Хмельницький національний університет
Факультет програмування
та комп'ютерних і телекомунікаційних систем
Кафедра кібербезпеки та комп'ютерних систем і мереж

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Розподілена корпоративна мережа підприємства
Назва теми

КвРКІ.170353.17.03.12 ПЗ
Шифр

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія»*
Назва

Виконав: студент IV курсу, група КІ–17–3 _____ Сташук Д.В.
Підпис, Ініціали, прізвище

Керівник _____ Ю.П. Кльоц
Підпис, дата, Ініціали, прізвище

Нормоконтролер _____ І.В. Муляр
Підпис, дата, Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки
та комп'ютерних систем
і мереж _____ Ю.П. Кльоц
Підпис, Ініціали, прізвище

«26» червня 2021 р.

Хмельницький 2021

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет Програмування та комп'ютерних і телекомунікаційних систем

Кафедра Кібербезпеки та комп'ютерних систем і мереж

Освітній рівень бакалавр

Галузь знань 12 Інформаційні технології

Спеціальність 123 Комп'ютерна інженерія

Освітня програма Освітня програма «Комп'ютерна інженерія»

ЗАТВЕРДЖУЮ

Завідувач кафедри Ю.П. Кльоц

" 05 " 02 2021 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Сташук Дар'ї Володимирівни

Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Розподілена корпоративна мережа підприємства

Керівник проекту (роботи) Кльоц Юрій Павлович

Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

кандидат технічних наук, доцент

Затверджена наказом ректора університету від 05.02.2021 № 11 додаток №7

2. Строк подання студентом проекту (роботи) на кафедру 29.06.2021

3. Вихідні дані до проекту (роботи) завдання на дипломне проектування

4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)

Предметна область і постановка задачі; Поняття «Корпоративна мережа»; SSH; Впровадження технологій VPN в корпоративну мережу і їх порівняльна оцінка; Створення комплексу систем корпоративної мережі; Proxy сервер.

5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)

Фізична схема локальної мережі

Логічна схема локальної мережі (E8)

Змодельована мережа (E8)

6. Консультанти розділів дипломного проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийн
Нормоконтроль	Муляр І.В., Доцент кафедри КБ		
Антиплагіат	Муляр І.В., Доцент кафедри КБ		

7. Дата видачі завдання « 08 » 02 2021 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів (розділів) дипломного проекту (роботи)	Термін виконання етапів проекту (роботи)	Приміт
1.	Підготовка вступного розділу	Березень - 1 декада	
2.	Огляд існуючих методів, засобів	Березень - 2 декада	
3.	Обгрунтування обраних рішень	Березень - 3 декада	
4.	Підготовка опису електричних схем	Квітень - 1 декада	
5.	Виконання розрахункової частини	Квітень - 1 декада	
6.	Підготовка ескізів креслень	Квітень - 2 декада	
7.	Формулювання висновків	Квітень - 3 декада	
8.	Розробка додатків	Травень - 1 декада	
9.	Погодження розділів з консультантом з нормоконтролю	Травень - 1 декада	
10.	Оформлення графічного матеріалу	Травень - 2 декада	
11.	Оформлення пояснювальної записки	Травень - 2 декада	
12.	Попередній захист кваліфікаційної роботи	Травень - 3 декада	
13.	Доопрацювання кваліфікаційної роботи	Травень - 3 декада	
14.	Подання роботи для перевірки на плагіат	Травень - 3 декада	
15.	Захист кваліфікаційної роботи	Червень - 1 декада	

Студент _____ Підпис Д.В. Сташук Ініціали, прізвище

Керівник проекту (роботи) _____ Підпис Ю.П. Кльоц Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: «Розподілена корпоративна мережа підприємства».

Автор роботи: Сташук Дар'я Володимирівна.

Керівник роботи: Кльоц Юрій Павлович.

Пояснювальна записка: 97 с., 33 рис., 4 таб., 6 дод., 17 джерел.

Графічна частина: 10 презентаційних слайдів.

ФІЗИЧНА СХЕМА ЛОКАЛЬНОЇ МЕРЕЖІ. ЛОГІЧНА СХЕМА ЛОКАЛЬНОЇ МЕРЕЖІ. ЗМОДЕЛЬОВАНА МЕРЕЖА.

Метою роботи є побудова захищеної корпоративної мережі.

У цій роботі отримано табличні значення пропускної здатності захищених інтернет каналів для технологій OpenVPN і SSH. Дана практична оцінка продуктивності цих каналів створеної корпоративної мережі. Отримані результати дозволяють зробити загальний висновок: при побудові корпоративної мережі доцільно використовувати обидві технології - за допомогою OpenVPN створювати захищені мережі, за допомогою SSH - ssh-тунелі і створення підключень для адміністрування.

Підпис студента  Дата 15.06.2021

№	формат	Позначення	Найменування	Кіл. листів	№ екз	Примітка
			Текстові документи			
		КвРКІ.170353.17.03.28 ПЗ	Пояснювальна записка	97		
			Графічні матеріали			
		КвРКІ.170353.17.03.28 Е8	Фізична схема локальної мережі	1		
		КвРКІ.170353.17.03.28 Е8	Логічна схема локальної мережі	1		
		КвРКІ.170353.17.03.28 Е8	Змодельована мережа	1		

Ар к	№ докум	Підпис	Дата	КвРКІ.170353.17.03.28 ВП			
обив	Стащук Д.В.			Розділена корпоративна мережа підприємства Відомість проекту	Літера	Аркуш	Аркушів
евір.	Кльоц Ю.П.				У	1	1
ир.	Мулар І.В.			ХНУ, КІ-17-3			
тв.	Кльоц Ю.П.						

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

МФУ - багатофункціональний пристрій, що виконує функції принтера, сканера, копіра.

Wi-fi - точка доступу.

Ip-телефони.

Web-сервер.

API- інтерфейс прикладного програмування

SQL- мову структурованих запитів

VPN- віртуальна приватна мережа

SSL- випробувані і перевірені стандарти

OpenVPN - це інструмент з відкритим вихідним кодом

PKI- Інфраструктуру Відкритих Ключів

TLS- безпека транспортного рівня

IETF - робоча група з питань Інтернет-інженерії

NAT- ніяких проблем з технологією

SSH-захищена оболонка

DH- Діффі-Хеллмана

RDP-протокол віддаленого робочого столу

CentOS-спільнота Операційна система ENTerprise

Colo - · Колокація, провайдерські сервера

TLS-ключ, потрібен і клієнтам і серверам

Nagios - гнучка система моніторингу роботи серверів

Cacti- відкрите джерело веб-додаток

Proxy - це служба в комп'ютерній мережі

SQUID- програмний пакет

ACL - список контролю доступу

IPCad- симулятор бухгалтерського обліку IPНіяких проблем з технологією NAT

OpenVPN - це інструмент з відкритим вихідним кодом

HTTP-потреби від клієнтів

Висока сумісність з firewall'м і посередниками WWW

SSH (Secure SHell)-це мережевий протокол рівня сеансу

ВСТУП

Останнім часом все частіше документообіг і передача корпоративної інформації відбувається в електронному вигляді той чи інший спосіб. Для цього вже існує безліч протоколів і методів передачі даних. Так, наприклад, електронний документообіг підприємства проводиться засобами платформи 1С, що має безліч різних конфігурацій під будь-які потреби бізнесу; пересилання документів по електронній пошті з використанням поштових протоколів POP, IMAP, SMTP; передача великих обсягів інформації за допомогою FTP протоколу; організація корпоративного сайту, використовуючи веб-технології.

Інформаційні технології 21 століття надають великі можливості щодо вдосконалення роботи підприємств, замінюючи людська праця машинним, підвищуючи зростання продуктивності праці і знижуючи витрати на персонал. Створюються нові і модернізуються діючі підприємства, територіально розосереджені в межах населеного пункту, міста або навіть країни, так як тепер засоби зв'язку набагато доступніше і дешевше.

Все це стало можливим, завдяки комп'ютеризації та використання мережевих технологій на підприємстві. Але є речі, про які не можна забувати: складність впровадження, безпеку, продуктивність, захищеність, надійність системи. Головними проблемами на сьогоднішній день стали безпеку і життєздатність комп'ютерних систем.[11]

Корпоративна інформація, передана через відкриту мережу Інтернет, легко може бути перехоплена за допомогою спеціальних програм-сніфферов - зловмисниками і використовуватися в корисливих цілях. Сюди відносяться найважливіша інформація, що міститься в конфіденційних документах. Крім цього можуть бути перехоплені логіни і паролі від корпоративної пошти або інших сервісів. Конфіденційність інформації, що передається виходить наперший план при створенні корпоративної мережі.

Захист інформації, що передається по каналах зв'язку, використовуючи паролювання документів або їх шифрування, не надає потрібного рівня безпеки,

так як будь-який пароль може бути зламаний і це лише питання часу(все залежить від його складності), а за допомогою криптоаналіза, можна виявити і шифрує ключ. Звичайно, можна використовувати великі і складні паролі, сучасні великі ключі шифрування, але все це знизить продуктивність, перетворивши простий механізм операції відправки в досить витратний по часових параметрів. Час буде витрачено на те, щоб захистити кілька файлів. Аякщо це треба робити постійно і у великих кількостях?

Якраз для вирішення зазначених суперечностей в корпоративних мережах використовуються різні протоколи Virtual Private Network. З їх допомогою створюються віртуальні канали зв'язку поверх мережі Інтернет. Вони дають можливість з'єднувати локальні мережі різних технологій і їх сегменти в одну корпоративну мережу. Але найголовніше гідність, власне заради чого вони й потрібні, 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 зловмисникові з'ясувати адресат переданої інформації.

Все це дає великі можливості для побудови захищеної мережі. Але якщо щось виходить з ладу, програма або обладнання серверів, то і захищений канал перестає працювати. За станом комп'ютерного парку постійно потрібно вести моніторинг, щоб час простою в разі падіння однієї ділянки мережі був мінімальним. Маючи безліч серверів і 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 і поштових повідомлень цене складе великих труднощів, і адміністратор завжди буде в курсі станумережі, сервісів і серверів, що входять в цю корпоративну мережу. [2]

Зазначені проблеми при побудові корпоративних мереж для конкретних підприємств показують, що процес їх створення не є тривіальним. Тому в рамках роботи ставляться і вирішуються завдання вибору і реалізації протоколів VPN, оцінки продуктивності отриманих каналів і способи моніторингу за станом корпоративної мережі в режимі реального часуконкретного підприємства.

РОЗДІЛ 1 ПРЕДМЕТНА ОБЛАСТЬ І ПОСТАНОВКА ЗАДАЧІ

1.1 Основні відомості про корпоративні мережі

1.2 Організація зв'язку

Перш ніж говорити про корпоративну (приватну) мережу, слід значення цих слів. За останні роки це сполучення слів стало досить поширеним і сучасним, що потроху стало втрачати сенс. У загальному розумінні корпоративна мережа - це система, що забезпечує передавання інформації між різноманітними додатками, що використовуються в системі корпорації. Зробивши висновки з цього цілком абстрактного визначення, розглянемо різні варіанти до створеннятаких систем і спробуємо наповнити поняття корпоративної мережі чітким змістом. При цьому припустимо, що мережа повинна бути максимально всеосяжною, тобто допускати інтеграцію вже наявних і майбутніх додатків з мінімально дозволеними витратами та обмеженнями.[12]

Корпоративна мережа, здебільшого, є територіально розподілена, тобто з'єднує офіси, підрозділи та інакші структури, що знаходяться на великій відстані один від одного. Зазвичай вузли корпоративної мережі виявляютьсярозміщеними в різних містах, а іноді і країнах. Правила, за якими будується така мережа, доволі сильно відрізняються від тих, що застосовуються при створенні локальної мережі, і також охоплює декілька будівель.[7] Головною різницею є застосування досить повільних орендованих ліній зв'язку у територіально розподіленій мережі. Якщо при формуванні локальної мережі основні затрати припадають на закупівлю спорядження і прокладку кабелю, то істотним елементом вартості в територіально-розподілених мережах виявляється орендна плата за застосування каналів, яка стрімко зростає зі збільшенням якості і швидкості доставки даних. Це обмеження є безкомпромісним, і при проектуванні корпоративної мережі варто вжити всі заходи для мінімізації об’ємів переданих даних. По інакшому ж корпоративна мережа не повинна вносити обмеження на те, котрі саме програми та яким образом, обробляють перенесення по ній інформацію.

Додатки слід розуміти як системне програмне забезпечення - системи керування базами даних, поштові системи, обчислювальні ресурси, файловий сервіс та інше, як і кошти, з якими працює останній користувач. Головними завданнями корпоративної мережі являються: взаємодія системних додатків, розміщення в різних вузлах та доступ до віддалених користувачів.

Організація каналів зв'язку - перша проблема, яку потрібно вирішувати при формуванні корпоративної мережі. Якщо в кордонах одного міста можливо розраховувати на оренду відмічених ліній, зокрема високошвидкісних, то переходячи до географічно віддалених вузлів, ціна оренди каналів стає астрономічною, а якість і безпечність часто виявляється доволі невисокими. Природним рішенням такої проблеми є використання вже наявних глобальних мереж. В такому випадку достатньо забезпечити канали від офісів до якомога ближчих вузлів мережі. Задачу доставки інформації поміж вузлами, глобальна мережа при цьому, візьме на себе. Навіть при формуванні невеликої мережі в межах певного міста, варто враховувати можливість подальшого розширення і застосування технології, сумісної з наявними глобальними мережами.

Періодично першою, а то і єдиною мережею, припущення про яку з’являється в голові, виявляється Інтернет. Використовуючи мережу Інтернет як основу для корпоративної мережі передавання даних, виникає дуже цікавий факт. Інтернет мережею-то якраз і не є. Це саме Інтернет - між мережа. Якщо подивитись всередину Інтернету, можна замітити, що інформація протікає через безліч зовсім незалежних і у переважній більшості некомерційних вузлів, пов'язаних через різні канали та мережі передавання даних.

Ще одна проблема Інтернету, широко обговорювана останнім часом - безпека. Якщо говорити на рахунок приватної мережі, повністю природним

представляється захистити передану інформацію від стороннього погляду. Несподіваність шляхів інформації поміж безліччю вільних вузлів Інтернет не лише збільшує ризик того, що будь-яких занадто цікавий оператор мережі здатен скласти ваші дані собі на диск (на техніці це не дуже складно), але і робить неспроможним визначення місця витоку інформації. Існують способи

шифрування інформації, які передаються, що дає змогу частково знайти рішення для цієї проблеми. Інший аспект проблеми безпеки знову ж пов'язаний з децентралізованого Інтернету – відсутність будь-кого, хто може обмежити доступ до ресурсів вашої приватної мережі. Так як це відкрита система, в якій абсолютно всі бачать всіх, то кожен бажаючий має можливість спробувати потрапити у вашу офісну мережу і мати доступ до всіх даних або програм. Є, звісно, засоби для захисту (для яких прийнято назву Firewall - по-німецьки "брандмауер" - протипожежна стіна). Проте вважати їх панацеєю не потрібно. Будь-який захист можливо зламати, тільки б це компенсувало вартість злому. Необхідно також зазначити, що зробити підключену до Інтернету систему непрацездатною можливо і, без втручання в вашу мережу. Існує несанкціонований доступ до управління мережевими вузлами або просто використання функціональності архітектури Інтернету для знищення доступу до певного сервера.[6] Тому неможливо рекомендувати Інтернет як основу для системи, яка вимагає надійності та конфіденційності. Має сенс підключитися до Інтернету в рамках корпоративної мережі

1.3 Поняття «Корпоративна мережа»

Корпоративна мережа-це складна система, що складається з тисяч різних компонентів: різних типів комп'ютерів, від настільних комп'ютерів до цілих серверних стійок, систем і додатків, мережевих адаптерів, комутаторів і маршрутизаторів і багато чого іншого.

Успішне функціонування промислових, фінансових та інших організацій багато в чому залежить від наявності єдиного інформаційного простору. Розвиток

Інформаційні системи дозволяють вам ефективно управляти потоком інформації, переданої між вашими співробітниками, і приймати своєчасні і розумні рішення, що забезпечують виживання вашого бізнесу в складній конкурентній боротьбі.

Корпоративна мережа-це складна система, яка може передавати різні дані між різними додатками, використовуваними в єдиній інформаційній системі організації.

Корпоративна мережа дозволяє створювати єдину базу даних для всіх підрозділів, вести електронний документообіг, організовувати конференц-дзвінки та проводити відеоконференції з віддаленими підрозділами, забезпечувати всі потреби організації в якісному телефонному та факсимільному місцевому, міжнародному та міжміському зв'язку, доступі в Інтернет та інших інтерактивних мережах. Все це скорочує час реагування на зміни, що відбуваються в компанії, і забезпечує найкраще управління всіма процесами в режимі реального часу. У той же час організація в меншій мірі залежить від операторів фіксованого і мобільного зв'язку. Часткова відмова в Послугах цих операторів дозволяє значно знизити витрати організації. Можна передавати будь-яку конфіденційну інформацію виробничого і фінансового характеру, вважаючи, що ніхто не має до неї доступу, крім уповноважених співробітників компанії [15]. Широка ілюстрація корпоративної мережі показана на Рис. 1.1.

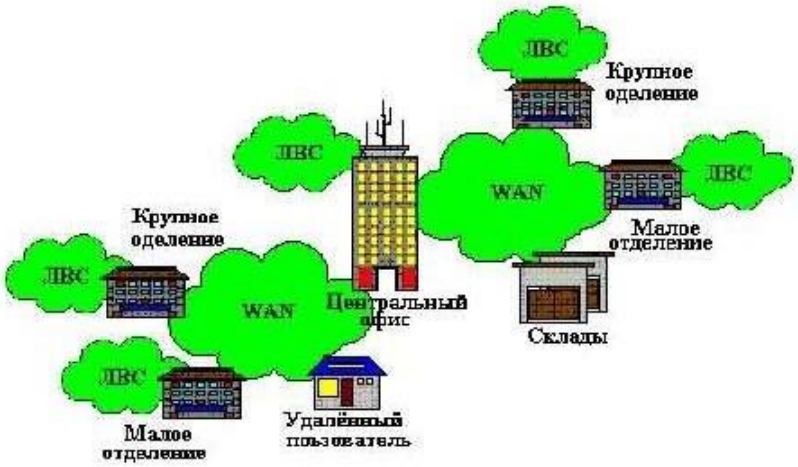


Рисунок.1.1 - Універсальна схема корпоративної мережі

Головне завдання системних інтеграторів і адміністраторів заключається в тому, щоб ця громіздка і неймовірно дорога система максимально обробляла потік інформації, що протікає між співробітниками, і дозволяла їм приймати вчасні і розумні рішення для забезпечення виживання підприємства в умовах жорсткої конкуренції. Оскільки життя не стоїть на місці, зміст корпоративної інформації, інтенсивність її потоку і спосіб її обробки постійно змінюються. Інтернет-транспорт, який може використовуватися практично всіма підприємствами, значно полегшує завдання створення мережі територіальних компаній, в той же час підкреслюючи завдання захисту корпоративних даних, коли вони передаються через надзвичайно загальнодоступну мережу з мільйонами "населення".

1.4 Структура корпоративної мережі

На Рис. 1.2 представлена можлива схема структури корпоративної мережі.

