Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)
Кафедра Інформатики
(повна назва)

КВАЛІФІКАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти перший (бакалаврський)

РОЗРОБКА СИСТЕМИ МОНІТОРІНГУ ПРОДУКТИВНОСТІ КОРПОРАТИВНОЇ МЕРЕЖІ
(тема)

Виконав:
студент 4 курсу, групи ІТІНФ-18-1
Сосницький О.В.
(прізвище, ініціали)

Спеціальності 122 Комп'ютерні науки
(код і повна назва спеціальності)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

Керівник доц. Сакало Є.С.
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ Кобилін О.А.
(підпис) (прізвище, ініціали)

2022 р.

Харківський національний університет радіоелектроніки

Факультет Інформаційно-аналітичних технологій та менеджменту
(повна назва)

Кафедра Інформатики
(повна назва)

Рівень вищої освіти перший (бакалаврський)

Спеціальність 122 Комп'ютерні науки
(код і повна назва)

Тип програми освітньо-професійна

Освітня програма Інформатика
(повна назва освітньої програми)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 2022 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

студентові Сосницькому Олександру Вадимовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Розробка системи моніторингу продуктивності корпоративної мережі

затверджена наказом університету від 16 травня 2022 року № 541Ст

2. Термін подання студентом роботи до екзаменаційної комісії 23 травня 2022 р.

3. Вихідні дані до роботи науково-методична та науково-технічна література, матеріали конференцій, дані інтернет-мережі, сервер платформи 1С, сервер бази даних MS SQL 2008, операційна система CentOs 5.5 з ланцюжками NAT у правилах iPtables, операційна система MS Windows 2003 R3, сервер Apache, proxy-сервер Squid.

4. Перелік питань, що потрібно опрацювати в роботі
1. Предметна область і постановка задачі.
2. Впровадження технологій VPN у корпоративну мережу і їх порівняльна оцінка.
3. Створення комплексу систем моніторингу корпоративної мережі.

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (п.5 включається до завдання за рішенням випускової кафедри) скріншоти форм застосунку, система моніторингу Nagios, open-source вебдодаток Cacti з інструментом RRDtool.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата
Консультант з дотримання діючих стандартів та норм	Доцент Бєлова Н.В.		

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Отримання завдання на кваліфікаційну роботу	18.04.2022	
2	Аналіз завдання, підбір літератури	18.04.22-21.04.22	
3	Аналіз літератури з досліджуваної проблеми	22.04.22-25.04.22	
4	Аналіз технічних засобів	26.04.22-30.04.22	
5	Розробка системи моніторингу	01.05.22-14.05.22	
6	Програмна реалізація	15.05.22-23.05.22	
7	Оформлення пояснювальної записки	24.05.22-26.05.22	
8	Перевірка на плагіат	27.05.22	
9	Рецензування	28.05.22	
10	Підготовка презентації та доповіді	29.05.22-30.05.22	
11	Занесення роботи в електронний архів	31.05.22	
12	Попередній захист кваліфікаційної роботи	31.05.22	

Дата видачі завдання 18 квітня 2022 р.

Студент _____

(підпис)

Керівник роботи _____ _____ доц. Сакало Є.С._____

(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ/ABSTRACT

Пояснювальна записка до кваліфікаційної роботи: 59 с., 6 табл., 20 рис., 1 дод., 30 джерел.

ТЕХНОЛОГІЯ OpenVPN, ТЕХНОЛОГІЯ SSH.

Об’єктом роботи є розробка системи моніторингу продуктивності корпоративної мережі.

Метою роботи є моніторинг корпоративної мережі, та впровадження технології OpenVPN та порівняльна оцінка.

Використано технології OpenVPN та SSH. Проведено дослідження моніторингу продуктивності корпоративної мережі.

У результаті роботи здійснена програмна системи моніторингу продуктивності корпоративної мережі.

OpenVPN TECHNOLOGY, SSH TECHNOLOGY.

The object of the research is the development of a system for monitoring the performance of the corporate network.

The aim of the research is to monitor the performance of the corporate network using OpenVPN and SSH technologies.

The OpenVPN and SSH technology used. The research of the performance of the corporate network is done.

As a result of implemented software implementation of the system for monitoring the performance of the corporate network.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

VPN – Virtual Private Network (віртуальна приватна мережа)

SSH – Secure SHell (безпечна оболонка)

ВСТУП

Останнім часом все частіше документообіг та передача корпоративної інформації відбувається в електронному вигляді тим чи іншим способом. Для цього вже існує безліч протоколів та методів передачі даних. Так, наприклад, електронний документообіг підприємства виробляється засобами платформи 1С, що має безліч різних конфігурацій під будь-які потреби бізнесу; пересилання документів електронною поштою з використанням поштових протоколів POP, IMAP, SMTP, передача великих обсягів інформації за допомогою протоколу FTP, організація корпоративного сайту за допомогою вебтехнологій.

Інформаційні технології 21 століття надають великі можливості щодо вдосконалення роботи підприємств, замінюючи людську працю машинною, підвищуючи зростання продуктивності праці та знижуючи витрати на персонал. Створюються нові та модернізуються діючі підприємства, територіально розосереджені в межах населеного пункту, міста або навіть країни, оскільки тепер засоби зв’язку набагато доступніші та дешевші.

Все це стало можливим завдяки комп’ютеризації та використанню мережевих технологій на підприємстві. Але є речі, про які не можна забувати: складність застосування, безпека, продуктивність, захищеність, надійність системи. Головними проблемами на сьогоднішній день стали безпека та життєздатність комп’ютерних систем.

Корпоративна інформація, що передається через відкриту мережу Інтернет, легко може бути перехоплена за допомогою спеціальних програм сніферів – зловмисниками та використовуватись у корисливих цілях. Сюди відносяться найважливіша інформація, що міститься у конфіденційних документах. Крім цього можуть бути перехоплені логіни та паролі від корпоративної пошти чи інших сервісів. Конфіденційність інформації, що передається, виходить на перший план при створенні корпоративної мережі.

Захист інформації, що передається каналами зв’язку, використовуючи паролювання документів або їх шифрування, не надає потрібного рівня безпеки, тому що будь-який пароль може бути зламаний і це лише питання часу (все залежить від його складності), а за допомогою криптоаналізу можна виявити і шифруючий ключ. Звичайно, можна використовувати великі та складні паролі, сучасні великі ключі шифрування, але все це знизить продуктивність, перетворивши простий механізм операції відправлення на досить затратний за тимчасовими параметрами. Час буде витрачено на захист декількох файлів. А якщо це треба робити постійно і у великій кількості?

Для вирішення зазначених протиріч у корпоративних мережах використовуються різні протоколи Virtual Private Network. З їхньою допомогою створюються віртуальні канали зв’язку поверх мережі Інтернет. Вони дають можливість поєднувати локальні мережі різних технологій та їх сегменти в одну корпоративну мережу. Але найголовніше перевага, що заради чого вони і необхідні, це шифрування всього трафіку, що проходить по тунелю на канальному рівні моделі OSI. Шифрування забезпечує захист від доступу до інформації, що передається, а інкапсуляція не дозволяє зловмиснику з’ясувати адресат інформації, що передається.

Все це дає більші можливості для побудови захищеної мережі. Але якщо щось виходить із ладу, програма чи обладнання серверів, то й захищений канал перестає працювати. За станом комп’ютерного парку постійно потрібно вести моніторинг, щоб час простою у разі падіння однієї ділянки мережі був мінімальним. Маючи безліч серверів та сервісів, не так просто дізнатися, де і що сталося. Засобами моніторингу можна стежити за цим, не оминаючи кожен сервер по одному. За допомогою зручних таблиць та поштових повідомлень це не складе великої праці, і адміністратор завжди буде в курсі стану мережі, сервісів та серверів, що входять до цієї корпоративної мережі.

Зазначені проблеми при побудові корпоративних мереж для конкретних підприємств показують, що їх створення не є тривіальним. Тому

в рамках роботи ставляться та вирішуються завдання вибору та реалізації протоколів VPN, оцінки продуктивності отриманих каналів та способи моніторингу за станом корпоративної мережі в режимі реального часу конкретного підприємства.

1 ПРЕДМЕТНА ОБЛАСТЬ І ПОСТАНОВКА ЗАДАЧІ

1.1 Основні відомості про корпоративні мережі

1.1.1 Організація зв’язку

Публічна мережа – це мережа, до якої може підключитися кожен. Найкращим і, мабуть, єдиним чистим прикладом такої мережі є Інтернет. Приватна мережа – це будь-яка мережа, доступ до якої обмежено. Прикладами приватних мереж є корпоративна мережа або мережа в школі.

Основна відмінність між загальнодоступними та приватними мережами, крім того факту, що доступ до приватної мережі жорстко контролюється, а доступ до загальнодоступної мережі – ні, полягає в тому, що адресацію пристроїв у загальнодоступній мережі слід уважно розглядати, тоді як адресацію на приватна мережа має трохи більше широти.

Як уже обговорювалося, для того, щоб хости в мережі могли спілкуватися за допомогою TCP/IP, вони повинні мати унікальні адреси. Це число визначає логічну мережу, до якої належить кожен хост, і адресу хоста в цій мережі. У приватній мережі з, скажімо, трьома логічними мережами і 100 вузлами в кожній мережі, адресація не є особливо складним завданням. Однак у мережі такого масштабу, як Інтернет, адресація дуже складна.

Безсумнівно, що корпоративна мережа, з усіма її наворотами, є дорожчою в налаштуванні в порівнянні з загальнодоступними мережами, для функціонування яких потрібні лише деякі точки доступу та належне підключення до Інтернету [1–6].

Корпоративна мережа дозволяє створити єдину для всіх підрозділів базу даних, вести електронний документообіг, організувати селекторні наради та проводити відеоконференції з віддаленими підрозділами, забезпечити всі потреби організації у високоякісному телефонному та факсимільному місцевому, міжнародному та міжміському зв’язку, доступі до Інтернету та інші інтерактивні мережі. Все це зменшує час реакції на зміни,

що відбуваються в компанії, та забезпечує оптимальне управління усіма процесами у реальному масштабі часу. При цьому знижується залежність організації від операторів фіксованого та мобільного зв'язку. Часткова відмова від послуг цих операторів дозволяє істотно скоротити витрати організації. З'являється можливість передавати будь-яку конфіденційну інформацію виробничого та фінансового характеру з упевненістю, що ніхто, крім уповноважених співробітників компанії, не має доступу до неї. Узагальнена схема корпоративної мережі представлена на рисунку 1.1.

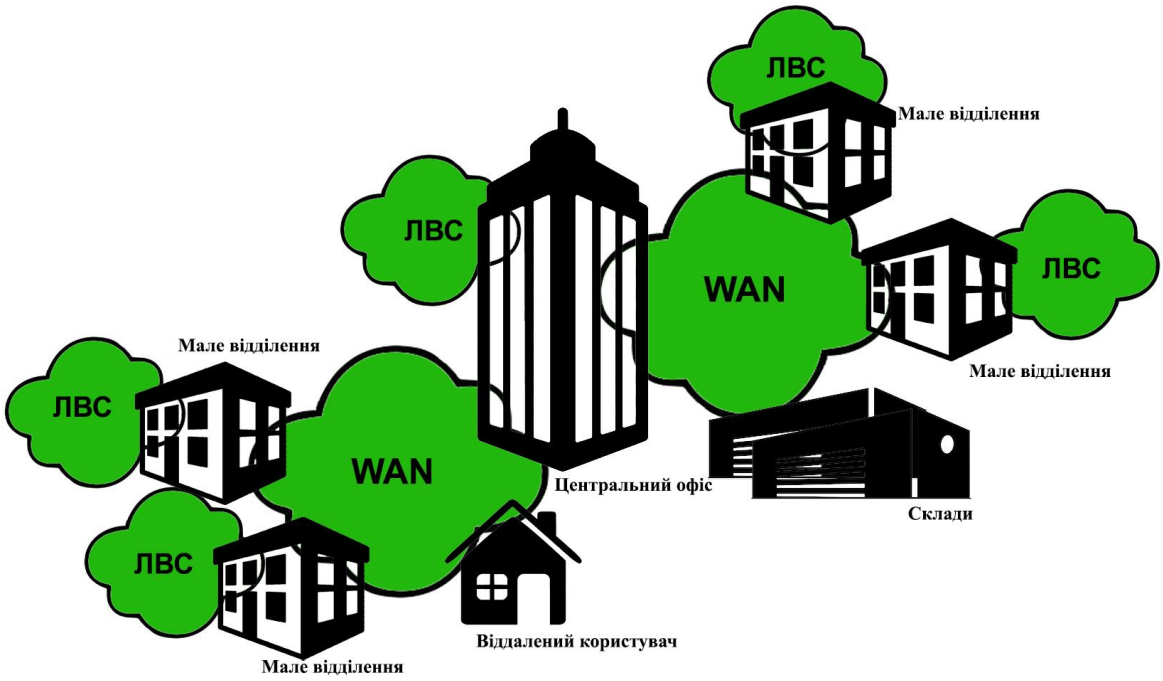

Рисунок 1.1 – Загальна схема корпоративної мережі

Основне завдання системних інтеграторів і адміністраторів полягає в тому, щоб ця громіздка і дуже дорога система якнайкраще справлялася з обробкою потоків інформації, що циркулюють між співробітниками підприємства і дозволяла приймати їм своєчасні та раціональні рішення, що забезпечують виживання підприємства у жорсткій конкурентній боротьбі. Оскільки життя не стоїть дома, те й зміст корпоративної інформації, інтенсивність її потоків і її обробки постійно змінюються. Транспорт

Інтернет – недорогий і доступний практично всім підприємствам – істотно полегшив завдання побудови територіальної корпоративної мережі, одночасно висунувши першому плані завдання захисту корпоративних даних під час передачі їх у надто загальнодоступну, публічну мережу з багатомільйонним «населенням».

