виконання тестування роботи підсистеми потрібно згенерувати будь-який трафік. У даному випадку для генерації трафіку використано підключення до інтернету.

Після генерації трафіку на панелі сенсора «PRTG Network Monitor» з'являться відповідні дані, наприклад дані про найбільш активних користувачів, з'єднань й протоколів(рисунок 3.3).

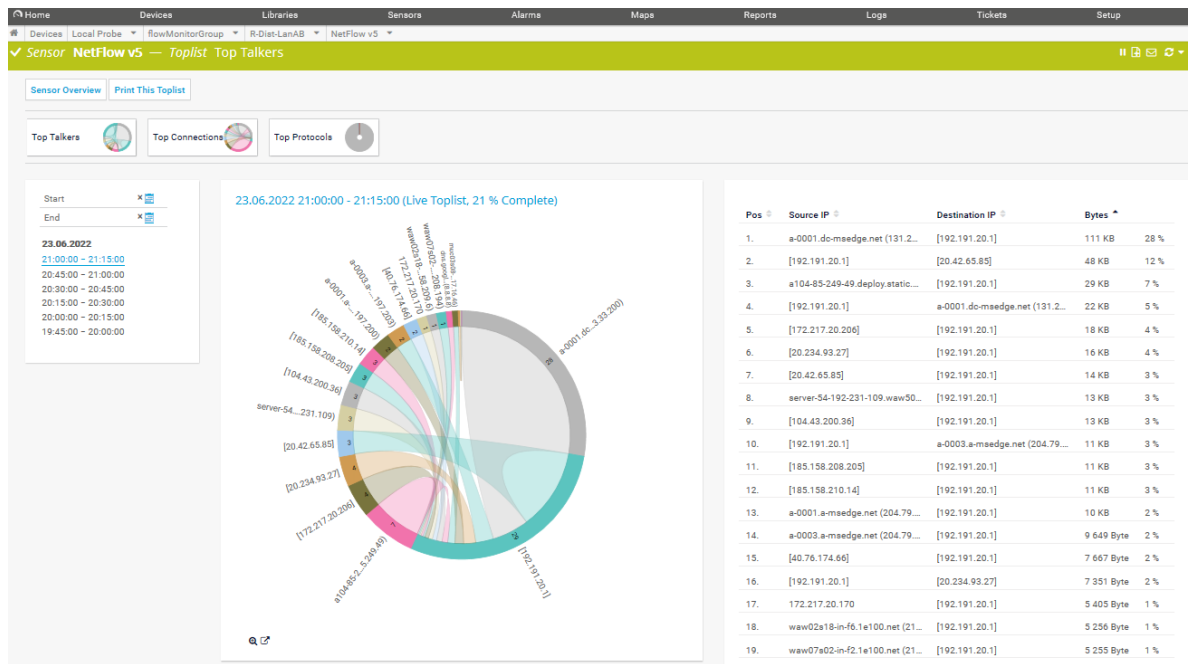


Рисунок 3.3 – Список найбільш активних користувачів

Також можливо переглянути статистичні графіки, що містять інформацію про залежність навантаження різними типами трафіку, що проходять крізь сенсор, від часу(рисунок 3.4).

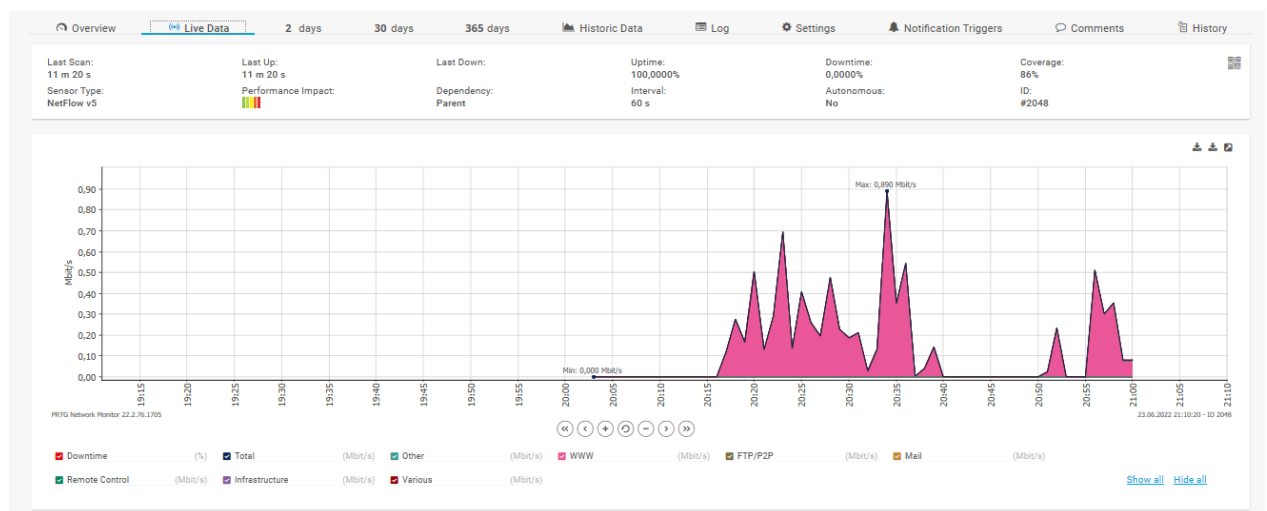


Рисунок 3.4 – Залежність навантаження різними типами трафіку від часу

На рисунку 3.5 показано історію навантаження на мережу у місці розташування сенсора.