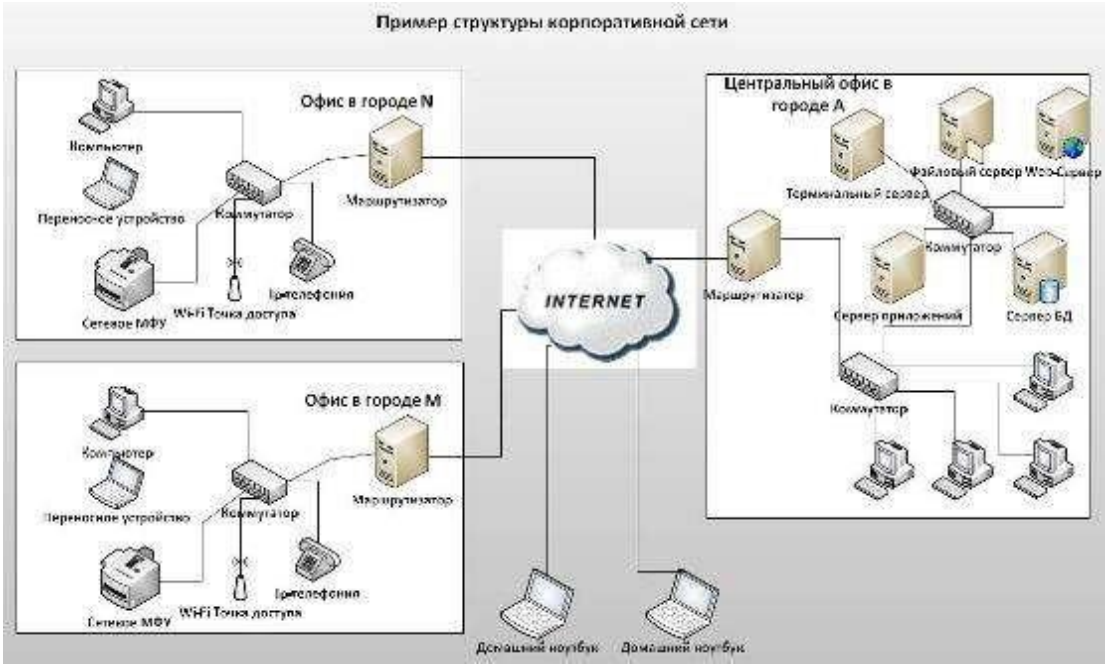


Рисунок 1.2 - Приклад структури корпоративної мережі

Виділимо основні пристрої:

1. Комп'ютер. Під ним мається на увазі стандартне робоче місце, найчастіше підключений до локальної мережі через кабель типу вита пара. На комп'ютері встановлено ПО необхідне для роботи персоналу (офісні додатки,1С, поштові агенти та т.п.), а також засоби для віддаленого адміністрування даного комп'ютера.

2. Переносний пристрій. Це може бути ноутбук, планшет, мобільний пристрій. Найчастіше підключення таких пристроїв до мережі проводиться за допомогою бездротового зв'язку. Несе ті ж функції, що і комп'ютер, але має головна відмінність від стаціонарного комп'ютера - мобільність.

3. Мережеве МФУ. МФУ - багатофункціональний пристрій, що виконуєфункції принтера, сканера, копіра. Підключення до мережі здійснюється шляхом мережевого кабелю. Якщо МФУ не має мережевого порту, то воно підключається до комп'ютера і за допомогою засобів операційної системи відкривається на доступ по мережі іншим користувачам.

4. Wi-fi точка доступу. Пристрій, за допомогою якого створюються бездротові мережі. Використовується для підключення ноутбуків і інших портативних пристроїв, що мають модуль wi-fi. Перевага перед кабельної системою полягає в мобільності і непотрібності протягувати кабель і псувати інтер'єр. Швидкість доступу в залежності від використовуваного стандарту може бути від 50 до 125 Мбіт/сек. Для захисту доступу до мережі є кілька стандартів забезпечення безпеки: WEP, WPA, WPA2 і т.д.

5. Ip-телефони. Система зв'язку, яка забезпечує передачу голосового сигналу через Інтернет або будь-яку іншу IP-мережу. Сигнали по каналу зв'язку передаються в цифровому вигляді і зазвичай перетворюються (стискаються) перед передачею для усунення надмірності.

6. Комутатор-це пристрій, призначений для підключення декількох вузлів комп'ютерної мережі в межах одного або декількох сегментів мережі. Комутатор передає дані тільки безпосередньо одержувачу, за винятком робить

широкомовний трафік (на MAC-адресу FF:FF:FF:FF: FF: FF: FF: FF) на всі вузли мережі. Це посилює продуктивність і безпеку мережі, усуваючи необхідність (і можливість) для інших сегментів мережі обробляти дані, які до них не відносяться.

7. Маршрутизатор. Мережеві пристрої вирішують пересилати Пакети мережевого рівня (Рівень 3 моделі OSI) між різними сегментами мережі на основі інформації про топологію мережі і певних правилах. Простіше кажучи, це пристрій, який з'єднує 2 або більше різних мереж (в нашому випадку локальну офісну мережу та інтернет). Маршрутизатори можуть бути як hardware, так і software. Hardware маршрутизатор-це готовий пристрій, який має основні функції маршрутизатора, вбудовані в його програмну оболонку. Software маршрутизатор-це окремий сервер, зазвичай використовує операційну систему linux/unix, на основі якого за допомогою засобів firewall'a налаштовуються правила маршрутизації і перемикання трафіку. При виборі певного типу маршрутизатора вони в основному керуються кількістю кінцевих користувачів, складністю необхідних норм і необхідної надійністю.

8. Термінальний сервер (terminal server). Сервер, який надає клієнту обчислювальні ресурси (процесорний час, дисковий простір, пам'ять) для вирішення певних завдань. Технічний сервер терміналів-це дуже потужний комп'ютер (або кластер), який підключається до клієнта терміналу по мережі-ці клієнти зазвичай являють собою малопотужні або застарілі робочі станції або служби віддалених користувачів, які використовуються для доступу до сервера терміналів, який сервер терміналів використовує для надання робочого столу.

Переваги термінального сервера

- Зменшення тимчасових затрат на адміністрування;
- Підвищення безпеки - зменшення ризику злому;
- Зниження затрат на програмне та апаратне забезпечення;

У більшості випадків роль операційної системи виконує Microsoft Windows Server.

9. Файловий сервер. Це виділений сервер, оптимізований для виконанняфайлових операцій введення-виведення. Призначений для зберігання файлів будь-якого типу. Зазвичай, має досить великий обсяг дискового простору, і, як правило, файл-сервер обладнаний RAID контролером для забезпечення швидкого запису і читання даних.

10. Web-сервер. Це сервер, який приймає HTTP-потреби від клієнтів, в основному веб-браузерів, і видає їм HTTP-відповіді, зазвичай спільно з HTML-файлом, зображенням, медіа-потоком, сторінкою або іншими даними. На ньому може бути розташований корпоративний сайт або будь-який інший веб-сервіс.

Найчастіше використовується операційна система сімейства linux/unix,так як вони в порівнянні з іншими більш надійні і більш продуктивні. У ролі самого веб-сервера виступає спеціальне програмне забезпечення, наприклад Apache або nginx.

11. Сервер додатків. Це програмна платформа, призначена для ефективного виконання процедур (програм, механічних операцій, скриптів) які підтримують побудову додатків. Сервер додатків діє як набір компонент доступних розробнику програмного забезпечення через API (інтерфейс прикладного програмування) визначений самою платформою.

На підприємстві, дуже часто використовується додаток 1С. У цієї програми є кілька варіантів роботи з базою даних: файловий режим - вся базазнаходиться в одному файлі (має сенс, коли працюють з базою клієнтів не більше 10-15 чоловік), клієнт-серверний режим - база даних знаходиться на sql сервері. У клієнт-серверному режимі користувачі не безпосередньо працюютьз базою даних, а через 1С сервер, який обробляє запити в зрозумілу форму для sql сервера.

Цей режим підвищує продуктивність, надійність, і покращує процеси адміністрування бази даних.

Якраз для таких цілей і існує сервер додатків.

12. Сервер БД. Сервер БД підтримує базу даних разом з даними, відповідає за цілісність і безпеку даних і забезпечує операції введення-виведення, коли клієнти отримують доступ до інформації. Більшість СУБД використовують мову SQL (мову структурованих запитів), оскільки вона спрощує опис логічної підмножини БД.

Призначення SQL:

- Створити базу даних і таблицю з детальним описом її структури;
- Виконання базових операцій з даними (таких як зміна, вставка і видалення даних з таблиць);
- Виконання складних і простих запитів.

Ключовою особливістю мови SQL є те, що він використовується для формування запитів, що описують деяку інформацію, яку необхідно отримати з бази даних, і програма сама вирішує, як вирішити цю проблему[1].

1.5 Віртуальні приватні мережі

1.5.1 Організація VPN

У сучасних умовах розвитку інформаційних технологій, переваги створення віртуальних приватних мереж незаперечні. Перш ніж перерахувати найбільш очевидні і корисні способи організації віртуальних приватних мереж, необхідно привести саме поняття.

Віртуальна приватна мережа або просто VPN (Virtual Private Network) - це технологія, при якій відбувається обмін інформацією з віддаленої локальною мережею по віртуальному каналу через мережу загального користування з імітацією приватного підключення «точка-точка». Під мережею загального користування можна мати на увазі як Інтернет, так і іншуинтрасеть[8].

Віртуальні приватні мережі дозволяють віддаленому користувачу, який пройшов аутентифікацію, скористатися корпоративною мережею нарівні з клієнтами центральної корпоративної мережі.

Центральна мережу будь-якої організації може аутентифікувати користувачів незважаючи на те, що вони отримують доступ через публічну мережу.

Вдало спроектована VPN може принести організації чимало вигоди. Її впровадження дозволяє:

· Розширити географію доступу співробітників до інфраструктури організації;

· Підвищити безпеку передачі інформації;

· Зменшити експлуатаційні витрати в порівнянні з традиційними глобальними мережами;

· Скоротити час передачі інформації і знизити витрати на відрядження;

· Підвищити продуктивність праці;

· Спростити топологію мережі;

· Збільшити мобільність користувачів і дати їм більш гнучкий графікроботи.

Основні властивості VPN:

· Безпеку;

· Надійність;

· Масштабованість;

· Керованість.

Розглянемо варіант організації мережі установи з філіями звикористанням віртуальних приватних мереж (рис. 1.3).

Рисунок 1.3 - Організація мережі установи з філіями звикористанням VPN

Особливості такої організації:

· Швидкість передачі даних. Провайдери можуть забезпечити достатньо високошвидкісний доступ в Інтернет, однак з локальної, перевіреної часом 100 Мбіт мережею він все одно не зрівняється. Але так чи так важливо щодня перекачувати сотні мегабайт інформації через організовану мережу? Для доступу до локального сайту підприємства, пересилання електронного листа з документом цілком достатньо швидкості, якої можуть забезпечити Інтернет-провайдери;

· Безпека переданих даних. При організації VPN передана інформація потрапляє в зовнішню мережу, тому про організацію безпеки доведетьсяподбати заздалегідь. Але вже сьогодні існують досить стійкі до атак алгоритмишифрування інформації, які дозволяють власникам переданих даних не турбуватися за безпеку;

· За організовану мережу нікому не треба платити. Плата за використання Інтернету в наші дні сама по собі досить демократична, а гнучкі тарифи дозволяю вибрати кожному оптимальний пакет;

Масштабованість системи. При відкритті нової філії або додавання співробітника, якому дозволено користуватися віддаленим доступом не потрібно ніяких додаткових витрат на комунікації.

· Гнучкість системи. Для VPN не має значення, звідки ви здійснюєте доступ. Окремо взятий співробітник може працювати з дому, а може під час читання пошти з корпоративного поштової скриньки фірми перебувати у відрядженні в абсолютно іншій державі.

Способи реалізації VPN:

1. У вигляді спеціального програмного та апаратного забезпечення. Реалізація VPN-мережі полягає у використанні спеціального набору програмного та апаратного забезпечення. Ця реалізація забезпечує високу продуктивність і, як правило, має високий ступінь безпеки.

2. В якості програмного рішення.

Використовують персональний комп'ютер із особливим та професійним програмним забезпеченням, що забезпечує функціональність VPN[10].

3. Інтегроване рішення

Функція VPN надає комплексне рішення, яке також вирішує проблеми фільтрації мережевого трафіку, забезпечення якості і обслуговування організації брандмауерів.

Способи організації VPN:

В VPN найбільш доцільно виділити наступні три основні способи:

1. Віддалений доступ окремо взятих співробітників до корпоративної мережі організації через модем або загальнодоступну мережу

Організація такої моделі віртуальної приватної мережі передбачає наявність VPN-сервера в центральному офісі, до якого підключаються віддалені клієнти. Дистанційні клієнти можуть працювати на дому, або, використовуючи переносний комп'ютер, з будь-якого місця планети, де єдоступ до всесвітньої павутини.

Даний спосіб організації віртуальної приватної мережі доцільно застосовувати в разі географічно не прив'язаний доступу співробітників до корпоративної мережі організації.

2. Зв'язок в одну загальну мережу територіально розподілених філій фірми. Цей спосіб називається Intranet VPN.

При організації такої схеми підключення потрібна наявність VPN серверів дорівнює кількості пов'язують офісів.

Даний спосіб доцільно використовувати як для звичайних філій, так і для мобільних офісів, які матимуть доступ до ресурсів головного офісу, а також без проблем обмінюватися даними між собою.

3. Так званий Extranet VPN, коли через безпечні канали доступу надається доступ для клієнтів організації. Набирає широке поширення в зв'язку з популярністю електронної комерції. В цьому випадку для віддалених клієнтів будуть дуже урізані можливості по використанню корпоративної мережі, фактично вони будуть обмежені доступом до тих ресурсів компанії, які необхідні при роботі зі своїми клієнтами, наприклад, сайту з комерційнимипропозиціями, а VPN використовується в цьому випадку для безпечного пересилання конфіденційних даних. Засоби захисту інформації - протоколи шифрування.

4. VPN клієнт/сервер. Він захищає дані, які передаються між двома вузлами корпоративної мережі (не Мережі). Особливістю цієї опції є те, що VPN створюються між вузлами, які зазвичай розташовані в одному і тому ж сегменті мережі, наприклад, між робочими станціями і серверами. Це часто буває, коли Вам потрібно створити кілька логічних мереж в одній фізичній мережі. Наприклад, коли Вам потрібно розділити трафік між фінансовим і кадровим відділами, отримаєте доступ до серверів, що знаходяться в одному фізичному сегменті. Ця опція аналогічна технології VLAN, але замість поділу трафіку вона використовує його шифрування..

1.5.2 OpenVPN

Оскільки дані в віртуальних приватних мережах передаються через загальнодоступну мережу, отже, вони повинні бути надійно захищені від сторонніх очей.

Для реалізації захисту переданої інформації існує безліч протоколів, які захищають VPN, але всі вони поділяються на два види і працюють в парі:

- Протоколи, інкапсулюючі дані і формують VPN з'єднання;
- Протоколи, шифрувальні дані всередині створеного тунелю.

Перший тип протоколів встановлює тунелюватись з'єднання, а другий тип відповідає безпосередньо за шифрування даних. Порівняємо дві реалізації створення VPN на основі стандарту IP sec і OpenVpn.

Для об'єднання в мережу декількох філій сьогодні найбільш часто використовується стандарт IPSec. Слабкі місця IPSec загальновідомі. Складна структура з досить непростий при певних обставинах конфігурацією, різні (в залежності від виробника) реалізації і «дірки» в системі безпеки, проблеми з Firewall'ом - ось лише деякі недоліки, постійно які підстьобують розробку сучасних технологій віртуальних приватних мереж (Virtual Private Network, VPN). Результатом стала поява проекту відкритого програмного забезпеченняOpenVPN. Остання його версія - 2.0 - пропонує набагато більш широкийспектр можливостей, багато в чому перевершують функціональність класичних VPN.

Технологія OpenVPN перетворилася в серйозну альтернативу IPSec. Організації, де не потрібно в обов'язковому порядку застосовуватиIPSec, можуть завдяки OpenVPN без великих витрат отримати численні переваги, раніше недоступні. Опції повсюдної захисту ноутбуків за допомогою центрального корпоративного firewall'a, тунелювання firewall'ов і посередників WWW, а також ретрансляції широкомовного трафіка помітно перевищують функціональний охоплення IPSec, причому використовувані технології (SSL, пристрої Tap/Tun) представляють собою випробувані і перевірені стандарти. OpenVPN стала найсучаснішою і надійної технологією VPN з доступних, при цьому безкоштовної

і дуже простий в налаштуванні.

Зупинимося на технології OpenVPN, щоб познайомитися з нею ближче. Створений в 2002 році, OpenVPN - це інструмент з відкритим вихідним кодом, який використовується для побудови site-to-site VPN мереж з використанням SSL/TLS протоколу або з розділяються ключами. Вінвиконує роль безпечного тунелю для передачі даних через один TCP/UDP порт в незахищеної мережі як Інтернет.

Перевага OpenVPN полягає в легкості інсталяції і настройки, що є рідкісним випадком для таких інструментів.

OpenVPN може бути встановлений практично на будь-яку платформу включаючи: OpenBSD, Windows 2000/XP/Vista, Linux, FreeBSD, Solaris, Mac OS X і NetBSD.

Linux системи повинні працювати на ядрі 2.4 або вище. Принципи конфігурації однакові для всіх платформ.

OpenVPN використовує клієнт/сервер архітектуру. Він повинен бути встановлений на всі вузли VPN мережі, де один вузол повинен бути сервером,а інші клієнтами.

OpenVPN створює TCP або UDP тунель, при цьому дані проходять через цей тунель шифруються. Стандартний порт для OpenVPN - UDP 1194, але можна використовувати будь-який інший TCP або UDP порт. З версії 2.0 один і той же порт можна використовувати для декількох тунелів на OpenVPNсервері.

Можна створити Ethernet (Міст) або IP (маршрутизація) VPN мережу використовуючи відповідні мережеві драйвера TAP або TUN. TAP/TUN доступні на всіх платформах і включені в ядро Linux починаючи з версії 2.4.

Опції докладно описані в сторінках довідкового керівництва (man pages).

При використанні статичних ключів, VPN шлюзи використовують один стандартний ключ для дешифрування і шифрування даних. В цьому випадку

настройка буде досить простий, але при цьому виникає проблема передачі і безпеки ключа. Якщо хтось заволодіє цим ключем, то він може дешифрувати дані.

Для того щоб уникнути цієї проблеми, необхідно використовувати Інфраструктуру Відкритих Ключів (PKI). При цьому кожен вузол володіє двома ключами: відкритий ключ, відомий всім і закритий ключ, доступний тільки його власнику. Таку структуру використовує OpenSSL, інтегрований вOpenVPN, для аутентифікації VPN вузлів перед тим як почати передавати зашифровані дані. Цей режим вважається кращим.

Звернемо увагу на структуру мережі і концепцію безпечних ключів для кращого розуміння OpenVPN.

Протягом багатьох років IPSec був єдиним протоколом який міг забезпечити шифрування даних в site-to-site і клієнт/сервер VPN мережах. На щастя ситуація змінилася з появою SSL протоколу. Призначений для забезпечення безпеки таких протоколів як HTTP, SSL дозволяє зараз забезпечити безпеку для усіх програм і шифрувати TCP або UDP тунелі в site- to-site і клієнт/сервер VPN мережах.

SSL (Secure Sockets Layers) був створений Netscape в 90-х. Було випущено дві версії v2 (1994) і v3 (1995). У 2001 IETF купила і оновила патент. В цей же час SSL був перейменований в TLS (Transport Layer Security).

SSL виконує дві основні задачі:

- Аутентифікація сервера і клієнта по засобом Інфраструктури Відкритих Ключів (PKI).
- Створює шифрування з'єднання між клієнтом і сервером для обміну повідомленнями.

Стандартна модель OSI складається з семи рівнів, в той час як чотирьох рівнева модель найбільш підходить для TCP/IP (рівень додатків, транспортний, мережевий, канальний, фізичний), який використовується величезною кількістю додатків.

SSL розташований між транспортним рівнем і рівнем додатки і буде шифрувати рівень програми.

Робота SSL проходить в 4 етапи:

1. SSL Handshake: Визначається метод шифрування для передачі даних;
2. SSL Change Cipher Spec: Створення і передача ключа між клієнтом ісервером на цю сесію;
3. SSL Alert: Доставка повідомлень SSL про помилки між клієнтом ісервером;
4. SSL Record: Передача даних.

Для шифрування і аутентифікації OpenVPN використовує OpenSSL,який є безкоштовним і поширюється з відкритим вихідним кодом.

