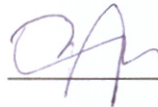


Міністерство освіти і науки України
Державний університет «Житомирська політехніка»
Факультет інформаційно-комп'ютерних технологій
Кафедра комп'ютерної інженерії та кібербезпеки

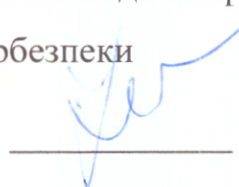
ПОЯСНЮВАЛЬНА ЗАПИСКА

до випускної кваліфікаційної роботи магістра
на тему: «Методи та засоби моніторингу мережі для
підвищення рівня кіберзахисту (на прикладі PRTG
Network Monitor)»

Виконав студент 2-го курсу групи КБм-24-1
спеціальності 125 «Кібербезпека та захист інформації»

 Андрій ФЕРЕНЗ

Керівник старший викладач кафедри комп'ютерної
інженерії та кібербезпеки

 Ігор ФАЛЬКОВСЬКИЙ

Рецензент доцент кафедри комп'ютерної інженерії та
кібербезпеки, кандидат педагогічних наук, доцент

 Олена ГОЛОВНЯ

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

ЗАТВЕРДЖУЮ

Завідувач
кафедри комп'ютерної
інженерії та кібербезпеки

 Андрій Єфіменко

6 жовтня 2025 р.

ЗАВДАННЯ

на випускню кваліфікаційну роботу магістра

Студент: Ференз Андрій Русланович

Тема роботи: «Методи та засоби моніторингу мережі для підвищення рівня кіберзахисту (на прикладі PRTG Network Monitor)»

затверджена Наказом університету від 6 жовтня 2025 р. №566/с

Термін здачі студентом закінченої роботи 23 грудня 2025 р.

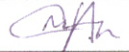
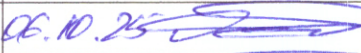
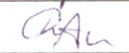
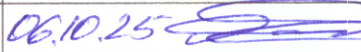
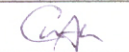
Вихідні дані роботи (зазначається предмет і об'єкт дослідження):

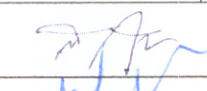
1. Топологія локальної мережі;
2. Система моніторингу PRTG Network Monitor.

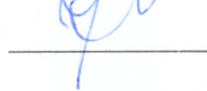
Обладнання та програмне забезпечення:

1. Мережевий емулятор GNS3 (v.2.2.49);
2. Гіпервізор Oracle VirtualBox (v.7.2.2);
3. ОС Windows 10;
4. ОС Windows Server 2022;
5. PRTG Network Monitor (v.25.3.110.1313).

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

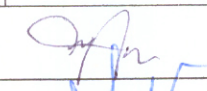
Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
1	Андрій ЄФІМЕНКО		10.06.25 
2	Андрій ЄФІМЕНКО		10.06.25 
3	Андрій ЄФІМЕНКО		10.06.25. 

Студент  Андрій ФЕРЕНЗ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

Календарний план

№ з/п	Назви етапів випускної кваліфікаційної роботи	Термін виконання етапів роботи	Примітка
1	Постановка завдання	06.10.2025 – 08.10.2025	Виконано
2	Розробка плану роботи	09.10.2025 – 10.10.2025	Виконано
3	Аналіз методів і засобів моніторингу мереж	13.10.2025 – 19.10.2025	Виконано
4	Порівняння наявних безкоштовних рішень моніторингу	20.10.2025 – 26.10.2025	Виконано
5	Дослідження архітектури та функціональних можливостей системи PRTG Network Monitor	27.10.2025 – 02.11.2025	Виконано
6	Розробка проєкту мережі та схеми адресації	03.11.2025 – 09.11.2025	Виконано
7	Проектування схеми роботи системи моніторингу в мережі	10.11.2025 – 11.11.2025	Виконано
8	Базове налаштування проєкту мережі в емуляторі GNS3	12.11.2025 – 24.11.2025	Виконано
9	Впровадження та налаштування PRTG Network Monitor	25.11.2025 – 29.11.2025	Виконано
10	Тестування працездатності мережі та роботи рішення моніторингу	30.11.2025 – 01.12.2025	Виконано
11	Оформлення пояснювальної записки	02.12.2025 – 12.12.2025	Виконано
12	Захист	23.12.2025	Виконано

Студент  Андрій ФЕРЕНЗ

Керівник  Ігор ФАЛЬКОВСЬКИЙ

АНОТАЦІЯ

Пояснювальна записка до випускної кваліфікаційної роботи на тему «Методи та засоби моніторингу мережі для підвищення рівня кіберзахисту (на прикладі PRTG Network Monitor)» складається зі вступу, трьох розділів, висновку, списку використаних джерел та додатків. Текстова частина викладена на 72 сторінках друкованого тексту. Пояснювальна записка має 14 сторінок додатків. Список використаних джерел містить 19 найменувань і займає 2 сторінки. В роботі наведено 71 рисунок та 2 таблиці. Загальний обсяг роботи – 86 сторінок.

Метою роботи є дослідження та практична реалізація методів моніторингу мережевої інфраструктури на базі PRTG Network Monitor для підвищення рівня кіберзахисту комп'ютерної мережі.

У ході роботи було розглянуто теоретичні аспекти систем моніторингу, їхнє призначення та функціональні можливості, а також проведено аналіз існуючих рішень, серед яких PRTG Network Monitor визначено, як уніфікований комерційний інструмент, що забезпечує швидке розгортання та ефективний збір даних. Виконано розробку проєкту комп'ютерної мережі на основі трирівневої ієрархічної моделі Cisco включаючи логічну та фізичну топологію з IP-адресацією. Спроектовано систему моніторингу, обґрунтовано вибір протоколів SNMPv3, NetFlow, WMI та Syslog для збору інформації. Проведено налаштування мережевої інфраструктури в емуляторі GNS3, включаючи конфігурацію пристроїв Cisco, розгортання служб Active Directory, DNS і DHCP та безпечного доступу. Виконано налаштування PRTG, в тому числі сенсорів та відправки сповіщень. Здійснено тестування працездатності системи та моделювання нештатних ситуацій, що підтвердило спроможність PRTG забезпечувати проактивний контроль, аналіз трафіку та підвищення стійкості мережі до загроз.

КЛЮЧОВІ СЛОВА: МОНІТОРИНГ, КІБЕРЗАХИСТ, PRTG, SNMP, WMI, NETFLOW, БЕЗПЕКА, СПОВІЩЕННЯ, ТОПОЛОГІЯ.

ANNOTATION

Explanatory note to the graduation qualification work on the topic «Methods and tools for network monitoring to enhance the level of cyber protection (using the example of PRTG Network Monitor)» consists of an introduction, three sections, a conclusion, a list of references, and appendices. The textual part is presented on 72 pages of printed text. The explanatory note includes 14 pages of appendices. The list of references contains 19 items and occupies 2 pages. The work includes 71 figures and 2 tables. The total volume of the work is 86 pages.

The purpose of the work is to research and practically implement methods of monitoring network infrastructure based on PRTG Network Monitor to enhance the cybersecurity level of a computer network.

During the work, theoretical aspects of monitoring systems, their purpose and functional capabilities were considered, as well as an analysis of existing solutions was conducted, among which PRTG Network Monitor was identified as a unified commercial tool that ensures rapid deployment and efficient data collection. A computer network project was developed based on Cisco's three-tier hierarchical model, including logical and physical topology with IP addressing. A monitoring system was designed, with justification for selecting SNMPv3, NetFlow, WMI, and Syslog protocols for data collection. Configuration of the network infrastructure was performed in the GNS3 emulator, including configuration of Cisco devices, deployment of Active Directory, DNS, and DHCP services, and secure access. PRTG configuration was carried out, including sensors and notification sending. Testing of the system's operability and simulation of emergency situations were performed, which confirmed PRTG's capability to provide proactive control, traffic analysis, and increased network resilience to threats.

KEYWORDS: MONITORING, CYBERSECURITY, PRTG, SNMP, WMI, NETFLOW, SECURITY, NOTIFICATIONS, TOPOLOGY.

ЗМІСТ

ВСТУП.....	8
РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМ МОНІТОРИНГУ	10
1.1 Призначення та ключові можливості систем моніторингу мережі	10
1.2 Аналіз існуючих рішень систем моніторингу	15
1.3 Структура та функціональні можливості PRTG Network Monitor	23
РОЗДІЛ 2 ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖІ З ВИКОРИСТАННЯМ PRTG NETWORK MONITOR.....	28
2.1. Розробка проєкту комп'ютерної мережі.....	28
2.2 Проєктування роботи системи моніторингу	33
2.3 Вибір обладнання.....	34
РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ	38
3.1 Первинне налаштування мережевої інфраструктури.....	38
3.2 Налаштування роботи PRTG Network Monitor	46
3.3 Тестування роботи мережі та системи моніторингу	59
ВИСНОВКИ.....	70
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	71
ДОДАТКИ.....	73

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

IP – Internet Protocol

IT – Information Technology

PRTG – Paessler Router Traffic Grapher

NMS – Network Monitoring System

QoS – Quality of Service

IT – Information Technology

CRM – Customer Relationship Management

ICMP – Internet Control Message Protocol

SNMP – Simple Network Management Protocol

RFC – Request For Comments

WMI – Windows Management Instrumentation

IPFIX – IP Flow Information Export

DDoS – Distributed Denial of Service

ВСТУП

Актуальність. Моніторинг мережі є ключовим елементом сучасних систем кіберзахисту, що забезпечує безперервний контроль за роботою мережевої інфраструктури, своєчасне виявлення інцидентів безпеки та запобігання загрозам. Зі зростанням масштабів корпоративних мереж, збільшенням кількості підключених пристроїв та ускладненням способів проникнення зловмисників виникає потреба у впровадженні централізованих і комплексних рішень моніторингу. Такі рішення дозволяють контролювати продуктивність обладнання, аналізувати журнали подій, відстежувати аномалії та прогнозувати можливі збої, що безпосередньо впливає на ефективність управління інформаційною безпекою.

В умовах ускладнення гібридних IT-інфраструктур (локальні пристрої, сервери, хмарні служби) та підвищення вимог до кібербезпеки, вибір оптимальної системи моніторингу стає важливим стратегічним рішенням. Адміністраторам необхідно не лише забезпечити технічну сумісність та охоплення всіх ресурсів, але й збалансувати економічну доцільність та швидкість впровадження. Тому при виборі такої системи вкрай необхідним є проведення структурованого порівняльного аналізу існуючих рішень для обґрунтування вибору інструменту, що гарантує максимальну ефективність контролю при мінімальних витратах часу та ресурсів.

Системи моніторингу, зокрема PRTG Network Monitor, поєднують широкі можливості контролю за мережею з функціоналом оперативного сповіщення та побудови статистичних звітів. Це дозволяє адміністраторам отримувати комплексну картину стану мережі в реальному часі, своєчасно виявляти проблеми та оптимізувати роботу інфраструктури. Використання подібних рішень дає змогу мінімізувати ризики втрат даних, збоїв у роботі сервісів та фінансових витрат, пов'язаних із порушенням безперервності бізнес-процесів.

Метою кваліфікаційної роботи є дослідження методів та засобів моніторингу мережі на прикладі використання рішення PRTG Network Monitor для підвищення рівня кіберзахисту корпоративної інфраструктури.

Для досягнення поставленої мети передбачено виконання таких завдань:

- провести аналіз наявних методів і засобів моніторингу мереж;
- проаналізувати наявні безкоштовні рішення моніторингу;
- дослідити архітектуру, принципи роботи та функціональні можливості системи PRTG Network Monitor;
- виконати проєктування мережевої інфраструктури;
- розробити методику впровадження системи моніторингу в мережі;
- виконати практичне налаштування комп'ютерної мережі, впровадити PRTG та протестувати його ефективність роботи.

Об'єктом дослідження є процес моніторингу корпоративної мережі, який є складовою системи інформаційної безпеки організації.

Предметом дослідження є методи, технології та інструменти моніторингу мережі на базі PRTG Network Monitor, які забезпечують контроль, аналіз, сповіщення, звітування і тим самим підвищує рівень кіберзахисту мережевої інфраструктури.

РОЗДІЛ 1. ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМ МОНІТОРИНГУ

1.1 Призначення та ключові можливості систем моніторингу мережі

Система моніторингу мережі (Network Monitoring System, NMS) – це програмно-апаратний комплекс, призначений для безперервного спостереження, збору, аналізу та візуалізації даних про стан, продуктивність, доступність і безпеку всіх компонентів інформаційно-технологічної інфраструктури, включаючи мережеві пристрої, сервери, віртуалізовані середовища та додатки. Метою системи моніторингу є проактивне виявлення несправностей та аномалій, що можуть призвести до погіршення якості обслуговування (QoS) або порушення цілісності мережі. Крім того вони повинні надання адміністраторам мережі гнучкі механізми оповіщення та перегляд звітності задля оптимізації ресурсів, планування потужностей і підвищення загального рівня кіберзахисту [1].

Сучасне визначення моніторингу мережі вже не обмежується лише встановленням інструменту здатного збирати дані про мережеву активність. В корпоративному середовищі, де інформаційні технології виконують критичну функцію, безпосередньо впливаючи на щоденну діяльність, вибір системи моніторингу має враховувати не лише технічні, але й бізнес-аспекти. Зокрема, ефективне рішення повинно сприяти підвищенню продуктивності праці співробітників та бути економічно раціональним. Незважаючи на те, що кожна мережа є унікальною, ідеальна система моніторингу повинна мати базовий набір обов'язкових функцій, реалізованих або інтегрованих через корисні додаткові модулі (плагіни) [2].

Прямий вплив ІТ на бізнес може проявлятися, як у простих, але надокучливих проблемах (наприклад, повільне завантаження вебсторінки або низька якість локального з'єднання), так і у серйозних інцидентах (наприклад, збій бази даних CRM, втрата важливого електронного листа або внутрішні порушення безпеки). Хоча для вирішення цих проблем існують різноманітні спеціалізовані рішення, найбільшу зручність та ефективність забезпечує система, що пропонує єдину панель доступу. Це дозволяє адміністратору

комплексно візуалізувати всю мережу та оперативно керувати несправностями, продуктивністю, конфігурацією та безпекою.

Для IT-адміністратора продуктивність, безпека та надійність мережі не є взаємовиключними поняттями. Навпаки, це взаємопов'язані елементи. Рішення, яке об'єднує управління всіма цими аспектами, забезпечує стабільність мережі та високу швидкість роботи.

Функціональні вимоги до систем моніторингу

Детальний розгляд головних завдань адміністратора мережі дозволяє сформулювати перелік обов'язкових функціональних вимог до системи моніторингу, які гарантують ефективну роботу з мінімальним часом простою [3-4].

1) Автоматичне виявлення. В умовах постійно зростаючої та розподіленої корпоративної інфраструктури автоматичне виявлення нових ресурсів є критично важливим, оскільки це мінімізує ризик ручних помилок. Оскільки додавання нових пристроїв відбувається регулярно, система повинна підтримувати як автоматичне сканування, так і можливість примусового виявлення за запитом адміністратора.

2) Інтелектуальна класифікація. Інфраструктура мережі може включати різноманітні ресурси: мережеві пристрої, сервери, додатки. Оскільки параметри, які визначають стан кожного типу ресурсу відрізняються, система повинна вміти автоматично класифікувати їх за типом. Також необхідна можливість логічного групування, наприклад, об'єднання пристроїв у кластерні середовища або за географічною ознакою, що значно спрощує візуалізацію та управління.

3) Глибокий моніторинг продуктивності. Зниження продуктивності є однією з найбільших проблем для адміністратора. Будь-який мережевий ресурс (внутрішній чи зовнішній) може спричинити уповільнення роботи. Несправності, такі як вихід з ладу апаратного забезпечення, збій WAN-каналу або крах бази даних, мають каскадний ефект і призводять до значних негативних наслідків. Ключові області, що адміністратор має контролювати для

забезпечення 100% доступності мережі, включають: моніторинг доступності, системних ресурсів (CPU, пам'ять, дисковий простір), пропускної здатності.

4) Аналіз даних та звітність. Інструменти моніторингу мережі збирають історичні дані та проводять аналіз тенденцій, допомагаючи організаціям зрозуміти особливості використання їхньої мережі. На основі цих звітів ІТ-команди можуть ідентифікувати проблеми продуктивності, здійснювати планування майбутніх оновлень та оптимізовувати мережеві ресурси. Звіти включають деталі про час безвідмовної роботи мережі, використання пропускної здатності, рівень помилок та інциденти безпеки. Наприклад, відділ ІТ університету може аналізувати звіти, щоб визначити піковий час використання пропускної здатності студентами і відповідно скоригувати мережеві політики.

5) Візуалізація та інформаційні панелі. Сучасні системи моніторингу часто включають графічні інформаційні панелі (дашборди), які відображають продуктивність мережі у режимі реального часу у зручному для сприйняття форматі. Ці дашборди допомагають адміністраторам швидко виявляти проблеми, усуваючи необхідність ручного аналізу необроблених даних. Вони містять діаграми, графіки та теплові карти, які надають інформацію про потоки трафіку, стан пристроїв та загрози безпеки.

6) Управління безпекою. Питання управління безпекою є невід'ємною складовою моніторингу, оскільки забезпечення цілісності та конфіденційності мережі є критично важливим завданням, що вимагає від адміністратора абсолютної безкомпромісності. У контексті кіберзахисту пріоритет надається проактивному виявленню та попередженню інцидентів. Хоча рішення для виявлення та запобігання вторгненням (IDS/IPS) зазвичай не входять до базового функціоналу NMS, підтримка інтеграції зі сторонніми утилітами є значною перевагою, що розширює арсенал засобів захисту. З метою забезпечення безпеки адміністратор зосереджує свою увагу на постійному контролі системних журналів, що є первинним джерелом інформації про потенційні загрози. Це включає аналіз Windows Event Logs, Syslogs, а також детальний перегляд

журналів брандмауерів для виявлення аномальної чи несанкціонованої активності.

7) Інтелектуальне сповіщення. Ефективна система моніторингу повинна мати вбудований механізм сповіщення, який дозволяє ІТ-команді продуктивно співпрацювати. Будь-який компонент мережі може вийти з ладу та дестабілізувати її роботу. Щоб запобігти збою або швидко усунути його, необхідно мати надійний механізм оповіщення, який надає інженеру змістовну інформацію про джерело проблеми, тим самим скорочуючи час реагування.

8) Масштабованість рішення. Система моніторингу не повинна сама стати точкою відмови. Сервер, на якому вона розміщена, так само вразливий, як і будь-який інший ресурс мережі. Тому підтримка надмірності та можливість автоматичного переходу на резервний сервер для забезпечення безперебійного моніторингу є ключовою вимогою, що гарантує надійність самого рішення.

Типові інструменти моніторингу

Для реалізації функцій моніторингу мережі використовуються стандартизовані протоколи та утиліти, які забезпечують збір даних про доступність, продуктивність і системні події. Серед фундаментальних інструментів виділяють Ping, SNMP, SYSLOG, NetFlow/IPFIX, WMI [5-6].

1) Ping є фундаментальною утилітою діагностики мережі, що працює на основі протоколу Internet Control Message Protocol (ICMP). Його основне призначення полягає у верифікації доступності та функціонального стану заданої IP-адреси. Шляхом відправлення пакету ICMP Echo Request та очікування відповіді Echo Reply, Ping дає змогу адміністратору швидко перевірити мережеве з'єднання між пристроями та виміряти час відгуку. Аналіз відповідей Ping є першим кроком у процесі усунення несправностей, допомагаючи локалізувати проблеми, пов'язані з недоступністю хоста,

2) SNMP (Simple Network Management Protocol) є стандартизованим мережевим протоколом прикладного рівня, що забезпечує проактивний збір інформації про стан і продуктивність керованих пристроїв. Архітектура протоколу базується на взаємодії між менеджером та агентом – програмним

компонентом, встановленим на керованому пристрої (маршрутизаторі чи сервері). Агент надає менеджеру доступ до даних управління, які зберігаються у формі змінних, дозволяючи отримувати детальну інформацію про апаратні ресурси (пам'ять, процесор) у реальному часі, а також здійснювати віддалену конфігурацію шляхом модифікації цих змінних. Комунікація між менеджером і агентом здійснюється за допомогою UDP портів 161 (запити) та 162 (асинхронні сповіщення, відомі як Trap).

Протокол SNMP існує у трьох основних версіях, кожна з яких доповнювала його функціональність та безпеку [7]:

- SNMP v1. Початкова версія, що використовує операції Get, GetNext, Set та Trap. Її головний недолік полягав у відсутності механізмів автентифікації та контролю доступу, що створювало значні проблеми безпеки.

- SNMP v2c. Покращена версія, що додала такі операції, як GetBulk (для ефективного отримання великих блоків даних) та Inform, підвищивши продуктивність, але все ще зберігаючи проблеми безпеки.

- SNMP v3. Найсучасніша версія, яка вирішила ключові проблеми безпеки V1 та V2 шляхом інтеграції механізмів автентифікації та шифрування, а також додала функції віддаленої конфігурації агентів.

3) Syslog є галузевим стандартом для централізованого системного журналювання. Його функціональність полягає у пересиланні та зберіганні системних повідомлень від різних пристроїв (маршрутизаторів, міжмережевих екранів, операційних систем) на єдиний віддалений сервер (колектор журналів). Syslog використовує порт UDP 514 для комунікації, що робить зв'язок ненадійним. Кожен пакет Syslog містить структуровану інформацію, включаючи Timestamp (час події), Hostname (ім'я хоста), Facility (категорія джерела) та Severity (рівень критичності). Рівні критичності, визначені RFC, дають змогу адміністратору швидко оцінити важливість події.

4) WMI (Windows Management Instrumentation). Для глибокого та детального моніторингу операційних систем Microsoft, включно з серверами та критично важливими додатками, застосовується технологія WMI. Це фірмовий

стандарт Microsoft, який дозволяє віддалено збирати значно ширший спектр інформації, ніж SNMP. Це включає детальні дані про стан служб, системні журнали, точне використання пам'яті та завантаження процесора, а також параметри продуктивності додатків, що працюють на сервері. Використання WMI необхідне для гарантування ефективності та стабільності бізнес-додатків, розміщених на платформі Windows, оскільки WMI забезпечує повний контроль над внутрішніми показниками системи.

5) Аналіз мережевих потоків (NetFlow/IPFIX). Критично важливим для моніторингу трафіку є використання технологій аналізу мережевих потоків, зокрема протоколу NetFlow (розроблений компанією Cisco) та його стандартизованого аналога IPFIX (IP Flow Information Export). Ці протоколи збирають детальні метадані про кожен мережевий потік (час, обсяг, IP-адреси джерела та призначення, порти, протоколи). Завдяки NetFlow/IPFIX адміністратори можуть ідентифікувати джерела найбільшого споживання пропускної здатності, виявляти аномалії трафіку (наприклад, ознаки DDoS-атак або несанкціонованої передачі даних) і проводити глибоке мережеве розслідування, відстежуючи активність користувачів у мережі.

1.2 Аналіз існуючих рішень систем моніторингу

Сучасний ринок систем моніторингу мережі відзначається значним розмаїттям, пропонуючи рішення, які можуть задовольнити потреби як малого бізнесу, так і великих корпоративних інфраструктур. Існуючі системи поділяються на дві основні категорії: комерційні (пропрієтарні) рішення, що надають комплексний функціонал, професійну підтримку та високу зручність використання (наприклад, PRTG Network Monitor) та безкоштовні рішення з відкритим кодом (open-source), які вимагають глибших технічних знань для налаштування, але забезпечують неперевершену гнучкість, необмежену масштабованість та відсутність ліцензійних витрат (наприклад, Zabbix, Nagios). Нижче наведено порівняльний аналіз найбільш поширених безкоштовних систем, що використовуються для забезпечення моніторингу мережі та підвищення кіберзахисту [8-10].

1) Zabbix є потужною системою моніторингу корпоративного рівня, яка розповсюджується як безкоштовне відкрите програмне забезпечення, що забезпечує складні функції візуалізації, автоматизації та глибокого моніторингу без необхідності ліцензійних відрахувань, рис.1.1. Система підтримує як агентний, так і безагентний моніторинг, має розподілену архітектуру та функцію автоматичного виявлення пристроїв. Ключова унікальна особливість Zabbix полягає у його потужному механізмі кореляції подій, який здатний аналізувати численні сповіщення для ідентифікації першопричини, що значно знижує "шум" сповіщень та прискорює процес вирішення проблем.

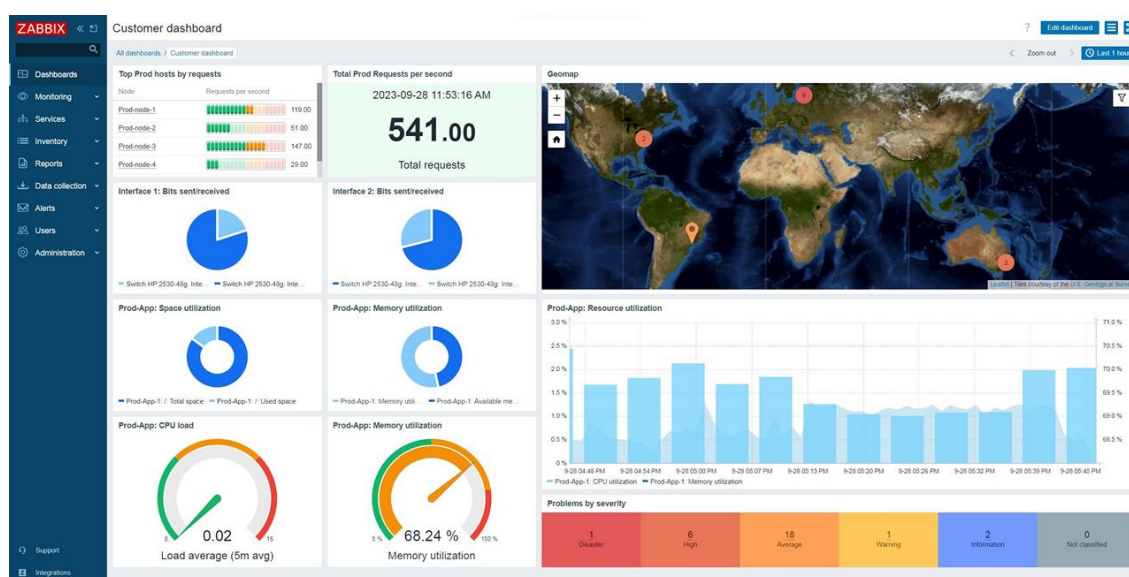


Рисунок 1.1 – Приклад використання Zabbix

Переваги:

- безкоштовне рішення корпоративного рівня, що забезпечує економічну ефективність для організацій;
- відмінна масштабованість для великих та розподілених мереж;
- надійна інтеграція з базами даних та висока продуктивність;
- обширна бібліотека готових шаблонів для швидкого налаштування.

Недоліки:

- складна початкова конфігурація;
- вища крива навчання порівняно з комерційними інструментами;
- веб-інтерфейс менш інтуїтивно зрозумілий, ніж у новіших аналогів;

– вимагає значних ресурсів для дуже великих впроваджень.

2) Prometheus є безкоштовним рішенням з відкритим кодом – хмарно-орієнтованим інструментом моніторингу, головним чином орієнтованим на збір та аналіз часових рядів метрик, рис.1.2. Він ідеально підходить для контейнерних середовищ, таких як Kubernetes, завдяки своїй Pull-архітектурі, де моніторинг здійснюється шляхом опитування цільових об'єктів. Система здатна збирати метрики з серверів, Kubernetes та різних мережевих пристроїв, використовуючи, зокрема, SNMP, а також інспектувати використання пропускної здатності. Для аналізу зібраних даних Prometheus використовує власну мову запитів PromQL, що дозволяє генерувати графіки та таблиці. Важливим компонентом є Alertmanager, який керує усіма налаштованими правилами сповіщень. Prometheus має відмінну інтеграцію з зовнішніми інструментами, наприклад, Grafana, для повноцінної візуалізації метрик.

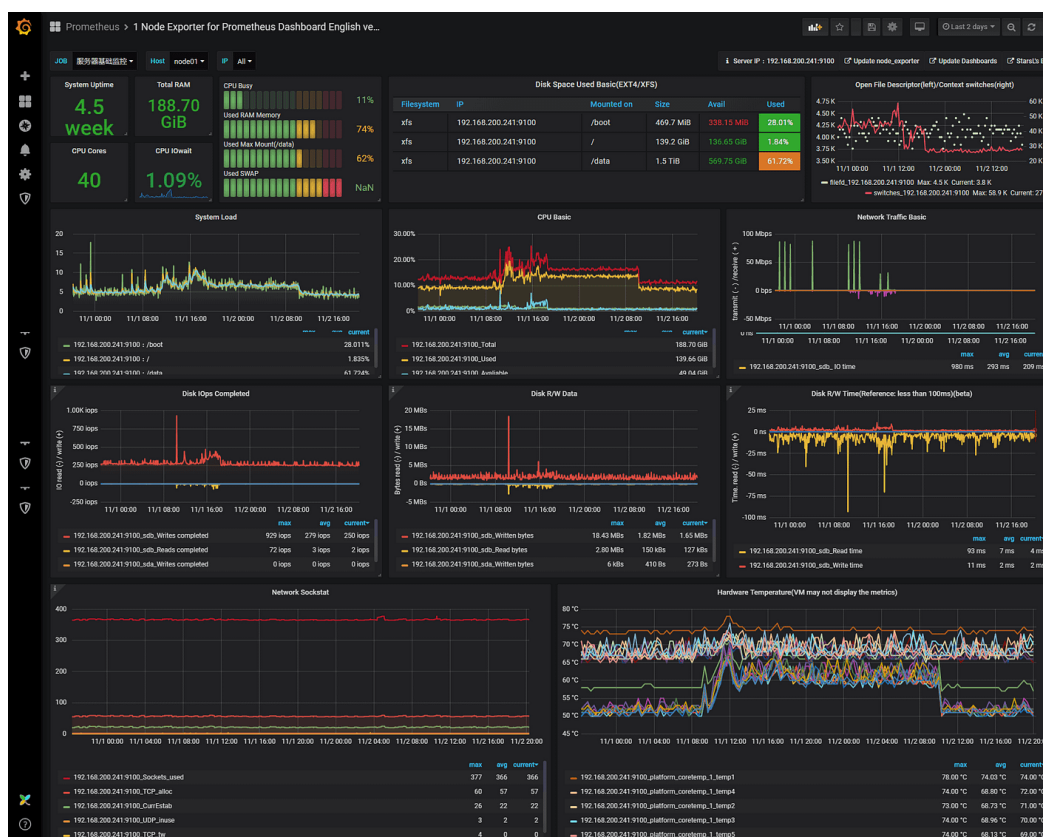


Рисунок 1.2 – Приклад використання Prometheus

Переваги:

– безкоштовне рішення з відкритим кодом;

- ідеальне рішення для контейнеризованих середовищ (Kubernetes);
- ефективне управління часовими рядами метрик та їхня висока швидкість обробки.

- потужна мова запитів PromQL та вбудований Alertmanager.

Недоліки:

- фокус переважно на метриках, менша інтеграція з логами;
- зазвичай вимагає використання зовнішніх інструментів (наприклад, Grafana) для повної візуалізації.

3) Nagios Core вважається піонером у сфері моніторингу з відкритим кодом, який продовжує пропонувати потужний фреймворк із неперевершеною гнучкістю та можливостями налаштування, рис.1.3. Його ключовою унікальною особливістю є розширена екосистема плагінів, яка налічує понад 5000 компонентів, розроблених спільнотою, що дозволяє контролювати практично будь-який пристрій, сервіс чи метрику. Система відома своєю потужною системою сповіщень та обробників подій для автоматизованого виправлення. Головним недоліком рішення є те, що конфігурація здебільшого здійснюється через текстові файли.