1.1.2 Структура корпоративної мережі

На рисунку 1.2 представлено можливу схему структури корпоративної мережі.

Рисунок 1.2 – Приклад структури корпоративної мережі

Виділимо основні пристрої:

– комп’ютер. Під ним мається на увазі стандартне робоче місце, найчастіше підключене до локальної мережі через кабель типу кручена пара. На комп’ютері встановлено ПЗ, необхідне роботи персоналу (офісні додатки,

1С, поштові агенти тощо.), і навіть засоби віддаленого адміністрування даного комп’ютера;

– переносний пристрій. Це може бути ноутбук, планшет, мобільний пристрій. Найчастіше підключення таких пристроїв до мережі здійснюється за допомогою бездротового зв’язку. Несе ті ж функції, що й комп’ютер, але головна відмінність від стаціонарного комп’ютера – мобільність;

– реалізувати алгоритм знаходження ліній і кіл на базі методу Хафа на зображеннях, отриманих в результаті обробки їх фільтром Кенні;

– мережеве БФП. БФП – багатофункціональний пристрій, який виконує функції принтера, сканера, копіра. Підключення до мережі здійснюється через мережевий кабель. Якщо МФУ не має мережного порту, воно підключається до комп’ютера і за допомогою засобів операційної системи відкривається на доступ по мережі іншим користувачам;

– Wi-Fi точка доступу. Пристрій, за допомогою якого створюються бездротові мережі. Використовується для підключення ноутбуків та інших портативних пристроїв, які мають модуль Wi-Fi. Перевага перед кабельною системою полягає в мобільності та непотрібності протягувати кабель та псувати інтер’єр. Швидкість доступу в залежності від стандарту може бути від 50 до 125 мбіт/сек. Для захисту доступу до мережі є кілька стандартів безпеки: WEP, WPA, WPA2 і т.д.;

– IP-телефонія. Система зв’язку, що забезпечує передачу мовного сигналу через мережу Інтернет або будь-які інші IP-мережі. Сигнал по каналу зв’язку передається в цифровому вигляді і, як правило, перед передачею перетворюється (стискається) для видалення надмірності;

– комутатор. Пристрій, призначений для підключення кількох вузлів комп’ютерної мережі в межах одного або кількох сегментів мережі. Комутатор передає дані лише безпосередньо одержувачу, виняток становить широкомовний трафік (на MAC-адресу FF:FF:FF:FF:FF:FF) усім вузлам мережі. Це підвищує продуктивність і безпеку мережі, позбавляючи решту

сегментів мережі необхідності (і можливості) обробляти дані, які їм не призначалися;

– маршрутизатор. Мережевий пристрій, на підставі інформації про топологію мережі та певних правил, приймає рішення про пересилання пакетів мережевого рівня (рівень 3 моделі OSI) між різними сегментами мережі. Простіше кажучи, це пристрій, який пов’язує 2 і більше різних мереж (у нашому випадку це локальна мережа офісу та Інтернет);

– файловий сервер. Це виділений сервер, який оптимізований для виконання файлових операцій введення-виводу. Призначений для зберігання будь-яких файлів. Як правило, має великий обсяг дискового простору, і, як правило, файл-сервер обладнаний RAID контролером для забезпечення швидкого запису та читання даних;

– Web-сервер. Це сервер, який приймає HTTP-запити від клієнтів, зазвичай веббраузерів, і видає їм HTTP-відповіді, зазвичай разом з сторінкою HTML, зображенням, файлом, медіа-потоком або іншими даними. На ньому може бути розміщений корпоративний вебсайт або будь-який інший вебсервіс;

– сервер програм. Це програмна платформа, призначена для ефективного виконання процедур (програм, механічних операцій, скриптів), які підтримують побудову застосунків. Сервер програм діє як набір компонентів доступних розробнику програмного забезпечення через API (Інтерфейс прикладного програмування) визначений самою платформою;

– термінальний сервер (сервер терміналів). Сервер, що надає клієнтам обчислювальні ресурси (процесорний час, пам’ять, дисковий простір) на вирішення завдань. Технічно термінальний сервер є дуже потужним комп’ютером (або кластером), з’єднаним по мережі з термінальними клієнтами, які, як правило, являють собою малопотужні або застарілі робочі станції або спеціалізовані рішення для доступу до термінального сервера.

Термінал сервер служить для дистанційного обслуговування користувача з наданням робочого столу:

1) переваги термінального сервера;
2) зниження тимчасових витрат на адміністрування;
3) підвищення безпеки – зниження ризику зломів;
4) зниження витрат на програмне та апаратне забезпечення;

– сервер БД. Сервер БД обслуговує базу даних та відповідає за цілісність та збереження даних, а також забезпечує операції введення-виводу при доступі клієнта до інформації. Більшість СУБД використовують мову SQL (Structured Query Language – мову структурованих запитів), оскільки вона зручна для опису логічних підмножин БД.

1.2 Віртуальні приватні мережі

1.2.1 Організація VPN

VPN розширює приватну мережу через загальнодоступну мережу, наприклад Інтернет. Це дає змогу користувачам надсилати та отримувати дані через спільні або загальнодоступні мережі, як якщо б їхні комп’ютерні пристрої були безпосередньо під’єднані до приватної мережі, і таким чином отримують переваги від функціональності, безпеки та політики керування приватною мережею. VPN створюється шляхом встановлення віртуального з’єднання «точка-точка» за допомогою використання виділених з’єднань, віртуальних протоколів тунелювання або шифрування трафіку.

VPN, що охоплює Інтернет, схожа на глобальну мережу (WAN). З точки зору користувача, доступ до розширених мережевих ресурсів здійснюється так само, як і до ресурсів, доступних у приватній мережі. Традиційні VPN характеризуються топологією «точка-точка», і вони не мають тенденції підтримувати або підключати широкомовні домени. Тому зв’язок, програмне забезпечення та мережа, які базуються на рівні 2 OSI і

широкомовних пакетах, таких як NetBIOS, що використовуються в мережах Windows, можуть не повністю підтримуватися або працювати не так, як у локальній мережі (LAN).

VPN безпечно з'єднують територіально відокремлені офіси організації, створюючи єдину цілісну мережу. Технологія VPN також використовується окремими користувачами Інтернету для захисту своїх бездротових транзакцій, для обходу географічних обмежень і цензури, а також для підключення до проксі-серверів з метою захисту особистої особи та місцезнаходження. VPN – це технологія безпеки, яка найбільше підходить для підключень окремих користувачів, а не безпечних підключень низки вбудованих пристроїв [3, 6-14].

Розглянемо варіант організації мережі установи з філіями з використанням віртуальних приватних мереж на рисунку 1.3.

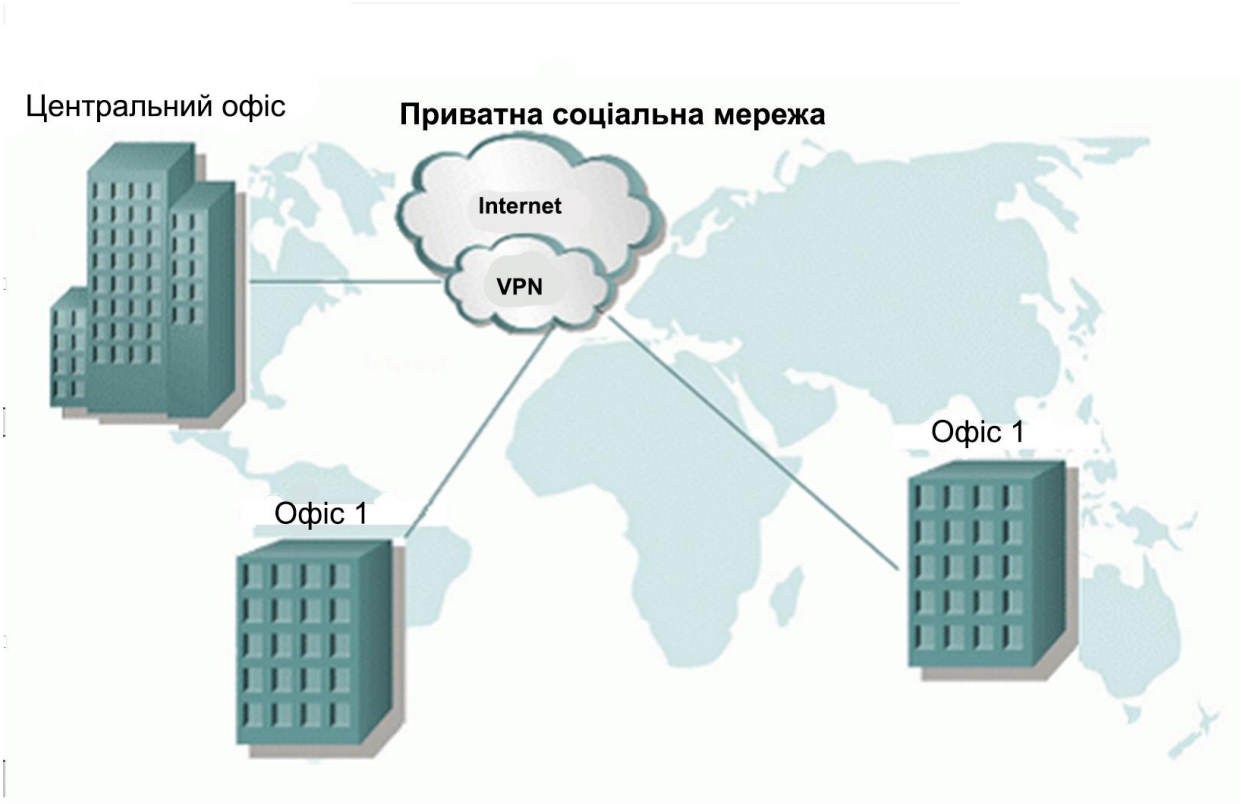

Рисунок 1.3 – Організація мережі установ з філіями з використанням VPN

Особливості такої організації:

У вигляді спеціального програмно-апаратного забезпечення – це реалізація VPN мережі здійснюється за допомогою спеціального комплексу програмно-апаратних засобів. Така реалізація забезпечує високу продуктивність і, як правило, високий рівень захищеності.

У вигляді програмного рішення – це використовують персональний комп'ютер із спеціальним програмним забезпеченням, що забезпечує функціональність VPN.

Інтегроване рішення – це функціональність VPN яку забезпечує комплекс, що вирішує також завдання фільтрації мережного трафіку, організації мережевого екрана та забезпечення якості обслуговування [15].

Способи організації VPN найбільш доцільно виділити такі три основні способи:

– віддалений доступ окремо взятих співробітників до корпоративної мережі організації через модем або загальнодоступну мережу;

– зв'язок у одну загальну мережу територіально розподілених філій фірми. Цей спосіб називається Intranet VPN;

– Client/Server VPN. Він забезпечує захист даних між двома вузлами (не мережами) корпоративної мережі.

1.2.2 SSH

SSH, або Secure Shell Protocol – це протокол віддаленого адміністрування, який дозволяє користувачам отримувати доступ, контролювати та змінювати свої віддалені сервери через Інтернет.

Служба SSH була створена як безпечна заміна незашифрованого Telnet і використовує криптографічні методи для забезпечення того, щоб усі зв'язки з віддаленим сервером відбувалися у зашифрованому вигляді. Він забезпечує

механізм для аутентифікації віддаленого користувача, передачі вхідних даних від клієнта до хосту та передачі результату назад клієнту.

Наведений нижче приклад показує типову підказку SSH. Будь-який користувач Linux або macOS може SSH на свій віддалений сервер безпосередньо з вікна терміналу.