Виділимо основні плюси і мінуси цієї технології:

+ Зрілі криптографічні алгоритми (SSL/TLS);
+ SSL/TLS є галузевими стандартами і входять в сферу відповідальності IETF (Internet Engineering Task Force);
+ Проста технологія, проста інсталяція, просте конфігурація;
+ TCP/UDP, для безлічі зовнішніх співробітників потрібен лише один порт;
+ Індивідуальна конфігурація для клієнтів;
+ Гнучкість внаслідок використання пристроїв Tun/Tap;
+ Ніяких проблем з технологією NAT;
+ Швидке повторне підключення, прозорість для DynDNS, сеанс зберігаються;
+ Стиснення;
+ Висока сумісність з firewall'м і посередниками WWW;
+ Продуктивність (досить малопотужних процесорів);
+ Модульна розширюється архітектура;
+ Виконання в просторі користувача - в Linux не потрібні

привілеїадміністратора;

+ Висока продуктивність навіть на старих машинах;

+ Формування трафіку вже включено;

- Ні спеціалізованих пристроїв;
- Дефіцит навченого персоналу;
- Відсутність інтерфейсів Web або інтерфейсів для адміністрування.

1.5.3 SSH

Ще один протокол, за допомогою якого можна створювати VPN - це Secure SHell.

SSH (Secure SHell)-це мережевий протокол рівня сеансу, який дозволяє віддалено управляти тунелюванням операційних систем і TCP-підключенням (наприклад, для передачі файлів). Функціональність аналогічна протоколу Telnet, але, на відміну від них, він шифрує весь трафік, включаючи кодову фразу Для передачі. SSH дозволяє вибирати різні алгоритми шифрування. SSH-клієнти та SSH-сервери для більшої кількості мережевих операційних систем доступні.

SSH дає змогу в незахищеному середовищі безпечно передавати практично будь-який другий мережевий протокол. Таким чином, ви можете не лише працювати на своєму комп'ютері віддалено завдяки командній оболонці, проте ділитись зашифрованими аудіо-або відео потоками (для прикладу, з веб-камери). SSH також може використовувати стислі дані передачі для подальшого шифрування.

Чи реалізована підтримка SSH у всіх системах UNIX? В аналогічних системах і в більшості систем SSH-клієнт і сервер є однією зі стандартних утиліт. Для операційних систем, відмінних від UNIX, існує також безліч реалізацій SSH-клієнтів.

SSH- протокол сеансового рівня. SSH-сервери зазвичай прослуховують з'єднання через TCP-порт 22. SSH аутентифікує сервер за допомогою стороннього

протоколу аутентифікації, заснованого на алгоритмі цифрового підпису RSA або DSA. Цифрові підписи RSA або DSA також можуть використовуватися для аутентифікації клієнтів, але також дозволяють виконувати аутентифікацію з використанням пароля або навіть IP-адреси хоста. Ідентифікація з паролем є найбільш поширеною; він безпечний, тому що пароль передається по каналу, який віртуально зашифрований. Аутентифікація за IP-адресою не безпечна, і ця функція часто відключається. Алгоритм Діффі-Хеллмана (DH) використовується для створення загального ключа (ключа сеансу). Щоб зашифрувати передані дані, використовуються алгоритми симетричного шифрування, Blowfish, AES або 3DES. Використовуйте HMAC-MD5/HMAC-SHA1 для перевірки цілісності переданих даних.

Для стиснення шифрованих даних може використовуватисяалгоритм LempelZiv (LZ77), який забезпечує такий же рівень стиснення, що іархіватор ZIP. Стиснення SSH включається опціонально.

Метод, званий тунелювання SSH, використовується для створення VPN-мережі. SSH-тунель-це тунель з'єднання для шифрування даних тунелю, який створюється за допомогою SSH-. Він використовується для захисту передачі даних в Інтернеті. Особливістю є те, що шифрується на одному кінці SSH-з'єднання і розшифровується на другому кінці не зашифрований трафік будь-якого протоколу.

Фактична реалізація може виконуватись декількома способами:

* Використовуйте програми, які можуть працювати за допомогою тунелірування SSH;

* Створіть тунель VPN, який працює практично з будь-яким додатком;

* Якщо програма працює з певним сервером, є можливість налаштувати SSH-клієнт так, щоб він обходив по SSH-тунелю TCP з'єднання до певного TCP-порту на комп'ютері, на якому SSH-клієнт запущений. Наприклад, за замовчуванням клієнти сервера терміналів підключаються до порту 3389. Потім, щоб встановити з'єднання з сервером через SSH-тунель, SSH-клієнт

налаштований на пересилання з'єднання з певного порту на локальному комп'ютері (до прикладу, порт 5000) на віддалений сервер (до прикладу, порт 3389 і server.com). В цьому випадку клієнт готується на з'єднання до сервера localhost (якщо SSH-клієнт працює на тій самій машині, що і клієнт терміналу) і порту 5000.

Плюси цієї технології створення vpn мереж в тому, що для реалізації не потрібно встановлювати і налаштовувати додатковий софт. Серверна іклієнтська частина зазвичай ставляться разом з unix/linux системою за замовчуванням. Так само варто відзначити, що настройка проходить набагатолегше, ніж у будь-якій іншій технології. Ця технологія, хоча трохи і поступається по продуктивності, але для створення захищених мереж підходить більше ніж протокол IPsec, так як по масштабованості і легкості настроювання каналів він в рази перевершує його.

1.6 Моніторинг корпоративних мереж

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

Терміном моніторинг мережі називають роботу системи, яка при виявленні збоїв повідомляє про них адміністратора за допомогою пейджера, пошти або інших засобівоповіщення і яка надає постійний нагляд за комп'ютерною мережею в пошуках несправних або повільних систем. Ці завдання є підмножиною завдань управління мережею.

Коли система виявлення вторгнень відстежує зовнішні загрози, система моніторингу мережі відстежує мережу на наявність проблем, викликаних перевантаженням і/або збоєм серверів, інших пристроїв або мережевих підключень.

Наприклад, для визначення стану веб-сервера монітор може періодично відправляти HTTP-запити для здобуття сторінок; для поштового сервера тестові повідомлення можуть відправлятися по протоколу SMTP і прийматися по

протоколу POP3 або IMAP[5].

Невдалий запит (для прикладу, коли з'єднання не можливе для встановлення, воно переривається тайм-аутом або коли повідомлення не отримано) в основному викликає відповідь від системи моніторингу. Реакція може бути:

* Надсилання попереджень системним адміністратором;

* Система захисту від збоїв буде активована автоматично, і система тимчасово зупинить проблемний сервер і замінить його резервним сервером доти, поки проблема не буде вирішена.

Крім відмов систем, процесів, устаткування, також стежать і за їх станомв цілому.

Знаючи, який потік інформації проходить через мережевий інтерфейс, можна буде вибрати оптимальний пакет Інтернету у постачальника, заощадивши при цьому не малі гроші. Зараз це досить актуальна проблема, такяк часто в бізнес центрах існує домовленість з провайдером про те, що тількивони мають право давати доступ в Інтернет. Отже, і цінова політика повністю встановлюється провайдером. Ціни абсолютно непорівнянні з тими, що встановлюються в процесі жорсткої конкуренції.

За графіками навантаження на процесор, обсягом займаної оперативної пам'яті, можна судити про достатність ресурсів сервера для задач, виконуваних на ньому. Це дає обгрунтування для поновлення сервера.

Практично у всіх фірмах є великі обсяги інформації, які включають в себе важливі документи, бази даних, архіви і т.д. Втрата цих документівпринесе фірмі великі збитки. Для того щоб завжди мати резервну копію цих файлів, налаштовуються плани резервного копіювання даних. Створюються образи даних і складаються на файл-сервері. За вільним місцем на файл-сервері і за створенням образів теж необхідно налаштовувати стеження.

Стеження найчастіше проводиться за станом серверів, маршрутизаторівта іншого мережевого обладнання. Грамотно налагоджена система моніторингу

може знизити кількість відмов мережі і збільшити її відмовостійкість. У той же час, адміністратори мережі будуть швидко і вчасносповіщені про неполадки.

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

1.7 Постановка завдання

Одне з основних вимог, що пред'являються до постановки і реалізації завдань дипломного проектування, полягає в тому, що всі результати і на їх основі висновки повинні бути отримані в реальних умовах на реальному підприємстві. Це дає можливість надати результатам дипломної роботи практично багато важать. Провівши роботу в реальних умовах, можна реальнооцінити ефективність використовуваних мережевих технологій на основі кількісної оцінки ефективності мережевих каналів.

Коротко опишемо предметну область. Фірма займається продажею саун, лазень і супутніх цьому матеріалів. Складається з офісу, складу і магазинів, територіально рознесених по всьому місту. Всі сервери розміщені у провайдера (колокація), а саме: сервера терміналів, сервер платформи 1 С, сервер бази даних MS SQL і маршрутизатор під управлінням операційної системи CentOs 5.5 з ланцюжками NAT в правилах і P tables.

В основному робота персоналу відбувається на серверах терміналів, що забезпечує деяку централізованість, простоту адміністрування (завжди легше адмініструвати 3 сервера, ніж 50 комп'ютерів) і, за рахунокналаштувань iP tables на маршрутизаторі, безпеку. Підключення йде по протоколу RDP (Remote Desctop Protokol). Так само для роботи постійно потрібно обмін інформацією між офісами. Підприємство працює з конфіденційною інформацією, тому важлива безпека передачі даних. Магазини працюю тільки з серверами, що знаходяться

у провайдера.

В офісі і на складі в якості маршрутизаторів виступає сервер під операційною системою Centos 5.5 з налаштованими ланцюжками nat в iptables. У магазинах стоять звичайні hardware маршрутизатори. На сервера терміналів, 1С сервер, сервер MS SQL 2008 встановлений операційна системаMS Windows 2003 R2.

Для побудови системи, яка має необхідними споживчими властивостямі функціонує в умовах реальних обмежень необхідно вирішити наступні завдання:

1. Створити захищену корпоративну мережу для підприємства;
2. Підключити по захищених каналах магазини до серверів;
3. Оцінити продуктивність створених каналів;
4. Створити систему моніторингу та оповіщення про проблеми з обладнанням корпоративної мережі.

Уявімо структуру проектованої корпоративної мережі підприємства у вигляді, як це показано на рис. 1.4.

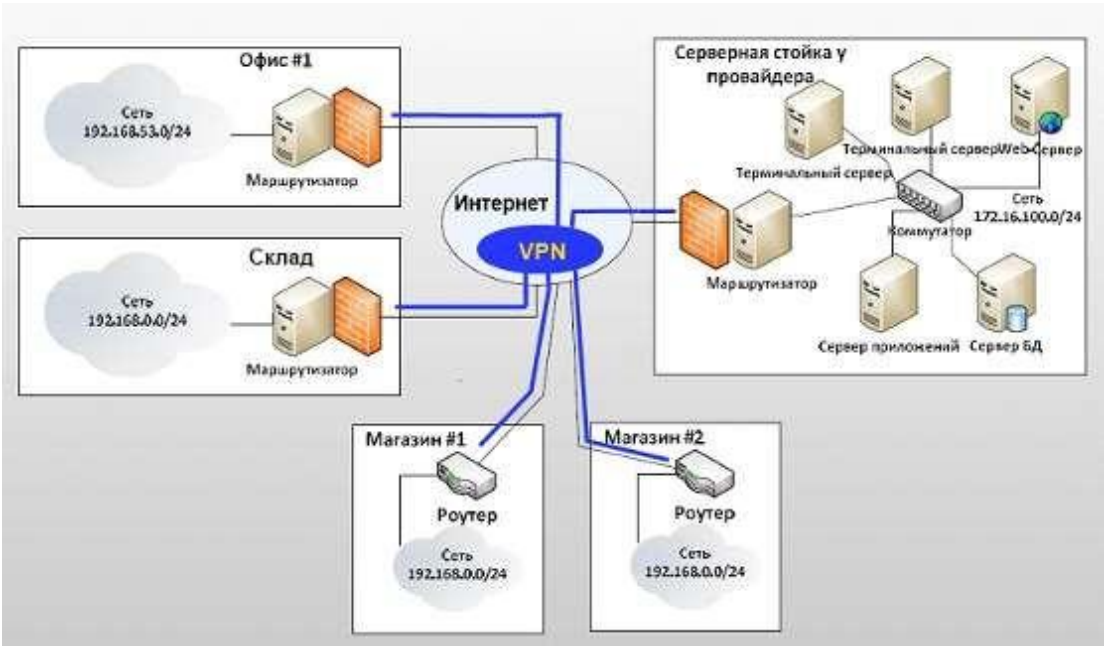


Рисунок. 1.4 - Проектована корпоративна мережа

1.8 Висновки

Отже , корпоративна мережа - це система, що забезпечує передання інформації між різноманітними додатками, що використовуються в системі корпорації. Вона здебільшого, є територіально розподіленою, тобто з'єднує офіси, підрозділи та інакші структури, що знаходяться на великих відстанях один від одного. Вузли корпоративної мережі можуть бути розміщені в різних містах та країнах. Першою проблемою, яку слід вирішувати при формуванні корпоративної мережі є організація каналів звязку. В більшості випадків якісь та безпечність при їх формуванні виявляється доволі невисокою.

Корпоративна мережа - це база для підрозділів, яка забезпечує потреби організацій проводити конференц-дзвінки, відеоконференції, інтернет подачу та здійснення якісних місцевих, міжміських та міжнарожних телефонних звязків, які в меншій мірі залежать від операторів телефонних та фіксальних передач та прийомів сигналів за допомогою технічних засобів електрозв'язку. Таким чином можна передавати будь-яку конфіденційну інформацію, до якої ніхто немає доступу окрім уповноважених співробітників компанії.

У сучасних умовах інформаційних технологій велику перевагу надають віртуальним приватним мережам. Характерною ознакою таких організацій є швидкість та безпека передачі даних. Найголовне, що за цю мережу нікому не потрібно платити та можна працювати з дому, навіть з поштової скринки фірми під час відрядження в будь-якій країні.

Важливі дані, захищають від людського ока завдяки двух видів безпеки, тунельного протоколу, який убезпечує з'єднання з сервером та здійсненням інкапсуляції, тобто кодування даних.

Ще одним важливим протоколом вважають мережовий, який дозволяє відокремлено орудувати тунелірованням операційних систем і TCP-підключенням передачі файлів[9].

Також для незмінності роботи корпоративної мережі, вирішують питання її моніторингу мережі, тобто роботи системи, яка повідомляє про помилки та

несправності адміністратору, за допомогою різних засобів сповіщення і надає неперервний контроль за комп'ютерною мережою в пошуках систем, які вийшли з ладу. Найчастіше проводиться спостереження за станом серверів маршрутизаторів та різноманітних мережових обладнань.

Отже, основні вимоги для постановки та здійснення завдань здебільшого полягає в тому, що всі результати та висновки отримані в дійсних умовах на реальних підприємствах, де постійно відбувається обмін інформацією між офісами та відбувається важлива передача даних з приватною тобто секретною інформацією. Магазини виконують певну роботу тільки з серверами, які розташовані тільки у провайдерах, сам маршрутизатор виступає в офісі та на складі під операційною системою з відповідно налаштованою низкою ланцюжків.

Отож, для кращої побудови системи потрібна захищена корпоративна мережа та вбезпечуваний канал магазинів і серверів, систем моніторингів та сповіщення про проблеми з устаткуванням корпоративної мережі.

РОЗДІЛ 2 ВПРОВАДЖЕННЯ ТЕХНОЛОГІЙ VPN В КОРПОРАТИВНУ МЕРЕЖУ І ЇХ ПОРІВНЯЛЬНА ОЦІНКА

2.1 Реалізація на основі технології OpenVPN

Спочатку об'єднаємо в одну корпоративну мережу офіс, склад і наші сервера у провайдера. Для цього нам потрібно побудувати захищені канали - тунелі тільки між маршрутизаторами, так як немає необхідності підключати кожен комп'ютер окремо.

Отже: є 3 маршрутизатора під управлінням ОС CentOs. Перекидання пакетів з Інтернету в мережу і назад здійснюється за допомогою технології NAT і правил iptables. корпоративний мережу моніторинг сервер

Дамо для зручності маршрутизаторів імена:

- В офісі: Office;
- На складі: Sklad;
- Колокація (провайдерські сервера): Colo;
- Магазин №1: mag 1
- Магазин №2: mag 2

Таблиця 2.1 - Мережеві налаштування маршрутизаторів:

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	-

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	-

Colo:

Мережа	інтерфейс	Ip адреса	маска	Шлюз
нтернет	eth2	195.2.240.68	255.255.255.252	195.2.240.60
локальна	eth1	172.16.100.8	255.255.255.0	-

Закінчення таблиці 2.1

Налаштування hardware маршрутизаторів в магазинах не грають ролі, тому їх пропустимо.

Приступимо до встановлення та налаштування.

CentOS (Community ENTerprise Operating System) - дистрибутив Linux, заснований на комерційному Red Hat Enterprise Linux компанії Red Hat і сумісний з ним. CentOS використовує програму yum для скачування і установки оновлень з репозиторіїв. Вся робота по налаштуванню і установці виробляється віддалено, використовуючи OpenSSH сервер на маршрутизаторах і клієнт putty.

Налаштуємо першим маршрутизатор Colo. Цей маршрутизатор буде виступати в ролі OpenVPN сервера.

Пакет OpenVPN не доступний в стандартному репозиторії, тому підключаємо додатковий репозиторій rpmforge:

colo>rpm-Uhv
http://apt.sw.be/redhat/e15/en/x86_64/rpmforge/RPMS//rpmforge-releasy-0.3.6-1.e15.rf.x86_64.rpm

Ця команда завантажує rpm пакет сховища та встановлює його.Тепер нам став доступний пакет OpenVPN, встановлюємо його:colo> yum install openvpn

OpenVPN встановлений. Далі потрібно згенерувати кореневийсертифікат сервера, сертифікати та ключі клієнтів, сертифікат і ключ сервера,tls ключ.

Для цього переходимо в конфігураційний каталог OpenVPN і створюємо каталог під наші майбутні ключі і каталог під конфігураційні файли клієнтів:

colo>cd/etc/openvpncolo>mkdir keys

colo> mkdir ccd

Завантажуємо змінні для генерації ключів в пам'ять і починаємо генерувати сертифікат авторизації:

colo>./vars colo>./build-ca

Generating a 1024 bit RSA private key

..... ++++++

.. ++++++

writing new private key to 'ca.key'

You are about to be asked to enter information that will be incorporatedinto your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

For some fields there will be a default value,If you enter '.', The field will be left blank.

Країна

Country Name (2 letter code) [US]: RU# Провінція

State or Province Name (full name) [CA]: SPB# Місто

Locality Name (eg, city) [SanFrancisco]: SPB

Назва фірми

Oganization Name (eg, company) [Fort-Funston]: server# Відділення фірми

Organizational Unit Name (eg, section) []: server# Ім'я серверу OpenVPN

Common Name (eg, your name or your server's hostname) [Fort-Funston CA]: server

Name []: server

Email Address [me@myhost.mydomain]:

Сертифікат X.509 створюємо для сервера:

colo>./build-key-server server# Країна

Country Name (2 letter code) [US]: RU# Провінція

State or Province Name (full name) [CA]: SPB# Місто

Locality Name (eg, city) [SanFrancisco]: SPB# Назва компанії

Organization Name (eg, company) [x]: server# Відділення компанії

Organizational Unit Name (eg, section) []: server# Ім'я серверу OpenVPN

Common Name (eg, your name or your server's hostname) []: server# Адреса пошти

Email Address [root @ localhost]:

Please enter the following 'extra' attributesto be sent with your certificate request

Пароль

A challenge password []: 123456789# Назва організації

An optional company name []: server

Далі постане питання про підписуванні сертифіката, погоджуємося. Створюємо для office ключ:

colo>./build-key-server office Generating a 1024 bit RSA private key

..... ++++++

..... ++++++

writing new private key to 'client.key'

You are about to be asked to enter information that will be incorporatedinto your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank

For some fields there will be a default value,If you enter '.', The field will be left blank.

- - - -.

Country Name (2 letter code) [US]: RU

State or Province Name (full name) [CA]: SPB Locality Name (eg, city) [SanFrancisco]: SPB Organization Name (eg, company) [server]: company Organizational Unit Name (eg, section) []: office

Common Name (eg, your name or your server's hostname) []: officeEmail Address [root @ localhost]:

Please enter the following 'extra' attributesto be sent with your certificate request

A challenge password []: 123456789An optional company name []: office

Таким самим способом, створюємо ключі для складу і двох магазинів.