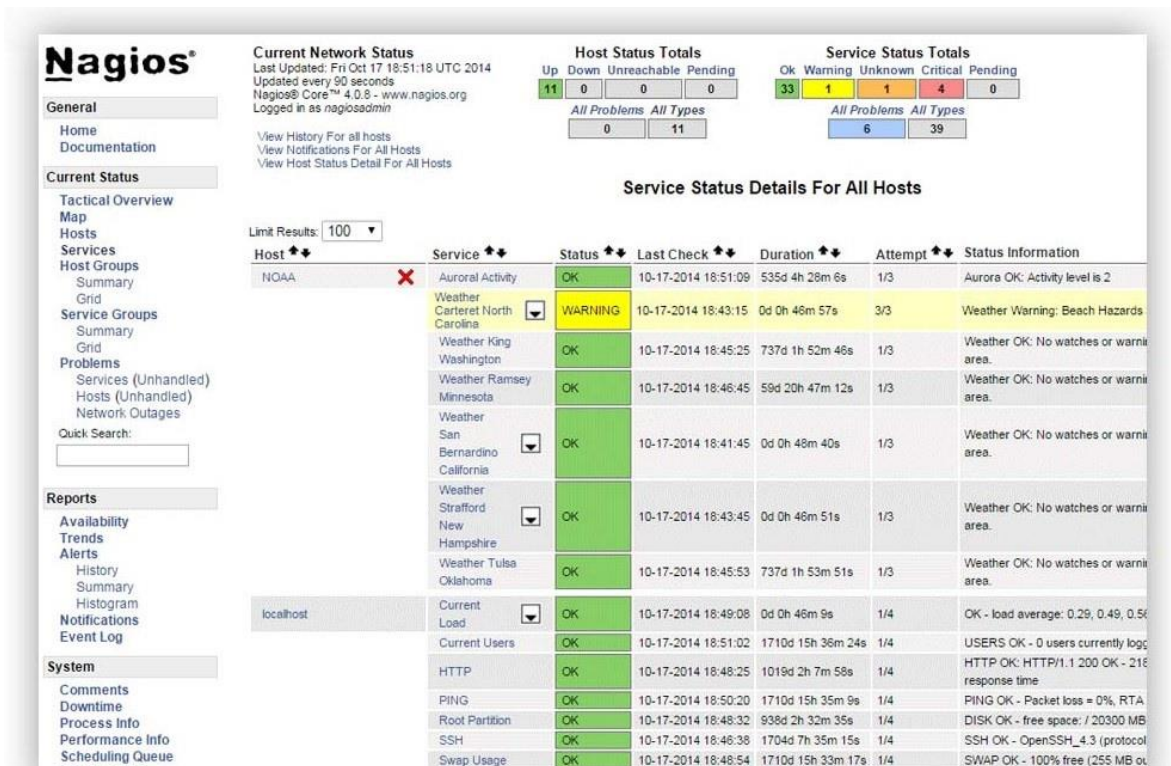


Рисунок 1.3 – Приклад використання Nagios Core

Переваги:

- повністю безкоштовне рішення з відкритим кодом;
- необмежений потенціал налаштування завдяки великій екосистемі плагінів;

- стабільна платформа з обширною документацією.

Недоліки:

- висока крива навчання порівняно з комерційними рішеннями;
- конфігурація переважно через текстові файли;
- менш сучасний користувацький інтерфейс;
- вимагає значно більше ручного налаштування та підтримки.

4) Icinga. Система Icinga була розроблена як відгалуження (fork) Nagios, поєднуючи стабільність свого попередника з сучасним, адаптивним інтерфейсом, покращеною інтеграцією з базами даних та розширеними можливостями звітності, рис.1.4. Icinga є безкоштовним рішенням з відкритим кодом. Її відмінною рисою є модульна архітектура, яка надає організаціям можливість обирати лише необхідні компоненти, створюючи таким чином максимально ефективне та адаптоване рішення. Icinga має вбудований REST API для інтеграції, підтримує моніторинг бізнес-процесів, а конфігурація може здійснюватися як через веб-інтерфейс, так і через конфігураційні файли.

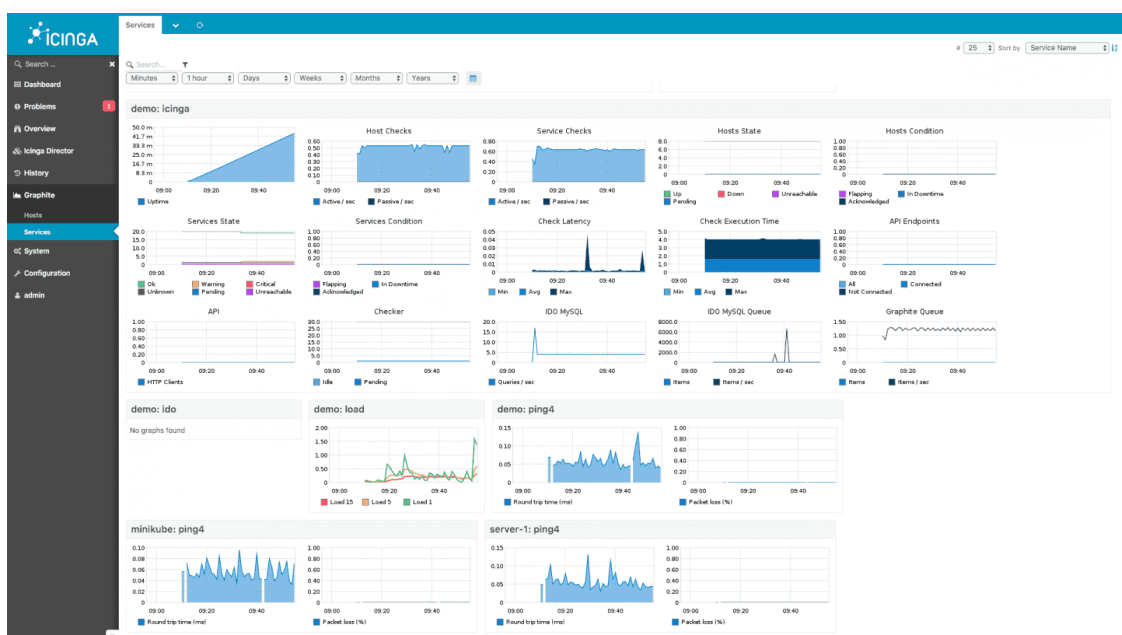


Рисунок 1.4 – Приклад використання Icinga

Переваги:

- безкоштовне рішення з відкритим кодом;
- більш сучасний та зручний інтерфейс, ніж у Nagios;
- краща інтеграція з базами даних, ніж у попередника;
- надійний API для інтеграції та автоматизації.

Недоліки:

- залишається складним у налаштуванні порівняно з комерційними інструментами;
- вимагає технічних знань для коректної конфігурації;
- менш вичерпна документація, ніж у Nagios;
- менша екосистема плагінів порівняно з Nagios.

5) Paessler PRTG Network Monitor (PRTG) є комерційним рішенням, що пропонує уніфікований підхід до моніторингу, який охоплює не лише мережі, а й сервери, додатки та інші ресурси, рис.1.5. Система відома своєю простотою використання, функцією автовиявлення та наявністю понад 200 попередньо налаштованих типів сенсорів. PRTG пропонує безкоштовну версію для невеликих середовищ з обмеженням до 100 сенсорів, що буде достатньою для невеликих мереж. Проте повнофункціональне використання вимагає придбання ліцензії, яка базується на кількості використання сенсорів. Система має зручний інтерфейс, гнучку систему оповіщення та мобільні додатки для контролю стану інфраструктури.

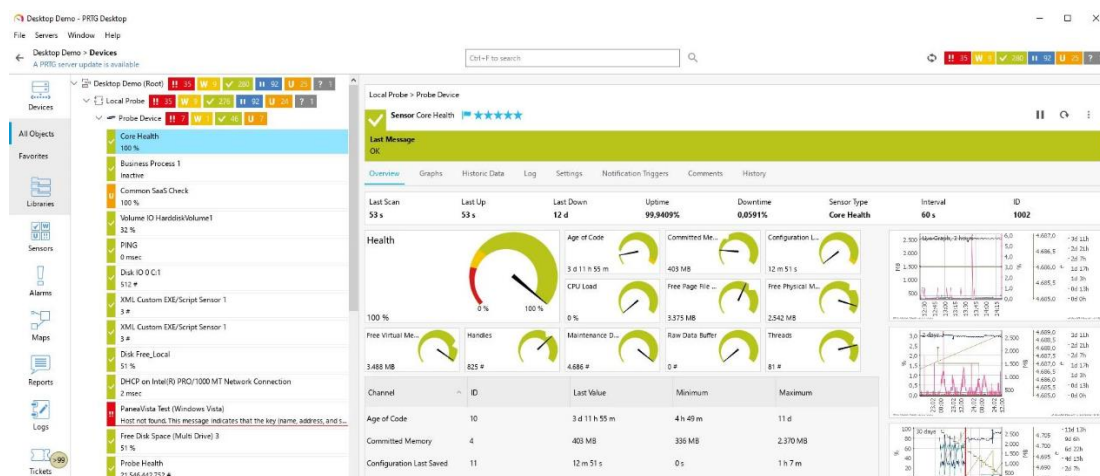


Рисунок 1.5 – Приклад використання PRTG Network Monitor

Переваги:

- прозоре ліцензування;
- комплексний моніторинг, що виходить за межі лише мережевих пристроїв (сервери, додатки);
- зручний інтерфейс, що вимагає мінімальної початкової конфігурації;
- мобільні додатки для моніторингу.

Недоліки:

- може стати дорогим при значному збільшенні кількості сенсорів;
- обмежені можливості гнучкого налаштування порівняно з деякими open-source рішеннями;
- функції звітності можуть бути менш зручними, ніж у спеціалізованих інструментах.

Таблиця 1.1

Таблиця основних характеристик систем моніторингу

	Zabbix	Prometheus	Nagios Core	Icinga	PRTG Network Monitor
Тип рішення	Безкоштовна (Open-Source)	Безкоштовна (Open-Source)	Безкоштовна (Open-Source)	Безкоштовна (Open-Source)	Комерційна (безкоштовна версія до 100 сенсорів)
ОС для розгортання сервера	Linux	Linux, macOS, Windows	Linux	Linux, Windows	Windows
Напрямок	Комплексний моніторинг	Часові ряди метрик	Комплексний моніторинг	Моніторинг, управління бізнес-процесами	Уніфікований моніторинг (мережі, сервери, додатки)
Складність налаштування	Висока (складна початкова конфігурація, висока крива навчання)	Середня/Висока (особливо налаштування Alertmanager та Grafana)	Висока (конфігурація через текстові файли, великий обсяг ручної роботи)	Середня/Висока (полегшена завдяки Web UI, але вимагає експертизи).	Низька/Середня (інтуїтивний інтерфейс, мінімальна початкова конфігурація).
Автоматичне виявлення	Так	Так	Ні (потребує плагінів)	Так	Так

Механізми сповіщення	Вбудований механізм з кореляцією подій	Використовує окремий компонент для обробки сповіщень	Потужна система з обробниками подій	Гнучка система сповіщень	Гнучкі налаштування сповіщення
Ключові переваги	Висока масштабованість; кореляція подій; обширна бібліотека шаблонів	Висока швидкість обробки метрик; потужний PromQL	Необмежений потенціал налаштування; велика екосистема плагінів; стабільна платформа.	Більш сучасний інтерфейс; модульна архітектура; надійний API.	Зручний інтерфейс; сенсорне ліцензування; комплексний моніторинг
Ключові недоліки	Складна початкова конфігурація; висока крива навчання; веб-інтерфейс менш інтуїтивний	Фокус на метриках; вимагає зовнішніх інструментів (Grafana) для візуалізації	Конфігурація через текстові файли; висока крива навчання; вимагає ручного обслуговування	Складна у налаштуванні; менша екосистема плагінів; вимагає технічних знань	Може стати дорогим (при зростанні сенсорів); обмежена кастомізація

На основі проведеного порівняльного аналізу вибір оптимального рішення для реалізації проєкту моніторингу повинен ґрунтуватись на дотриманні балансу між функціональністю, складністю впровадження та оперативністю розгортання. Хоча системи з відкритим кодом (Zabbix, Nagios, Prometheus) пропонують необмежену масштабованість, відкрите налаштування та можливість розгортання на Linux, їхня складність підтримки та значні витрати часу на первинне налаштування є одним з негативних стримуючих факторів. На противагу цьому, Paessler PRTG Network Monitor, попри свій комерційний статус, вирізняється мінімальною складністю налаштування, гнучкого механізму відправки сповіщень широким обсягом сенсорів та інтуїтивним інтерфейсом, що дозволяє швидко розгорнути комплексний моніторинг серверів і мережевих пристроїв. Враховуючи, що PRTG надає постійну безкоштовну версію з лімітом до 100 сенсорів, цього обсягу цілком достатньо для ефективного покриття потреб невеликої мережі. А із зростанням кількості сенсорів можна буде додатково оформити ліцензію. Таким чином, PRTG Network Monitor є найбільш доцільним

вибором для швидкого, надійного та зручного впровадження системи моніторингу мережі будь-якого розміру.

1.3 Структура та функціональні можливості PRTG Network Monitor

PRTG Network Monitor – це інструмент моніторингу мережі, розроблений компанією Paessler AG. Розгортання PRTG Core Server здійснюється на операційних системах Microsoft Windows (зокрема Windows Server 2022, 2019, 2016, а також Windows 11 та 10). Він є одним із найпопулярніших рішень на ринку, пропонуючи як корпоративну, так і безкоштовну версію з обмеженими можливостями. Інструмент допомагає адміністраторам відстежувати стан і продуктивність усієї IT-інфраструктури, включаючи сервери, комутатори, маршрутизатори та додатки. PRTG підтримує різні типи моніторингу, зокрема SNMP, Syslog, WMI, NetFlow, jFlow, sFlow, IPFIX та аналіз пакетів (packet sniffing), забезпечуючи глибоке розуміння продуктивності мережі та потенційних проблем. Система надає оновлення у реальному часі та детальні звіти, що сприяє швидкій діагностиці несправностей. Продукт поставляється з понад 200 типами попередньо встановлених сенсорів для централізованого багатосистемного моніторингу з можливістю створювати індивідуальні сенсори для відстеження доступності певних служб. Завдяки централізованому дашборду з налаштованими віджетами, PRTG забезпечує зручний моніторинг ключових показників. Інструмент може бути розгорнутий як локально, так і у хмарі [11].

Механізми збору даних PRTG

PRTG отримує дані про стан мережі, використовуючи широкий спектр стандартних протоколів, що забезпечує комплексний контроль [12]:

- базовий моніторинг. Використовуються Ping та SNMP для перевірки доступності пристроїв та збору основних метрик;
- веб-сервіси. Здійснюються веб-запити через HTTP та HTTPS;
- електронна пошта. Застосовуються протоколи POP3, IMAP, SMTP для моніторингу поштових служб;
- апаратні параметри. Використовується SNMP, SSH та SOAP (Simple Object Access Protocol);

– використання пропускну́ї здатності. Застосовуються технології Flow (включно з NetFlow, jFlow, sFlow, IPFIX), Packet Sniffing (аналіз пакетів) та SNMP;

– системи Windows. Використовуються засоби Windows Management Instrumentation (WMI) для глибокого моніторингу операційних систем.

– інші інтерфейси. Забезпечується використання SSH та скриптів (наприклад, PowerShell та Python) для гнучкого розширення функціоналу.

Ключові функціональні можливості PRTG

Функціонал PRTG є комплексним і містить низку особливостей, які роблять його ефективним інструментом для адміністраторів.

1) Моніторинг мережі. PRTG пропонує моніторинг у реальному часі за мережевими пристроями, включаючи маршрутизатори, комутатори, міжмережеві екрани та точки доступу Wi-Fi. Надає інформацію про трафік, затримку, втрату пакетів та інші параметри, забезпечуючи безперебійну роботу мережі.

2) Моніторинг серверів та пристроїв. Здійснюється контроль стану та продуктивності серверів. Відстежуються ключові параметри, такі як використання CPU, пам'яті, дискового простору, а також надсилаються сповіщення про апаратні збої.

3) Моніторинг додатків. PRTG може контролювати роботу різних критично важливих додатків, таких як Microsoft Exchange, SQL, Apache, забезпечуючи їхню ефективну та оптимізовану продуктивність.

4) Моніторинг хмарних середовищ. Система підтримує Amazon Web Services (AWS), Microsoft Azure, Google Cloud та інші хмарні служби, забезпечуючи повну видимість розподіленої інфраструктури, незалежно від того, розміщена вона у хмарі чи локально.

5) Інтерфейс, візуалізація та доступність. PRTG пропонує п'ять різних користувацьких інтерфейсів, включаючи HTTP- та SSL-доступ із будь-якого ПК, а також спеціальні мобільні додатки для iPad або інших пристроїв. Система має

зручний графічний інтерфейс для відображення живих та історичних даних та дозволяє створювати власні дашборди.

6) Комплексний моніторинг. Система пропонує понад 200 типів попередньо налаштованих сенсорів, які покривають усі аспекти мережевого контролю, включаючи моніторинг додатків, сервісів, QoS, SLA, LAN, WAN, VPN, а також часу роботи та простою мережі.

7) Гнучке сповіщення. PRTG надає сповіщення за допомогою різних механізмів – електронної пошти, SMS та SNMP. Можливе налаштування складних умов сповіщення (наприклад, видача сповіщення, якщо умови X та Y є істинними).

8) Розподілений моніторинг. Система підтримує розподілений моніторинг, який дозволяє головному офісу відстежувати всі віддалені об'єкти, а також окремі мережі всередині компанії (наприклад, DMZ та LAN).

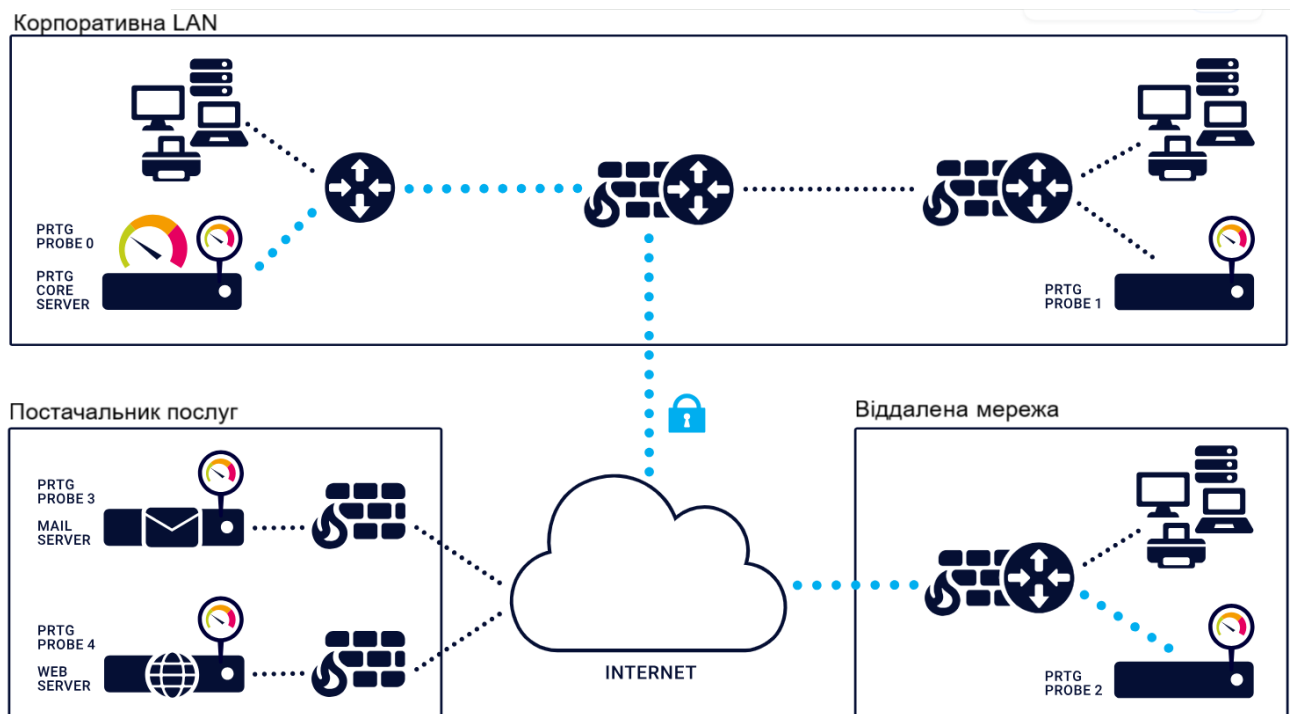


Рисунок 1.6 – Розподілений моніторинг через віддалені зонди (probes)

9) Детальна звітність. Інструмент надає можливість отримання поглиблених звітів у форматах HTML або PDF з можливістю налаштувати автоматичну періодичну генерацію за визначені дати. Моніторингові дані можуть бути експортовані у форматах HTML, XML, CSV.

10) Кластеризація та відмовостійкість (Clustering & HA). Для забезпечення 100% безвідмовної роботи доступна функція кластеризації (Clustering). Кластер PRTG складається з головного (Primary Master) та резервних (Failover) вузлів. У разі відмови головного вузла, майстер-роль автоматично перебирає на себе резервний вузол, що гарантує безперервний моніторинг [13].

Висновок до першого розділу

У ході роботи над розділом було визначено, що система моніторингу мережі (NMS) є ключовим програмно-апаратним комплексом, що став важливим інструментом для забезпечення проактивного виявлення несправностей та кіберзахисту. Ефективна система моніторингу повинна мати інтегровану функціональність, що включає автоматичне виявлення ресурсів, глибокий моніторинг продуктивності, централізовану візуалізацію (дашборди) та аналіз історичних даних. Не менш важливим є підтримка масштабованості та відмовостійкості. Реалізація функцій моніторингу базується на стандартизованих протоколах, серед яких Ping (доступність), SNMP (метрики та безпека), WMI (моніторинг Windows), Syslog (централізоване журналювання) та NetFlow/IPFIX (аналіз трафіку), забезпечуючи адміністратору єдину панель управління для оперативного реагування.

У ході аналізу існуючих рішень було встановлено, що ринок систем моніторингу поділяється на дві основні категорії: безкоштовні open-source інструменти (Zabbix, Prometheus, Nagios Core, Icinga) та комерційні системи (Paessler PRTG Network Monitor). Рішення з відкритим кодом пропонують необмежену масштабованість, гнучкість налаштування (часто на Linux) та нульові ліцензійні витрати, але вимагають високої технічної експертизи та значних ресурсів на первинну конфігурацію. Рішення PRTG, хоча й є комерційним (з безкоштовною версією до 100 сенсорів) та розгортається на Windows, проте вирізняється мінімальною складністю налаштування, зручним уніфікованим інтерфейсом та швидким розгортанням.

Під час розгляду структури та функціональних можливостей було встановлено, що PRTG Network Monitor є уніфікованим комерційним

інструментом, розробленим для забезпечення комплексного моніторингу всієї ІТ-інфраструктури. Його ключова перевага полягає у низькій складності налаштування, централізованому підході та використанні понад 200 попередньо налаштованих сенсорів для відстеження мереж, серверів, додатків та хмарних сервісів (AWS, Azure). PRTG використовує широкий спектр протоколів збору даних, включаючи SNMP, WMI, NetFlow/IPFIX та Packet Sniffing. Для забезпечення надійності та масштабованості система підтримує розподілений моніторинг за допомогою Remote Probes і опціональну кластеризацію, що забезпечує безвідмовну роботу завдяки автоматичному переходу на резервний вузол. Комплексний функціонал доповнюється гнучким механізмом сповіщень, інтуїтивно зрозумілим інтерфейсом, мультиплатформенним доступом та гнучкою можливістю створення звітів.

Підсумовуючи, у результаті проведеного аналізу визначено основні принципи побудови систем моніторингу мережевої інфраструктури, їх переваги та обмеження. На основі порівняльного аналізу обґрунтовано вибір системи PRTG Network Monitor як оптимального рішення для реалізації завдання моніторингу корпоративної мережі, що поєднує високу продуктивність, гнучкість налаштувань і зручність адміністрування. Це рішення стане основою для подальшого проєктування й практичної реалізації системи у наступних розділах роботи.

РОЗДІЛ 2 ПРОЄКТУВАННЯ СИСТЕМИ МОНІТОРИНГУ МЕРЕЖІ З ВИКОРИСТАННЯМ PRTG NETWORK MONITOR

2.1. Розробка проєкту комп'ютерної мережі

Вибір топології локальної мережі є одним із ключових етапів проєктування, оскільки саме вона визначає взаємозв'язок між пристроями та ефективність роботи всієї інфраструктури. Топологія може описувати як фізичне розташування обладнання (комутаторів, маршрутизаторів, серверів, робочих станцій), так і логічні шляхи їх взаємодії між собою. Від правильності вибраної структури залежить продуктивність, стабільність і масштабованість мережі, а також спрощується пошук і усунення несправностей.

Основними факторами, які впливають на вибір топології, є кількість користувачів, масштаби майбутнього розширення, вимоги до пропускну здатності, надійності та безпеки. Також враховуються економічні аспекти, зокрема вартість прокладання кабельної інфраструктури, встановлення активного обладнання та подальшого обслуговування. При проєктуванні важливо передбачити можливість швидкого усунення несправностей, а також можливість майбутнього розширення без суттєвих змін у мережевій архітектурі.

Оптимальним рішенням для побудови локальної мережі є використання трирівневої моделі, яка складається з рівня ядра, рівня розподілу та рівня доступу, рис.2.1. Такий підхід забезпечує масштабованість, гнучкість та високий рівень відмовостійкості. Завдяки цій структурі мережа легко адаптується до зростання кількості вузлів та забезпечує зручне централізоване управління [14].

Щоб детально оцінити можливості використання даного підходу, доцільно розглянути функції кожного з рівнів окремо. Кожний з них виконує власні завдання, але водночас тісно пов'язаний з іншими, формуючи єдину і узгоджену інфраструктуру.

Хоча даний підхід і потребує більших витрат та складнішого планування, в перспективі це забезпечує довгострокову надійність і простіше розширення мережі.

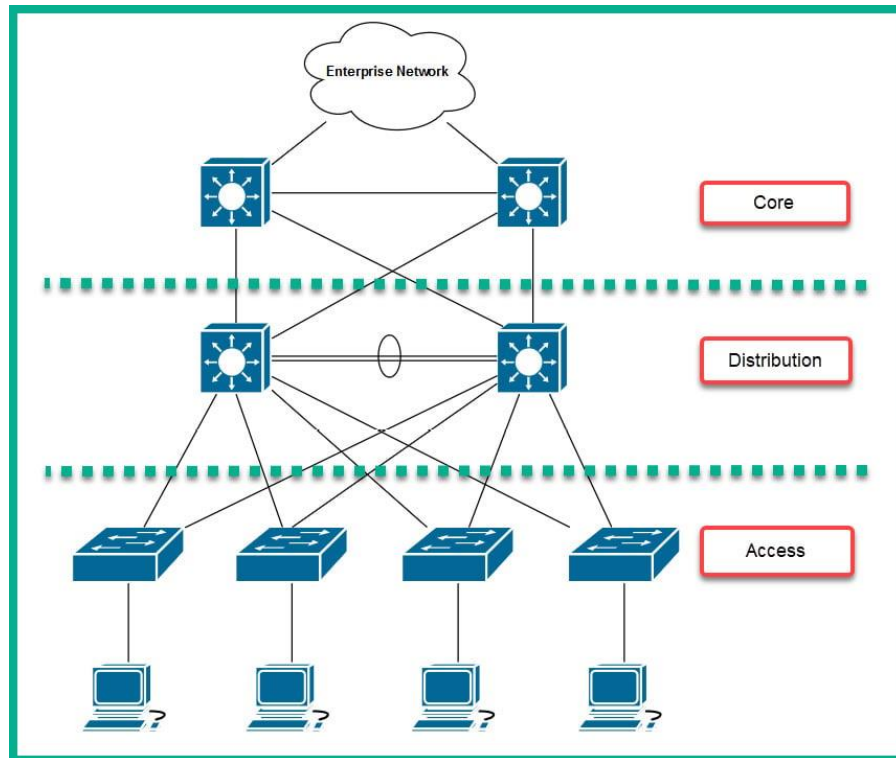


Рисунок 2.1 – Трирівнева модель мережі

Рівень доступу (Access Layer) є базовим рівнем у трирівневій моделі мережі, який забезпечує підключення кінцевих пристроїв користувачів: комп'ютерів, ноутбуків, принтерів, IP-телефонів та інших клієнтських вузлів. На цьому рівні реалізуються механізми початкової аутентифікації, контролю доступу та сегментації трафіку. Даний рівень має велике значення для зручності адміністрування, оскільки саме тут визначається, які ресурси доступні користувачам. Вдосконалення рівня доступу напряду впливає на комфорт роботи співробітників та якість обслуговування кінцевих пристроїв.

Рівень розподілу (Distribution Layer) виконує функції агрегації трафіку з рівня доступу та відповідає за впровадження політик безпеки, маршрутизації між VLAN, балансування навантаження й контроль доступу до ресурсів. Це проміжна ланка між кінцевими вузлами і ядром мережі, яка дозволяє централізовано застосовувати політики та спрощує адміністрування складних інфраструктур. Саме на цьому рівні адміністратори можуть впроваджувати механізми резервування, які підвищують відмовостійкість, а також забезпечувати ефективне використання ресурсів мережі.

Рівень ядра (Core Layer) виконує роль високошвидкісного магістрального сегмента, який з'єднує всі підсистеми мережі та забезпечує надійний транзит великих обсягів даних між ними. Його головні характеристики – висока пропускна здатність, мінімальні затримки та відмовостійкість завдяки дублюванню каналів і обладнання. Рівень ядра забезпечує основу для стабільної роботи критично важливих сервісів, таких як корпоративні додатки, системи зберігання даних та зовнішні комунікації.

Спираючись на принципи побудови трирівневої моделі, для проєкту було розроблено відповідну структурну топологію мережі невеликої організації. Нижче наведено її структурну схему, що демонструє логічну організацію мережі, розподіл функцій між різними сегментами та кількість пристроїв, рис.2.2.

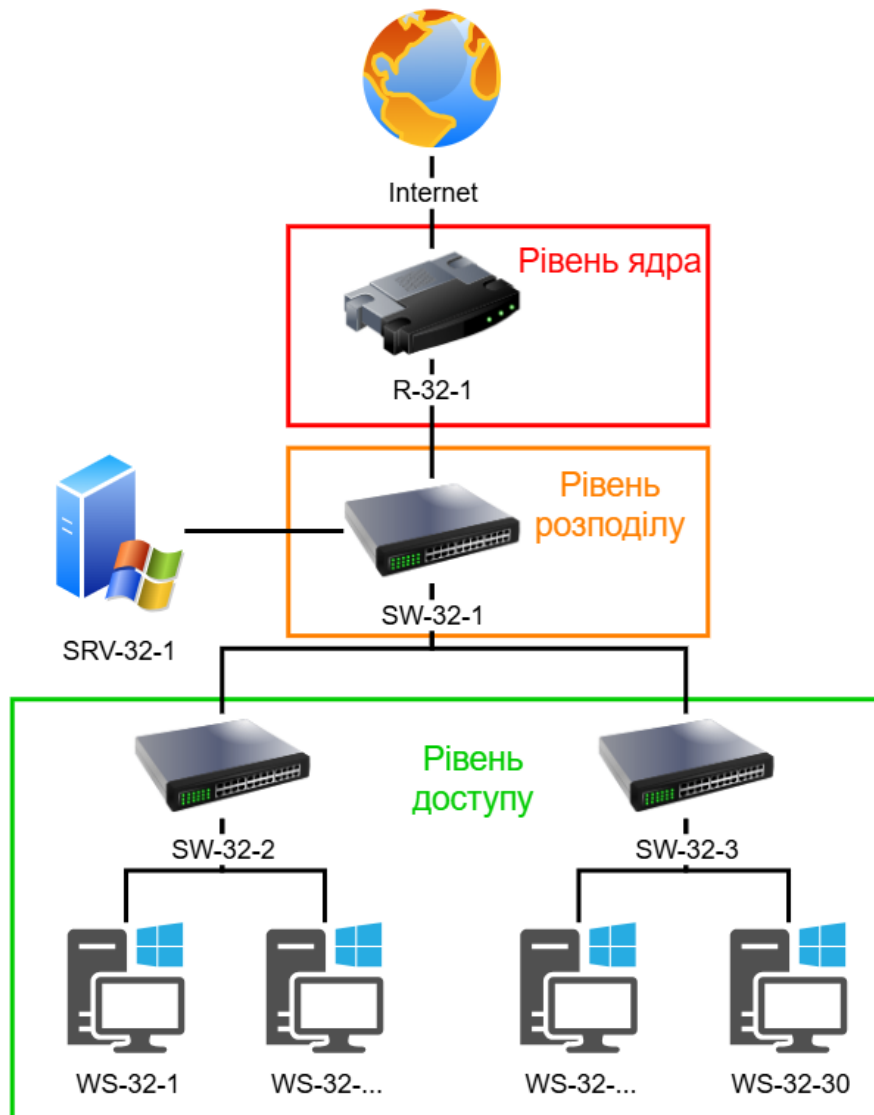


Рисунок 2.2 – Структурна схема мережі

Детальніше розглянемо кожен рівень. На рівні ядра присутній маршрутизатор R-32-1, який забезпечує доступ пристроїв локальної мережі до Інтернету.