Команда ключа SSH повідомляє вашій системі, що ви хочете відкрити зашифроване з'єднання Secure Shell. «user» представляє обліковий запис, до якого потрібно отримати доступ. Наприклад, ви можете отримати доступ до користувача root, який в основному є синонімом системного адміністратора з повними правами змінювати будь-що в системі. «hos» означає комп'ютер, до якого потрібно отримати доступ. Це може бути IP-адреса (наприклад, 244.235.23.19) або доменне ім'я (наприклад, www.xyzdomain.com).

Принцип роботи SSH полягає в тому, що використовується модель клієнт-сервер для автентифікації двох віддалених систем і шифрування даних, які передаються між ними.

SSH за замовчуванням працює на порту TCP 22 (хоча це можна змінити, якщо потрібно). Хост (сервер) прослуховує порт 22 (або будь-який інший призначений порт SSH) для вхідних підключень. Він організовує безпечне з'єднання, автентифікуючи клієнта та відкриваючи правильне середовище оболонки, якщо перевірка пройшла успішно.

Останнім етапом перед тим, як користувач отримує доступ до сервера, є аутентифікація його/її облікових даних. Для цього більшість користувачів SSH використовують пароль. Користувача просять ввести ім'я користувача, а потім пароль. Ці облікові дані безпечно проходять через симетрично зашифрований тунель, тому немає шансів, що вони будуть захоплені третьою стороною.

Це набір асиметричних ключів, які використовуються для автентифікації користувача без необхідності введення пароля [16-20].

1.3 Моніторинг корпоративних мереж

Для підвищення надійності роботи корпоративної мережі необхідно вирішити питання її моніторингу.

Терміном моніторингу мережі називають роботу системи, яка виконує постійне спостереження за комп'ютерною мережею у пошуках повільних або несправних систем та яка при виявленні збоїв повідомляє про них мережному адміністратору за допомогою пошти, пейджера або інших засобів сповіщення. Ці завдання є підмножиною завдань управління мережею.

У той час як система виявлення вторгнень стежить за появою загроз ззовні, система моніторингу мережі виконує спостереження за мережею в пошуках проблем, викликаних перевантаженими та/або серверами, іншими пристроями або мережевими з'єднаннями, що відмовили.

Наприклад, щоб визначити стан вебсервера, програма, яка виконує моніторинг, може періодично надсилати запит HTTP на отримання сторінки; для поштових серверів можна надіслати тестове повідомлення SMTP і отримати IMAP або POP3.

Невдалі запити (наприклад, коли з'єднання не може бути встановлено, воно завершується по тайм-ауту, або коли повідомлення не було доставлено) зазвичай викликають реакцію з боку системи моніторингу. Як реакція може бути:

– надіслано сигнал тривоги системному адміністратору;

– автоматично активована система захисту від збоїв, яка тимчасово виведе проблемний сервер з експлуатації, замінивши його резервним, доки проблема не буде вирішена.

Крім відмов систем, процесів, обладнання також стежать і за їх станом в цілому.

Знаючи, який потік інформації проходить через мережевий інтерфейс, можна буде вибрати оптимальний пакет Інтернету у постачальника, заощадивши не менші гроші. Зараз це досить актуальна проблема, оскільки

часто у бізнес-центрах існує домовленість із провайдером про те, що вони мають право давати доступ в Інтернет. Відтак і цінова політика повністю встановлюється провайдером. Ціни абсолютно непорівнянні з тими, що встановлюються у процесі жорсткої конкуренції.

За графіками навантаження на процесор, обсягу займаної оперативної пам’яті, можна будувати висновки про достатності ресурсів сервера для завдань, виконуваних у ньому. Це дає обґрунтування для оновлення сервера.

Практично у всіх фірмах є великі обсяги інформації, які включають важливі документи, бази даних, архіви і т.д. Втрата цих документів завдасть фірмі великих збитків. Щоб завжди мати резервну копію цих файлів, налаштовуються плани резервного копіювання даних. Створюються образи даних та складаються на файл-сервері. За вільним місцем на файл-сервері та за створенням образів теж необхідно налаштовувати стеження.

Спостереження найчастіше проводиться за станом серверів, маршрутизаторів та іншого мережного обладнання. Грамотно налаштована система моніторингу може знизити кількість відмов мережі і збільшити її відмовостійкість. У той же час, адміністратори мережі будуть швидко та вчасно оповіщені про неполадки.

Єдиним недоліком таких систем є складність створення та налаштування. Існує безліч готових комплексних рішень, але не завжди з тих чи інших причин вони підходять під налагоджену і налагоджену корпоративну мережу. Тому доводиться вибирати та комбінувати ці системи для досягнення бажаного результату.

1.4 Постановка задачі

Одне з основних вимог, що висуваються до постановки та реалізації проектування, полягає в тому, що всі результати та на їх основі висновки мають бути отримані у реальних умовах на реальному підприємстві. Це дає

можливість надати результатам роботи практичної значущості. Провівши роботу в реальних умовах, можна реально оцінити ефективність використовуваних мережевих технологій на основі кількісної оцінки продуктивності мережевих каналів.

Коротко опишемо предметну область. Фірма займається продажем саун, лазень і супутніх матеріалів. Складається з офісу, складу та магазинів, територіально рознесених по всьому місту. Усі сервери розташовані у провайдера (коллокація), а саме: сервери терміналів, сервер платформи 1С, сервер бази даних MS SQL та маршрутизатор під керуванням операційної системи CentOs 5.5 з ланцюжками NAT у правилах iPtables.

В основному робота персоналу відбувається на серверах терміналів, що забезпечує деяку централізованість, простоту адміністрування (завжди легше адмініструвати 3 сервери ніж 50 комп'ютерів) і, за рахунок налаштувань iPtables на маршрутизаторі, безпека. Підключення йде за протоколом RDP (Remote Desctop Protokol). Також для роботи постійно потрібен обмін інформацією між офісами. Підприємство працює з конфіденційною інформацією, тому важлива безпека передачі даних. Магазини працюю лише з серверами, що знаходяться у провайдера.

В офісі та на складі як маршрутизатор виступає сервер під операційною системою Centos 5.5 з налаштованими ланцюжками nat в iptables. У магазинах стоять стандартні hardware маршрутизатори. На сервері терміналів, 1С сервер, сервер MS SQL 2008 встановлено операційну систему MS Windows 2003 R2.

Об'єктом роботи є захищена корпоративна система.

Метою роботи є аналіз даних, що базуються на використанні різних технологіях та їх порівняння.

Для досягнення мети необхідно споживчі властивості які функціонують в умовах реальних обмежень, тому необхідно вирішити наступні завдання:

– створити захищену корпоративну мережу для підприємства;

– підключити захищеними каналами магазини до серверів;

– оцінити продуктивність створених каналів;

– створити систему моніторингу та оповіщення про проблеми з обладнанням корпоративної мережі.

Подамо структуру проектованої корпоративної мережі підприємства у вигляді, як показано на рисунку 1.4.

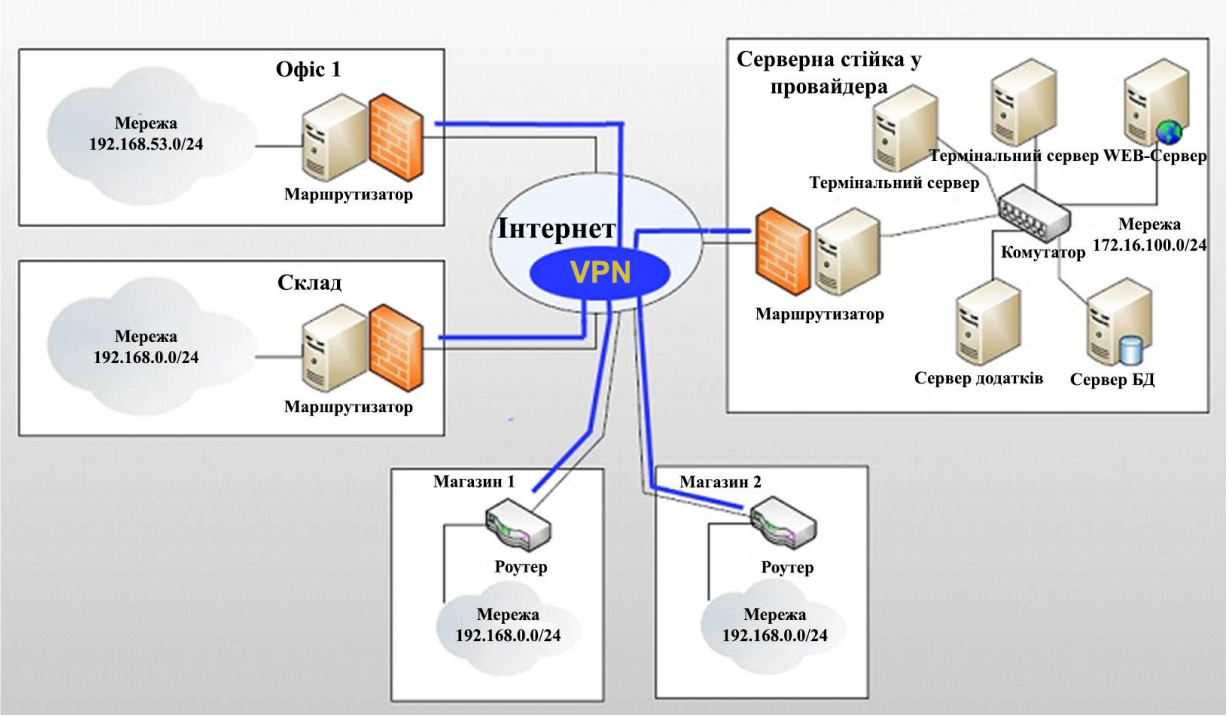

Рисунок 1.4 – Проект корпоративної мережі

2 ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ VPN У КОРПОРАТИВНУ МЕРЕЖУ І ЇХ ПОРІВНЯЛЬНА ОЦІНКА

2.1 Реалізація на основі технології OpenVPN

Спочатку об’єднаємо в одну корпоративну мережу офіс, склад та наші сервери у провайдера. Для цього нам потрібно побудувати захищені канали – тунелі лише між маршрутизаторами, тому що немає потреби підключати кожен комп’ютер окремо.

Отже є 3 маршрутизатори під керуванням ОС CentOs. Перекидання пакетів з Інтернету в мережу і назад здійснюється за допомогою технології NAT та правил iptables.

Дамо для зручності маршрутизаторам імена:

– в офісі: Office;

– на складі: Sklad.

Колокація (сервера у провайдера) – це Colo. Для магазинів mag1 та mag2 відповідною.

Мережеві налаштування показані у таблицях 2.1 – 2.3.

Таблиця 2.1 – Мережеві налаштування Office

Мережа	Інтерфейс	Ip адреса	Маска	Шлюз
Інтернет	eth2	213.182.175.230	255.255.255.252	213.182.175.229
Локальна	eth1	192.168.53.250	255.255.255.0	–

Таблиця 2.2 – Мережеві налаштування Sklad

Мережа	Інтерфейс	Ip адреса	Маска	Шлюз
Інтернет	eth2	79.142.87.206	255.255.255.252	79.142.87.211
Локальна	eth1	192.168.0.1	255.255.255.0	–

Таблиця 2.3 – Мережеві налаштування Colo

Мережа	Інтерфейс	Ip адреса	Маска	Шлюз
Інтернет	eth2	195.2.240.68	255.255.255.252	195.2.240.60
Локальна	eth1	172.16.100.8	255.255.255.0	–

Налаштування hardware маршрутизаторів у магазинах не відіграють ролі, тому їх пропустимо.

Налаштуємо першим маршрутизатор Colo. Цей маршрутизатор виступатиме в ролі OpenVPN сервера. Пакет OpenVPN недоступний у стандартному репозиторії, тому підключаємо додатковий репозиторій rpmforge.

Тепер став доступний пакет OpenVPN, встановлюємо його.

OpenVPN встановлено. Далі потрібно згенерувати кореневий сертифікат сервера, сертифікати та ключі клієнтів, сертифікат та ключ сервера, tls ключ. Для цього переходимо до конфігураційного каталогу OpenVPN і створюємо каталог під наші майбутні ключі та каталог під конфігураційні файли клієнтів.

Далі завантажуємо змінні для генерації ключів на згадку і починаємо генерувати сертифікат авторизації.

Створюємо сертифікат X.509 для сервера.

Далі з’явиться питання про підписання сертифікату, погоджуємось. Створюємо ключ для office та ключ для tls-автентифікації.

Після всіх цих маніпуляцій у каталозі keys/ з’являються такі файли:

– ca.crt – головний CA сертифікат, цей файл потрібний і клієнту та серверу;

– dh1024.pem – ключ Діффі Хельман, цей файл потрібен лише серверу;

– server.crt – сертифікат сервера, потрібен лише серверу;

– server.key – ключ сервера, потрібен лише серверу (секретний файл);

– office.crt, sklad.crt, mag1.crt, mag2.crt – сертифікати клієнтів, потрібні лише відповідним клієнтам;

– office.key, sklad.key, mag1.key, mag2.key – ключі клієнтів потрібні лише відповідним клієнтам (секретні файли);

– ta.key – TLS-ключ, потрібен і клієнтам та серверу.