Створюємо ключ Діффі Хельман для обміну ключами по незахищеному каналу:

colo>./build-dh

Створюємо ключ для tls-аутентифікації:

colo> openvpn --genkey --secret keys/ta.key

Після всіх цих маніпуляцій в каталозі keys/з'являються такі файли:

· Ca.crt - Головний сертифікат CA, цей файл необхідний і клієнту, і серверу;

· Dh1024.pem - ключ Діффі Хельман, цей документ необхідний лише серверу;

· Server.crt - Сертифікат сервера, лише для сервера;

· Server.key - Ключ сервера, необхідний лише для сервера (засекречений файл);

· Office.crt, sklad.crt, mag1.crt, mag2.crt - Сертифікати клієнтів, потрібні тільки відповідним клієнтам;

· Office.key, sklad.key, mag1.key, mag2.key - Ключі клієнтів, потрібні

тільки відповідним клієнтам (секретні файли);

· Ta.key - TLS-ключ, потрібен і клієнтам і сервера.

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

На цьому операції з генерацією ключів і сертифікатів закінчені, переходимо до налаштування сервера і клієнтів. Створюємо конфігураційний файл server.conf наступного вмісту:

Порт на якому працює серверport 5000

Протокол udpproto udp

Використовуваний тип пристрою і номерdev tun0

Вказуємо CA файл

ca /etc/openvpn/keys/ca.crt

Вказуємо файл з сертифікатом сервераcert /etc/openvpn/keys/server.crt

Вказуємо файл з ключем серверу

key /usr/local/etc/openvpn/keys/server.key# Вказуємо файл Діффі Хелман

dh /usr/local/etc/openvpn/keys/dh1024.pem

Задаємо IP-адреса сервера і маску підмережі віртуальної мережіserver 10.10.200.0 255.255.255.0

Задаємо маршрути, які передаємо клієнтам, і маску підмережі длятого, щоб вони бачили мережу за OpenVPN сервером

Colo

push "route 172.16.100.0 255.255.255.0"

Office

push "route 192.168.53.0 255.255.255.0"

Sklad

push "route 192.168.0.0 255.255.255.0"

Вказуємо, де зберігаються файли з настройками IP-адрес клієнтівclient-config-dir ccd

Додаємо маршрути сервер-клієнтroute 10.10.200.0 255.255.255.0

Office

route 192.168.53.0 255.255.255.0

Sklad

route 192.168.0.0 255.255.255.0

Дозволяє бачити клієнтам один одного (по віртуальним IP) за замовчуванням клієнти бачать тільки сервер

client-to-client

Включаємо TLS аутіфікаціютls-server

Вказуємо tls-ключ tls-auth keys/ta.key 0

Таймаут до реконектуtls-timeout 120

Вибираємо алгоритм хешуванняauth MD5

Включаємо шифрування пакетівcipher BF-CBC

Перевіряємо активність підключення кожні 10 секунд, якщо протягом120 сек. немає відповіді, підключення закривається

keepalive 10 120

Стиснення трафікуcomp-lzo

Від якого користувача і групи буде працювати OpenVPNuser nobody

group nobody

Чи не перечитувати ключі після отримання SIGUSR1 або ping-restart persist-key

Тримати і перевідкривати TUN \ TAP пристрій, після отримання SIGUSR1 або ping-restart

persist-tun

Логування

status/var/log/openvpn/openvpn-status.loglog /var/log/openvpn/openvpn.log

Рівень інформації для налагодженняverb 3

Створюємо файли з настройками для клієнтів. У каталозі/etc/openvpn/ccd на сервері створюємо файл office, sklad, mag1, mag2 (ім'я файлу - ім'я на яке

видано сертифікат) такого змісту:

office

ifconfig-push 10.10.200.2 10.10.200.1

iroute 192.168.53.0 255.255.255.0

sklad

ifconfig-push 10.10.200.3 10.10.200.1

iroute 192.168.53.0 255.255.255.0

mag1

ifconfig-push 10.10.200.4 10.10.200.1mag2

ifconfig-push 10.10.200.5 10.10.200.1

Цими настройками видали клієнтам з відповідними сертифікатами віртуальні ip адреси, шлюз 10.10.200.1 і задали маршрут через тунель до мережі за клієнтами. Для магазинів маршрут не задано, так як в нашу задачуне входить підключення цих мереж.

На цьому настройка сервера закінчується, запускаємо OpenVPN:colo> service openvpn start

Якщо все правильно, то повинно з'явитися віртуальне tun пристрій:colo> ifconfig tun0

tun0 Link encap: UNSPEC HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00

inet addr: 10.10.200.1 PtP: 10.10.200.2 Mask: 255.255.255.255

UP POINTOPOINT RUNNING NOARP MULTICAST MTU 1500 Metric:

1

RX packets: 9 errors: 0 dropped: 0 overruns: 0 frame: 0

TX packets: 24 errors: 0 dropped: 0 overruns: 0 carrier: 0

collisions: 0 txqueuelen: 100

Якщо пристрій не з'явилося, значить є помилки в конфігураційних файлах. Дивимося лог і усуваємо помилку, далі знову стартуємо.

Переходимо до налаштування клієнтів. Всі конфігураційні файли однакові,

тому розглянемо один з них. На маршрутизаторах office і skladвстановлюємо OpenVPN, так само як і для сервера.

Створимо конфігураційний файл client.conf:dev tun

proto udp

remote 195.2.240.68 # (реальний ip сервера)

port 5000client

resolv-retry infiniteca keys/ca.crt

cert keys/client.crt key keys/client.keytls-client

tls-auth keys/ta.key 1auth MD5

cipher BF-CBC

ns-cert-type servercomp-lzo

persist-keypersist-tun

Додавання маршруту до мережі за сервером. Цей рядок не потрібнадля конфиг. файлів магазинів

up/etc/openvpn_up.sh

status/var/log/openvpn/openvpn-status.loglog/var/log/openvpn/openvpn.log

verb 3

Створимо скрипт openvpn_up.sh для автоматичного додаваннямаршруту:

#!/Bin/sh/Sbin /route add -net 172.16.100.0 netmask 255.255.255.0 gw 10.10.200.1

tun0

На цьому настройка OpenVPN закінчена. Копіюємо ці файли на office і sklad. Далі запускаємо OpenVPN. Якщо не запустився, дивимося логи.

Але на цьому ще 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:

colo> iptables --t nat --A POSTROUTING --s 10.10.200.0/24 --o eth1 --j MASQUERADE

Тепер 3 мережі «бачать» одне одного. Налаштуємо підключення з магазинів до серверів. На комп'ютерах в магазинах, варто операційна система Windows XP. Беремо з офіційного сайту дистрибутив OpenVPN і встановлюємо. Потім в установленому каталозі в папку config кладемо наші ключі і конфігураційний файл mag1. Після цього можна запускати.

На цьому етапи настройки завершені. Маючи захищену корпоративну мережу, можна підключатися безпосередньо до серверів. Перевірити шифрування можна, прослухавши трафік на одному з роутерів командою TCPDUMP.

Приклад виведення нешифрованих трафіку:

18: 27: 15.752295 IP cl230-175-182-213.cl.metrocom.ru.40887> 195.2.240.68.ssh:. 2826496: 2827944 (1448) ack 1009 win 10080 <nop, nop, timestamp 2791385847 256970382>

18: 27: 15.752347 IP 195.2.240.68.ssh> cl230-175-182-213.cl.metrocom.ru.40887:. ack 2783056 win 65535 <nop, nop, timestamp 256970382 2791385774, nop, nop, sack 1 {2785952: 2827944}>

18: 27: 15.755042 IP cl230-175-182-213.cl.metrocom.ru.40887> 195.2.240.68.ssh:. 2827944: 2829392 (тисячі чотиреста сорок вісім) ack 1009 win 10080 <nop, nop, timestamp 2791385850 256970382>

18: 27: 15.755096 IP 195.2.240.68.ssh> cl230-175-182-213.cl.metrocom.ru.40887:. ack 2783056 win 65535 <nop, nop, timestamp 256970382 2791385774, nop, nop, sack 1 {2785952: 2829392}>

Приклад зашифрованого:

18: 24: 18.247960 IP 195.2.240.68.sieve> cl230-175-182-213.cl.metrocom.ru.sieve: UDP, length 113

18: 24: 18.248040 IP 195.2.240.68.sieve> cl230-175-182-213.cl.metrocom.ru.sieve: UDP, length 113

18: 24: 18.250915 IP cl230-175-182-213.cl.metrocom.ru.sieve>

195.2.240.68.sieve: UDP, length 1 441

18: 24: 18.251291 IP 195.2.240.68.sieve> cl230-175-182-

213.cl.metrocom.ru.sieve: UDP, length 113

2.2 Реалізація на основі технології SSH

2.2.1 SSH -туннель

Припустимо, що офіс, склад і магазини (інформація про мережу в пункті2.1) працюють тільки на серверах в термінальному режимі. Тоді існує дуже простий, а найголовніше швидкий спосіб організації VPN тунелю. За допомогою пакета OpenSSH на software маршрутизаторах можна робити шифрований канал тільки по одному потрібного порту. Для роботи з термінальним сервером, клієнти використовують протокол RDP, який використовує 3389 порт (схема такої роботи представлена на малюнку 2.1). Синім, відзначений ssh-тунель, по якому буде працювати RDP протокол.

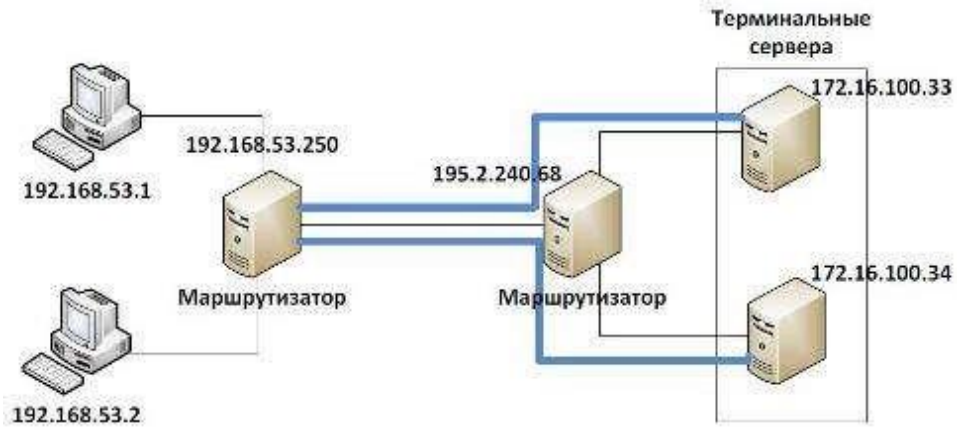


Рисунок.2.1 - Використання ssh-тунелів

Реалізація, як говорилося раніше, дуже проста, тільки у OpenSSH є недолік: при великому просте каналу він рветься. Але і для цієї проблеми є просте рішення. Пакет autoSSH, по додатковому порту при просте шле heartbeat пакет і канал не падає. Створимо 2 каналу до двох термінальнихсерверів:

colo> export AUTOSSH_DEBUG = 1 colo> export AUTOSSH_GATETIME = 0colo> export AUTOSSH_PORT = 20037

colo> autossh -f -N -g -l root -L 1002: 172.16.100.33: 3389 195.2.240.68

colo> export AUTOSSH_PORT = 20040

colo> autossh -f -N -g -l root -L 1002: 172.16.100.34: 3389 195.2.240.68

Розглянемо команди докладніше:

colo> autossh -f -N -g -c aes256 -l root -L 1002: 172.6.100.33: 3389 195.2.240.68

параметри:

- -F: Працювати в фоновому режимі, а не підключатися на хост;
- -N: Чи не виконувати віддалені команди;
- -G: Дозволяє підключення віддалених хостів;
- -C: Включаємо шифрування;
- -L: Ім'я користувача, від якого підключаємося до сервера;
- -L Прописуємо, який локальний порт використовуємо для підключенняі на який сервер і порт підключаємося.

На цьому настройка шифрованого тунелю закінчена і можна працювати! Якщо нам потрібно додати ще один тунель, то за допомогою команди export AUTOSSH_PORT = 20050 додаємо ще один порт для посилки heartbeat пакетів і прописуємо ту ж команду підняття ssh тунелю, але вже з іншим портом.

2.2.2 SSH VPN

Реалізуємо ту ж схему корпоративної мережі, яку створювали за допомогою пакета OpenVPN, але вже за допомогою вбудованого в linux системи пакета OpenSSH. Нам вистачить розглянути з'єднання 2-х мереж, так як для підключення ще одного постачальника послуг потрібно буде провести ті ж самі дії.[13]

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

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

Спочатку потрібно дописати в конфігураційний файл OpenSSH рядки, що він має право створювати пристрої tun/tap і заходити з правами root. У файлі конфігурації/etc/ssh/sshd_config, повинні стояти такі опції:

PermitRootLogin yesPermitTunnel yes

У нас є дві мережі, мережа office з адресою 192.168.53.0/24 і мережу coloз адресою 172.16.100.0/24. Для створення захищеної VPN мережі потрібно виконати наступні дії:

1. Підключитися з одного маршрутизатора через SSH на інший з опцією -w;
2. Налаштування IP адреси SSH тунелю робиться раз на сервері і на клієнті.
3. Додати маршрут для обох мереж.
4. Якщо потрібно, включити NAT на внутрішньому інтерфейсі шлюзу.

Будемо підключатися 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 wc параметрами 0: 0 говоримо, що при підключенні створити на клієнті і сервері віртуальні пристрої tun0. Параметр - c включає шифрування, параметр -C стиснення трафіку.

office> ssh -c aes256 -C -w0: 0 root@195.2.240.68

Наступні команди вже виконуються на маршрутизаторі мережі colo. Задаємо ip адресу і маску підмережі

colo> ifconfig tun0 10.0.1.1 netmask 255.255.255.252# Додаємо маршрут до мережі office

colo> route add -net 192.168.53.0 netmask 255.255.255.0 dev tun0# Включаємо NAT, якщо не включений

colo> echo1>/proc/sys/net/ipv4/ip_forward

Прописуємо основному за рахунок коштів iptables для перекидання пакетів з VPN мережі в реальну

colo> iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADEТепер налаштуємо машрутізатор office:

office> ifconfig tun0 10.0.1.2 netmask 255.255.255.252

office> route add -net 172.16.100.0 netmask 255.255.255.0 dev tun0office> echo 1> / proc / sys / net / ipv4 / ip_forward

office> iptables -t nat -A POSTROUTING -o eth1 -j

На цьому настройка закінчена, VPN мережа побудована. Дляпідключення окремих комп'ютерів з операційною системою Windows XP (магазини), використовується клієнт SSH Put ty.

2.3 Оцінка продуктивності каналів корпоративної мережі

У розділах 2.2.1 і 2.2.2 розглянуті дві технології (OpenVPN, SSH) створення захищених корпоративних мереж, використовуючи VPN. На сьогоднішній день технологія OpenVPN лідирує на ринку побудови захищених мереж, в той час як тунелірування за допомогою SSH тільки починає входити в повсякденність. Для того щоб зрозуміти яку технологію необхідно застосувати в реальних умовах при конкретних вимогах, пропонованих корпоративної мережі, потрібно оцінити їх продуктивність і обгрунтувати їх переваги і недоліки. [3]

Почати слід з продуктивності захищених каналів. На рис. 2.2 представлена побудована корпоративна мережа, продуктивність захищених каналів якої, використовуючи програму iPerf, необхідно оцінити. За допомогою клієнтської частини генерується трафік і відправляється на серверну частину. При отриманні даних генерується звіт про швидкістьпередачі даних.

2.3.1 Оцінка продуктивності при використанні технології

OpenVPN Для побудови графіків продуктивності каналу створеного за допомогою OpenVPN будемо використовувати дані, отримані при тестуванні з додатка 1.

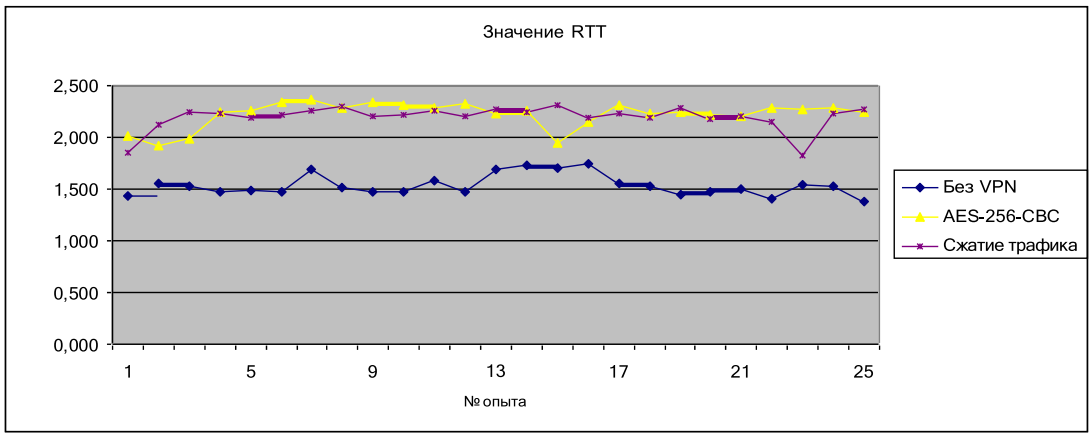


Рисунок 2.2 - Графіки значень RTT

На рис. 2.2 представлені графіки значень RTT. З них видно, що різницяміж каналом без VPN і каналом з використанням VPN, не є суттєвою. Також включення опції стиснення не впливає на час відгуку.

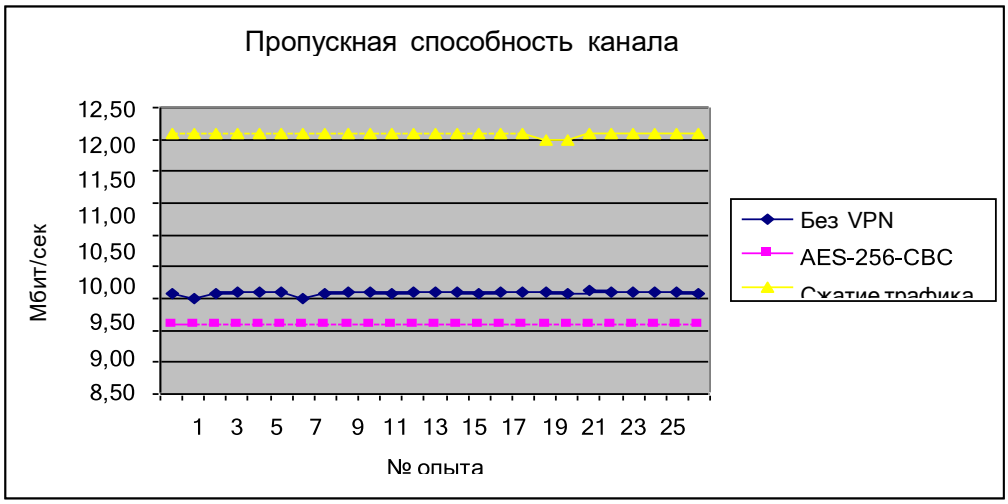


Рисунок 2.3 - Графіки пропускної здатності каналу

На рис. 2.3 представлені графіки пропускної здатності каналу, з яких можна зробити наступні висновки:

· При використанні створеного каналу VPN з шифруванням за допомогоюключа AES-256-CBC втрата в продуктивності 0,5 Мбіт /секунду, що склало 5,1%від каналу без використання VPN;

· При включенні стиснення шифрованого трафіку спостерігаємо прирістшвидкості в 3 Мбіт/сек, що склало 32.9%.