На рівні розподілу знаходиться комутатор SW-32-1, що забезпечує взаємодію між усіма іншими пристроями, а також зв'язок з маршрутизатором R-32-1. До даного комутатора також підключений SRV-32-1 на ОС Windows Server 2022.

На рівні доступу розміщені комутатори SW-32-2 та SW-32-3, до яких підключені клієнтські станції WS-32-1, WS-32-..., WS-32-... та WS-32-30 через виту пару. Обидва комутатори рівня доступу підключені до комутатора рівня розподілу SW-32-1.

Використання трирівневої топології при розробці мережі забезпечує чітке розмежування функцій: маршрутизатор на рівні ядра керує підключенням до Інтернету, комутатор на рівні розподілу забезпечує з'єднання між пристроями та управління трафіком, а до комутаторів на рівні доступу підключені робочі станції до загальної мережі. Така структура покращує ефективність мережі, полегшує адміністрування і забезпечує кращу масштабованість та надійність.

Загалом в проєкті використано 1 маршрутизатор, 3 комутатори, 1 сервер та щонайменше 30 клієнтських станцій працівників.

Під час проєктування мережі не менш важливо правильно спланувати розподіл IP-адресації для ефективного використання наявного простору. У даному випадку передбачено окрему публічну мережу для каналу маршрутизатора до Інтернету та одну локальну. При цьому всі пристрої локальної мережі будуть включені до домену ferenz.net

R-32-1 – Internet: 205.125.32.0/30

R-32-1 – SW-32-1: 192.168.32.0/24

Детальний розрахунок адрес для локальної мережі наведений нижче на табл.2.1.

Адресація локальної мережі

Призначення адрес	IP-адреса
Адреса мережі	192.168.32.0
Маска мережі	255.255.255.0(/24)
Мінімальна адреса	192.168.32.1
Максимальна адреса	192.168.32.254
Шлюз за замовчуванням	192.168.32.254
Призначені комутаторам	192.168.32.250 – 192.168.32.252
Діапазон адрес майбутніх пристроїв	192.168.32.1 – 192.168.32.30
Діапазон вільних адрес	192.168.32.31 – 192.168.32.229

Нижче на рис.2.3 представлено фізичну топологію мережі із зазначеними параметрами адресації для пристроїв мережі.

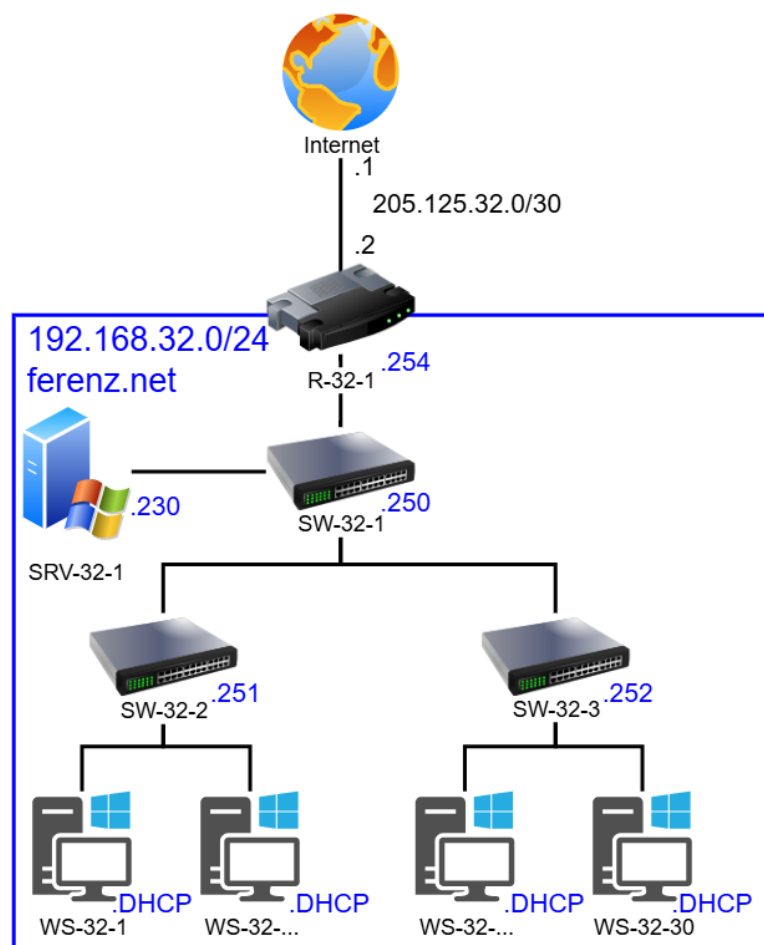


Рисунок 2.3 – Фізична топологія мережі

2.2 Проєктування роботи системи моніторингу

PRTG підтримує понад 200 типів сенсорів для всіх поширених мережевих сервісів, зокрема HTTP, SMTP/POP3, FTP та інші. Підтримуються такі основні протоколи та методи збору даних: SNMP (v1, v2c, v3), WMI для пристроїв Windows, NetFlow (V5, V9), IPFIX, sFlow, jFlow, а також пакетний аналіз (Packet Sniffing) [15].

В даному проєкті сервер PRTG буде розміщений на сервері SRV-32-1 під керуванням Windows Server 2022. Розміщення PRTG саме на даному сервері дозволяє централізувати збір даних, мінімізувати затримки при комунікації з клієнтами. Клієнтами ж в даній структурі виступатимуть усі інші мережеві та кінцеві пристрої локальної мережі і відповідно сам сервер.

Дані до сервера PRTG будуть надходити з використанням наступних протоколів:

- SNMPv3: комутатори SW-32-1, SW-32-2, SW-32-3 та маршрутизатор R-32-1. Використання SNMPv3 забезпечує безпечний збір інформації про стан пристроїв, навантаження інтерфейсів та інші системні показники без необхідності встановлення додаткового програмного забезпечення на пристрої;
- Syslog: маршрутизатор R-32-1 та комутатори. Syslog забезпечує централізований збір і зберігання системних подій, журналів безпеки та повідомлень про помилки з мережевих пристроїв.
- NetFlow v9: маршрутизатор R-32-1. NetFlow дозволяє детально аналізувати мережевий трафік і облік потоків, що особливо важливо для оцінки завантаженості каналів та планування пропускну здатності. Вибір останньої версії v9 обумовлений її підтримкою розширених даних про потоки та гнучкістю для інтеграції з PRTG.
- WMI: кінцеві станції Windows. WMI забезпечує збір інформації про апаратні ресурси, процеси, сервіси та інші показники стану ОС Windows, що дозволяє відстежувати роботу робочих станцій у реальному часі без встановлення стороннього програмного забезпечення.

Вибір саме цих протоколів збору даних зумовлений їх функціональними можливостями та доцільністю використання. Syslog, SNMP і NetFlow забезпечують моніторинг мережевих пристроїв і каналів зв'язку, надаючи детальну статистику про завантаженість інтерфейсів і структуру трафіку. WMI використовується для контролю стану серверів та робочих станцій Windows, що дозволяє відстежувати роботу апаратних ресурсів і сервісів без необхідності встановлення додаткового програмного забезпечення. У комплексі ці протоколи формують цілісну картину стану мережевої інфраструктури та забезпечують можливість своєчасного реагування на збої чи відхилення у роботі системи.

Нижче на рис.2.4 наведено візуальну організацію збору даних у проєкті мережі з позначенням протоколів, що застосовуються.

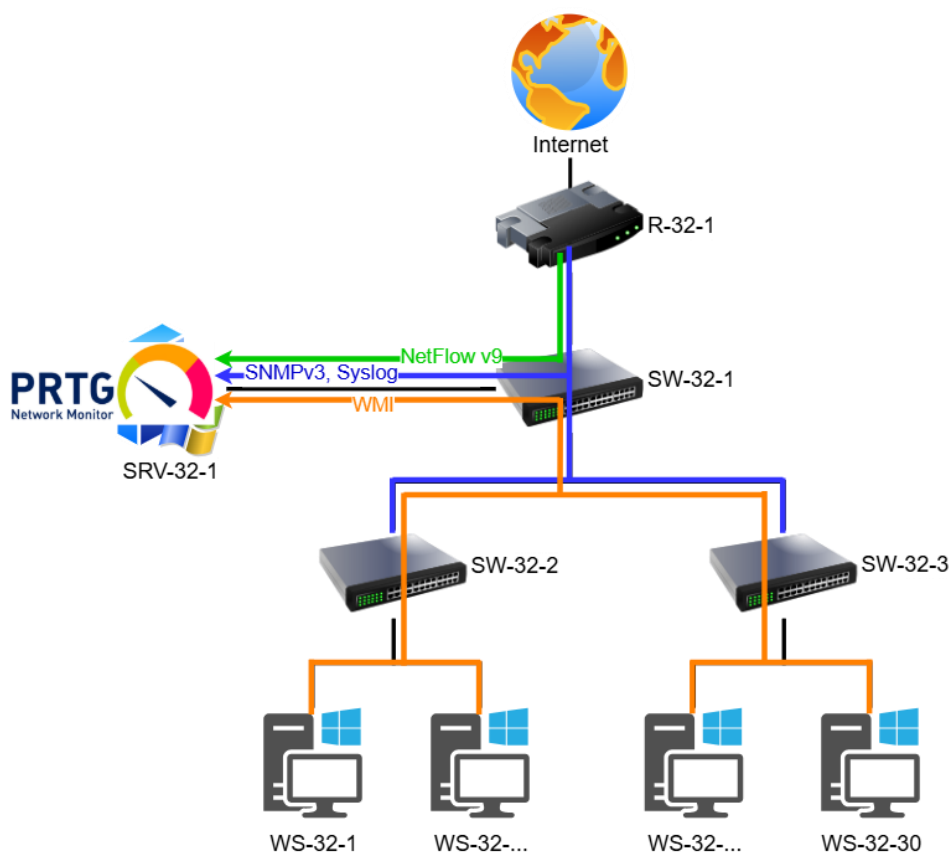


Рисунок 2.4 – Структура передачі даних до сервера PRTG в проєкті мережі

2.3 Вибір обладнання

Ключовим етапом проєктування є підбір обладнання. Під час вибору маршрутизатора необхідно враховувати його продуктивність, кількість та типи інтерфейсів, здатність до масштабування, наявність функцій безпеки й

управління трафіком, рівень надійності, вартість, підтримку актуальних протоколів, а також можливості для віддаленого адміністрування.

Тому модель Cisco ISR4321/K9 є вдалим вибором для побудови захищеної корпоративної мережі організацій будь-якого розміру, рис.2.5. Дана модель належить до серії інтегрованих сервісних маршрутизаторів і працює під керуванням програмного забезпечення Cisco IOS XE, що забезпечує високу продуктивність, масштабованість і гнучкість у впровадженні нових сервісів. Завдяки апаратному прискоренню шифрування пристрій ефективно підтримує VPN-з'єднання, включаючи IPsec та L2TP, а також гарантує безпечний доступ для мобільних користувачів. Модульний форм-фактор із двома слотами NIM дозволяє розширювати функціональні можливості маршрутизатора під потреби конкретної мережі. Наявність сучасних протоколів (DHCP, PPPoE, IPsec) і інтерфейсів (2 порти Gigabit Ethernet RJ-45, 1 SFP, 1 USB 2.0) робить Cisco ISR4321/K9 універсальним та надійним рішенням для організацій, що потребують стабільного та безпечного мережевого середовища [16].



Рисунок 2.5 – Маршрутизатор Cisco ISR 4321/K9

Під час визначення відповідної моделі комутатора необхідно звертати увагу на пропускну здатність, кількість і тип портів, можливість масштабування та резервування, наявність механізмів безпеки й керування трафіком, надійність обладнання, відповідність сучасним стандартам і протоколам, а також підтримка відповідних засобів для централізованого або віддаленого адміністрування.

Модель Cisco Catalyst 1300 є вдалим вибором для побудови надійної корпоративної мережі малого чи середнього підприємства, рис.2.6. Це керований комутатор рівня L2/L3, що поєднує гнучкість, високу продуктивність та розширені можливості безпеки. Завдяки наявності 48 Gigabit Ethernet портів та 4

SFP+ інтерфейсів він забезпечує масштабованість та підтримує підключення великої кількості пристроїв, в тому числі з використанням PoE для живлення IP-телефонів або точок доступу. Пропускна здатність у 176 Гбіт/с та підтримка пакетної продуктивності понад 130 млн пакетів за секунду гарантують стабільну роботу навіть у ресурсоємних сценаріях. Комутатор підтримує сучасні протоколи керування, зокрема SNMP, який дозволяє інтегрувати його з системами моніторингу. Завдяки надійності, простоті адміністрування та широкому набору функцій серія Catalyst 1300 забезпечує ефективне управління трафіком, сегментацію мережі та високу безпеку, роблячи її оптимальним рішенням для сучасних офісних інфраструктур [17].



Рисунок 2.6 – Комутатор Cisco Catalyst 1300-48P-4X

Для організації роботи серверу SRV-32-1 було обрано операційну систему Windows Server 2022, яка забезпечує широкий спектр серверних ролей, ефективне управління ресурсами та високий рівень безпеки. На цьому сервері планується розміщення системи моніторингу PRTG Network Monitor, що вимагає стабільної роботи при обробці великої кількості даних від мережевих пристроїв та кінцевих станцій. Для цього обрано багатоядерний процесор Intel Xeon, 32 ГБ оперативної пам'яті DDR4, SSD-накопичувач об'ємом 1 ТБ для швидкого доступу до даних та мережевий інтерфейс Gigabit Ethernet для надійного обміну інформацією. Така конфігурація дозволяє PRTG збирати, зберігати та обробляти статистику від пристроїв, та своєчасно формувати сповіщення про неполадки або аномалії в роботі мережевої інфраструктури, забезпечуючи ефективне керування мережею.

Для кінцевих робочих станцій було обрано використання ОС Windows 10, яка забезпечує стабільну та сумісну платформу для роботи користувачів, а також підтримує функції WMI для віддаленого збору даних системи. Вибір Windows 10

зумовлений її широким розповсюдженням, надійністю та здатністю підтримувати сучасні корпоративні протоколи та безпекові механізми. Для ефективного роботи всі станції оснащені процесорами Intel Core i5 або вище, 8–16 ГБ оперативної пам'яті, SSD-дисками об'ємом від 256 ГБ для швидкого доступу до даних та гігабітними мережевими картами. Така конфігурація забезпечує стабільну швидку роботу додатків та легку інтеграцію з системою моніторингу.

Висновки до другого розділу

У першому підрозділі було виконано розробку проекту комп'ютерної мережі, обґрунтовано вибір трирівневої моделі та детально описано функції рівнів ядра, розподілу та доступу. Було визначено структуру підключення мережеских пристроїв, включаючи маршрутизатор R-32-1 для доступу до Інтернету, комутатори SW-32-1, SW-32-2 та SW-32-3 та підключення кінцевих станцій, а також сервер SRV-32-1. Окремо було спроектовано IP-адресацію мережі та продемонстровано фізичну та логічну топології мережі, що забезпечує чітке розмежування функцій, ефективне управління трафіком, масштабованість і надійність інфраструктури.

Було спроектовано роботу системи моніторингу на базі PRTG, визначено сервер SRV-32-1, як центральний елемент збору даних та описано джерела інформації від усіх пристроїв. Було обґрунтовано використання SNMPv3 та Syslog для комутаторів та маршрутизатора, NetFlow v9 для мережевого трафіку на маршрутизаторі та WMI для моніторингу кінцевих станцій Windows, що разом дозволяє отримувати повну і актуальну інформацію про стан інфраструктури без встановлення додаткового ПЗ на пристрої.

Наостанок було виконано обґрунтування вибору обладнання для побудови проекту мережі. Обрано маршрутизатор Cisco ISR4321/K9 та комутатор Cisco Catalyst 1300, що забезпечують високу продуктивність, безпеку та підтримку сучасних мережеских протоколів. А сервер на ОС Windows Server 2022 та станції з ОС Windows 10 забезпечать стабільну та ефективну роботу мережевої інфраструктури організації.

РОЗДІЛ 3 ПОБУДОВА, НАЛАГОДЖЕННЯ ТА ТЕСТУВАННЯ РОБОТИ МЕРЕЖІ

3.1 Первинне налаштування мережевої інфраструктури

Для тестування та відпрацювання конфігурації мережі буде використовуватися емулятор GNS3 [18], що дозволяє створювати віртуальні мережі з комплексною структурою. Програма підтримує інтеграцію з віртуальними машинами та різними образами операційних систем, які дають змогу моделювати роботу серверів і робочих станцій у реальному середовищі. Завдяки інтуїтивному інтерфейсу можна ефективно налагоджувати з'єднання, перевіряти маршрутизацію та тестувати різні мережеві сценарії. Схема проєкту мережі в емуляторі наведена на рис.3.1.

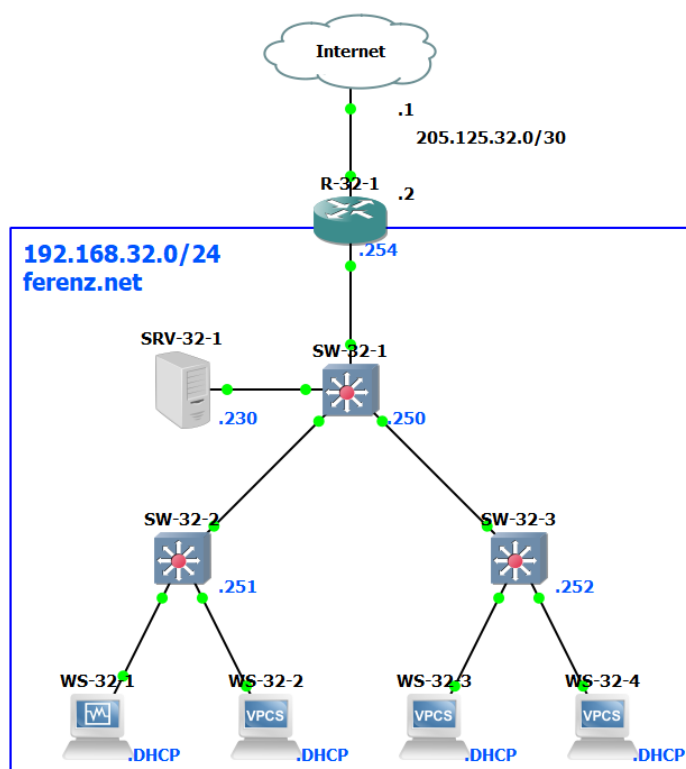


Рисунок 3.1 – Проєкт в мережі GNS3

Перейдемо до налагоджень. Спершу на маршрутизаторі R-32-1 було виконано базову конфігурацію. Змінено ім'я хоста на R-32-1, налаштовано інтерфейси FastEthernet 0/0 та 0/1 з відповідними IP-адресами для з'єднання з Інтернетом та комутатором SW-32-1. Визначено NAT для трансляції внутрішніх

адрес у зовнішній інтерфейс. Встановлено доменне ім'я ferenz.net, налаштовано DNS-сервер із адресою 192.168.32.230. Створено список доступу для внутрішньої мережі та прописано маршрут за замовчуванням до шлюзу 205.125.32.1 для забезпечення виходу в Інтернет, рис.3.2.

```
R-32-1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R-32-1(config)#hostname R-32-1
R-32-1(config)#interface fa0/0
R-32-1(config-if)#description LINK-TO-INTERNET
R-32-1(config-if)#ip address 205.125.32.2 255.255.255.252
R-32-1(config-if)#ip nat outside
R-32-1(config-if)#no shutdown
R-32-1(config-if)#exit
R-32-1(config)#interface fa0/1
R-32-1(config-if)#description LINK-TO-SW-32-1
R-32-1(config-if)#ip address 192.168.32.254 255.255.255.0
R-32-1(config-if)#ip nat inside
R-32-1(config-if)#no shutdown
R-32-1(config-if)#exit
R-32-1(config)#ip domain-name ferenz.net
R-32-1(config)#ip domain-lookup
R-32-1(config)#ip dns server
R-32-1(config)#ip name-server 192.168.32.230
R-32-1(config)#access-list 1 permit 192.168.32.0 0.0.0.255
R-32-1(config)#ip nat inside source list 1 interface fastethernet 0/0 overload
R-32-1(config)#ip route 0.0.0.0 0.0.0.0 205.125.32.1
```

Рисунок 3.2 – Налаштування маршрутизатора R-32-1

Для підвищення безпеки та запобігання несанкціонованому доступу до мережі виконується виконано виділення окремого VLAN для невикористовуваних портів. Для цього, було створено VLAN 999 із назвою UNUSED-PORTS. Далі для всіх непідключених портів (eth0/1-3, eth1/0-3, eth2/0-3, eth3/0) встановлено режим доступу (access) і прив'язано їх до VLAN 999, після чого порти були відключені (shutdown). Аналогічні дії виконуються і на інших комутаторах мережі, рис.3.3.

```
SW-32-1(config)#vlan 999
SW-32-1(config-vlan)#name UNUSED-PORTS
SW-32-1(config-vlan)#exit
SW-32-1(config)#interface range eth0/1-3, eth1/0-3, eth2/0-3, eth3/0
SW-32-1(config-if-range)#switchport mode access
SW-32-1(config-if-range)#switchport access vlan 999
SW-32-1(config-if-range)#shutdown
```

Рисунок 3.3 – Відключення незадіяних портів комутатора та переведення їх у VLAN 999

Для забезпечення синхронізацій часу в мережі та коректного відображення логів і подій на мережевих пристроях налаштовано часовий пояс (EET), правила переходу на літній час (EEST) та підключення до NTP-сервера SRV-32-1. Також активовано оновлення календаря та проставлення міток часу для записів логів із точністю до мілісекунд, рис.3.4. Аналогічні налаштування виконано на всіх комутаторах мережі.

```
R-32-1(config)#clock timezone EET 2
R-32-1(config)#clock summer-time EEST recurring last Sunday March 03:00 last Sunday October 04:00
R-32-1(config)#ntp server SRV-32-1
R-32-1(config)#ntp update-calendar
R-32-1(config)#service timestamps log datetime localtime msec
```

Рисунок 3.4 – Налаштування синхронізації часу

Для забезпечення безпечного віддаленого доступу до мережевих пристроїв було налаштовано пароль на привілейований вхід, створено обліковий запис адміністратора з максимальним рівнем привілеїв та активовано локальну автентифікацію для доступу через SSH на лінії VTY і консоль, рис.3.5. Такі ж самі налаштування виконано і на комутаторах мережі.

```
R-32-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R-32-1(config)#enable secret passSec
R-32-1(config)#username admin privilege 15 secret passAdmin
R-32-1(config)#line vty 0 4
R-32-1(config-line)#transport input ssh
R-32-1(config-line)#login local
R-32-1(config-line)#exit
R-32-1(config)#line cons 0
R-32-1(config-line)#login local
R-32-1(config-line)#exit
R-32-1(config)#crypto key generate rsa modulus 1024
R-32-1(config)#ip ssh version 2
R-32-1(config)#ip ssh time-out 30
```

Рисунок 3.5 – Налаштування облікового запису адміністратора та SSH

Переходимо до налагодження SRV-32-1. Спочатку необхідно задати статичну IP-адресу відповідно до виконаного розподілу адресації пристроїв, рис.3.6.

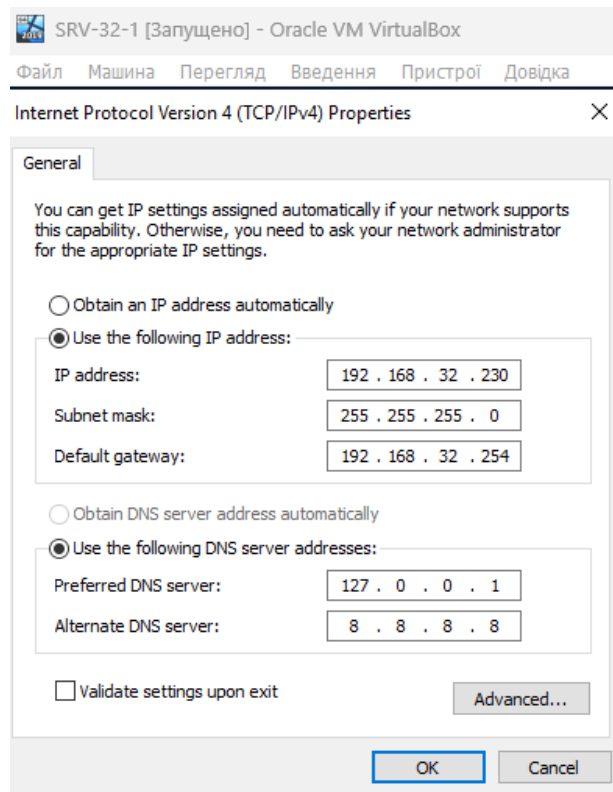


Рисунок 3.6 – Налаштування адресації SRV-32-1

Наступним етапом проводиться встановлення усіх необхідних ролей та компонентів, що забезпечують роботу служби Active Directory, рис.3.7-3.8. Після цього здійснюється створення нового домену, який стане основою для централізованого управління користувачами, ресурсами та політиками безпеки в корпоративній мережі, рис.3.9.

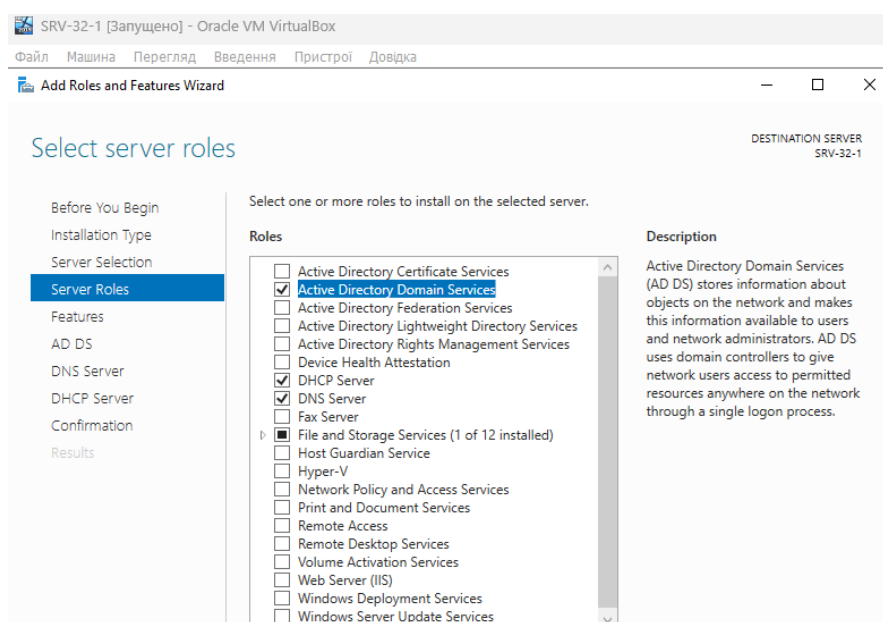


Рисунок 3.7 – Вибір ролей сервера для встановлення

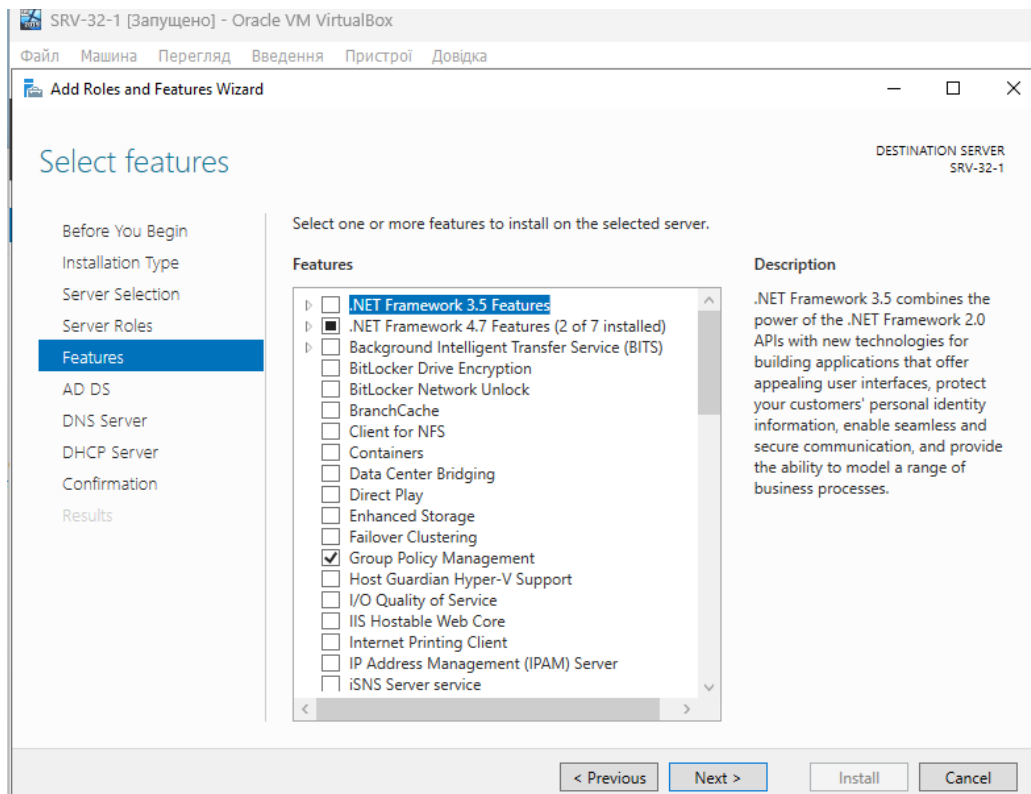


Рисунок 3.8 – Вибір компонентів сервера для встановлення

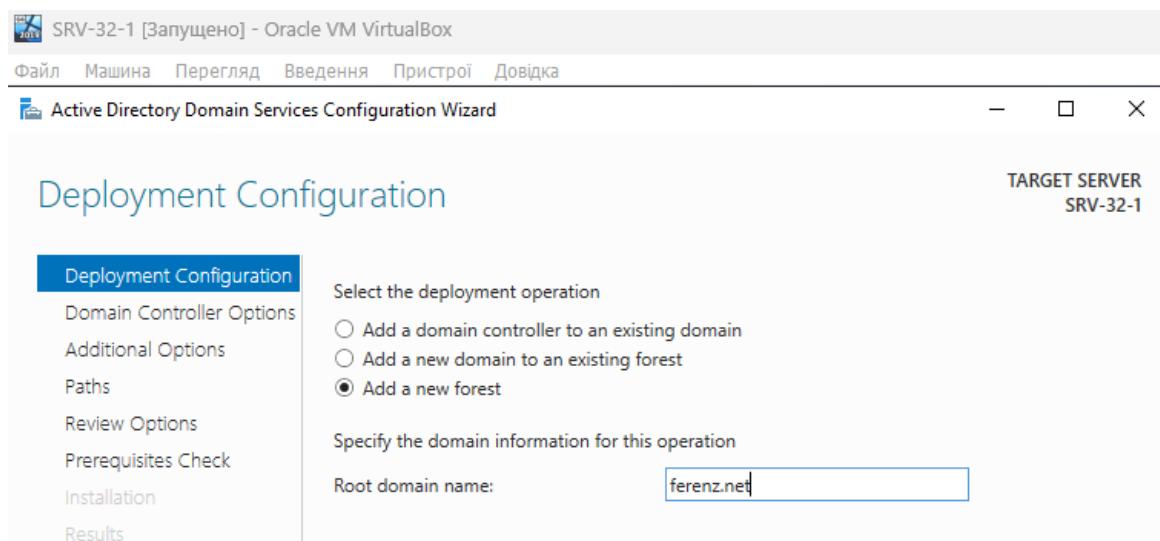


Рисунок 3.9 – Створення домену ferenz.net

Далі здійснюється налаштування служби DHCP-сервера, яка відповідає за автоматичну видачу мережевих параметрів клієнтським пристроям у мережі. Обов'язково потрібно вилучити з пулу DHCP статичні адреси, які вже закріплені за мережевими пристроями, щоб уникнути можливих конфліктів у мережі, рис.3.10-3.11.

SRV-32-1 [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 32 . 1

End IP address: 192 . 168 . 32 . 254

Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

Рисунок 3.10 – Налаштування DHCP-сервера

SRV-32-1 [Запущено] - Oracle VM VirtualBox

Файл Машина Перегляд Введення Пристрої Довідка

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.

Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address: End IP address:

1 Add

Excluded address range:

192.168.32.230 to 192.168.32.254 Remove

Subnet delay in milli second:

0

< Back Next > Cancel

Рисунок 3.11 – Виключення статичних адрес з пулу

На наступному етапі створюються статичні DNS-записи для мережевих пристроїв, таких як маршрутизатор та комутатори, що дозволяє забезпечити швидкий і надійний доступ до них у межах локальної мережі за їх іменами імен та спростити подальше адміністрування інфраструктури, рис.3.12.

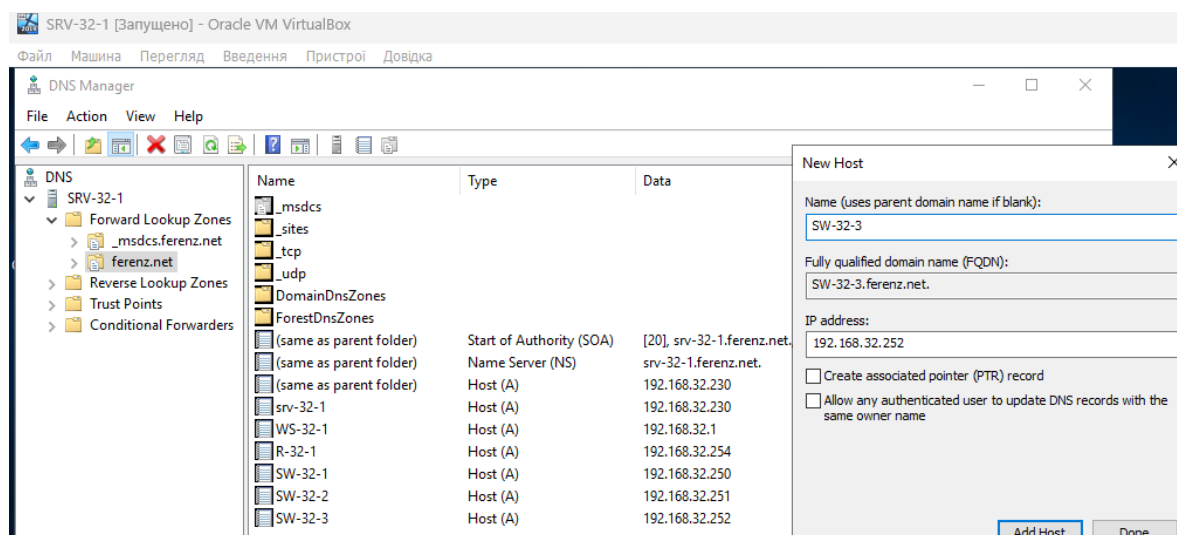


Рисунок 3.12 – Додання DNS-записів для мережевих пристроїв

Далі виконується створення облікових записів користувачів у домені, що дозволяє централізовано керувати доступом до мережевих ресурсів та підвищує безпеку корпоративної мережі, рис.3.13.

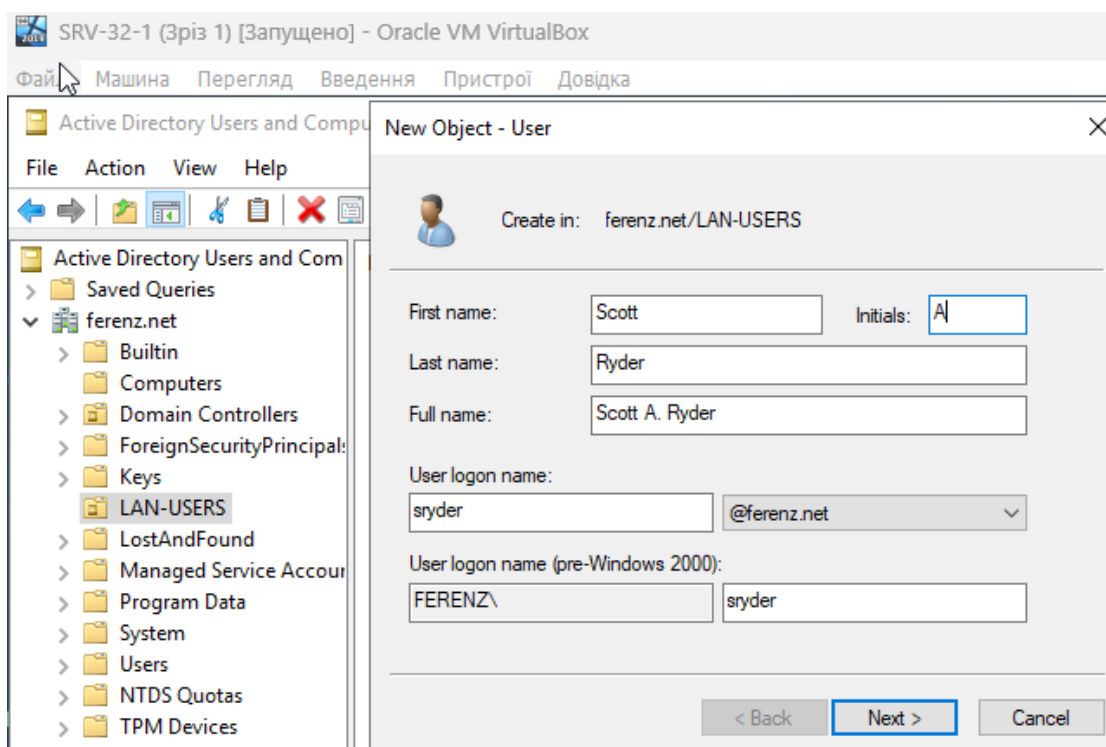


Рисунок 3.13 – Створення облікового запису користувача

На робочих станціях налаштовується автоматичне отримання IP-адрес автоматично через DHCP, що дозволяє спростити адміністрування мережі, після чого комп'ютери слід приєднати до домену ferenz.net для централізованого управління користувачами, груповими політиками та доступом до ресурсів мережі, рис.3.14-3.15.

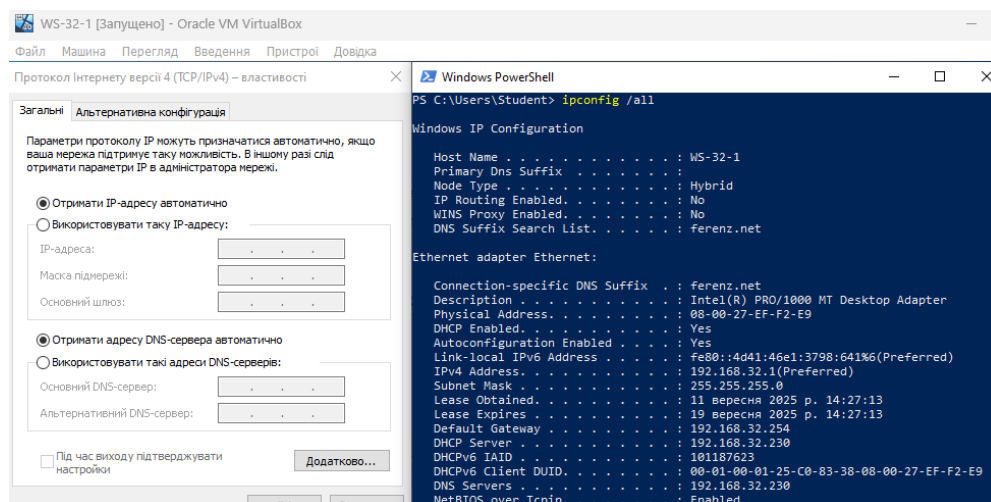


Рисунок 3.14 – Налаштування параметрів адресації

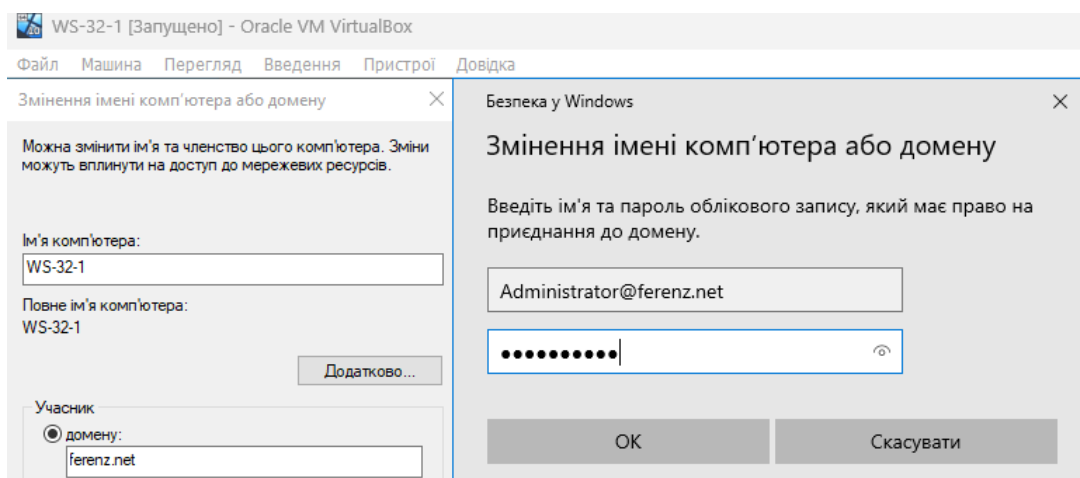


Рисунок 3.15 – Підключення комп'ютера до домену ferenz.net

Після перезавантаження пристрою користувачі домену можуть успішно входити в систему використовуючи створені раніше облікові записи, рис.3.16. Після входу, використовуючи утиліту пінг, можна переконатись в наявності зв'язку з іншими пристроями та доступу до ресурсів Інтернету, рис. 3.17. На цьому базове налаштування мережі та пристроїв завершено.

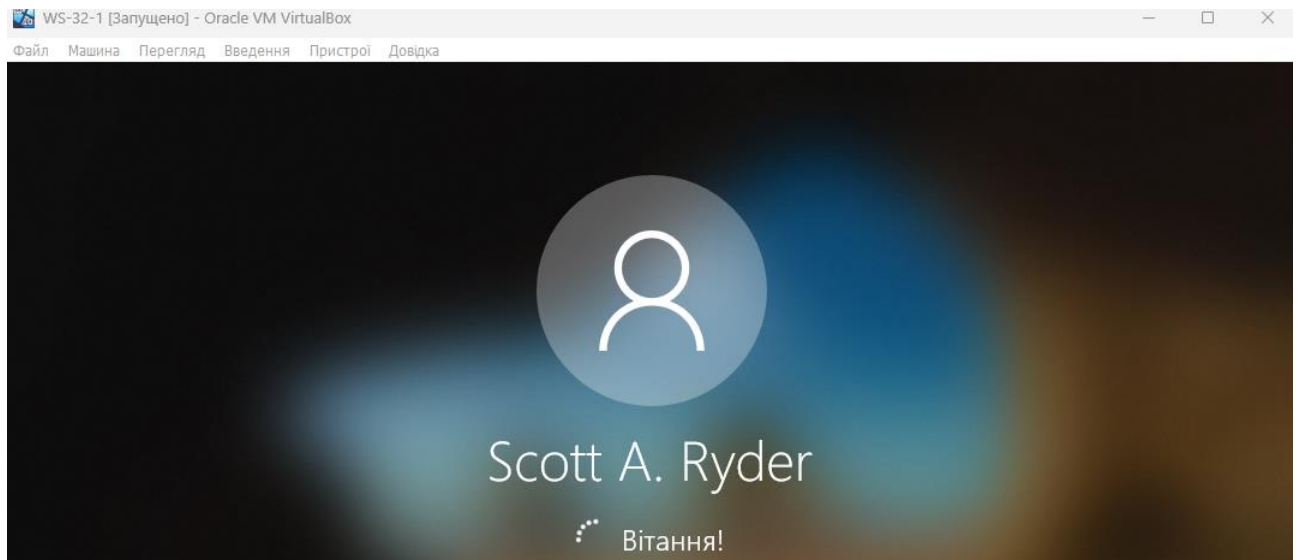


Рисунок 3.16 – Вхід в систему робочої станції

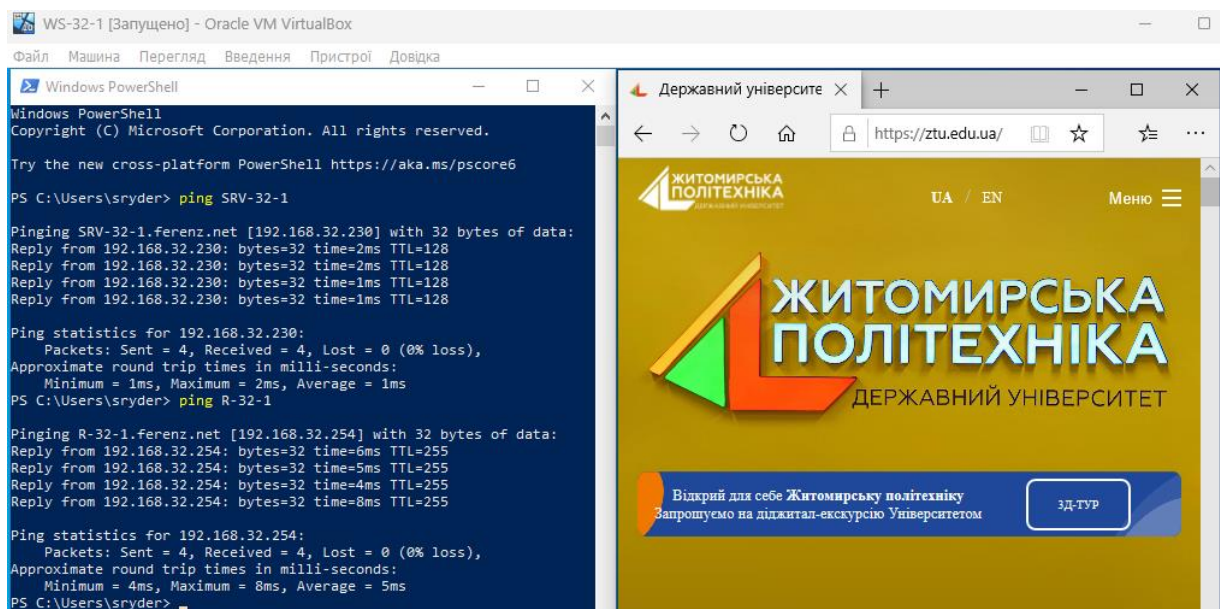


Рисунок 3.17 – Перевірка зв'язку з локальними пристроями та зовнішніми ресурсами Інтернету

3.2 Налаштування роботи PRTG Network Monitor

Перейдемо до встановлення системи моніторингу. Для цього на офіційному сайті Paessler вказуємо робочу пошту, копіюємо ліцензійний ключ та завантажуюмо інсталятор [19]. Після завантаження запускаємо інсталятор та слідуємо вказівкам. Під час встановлення важливо вказати персональну пошту та ліцензійний ключ, який було отримано раніше, рис.3.18-3.19.

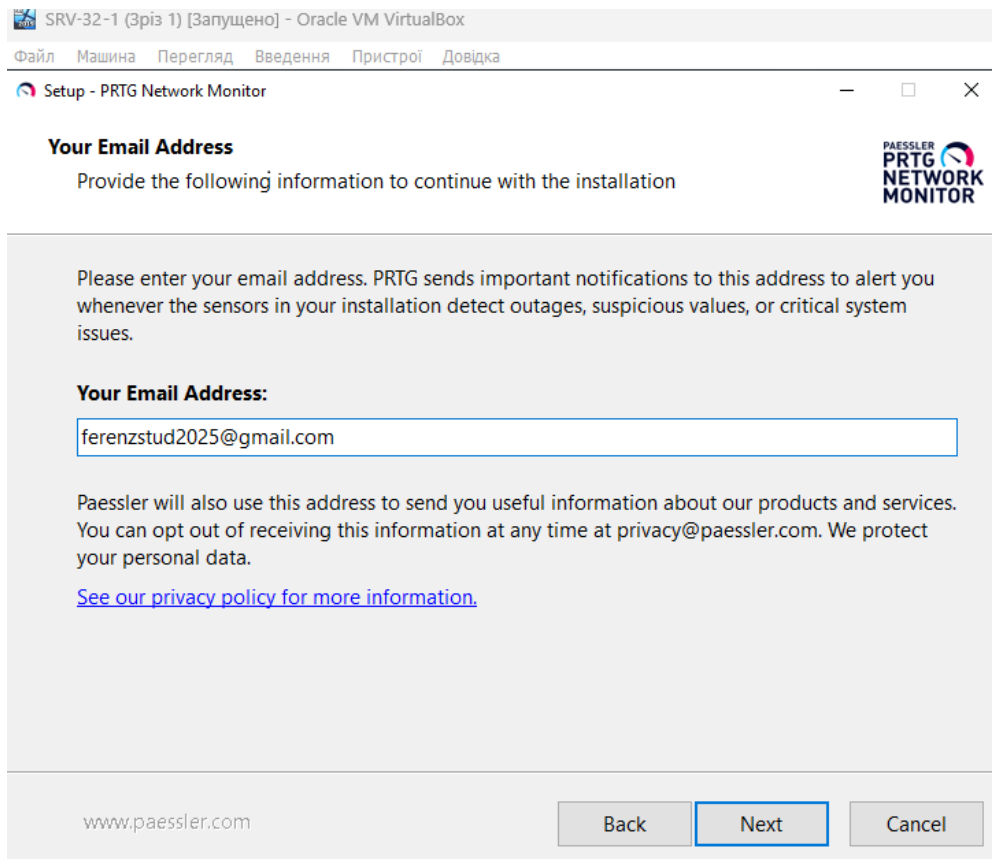


Рисунок 3.18 – Процес встановлення PRTG Network Monitor

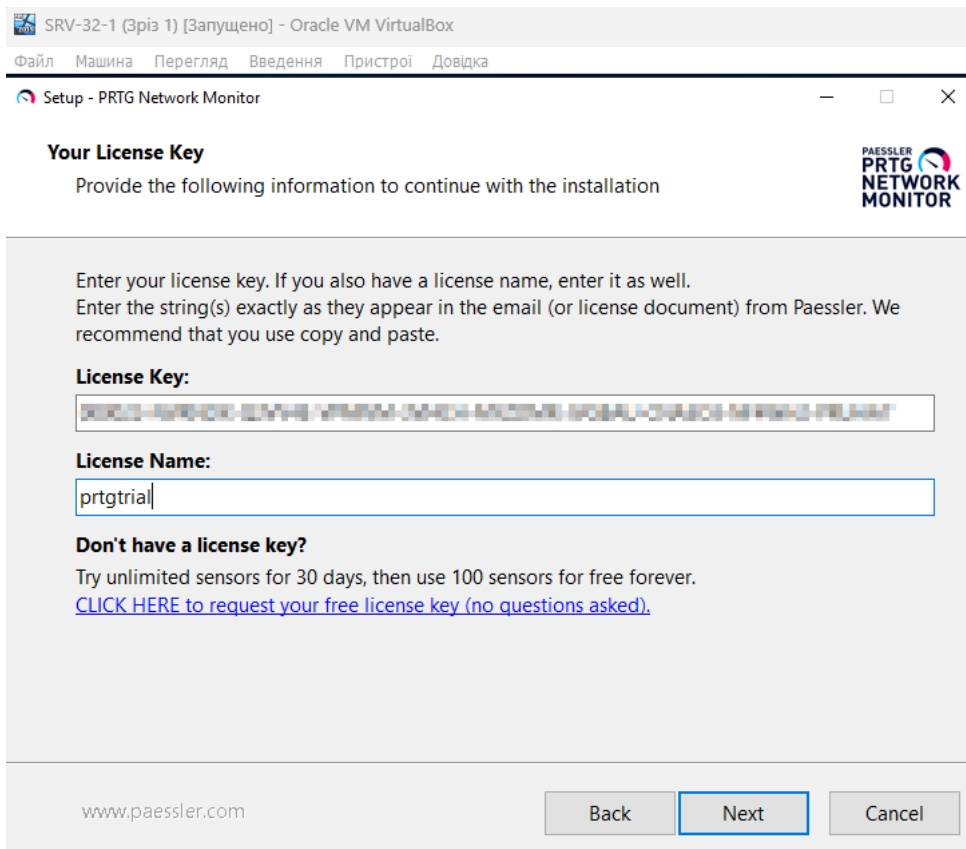


Рисунок 3.19 – Процес встановлення PRTG Network Monitor

Доступ до PRTG можна отримати через веб-інтерфейс або через спеціальний фірмовий застосунок для Windows, який слід додатково встановити (PRTG Desktop). Проте надалі розглянемо традиційний метод роботи через веб-браузер. Для цього слід просто ввести адресу пристрою на якому розгорнуто PRTG, тобто `http://srv-32-1` і пройти процедуру аутентифікації, рис.3.20.

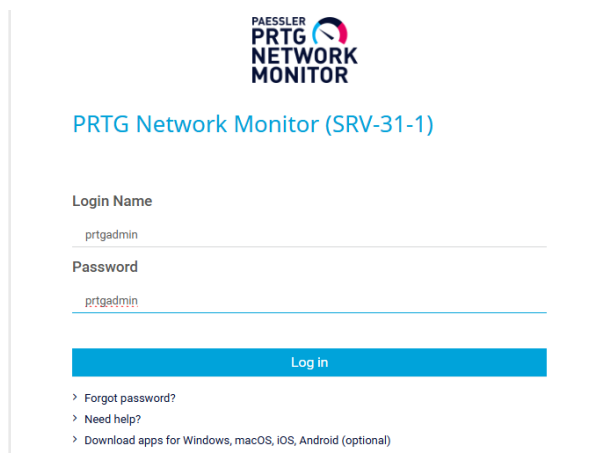


Рисунок 3.20 – Аутентифікація

Після входу нам запропонують перейти до використання SSL/TLS сертифікатів з метою підвищення захищеності передачі даних. Тому погоджуємося з цим і наступний вхід до веб-інтерфейсу будемо виконувати з використанням протоколу `https`, рис.3.21.

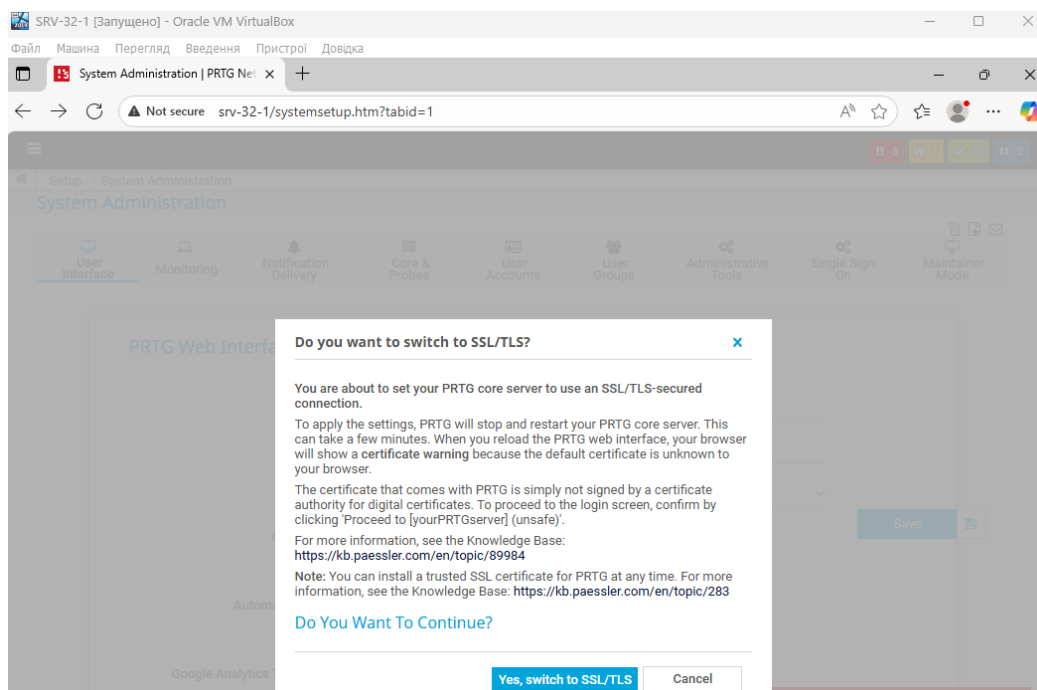


Рисунок 3.21 – Налаштування на використання SSL/TLS сертифікатів

В продуктивних середовищах рекомендується замінити сапопідписаний сертифікат PRTG на довірений, втім в тестовому середовищі залишимо все як є і надалі будемо ігнорувати попередження пов'язані з цим. Після входу в систему вкрай важливо також змінити стандартний пароль користувача prtgsadmin, рис.3.22.

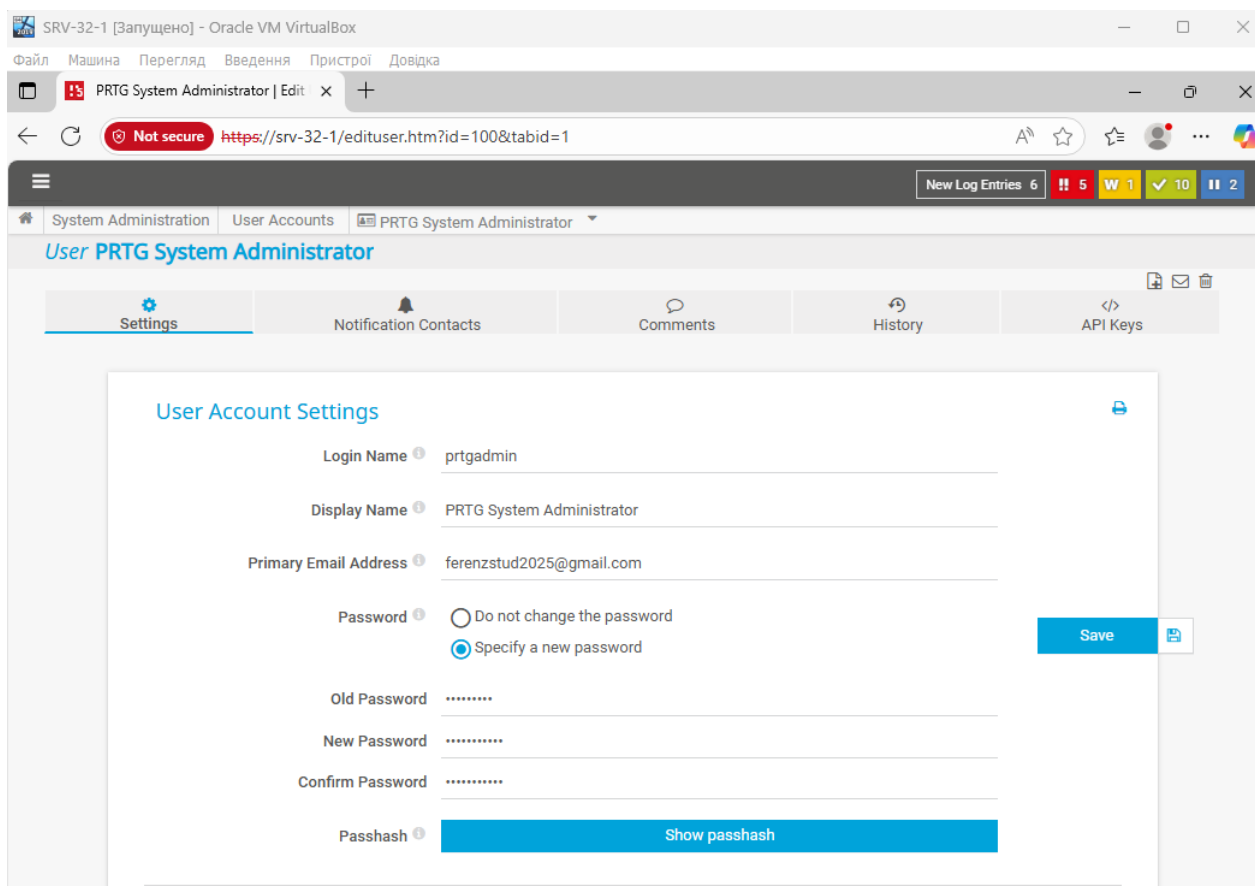


Рисунок 3.22 – Зміна стандартного паролю користувача prtgsadmin

Щоб забезпечити збір даних через WMI та SNMPv3 у PRTG, необхідно попередньо налаштувати відповідні облікові дані. Для WMI слід вказати домен і користувача з необхідними правами доступу, що дозволить системі коректно отримувати інформацію з робочих станцій і серверів, рис.3.23.

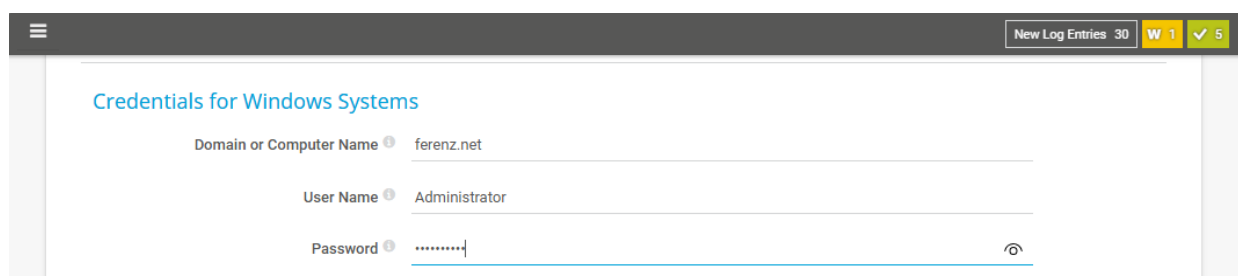


Рисунок 3.23 – Введення облікових даних користувача

Далі налаштуємо параметри SNMPv3, вказавши відповідну версію SNMP, логін та пароль користувача, методи хешування та шифрування і пароль шифрування, рис.3.24.