Отже, на сервері залишаються файли ca.crt, dh1024.pem, server.crt, server.key, ta.key, а клієнтам віддаються ca.crt, dh1024.pem та їх ключі із сертифікатами.

На цьому операції з генерацією ключів та сертифікатів закінчені, далі переходимо до налаштуваннясервера та клієнтів. Створюємо файл конфігурації server.conf.

Створюємо файли з налаштуваннями для клієнтів. У каталозі /etc/openvpn/ccd на сервері створюємо файл office, sklad, mag1, mag2 (ім’я файлу – ім’я якому видано сертифікат).

Цими налаштуваннями видали клієнтам з відповідними сертифікатами віртуальні ip адреси, шлюз 10.10.200.1 та задали маршрут через тунель до мережі за клієнтами. Для магазинів маршрут не ставимо, тому що в наше завдання не входить підключення цих мереж.

На цьому налаштування сервера закінчується, запускаємо OpenVPN.

Якщо все правильно, то має з’явитись віртуальний tun пристрій.

Якщо пристрій не з’явився, це означає, що в конфігураційних файлах є помилки. Дивимося балку і усуваємо помилку, далі знову стартуємо.

Переходимо до налаштуванняклієнтів. Всі файли конфігурації однакові, тому розглянемо один з них. На маршрутизаторах office і sklad встановлюємо OpenVPN, як і для сервера. Далі створимо конфігураційний файл client.conf.

Далі створимо скрипт openvpn_up.sh для автоматичного додавання маршруту.

На цьому налаштування OpenVPN закінчено. Копіюємо ці файли на office та sklad. Далі запускаємо OpenVPN. Якщо не запустився, дивимось логи.

Але на цьому не все. Тепер нам треба включити трансляцію адрес (NAT) щоб пакети від клієнтської машини, потрапляючи на сервер, могли піти в Інтернет і відповідно поверталися назад.

Тепер 3 мережі «бачать» один одного. Налаштуємо підключення з магазинів до серверів. На комп'ютерах у магазинах стоїть операційна система Windows XP. Завантажуємо з офіційного сайту дистрибутив OpenVPN та встановлюємо. Потім у встановленому каталозі у папку config кладемо наші ключі та конфігураційний файл mag1. Після цього можна запускати.

На цьому етапи налаштування завершено. Маючи захищену корпоративну мережу, можна підключатись безпосередньо до серверів. Перевірити шифрацію можна, прослухавши трафік на одному з роутерів командою TCPDUMP [11-13].

2.2 Реалізація на основі технології SSH

Реалізуємо ту ж схему корпоративної мережі, яку створювали за допомогою пакету OpenVPN, але вже за допомогою вбудованого в linux системи пакета OpenSSH. Нам вистачить розглянути з'єднання 2-х мереж, так як для підключення ще однієї мережі потрібно буде провести ті самі дії.

З версії 4.3 OpenSSH підтримує пристрої tun/tap, що дозволяють створювати шифрований тунель. Це дуже схоже на OpenVPN, заснований на TLS.

Шифрований тунель створюється на основі одного TCP з'єднання, що дуже зручно, для швидкого підняття простого VPN, на IP.

Спочатку потрібно дописати в конфігураційний файл OpenSSH рядки, що він має право створювати пристрої tun/tap та заходити з правами root.

У нас є дві мережі, мережа office з адресою 192.168.53.0/24 та мережа colo з адресою 172.16.100.0/24. Для створення захищеної VPN мережі потрібно зробити наступні дії:

– підключиться з одного маршрутизатора через SSH на інший із опцією -*w*;

– налаштування IP адреси SSH тунелю робиться один раз на сервері та на клієнті;

– додати маршрут для обох мереж;

– якщо потрібно, увімкніть NAT на внутрішньому інтерфейсі шлюзу.

Підключатимемося з мережі office до мережі colo. З'єднання починається з маршрутизатора office, а команди виконуються на маршрутизаторі мережі colo, тобто налаштовуємо маршрутизатор colo:

За допомогою опції -*w* с параметрами 0:0 кажемо, що при підключенні створити на клієнті та сервері віртуальні пристрої tun0. Параметр –*c* включає шифрацію, параметр –*C* стиск трафіку.

Далі виконуємо команди на маршрутизаторі мережі colo:

– задаємо ip адресу та маску підмережі;

– додаємо маршрут до мережі office;

– вмикаємо NAT, якщо не увімкнено;

– прописуємо правило за допомогою засобів iptables для перекидання пакетів з мережі VPN в реальну.

Далі налаштуємо машрутизатор office.

На цьому налаштування закінчено, мережа VPN побудована. Для підключення окремих комп'ютерів з операційною системою Windows XP (магазини) використовується клієнт SSH Putty.

2.3 Оцінка продуктивності каналів корпоративної мережі

У розділах 2.1 та 2.2 розглянуто дві технології (OpenVPN, SSH) створення захищених корпоративних мереж, використовуючи VPN. На сьогоднішній день технологія OpenVPN лідирує на ринку побудови захищених мереж, тоді як тунелювання за допомогою SSH тільки починає входити до повсякденності. Для того щоб зрозуміти яку технологію необхідно застосувати в реальних умовах за конкретних вимог, що пред'являються корпоративної мережі, потрібно оцінити їхню продуктивність і обґрунтувати їх переваги та недоліки.

Почати слід із продуктивності захищених каналів. На рисунку 1.4 представлена побудована корпоративна мережа, продуктивність захищених каналів якої, використовуючи програму iPerf, необхідно оцінити. За допомогою клієнтської частини генерується трафік та відправляється на серверну частину. При отриманні даних генерується звіт швидкості передачі даних [16-20].

2.3.1 Оцінка продуктивності використання технології OpenVPN

Для побудови графіків продуктивності каналу створеного за допомогою OpenVPN використовуватимемо дані, отримані при тестуванні з додатка А.

На рисунку 2.1 наведено графіки значень RTT. З них видно, що різниця між каналом без VPN і каналом з використанням VPN не є суттєвою. Також включення опції стиснення не впливає на час відгуку.

На рисунку 2.2 представлені графіки пропускної спроможності каналу, з яких можна зробити такі висновки.

При використанні створеного каналу VPN із шифрацією за допомогою ключа AES-256-CBC втрата у продуктивності 0,5 мбіт/сек, що склало 5,1% від каналу без використання VPN.

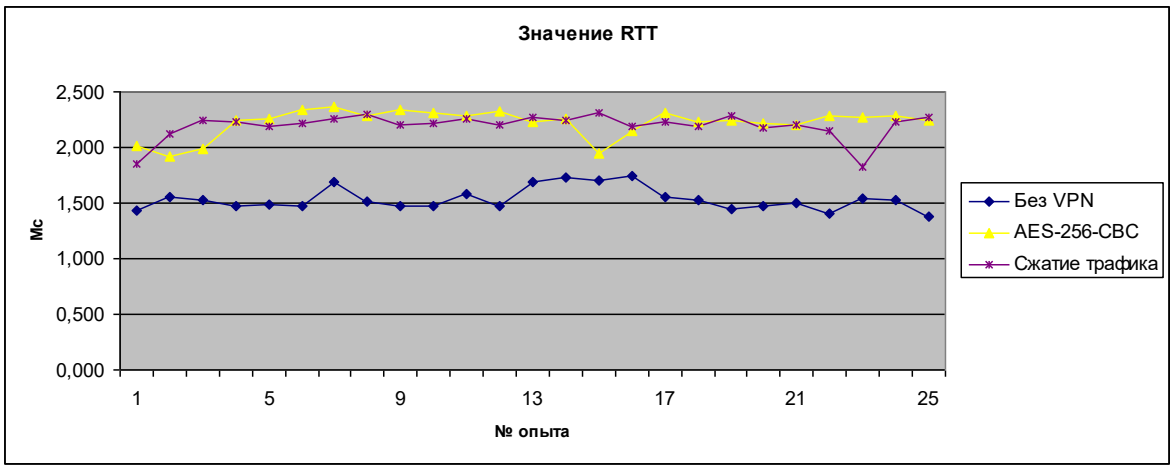

Рисунок 2.1 – Графіки значень RTT

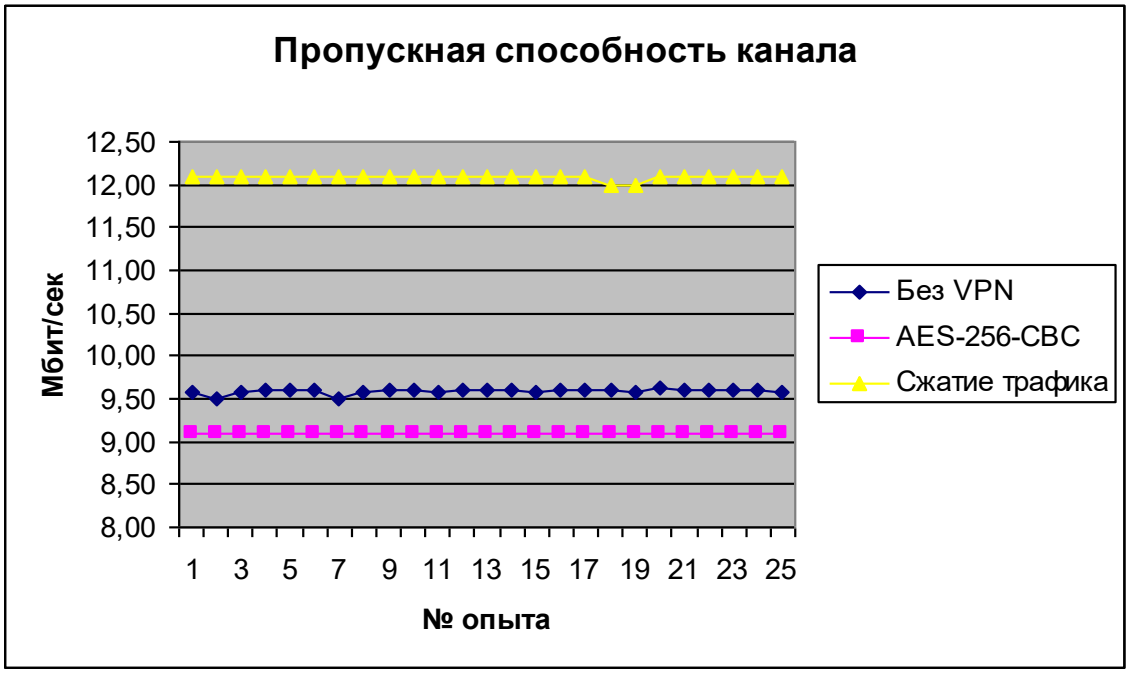

Рисунок 2.2 – Графіки пропускної спроможності каналу

При включенні стиснення шифрованого трафіку спостерігаємо приріст швидкості 3 мбіт/сек, що становить 32,9%.

На рисунку 2.3 представлені графіки завантаження ЦП на маршрутизаторах при використанні OpenVPN із шифрацією трафіку, при включеному та відключеному стисканні.

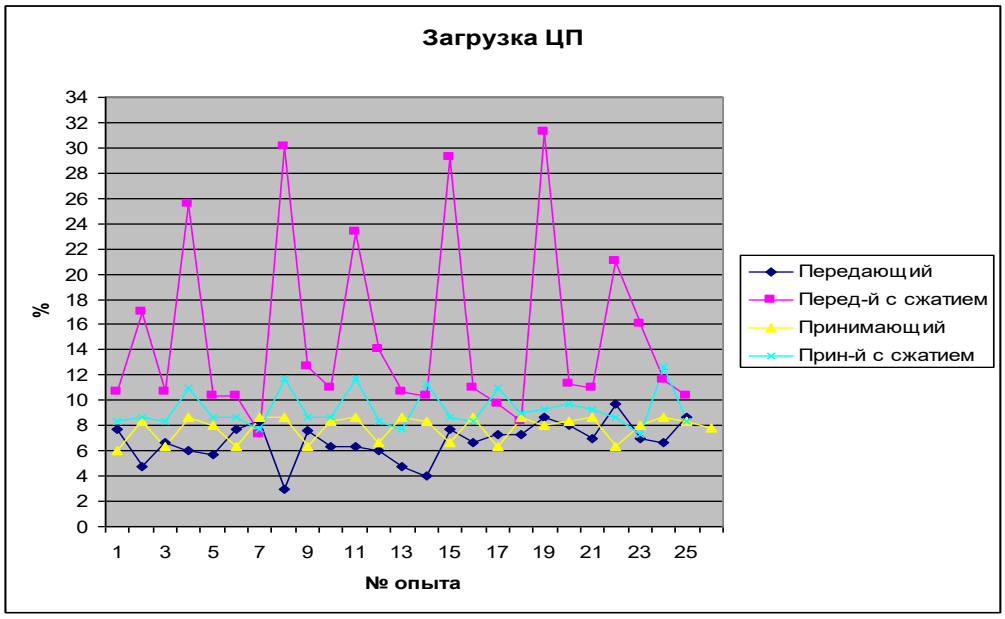

Рисунок 2.3 – Графіки завантаження ЦП

За середніми значеннями завантаження, як і належало, найвище навантаження дає шифрація трафіку з використанням стиснення – 14,992%.