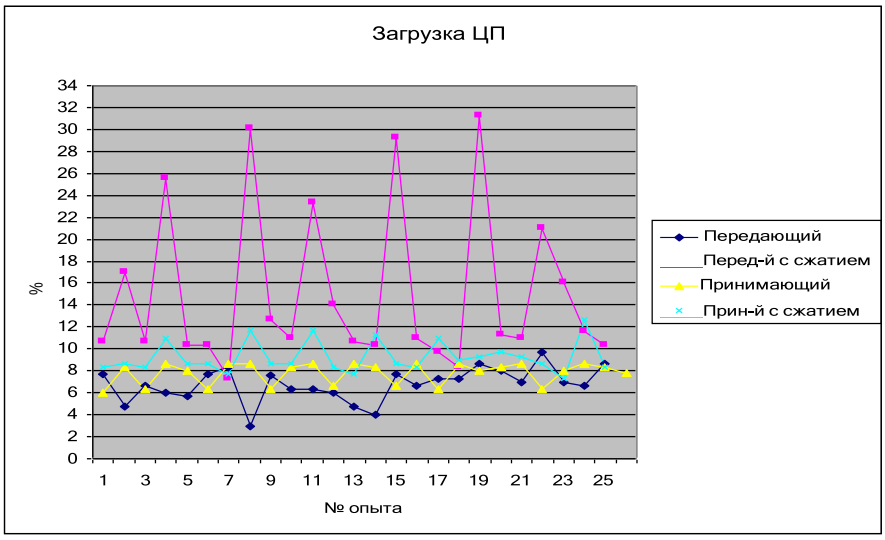


Рисунок 2.4 - Графіки завантаження ЦП

На рис. 2.4 представлені графіки завантаження ЦП на маршрутизаторах при використанні OpenVPN з шифруванням трафіку, при включеному і вимкненому стисненні. За середнім значенням завантаження, як і належало, найвищу навантаження дає шифрування трафіку з використанням стиснення - 14.992%.

Грунтуючись на отриманих графіках, зробимо оцінку продуктивності каналів VPN, побудованих за допомогою OpenVPN.

1. Критерій «Завантаження ЦП» при отриманих значеннях є несуттєвим, оскільки це маршрутизатор і інших процесів вимагають велике споживання ЦП;

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

3. На графіках пропускної здатності каналів можна спостерігати падінняшвидкості при використанні коштів VPN на 0,5 Мбіт/сек в середньому. В даний час це не є суттєвим, так як Інтернет-провайдери надають свої послугина великих швидкостях, де таке падіння не буде грати великої ролі.

4. При використанні стиснення трафіку видно помітний приріст до пропускної здатності каналу, на 3 Мбіт/сек. Звичайно при цьому сильнозростає завантаження на ЦП, але як говорилося раніше, це не грає великої ролі.Підведемо підсумки. Створюючи захищену корпоративну мережу на основі технології OpenVPN, отримуємо одну загальну мережу на кілька офісів з шифрування переданих даних і приростом швидкості за рахунок стиснення трафіку з зручністю обміну інформацією. Технологія OpenVPN повністювиправдовує себе. Її використання веде до зростання продуктивності праці зінформацією по мережі. З мінусів виділяється деяка складність настройки і створення VPN мережі. З плюсів - кроссплатформеність.

Оцінка продуктивності при використанні технології SSH

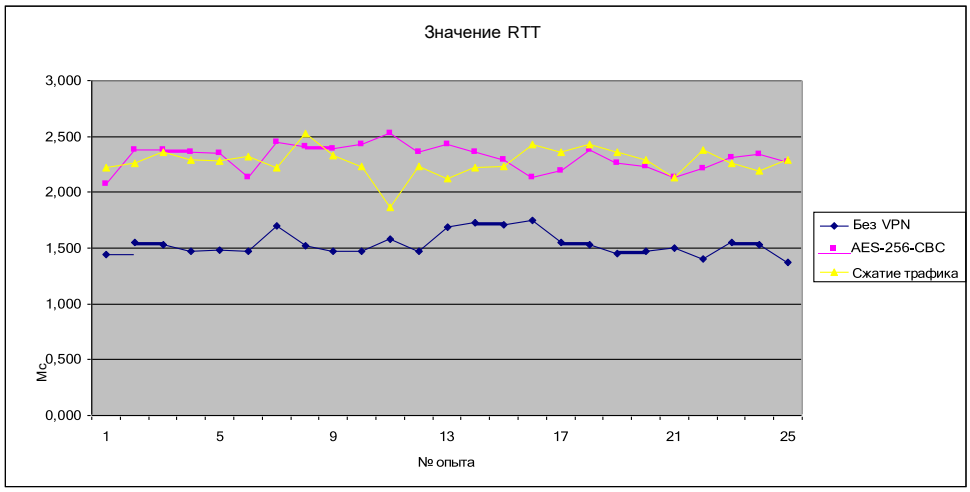


Рисунок 2.5 - Графіки значень RTT

Для побудови графіків продуктивності каналу створеного за допомогою SSH будемо використовувати дані, отримані при тестуванні з додатка 2.

На рис. 2.5 представлені графіки, за якими можна судити про час відгуку при роботі ssh. В середньому час збільшилася на 0.8 мс. Це значення не є

критичним навіть для самих вибагливих програм.

На рис. 2.6 представлені графіки пропускної здатності каналу. Результати вийшли приблизно такими ж, що і при використанні OpenVPN.

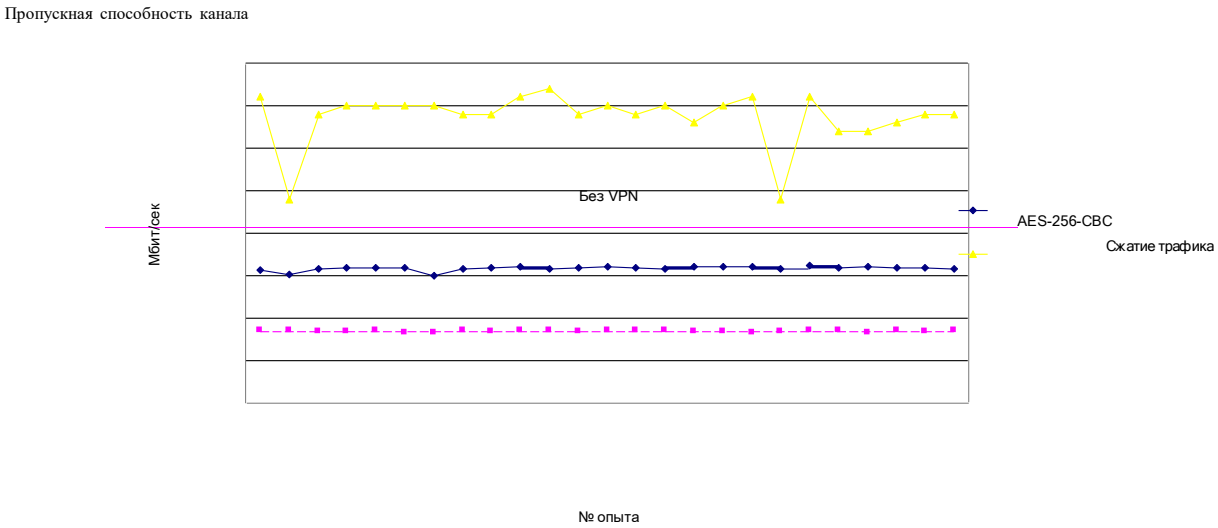


Рисунок 2.6 - Графіки пропускної здатності каналу

2.3.2 Вибір між технологіями SSH і OpenVPN

Складемо порівняльну таблицю, опираючись на отримані дослідним шляхом дані.

Таблиця 2.2 - Порівняльна таблиця SSH і OpenVPN

	OpenVPN	SSH
Складність створення	Досить складна настройка. Складність настройки маршрутизації длядекількох мереж, можливі труднощі з firewall.	Легка настройка, яка не потребує особливих знань. На все створення йде не більше 10 хвилин.

Масштабованість	Підключення ще однієї мережі або клієнта, тягнеза собою зміну конфігураційних файлівна сервері і додавання їхна клієнта. За рахунок OpenVPNклієнта під Windows маєперевагу перед SSH. Не вимагає навчанняперсоналу.	Для підключення ще однієї мережі потрібно повторити ті ж дії, що і при об'єднанні попередніх. Для підключення Windows комп'ютерів, потрібно одноразове навчання персоналу.
Продуктивність	За рахунок стисненняможна добитисявідмінних результатів, що перевищуютьвихідну сполуку. Стиснення йде вибірково, тобто що стиснути можна - пропускається. Це зменшує навантаженняна ЦП.	Продуктивність трохи нижче, ніж у OpenVPN. Стискається весь трафік – великі навантаження на ЦП.
Завантаження ЦП	В середньому не більше 15%	В середньому не більше 38%
Кросплатформеність	Так	Так
RTT	На 0,5 мс більше, ніж у вихідного з'єднання	На 0,8 мс більше, ніж у вихідного з'єднання
Документація	Маса документації на офіційному сайті. Численні форумита обговорення.	Документація є в вбудованому довіднику. Інформації по налаштуванню поки що мало.
Доп. можливості	-	Створення ssh-тунелів.

Впровадження в сущ. мережа	Можуть бути проблеми з налаштуванням firewall'a.	Легке впровадження.
Захищеність	Шифрація 256 бітовим AES ключем	Шифрація 256 бітовим AES ключем
Поширеність	Лідируюча технологія створення VPN мереж.	Сам протокол ssh існує дуже давно, але створення ssh VPN мереж на сьогоднішній день зустрічається рідко.

Закінчення таблиці 2.2

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

2.4 Висновки

Для реалізації технології OpenVPN, все об'єднуємо в одну корпоративну мережу, та будуємо захищені канали. Згадане з' єднання створене для кодуванням, яке необхідне у роботі між двома клієнськими машинами, VPN серверами для спільної роботи кількох клієнтів. З приводу реалізації на основі SSN технологій то вони бувають різноманітними Найпростішим та найшвидшим способом організації тунелю є маршрутизатор, який потрібно робити за допомогою кодового каналу по одному потрібному порту. Даний процес здійснюють для віддаленого керування комп'ютером і тунелювання TCP - з' єднань, для передачі файлів. SSH також дозволяєвибирати різноманітні види кодування, криптографічною безпекою протоколу SSH- який не є фіксований.

Отже, продуктивність при використанні стиснення трафіку зросла приблизно на 25%, але при цьому значно зросло навантаження на ЦП. З переваг

цієї технології хочеться виділити можливість створення ssh-тунелів по окремих портів, що за певних умов дає безліч плюсів, наприклад, можливість мати автоматичне включення резервного каналу, при відсутності зв'язку на одному з маршрутизаторів. Також потрібно відзначити простоту створення і налаштування VPN мережі, кроссплатформенность, висока надійність, легка масштабованість.

РОЗДІЛ 3 СТВОРЕННЯ КОМПЛЕКСУ СИСТЕМ КОРПОРАТИВНОЇ МЕРЕЖІ

3.1 Спостереження за станом серверів та мережевого обладнання. Nagios

Nagios - гнучка система моніторингу роботи серверів. В основному її використовують для моніторингу великої кількості серверів. Nagios - це комп'ютерна система з відкритим вихідним кодом і програма моніторингу мережі. Він використовується для моніторингу, моніторингу стану обчислювальних вузлів і служб, повідомлення адміністраторів, якщо будь-які служби припиняють або відновлюють роботу. У нашому випадку, будемо стежити за маршрутизаторами, серверами і процесами, запущеними на них. Систему Nagios для зручності настройки поставимо на маршрутизатор colo.

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

Встановлюємо компілятор мови C, його бібліотеки і графічні інструменти

colo> yum install gcc glibc glibc-common gd gd-devel# Встановлюємо web-сервер Apache

colo> yum install httpd

Створюємо користувача і групу з правами яких буде працювати nagios

colo> useradd -m nagios

colo> groupadd nagcmd

Створюємо пароль для користувачаcolo> passwd nagios

Додаємо nagios і apache в одну групу, щоб не було проблем з правамина запуск скриптів на web-сервері

colo>/usr/sbin/usermod -a -G nagcmd nagios colo>/usr/sbin/usermod -a -G nagcmd apacheСтавимо систему:

Скачиваем останню версію системи і модулі до неї

colo> wget http://osdn.dl.sourceforge.net/sourceforge/nagios/nagios-3.2.1.tar.gz

colo>wget http://osdn.dl.sourceforge.net/sourceforge/nagiosplug/nagios-plugins-1.4.15.tar.gz

Розпаковуємо архів, що скачав і переходимо в каталогcolo> tar xzf nagios-3.2.1.tar.gz

colo> cd nagios-3.2.1

#Конфігуріруем інсталяційний пакет і перевіряємо задоволення залежностей

colo>./ configure

Якщо все добре, пройшло без помилок, збираємо пакет і встановлюємо colo> make all

colo> make install colo> make install-init

colo> make install-config

colo> make install-commandmode

Прописуємо настройки в Apachecolo> make install-webconf

Проробляємо ті ж дії для додаткових модулівcolo> tar xzf nagios-plugins-1.4.11.tar.gz

colo> cd nagios-plugins-1.4.11colo>./ configure

colo> make

colo> make install

Ставимо пароль на вхід в web-інтерфейс за допомогою утилітиhtpasswd

colo> htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin# Перевіряємо правильність конфігураційного файлу

colo> / usr / local / nagios / bin / nagios -v /usr/local/nagios/etc/nagios.cfg# Якщо помилок і попереджень немає, запускаємо Nagios і Apache colo> service nagios start

colo> service httpd restart

Перевірити те, що система запрацювала, можна зайшовши на web-інтерфейс: http://ip.адрес.сервера/nagios. У нашому випадку ip-адреса: 195.2.240.68. Якщо сервер Apache запущений і сайт системи nagios в конфігураційний файл прописаний вірно, то повинні побачити сторінку авторизації. Після введення зв'язки логін-пароль має відкритися сторінка вітання Nagios. Якщо з якоїсь причини цього не сталося, дивимося помилки в логах apache в каталозі/var/log/httpd.

Розглянемо навігаційне меню:

· Home - Сторінка вітання. Можна дізнатися про можливі оновленнясистеми;

· Documentation - Велика кількість документації по налаштуванню системи;

· Tactical Overview - Являє собою збір короткої інформації про об'єкти,за якими ведеться моніторинг;

· Map - Показує карту мережі, відзначаючи зеленим кольором працюютьсервера і червоним відключені (рис. 3.1);

· Hosts - Показує стан кожного об'єкта, що спостерігається в окремо

· Services - Показує стан запущених процесів на серверах, а також RTT,кількість вільного місця, завантаження процесора і пам'яті (рис. 3.2);

· Event log - Звіти системи моніторингу.

Всі інші пункти меню є різновидами вищеперелічених, додаючи зручності перегляду інформації, наприклад розбита по групах.

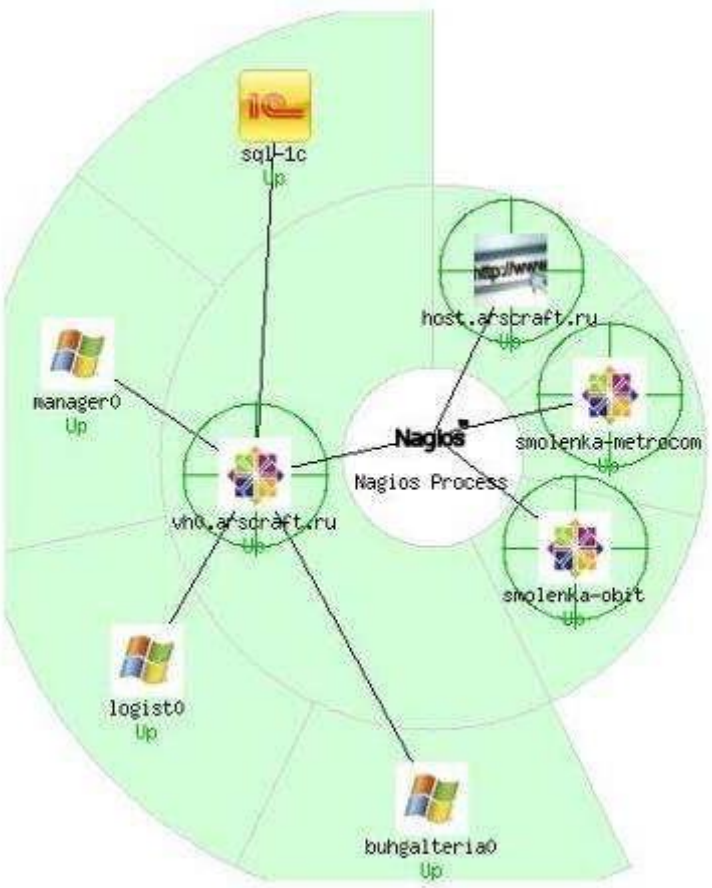


Рисунок 3.1 - Подання пункту меню Map

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 настроюються методи спостереження і об'єкти, за якими стежимо. Розташовані ці файли в директорії/usr/local/nagios/etc.

Розглянемо їх докладніше:

1. nagios.cfg - Головний конфігураційний файл. У ньому описано, де лежать інші файли, оголошені змінні, налаштовується система логів, під яким користувачем працювати і т.д.;
2. commands.cfg - Файл, в якому описані команди для опитування серверів про їх працездатності, запущених процесів і т.д.;
3. contacts.cfg - Описано контакти, яким треба посилати оповіщення системи про збої на серверах;
4. groups.cfg - Описуються групи і сервера, які в них входять;
5. hosts.cfg - Описується шаблон у доданому обладнання. У ньому вказується період опитування серверів, час відсилання попереджень;
6. WindowsServer.cfg - Приклад опису Windows сервера;
7. LinuxServer.cfg - Приклад опису Linux сервера.

Опитування серверів йде по протолку SNMP (Simple Network Management Protocol - протокол легкого керування мережами). Для спостереження за Windows серверами, потрібно додатково поставити програму Nsclient ++.

Розглянемо приклад конфігураційного файлу Windows сервера:define host

{

Використовуємо шаблон, створений заздалегідь use generic-host;

Ім'я сервера host_name sql-1c;

Альяс на ім'я (псевдонім)alias sql-1c;

Вказуємо, чи є перед цим сервером ще один сервер. Це потрібно для деревовидного уявлення мережі

parents vh0.arscraft.ru;# Ip адреса сервера

address 172.16.100.34; IP address of the host

Іконка для відображення в web-інтерфейсі. необов'язковий параметр icon_image 1c.jpg

statusmap_image 1c.jpg

Додаткову інформацію про сервер можна записати тутnotes_url http://vh0.arscraft.ru/nagios/notes/info-sql1c.txt

}

Оголошуємо сервіси, за якими будемо стежити. Так як це 1С і sql сервер, будемо стежити за працездатністю цих процесів, а також занавантаженням на процесор.

Стежимо за 1С процесомdefine service {

use generic-service host_name sql-1c service_description Ragent

check_command check_nt! PROCSTATE! -d SHOWALL -l ragent.exe

}

Стежимо за sql процесомdefine service {

use generic-servicehost_name sql-1c

service_description SQL-Server

check_command check_nt! PROCSTATE! -d SHOWALL -l sqlservr.exe

}

Стежимо за навантаженням на процесорdefine service {

use generic-service host_name sql-1c service_description CPU Load

check_command check_nt! CPULOAD! -l 5,80,90

}

Додавання Linux-сервера нічим не відрізняється від Windows. Далі додаємо файли серверів, за якими будемо стежити, і перевіряємо всі конфігураційні файли на правильність командою [14]:

colo>usr/local/nagios/bin/nagios -v/usr/local/nagios/etc/nagios.cfg

Якщо помилок і попереджень немає, перезавантажуємо Nagios: colo> service nagios reload

Можна зайти на сайт і подивитися що вийшло.

На цьому загальна настройка закінчується, але можна продовжувати налаштовувати систему під свої потреби.

Систему оповіщення можна налаштовувати для кожного сервера і процесу по-різному, в залежності від завдання. При спрацьовуванні умови на пошту системного адміністратора приходить лист наступного змісту:

***** Nagios ***** Notification Type: PROBLEMHost: 1c-sql

State: DOWN

Address: 172.16.100.34

Info: (Host Check Timed Out)

Date / Time: Tue Apr 12 9:43:56 MSD 2011

В результаті установки і настройки системи Nagios з'являються такі можливості моніторингу корпоративної мережі:

· Моніторинг служб мереж (POP3, SMTP, HTTP, ICMP, NNTP і т.д.);

· Моніторинг працездатності хоста (завантаження процесора, використання диска, системні журнали) в переважній кількості мережевих операційних систем;

· Проста архітектура модулів розширення (плагінів) дозволяє легко розробляти власні методи тестування сервісів з використанням будь-якої мови програмування за вашим вибором (Shell, C++, Perl, Python, PHP, C# і т.д.).;

· Перевірка паралельної служби;

· Можливість визначення ієрархії вузлів мережі за допомогою наступних методів

· "Батьківський" хост, який дозволяє ідентифікувати і розрізняти відмовив хост і недоступний хост;

· Надсилання повідомлення при виникненні проблем із хостом або службою (SMS, поштою або будь-яким іншим способом, який визначає користувач через модуль системи)

· Змога визначати обробники подій, що відбулися із хостами або службами для попереджувального вирішення проблем;

· Автоматичне обертання файлів журналів;

· Змога організації загальної роботи кількох систем моніторингу для збільшення надійності та формування розподіленої системи моніторингу;

· Включає утиліту nagiostats, яка відображає загальне зведення по всім хостам, за якими ведеться моніторинг.