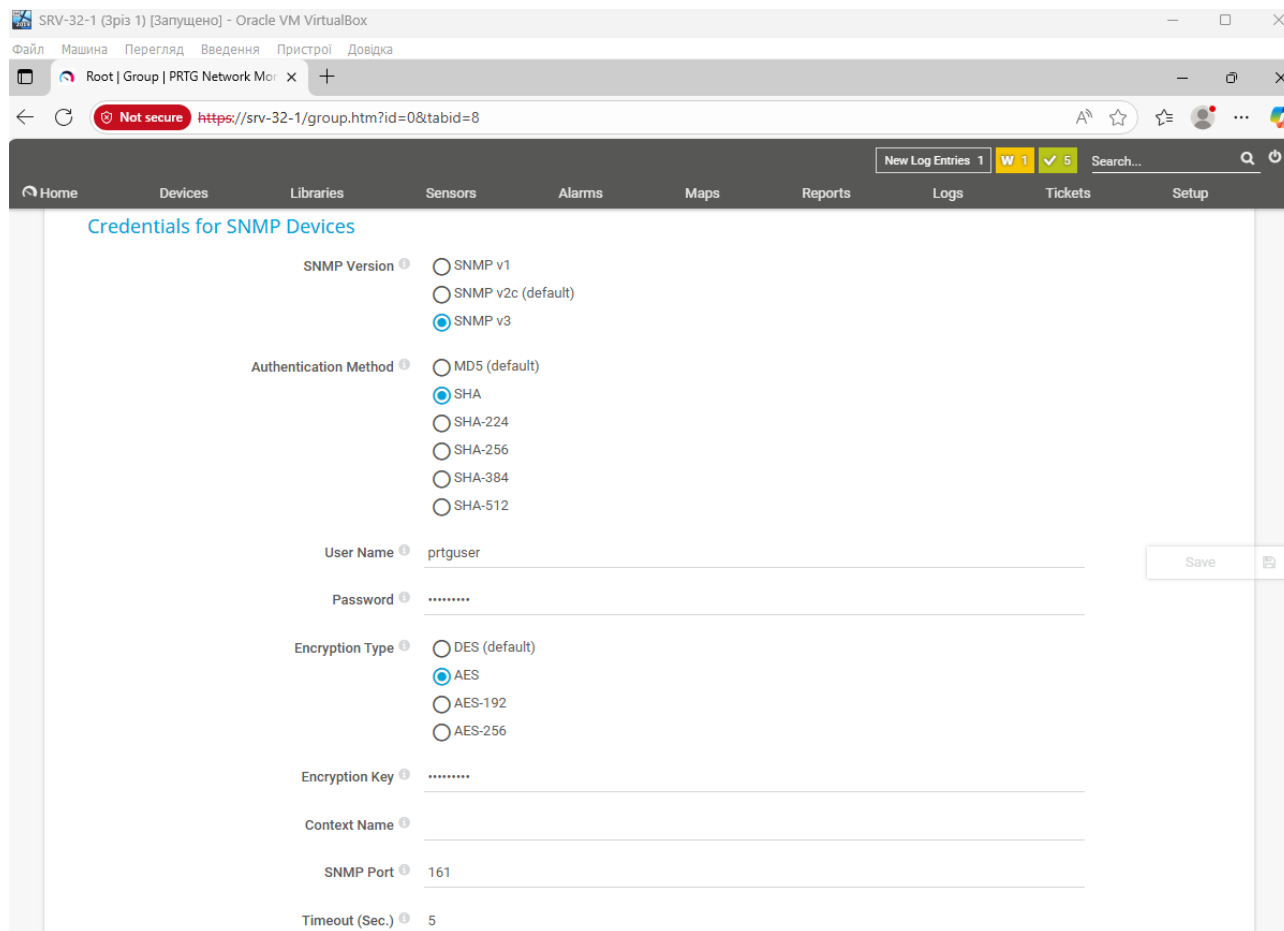


Рисунок 3.24 – Налаштування параметрів SNMPv3 в PRTG

Тепер перейдемо до налаштування параметрів передачі на мережевих пристроях. Спершу налаштуємо параметри протоколу SNMPv3. Для цього на пристрої слід вказати відповідні параметри безпеки, такі як автентифікація та шифрування, які були задані на попередньому кроці, а також вказати кінцевий хост для отримання сповіщень, тобто SRV-32-1. Також було створено SNMP-групу PRTG, яка дозволяє виконувати лише читання даних, а не їх перезапис. Аналогічно виконуємо на всіх мережевих пристроях, рис.3.25.

```
R-32-1(config)#snmp-server view ALL-ACCESS iso included
R-32-1(config)#snmp-server group PRTG v3 priv read ALL-ACCESS
R-32-1(config)#snmp-server user prtguser PRTG v3 auth sha AuthPass priv aes 128 PrivPass
R-32-1(config)#snmp-server host Srv-32-1 version 3 priv prtguser
```

Рисунок 3.25 – Налаштування параметрів SNMPv3

Далі виконаємо конфігурацію технології NetFlow v9 на маршрутизаторі R-32-1. Спочатку, було увімкнено збір IP-потоків на відповідних інтерфейсах. Після цього виконано налаштування параметрів NetFlow, зокрема, визначено версію протоколу та встановлено таймаути для активних і неактивних потоків. Останнім кроком є вказання кінцевого сервера моніторингу для відправки зібраних даних, рис.3.26.

```
R-32-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-32-1(config)#interface fa0/0
R-32-1(config-if)#ip route-cache flow
R-32-1(config-if)#exit
R-32-1(config)#interface fa0/1
R-32-1(config-if)#ip route-cache flow
R-32-1(config-if)#exit
R-32-1(config)#ip flow-export version 9
R-32-1(config)#ip flow-cache timeout active 5
R-32-1(config)#ip flow-cache timeout inactive 10
R-32-1(config)#ip flow-export destination Srv-32-1 9991
```

Рисунок 3.26 – Налаштування параметрів SNMPv3

Для мережевих пристроїв лишається налаштувати параметри передачі подій через Syslog. Спочатку вказується адреса сервера, куди будуть відправлятися повідомлення та визначається мінімальний рівень їх важливості (severity level). Далі включаємо роботу журналу та налаштовуємо ведення запису подій, пов'язаних як з успішними, так і з невдалими спробами авторизації на пристрої. Аналогічні дії виконуються і на всіх комутаторах, рис.3.27.

```
R-32-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R-32-1(config)#logging host SRV-32-1
R-32-1(config)#logging trap informational
R-32-1(config)#logging on
R-32-1(config)#login on-failure log
R-32-1(config)#login on-success log
```

Рисунок 3.27 – Налаштування параметрів відправки сповіщень через Syslog

Лишається лише налагодити роботу WMI на робочих станціях. Для цього на комп'ютері слід перейти в параметри налаштування брандмауера Windows і включити вхідне правило використання трафіку WMI, тим самим даючи можливість PRTG запитувати необхідні дані від станції, рис.3.28.

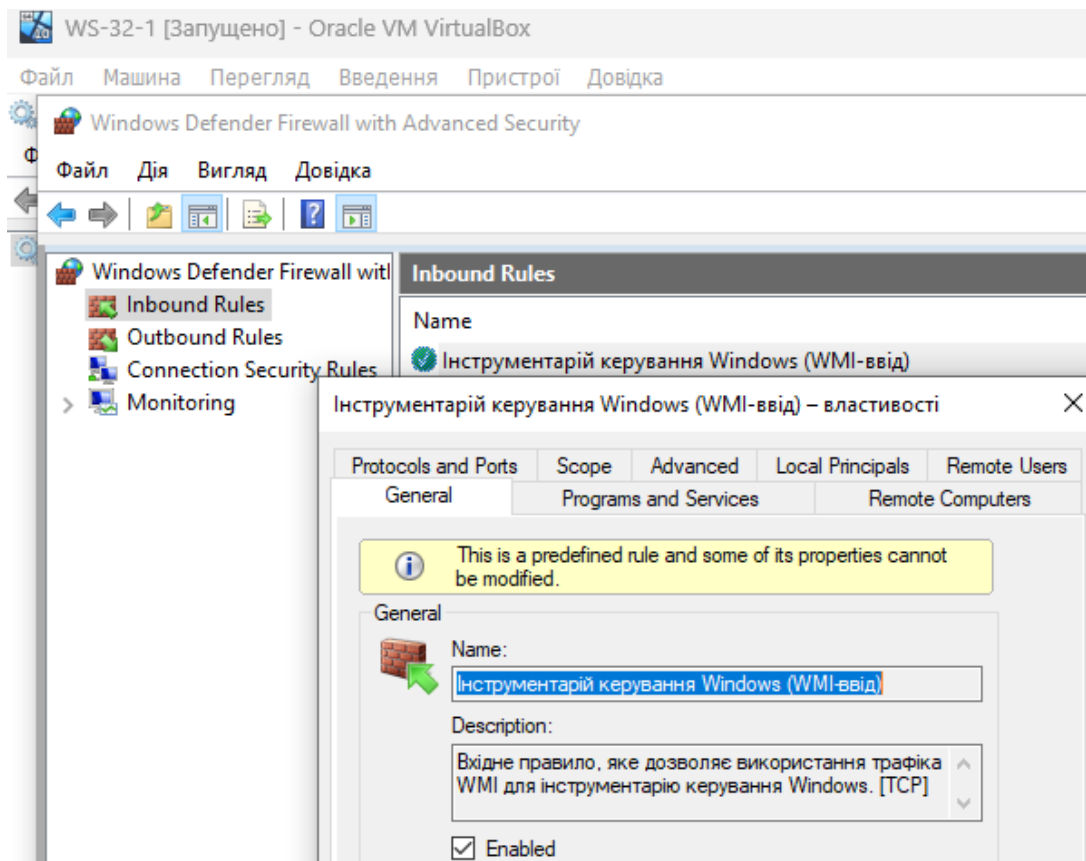


Рисунок 3.28 – Налаштування правила брандмауера для WMI на робочій станції

Перейдемо до додавання сенсорів. Спершу для цього створимо групу автоматичного виявлення (Auto-Discovery Group) для мережевих пристроїв Cisco. Це дозволяє системі моніторингу виконати сканування заданого діапазону адрес та автоматично додавати всі пристрої, що відповідають відповідному шаблону. Такий підхід значно пришвидшує процес додання пристроїв та автоматично виконає додання необхідних базових сенсорів, рис.3.29.

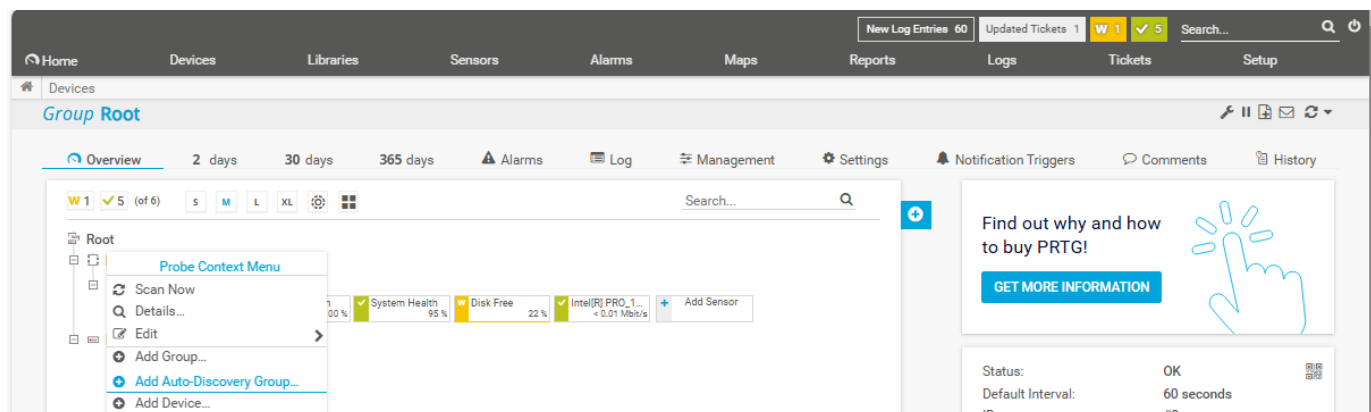


Рисунок 3.29 – Створення групи автоматичного виявлення для мережевих пристроїв

В наступному вікні слід дати назву групі, обрати шаблон пристроїв (Cisco) та вказати доменні імена пристроїв, які слід додати в цю групу, рис.3.30-3.31.

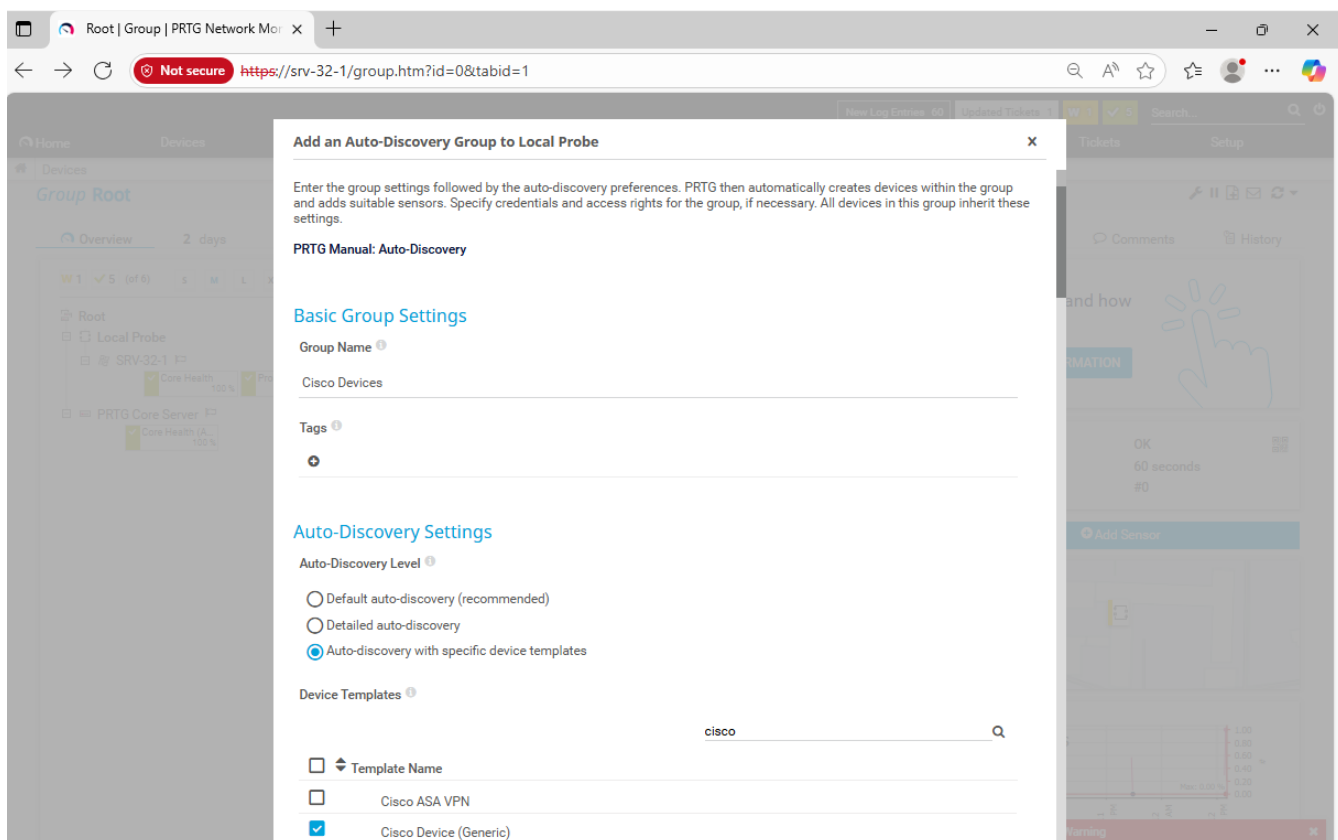


Рисунок 3.30 – Налаштування групи автоматичного виявлення

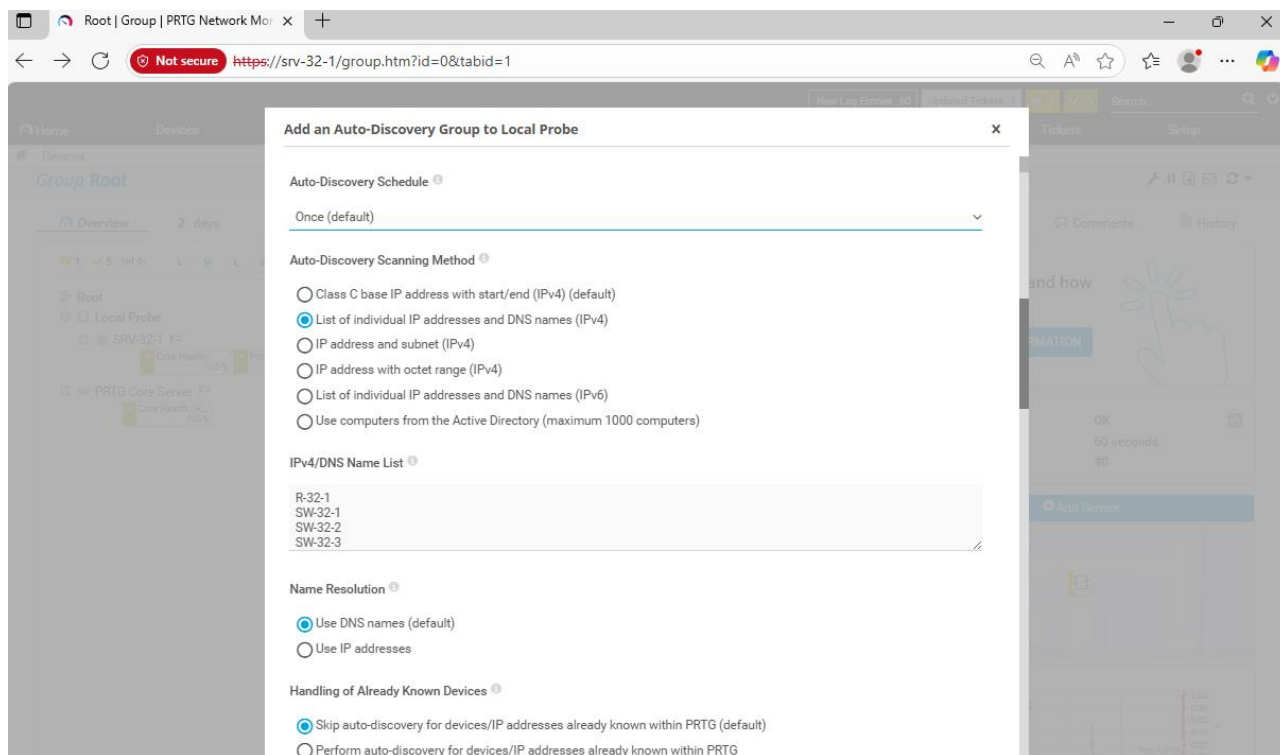


Рисунок 3.31 – Налаштування групи автоматичного виявлення

У результаті PRTG успішно додає всі зазначені пристрої до моніторингу, після чого стає доступним перегляд даних з деяких автоматично доданих сенсорів, рис.3.32.

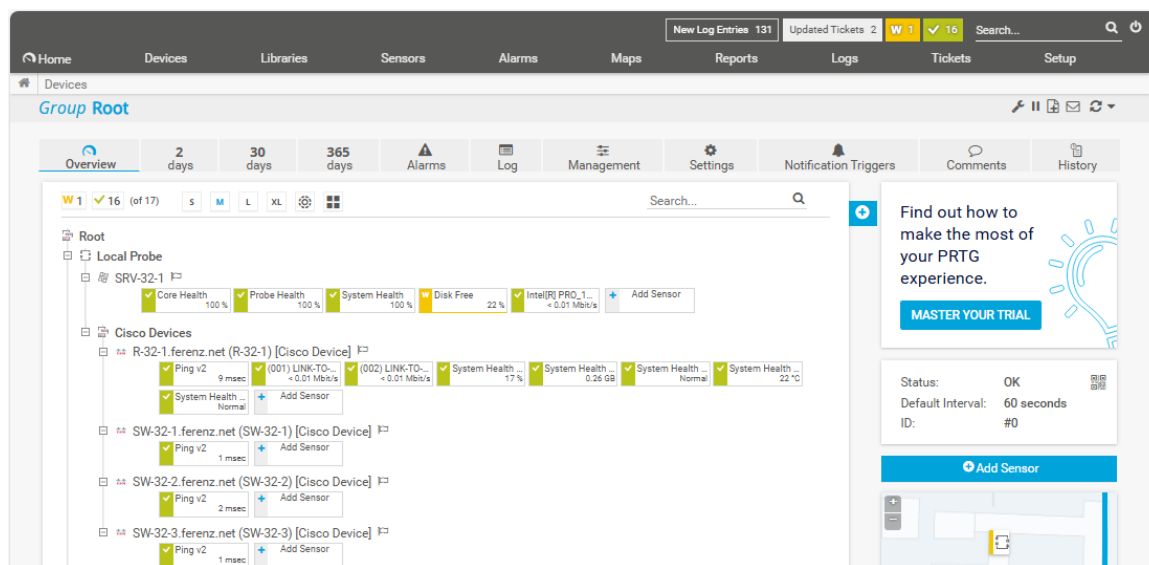


Рисунок 3.32 – Результат додання мережевих пристроїв до групи

В результаті для комутаторів був доданий лише єдиний сенсор «Ping v2», тому слід вручну додати інші потрібні сенсори. Для цього натискаємо кнопку «Add Sensor» біля відповідного пристрою та обираємо потрібний тип сенсора. Спершу для всіх мережевих пристроїв виконаємо додання сенсору «SNMP Traffic», що забезпечить отримання загальної інформації від них через SNMP, рис.3.33-3.35.

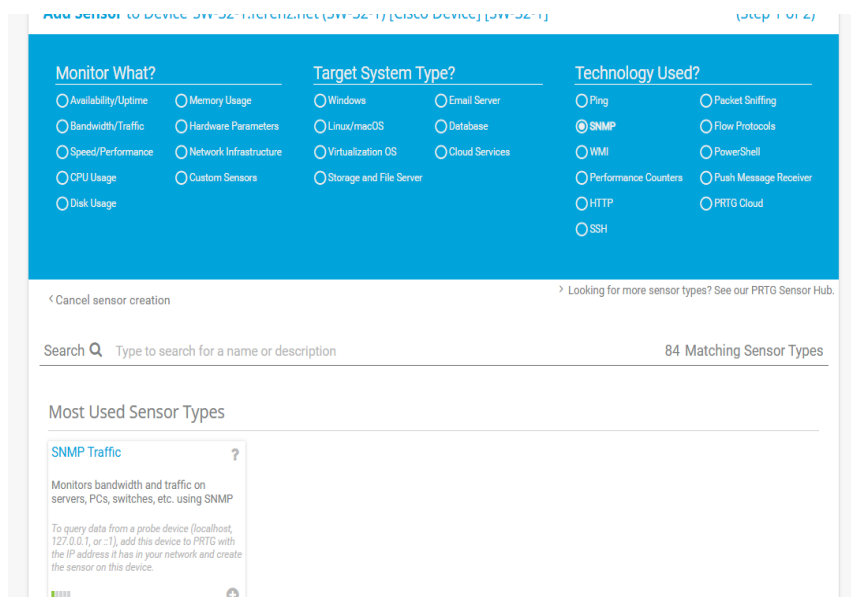


Рисунок 3.33 – Вибір сенсору SNMP Traffic

Add Sensor (Step 2 of 2) | PRTG N x +

Not secure https://srv-32-1/addsensor4.htm?id=2074&tmpid=3

New Log Entries 244 Updated Tickets 3 W 1 16

Add Sensor to Device SW-32-1.ferenz.net (SW-32-1) [Cisco Device] [SW-32-1] (Step 2 of 2)

< Cancel

Basic Sensor Settings

Parent Tags vendors_Cisco

Tags bandwidthsensor x snmptrafficsensor x +

Priority ★★☆☆☆

Traffic Specific

Create

Select all connected interfaces Select all disconnected interfaces Deselect all interfaces

Interface Number Search...

☒	Name	Status	Speed	Type	64 bit	Internal name
☒	(001) Ethernet0/0 Traffic	Connected	10 MBit/s	Ethernet	Yes	Ethernet0/0
☒	(002) Ethernet0/1 Traffic	Not Connected	10 MBit/s	Ethernet	Yes	Ethernet0/1
☒	(003) Ethernet0/2 Traffic	Not Connected	10 MBit/s	Ethernet	Yes	Ethernet0/2
☒	(004) Ethernet0/3 Traffic	Not Connected	10 MBit/s	Ethernet	Yes	Ethernet0/3
☒	(005) Ethernet1/0 Traffic	Not Connected	10 MBit/s	Ethernet	Yes	Ethernet1/0
☒	(006) Ethernet1/1 Traffic	Not Connected	10 MBit/s	Ethernet	Yes	Ethernet1/1

Рисунок 3.34 – Додання сенсору SNMP Traffic

Add Sensor (Step 2 of 2) | PRTG N x +

Not secure https://srv-32-1/addsensor4.htm?id=2074&tmpid=3

New Log Entries 244 Updated Tickets 3 W 1 16

Additional Channels

☒ Errors in and errors out

☒ Discards in and discards out

☐ Unicast packets in and unicast packets out

☐ Non unicast packets in and non unicast packets out (32-bit only)

☐ Multicast packets in and multicast packets out (64-bit only)

☐ Broadcast packets in and broadcast packets out (64-bit only)

☐ Unknown Protocols

Connection Status Handling

☐ Show down status for all disconnected states

☒ Show down status when disconnected, ignore when deactivated

☐ Ignore all disconnected states (default)

Create

Name for Traffic In Channel Traffic In

Name for Traffic Out Channel Traffic Out

Name for Traffic Total Channel Traffic Total

Sensor Display

Graph Type

☐ Show channels independently (default)

☒ Stack channels on top of each other

☐ Show in and out traffic as positive and negative area graph

Рисунок 3.35 – Додання сенсору SNMP Traffic

Після цього виконаємо перехоплення і аналіз пакетів між пристроями з використанням Wireshark. Завдяки цьому можемо переконатись, що дані через протокол SNMPv3 передаються по мережі в зашифрованому вигляді, що унеможливорює перехоплення даних для сторонніх осіб, рис.3.36.

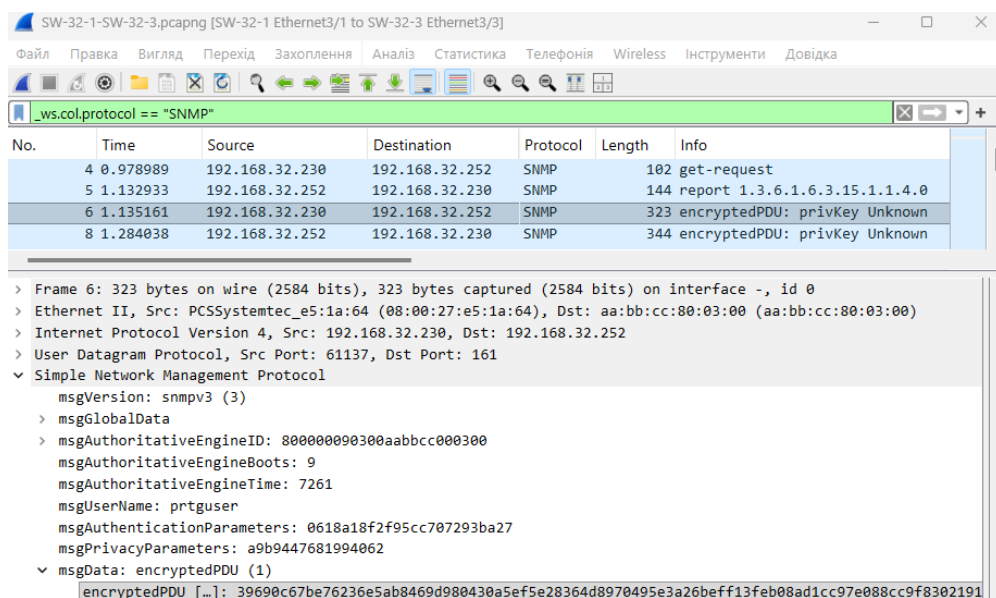


Рисунок 3.36 – Перехоплені зашифровані пакети протоколу SNMPv3

Подібним чином додаємо сенсор на збір Syslog-подій для всіх мережевих пристроїв та сенсор Netflow для маршрутизатора R-32-1, рис.3.37-3.38.

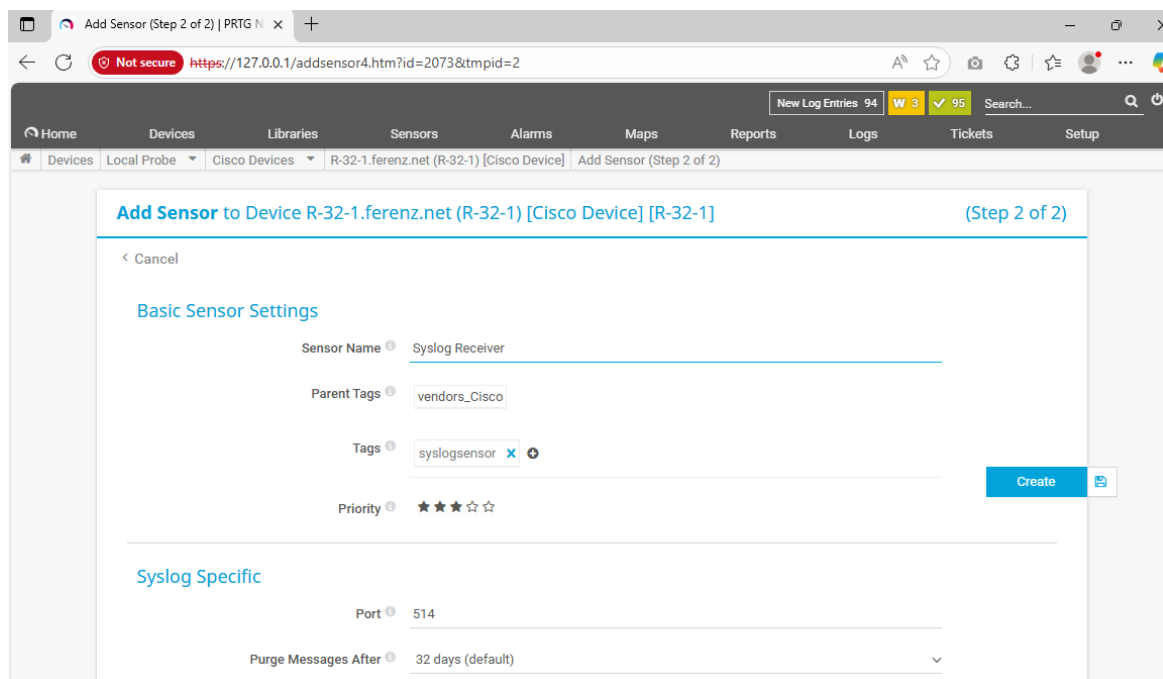


Рисунок 3.37 – Додання сенсору Syslog

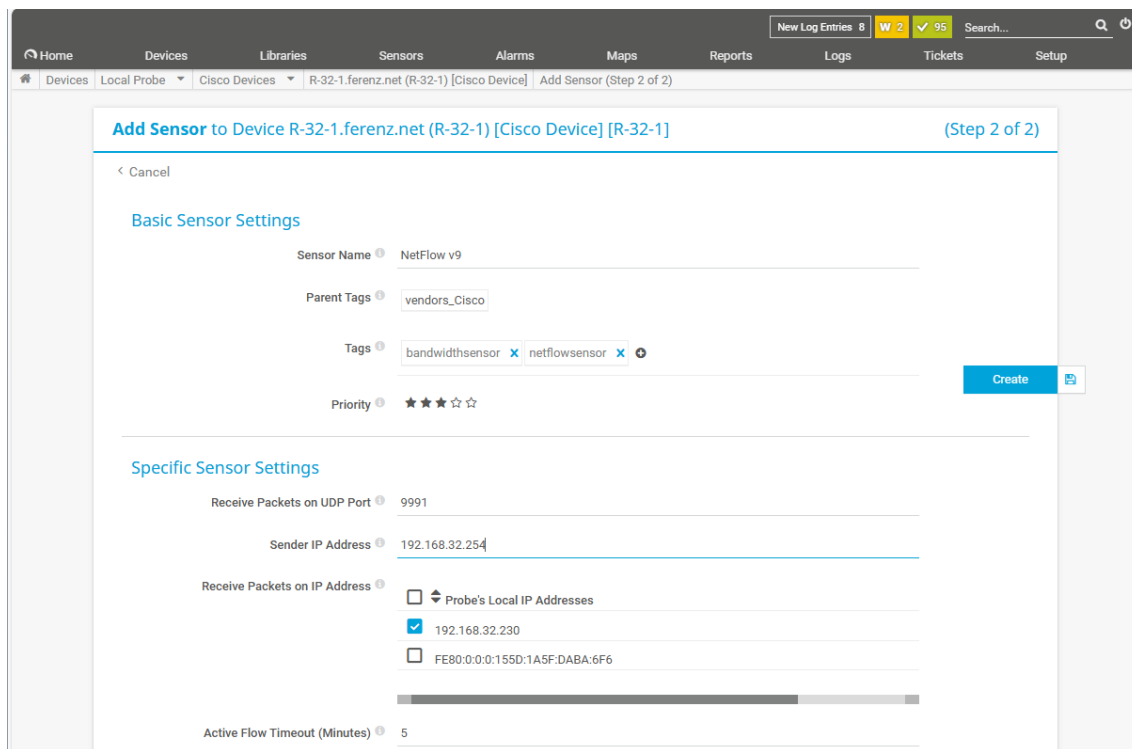


Рисунок 3.38 – Додання сенсору Netflow v9

За тим же принципом додаємо інші сенсори моніторингу стану системи для сервера та кінцевої робочої станції WS-32-1. В остаточному підсумку маємо наступний вигляд вікна де загалом використано рівно 100 сенсорів, рис.3.39.