Date Time	Total (volume)	Total (speed)	Other (volume)	Other (speed)	WWW (volume)	WWW (speed)	FTP/P2P (volume)	FTP/P2P (speed)	Mail (volume)	Mail (speed)	Remote Control (volume)
Summ (of 58 values)	57 MB		0 MB		57 MB		0 MB		< 0,01 MB		0 MB
Averages (of 58 values)	0,98 MB	0,14 Mbit/s	0 MB	0 Mbit/s	0,98 MB	0,14 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB

Date Time *	Total (volume) Ⓢ	Total (speed) Ⓢ	Other (volume) Ⓢ	Other (speed) Ⓢ	WWW (volume) Ⓢ	WWW (speed) Ⓢ	FTP/P2P (volume) Ⓢ	FTP/P2P (speed) Ⓢ	Mail (volume) Ⓢ	Mail (speed) Ⓢ	Remote Control (volume) Ⓢ
23.06.2022 21:02:00	0,11 MB	0,02 Mbit/s	0 MB	0 Mbit/s	0,11 MB	0,02 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 21:01:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 21:00:00	0,02 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0,02 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:59:00	0,57 MB	0,08 Mbit/s	0 MB	0 Mbit/s	0,57 MB	0,08 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:58:00	2,54 MB	0,36 Mbit/s	0 MB	0 Mbit/s	2,54 MB	0,35 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:57:00	2,16 MB	0,30 Mbit/s	0 MB	0 Mbit/s	2,14 MB	0,30 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:56:00	3,67 MB	0,51 Mbit/s	0 MB	0 Mbit/s	3,64 MB	0,51 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:55:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:54:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:53:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:52:00	1,68 MB	0,24 Mbit/s	0 MB	0 Mbit/s	1,67 MB	0,23 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB
23.06.2022 20:51:00	0,16 MB	0,02 Mbit/s	0 MB	0 Mbit/s	0,16 MB	0,02 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:50:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:49:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:48:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:47:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:46:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:45:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:44:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:43:00	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:41:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:40:00	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	< 0,01 MB	< 0,01 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB
23.06.2022 20:39:00	1,03 MB	0,14 Mbit/s	0 MB	0 Mbit/s	1,02 MB	0,14 Mbit/s	0 MB	0 Mbit/s	0 MB	0 Mbit/s	0 MB

Рисунок 3.5 – Історія навантаження на мережу

На оглядовій панелі сенсора також відображається й інформація про навантаження на мережу у момент останнього отримання даних з сенсору(рисунок 3.6).



Рисунок 3.6 – Навантаження на мережу у момент останнього отримання даних

Висновки з розділу:

В останньому розділі було проведено налагодження пристроїв мережі, а саме налагодження адресації, налаштування маршрутизації й налагодження NAT для отримання доступу з тестової мережі до мережі інтернет. Після основного налагодження пристроїв, було проведено налаштування маршрутизаторів рівня розподілу в якості сенсорів для прослуховування трафіку. В якості колектора/маршрутизатора було використано віртуальну машину із встановленим програмним забезпеченням PRTG Network Monitor. Під кінець було перевірено роботу підсистеми за рахунок генерування трафіку й огляду інформації, отриманої від сенсорів.

		Рабчинський М.О.			КІК.КР.Б – 125 – 26 – ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		47

ВИСНОВКИ

У першому розділі було визначено поняття систем аналізу трафіку, тобто системи NTA призначені для перехоплення потоків даних та виявлення ознак складних цільових атак. Отже існує достатня кількість додатків від «легкого» ntopng, що може бути використаний на мобільних пристроях, до Scrutinizer, що є повноцінною системою реагування на інциденти.

У другому розділі було визначено топологію й виконано проектування тестової мережі. Отже мережа має трьохрівневу організацію, а на рівні доступу має чотири локальні мережі. Було визначено розташування сенсорів й колекторів/аналізаторів NetFlow. Також було проведено розрахунок адрес мережі й складено схему адресації.