Переваги використання системи Nagios для моніторингу за корпоративною мережею незаперечні. Системний адміністратор завжди буде в курсі стану серверів і в найкоротші терміни зможе попередити або усунути проблему. Установка і настройка для обслуговуючого персоналу не повинна бути складною.

3.1 Спостереження за продуктивністю серверів. Cacti

Cacti - open-source веб-додаток, система дозволяє будувати графіки за допомогою RRDtool. Cacti збирають статистику за певні проміжки часу і дозволяють відображати їх графічно. Більшість стандартних шаблонів використовуються для відображення статистики завантаження процесора, виділення оперативної пам'яті, кількість 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 можливунеобхідність upgrad'a сервера і оптимізації робіт в пікові години для зниженнянавантаження.

Встановлювати і налаштовувати систему будемо на маршрутизатор colo. Система Cacti вимагає великої кількості додаткового ПЗ. Веб-сервер у нас фільтром, і цей пункт пропускаємо і починаємо установку:

Встановлюємо додаткове ПО: Mysql, php, perl і бібліотеки для них

colo> yum install mysql mysql-server mysql-devel httpd httpd-devel php php-mysql php-gd phpimap

php-ldap php-odbc php-pear php-xml php-xmlrpc php-mcrypt curl curl-develperl-lib libxml2 php-mbstring phpmyadmin

Запускаємо mysql. Одночасно відбувається його конфігурація

colo> service mysqld start

Переходимо до установки Cacti:

Встановимо залежності потрібні Cacti

colo> yum install -y net-snmp net-snmp-utils rrdtool php-snmp

Додаємо в автозавантаження і запустимо сервіс SNMP colo> chkconfig snmpd on

colo> service snmpd start

Скачиваем пакети Cacti:

colo> wget www.cacti.net/downloads/cacti-0.8.7g.tar.gz

colo> wget www.cacti.net/downloads/pia/cacti-plugin-0.8.7g-PA-v2.9.tar.gz# Разархівіруем їх

colo> tar -xzvf cacti-0.8.7g.tar.gz

colo> tar -xzvf cacti-plugin-0.8.7g-PA-v2.9.tar.gz

Створюємо робочу папку Cacti на сервері colo>mkdir/var/www/cacti

Копіюємо вміст розпакованої папки Cacti в робочу папку Cacticolo> cp -rf cacti-0.8.7g/*/var/www/cacti/

Створюємо в системі користувача для Cacti і дамо йому відповідні права

colo> useradd -c CactiUser -d/var/www/cacti/-s/sbin/nologin cactiusercolo> chown -R cactiuser/var/www/cacti/log/var/www/cacti/rra

Створюємо базу даних для Cacti з привілеями для cactiuser:colo> mysql -u root -p

Enter password:

Welcome to the MySQL monitor. Commands end with; or\g.Your MySQL connection id is 55

Server version: 5.0.77 Source distribution

Type 'help;' or '\ h' for help. Type '\ c' to clear the buffer.mysql> create database cacti;

mysql> GRANT ALL ON cacti. * TO cactiuser @ localhost IDENTIFIEDBY 'password';

mysql> flush privileges;mysql> quit

Імпортуємо структуру Cacti в її базу

colo> mysql -u cactiuser -p cacti </var/www/cacti/cacti.sql Enter password: (password)

Налаштовуємо доступ Cacti в її базу даних colo> nano /var/www/cacti/include/config.php

$ Database_type = "mysql";

$ Database_default = "cacti";

$ Database_hostname = "localhost";

$ Database_username = "cactiuser";

$ Database_password = "password";

$ Database_port = "3306";

#Переходимо в робочу директорію Cacti і встановлюємо фіксиофіційними патчами

colo> cd / var / www / cacti

colo>get

www.cacti.net/downloads/patches/0.8.7g/data_source_deactivate.patch

colo> wget www.cacti.net/downloads/patches/0.8.7g/graph_list_view.patch colo> wget www.cacti.net/downloads/patches/0.8.7g/html_output.patch

colo>wget

www.cacti.net/downloads/patches/0.8.7g/ldap_group_authenication.patch

colo>wget

www.cacti.net/downloads/patches/0.8.7g/script_server_command_line_parse.patch

colo> wget www.cacti.net/downloads/patches/0.8.7g/ping.patch

colo> wget www.cacti.net/downloads/patches/0.8.7g/poller_interval.patchcolo> patch -p1 -N <data_source_deactivate.patch

colo> patch -p1 -N <graph_list_view.patchcolo> patch -p1 –N <html_output.patch

colo> patch -p1 -N <ldap_group_authenication.patch

colo> patch -p1 -N <script_server_command_line_parse.patchcolo> patch -p1 -N <ping.patch

colo> patch -p1 -N <poller_interval.patch

Створюємо cacti.conf з наступним змістом, щоб включити вебдоступ

colo> nano /etc/httpd/conf.d/cacti.conf

Alias / cacti / var / www / cacti

<Directory / var / www / cacti />DirectoryIndex index.php Options -Indexes AllowOverride all order deny, allowdeny from all allow from 192.168.1.0/24 (you can do it like "allow from all")

AddType application / x-httpd-php.phpphp_flag magic_quotes_gpc on php_flag track_vars on

</ Directory>

Перезавантажуємо веб-сервер Апачcolo> service httpd restart

Створюємо завдання Cron для Cacticolo> nano /etc/cron.d/cacti

* / 5 * * * * cactiuser php /var/www/cacti/poller.php> / dev / null 2> & 1

З цього моменту можна, можливо почати використовувати базову інсталяцію Cacti. Додавленіе серверів, за якими будемо стежити, здійснюється через веб-інтерфейс, доступний за адресою: http:

//ip.адрес.сервера/cacti. Але спочатку потрібно поставити на відслідковують сервера пакет snmp і переписати конфігураційний файл доступу

/etc/snmp/snmpd.conf:

syslocation Test.syscontact INF <sysadmin@arscraft.ru># sec.name source community (password)

com2sec Mybox localhost public com2sec cacti ip.адреса.сервера public com2sec Outside default public

group.name sec.model sec.namegroup RWGroup v2c Mybox group ROGroup v1 cacti

group ROGroup v2c cactigroup Others v2c Outsideview all included.1 80

view system included system fe

context sec.model sec.level prefix read write notifaccess ROGroup "" any noauth exact all none none access RWGroup "" v2c noauth exact all all all

access Others "" v2c noauth exact system none all

приклади одержаних графіків представлені на малюнках 3.3, 3.4, 3.5, 3.6

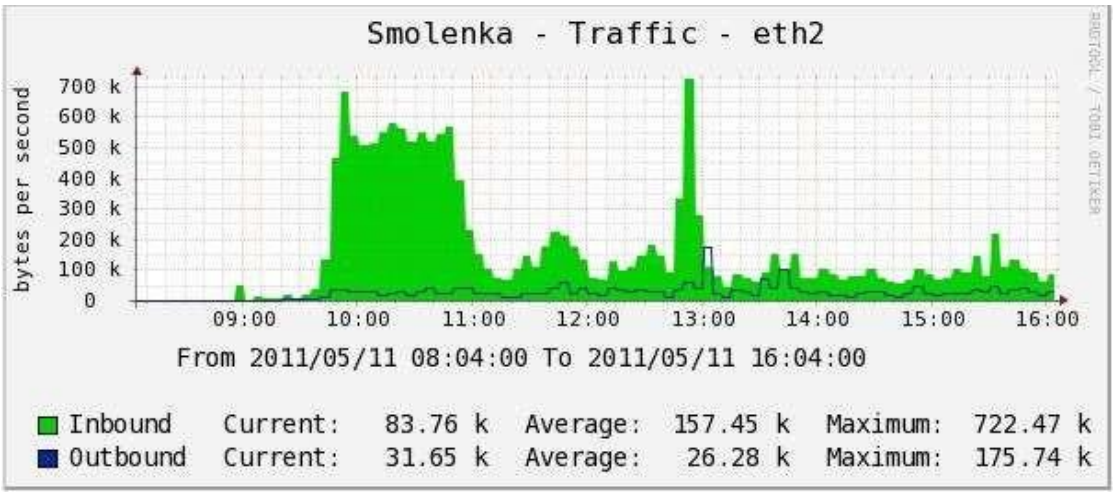


Рисунок 3.3 - Графік використання Інтернет-каналу

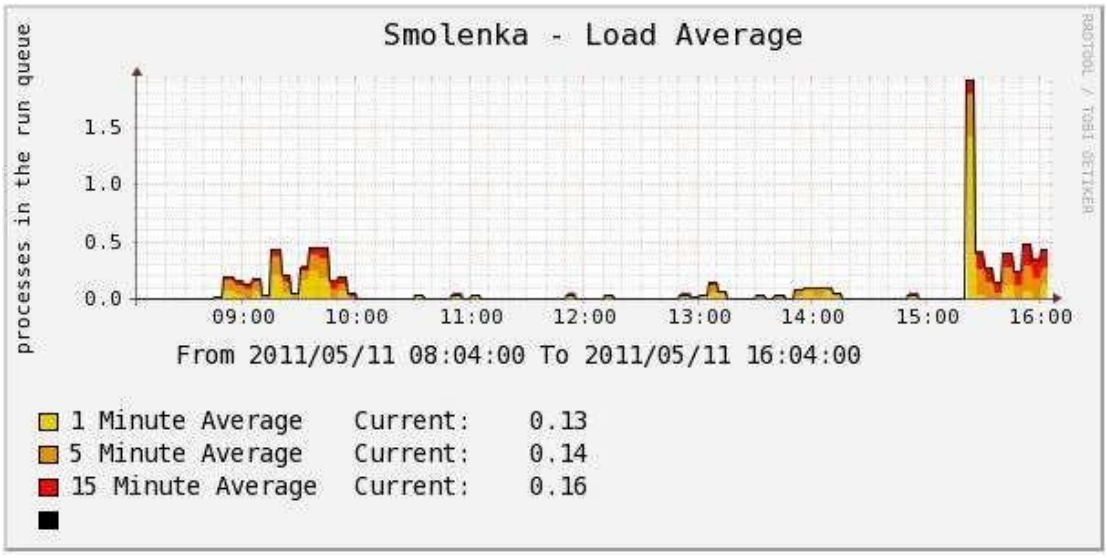


Рисунок 3.4 - Графік середнього завантаження процесора

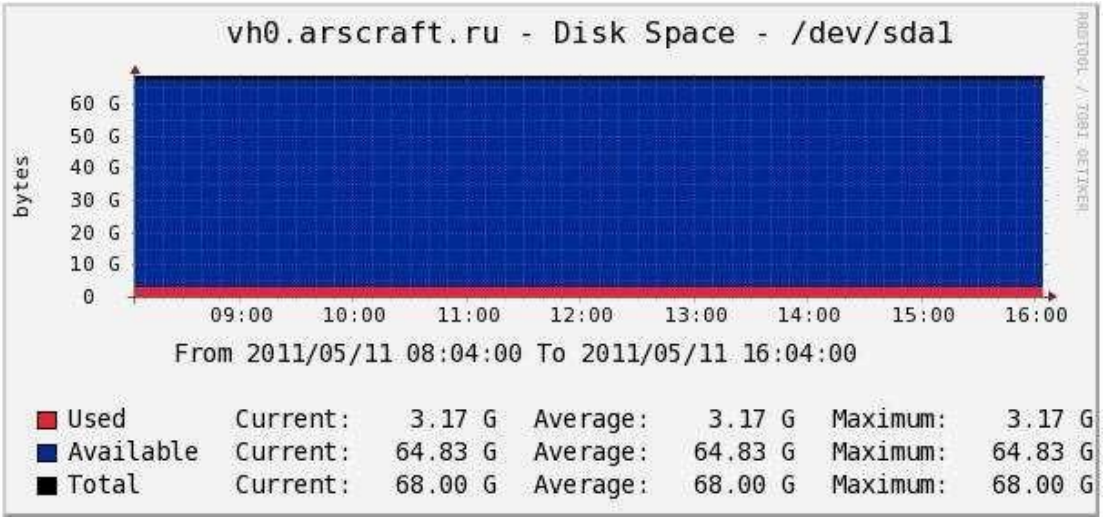


Рисунок 3.5 - Графік використання дискового простору

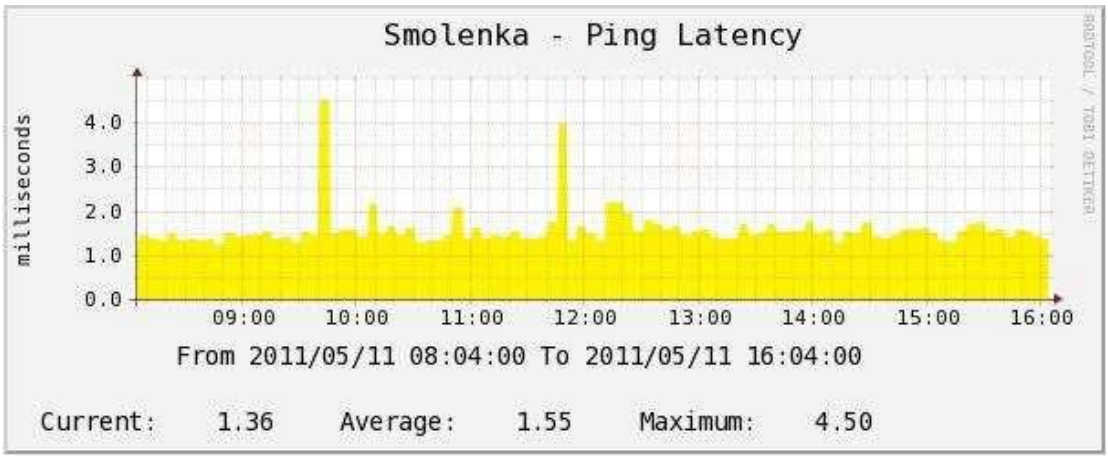


Рисунок 3.6 - Графік відгуку сервера (RTT)

3.2 Фільтрація і аналіз трафіку корпоративної мережі

3.2.1 Proxy сервер

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

1. Найбільш поширений спосіб потрапляння шкідливих програм на комп'ютер відбувається при перегляді веб-сторінок сумнівного контенту, перегляді банерів і скачуванні різного софту;

2. Один з найбільш частих вимог керівництва організації, є обмеження доступу на розважальні сайти і соціальні мережі.

Щоб здійснювати фільтрацію, потрібно щоб весь http трафік проходив через спеціальний proxy сервер.

Proxy сервер-це служба в комп'ютерній мережі, яка дозволяє клієнтам робити непрямі запити до інакших служб мережі. В першу чергу клієнт під'єднується до proxy-сервера і запитує будь-який ресурс (наприклад, електронну пошта), який знаходиться на інакшому сервері. Потім proxy-сервер або під'єднується до зазначеного сервера і витягує з нього ресурс, або повертає зі свого власного кешу ресурс (тоді, коли у proxy-сервера наявний власний кеш). У окремих випадках запит клієнта або відгук сервера, proxy-сервер буде змінювати для будь-якої мети. Крім того, proxy-сервер надає дозвіл на захист клієнтського комп'ютера від певних атак мережі і надає допомогу в підтримці анонімності клієнтів.

Реалізувати перекидання запитів на proxy-сервер можна двома шляхами:

1. Явно вказати в браузері адресу proxy-сервера (не рекомендується через незручності перемикання в разі падіння сервера);

2. Пересилати весь трафік, що прийшов на порти 80, 8080 маршрутизатора на proxy-сервер за допомогою правил і P tables.

У дипломі я буду використовувати другий метод. Proxy-сервер будемо встановлювати на маршрутизатор colo. Як ПО встановимо proxy- сервер SQUID.[4]

Squid - програмний пакет, який реалізує функцію кешуючого proxy- сервера для протоколів HTTP, FTP, Gopher і (в разі відповідних налаштувань) HTTPS. Розроблено співтовариством як програма з відкритим вихідним кодом (поширюється відповідно до GNU GPL). Всі запити виконує як один Неблокована процес введення/виводу.

Установка проводиться з стандартного сховища однією командою:

colo> yum install squid

Після першої установки необхідно проинициализировать кеш:

colo> squid -z

Переходимо до налаштування. Потрібно вирішити наступне завдання - закрити доступ на розважальні сайти і соціальні мережі, закрити доступ на скачку *.exe, *.sys, *.bat, *.sys, *.mp3, *.avi, *.mp4, *.mov файлів.

Основна конфігурація proxy-сервера знаходиться в файлі/etc/squid/squid.conf. Відредагуємо його під нашу задачу:

Вказуємо порт на якому будемо слухати запити, і вказуємо тип Proxy «прозорий», тому що пересилаємо пакети засобами маршрутизатораhttp_port 3128 transparent

ACL (Access Control List - список контролю доступу) - визначає, хто або що може отримувати доступ до певного об'єкта і які дії заборонені або дозволені цим суб’єктом виконувати над об'єктом. Використовуючи acl, характеризуємо об'єкти, які будемо використовувати.

Описуємо об'єкти і створюємо правила доступу до нихacl all src 0.0.0.0/0.0.0.0

acl manager proto cache_object

acl localhost src 127.0.0.1/255.255.255.255acl to_localhost dst 127.0.0.0/8

acl SSL_ports port 443

acl Safe_ports port 80 # http acl Safe_ports port 21 # ftp acl Safe_ports port 443 # https

acl Safe_ports port 70 # gopheracl Safe_ports port 210 # wais

acl Safe_ports port 1025-65535 # unregistered portsacl Safe_ports port 280 # http-mgmt

acl Safe_ports port 488 # gss-http acl Safe_ports port 591 # filemaker

acl Safe_ports port 777 # multiling httpacl CONNECT method CONNECT

http_access allow manager localhost

http_access deny manager http_access deny! Safe_ports

http_access deny CONNECT! SSL_ports

Описуємо нашу локальну мережу acl localnet src 172.16.100.0/24

Описуємо файл, в якому записані розширення заборонених типівфайлів

acl banfiles urlpath_regex -i "/etc/squid/include/permblock.files.acl"

Описуємо файл, в якому записаний список сайтів, заборонених до перегляду

acl banurl dstdomain -i "/etc/squid/include/permblock.url.acl"

Створюємо список для аудіо та відео контенту за допомогою mime acl banvideo rep_mime_type content-type audioacl banvideo

rep_mime_type content-type video

Забороняємо доступ з мережі до заборонених типам файлів, сайтам контенту.

http_access deny localnet banfiles http_access deny localnet banurl http_reply_access deny all banvideo

Дозволяємо доступ мережі для всього іншого трафікуhttp_access allow localnet

Для всіх інших забороняємо всеhttp_access deny all

Не забудь залишити права для адміністратора, додавши потрібну aclзапис. Розглянемо файли із заборонними списками:

Permblock.files.acl:

\.Exe $

\.Msi $

\.Bat $

\.Sys $ Permblock.url.acl:

.vkontakte.ru

.odnoklassniki.ru

.durov.ru

.vk.ru

.youtube

.rutube

...

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

$ Fw -t nat -A PREROUTING -p tcp -m multiport --dport 80,8080 -i eth1 -j DNAT --to 127.0.0.1:3128

Тепер трафік йде через proxy-сервер з фільтрацією. Також за допомогою Proxy-сервера при необхідності можна створювати ліміти по споживанню трафіку, працювати за розкладом і замінювати рекламні банери на web- сторінках на свої.