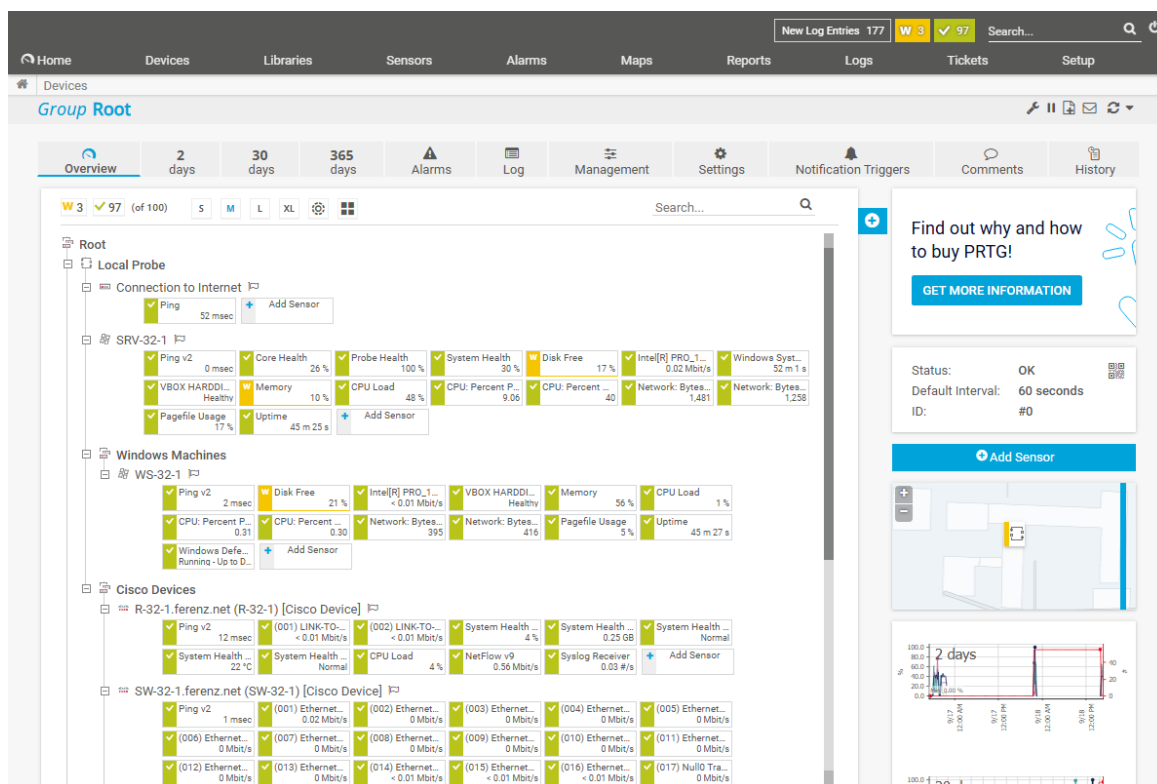


Рисунок 3.39 – Сумарний вигляд всіх доданих сенсорів та пристроїв

Лишається налаштувати можливість відправки сповіщень на електронну пошту з використанням протоколу SMTP. В даному вікні обираємо параметри механізму доставки, попередньо налаштовану електронну пошту відправника, ім'я відправника та порт. Також можна обрати тип автентифікації, метод шифрування (наприклад, SSL/TLS) та перевірити з'єднання за допомогою кнопки «Test SMTP Settings». Додатково можна налаштувати відправку сповіщень через SMS, але поки пропустим дане налаштування. рис.3.40.

The screenshot displays the 'System Administration' section of the PRTG software, specifically the 'Notification Delivery' tab. The 'SMTP Delivery' section is active, showing various configuration options. The 'Delivery Mechanism' is set to 'Use one SMTP relay server (recommended in LANs/NATs)'. The 'Sender Email Address' is 'ferenzstud2025@gmail.com', and the 'Sender Name' is 'PRTG Network Monitor'. The 'HELO Ident' is 'SRV-32-1', the 'SMTP Relay Server' is 'smtp.gmail.com', and the 'SMTP Relay Port' is '465'. For 'SMTP Relay Authentication', 'Use standard SMTP authentication' is selected. The 'SMTP Relay User Name' is 'ferenzstud2025@gmail.com' and the password is masked with dots. Under 'Connection Security', 'Use SSL/TLS if the server supports it (default)' is selected. The 'SSL/TLS Method' is set to 'TLS 1.2'. A 'Test SMTP Settings' button is visible. Below this, the 'SMS Delivery' section is partially visible, with 'Disable SMS delivery (default)' selected for the 'Configuration Mode'.

SMTP Delivery

Delivery Mechanism ☐ Use direct delivery with the built-in email server (default)
☒ Use one SMTP relay server (recommended in LANs/NATs)
☐ Use two SMTP relay servers (primary and fallback server)

Sender Email Address

Sender Name

HELO Ident

SMTP Relay Server

SMTP Relay Port

SMTP Relay Authentication ☐ Use no authentication (default)
☒ Use standard SMTP authentication
☐ Use SASL authentication

SMTP Relay User Name

SMTP Relay Password

Connection Security ☒ Use SSL/TLS if the server supports it (default)
☐ Do not use connection security

SSL/TLS Method ☐ Auto-Negotiate (TLS 1.0 or higher)
☐ SSLv3
☐ TLS 1.0
☐ TLS 1.1
☒ TLS 1.2
☐ TLS 1.3

Test SMTP Settings

SMS Delivery

Configuration Mode ☒ Disable SMS delivery (default)
☐ Select an SMS provider from a list of providers
☐ Enter a custom URL for a provider not listed

Рисунок 3.40 – Налаштування параметрів SMTP

Також можемо налаштувати параметри відправки сповіщень у випадку зміни стану сенсорів на «Down». В даному випадку, якщо сенсор понад 200 секунд перебуватиме в стані недоступності, то PRTG надішле відповідне push-повідомлення у веб-інтерфейсі PRTG та сповіщення на електронну пошту. Дане налаштування дозволить адміністратору більш оперативно реагувати на виникнення будь-яких надзвичайних ситуацій в мережі, рис.3.41.

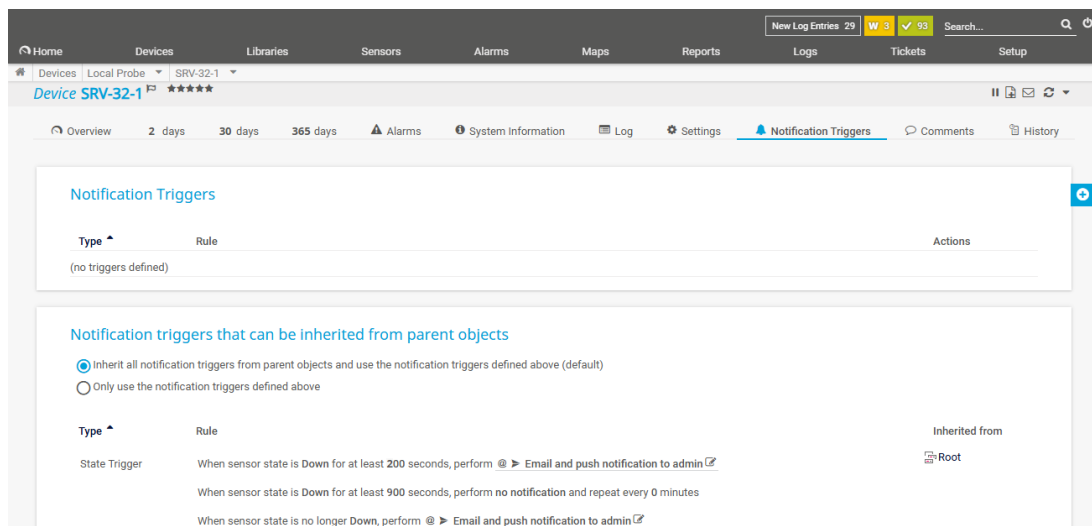


Рисунок 3.41 – Налаштування параметрів відправки сповіщень

3.3 Тестування роботи мережі та системи моніторингу

Перейдемо до перевірки роботи системи моніторингу. Перш за все в самому головному меню можемо переглянути загальний стан сенсорів. Крім цього тут наведено стан сенсорів, як видно три з них мають стан попередження (Warning), рис.3.42.

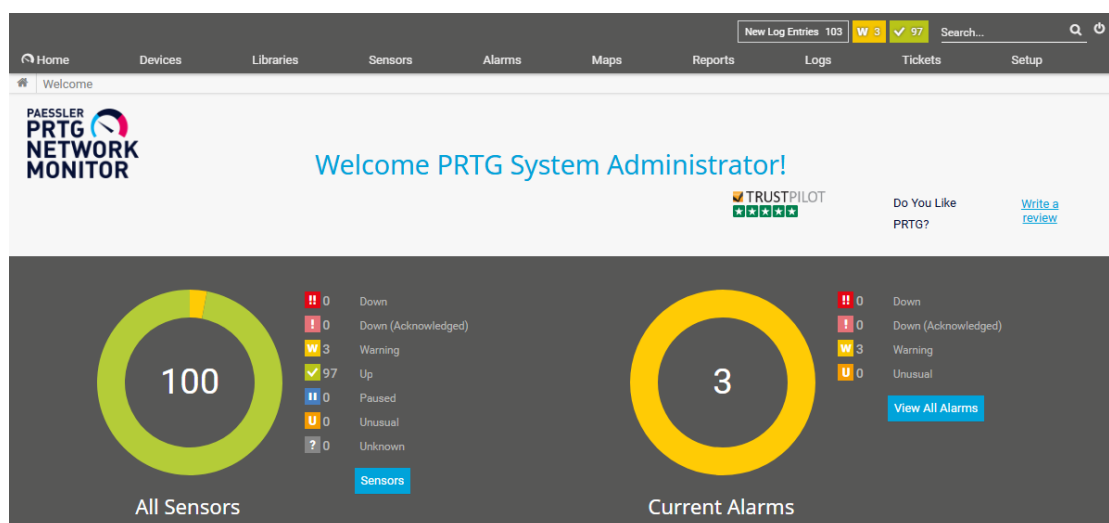
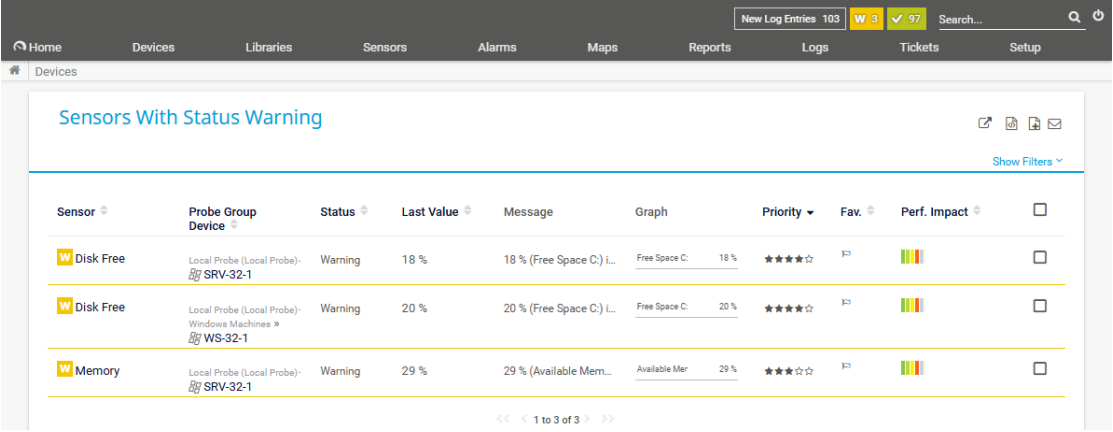


Рисунок 3.42 – Головне вікно PRTG Network Monitor

Переглянемо сповіщення що надійшли. В цьому списку показано три попередження: два сенсори «Disk Free», що сигналізують про низький рівень вільного місця на дисках SRV-32-1 (18%) та WS-32-1 (20%), а також сенсор «Memory», який вказує на недостатній обсяг вільної оперативної пам'яті (29%) на пристрої SRV-32-1. Завдяки цьому, системний адміністратор може оперативно реагувати на ці попередження, запобігаючи можливим проблемам, таким як переповнення диска, нестача ресурсів пам'яті, тощо, рис.3.43.



The screenshot shows the PRTG Network Manager interface with a dark theme. The top navigation bar includes links for Home, Devices, Libraries, Sensors, Alarms, Maps, Reports, Logs, Tickets, and Setup. A status bar at the top right indicates 'New Log Entries 103', 'W 3', and '97'. The main content area is titled 'Sensors With Status Warning' and contains a table with the following data:

Sensor	Probe Group Device	Status	Last Value	Message	Graph	Priority	Fav.	Perf. Impact	
Disk Free	Local Probe (Local Probe)- SRV-32-1	Warning	18 %	18 % (Free Space C:) L...	Free Space C: 18 %	★★★★☆	32		☐
Disk Free	Local Probe (Local Probe)- Windows Machines » WS-32-1	Warning	20 %	20 % (Free Space C:) L...	Free Space C: 20 %	★★★★☆	32		☐
Memory	Local Probe (Local Probe)- SRV-32-1	Warning	29 %	29 % (Available Mem...	Available Mem 29 %	★★★★☆	32		☐

At the bottom of the table, there is a pagination control showing '<< 1 to 3 of 3 >>'.

Рисунок 3.43 – Список сенсорів зі статусом «Warning»

Тепер зімітуємо ситуація недоступності одного з елементів мережі, для прикладу робочої станції WS-32-1. Для цього відімкнемо відповідний мережевий кабель до комп'ютера WS-32-1, рис.3.44.

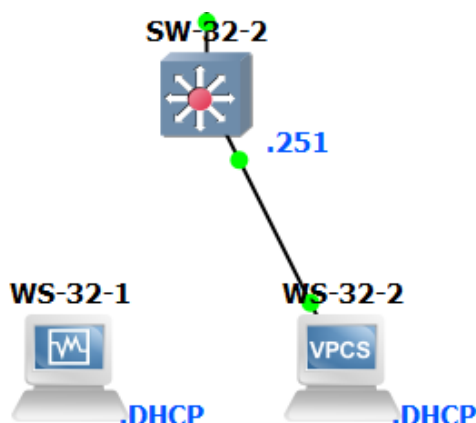


Рисунок 3.44 – Відімкнення мережевого кабелю до комп'ютера WS-32-1

І через кілька десятків секунд в меню PRTG з'явилося сповіщення про припинення роботи сенсору «Ping v2» на WS-32-1, рис.3.45.

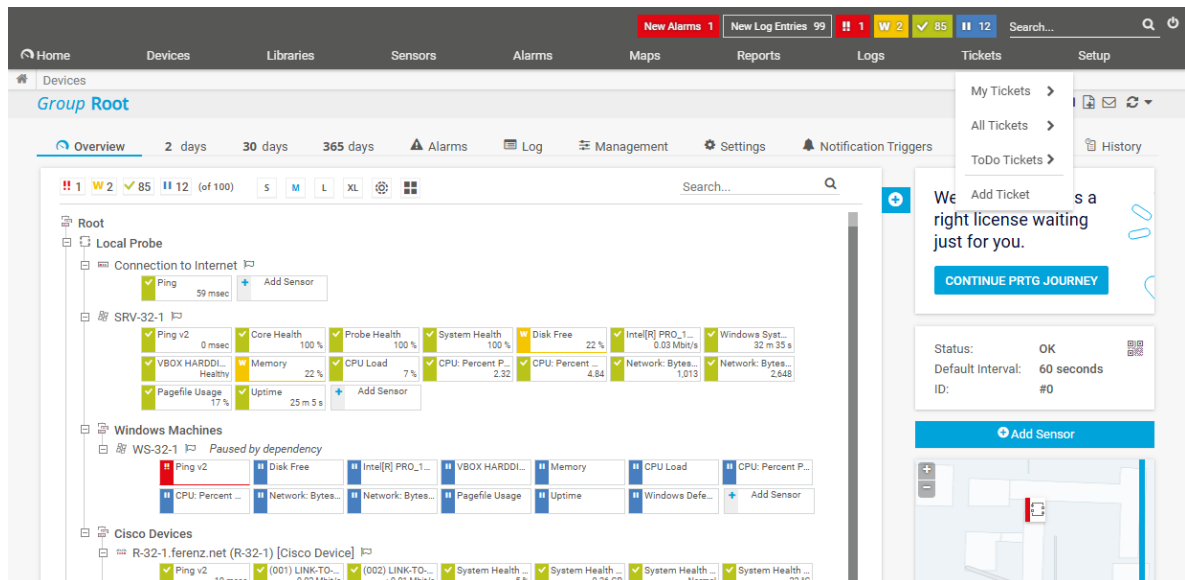


Рисунок 3.45 – Зупинка роботи сенсору «Ping v2» WS-32-1

А через декілька хвилин на електронну пошту надійшов лист від PRTG з інформацією стосовно згаданої події. Тут можна отримати інформацію коли було зафіксовано проблему з сенсорами та переглянути попередню історію роботи даного сенсору у вигляді діаграми, рис.3.46.

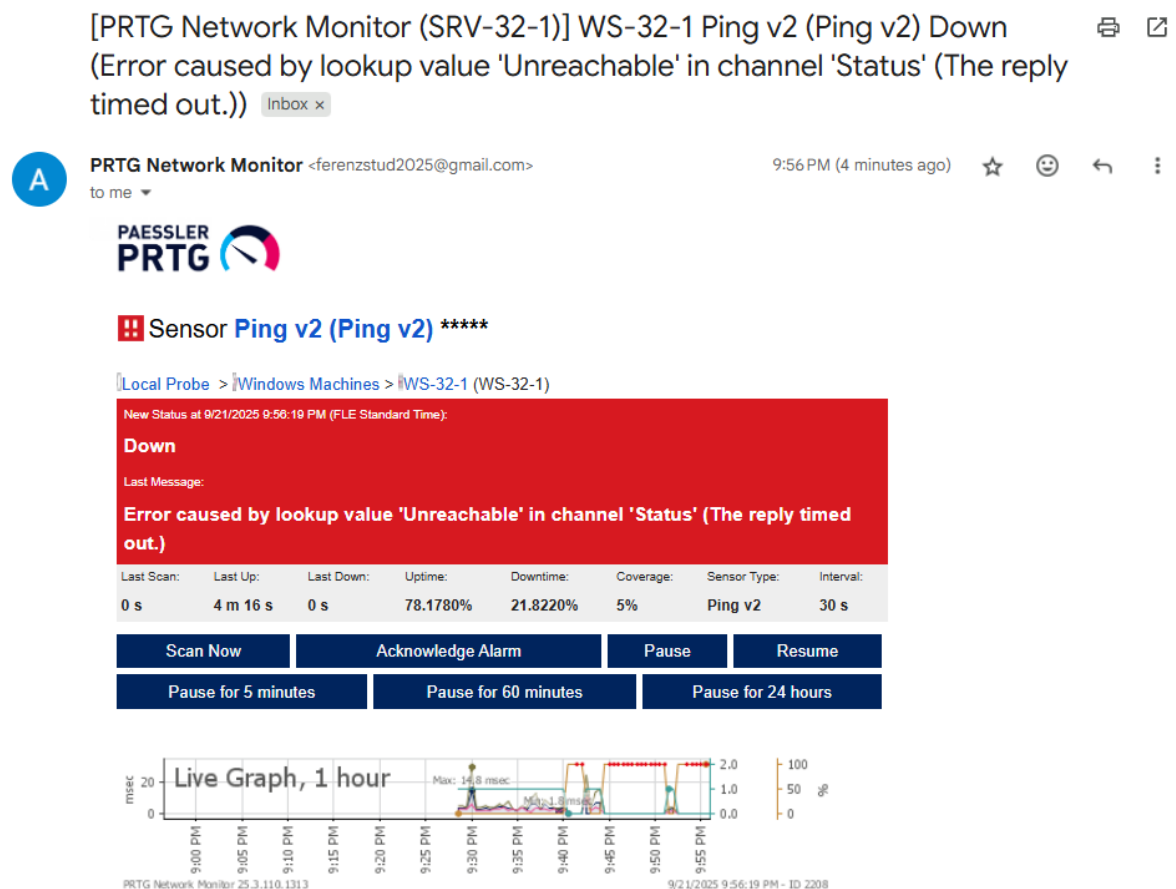


Рисунок 3.46 – Сповіщення про недоступність пристрою WS-32-1

Тепер підключимо назад кабель до WS-32-1 та почекаємо декілька хвилин поки на пошту не надійде новий лист від PRTG. У цьому випадку, повідомлення сповіщає, що пристрій WS-32-1, який раніше був недоступним, тепер знову в стані «Up» (доступний). У листі також вказано точний час простою і візуальну інформацію про стан сенсора у вигляді графіку, рис.3.47.

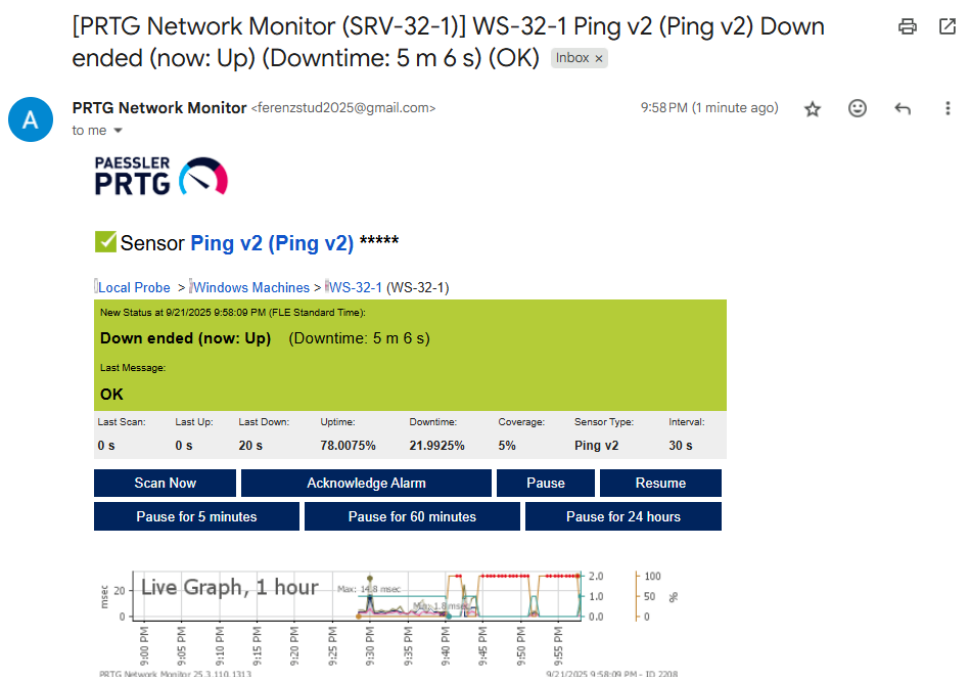


Рисунок 3.47 – Сповіщення про доступність пристрою WS-32-1

Тепер перевіримо можливість підключення до мережевих пристроїв через SSH та роботу сенсору пов'язаного зі збором подій Syslog. Для цього із сервера SRV-32-1 здійснюється віддалене підключення до маршрутизатора R-32-1. Спершу введемо некоректні дані для неіснуючого користувача test1, а потім правильні облікові дані для admin, рис.3.48.

```

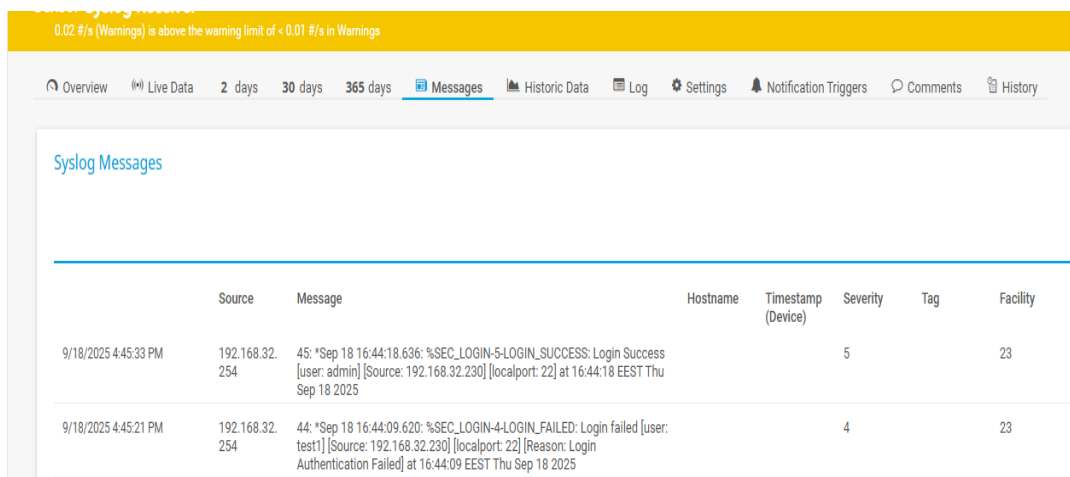
SRV-32-1 (Зріз 1) [Запущено] - Oracle VM VirtualBox
Файл  Машина  Перегляд  Введення  Пристрої  Довідка

OpenSSH SSH client
PS C:\Users\Administrator> ssh test1@R-32-1 -c aes256-cbc
Password:
Password:
Password:
test1@r-32-1's password:
PS C:\Users\Administrator> ssh admin@R-32-1 -c aes256-cbc
Password:

R-32-1#sh clock
*16:44:24.452 EEST Thu Sep 18 2025
R-32-1#
  
```

Рисунок 3.48 – Віддалене підключення до маршрутизатора R-32-1

Після цього переглянемо інформацію стосовно сенсору Syslog для R-32-1. Через вкладку «Messages» можемо переглянути отримані події від пристрою. Можна побачити, що о 16:45:11, 16:45:16 і 16:45:21 зафіксовано невдалі спроби аутентифікації з IP-адреси 192.168.32.230 (SRV-32-1) через порт 22 (SSH). Натомість о 16:45:33 було зареєстровано успішний вхід до системи під користувачем admin. Для кожної події вказано рівень важливості (Severity) та категорію (Facility), рис.3.49.



	Source	Message	Hostname	Timestamp (Device)	Severity	Tag	Facility
9/18/2025 4:45:33 PM	192.168.32.254	45: *Sep 18 16:44:18.636: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: admin] [Source: 192.168.32.230] [localport: 22] at 16:44:18 EEST Thu Sep 18 2025			5		23
9/18/2025 4:45:21 PM	192.168.32.254	44: *Sep 18 16:44:09.620: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: test1] [Source: 192.168.32.230] [localport: 22] [Reason: Login Authentication Failed] at 16:44:09 EEST Thu Sep 18 2025			4		23

Рисунок 3.49 – Перегляд отриманих подій на сенсорі «Syslog»

Перевіримо роботу сенсора Netflow для R-32-1. Відкривши його побачимо візуалізацію мережевих з'єднань у вигляді кругової діаграми, яка демонструє взаємозв'язок між різними IP-адресами та пристроями. Зліва на панелі є можливість вибрати різні часові проміжки для більш гнучкого аналізу, рис.3.50.

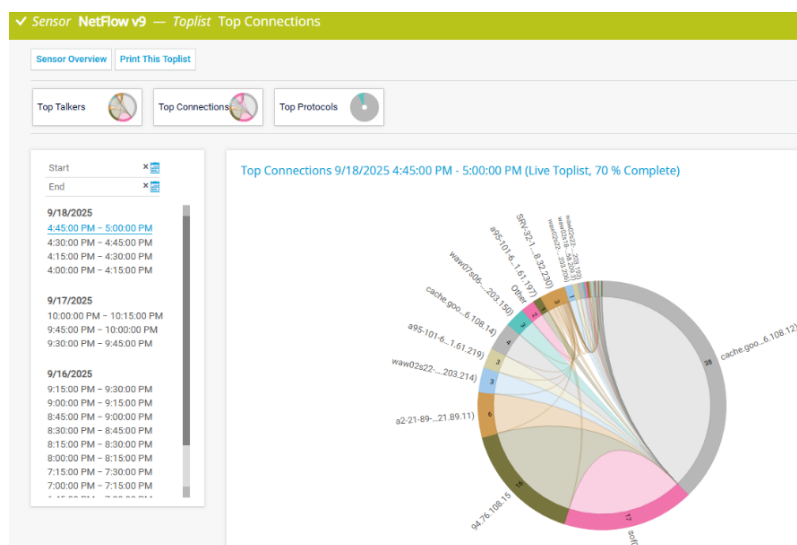


Рисунок 3.50 – Зібрана інформація зі сенсору «Netflow v9»

Також тут можемо переглянути аналітичний дашборд NetFlow, який надає детальний огляд мережевого трафіку. Можемо переглянути найбільш активні джерела трафіку (Top Talkers), найпопулярніші з'єднання (Top Connections), найбільш використовувані протоколи (Top Protocols) переглянути мінімальну та максимальну швидкість передачі даних по кожній категорії трафіку, рис.3.51.

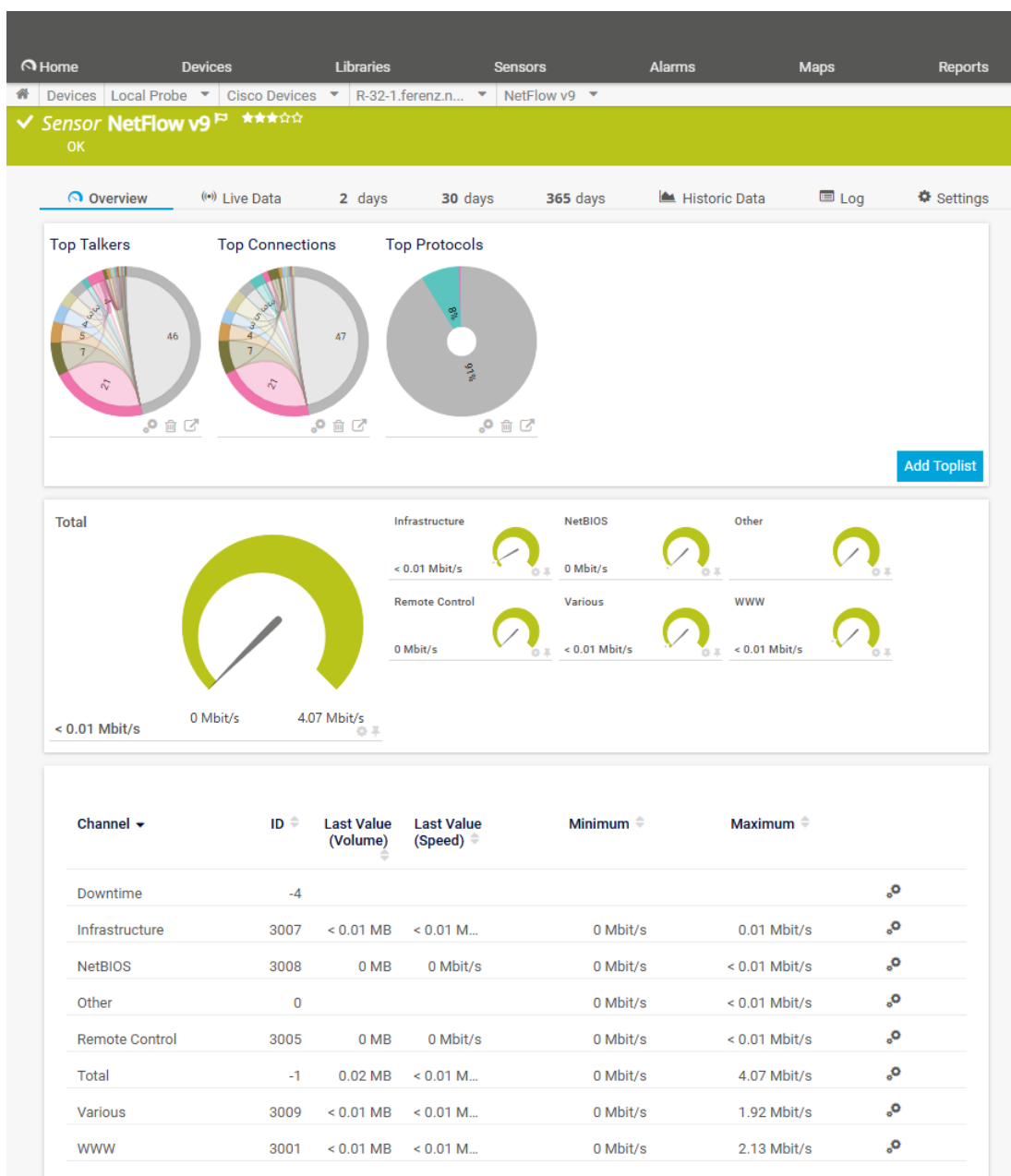


Рисунок 3.51 – Зібрана інформація зі сенсору «Netflow v9» для R-32-1

Далі переглянемо загальну інформацію по всім сенсори для кожного доданого пристрою, рис.3.52-3.53. Розширені варіанти рисунків наведені на додатку Б.