На основі отриманих графіків, здійснимо оцінку продуктивності каналів VPN, побудованих за допомогою OpenVPN.

Критерій «Завантаження ЦП» при отриманих значеннях є несуттєвим, оскільки це маршрутизатор та інших процесів, що потребують великого споживання ЦП, немає.

Критерій «RTT» також є несуттєвим, оскільки різниця від часу відгуку при дослідах без VPN виявилася найменше на 0,5 мс.

На графіках пропускної спроможності каналів можна спостерігати падіння швидкості використання коштів VPN на 0,5 мбіт/сек у середньому. В даний час це не є суттєвим, так як Інтернет-провайдери надають свої послуги на великих швидкостях, де таке падіння не відіграватиме великої ролі.

При використанні стиснення трафіку видно помітний приріст пропускної спроможності каналу, на 3 мбіт/сек. Звичайно, при цьому сильно зростає завантаження на ЦП, але як говорилося раніше, це не відіграє великої ролі.

Підведемо підсумки. Створюючи захищену корпоративну мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифрацією даних, що передаються, і приростом швидкості за рахунок стиснення трафіку зі зручністю обміну інформацією. Технологія OpenVPN повністю виправдовує себе. Її використання веде до зростання продуктивності роботи з інформацією через мережу. З мінусів виділяється деяка складність налаштування та створення VPN мережі. З плюсів – кросплатформність.

2.3.2 Оцінка продуктивності використання технології SSH

Для побудови графіків продуктивності каналу створеного за допомогою SSH використовуватимемо дані, отримані при тестуванні з додатка А.

На рисунку 2.4 представлені графіки, якими можна будувати висновки про час відгуку під час роботи ssh. У середньому час збільшився на 0,8 мс. Це значення не є критичним навіть для найвибагливіших програм.

На рисунку 2.5 представлені графіки пропускної спроможності каналу. Результати вийшли приблизно такими, що і при використанні OpenVPN.

На рисунку 2.6 представлені графіки завантаження ЦП при використанні ssh із шифрацією зі стисненням трафіку та без. При включенні шифрації видно великий стрибок навантаження на ЦП. Середнє значення – 37,9%. Це досить багато, але не є критичним.

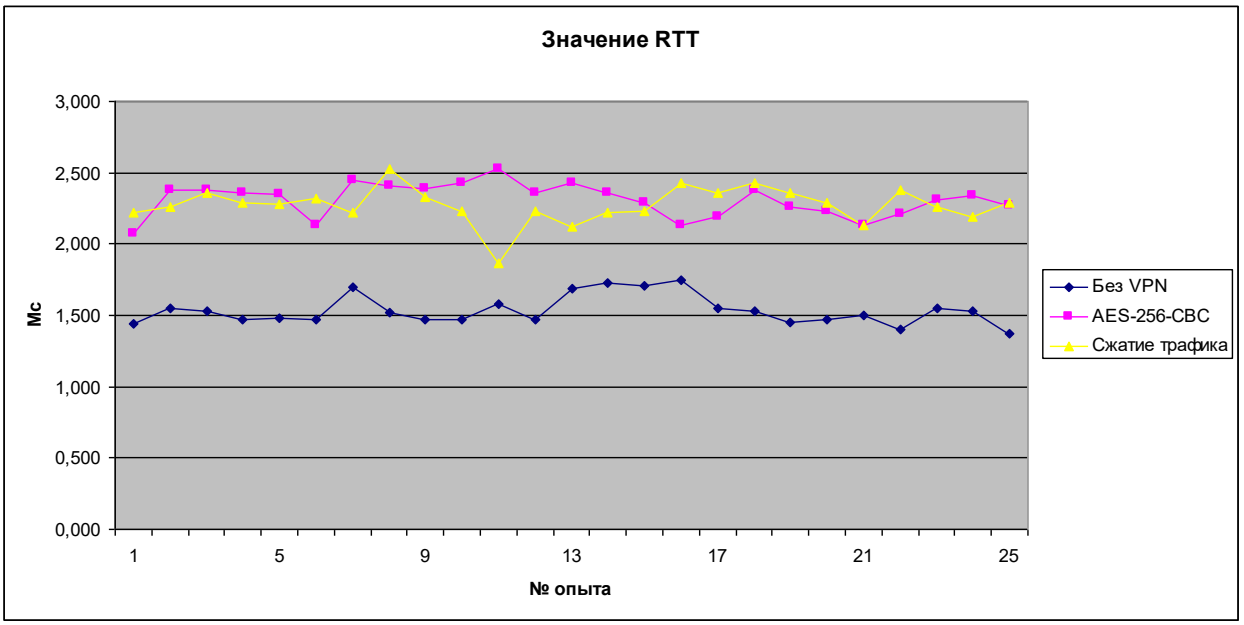

Рисунок 2.4 – Графіки значень RTT

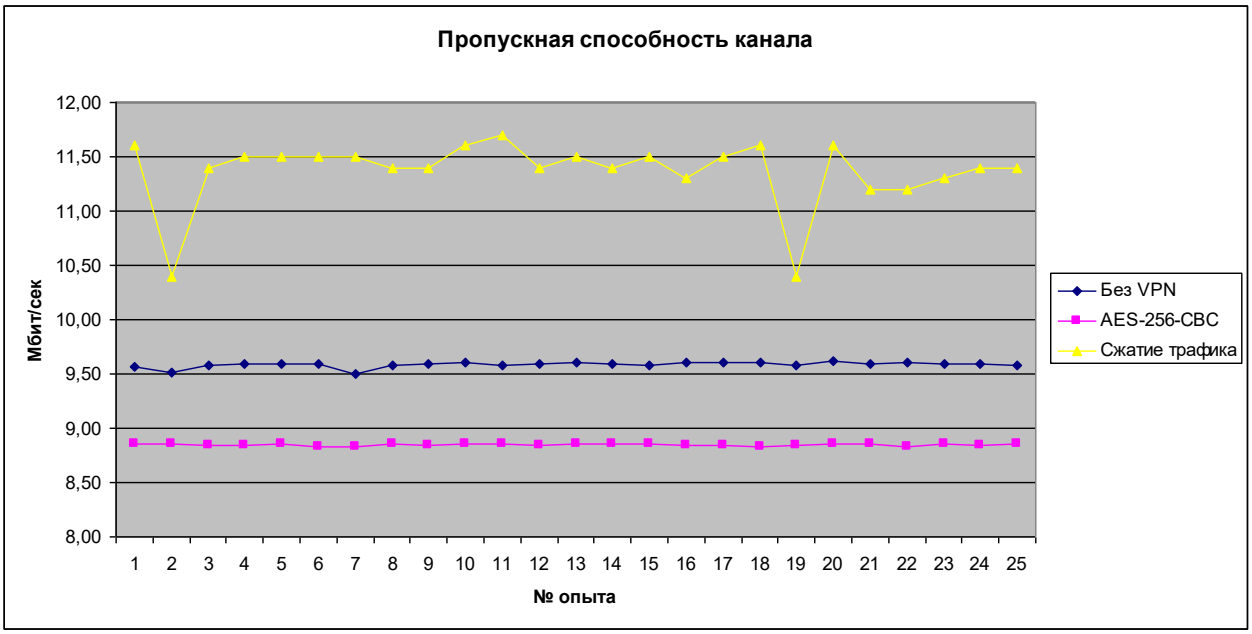

Рисунок 2.5 – Графіки пропускної спроможності каналу

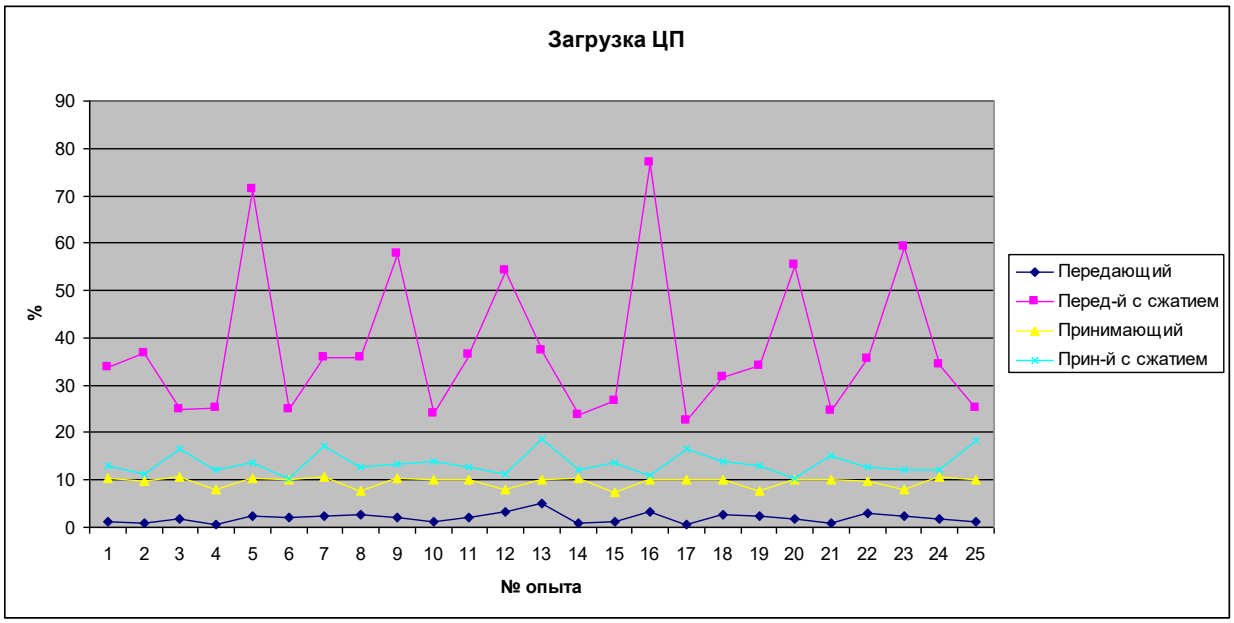

Рисунок 2.6 – Графіки завантаження ЦП

З отриманих даних можна зробити такий висновок: продуктивність при використанні стиснення трафіку зросла приблизно на 25%, але при цьому значно збільшилося навантаження на ЦП. З переваг цієї технології хочеться виділити можливість створення ssh-тунелів по окремих портах, що за певних умов дає безліч плюсів, наприклад, можливість мати автоматичне включення резервного каналу, за відсутності зв'язку на одному з маршрутизаторів. Також потрібно відзначити простоту створення та налаштування VPN мережі, кросплатформеність, висока надійність, легка масштабованість.

2.3.3 Вибір між технологіями SSH та OpenVPN

Порівняння технологій SHH та OpenVPN ґрунтуючись на отриманих дослідним шляхом даних показано у таблиці 2.4.

Таблиця 2.4 – Порівняльна таблиця

	OpenVPN	SSH
Складність створення	Досить складне настроювання. Складність налаштування маршрутизації для кількох мереж, можливі проблеми з firewall.	Легке налаштування, що не потребує особливих знань. На все виробництво йде не більше 10 хвилин.
Масштабованість	Підключення ще однієї мережі або клієнта, тягне за собою зміну конфігураційних файлів на сервері і додавання їх на клієнта. За рахунок OpenVPN клієнта під Windows має перевагу перед SSH. Не потребує навчання персоналу.	Для підключення ще однієї мережі потрібно повторити ті ж дії, що й під час об’єднання попередніх. Для підключення Windows комп’ютерів потрібно одноразове навчання персоналу.
Продуктивність	Стиснення йде вибірково, тобто. що стиснути не можна – пропускається. Це зменшує навантаження на ЦП.	Продуктивність трохи нижча, ніж OpenVPN. Стискається весь трафік – великі навантаження на ЦП.
Завантаження ЦП	В середньому не більше ніж 15%	В середньому не більше ніж 38%
Кросплатформеність	Так	Так

Продовження таблиці 2.4

	OpenVPN	SSH
RTT	На 0,5 мс більше, ніж у вихідної сполуки	На 0,8 мс більше, ніж у вихідної сполуки
Документація	Маса документації на офіційному сайті. Численні форуми та обговорення.	Документація є у вбудованому довіднику. Інформації з налаштування поки що мало.
Дод. можливості	–	Створення ssh-тунелів.
Використання в сущ. мережа	Можуть бути проблеми з налаштуванням firewall'а.	Легке використання.
Захищеність	Шифрація 256 бітним ключем AES	Шифрація 256 бітним ключем AES
Поширеність	Лідируюча технологія створення VPN мереж.	Сам протокол ssh існує дуже давно, але створення ssh VPN мереж на сьогоднішній день зустрічається рідко.