3.2.2 Аналізатор логів Proxy сервера

Ще однією з частих завдань є аналіз трафіку з двох причин:

1. Спостереження за діяльністю співробітника. Запобігання порушення дисципліни і правил роботи в компанії;
2. Створення лімітів на трафік, для зниження витрат компанії.

Proxy-сервер Squid при проходженні трафіку записує всю інформацію (звідки запит, що запитують, час, розмір і т.д.) в log файл. Залишається лише проаналізувати його і вивести інформацію в зручному для людини вигляді. Приклад лога proxy-сервера Squid:

1305189384.038 340 84.52.97.69 TCP_MISS/200 33232 GET

http://www.banius.ru/manager/zakaz/ shop6 DIRECT/77.222.42.202 text/html

1305189384.369 147 84.52.97.69 TCP_MISS/200 7306 GET

http://www.banius.ru/manager/modules/ms/images/li.gifshop6DIRECT/77.222.42.202 text / html

1305189448.705 1001 195.239.137.178 TCP_MISS / 200 1363 POST

http://mail.google.com/a/banius.ru/? shop7 DIRECT / 74.125.79.18 text / javascript1305189550.826 243750 195.239.137.178 TCP_MISS / 200 638 GET

http://mail.google.com/a/banius.ru/channel/bind? shop7 DIRECT / 74.125.79.18text / plain

Аналізувати трафік будемо спеціальним безкоштовним ПО LightSquid.

Всі необхідні компоненти (Perl, Gd, httpd) вже були встановленіраніше, тому переходимо безпосередньо до встановлення LightSquid:

Беремо з сайту http://lightsquid.sourceforge.net/ останню версію програми версії 1.8.

Разархівіруем скачав архів у каталог/var/www/html/colo>tar –xzf lightsquid-1.8.tgz

colo>cd lightsquid-1.8

Даємо права на виконання скриптівcolo>chmod+x*.cgi

colo>chmod+x*.pl

colo>chown-R apache: apache*

Вносимо зміни в файл конфігурації Apache/etc/httpd/conf/httpd.conf Alias/lightsquid"/usr/local/www/lightsquid-1.8"

<Directory"/var/www/html/lightsquid-1.8">AddHandler cgi-script.cgi

AllowOverride All

</ Directory>

Перезавантажуємо web-сервер для застосування змінcolo> service httpd restart

Переходимо в каталог з розпакованим lightsquid colo>cd/var/www/html/lightsquid-1.8

Перевіряємо на правильність файл конфігурації. Якщо видає помилки, швидше за все неправильно написані шляху до потрібних програмі каталогів. Виправити це можна в файлі lightsquid.cfg

colo>./check-setup.pl

Якщо помилок немає, то додаємо завдання аналізу трафіку щопівгодини в cron

colo>crontab-e

*/55 * * * */var/www/html/lightsquid-1.8/lightparser.pl

На цьому установка закінчена. При необхідності, є можливість занести адреси, з яких йде трафік, в групи і дати їм імена.

Перевірити роботу можна за адресою http://ip.адрес.сервера/lightsquid. Приклад роботи аналізатора трафіку представлений на малюнках 3.7, 3.8, 3.9.

Отчёт по использованию интернета, прокси-сервер Squid.

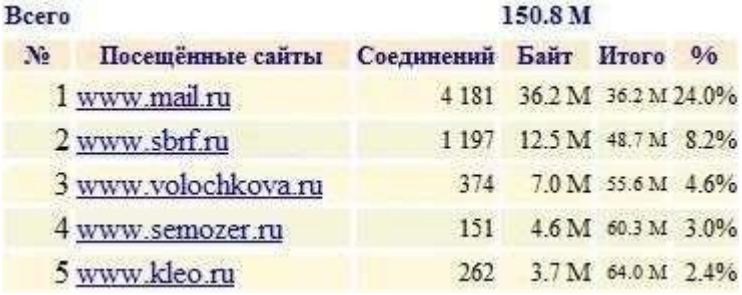
Дата: **06 Май 2011 (Обновлено :: 11:30 :: 12 Май 2011)**

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

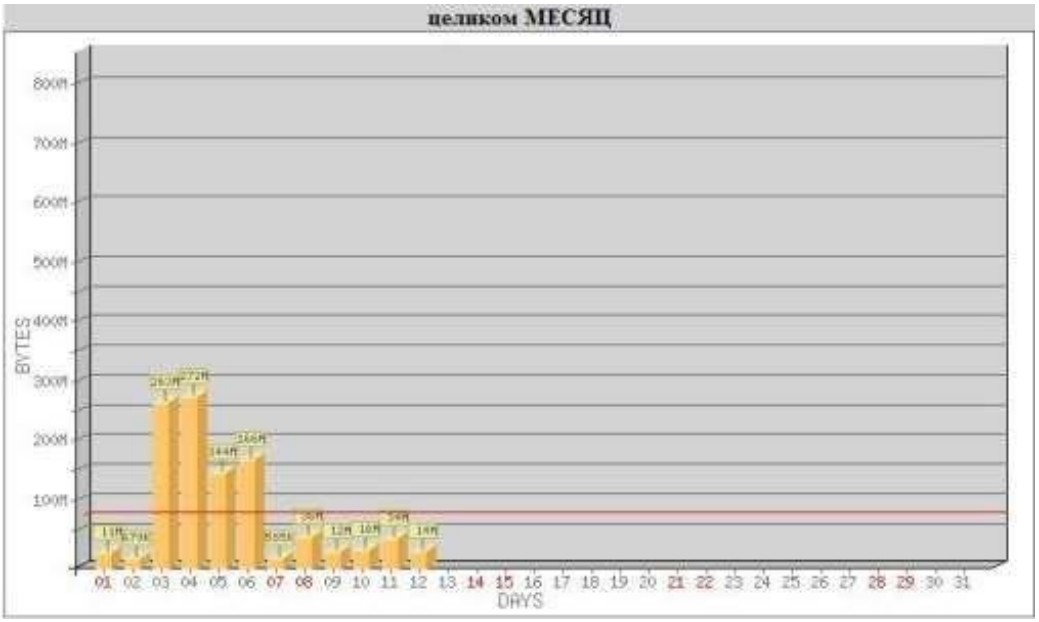


Рисунок 3.9 - Графік по використанню трафіку по днях

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 тільки частково, так як вважається тільки http трафік.

Часто провайдери надають приватним особам і організаціям доступ в мережу Інтернет не безлімітний, а трафіковий, тобто накладають обмеження на кількість скачали і відданих даних. За перевищення трафіку припадатиме сильно переплачувати. Тому моніторинг за трафіком є важливим завданням.

Є безліч білінгових систем, які включають в себе функцію підрахунку трафіку, але там надто 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 декількома механізмами, наприклад черезінтерфейси BPF, libpcap і iptables. Є один недолік: результати виводятьсяпрямо в консоль, без будь-якої фільтрації. Тому до пакету IPCad потрібно доопрацювати інтерфейс.

Почнемо з установки IPCad:

router> wget http://lionet.info/soft/ipcad-3.6.6.tar.gz

Розпаковуємо архів і переходимо в каталогrouter> tar -xvzf ipcad-3.6.6.tar.gz

router> cd ipcad-3.6.6

Конфігуріруем пакетrouter>./configure

Збираємо і встановлюємо пакетrouter> make

router> make install

Перероблюємо конфігураційний файл під свої потребиrouter> nano /usr/local/etc/ipcad.conf

Вказуємо не розбирати трафік по портам. Ця опція сильно навантажує маршрутизатор

capture-ports disable;

Вказуємо, який інтерфейс слухатиinterface eth1;

Настройки програми за замовчуваннямnetflow export version 5;

netflow export destination 127.0.0.1 9998;pidfile = /var/run/ipcad.pid;

dumpfile = ipcad.dump;buffers = 64k;

Розділяти статистику по кожному IP-адресою 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 біта адреси, що належить даному адресного діапазону

aggregate 192.168.23.0/24 strip 32;

Описуємо політики доступу до статистики ipcad. root може повністю управляти (робити backup, переглядати і змінювати таблиці підрахунку). Всі інші можуть лише переглядати статистику.

rsh enable at 127.0.0.1; rsh root@127.0.0.1 admin;

rsh root@127.0.0.1 backup;rsh root@127.0.0.1;

rsh 127.0.0.1 view-only;

"Час життя" і тайм-аут IP пакета.rsh ttl = 3;

rsh timeout = 30;

Опція 'memory_limit задає кількість пам'яті для зберігання вмістуодного потоку даних.

memory_limit = 10m;

Для отримання статистики запускаємо програму:

colo>/usr/local/bin/ipcad -rds colo> rsh localhost show ip accounting

Отримаємо висновок 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/secFlow entries made: 569 NetFlow cached flows: 27

Memory usage: 0% (63728 from 10485760)Free slots for rsh clients: 9

IPCAD uptime is 49 days 51 minutes

Такий результат не всім буде зрозумілий, та й запускати програмувручну не найзручніший спосіб підраховувати трафік. Для вирішення цієї проблеми потрібно створити зручний веб-інтерфейс. Всю інформацію протрафік будемо заносити в базу даних СУБД MySql. Створюємо базу даних stat і потрібні нам таблиці (users, download, upload, tmp), в які будемо записувати статистику.

Створимо скрипт "stat.sh", який буде запускати команду отримання статистики і записувати результат в файл, а потім запускати скрипт "collect.pl", що відповідає за додавання інформації в базу даних.

Скрипт stats.sh:

```
#!/Bin/bash
rsh 127.0.0.1 clear ip accounting>/dev/null
rsh 127.0.0.1 show ip accounting checkpoint>/tmp/ipcad.stat
/usr/local/etc/collect.plrm/tmp/ipcad.stat
```

Частина скрипта collect.pl:

```
#!/Usr/bin/perluse DBI;
#Логін: Пароль
$ Dbuser = "root";
$ Dbpassword = "password";
dbh = DBI-> connect ("DBI: mysql: stat: localhost", $ dbuser, $ dbpassword)or die "can not connect to database", $ dbh-> errstr,_____LINE__;
open (FIL, "/tmp/ipcad.stat") || die;while ($ line = <FIL>) {
@mass = split ( "", $ line);
$ Dbh -> do ("INSERT INTO`tmp`(`id`, `date`, `time`, `src`, `srcp`, `dst`,
`dstp`, ` bytes`, `proto`, ` class`) VALUES (', CURDATE (), CURTIME () $
}
close (FIL);
```

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

```
router> crontab -e
0,20,40,55 * * * */usr/local/etc/stat
```

Тепрь всі потрібні дані знаходяться в базі даних, залишилося тільки витягнути їх на сайт. Для цього розробляємо кілька web-сторінок. Код головної сторінки index.php знаходиться в додатку 3.

В результаті отримуємо систему підрахунку трафіку в зручному табличному вигляді (рис. 3.10), з наступними можливостями:

· Облік будь-якого трафіку для кожного користувача окремо;

· Встановлення ліміту трафіку, при перевищенні якого на пошту системному адміністратору приходить 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	[illegible]	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	[illegible]	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 ипользования Інтернет трафіку

3.4 Висновки

Під час спостереження за станом серверів та мережевого обладнання Nagios, я дізналась, що даний прилад застосовують для безперервного спостереження за довкіллям та суспільством, результати якого служать для обґрунтування оргагізаційних рішень потреб безпеки людей та об'єктів економіки. Системний адміністратор завжди повідомлений станом серверів і в короткостроковий термін попереджає та ліквідує проблему.

Слідкуючи за продуктивністю серверів Cacti, я краще ознайомилась з даним веб-додатком та дізналась, що за допомогою RRDtool можна будувати різні графіки. Даний додаток збирає інформацію та показники за певні проміжки часу і відтворює їх на графіку.

За допомогою цієї системи, ми можемо дізнатись, коли на сервери бувають піки та перевантаження, застосовування ресурсів серверів протягом доби, неділі, місяця.

Proxy сервер - це комп'ютерна програма, що дозволяє суспільствові виконувати не прямі звертання до мережевих сервісів,також надає захист від нападів мережі та надавати анонімність клієнтів.

Облік трафіку корпоративної мережі є дуже важливим, так як в більшості випадків доступ в інтернет не обмежений лімітом тобто нелімітований, а трафіковий, тоді накладають обмеження скачаних і відданих даних, за перевищення підключення доведеться багато переплачувати.

ВИСНОВКИ

В результаті виконання дипломної роботи отримані наступні результати:

1. Побудована захищена корпоративна мережа на основі VPN, використовуючи технології OpenVPN і SSH;

2. Розглянуто методи організації VPN мереж: клієнт-серверний, тунелірування, точка-точка;

3. Отримано табличні значення пропускної здатності захищених інтернет каналів для технологій OpenVPN і SSH. Дана практична оцінка продуктивності цих каналів створеної корпоративної мережі. Отримані результати дозволяють зробити загальний висновок: при побудові корпоративної мережі доцільно використовувати обидві технології - за допомогою OpenVPN створювати захищені мережі, за допомогою SSH - ssh- тунелі і створення підключень для адміністрування;

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

5. З метою фільтрації трафіку і стеження за діяльністю персоналу встановлено, налаштований і введений в роботу proxy-сервер;

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

7. Розроблено web-інтерфейс для системи обліку трафіку.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Астахова, И.Ф. Компьютерные науки. Деревья, операционные системы, сети / И.Ф. Астахова и др. - М.: Физматлит, 2013. - 88 с.
2. Кузин, А.В. Компьютерные сети: Учебное пособие / А.В. Кузин, Д.А. Кузин. - М.: Форум, 2018. - 704 с.
3. Максимов, Н.В. Компьютерные сети: Учебное пособие / Н.В. Максимов, И.И. Попов. - М.: Форум, 2017. - 320 с.
4. Новожилов, Е.О. Компьютерные сети / Е.О. Новожилов. - М.: Academia, 2016. - 352 с.
5. Олифер, В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. Стандарт третьего поколения / В.Г. Олифер, Н.А. Олифер.. - СПб.: Питер, 2013. - 944 с.
6. Соколов, А.В. Захист інформації в розподілених корпоративних мережах і системах / А.В. Соколов, В.Ф. Шаньгін – М.: ДМК Пресс, 2002. - 656с.
7. Таненбаум, Э.С. Компьютерные сети / Э.С. Таненбаум, Д. Уэзеролл. - СПб.: Питер, 2018. - 512 с.
8. Олег Колесников, Брайан Хетч. LINUX. Створення віртуальних приватних мереж (VPN) - Видавництво "КУДИЦ-ОБРАЗ" 2002 р - 464 с.
9. Шубин, В. И. Беспроводные сети передачи данных / В.И. Шубин, О.С. Красильникова. – М.: Вузовская книга, 2013. – 104 с.
10. Персональный компьютер и Интернет. Пособие для начинающих пользователей ПК. – М.: Альянс-пресс, 2003. – 512 с
11. Этот плохой хороший интернет. Техника безопасности в компьютерных сетях. – М.: Даниловский Благовестник, 2013. – 176 с.
12. Вільна енциклопедія: [Електронний ресурс]. URL: http://www.wikipedia.org (дата звернення 06.05.2021).
13. Статті про linux системах: [Електронний ресурс]. URL: http://www.opennet.ru (дата звернення 10.05.2021).
14. Статті про встановлення та налаштування різних пакетів програм під Linux /

Unix системи: [Електронний ресурс]. URL: http://www.lissyara.su (дата звернення 07.05.2021).

15. Колективний блог новин, аналітичних статей, пов'язаних з високими технологіями та Інтернетом: [Електронний ресурс]. URL: http://habrahabr.ru (дата звернення 04.05.2021).
16. Быстрая разработка программ. Принципы, примеры, практика. /Роберт Мартин, Джеймс Ньюкирк, Роберт Косс — Изд-во: Диалектика-Вильямс, 2004. — 752 с.
17. Дакетт, Джон HTML и CSS. Разработка и дизайн веб-сайтов (+ CD-ROM). /Джон Дакетт — Эксмо - Москва, 2013. - 480 с.

ДОДАТОК А

(обовязковий)

Таблиця значень пропускної здатності Інтернет каналу, використовуючи OpenVPN

№	без VPN		OpenVPN							
		AES-256-CBC	Шифрування з стисненням трафіку							
	RTT	швидкість	RTT	швидкість	Цп №1	Цп №2	RTT	швидкість	Цп №1	Цп №2	
1	1,438	9,57	2,016	9,10	7,7	6	1,856	12,10	10,7	8,3	
2	1,551	9,51	1,925	9,10	4,7	8,3	2,119	12,10	17	8,7	
3	1,532	9,58	1,990	9,10	6,6	6,3	2,245	12,10	10,7	8,3	
4	1,474	9,59	2,246	9,09	6	8,7	2,236	12,10	25,6	11	
5	1,481	9,59	2,258	9,10	5,7	8	2,191	12,10	10,3	8,7	
6	1,471	9,59	2,344	9,10	7,7	6,3	2,212	12,10	10,3	8,7	
7	1,694	9,50	2,360	9,10	8,3	8,7	2,262	12,10	7,3	7,7	

8	1,519	9,58	2,285	9,10	3	8,7	2,304	12,10	30,1	11,7	
9	1,470	9,59	2,336	9,09	7,6	6,3	2,208	12,10	12,7	8,7	
10	1,470	9,60	2,317	9,09	6,3	8,3	2,212	12,10	11	8,7	
11	1,575	9,58	2,282	9,09	6,3	8,7	2,258	12,10	23,3	11,7	
12	1,475	9,59	2,319	9,10	6	6,7	2,203	12,10	14	8,3	
13	1,686	9,60	2,224	9,09	4,7	8,7	2,267	12,10	10,7	7,7	
14	1,725	9,59	2,258	9,10	4	8,3	2,238	12,10	10,3	11,3	
15	1,706	9,58	1,941	9,09	7,7	6,7	2,312	12,10	29,3	8,7	
16	1,744	9,60	2,155	9,10	6,7	8,7	2,187	12,10	11	8,3	
17	1,551	9,60	2,313	9,09	7,3	6,3	2,224	12,10	9,7	11	
18	1,529	9,60	2,226	9,10	7,3	8,7	2,190	12,00	8,3	9	
19	1,449	9,58	2,240	9,09	8,7	8	2,288	12,00	31,3	9,3	

20	1,467	9,62	2,218	9,10	8	8,3	2,176	12,10	11,3	9,7	
21	1,499	9,59	2,200	9,10	7	8,7	2,196	12,10	11	9,3	
22	1,399	9,60	2,283	9,09	9,7	6,3	2,150	12,10	21	8,7	
23	1,545	9,59	2,264	9,10	7	8	1,825	12,10	16	7,3	
24	1,530	9,59	2,278	9,09	6,6	8,7	2,226	12,10	11,6	12,7	
25	1,374	9,58	2,244	9,09	8,7	8,3	2,273	12,10	10,3	8,3	
Ср	1,534	9,584	2,221	9,096	6,772	7,788	2,194	12,092	14,992	9,272	

У додатку 1 використані наступні позначення:

· № - номер досвіду. Під досвідом розуміємо передачу файлу з однієї мережі в іншу протягом 10 секунд;

· Без VPN - досліди проводилися без використання технології VPN;

AES-256-CBC - продуктивність каналу при шифрування даних, що передаються за допомогою 256 бітного ключа AES;

· Шифрування з стисненням трафіку - продуктивність каналу при використанні стиснення шифрованого трафіку;

· RTT - час між відправленням запиту й одержанням відповіді в мілісекундах (Round Trip Time);

· Швидкість - пропускна здатність каналу, яка вимірюється в Мбіт / сек;

· Цп1 - завантаження центрального процесора на передавальному маршрутизаторі;

· Цп2 - завантаження центрального процесора на приймаючому маршрутизаторі;

· Ср - середнє арифметичне значення.