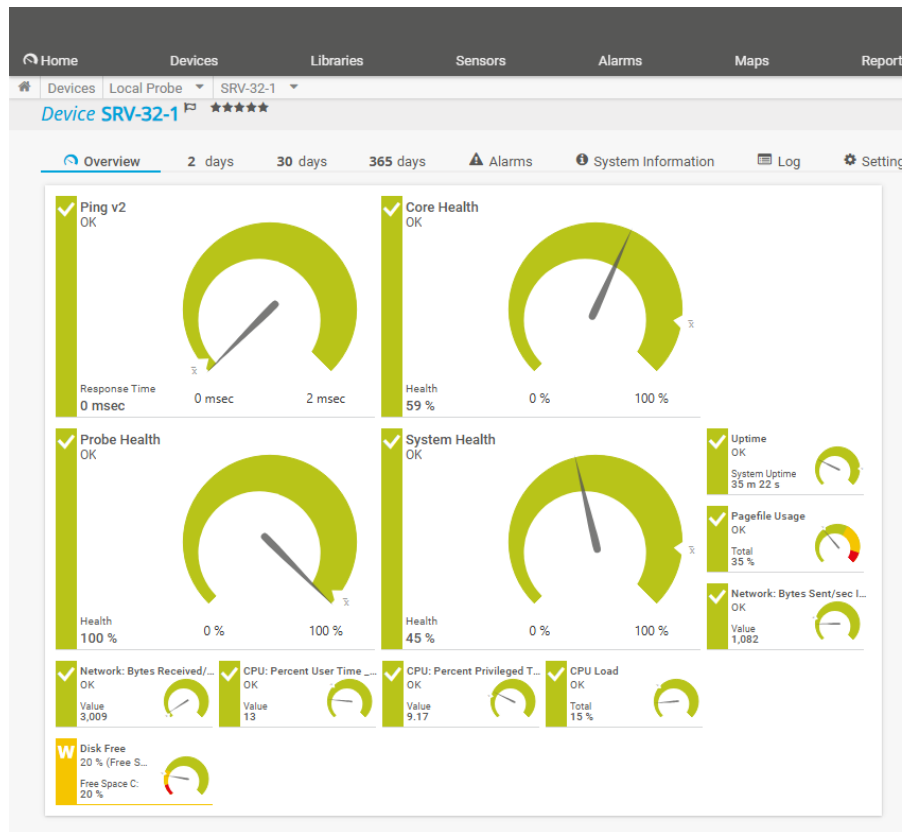


Рисунок 3.52 – Загальна інформація по всім сенсорам для SRV-32-1

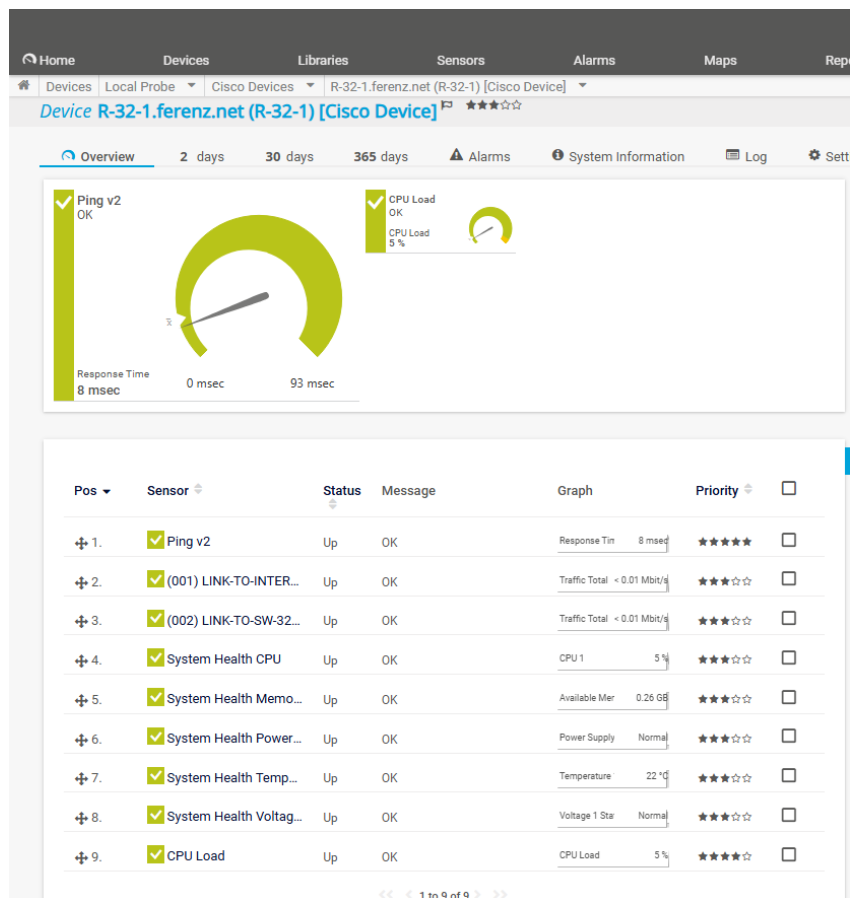


Рисунок 3.53 – Загальна інформація по всім сенсорам для R-32-1

Крім того, у PRTG передбачена можливість вказати місце розташування пристроїв, що особливо зручно у випадку, коли вони знаходяться в різних локаціях, рис.3.54.

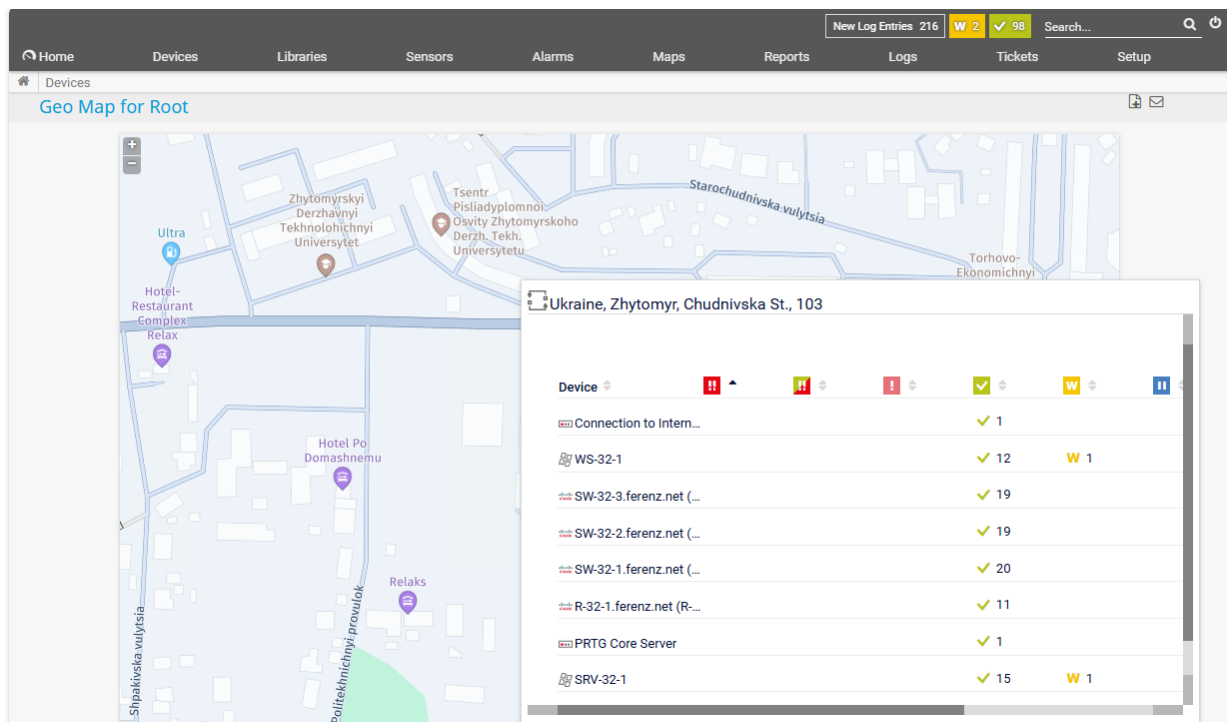


Рисунок 3.54 – Карта з розташуванням доданих пристроїв

Наостанок розглянемо функцію створення звітів. Для цього слід обрати шаблон звіту та обрати необхідні для нас пристрої та сенсори. В даному випадку сформуємо звіт по всім сенсорам сервера SRV-32-1, рис.3.55-3.56.

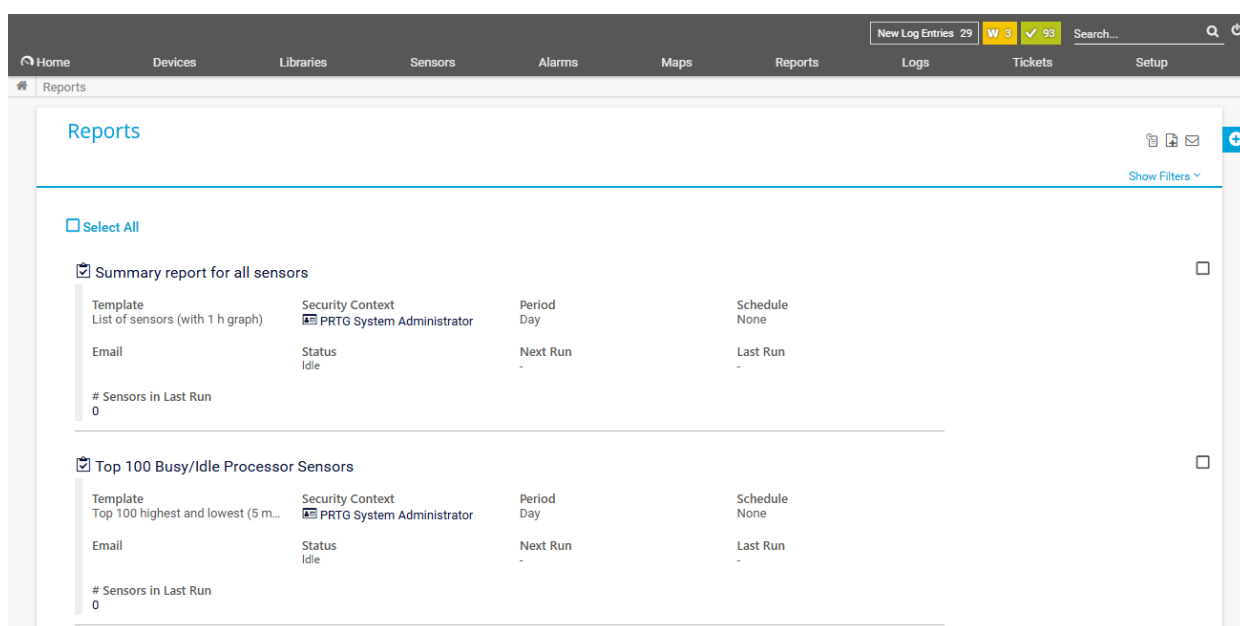


Рисунок 3.55 – Вибір шаблону звіту

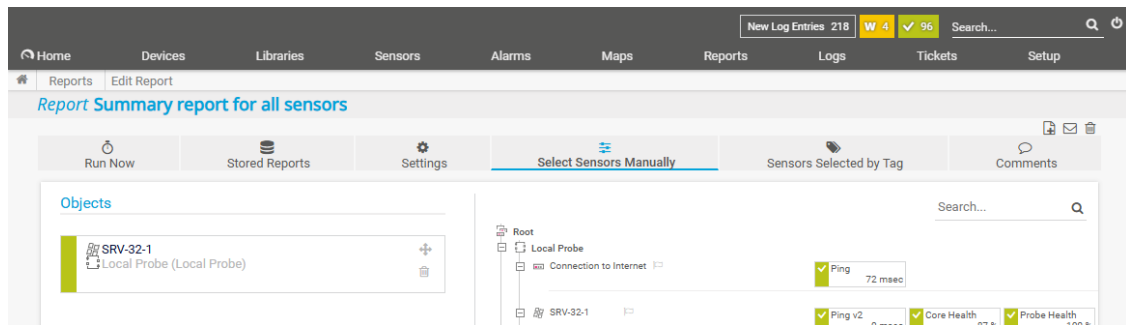


Рисунок 3.56 – Вибір пристроїв та сенсорів для звіту

Тепер слід зазначити часовий період за який бажаємо отримати звітність та обрати формат отримання. В даному випадку вкажемо, щоб готовий звіт відразу був надісланий на нашу персональну пошту, рис.3.57.

Рисунок 3.57 – Налаштування часового періоду збору даних для звіту, формат створення та електронну пошту отримувача

За кілька хвилин на електронну пошту надходить лист зі звітом у форматі PDF. Його можна завантажити та переглянути, при цьому всі дані в ньому представлені у вигляді діаграм, рис.3.58–3.59. Повна версія звіту наведена в додатку В.

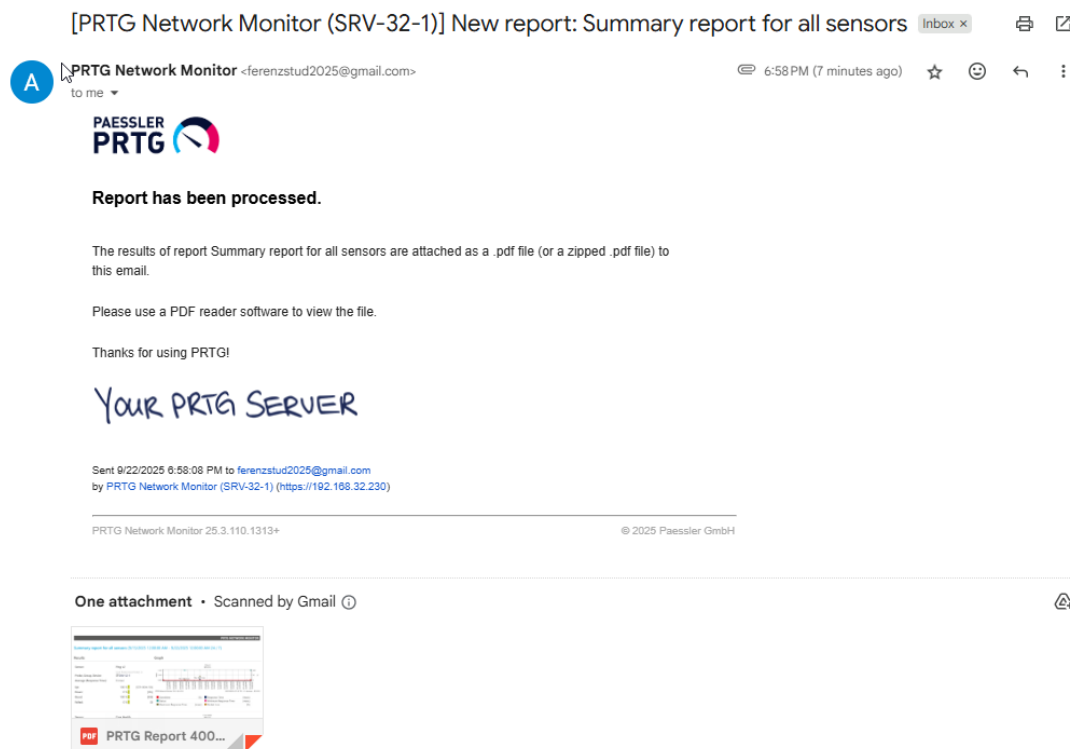


Рисунок 3.58 – Отриманий лист від PRTG зі сформованим звітом

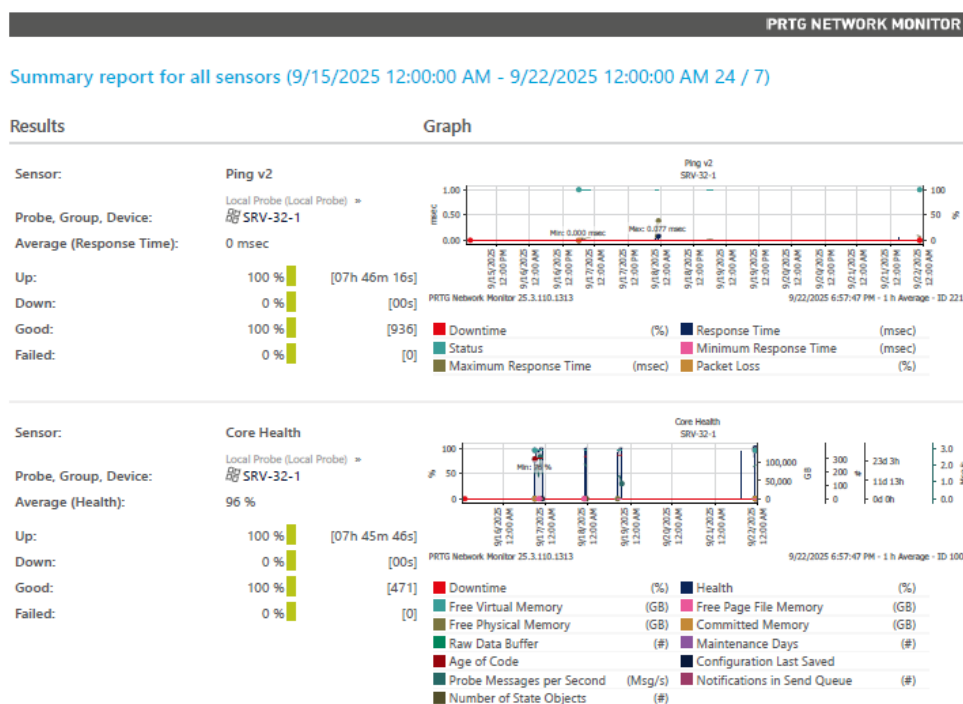


Рисунок 3.59 – Перегляд звіту (частина)

Висновки до третього розділу

У ході виконання даного розділу було реалізовано первинне налаштування мережевої інфраструктури в середовищі GNS3, виконано базову конфігурацію маршрутизаторів і комутаторів, налаштовано NAT, DNS, NTP, SSH та виділено VLAN для невикористаних портів. Здійснено налаштування сервера SRV-32-1 із встановленням ролей Active Directory, DNS і DHCP, створено домен та облікові записи користувачів, а також приєднано робочі станції до домену та перевірено наявність зв'язку між пристроями мережі.

Було встановлено та налаштовано систему моніторингу PRTG Network Monitor, виконано конфігурацію облікових даних для WMI та SNMPv3, а також налаштовано протоколи Syslog і NetFlow для збору даних із мережевих пристроїв. Виконано автоматичне та ручне додавання сенсорів, що дозволило відстежувати поточний стан і статус роботи маршрутизатору, комутаторів, серверу і робочих станцій, у тому числі стан інтерфейсів, їх трафік, події Syslog та IP-потоки. Для перевірки безпеки було здійснено аналіз переданих SNMPv3-пакетів у Wireshark, що підтвердило їх шифрування. Також налаштовано механізм сповіщень про події через електронну пошту, що забезпечує оперативне інформування адміністратора про зміни в роботі сенсорів.

Наприкінці було проведено тестування працездатності системи моніторингу PRTG, під час якого перевірено роботу сенсорів, механізмів сповіщень та коректність збору даних з мережевих пристроїв. Було змодельовано різні ситуації, зокрема перевищення порогових значень використання ресурсів, недоступність робочої станції та спроби підключення через SSH, що дало змогу перевірити відображення подій у Syslog і своєчасність отримання сповіщень. Додатково протестовано функціонування сенсора NetFlow, переглянуто статистику по трафіку, загальний стан сенсорів та відображення пристроїв на карті мережі. Окремо було сформовано автоматичний звіт у форматі PDF з діаграмами, що підтвердило можливість централізованого контролю та аналізу роботи мережі.

ВИСНОВКИ

У ході роботи над розділом було розглянуто теоретичні засади роботи систем моніторингу мережі, які є критично важливим для забезпечення проактивного виявлення несправностей та кіберзахисту. Було виконано аналіз популярних безкоштовних рішень систем моніторингу таких, як Zabbix, Prometheus, Nagios Core, Icinga та Paessler PRTG. Було детально розглянуто функціональні можливості PRTG, що включають швидкість розгортанням, уніфікований інтерфейс та використанням понад 200 попередньо налаштованих сенсорів для забезпечення комплексного моніторингу всієї IT-інфраструктури, включаючи мережі, сервери та хмарні сервіси.

У другому розділі було успішно розроблено проєкт комп'ютерної мережі на базі тривірневої моделі Cisco (ядро, розподіл, доступ) включаючи логічну та фізичну топологію з детальною IP-адресацією. Центральною частиною реалізації став вибір мережевого обладнання Cisco та обґрунтування технічних вимог для серверу Windows Server 2022 і кінцевих станцій Windows 10. Виконано проєктування роботи системи моніторингу на базі PRTG Network Monitor.

У ході виконання третього розділу було успішно здійснено практичну реалізацію, налаштування і тестування спроектованої мережевої інфраструктури у середовищі GNS3, включаючи базову конфігурацію мережевих пристроїв та розгортання централізованих служб на сервері SRV-32-1 (Active Directory, DNS, DHCP). Ключовим етапом стало впровадження та налаштування системи моніторингу PRTG Network Monitor, де було конфігуровано сенсори використовуючи протоколи збору даних SNMPv3, NetFlow v9, WMI та Syslog. Працездатність системи була підтверджена тестуванням і моделюванням аварійних ситуацій (перевищення порогів використання, недоступність вузла), а також перевіркою шифрування SNMPv3-пакетів, формуванням звітів та можливість відправки сповіщень, довівши спроможність системи забезпечувати оперативний контроль та своєчасне сповіщення адміністратора.

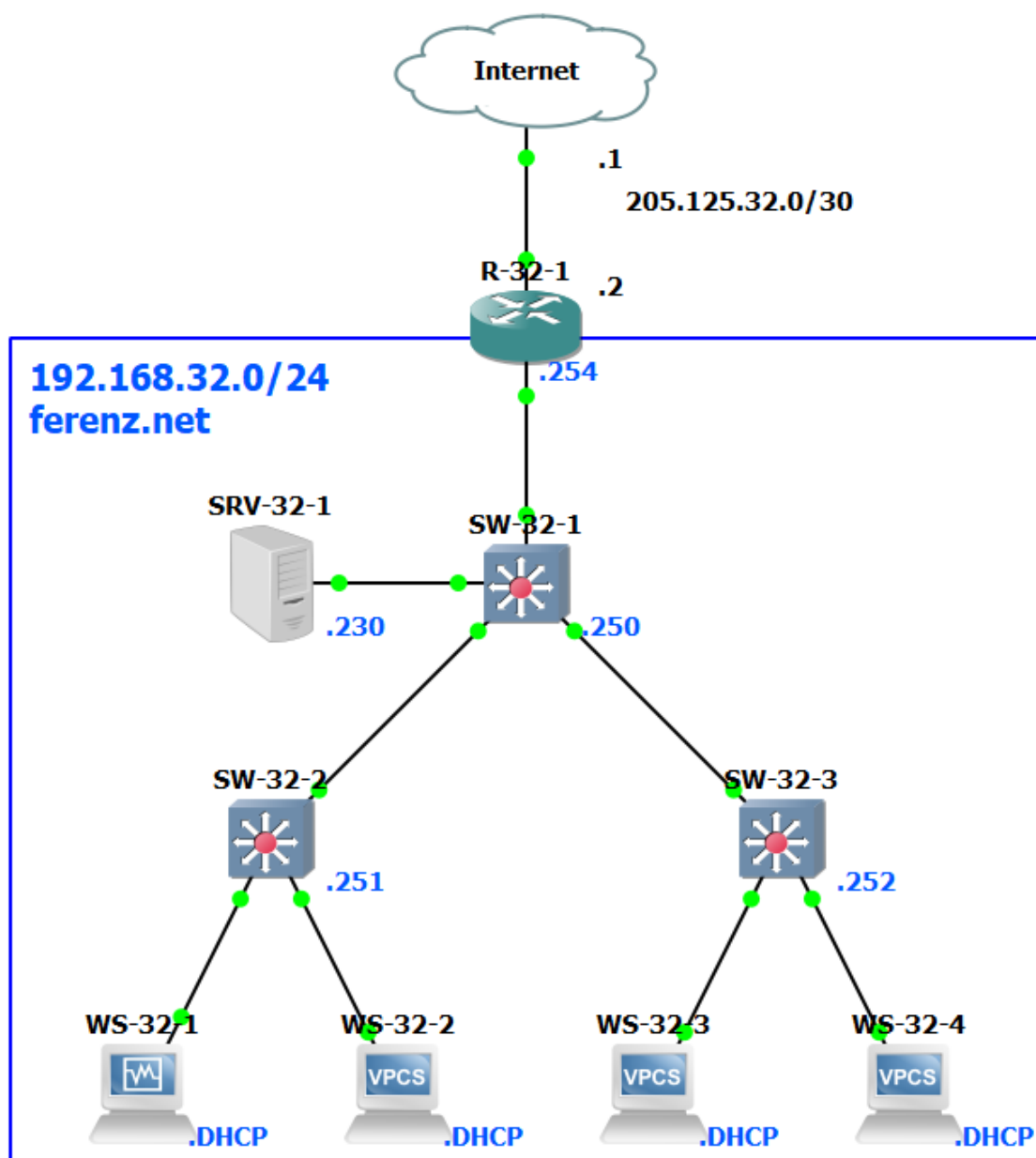
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. What Is Network Monitoring? [Електронний ресурс]. – Режим доступу: <https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/network-monitoring/>
2. Lee, S. Network monitoring: Present and future [Text] / S. Lee, K. Levanti, H. S. Kim // Computer networks. – 2014. – Vol. 65
3. Ultimate Guide to Network Monitoring. [Електронний ресурс]. – Режим доступу: <https://www.dnsstuff.com/network-monitoring>
4. B. Hale, «Network management—back to the basics» Solarwinds Whitepaper, vol. 16, 2012
5. Types of Network Management Protocols. [Електронний ресурс]. – Режим доступу: <https://www.liveaction.com/resources/blog-post/types-of-network-management-protocols/>
6. Ференз А.Р., Фальковський І.Г. Огляд мережевих протоколів, що використовуються для моніторингу // Тези доповідей VIII Всеукраїнської науково-технічної конференції «Комп'ютерні технології: інновації, проблеми, рішення», м. Житомир, 02-03 грудня 2025 року
7. SNMPv1 vs. V2c vs. V3 – SNMP Versions Comparison. [Електронний ресурс]. – Режим доступу: <https://www.parkplacetechnologies.com/blog/snmpv1-vs-v2c-vs-v3-versions-comparison/>
8. 24 Best System Monitoring Tools Reviewed in 2025. [Електронний ресурс]. – Режим доступу: <https://thectoclub.com/tools/best-system-monitoring-tools/>
9. The 7 Best Free Monitoring Software on the Market. [Електронний ресурс]. – Режим доступу: <https://instatus.com/blog/free-monitoring-services>
10. Top 10 Network Monitoring Tools for 2025. [Електронний ресурс]. – Режим доступу: <https://uptrace.dev/tools/network-monitoring-tools>
11. PRTG Network Monitor: All-in-One Network Monitoring Software. [Електронний ресурс]. – Режим доступу: <https://www.paessler.com/prtg>

12. What is PRTG? [Электронный ресурс]. – Режим доступа: <https://www.virtualhostedpbx.net/what-is-prtg>
13. PRTG Manual: Failover Cluster. A Complete Guide to Effective Network, Server, and IT Infrastructure Monitoring. [Электронный ресурс]. – Режим доступа: https://www.paessler.com/manuals/prtg/failover_cluster
14. A Guide to Simple Two-Tier, Three-Tier, and Spine-Leaf Designs. [Электронный ресурс]. – Режим доступа: [Электронный ресурс]. – Режим доступа: <https://learningnetwork.cisco.com/s/question/0D56e0000EBtd2dCQB/a-guide-to-simple-twotier-threetier-and-spineleaf-designs>
15. System requirements for Paessler PRTG. [Электронный ресурс]. – Режим доступа: https://www-assets.paessler.com/stopaeneos-target-container-prod/1c8070f41a274e4d15d62bbc44f7ddf0ddd453df/System-Requirements_EN.pdf
16. Cisco 4321 Integrated Services Router. [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/support/routers/4321-integrated-services-router/model.html>
17. Cisco Catalyst 1300 Series Switches. [Электронный ресурс]. – Режим доступа: <https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-1300-series-switches/nb-06-cat1300-ser-data-sheet-cte-en.html>
18. GNS3. [Электронный ресурс]. – Режим доступа: <https://gns3.com/software/download>
19. PRTG Network Monitor - Download and install now. [Электронный ресурс]. – Режим доступа: <https://www.paessler.com/prtg/download-1>

ДОДАТКИ

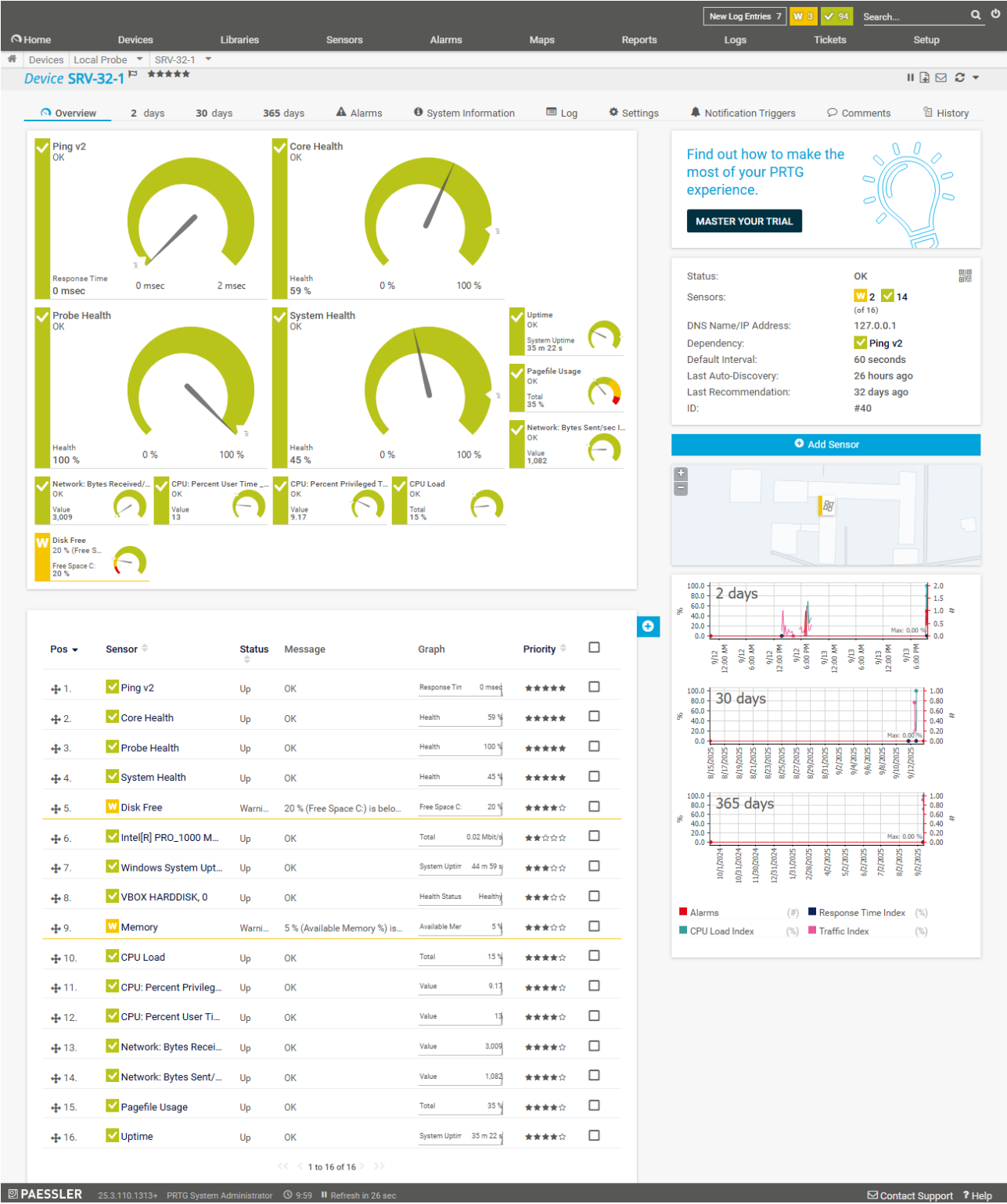
Схема проєкту мережі в емуляторі GNS3



Таблиця адресації пристроїв мережі

Мережа /Пристрій	Інтерфейс/Мережний адаптер/Шлюз	ІР-адреса	Маска	Пре- фікс
WAN	—	205.125.32.0	255.255.255.252	/30
LAN	—	192.168.32.0	255.255.255.0	/24
Маршрутизатор R-32-1	Eth0	205.125.32.2	255.255.255.252	/30
	Eth1	192.168.32.254	255.255.255.0	/24
Комутатор SW-32-1	Інтерфейс Vlan 1	192.168.32.250	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.32.254	—	
Комутатор SW-32-2	Інтерфейс Vlan 1	192.168.32.251	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.32.254	—	
Комутатор SW-32-3	Інтерфейс Vlan 1	192.168.32.252	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.32.254	—	
Сервер SRV-32-1	Eth0	192.168.32.230	255.255.255.0	/24
	Шлюз за замовчуванням	192.168.32.254	—	
Робочі станції WS-32-1 – WS-35-4	Eth0	DHCP		
	Шлюз за замовчуванням			

Інформація стосовно SRV-32-1



Інформація стосовно SRV-32-1 (продовження)

Home

Devices

Libraries

Sensors

Alarms

Maps

Reports

Logs

Tickets

Setup

New Log Entries 28

W 4

92

Search...