Розглянувши всі плюси та мінуси, кращим рішенням буде використання обох технологій разом. Від SSH взяти SSH-тунелі, а від OpenVPN створення VPN мереж.

3 СТВОРЕННЯ КОМПЛЕКСУ СИСТЕМ МОНІТОРИНГУ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Спостереження за станом серверів та мережевого обладнання. Nagios

Nagios – гнучка система моніторингу роботи серверів. Здебільшого її використовують для моніторингу великої кількості серверів. Nagios – це програма моніторингу комп'ютерних систем та мереж з відкритим кодом. Призначена для спостереження, контролю стану обчислювальних вузлів та служб, що сповіщає адміністратора у тому випадку, якщо якісь із служб припиняють або відновлюють свою роботу. У нашому випадку, слідкуватимемо за маршрутизаторами, серверами та процесами, запущеними на них. Систему Nagios для зручності налаштування поставимо на маршрутизатор colo [19-24].

Nagios включає засоби стеження, а також web-інтерфейс для управління і перегляду поточного стану серверів. Тому, крім установки самої системи, потрібно встановити web-сервер. Почнемо з встановлення необхідних компонентів:

– встановлюємо компілятор мови C, його бібліотеки та графічні інструменти;

– встановлюємо вебсервер Apache;

– створюємо користувача та групу з правами яких працюватиме nagios;

– створюємо пароль для користувача;

– додаємо nagios та apache в одну групу, щоб не було проблем із правами на запуск скриптів на web-сервері;

– ставимо систему та завантажуємо останню версію системи та модулі до неї;

– розпаковуємо завантажений архів і переходимо в каталог;

– конфігуруємо інсталяційний пакет та перевіряємо задоволення залежностей;

– якщо все добре, пройшло без помилок, збираємо пакет та встановлюємо;

– прописуємо налаштування в Apache;

– виконуємо ті ж дії для додаткових модулів;

– ставимо пароль на вхід до web-інтерфейсу за допомогою утиліти htpasswd;

– перевіряємо правильність конфігураційного файлу;

– якщо помилок та попереджень немає, запускаємо Nagios та Apache.

Перевірити, що система запрацювала, можна зайшовши на web-інтерфейс за адресою «http://ip.адрес.сервера/nagios». У нашому випадку ip-адреса – це «195.2.240.68». Якщо сервер Apache запущений і сайт системи nagios в файл конфігурації прописаний правильно, то повинні побачити сторінку авторизації. Після введення зв’язки логін-пароль відкриється сторінка вітання Nagios. Якщо з якоїсь причини цього не сталося, дивимося помилки у логах apache у каталозі «/var/log/httpd».

Розглянемо навігаційне меню:

– Home – сторінка привітання. Можна дізнатися про можливі оновлення системи;

– Documentation – велика кількість документації щодо налаштування системи;

– Tactical Overview – являє собою збирання короткої інформації про об’єкти, за якими ведеться моніторинг;

– Map – відображає карту мережі, позначаючи зеленим кольором працюючі сервери та червоним відключені на рисунку 3.1;

– Hosts – воказує стан кожного об’єкта, що спостерігається, окремо;

– Services – показує стан запущених процесів на серверах, а також RTT, кількість вільного місця, завантаження процесора та пам’яті на рисунку 3.2;

– Event log – звіти системи моніторингу.

Всі інші пункти меню є різновидами перерахованих вище, додаючи зручності перегляду інформації, наприклад розбита за групами.

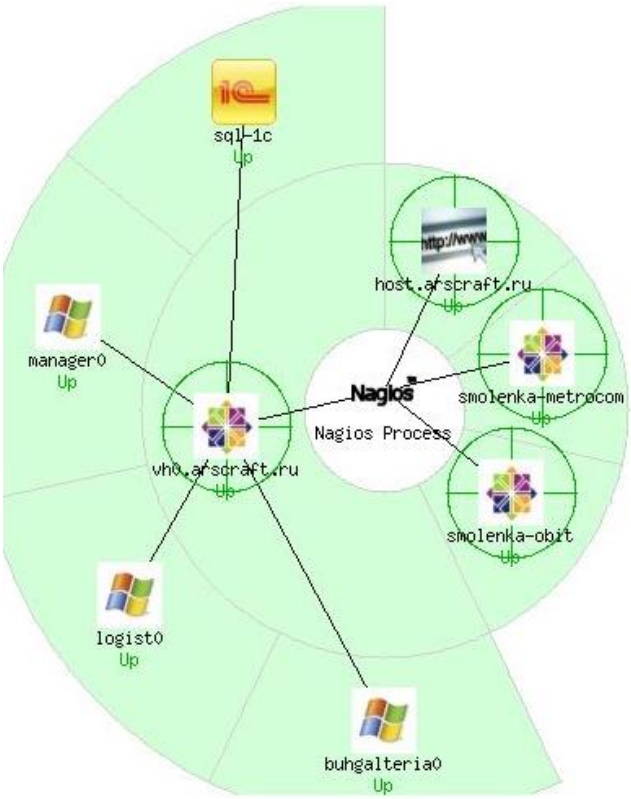

Рисунок 3.1 – Подання пункту меню Map

sql-1c	C:\ Drive Space	OK	05-11-2011 01:13:53	1d 4h 12m 17s	c: - total: 80.01 Gb - used: 21.01 Gb (26%) -
	CPU Load	OK	05-11-2011 01:15:02	0d 11h 41m 8s	CPU Load 0% (5 min average)
	Memory Usage	OK	05-11-2011 01:14:15	24d 9h 40m 48s	Memory usage: total:17212.59 Mb - used: 154
	Ragent	OK	05-11-2011 01:07:19	4d 1h 48m 51s	ragent.exe: Running
	SQL-Server	OK	05-11-2011 01:06:28	24d 9h 45m 17s	sqlservr.exe: Running
	Uptime	OK	05-11-2011 01:09:37	8d 2h 6m 33s	System Uptime - 0 day(s) 11 hour(s) 36 minut
vh0.arscraft.ru	Current Load	OK	05-11-2011 01:11:59	31d 10h 30m 8s	OK - load average: 0.00, 0.00, 0.00
	Current Users	OK	05-11-2011 01:13:08	31d 10h 36m 29s	USERS OK - 1 users currently logged in
	HTTP	WARNING	05-11-2011 01:14:17	31d 10h 35m 31s	HTTP WARNING: HTTP/1.1 403 Forbidden - 52
	PING	OK	05-11-2011 01:15:25	25d 8h 44m 29s	PING OK - Packet loss = 0%, RTA = 0.09 ms
	Root Partition	OK	05-11-2011 01:11:34	31d 10h 33m 33s	DISK OK - free space: / 66387 MB (95% inod
	SSH	OK	05-11-2011 01:12:43	31d 10h 32m 35s	SSH OK - OpenSSH_4.3 (protocol 2.0)
	Swap Usage	OK	05-11-2011 01:12:06	31d 10h 31m 36s	SWAP OK - 100% free (509 MB out of 509 MI
	Total Processes	OK	05-11-2011 01:13:14	31d 10h 30m 37s	PROCS OK: 27 processes with STATE = RSZ

Рисунок 3.2 – Подання пункту меню Services

Система моніторингу Nagios працює на декількох конфігураційних файлах, за допомогою яких налаштовуються методи стеження та об’єкти, за якими слідкуємо. Розташовані ці файли в директорії /usr/local/nagios/etc.

Розглянемо їх докладніше:

– nagios.cfg – головний файл конфігурації. У ньому описано, де лежать інші файли, оголошено змінні, налаштовується система логів, під яким користувачем працювати тощо;

– commands.cfg – файл, в якому описані команди для опитування серверів про їхню працездатність, запущені процеси тощо;

– contacts.cfg – описані контакти, яким треба надсилати оповіщення системи про збої на серверах;

– groups.cfg – описуються групи та сервери, які до них входять;

– hosts.cfg – описується шаблон для обладнання, що додається. У ньому вказується період опитування серверів, час відсилання попереджень;

– WindowsServer.cfg – приклад опису Windows сервера;

– LinuxServer.cfg – приклад опису Linux сервера.

Опитування серверів йде по протоколу SNMP (Simple Network Management Protocol – протокол простого управління мережами). Для стеження за Windows серверами потрібно додатково поставити програму Nsclient++.

Оголошуємо сервіси, за якими слідкуватимемо. Так як це 1С і SQL Server, будемо стежити за працездатністю цих процесів, а також за навантаженням на процесор.

Додавання сервера Linux нічим не відрізняється від Windows. Далі додаємо файли серверів, за якими слідкуватимемо, і перевіряємо всі конфігураційні файли на правильність. Якщо помилок та попереджень немає, перезавантажуємо Nagios. Тепер можливо зайти на сайт та подивитися що вийшло.

На цьому загальне налаштування закінчується.

Систему оповіщення можна налаштувати для кожного сервера та процесу по-різному, залежно від завдання. При спрацюванні умови на пошту системного адміністратора надходить лист такого змісту.

В результаті встановлення та налаштування системи Nagios з’являються такі можливості моніторингу корпоративної мережі:

– моніторинг мережевих служб (SMTP, POP3, HTTP, NNTP, ICMP тощо);

– моніторинг стану хостів (завантаження процесора, використання диска, системні логи) у більшості мережевих операційних систем;

– проста архітектура модулів розширень (плагінів) дозволяє, використовуючи будь-яку мову програмування на вибір (Shell, C++, Perl, Python, PHP, C# та інші), легко розробляти власні способи перевірки служб;

– паралельна перевірка служб;

– можливість визначати ієрархії хостів мережі за допомогою «батьківських» хостів, дозволяє виявляти та розрізняти хости, що вийшли з ладу, та ті, які недоступні;

– надсилання оповіщень у разі виникнення проблем зі службою або хостом (за допомогою пошти, смс або будь-яким іншим способом, визначеним користувачем через модуль системи);

– можливість визначати обробники подій, що відбулися зі службами або хостами, для проактивного вирішення проблем;

– автоматична ротація лог-файлів;

– можливість організації спільної роботи кількох систем моніторингу з метою підвищення надійності та створення розподіленої системи моніторингу;

– включає утиліту nagiostats, яка виводить загальне зведення по всіх хостах, якими ведеться моніторинг.

Переваги використання системи Nagios для моніторингу за корпоративною мережею є незаперечними. Системний адміністратор завжди

буде в курсі стану серверів і в найкоротший термін зможе попередити або усунути проблему. Встановлення та налаштування для обслуговуючого персоналу не повинно бути складним.

3.2 Спостереження за продуктивністю серверів. Cacti

Cacti – open-source вебдодаток, система дозволяє будувати графіки за допомогою RRDtool. Cacti збирає статистичні дані за певні часові інтервали та дозволяє відобразити їх у графічному вигляді. Переважно використовуються стандартні шаблони для відображення статистики із завантаження процесора, виділення оперативної пам’яті, кількості запущених процесів, використання дискових ресурсів, використання вхідного/вихідного трафіку.

Ця система допоможе дізнатися, коли на серверах бувають піки навантаження, використання ресурсів серверів протягом дня, тижня, місяця. Проаналізувавши отримані графіки, можна говорити про можливу необхідність upgrad сервера та оптимізацію робіт у піковий годинник для зниження навантаження [25-29].

Встановлювати та налаштувати систему будемо на маршрутизатор colo. Система Cacti потребує великої кількості додаткового програмного забезпечення. Вебсервер у нас вже встановлений, тому цей пункт пропускаємо та починаємо встановлення:

- встановлюємо додаткове ПЗ: Mysql, php, perl та бібліотеки для них;
- запускаємо mysql. Одночасно відбувається його конфігурація;
- встановимо залежності потрібні Cacti;
- додаємо в автозавантаження та запустимо сервіс SNMP;
- завантажуємо пакети Cacti;
- розархівуємо їх;

– створюємо робочу папку Cacti на сервері;

– створюємо робочу папку Cacti на сервері;

– копіюємо вміст розпакованої папки Cacti у робочу папку Cacti;

– створюємо в системі користувача для Cacti і дамо йому відповідні права;

– створюємо базу даних для Cacti з привілеями для cactivor;

– імпортуємо структуру Cacti у її базу;

– налаштовуємо доступ Cacti до її бази даних;

– переходимо в робочу директорію Cacti та встановлюємо фікси офіційними патчами;

– чтворюємо cacti.conf з таким змістом, щоб увімкнути вебдоступ;

– далі використовуємо базову інсталяцію Cacti. Додавання серверів, за якими слідкуватимемо, здійснюється через вебінтерфейс, доступний за адресою: http://ip.адреса.сервера/cacti. Але спочатку потрібно поставити на сервері, що відстежуються, пакет snmp і переписати конфігураційний файл доступу /etc/snmp/snmpd.conf.