ДОДАТОК Б

(обов’язковий)

Таблиця значень пропускної здатності Інтернет каналу,використовуючи SSH

№	без VPN			SSH						
		AES-256-CBC	Шифрування з стисненням трафіку							
	RTT	швидкість	RTT	швидкість	Цп №1	Цп №2	RTT	швидкість	Цп №1	Цп №2	
1	1,438	9,57	2,068	8,85	1,3	10,3	2,224	11,60	33,8	13	
2	1,551	9,51	2,374	8,85	1	9,7	2,258	10,40	36,7	11,3	
3	1,532	9,58	2,379	8,84	1,7	10,7	2,360	11,40	25	16,6	
4	1,474	9,59	2,354	8,84	0,7	8	2,285	11,50	25,3	12	

5	1,481	9,59	2,348	8,85	2,3	10,3	2,282	11,50	71,3	13,7	
6	1,471	9,59	2,133	8,83	2	10	2,319	11,50	24,9	10,3	
7	1,694	9,50	2,451	8,83	2,3	10,7	2,224	11,50	35,7	17,30	
8	1,519	9,58	2,411	8,86	2,7	7,7	2,524	11,40	35,9	12,7	
9	1,470	9,59	2,390	8,84	2	10,3	2,326	11,40	57,7	13,3	
10	1,470	9,60	2,423	8,85	1,3	10	2,232	11,60	24	14	
11	1,575	9,58	2,524	8,86	2	10	1,864	11,70	36,3	12,7	
12	1,475	9,59	2,354	8,84	3,3	8	2,235	11,40	54,3	11,3	
13	1,686	9,60	2,423	8,85	5	10	2,120	11,50	37,3	18,6	
14	1,725	9,59	2,354	8,85	1	10,3	2,221	11,40	23,6	12	

15	1,706	9,58	2,294	8,86	1,3	7,3	2,228	11,50	26,6	13,7	
16	1,744	9,60	2,133	8,84	3,3	10	2,423	11,30	77	11	
17	1,551	9,60	2,187	8,84	0,7	10	2,354	11,50	22,6	16,7	
18	1,529	9,60	2,374	8,83	2,7	10	2,423	11,60	31,7	14	
19	1,449	9,58	2,258	8,84	2,3	7,7	2,354	10,40	34,1	13	
20	1,467	9,62	2,235	8,85	1,7	10	2,294	11,60	55,4	10,3	
21	1,499	9,59	2,133	8,85	1	10	2,133	11,20	24,7	15	
22	1,399	9,60	2,212	8,83	3	9,7	2,374	11,20	35,6	12,7	
23	1,545	9,59	2,305	8,85	2,3	8	2,258	11,30	59,1	12	
24	1,530	9,59	2,336	8,84	1,7	10,7	2,190	11,40	34,3	12	

25	1,374	9,58	2,273	8,86	1,3	10	2,288	11,40	25,3	18,3	
Ср	1,534	9,584	2,309	8,845	1,704	8,140	2,272	11,368	37,928	13,500	

У додатку 2 використані наступні позначення:

· № - номер досвіду. Під досвідом розуміємо передачу файлу з однієї мережі в іншу протягом 10 секунд;

· Без VPN - досліди проводилися без використання технології VPN;

· AES-256-CBC - продуктивність каналу при шифрування даних, що передаються за допомогою 256 бітного ключа AES;

· Шифрування з стисненням трафіку - продуктивність каналу при використанні стиснення шифрованого трафіку;

· RTT - час між відправленням запиту й одержанням відповіді в мілісекундах (Round Trip Time);

· Швидкість - пропускна здатність каналу, яка вимірюється в Мбіт / сек;

· Цп1 - завантаження центрального процесора на передавальному маршрутизаторі;

· Цп2 - завантаження центрального процесора на приймаючому маршрутизаторі;

· Ср - середнє арифметичне значення.

ДОДАТОК В

(обов’язковий)

Код сторінки web-інтерфейсу

Index.php:

```
<? Php include "check.php"; ?>
<Html>
<Head>
<? Php
include ( "global.php");
Global $ funk, $ yearmonth;
db_connect ();
?>
<Meta name = "GENERATOR" content = "Quanta Plus">
<Meta http-equiv = "Content-Type" content = "text / html; charset = utf-8">
<LINK rel = "stylesheet" href = "style.css" type = "text / css">
</ Head>
<Body>
<Table class = inv-head align = left>
<Tr>
<Td align = left valign = top>
<H3> Персональна статистика: <br>
<? Php
// get checked ips
$ Query = "SELECT checkedip, uname, INET_NTOA (checkedip) from users order by checkedip";
$ Result = mysql_query ($ query);
if ($ result) {
echo "<form method = GET name = checkedips action = index.php>
IP: <select name = checkedip onChange = checkedips.submit ()>
```

```
<Option> --------
";
while ($ b = mysql_fetch_array ($ result))
{
if ($ checkedip == $ b [0]) {echo "<option value = $ b [0] selected = selected>
$ b [2]: $ b [1]";}
else {echo "
<Option value = $ b [0]> $ b [2]: $ b [1]
";}}
echo "</ select>
<Input type = hidden name = funk value = $ funk>
місяць <select name = month onChange = checkedips.submit ()>
";
$ I = 0;
foreach ($ mm as $ m_) {
$ I ++;
if ($ month == $ i) echo "<option value = $ i selected = selected> $ m_";
else echo "<option value = $ i> $ m_";
}
}
?>
</ Select>
<Select name = year onChange = checkedips.submit ()>
<? Php
foreach ($ yy as $ y_) {
if ($ year == $ y_) echo "<option value = $ y_ selected = selected> $ y_";
else echo "<option value = $ y _> $ y_";
}
?>
</ Select>
```

рік

</ Form> </ h3>

<Ul>   Statistic on all users </ li> </ ul>

<Ul> <? Php echo "

<Li> Завантаження з Інтернет за місяць

<Li> Завантаження з Інтернет по днях

<Li> Відвантаження в Інтернет по днях

<Li> Відвідини Інтернет

</ Ul>

<Ul>

<Li> Локальні мережі

<Li> Користувачі

</ Ul>

<Ul>

<Li> Вихід </ li>

</ Ul>

";

echo "<h3> <font color = yellow> :: $ now :: </ font> </ form> </ h3>";

include ("calendar.php"); ?>

<Td align = left valign = top>

<? Php

if ($ funk == "print_time" || $ funk == "print_time_upload" || $ funk ==

"print_inet" || $ funk == "print_lan") {$ funk ($ year, $ month, $ lim) ;}

else

if ($ _GET ['ch'] == 1) all ();
else $ funk ($ year, $ month);

mysql_close ();

?>

</ Table>

</ Td>

</ Tr>

<Tr> <td colspan = 2>

& Nbsp;

<P align = "right"> <font size = "4"> <? Php echo "<b> Тих. Підтримка: sysadmin@arscraft.ru </ b>";?>

</ Td>

</ Tr>

</ Table>

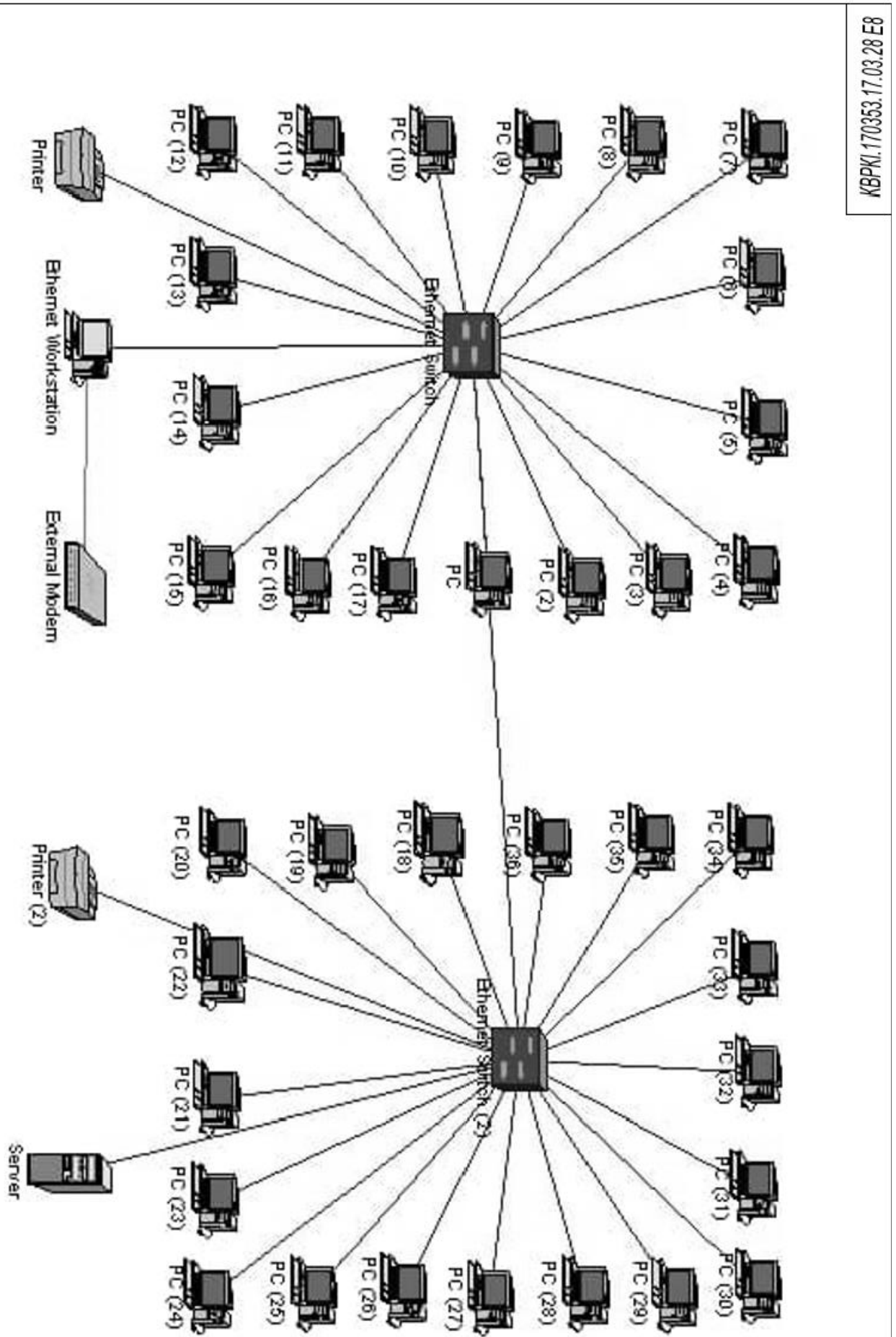
</ Body>

</ Html>

ДОДАТОК Г

(Обов' язковий)

Копія креслення «Змодельована мережа»



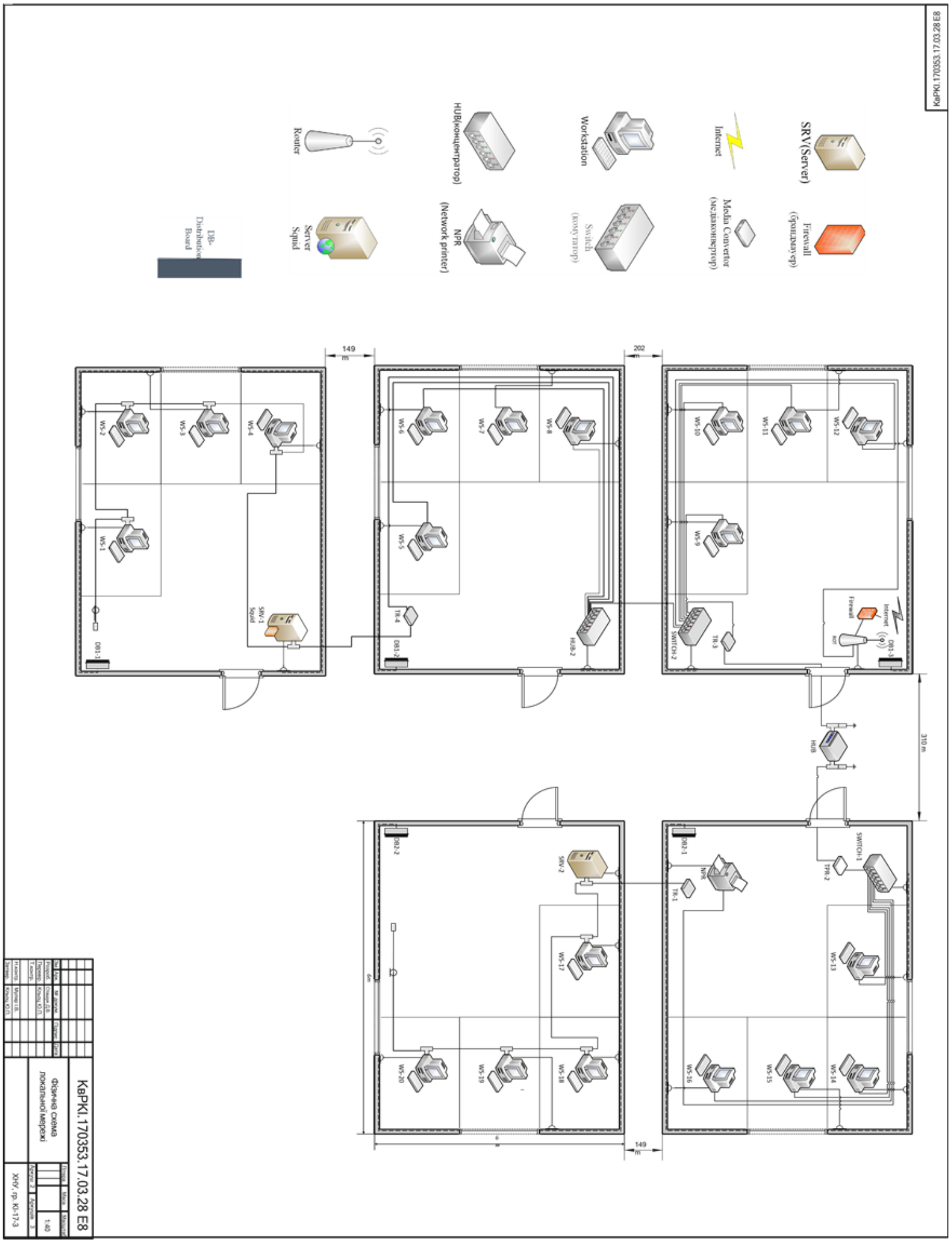
КВРКІ.170353.17.03.28 Е8

Зм.	Арк.	№ докум.	Підпис	Дата	КВРКІ.170353.17.03.28 Е8						
Розроб.	Ставицький Д.				Розподілена корпоративна мережа підприємства Змодельована мережа		Літера	Маса	Масштаб		
Перевір.	Шевченко К.І.						Н				
Т. контр.							Аркуш 1	Аркушів 3			
Н. контр.	Пилипчук І.В.					ХНУ, КІ-17-3					
Затв.	Шевченко К.І.										

ДОДАТОК Д

(обов’ язковий)

Копія кресоення «Фізична схема локальної мережі»



ДОДАТОК Е

(обов'язковий)

Копія креслення «Логічна схема локальної

UNICHECK

Ім'я користувача:
Кафедра КІ

Дата перевірки:
29.06.2021 12:46:26 EEST

Дата звіту:
29.06.2021 13:49:18 EEST

ID перевірки:
1008364072

Тип перевірки:
Doc vs Internet + Library

ID користувача:
100005591

Назва документа: Ставшук_Розподілена корпоративна мережа підприємства

Кількість сторінок: 80 Кількість слів: 14135 Кількість символів: 106556 Розмір файлу: 1.15 MB ID файлу: 100843360

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

11.6%
Схожість

Найбільша схожість: 2.5% з Інтернет-джерелом (https://habr.com/en/post/115493)

11% Джерела з Інтернету | 344 ..... Сторінка 82

0.71% Джерела з Бібліотеки | 65 ..... Сторінка 84

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

86.8%
Вилучень

Деякі джерела вилучено автоматично (фільтри вилучення: кількість знайдених слів є меншою за 8 слів та 0%)

Немає вилучених Інтернет-джерел

86.8% Вилученого тексту з Бібліотеки | 1 ..... Сторінка 84

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 234

Підозріле форматування | 21 сторінка

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 14%**

	Документ		Суммарное совпадение по Базе Данных	
	Символы	Лексемы	Символы	Лексемы
ID: 94589 Название: Розподілена корпоративна мережа піжприємства Добавлено в БД: 2021-06-17 Авторы: Сташук Д.В. Руководители: Кльоц Ю.П. Консультанты: Оппоненты:	86399	868	122 (0%)	3 (0%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА ДИПЛОМНИЙ ПРОЕКТ

Дипломник Ставчук Дар'я Володимирівна
Тема Комп'ютерна мережа Хмельницького національного університету
Спеціальність 123 Комп'ютерна інженерія

Обсяг дипломного проекту:

кількість листів креслень 4; кількість сторінок записки 95

1. Короткий зміст ДП та прийнятих рішень. В рамках дипломного проекту розроблено проект розподіленої корпоративної мережі підприємства

2. Висновок про відповідність ДП дипломному завданню Дипломний проект у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині даного проекту

3. Характеристика виконання кожного розділу проекту, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому, теоретичному, розділі дипломного проекту якісно та в повній мірі розглянуті методи вирішення поставленої задачі, був проаналізований кожен аспект, який стосується теми дипломного проекту. У наступному розділі було здійснено обґрунтування обраної структури мережі на основі порівняння різних можливих варіантів побудови цієї мережі. У основній проектній частині диплому була реалізована сучасними методами та рішеннями логічна структуризація мережі. Проектування виконано в середовищі Cisco Packet Tracer. Спроектована мережа дозволить забезпечити потреби користувачів розподіленої мережі та враховує необхідність передачі конфіденційної інформації зовнішніми каналами зв'язку.

4. Позитивні сторони проекту Дипломний проект відповідає сучасним вимогам до проектування корпоративних мереж та містить ряд рішень, що забезпечують роботу в єдиній мережі територіально віддалених офісів. Побудована мережа передбачає використання наявних підключень до провайдерів та заміну магістрального обладнання, що має підтримку відповідних протоколів

5. Негативні сторони проекту недостатня увага приділена налаштуванням комутаторів. Недостатньо приділено уваги використанню SSL сертифікатів.

6. Оцінка графічного оформлення та пояснювальної записки проекту Графічне оформлення виконане відповідно до суті дипломного проекту. У перших трьох (основних) листах креслення відображені основні фізичні та логічні зв'язки мережі, використання технології логічної структуризації мережі. В загальному графічне оформлення виконане на належному рівні, єдиним недоліком є нерівномірність розмірів шрифтів, що робить розгляд графічних креслень дискомфортним. Пояснювальна записка відповідає задекларованим нормам для її оформлення.

7. Відгук про проект в цілому В загальному дипломний проект вирішує поставлену задачу, однак має ряд зауважень. В роботі недостатньо висвітлені аспекти роботи спроектованої мережі.

8. Інші зауваження

9. Оцінка дипломного проекту Розглянувши позитивні та негативні сторони представленого дипломного проекту, можна зробити висновок, що він заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Корнієва Людмила Олександрівна, доцент кафедри автоматизації, комп'ютерно-інтегрованих технологій і телекомунікацій

«15» червня 2021 р. _____ (підпис)

ХНУ. Зам. 54, тир. 6000, 2007.

Завідувачу кафедри КІСП
д-р.техн.наук, проф. Говорущенко Т. О.

Станчук Дар'я Володимирівна
ПІБ здобувача вищої освіти

ФПКТС, 4 курсу, групи КІ-17-3

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіатоповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

29.06.2021
дата

підпис

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ ТА КОМП'ЮТЕРНИХ СИСТЕМ І МЕРЕЖ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:

Назва: Розподілена корпоративна мережа підприємства

Автор: Д.В. Сташук

Спеціальність: 123 – Комп'ютерна інженерія

Освітня програма: освітньо-професійна

Науковий керівник: Ю.П. Кльоц, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Запозичення виявлені в роботі, є законними і не є плагіатом, оскільки:

1) запозичення розміщені в розділах аналізу існуючих аналогів та технологій, які не описують безпосередньо авторське дослідження і не стосуються результатів роботи;
2) усі запозичення фрагментарні, або мають належним чином оформлені посилання;
3) окремі виявлені збіги є загальновживаними шаблонами, що використовуються при оформлені текстової документації, а саме шаблони рамок
4) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латиських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту, використання абревіатур.

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ідентичності/схожості, складає 11,6% і адресується до 342 першоджерел, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

Керівник роботи _____ Ю.П. Кльоц

Гарант ОП _____ С.М. Лисенко

Завідувач кафедри КБКСМ _____ Ю.П. Кльоц