Devices

Local Probe

SRV-32-1

Device SRV-32-1

Overview

2 days

30 days

365 days

Alarms

System Information

Log

Settings

Notification Triggers

Comments

History

System Information

> System

> Hardware

> Software

> Users

> Services

> Processes

System

15 M 56 S Ago

Name	Value
Bios Serial Nu...	0
IPAddress / In...	fe80::155d:1a5f:daba:6f6
IPAddress / In...	192.168.32.230
MACAddress ...	08:00:27:E5:1A:64
Windows Ver...	Microsoft Windows Server 2019 Standard

Hardware

14 M 39 S Ago

Name	Class	Caption	Properties
\\.\PHYSICAL...	DiskDrive	VBOX HARDDISK	More Info
12th Gen Inte...	Processor	Intel64 Family 6 Mo...	More Info
High Definitio...	SoundDevice	High Definition Audi...	More Info
Intel(R) PRO/...	NetworkAdapter	[00000001] Intel(R) ...	More Info
Microsoft Ker...	NetworkAdapter	[00000000] Microso...	More Info
Microsoft Pri...	Printer	Microsoft Print to P...	More Info
Microsoft XP...	Printer	Microsoft XPS Doc...	More Info
VBOX CD-RO...	CDROMDrive	VBOX CD-ROM	More Info

Software

17 M 6 S Ago

Name	Version	Properties
Microsoft Cor...	140.0.3485.66	More Info
Nmap Project...	1.60	More Info
Oracle and/or...	7.0.24.167081	More Info
Paessler Gmb...	25.6.0	More Info
Paessler Gmb...	25.6.0	More Info
Paessler Gmb...	25.3.110.1313	More Info

Users

17 M 41 S Ago

Name	Domain
DWM-1	SRV-32-1
LOCAL SERVI...	SRV-32-1
NETWORK SE...	SRV-32-1
SYSTEM	NT AUTHORITY
UMFD-0	SRV-32-1
UMFD-1	SRV-32-1
WS-32-1\$	FERENZ

Services

15 M 16 S Ago

Items: 50

Name	State	Startup Type	Properties
ADWS	Running	Auto	More Info
AJRouter	Stopped	Manual	More Info
ALG	Stopped	Manual	More Info
AppIDSvc	Stopped	Manual	More Info
AppInfo	Stopped	Manual	More Info
AppMgmt	Stopped	Manual	More Info
AppReadiness	Stopped	Manual	More Info
AppVClient	Stopped	Disabled	More Info

Processes

16 M 30 S Ago

Process Name	Creation Time	PID
svchost.exe	2025-09-13 21:16:58	2548
svchost.exe	2025-09-13 21:16:55	1544
svchost.exe	2025-09-13 21:14:26	740
svchost.exe	2025-09-13 21:14:27	976
svchost.exe	2025-09-13 21:14:38	1980
svchost.exe	2025-09-13 21:14:27	820
svchost.exe	2025-09-13 21:14:37	1804
svchost.exe	2025-09-13 21:14:27	1268
svchost.exe	2025-09-13 21:14:38	2040
svchost.exe	2025-09-13 21:14:38	2028
svchost.exe	2025-09-13 21:14:27	992

What is System Information?

PRTG uses WMI and SNMP to request various system information from your device and shows the results on this page. You get system information for Windows devices that run at least Windows 10, and for Linux, Unix, or other devices that provide SNMP access. Please note that this feature does not fully support all device types. The completeness of your data depends on your system and on the protocols you use.

The following prerequisites are necessary:

- Credentials for the target system in the parent group or device settings
- WMI enabled on probe and target computer for Windows systems
- SNMP enabled on the target device
- Remote Registry Windows service enabled on the target computer
- Remote Procedure Call Windows service enabled on the target computer

If you need more help, see the Knowledge Base: <https://kb.paessler.com/en/topic/67824>

PAESSLER

25.3.110.1313+ PRTG System Administrator 9:36 Refresh in 20 sec

Contact Support Help

Інформація стосовно SRV-32-1 (продовження)

Home

Devices

Libraries

Sensors

Alarms

Maps

Reports

Logs

Tickets

Setup

DevicesLocal ProbeSRV-32-1

Device SRV-32-1

Overview2 days30 days365 daysAlarmsSystem InformationLogSettingsNotification TriggersCommentsHistory

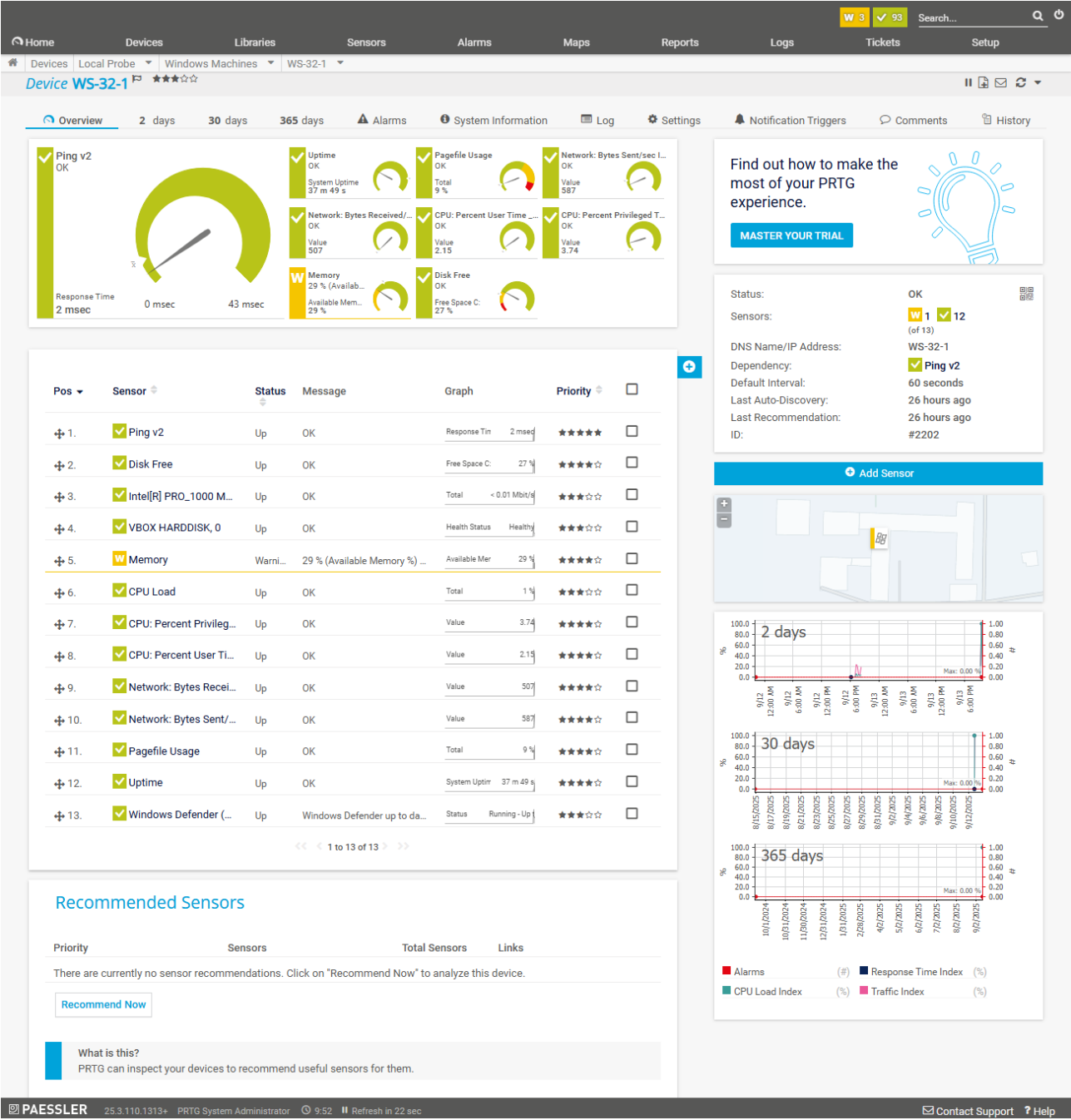
Log

Items: 50Show Filters

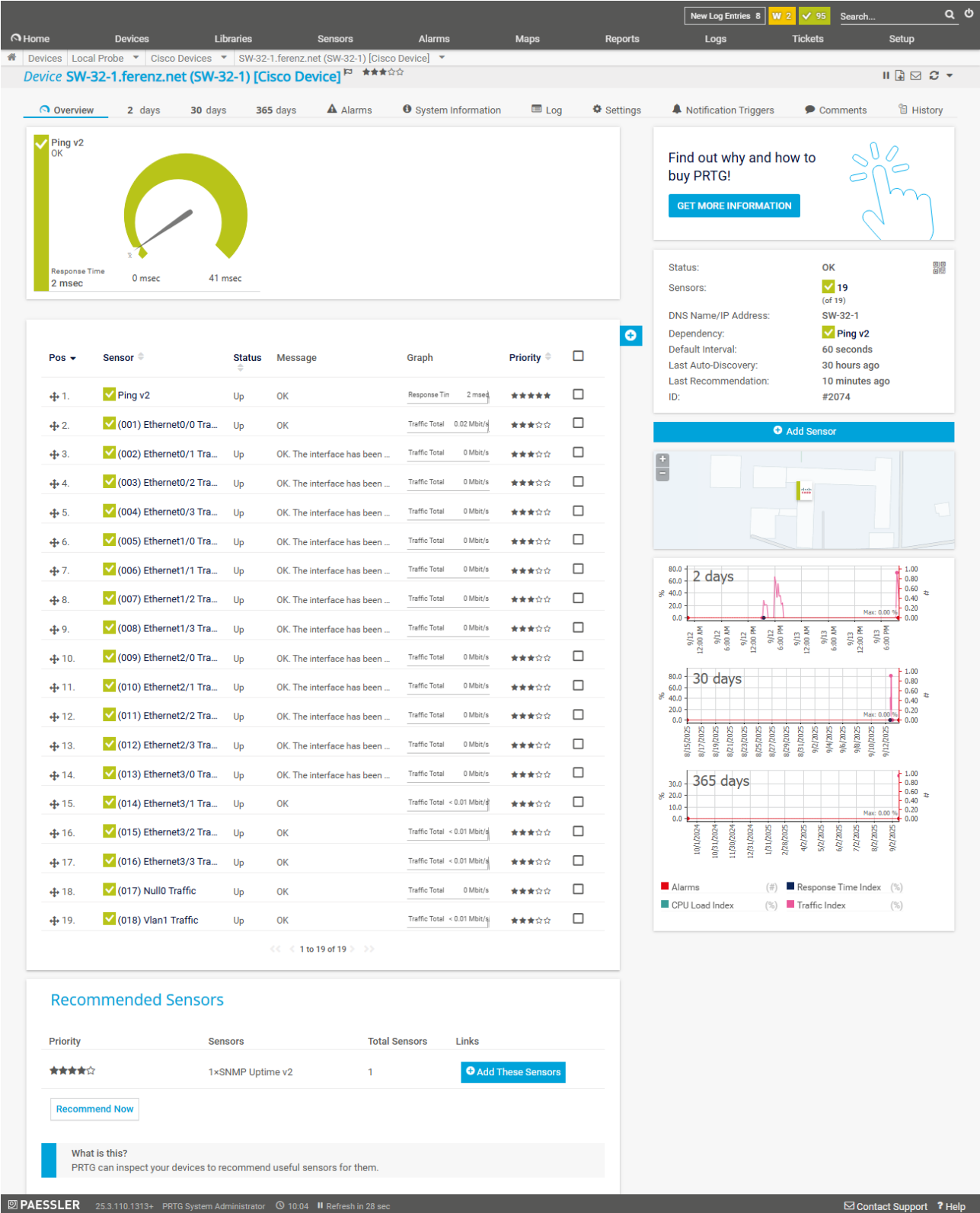
Date Time	Sensor	Status	Message
9/13/2025 9:36:58 PM	System Health	Up	45 %
9/13/2025 9:34:57 PM	System Health	Warning	54 % (System CPU Load) is above the warning limit of 50 % in Sys
9/13/2025 9:27:56 PM	Memory	Warning	20 % (Available Memory %) is below the warning limit of 30 % in A
9/13/2025 9:24:50 PM	System Health	Up	100 %
9/13/2025 9:23:50 PM	System Health	Warning	54 % (System CPU Load) is above the warning limit of 50 % in Sys
9/13/2025 9:20:50 PM	System Health	Down	96 % (System CPU Load) is above the error limit of 90 % in System
9/13/2025 9:20:29 PM	Network: Bytes Received/sec Intel...	Up	4,249
9/13/2025 9:20:23 PM	Network: Bytes Sent/sec Intel[R] ...	Up	1,608
9/13/2025 9:20:18 PM	CPU: Percent User Time _Total	Up	72
9/13/2025 9:20:11 PM	CPU Load	Up	99 %
9/13/2025 9:20:05 PM	Intel[R] PRO_1000 MT Desktop A...	Up	0.03 Mbit/s
9/13/2025 9:19:59 PM	CPU: Percent Privileged Time _To...	Up	27
9/13/2025 9:19:26 PM	Uptime	Up	5 m 9 s
9/13/2025 9:19:14 PM	Pagefile Usage	Up	6 %
9/13/2025 9:19:08 PM	Disk Free	Warning	22 % (Free Space C:) is below the warning limit of 25 % in Free Sp
9/13/2025 9:19:04 PM	VBOX HARDDISK, 0	Up	Healthy
9/13/2025 9:18:56 PM	Memory	Up	44 %
9/13/2025 9:18:53 PM	Windows System Uptime	Up	4 m 36 s
9/13/2025 9:18:50 PM	Ping v2	Up	0 msec
9/13/2025 9:18:50 PM	System Health	Up	100 %
9/13/2025 9:18:47 PM	Probe Health	Up	100 %
9/13/2025 9:18:44 PM	Core Health	Up	100 %
9/13/2025 9:17:49 PM	Probe Health	Down	Probe disconnected (Disconnected)
9/12/2025 7:59:36 PM	Probe Health	Down	Probe disconnected (Disconnected)
9/12/2025 7:49:55 PM	System Health	Up	55 %
9/12/2025 7:48:55 PM	System Health	Warning	70 % (System CPU Load) is above the warning limit of 50 % in Sys
9/12/2025 7:39:55 PM	System Health	Up	75 %
9/12/2025 7:38:55 PM	System Health	Warning	52 % (System CPU Load) is above the warning limit of 50 % in Sys
9/12/2025 7:33:55 PM	System Health	Up	40 %
9/12/2025 7:32:51 PM	System Health	Warning	60 % (System CPU Load) is above the warning limit of 50 % in Sys
9/12/2025 7:28:29 PM	Child Object Dele...	Sensor "VBOX HARDDISK, 0"	
9/12/2025 7:27:14 PM	Child Object Dele...	Sensor "CPU: Processor Queue Length "	
9/12/2025 7:25:04 PM	Child Object Dele...	Sensor "Memory"	
9/12/2025 7:25:04 PM	Child Object Dele...	Sensor "Disk Free"	
9/12/2025 7:24:38 PM	Child Object Dele...	Sensor "CPU Load"	
9/12/2025 7:22:01 PM	Child Object Dele...	Sensor "Thread: Context Switches/sec _Total/_Total"	
9/12/2025 7:20:51 PM	Child Object Dele...	Sensor "Network: Bytes Total/sec Intel[R] PRO_1000 MT Desktop	
9/12/2025 7:20:18 PM	Child Object Dele...	Sensor "Memory: Pool Nonpaged Bytes "	
9/12/2025 7:20:18 PM	Child Object Dele...	Sensor "Memory: Pages/sec "	
9/12/2025 7:20:18 PM	Child Object Dele...	Sensor "Memory: Page Writes/sec "	
9/12/2025 7:20:18 PM	Child Object Dele...	Sensor "Memory: Page Reads/sec "	
9/12/2025 7:20:18 PM	Child Object Dele...	Sensor "Memory: Page Faults/sec "	
9/12/2025 7:19:43 PM	Child Object Dele...	Sensor "Volume IO HarddiskVolume1"	
9/12/2025 7:19:43 PM	Child Object Dele...	Sensor "Volume IO C:"	
9/12/2025 7:19:43 PM	Child Object Dele...	Sensor "Volume IO _Total"	
9/12/2025 7:19:43 PM	Child Object Dele...	Sensor "Disk IO 0 C:"	
9/12/2025 7:19:43 PM	Child Object Dele...	Sensor "Disk IO _Total"	
9/12/2025 7:19:19 PM	Child Object Dele...	Sensor "Intel[R] PRO_1000 MT Desktop Adapter"	
9/12/2025 7:18:26 PM	Child Object Dele...	Sensor "Physical Disk: Percent Disk Time 0 C:"	
9/12/2025 7:18:26 PM	Child Object Dele...	Sensor "Physical Disk: Percent Disk Time _Total"	

<< < 1 to 50 >

Інформація стосовно WS-32-1



Інформація стосовно SW-32-1



3bit 3 SRV-32-1

PRTG NETWORK MONITOR

Summary report for all sensors (9/15/2025 12:00:00 AM - 9/22/2025 12:00:00 AM 24 / 7)

Results

Graph

Sensor: Ping v2

Local Probe (Local Probe) »

SRV-32-1

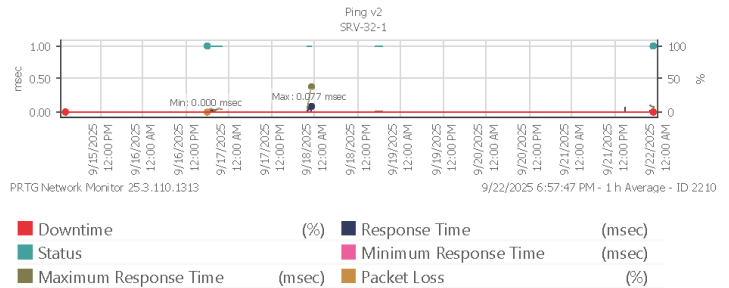
Average (Response Time): 0 msec

Up: 100 % [07h 46m 16s]

Down: 0 % [00s]

Good: 100 % [936]

Failed: 0 % [0]



Sensor: Core Health

Local Probe (Local Probe) »

SRV-32-1

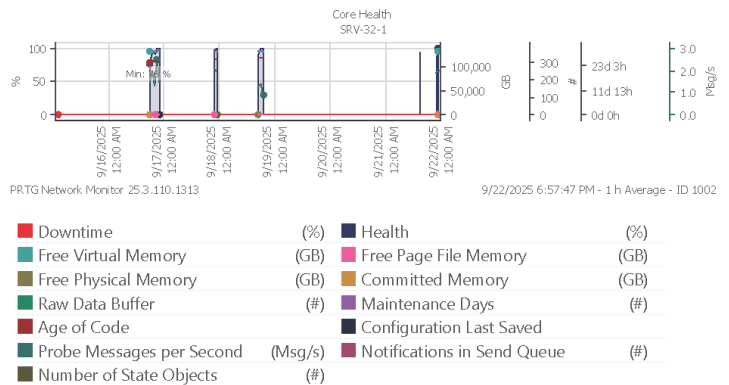
Average (Health): 96 %

Up: 100 % [07h 45m 46s]

Down: 0 % [00s]

Good: 100 % [471]

Failed: 0 % [0]



Sensor: Probe Health

Local Probe (Local Probe) »

SRV-32-1

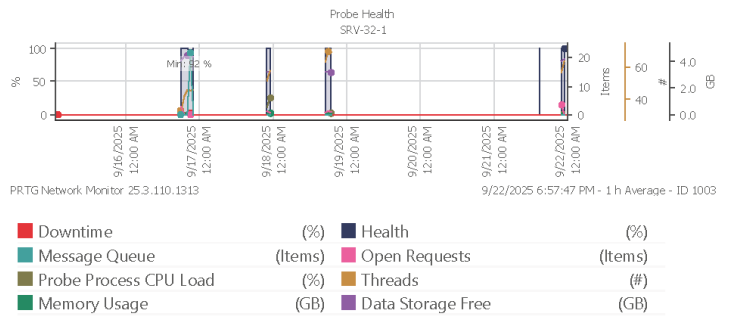
Average (Health): > 99 %

Up: 99.785 % [07h 44m 46s]

Down: 0.215 % [01m 00s]

Good: 99.576 % [470]

Failed: 0.424 % [2]



Sensor: System Health

Local Probe (Local Probe) »

SRV-32-1

Average (Health): 95 %

Up: 99.141 % [07h 41m 46s]

Down: 0.859 % [04m 00s]



Звіт з SRV-32-1 (продовження)

Good:	98.097 %	[464]	Downtime	(%)	Health	(%)
Failed:	1.903 %	[9]	System CPU Load	(%)	Available Memory	(GB)

Sensor:

Probe, Group, Device:

Average (Free Space C:):

Up:

Down:

Good:

Failed:

Disk Free

Local Probe (Local Probe) »

SRV-32-1

20 %

100 %

0 %

100 %

0 %

[07h 41m 46s]

[00s]

[466]

[0]

Disk Free

SRV-32-1

Max: 28.0 %

Min: 13.1 %

9/22/2025 6:57:47 PM - 1 h Average - ID 1004

Sensor:

Probe, Group, Device:

Average (Total):

Total (Total):

Up:

Down:

Good:

Failed:

Intel[R] PRO 1000 MT Desktop Adapter

Local Probe (Local Probe) »

SRV-32-1

0.06 Mbit/s

197 MB

100 %

0 %

100 %

0 %

[07h 36m 46s]

[00s]

[461]

[0]

Intel[R] PRO 1000 MT Desktop Adapter

SRV-32-1

Max: 0.147 Mbit/s

Min: 0.000 Mbit/s

9/22/2025 6:57:47 PM - 1 h Average - ID 1005

Sensor:

Probe, Group, Device:

Average (System Uptime):

Up:

Down:

Good:

Failed:

Windows System Uptime

Local Probe (Local Probe) »

SRV-32-1

1 h 23 m

100 %

0 %

100 %

0 %

[07h 45m 46s]

[00s]

[471]

[0]

Windows System Uptime

SRV-32-1

Max: 3 h 28 m

Min: 6 m 34 s

9/22/2025 6:57:48 PM - 1 h Average - ID 2205

Sensor:

Probe, Group, Device:

Average (Health Status):

Up:

Down:

Good:

Failed:

VBOX HARDDISK, 0

Local Probe (Local Probe) »

SRV-32-1

100 %

100 %

0 %

100 %

0 %

[07h 43m 40s]

[00s]

[468]

[0]

VBOX HARDDISK, 0

SRV-32-1

Max: 100 %

Min: 0 %

9/22/2025 6:57:48 PM - 1 h Average - ID 2206

Sensor:

Probe, Group, Device:

Average (Available Memory %):

Up:

Memory

Local Probe (Local Probe) »

SRV-32-1

27 %

100 %

[07h 45m 46s]

Memory

SRV-32-1

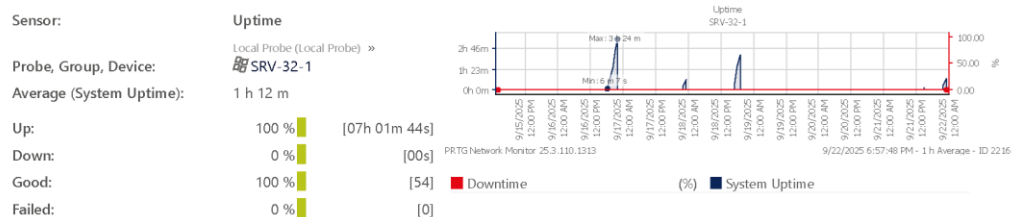
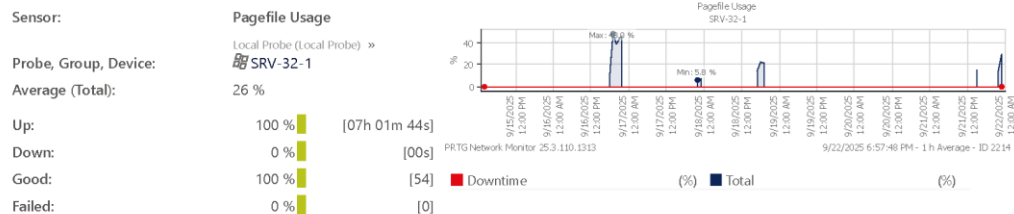
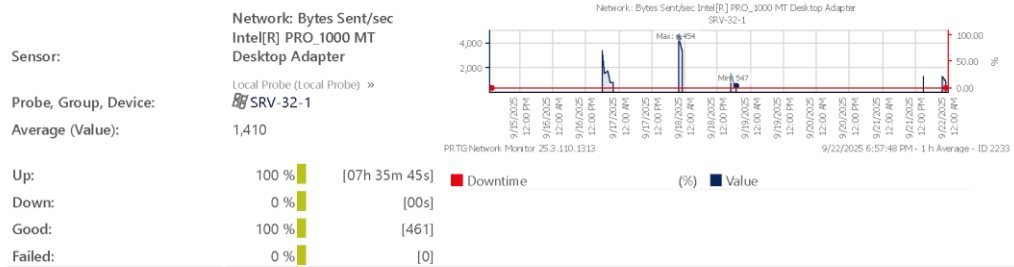
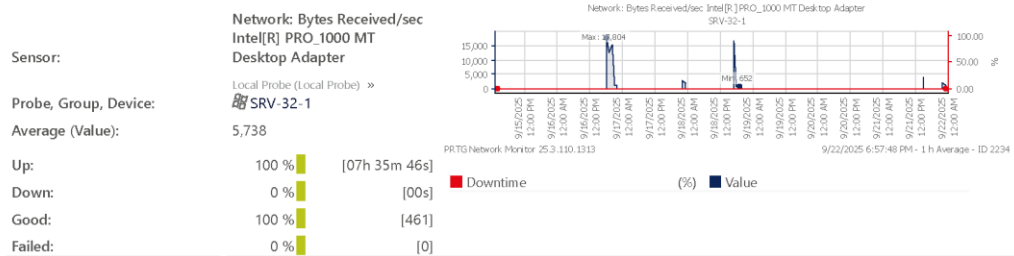
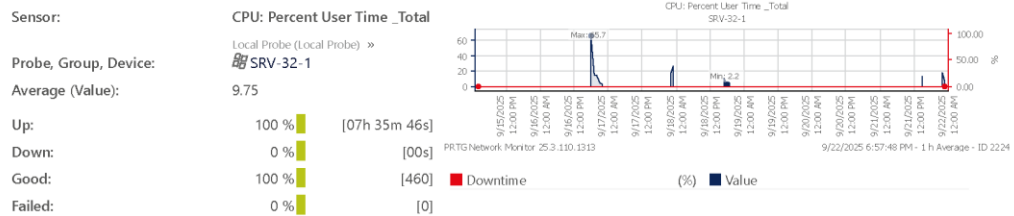
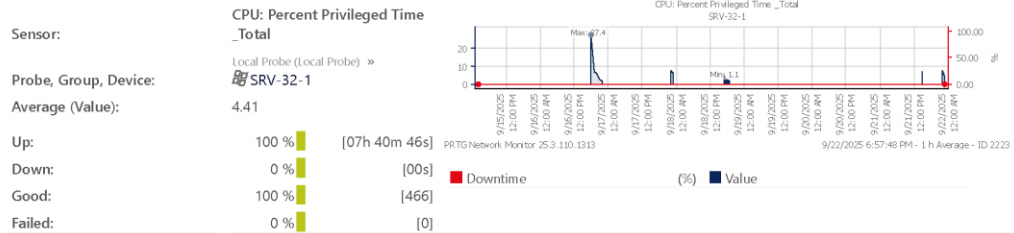
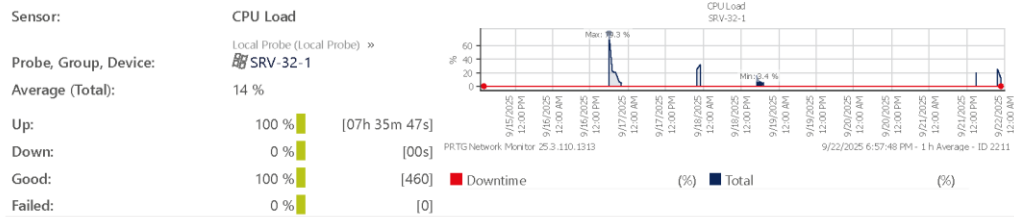
Max: 34.4 %

Min: 28.3 %

9/22/2025 6:57:48 PM - 1 h Average - ID 2207

Звіт з SRV-32-1 (продовження)

Down:	0 %	[00s]	Downtime	(%)	Available Memory %	(%)
Good:	100 %	[470]	Available Memory	(GB)		
Failed:	0 %	[0]				



Конфігураційні файли мережевих пристроїв

R-32-1:

```

upgrade fpd auto
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
!
hostname R-32-1
!
boot-start-marker
boot-end-marker
!
!
enable secret 5
$1$SNKD$k41DcNbQluK0/VPObWRax1
!
no aaa new-model
clock timezone EET 2 0
clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
no ip icmp rate-limit unreachable
!
!
ip flow-cache timeout inactive 10
ip flow-cache timeout active 5
ip domain name ferenz.net
ip name-server 192.168.32.230
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
username admin privilege 15 secret 5
$1$COSW$YRpqAYapvYvSYfZ/TSKe/1
!
redundancy
!
!
ip tcp synwait-time 5
ip ssh time-out 30
ip ssh version 2
!
!
interface FastEthernet0/0
description LINK-TO-INTERNET
ip address 205.125.32.2 255.255.255.252
ip flow ingress
ip nat outside
ip virtual-reassembly in
duplex auto
speed auto
!
interface FastEthernet0/1
description LINK-TO-SW-32-1
ip address 192.168.32.254 255.255.255.0
ip flow ingress
ip nat inside
ip virtual-reassembly in
duplex auto
speed auto
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip flow-export version 9
ip flow-export destination 192.168.32.230
9991
!
ip dns server
ip nat inside source list 1 interface
FastEthernet0/0 overload
ip route 0.0.0.0 0.0.0.0 205.125.32.1
!
logging host 192.168.32.230
access-list 1 permit 192.168.32.0 0.0.0.255
no cdp log mismatch duplex
!
snmp-server group PRTG v3 priv read ALL-
ACCESS
snmp-server view ALL-ACCESS iso included
snmp-server enable traps entity-sensor
threshold
snmp-server host 192.168.32.230 version 3
priv prtguser
!
!
control-plane
!
!
!
mgcp profile default

```

```

!
!
gatekeeper
shutdown
!
!
line con 0
exec-timeout 0 0
privilege level 15
logging synchronous
login local
stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
login local
transport input ssh
!
ntp update-calendar
ntp server SRV-32-1
!
End

```

SW-32-1:

```

version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
localtime
no service password-encryption
service compress-config
!
hostname SW-32-1
!
boot-start-marker
boot-end-marker
!
!
logging discriminator EXCESS severity drops
6 msg-body drops EXCESSCOLL
logging buffered 50000
logging console discriminator EXCESS
enable secret 5
$1$r43c$WAhenxqr1EQJ2qmw1A.Bb1
!
username admin privilege 15 secret 5
$1$e67d$u.MQ7mM1E5BwCBPWsp2d11
no aaa new-model
clock timezone EET 2 0

```

```

clock summer-time EEST recurring last Sun
Mar 3:00 last Sun Oct 4:00
!
!
!
!
no ip routing
no ip icmp rate-limit unreachable
!
!
!
ip domain-name ferenz.net
ip name-server 192.168.32.230
no ip cef
no ipv6 cef
!
!
spanning-tree mode pvst
spanning-tree extend system-id
!
!
interface Ethernet0/0
!
interface Ethernet0/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet0/2
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet0/3
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/0
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/1
switchport access vlan 999
switchport mode access
shutdown
!
interface Ethernet1/2
switchport access vlan 999
switchport mode access
shutdown

```

```

!
interface Ethernet1/3
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet2/0
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet2/1
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet2/2
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet2/3
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet3/0
  switchport access vlan 999
  switchport mode access
  shutdown
!
interface Ethernet3/1
!
interface Ethernet3/2
!
interface Ethernet3/3
!
interface Vlan1
  ip address 192.168.32.250 255.255.255.0
  no ip route-cache
!
ip default-gateway 192.168.32.254
ip forward-protocol nd
!
ip tcp synwait-time 5
ip http server
!
ip ssh time-out 30
ip ssh version 2
ip ssh server algorithm encryption aes128-ctr
aes192-ctr aes256-ctr

```

```

ip ssh client algorithm encryption aes128-ctr
aes192-ctr aes256-ctr
!
!
!
!
snmp-server group PRTG v3 priv read ALL-
ACCESS
snmp-server view ALL-ACCESS iso included
snmp-server host 192.168.32.230 version 3
priv prtguser
!
control-plane
!
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  login local
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
line vty 0 4
  login local
  transport input ssh
!
ntp update-calendar
ntp server SRV-32-1
!
!
end

```