Приклади графіків, що вийшли, представлені на рисунках 3.3 - 3.6.

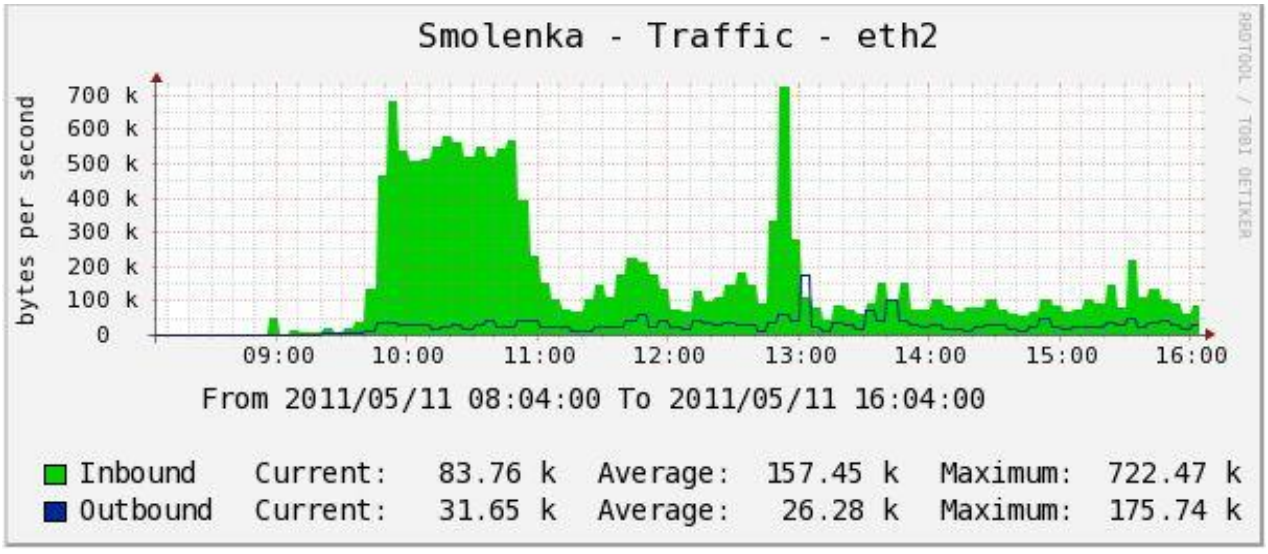

Рисунок 3.3 – Графік використання Інтернет-каналу

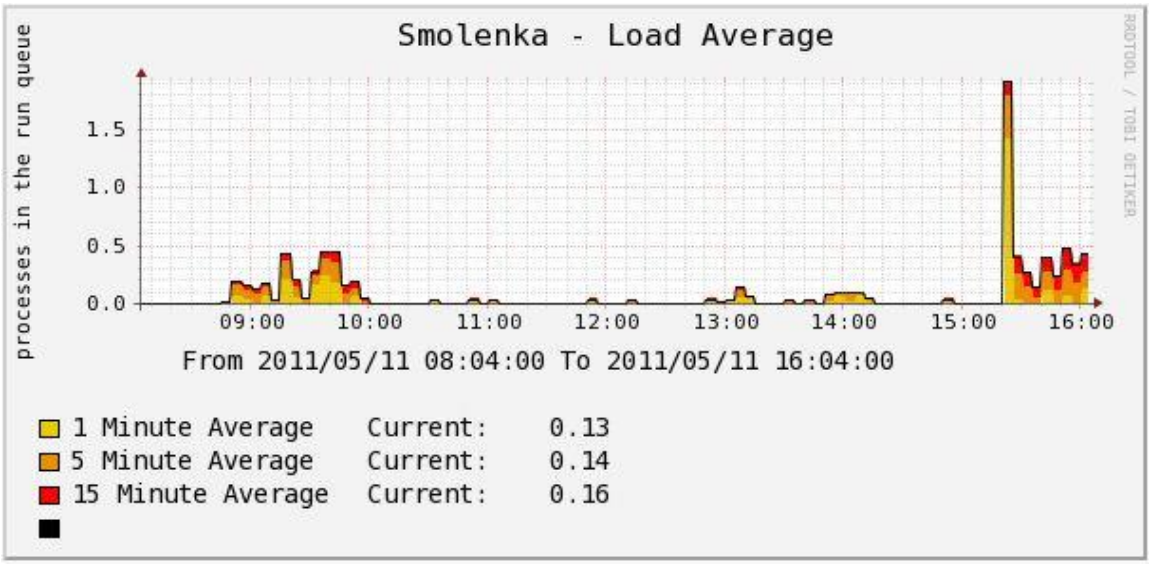

Рисунок 3.4 – Графік середнього завантаження процесора

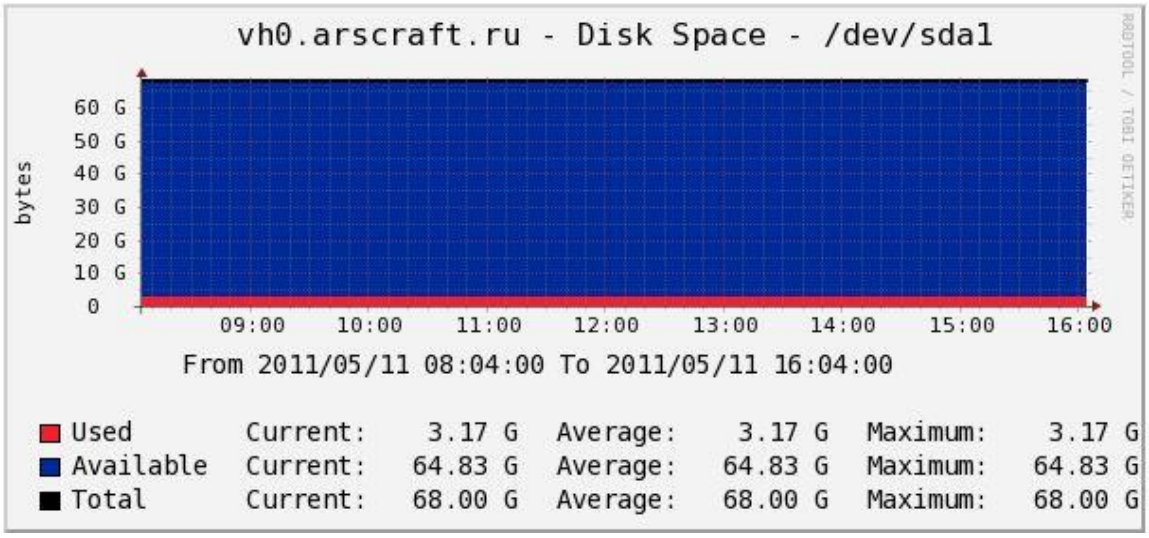

Рисунок 3.5 – Графік використання дискового простору

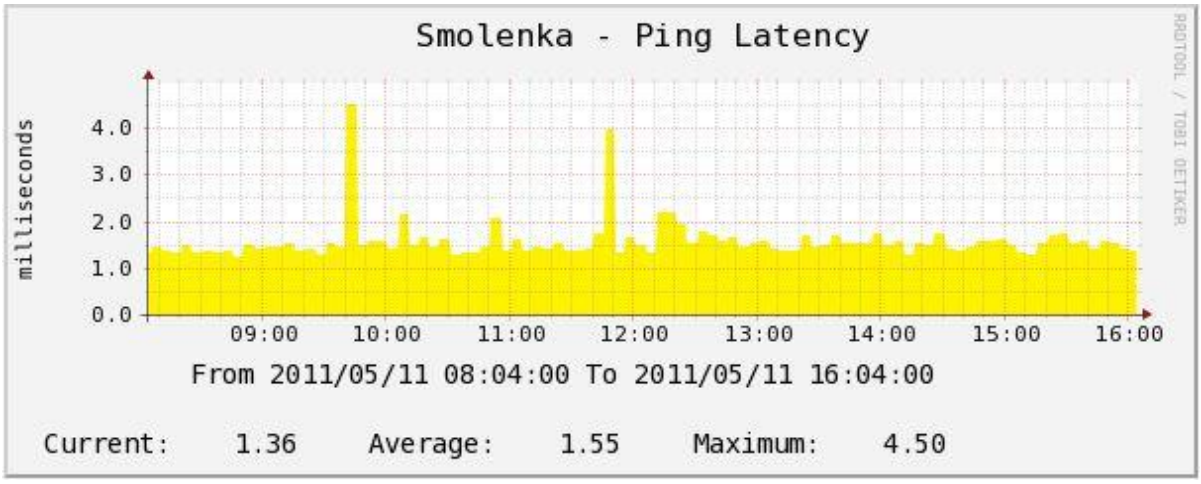

Рисунок 3.6 – Графік відгуку сервера (RTT)

3.3 Фільтрування та аналіз трафіку корпоративної мережі

3.3.1 Proxy сервер

Часто у фірмах, на підприємствах, де робочий персонал має доступ до мережі Інтернет, потрібна фільтрація вхідного трафіку. Потрібно це з двох простих причин.

По перше найбільш поширений спосіб попадання шкідливих програм на комп'ютер відбувається під час перегляду вебсторінок сумнівного контенту, перегляду банерів та скачування різного софту.

По друге однією з найчастіших вимог керівництва організації є обмеження доступу на розважальні сайти та соціальні мережі. Щоб здійснювати фільтрацію, потрібно, щоб весь http трафік проходив через спеціальний proxy сервер.

Proxy сервер – служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до proxy-серверу та запитує якийсь ресурс (наприклад, e-mail), розташований на іншому сервері. Потім proxy-сервер або підключається до вказаного сервера і отримує ресурс у нього, або повертає ресурс із власного кеша (у разі, якщо proxy має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінений proxy-сервером у певних цілях. Також proxy-сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак та допомагає зберігати анонімність клієнта [6, 11, 12, 30].

Реалізувати перекидання запитів на proxy-сервер можна двома шляхами:

– явно вказати в браузері адресу proxy-сервера (не рекомендується через незручність перемикання у разі падіння сервера);

– пересилати весь трафік, що надійшов на порти 80, 8080 маршрутизатора на proxy-сервер за допомогою правил iPtables.

У роботі використовуватимиця другий метод. Proxy-сервер

встановлюватимемо на маршрутизатор colo. Як ПЗ встановимо proxy-сервер SQUID.

Squid – програмний пакет, що реалізує функцію кешування proxy-сервера для протоколів HTTP, FTP, Gopher і (у разі відповідних налаштувань) HTTPS. Розроблений спільнотою як програма з відкритим вихідним кодом (розповсюджується відповідно до GNU GPL). Всі запити виконує як один неблокований процес введення/виводу. Установка проводиться зі стандартного репозиторію та після першої установки необхідно проініціалізувати кеш.

Далі переходимо до налаштування. Потрібно вирішити наступне завдання – закрити доступ на розважальні сайти та соціальні мережі, закрити доступ на скачку *.exe, *.sys, *.bat, *.sys, *.mp3, *.avi, *.mp4, *.mov файлів.

Основна конфігурація proxy-сервера міститься у файлі /etc/squid/squid.conf. Відредагуємо його під наше завдання:

– вказуємо порт у якому слухатимемо запити, і вказуємо тип Proxy «прозорий», т.к. пересилаємо пакети засобами маршрутизатора;

– описуємо об’єкти та створюємо правила доступу до них;

– описуємо нашу локальну мережу;

– описуємо файл, у якому записані розширення заборонених типів файлів;

– описуємо файл, в якому записано список сайтів, заборонених для перегляду;

– створюємо список для аудіо та відео контенту за допомогою mime типів;

– забороняємо доступ із мережі до заборонених типів файлів, сайтів та контенту;

– дозволяємо доступ мережі для решти трафіку;

– для всіх інших забороняємо все;

– не забудемо залишити права адміністратора, додавши потрібну acl запис. Розглянемо файли із забороннними списками;

– залишилося перенаправити запити з 80, 8080 портів на 3128. Додаємо в ланцюжок iptables наступне правило.

Тепер трафік йде через проксі-сервер із фільтрацією. Також за допомогою Proxy-сервера при необхідності можна створювати ліміти споживання трафіку, працювати за розкладом та замінювати рекламні банери на web-сторінках на свої.

3.3.2 Аналізатор логів Proxy сервера

Ще одним із найчастіших завдань є аналіз трафіку з двох причин:

– спостереження за діяльністю співробітника. Запобігання порушенням дисципліни та правил роботи в компанії;

– створення лімітів на трафік для зниження витрат компанії.

Proxy-сервер Squid при проходженні трафіку записує всю інформацію (звідки запит, що запитують, час, розмір тощо) у log файл. Залишається лише проаналізувати його та вивести інформацію у зручному для людини вигляді.

Аналізувати трафік будемо спеціальним безкоштовним ПЗ LightSquid.