В останньому розділі було проведено налагодження пристроїв мережі. Після основного налагодження пристроїв, було проведено налаштування маршрутизаторів рівня розподілу в якості сенсорів для прослуховування трафіку. Під кінець було перевірено роботу підсистеми за рахунок генерування трафіку й огляду інформації, отриманої від сенсорів.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				48
Змн.	Арк.	№ докум.	Підпис	Дата		

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. sFlow Version 5 [Електронний ресурс] URL:
https://sflow.org/sflow_version_5.txt
2. sFlow Monitoring Technology [Електронний ресурс] URL:
<https://www.juniper.net/documentation/us/en/software/junos/network-mgmt/topics/topic-map/sflow-monitoring-technology.html>
3. PRTG Network Monitor User Manual [Електронний ресурс] URL:
<https://www.prtg-monitoring.sk/upload/download/prtg-manual.pdf>
4. PRTG Manual: Manage Device Tree [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/manage_device_tree
5. PRTG Manual: Group Settings [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/group_settings#basic
6. PRTG Manual: Device Settings [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/device_settings#basic
7. PRTG Manual: NetFlow v5 Sensor [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/netflow_v5_sensor
8. PRTG Manual: NetFlow v9 (Custom) Sensor [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/netflow_v9_custom_sensor
9. RTG Manual: NetFlow v9 Sensor [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/netflow_v9_sensor
10. PRTG Manual: sFlow Sensor [Електронний ресурс] URL:
https://www.paessler.com/manuals/prtg/sflow_sensor
11. CyberOps Associate: Network Security Infrastructure [Електронний ресурс] URL: <https://www.netacad.com>
12. CyberOps Associate: Network Monitoring and Tools [Електронний ресурс] URL: <https://www.netacad.com>
13. Руководство по использованию NetFlow для учета трафика [Електронний ресурс] URL: https://www.opennet.ru/docs/RUS/netflow_bsd/

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				49
Змн.	Арк.	№ докум.	Підпис	Дата		

14. NetFlow Version 9 Flow-Record Format [Електронний ресурс] URL:
https://www.cisco.com/en/US/technologies/tk648/tk362/technologies_white_paper09186a00800a3db9.html
15. InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks [Електронний ресурс] URL:
<https://www.ietf.org/rfc/rfc3176.txt>
16. GNS3 Documentation [Електронний ресурс] URL: http://distfiles.pld-linux.org/by-md5/0/c/0c9cd5c97d0f19f4c00f4e3abd316c87/GNS3-0.4_documentation.pdf
17. Connect GNS3 to the Internet (local server) [Електронний ресурс] URL:
<https://docs.gns3.com/docs/using-gns3/advanced/connect-gns3-internet>
18. Cisco IOS images for Dynamips [Електронний ресурс] URL:
<https://docs.gns3.com/docs/emulators/cisco-ios-images-for-dynamips>
19. Installing Your Cisco 1700 Router Quick Start Guide [Електронний ресурс] URL:
<https://www.cisco.com/en/US/docs/routers/access/1700/1720/hardware/quick/guide/1700qsg.html>
20. Cisco 3745 Router Quick Start Guide [Електронний ресурс] URL:
<https://www.cisco.com/en/US/docs/routers/access/3700/3745/hardware/quick/guide/3745qsg.html>
21. Cisco 7200 VXR Installation and Configuration Guide [Електронний ресурс] URL:
https://www.cisco.com/c/en/us/td/docs/routers/7200/install_and_upgrade/7200vxr_install_config/72vxicg.pdf
22. Catalyst 2960 Switch Software Configuration Guide [Електронний ресурс] URL:
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2960/software/release/12-2_40_se/configuration/guide/scg.pdf

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росініський Ю.М.				50
Змн.	Арк.	№ докум.	Підпис	Дата		

23. A Beginner's Guide to Ethernet 802.3 Application Note [Электронный ресурс] URL: <https://www.analog.com/media/en/technical-documentation/application-notes/ee-269.pdf>
24. The No Sweat Guide to Network Topology Auvik [Электронный ресурс] URL: https://www.auvik.com/wp-content/uploads/2015/04/The_No_Sweat_Guide_to_Network_Topology_Auvik.pdf
25. Эд Уилсон. "Мониторинг и анализ сетей. Методы выявления неисправностей", 2012. – 386 с.
26. М. Лукас. "Network Flow Analysis 1st Edition, Kindle Edition", 2010. – 244 с.
27. К. Сандерс. " Анализ пакетов: практическое руководство по использованию Wireshark и tcpdump для решения реальных проблем в локальных сетях", 2019. – 448 с.
28. В. Олифер, Н. Олифер. "Компьютерные сети. Принципы, технологии, протоколы. Учебник, 4-е издание", 2016. – 944 с.
29. А. Сергеев. "Основы локальных компьютерных сетей", 2016. – 184 с.
30. Э. Таненбаум, Д. Уэзеролл. "Компьютерные сети" 5-е изд. 2016. – 960 с.

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росінський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		51

ДОДАТКИ

		Рабчинський М.О.			КІК.КР.Б - 125 - 26 - ПЗ	Арк.
		Росієнський Ю.М.				
Змн.	Арк.	№ докум.	Підпис	Дата		52

Повна схема мережі