Усі необхідні компоненти (Perl, Gd, httpd) вже були встановлені раніше, тому переходимо безпосередньо до встановлення LightSquid:

– завантажуємо із сайту http://lightsquid.sourceforge.net/ останню версію програми версії 1.8;

– розархівуємо завантажений архів у каталог /var/www/html/;

– вносимо зміни до файлу конфігурації Apache /etc/httpd/conf/httpd.conf;

– перезавантажуємо web-сервер для застосування змін;

– переходимо в каталог з розпакованим lightsquid;

– перевіряємо на правильність конфігураційного файлу. Якщо видає помилки, швидше за все, неправильно написані шляхи до потрібних програм каталогів. Виправити це можна у файлі lightsquid.cfg;

– якщо помилок немає, то додаємо завдання аналізу трафіку кожні півгодини cron.

На цьому встановлення закінчено. При необхідності, є можливість занести адреси, з яких йде трафік, до груп та дати їм імена.

Перевірити роботу можна за адресою http://ip.адреса.сервера/lightsquid.

Приклад роботи аналізатора трафіку представлений на рисунках 3.7 - 3.9.

Отчёт по использованию интернета, прокси-сервер Squid.

Дата: **06 Май 2011 (Обновлено :: 11:30 :: 12 Май 2011)**

Популярные сайты (отчёт)

Кто скачал БОЛЬШИЕ файлы (отчёт)

№	Время	Пользователь	Ф.И.О	Соединений	Байт	%	Группа
1		sauna	sauna user name	20 558	150.8 M	90.2%	01. sauna
2		baltsib	baltsib user name	1 880	12.0 M	7.1%	03. baltsib
3		banius	banius user name	74	4.3 M	2.5%	02. banius

Рисунок 3.7 – Приклад звіту LightSquid

Всего **150.8 M**

№	Посещённые сайты	Соединений	Байт	Итого	%
1	www.mail.ru	4 181	36.2 M	36.2 M	24.0%
2	www.sbrf.ru	1 197	12.5 M	48.7 M	8.2%
3	www.volochkova.ru	374	7.0 M	55.6 M	4.6%
4	www.semozer.ru	151	4.6 M	60.3 M	3.0%
5	www.kleo.ru	262	3.7 M	64.0 M	2.4%

Рисунок 3.8 – Відвідані сайти

Рисунок 3.9 – Графік щодо використання трафіку по днях

3.3.3 Облік трафіку корпоративної мережі. Розробка web-інтерфейсу

Якщо стеження за діяльністю співробітника можна реалізувати засобами аналізу http трафіку, то завдання підрахунку трафіку вирішується лише частково, оскільки вважається лише http трафік.

Часто провайдери надають приватним особам та організаціям доступу до мережі Інтернет не безлімітний, а трафіковий, тобто накладають обмеження на кількість завантажених та відданих даних. За перевищення трафіку доводиться сильно переплачувати. Тому моніторинг за трафіком є важливим завданням.

Є безліч білінгових систем, які включають функцію підрахунку трафіку, але там занадто багато не потрібних нам можливостей і функцій. Існує програма IPCad, яка може допомогти вирішити задачу.

IPCad (Cisco IP accounting simulator) – це програма для обліку трафіку, яка може вести підрахунок кількома механізмами, наприклад, через інтерфейси BPF, libpcap та iptables. Є один недолік: результати виводяться до консолі, без будь-якої фільтрації. Тому до пакету IPCad потрібно

доопрацювати інтерфей:

– почнемо з установки IPCad;

– конфігуруємо пакет;

– збираємо та встановлюємо пакет;

– переробляємо конфігураційний файл під свої потреби;

– вказуємо не розбирати трафік портами. Ця опція сильно навантажує маршрутизатор;

– вказуємо, який інтерфейс слухати;

– установки програми за замовчуванням.

Розділяти статистику по кожній IP-адресі для підмережі 192.168.23.0/24:

– «aggregate 192.168.0.0/24» вказує ipcad діапазон адрес мережі;

– «strip 32» означає, що в статистику необхідно заносити всі 32 біти адреси, що належить даному адресному діапазону.

Описуємо політики доступу до статистики IPCAD.root може повністю управляти (робити backup, переглядати та змінювати таблиці підрахунку). Всі інші можуть лише переглядати статистику. Отримаємо виведення в консоль:

192.168.23.14 83.156.177.10 1 131
178.67.60.119 192.168.23.14 1 305
192.168.23.14 202.152.243.92 1 131
192.168.23.14 178.67.60.119 1 131
192.168.23.14 77.77.44.16 1 131
192.168.23.196 192.168.23.201 2873 186687
192.168.23.201 192.168.23.196 4274 3838143

Accounting data age is 4
Accounting data age exact 269

Accounting data saved 1305215070

Interface eth1: received 375320822, 5 m average 41518 bytes/sec, 60 pkts/sec

Flow entries made: 569

NetFlow cached flows: 27

Memory usage: 0% (63728 від 10485760)

Free slots for rsh clients: 9

IPCAD uptime is 49 days 51 minutes

Такий результат не всім буде зрозумілий, та й запускати програму вручну не найзручніший спосіб підраховувати трафік. Для вирішення цієї проблеми необхідно створити зручний вебінтерфейс. Усю інформацію про трафік будемо заносити до бази даних СУБД MySql. Створюємо базу даних stat та необхідні нам таблиці (users, download, upload, tmp), в які будемо записувати статистику.

Створимо скрипт «stat.sh», який запускатиме команду отримання статистики та записуватиме результат у файл, а потім запускатиме скрипт «collect.pl», який відповідає за додавання інформації до бази даних.

Скрипт stat.sh потрібно запускати кожні 20-25 хвилин, тому додаємо завдання в cron.

Тепер усі потрібні дані знаходяться у базі даних, залишилося лише витягнути їх на сайт. Для цього розробляємо кілька вебсторінок. У результаті отримуємо систему підрахунку трафіку у зручному табличному вигляді на рисунку 3.10, з наступними можливостями:

– облік будь-якого трафіку для кожного користувача окремо;

– встановлення ліміту трафіку, при перевищенні якого на пошту системному адміністратору надходить повідомлення.

IP	Downloads(MB)	Uploads(MB)	Online
192.168.23.40	53	17	
192.168.23.38	63	8	
192.168.23.41	67	21	
192.168.23.234	492	17	
192.168.23.32	151	10	
192.168.1.255	0	0	
192.168.23.14	44	10	
192.168.23.174	274	58	
192.168.23.194	494	21	
192.168.23.17	2	0	
192.168.23.16	53	5	
192.168.23.13	14	5	
192.168.23.12	48	14	
192.168.23.15	61	7	
192.168.23.39	100	8	
192.168.23.183	27	2	
192.168.23.217	1289	32	

Рисунок 3.10 – Таблиця використання Інтернет-трафіку

ВИСНОВКИ

У рамках кваліфікаційної роботи було побудовано захищену корпоративну мережу на основі VPN, використовуючи технології OpenVPN та SSH.

Розглянуто методи організації VPN мереж: клієнт-серверний, тунелювання, точка-точка.

Отримано табличні значення пропускної спроможності захищених інтернет каналів для технологій OpenVPN та SSH. Дано практичну оцінку продуктивності цих каналів створеної копроративної мережі. Отримані результати дозволяють зробити загальний висновок: при побудові корпоративної мережі доцільно використовувати обидві технології – за допомогою OpenVPN створювати захищені мережі, за допомогою SSH-sun-тунелі та створення підключень для адміністрування.

Розглянуто рішення для моніторингу корпоративної мережі: Nagios, Cacti, Ipcad, LightSquid. Зроблено висновок про використання цих рішень в одному комплексі.

З метою фільтрації трафіку та стеження за діяльністю персоналу встановлено, налаштовано та введено в роботу proxy-сервер.

Введено в експлуатацію систему моніторингу, що складається з розглянутих у роботі компонентів: Nagios, Cacti, Ipcad, LightSquid;

Розроблено web-інтерфейс для системи обліку трафіку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Соколов, О. В., Шаньгін, В. Ф. (2002). Захист інформації у розподілених корпоративних мережах та системах: навч. посібник.

2. Олифер, В. Г., Олифер Н.А. (2001). Комп'ютерні мережі. Принципи, технології, протоколи: навч. посібник.

3. Колесніков, О. В., Брайан Хетч. (2002). LINUX. Створення віртуальних приватних мереж (VPN): навч. посібник.

4. Rosenberg, J. (2017) Rugged Embedded Systems, *Embedded security*, 7, pp. 14-23.

5. Faircloth, J. (2017) Penetration Tester's Open-Source Toolkit (Fourth Edition), *Wireless penetration testing*, 1, pp. 1-26.

6. Rosenberg, J. (2000) IP Addressing & Subnetting INC IPV6, *Private Addressing and Subnetting Large Networks*, 6, pp. 15-28.

7. What is a VPN. URL: https://www.expressvpn.com/go/what-is-vpn-1?category=VPN&subcategory=info&lang=en&gclid=Cj0KCQjwvqeUBhCBARIsAOdt45bm2rLvGQSb1HDdB5WaJMGbFqnP-fLFvnnyfNSraao2-hge9ha7JO8aAoATEALw_wcB (дата звернення 29.04.2022).

8. Ghorbani, A. (2015) Characterization of Encrypted and VPN Traffic using Time-related Features, *University of New Brunswick*, 1, pp. 1-14.

9. Richard C. Harlan (2014) Enhance and Modify Network Monitoring Tool (Cacti), *Department of Electronic Engineering*, 3, pp. 8-15.

10. Richard C. Harlan (2006) Wireless Sensor Network-Management System, An Adaptive Policy-Based Management for Wireless Sensor Networks, *WinMS*, 1, pp. 1-18.

11. Markus, F. (2006). Openvpn: Building and Integrating Virtual Private Networks: навч. посібник.

12. Muhammad Iqbal, Imam Riadi (2019) Analysis of Security Virtual Private Network (VPN) Using OpenVPN, *International Journal of Cyber-Security and Digital Forensics*, 1, pp. 1-8.

13. Eric F. Crist, Jan Just Keijser (2015). Mastering OpenVPN: навч. посібник.

14. Zhensheng Zhang, Ya-Qin Zhang, Xiaowen Chu & Bo Li (2004) An Overview of Virtual Private Network (VPN): IP VPN and Optical VPN, *Photonic Network Communications*, 2, pp. 8-28.

15. Derrick Rountree (2011) Security for Microsoft Windows System Administrators, *Network Security*, 4, pp. 13-18.

16. What Is SSH: Understanding Encryption, Ports and Connection. URL: https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work#What_Is_SSH (дата звернення 29.04.2022).

17. Private Network. URL: https://www.sciencedirect.com/topics/computer-science/private-network (дата звернення 29.04.2022).

18. Стивен Б. (2017). Віртуальні приватні мережі: навч. посібник.

19. Nagios Based Enhanced IT Management System. URL: https://www.researchgate.net/publication/225284738_Nagios_Based_Enhanced_IT_Management_System (дата звернення 05.05.2022).

20. Richard C. Harlan (2003) Network management with Nagios, *Linux Journal*, 1, pp. 1-3.

21. Nagios Tutorial: Continuous Monitoring with Nagios Core and XI. URL: https://phoenixnap.com/blog/nagios-monitoring-tutorial (дата звернення 05.05.2022).

22. Nagios Log Server. URL: https://docs.nxlog.co/userguide/ (дата звернення 05.05.2022).

23. Centralized Log Management, Monitoring and Analysis Software. URL: https://www.nagios.com/products/nagios-log-server/ (дата звернення 06.05.2022).

24. Nagios Core 4 – Introduction. URL: https://support.nagios.com/kb/article/nagios-core-4-introduction-684.html (дата звернення 06.05.2022).

25. Network Monitoring & Management Using Cacti. URL: https://nsrc.org/workshops/2020/ekiti-connect/netmgmt/en/cacti/cacti-from-packages.pdf (дата звернення 06.05.2022).

26. The Cacti Manual. URL: https://files.cacti.net/docs/pdf/manual.pdf (дата звернення 06.05.2022).

27. Configure Cacti to Monitor a Network Devices. URL: https://www.unixmen.com/configure-cacti-monitor-network-devices/ (дата звернення 06.05.2022).

28. Overview of Cacti Watcher Function – IMG. URL: https://www.dialogic.com/webhelp/img1010/10.5.3/webhelp/ov_cacti_watcher.htm (дата звернення 06.05.2022).

29. Wang, F., Wang P., Wang, Y., Zhang, Z. C. (2016) The network monitoring system based on Cacti for EAST, *2016 IEEE-NPSS Real Time Conference (RT)*, 3, pp. 11-23.

30. Richard C. Harlan (2006) Wireless Sensor Network-Management System, An Adaptive Policy-Based Management for Wireless Sensor Networks, *WinMS*, 5, pp. 34-58.