МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Кафедра Комп'ютерних систем та мереж

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
комп'ютерних систем та мереж

_____Жуков І.А.

« ____ » _____ 2021 р.

ДИПЛОМНИЙ ПРОЕКТ

(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ

"БАКАЛАВР"

Тема: Мережа підприємства з віддаленими філіями

Виконавець: Василенков К.І.

Керівник: Фоміна Н.Б.

Нормоконтролер: Журавель С.В.

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет кібербезпеки, комп'ютерної та програмної інженерії
Кафедра комп'ютерних систем та мереж
Напрям (спеціальність) 123 "Комп'ютерна інженерія"
(шифр, найменування)

ЗАТВЕРДЖУЮ
Завідувач кафедри
комп'ютерних систем та мереж

_____Жуков І.А.

« ____ » _____ 2021 р.

З А В Д А Н Н Я
на виконання дипломного проекту

Василенкова Кирила Ігоровича
(прізвище, ім'я, по батькові)

1.Тема проекту (роботи): Мережа підприємства з віддаленими філіями

затверджена наказом ректора від "26" квітня 2021 року № 648 /ст.

2.Термін виконання проекту (роботи):): з 24.05.2021 до 20.06.2021
3. Вихідні дані до роботи: 1) вимоги до комп'ютерної мережі;
2) необхідні до реалізації типи використання комп'ютерної мережі.

4.Зміст пояснювальної записки (перелік питань, що підлягають розробці):
1) необхідність впровадження дистанційного навчання у вищих навчальних закладах;
2) інструменти балансування навантаження комп'ютерних мереж;
3) реалізація проекту об'єднанню локальних мереж офісів.

5. Перелік обов'язкового графічного матеріалу:
Презентація *Power Point*

6. Календарний план

№ п/п	Етапи виконання дипломного проекту	Термін виконання етапів	Примітка
1	Провести аналіз літератури за темою дипломної роботи та аналіз існуючих систем	24.05.21 - 26.05.21	
2	Вивчити спеціальну літературу і технічну документацію	27.05.21- 28.05.21	
3	Проаналізувати можливості управління налаштування територіально розподіленої мережі між декількома офісами компанії та написати розділ 1	29.05.21- 31.05.21	
4	Проаналізувати методи і інструменти балансування навантаження в комп’ютерній мережі та написати розділ 2	01.06.21- 02.06.21	
5	Реалізувати проект по об'єднанню локальних мереж офісів та написати розділ 3	03.06.21- 05.06.21	
6	Оформити пояснювальну записку иа супроводжувальну документацію	06.06.21- 12.06.21	
7	Підготовити графічний демонстраційний матеріал	13.06.21- 20.06.21	

7. Дата видачі завдання «24» травня 2021 р.

Керівник дипломного проекту _____ Фоміна Н.Б.
(підпис)

Завдання прийняв до виконання _____ Василенков К.І.
(підпис студента)

РЕФЕРАТ

Пояснювальна записка до дипломного проекту “Мережа підприємства з віддаленими філіями”: 60 с., 21 рис., 25 літературних джерел, 1 додаток.

VPN, РОЗПОДІЛЕНА КОМП’ЮТЕРНА МЕРЕЖА, БАЛАНСУВАННЯ НАВАНТАЖЕННЯ, ТУНЕЛЬ, МОНІТОРИНГ МЕРЕЖІ

Мета дипломного дослідження – розробити та налаштувати мережа підприємства з віддаленими філіями.

Об’єкт дипломного дослідження – розподілені корпоративні комп’ютерні мережі.

Предмет дипломного дослідження – мережа підприємства з віддаленими філіями.

Результати дипломної роботи можна використовувати при розробці мереж підприємств з віддаленими філіями та у навчальному процесі.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СКОРОЧЕНЬ, ТЕРМІНІВ

COM-порт	–	*Communications port*
GPRS	–	*General Packet Radio Service*
LAN	–	*Local Area Network*
WAN	–	*World Area Network*
ЕОМ	–	електронно обчислювальна машина
ОС	–	обчислювальна система
ARP	–	*Address Resolution Protocol*
ICE	–	*Intrusion Countermeasures Electronics*
ICMP	–	*Internet Control Message Protocol*
IP	–	*Internet Protocol*
ISO	–	*International Organization for Standardization*
OSI	–	*Open Systems Interconnection*
SPA	–	*Sender protocol address*
SSL	–	*Secure Sockets Layer*
UI	–	*User Interface*

ВСТУП

Актуальність. Головна мета об'єднання локальних мереж офісів - забезпечити прозорий доступ до територіально-розподілених інформаційних ресурсів організації. Об'єднання мереж офісів дозволяє вирішити наступні, найбільш поширені завдання:

– використовувати єдину номерну ємність офісної АТС;

– забезпечити авторизацію пользовтателей для доступу до ресурсів (загальні папки, інтранет-сайт, електронна пошта та ін.) незалежно від їх поточного місця розташування;

– забезпечувати захищений доступ співробітників організації до ресурсів, розташованим в різних офісах (наприклад, забезпечити роботу співробітників з сервером спеціалізованого ПЗ, встановленим в одному з офісів);

– працювати на віддаленому комп'ютері за допомогою термінального доступу (віддалене управління робочим столом);

– підвищити ефективність і опреративность служби технічної підтримки за рахунок можливості віддаленого управління комп'ютерами, серверами та іншим обладнанням, а також ефективного використання вбудованих засобів *Windows* для надання допомоги - Віддалений помічник.

Для того щоб об'єднати локальні мережі офісів і віддалених філій, застосовують технологію віртуальних приватних мереж - *VPN* (*Virtual Private Network*). Дана технологія призначена для криптографічного захисту даних, що передаються по комп'ютерних мережах. Віртуальна приватна мережа являє собою сукупність мережевих з'єднань між декількома *VPN*-шлюзами, на яких виробляється шифрування мережевого трафіку. *VPN*-шлюзи ще називають криптографічними шлюзами або крипто-шлюзами.

Існують два методи побудови єдиної захищеної корпоративної мережі організації:

– з використанням обладнання і відповідного комплексу послуг інтернет-провайдера;

– з використанням власного обладнання, розташованого в головному офісі та філіях.

Дане рішення може бути застосовано, якщо головний офіс і філії підключені до Інтернет через одного інтернет-провайдера. Якщо відділення компанії розкидані по містах, та ще в різних країнах, навряд чи знайдеться провайдер, який зможе надати вам необхідний рівень сервісу, та ще за прийнятні гроші.

Якщо ваші офіси знаходяться в межах одного міста, дізнайтеся у вашого інтернет-провайдера, чи може він забезпечити об'єднання локальних мереж ваших офісів в єдину мережу. Можливо це рішення буде оптимальним для вас за вартістю.

Метод об'єднання двох мереж із застосуванням технології *VPN* в англозязичной літературі називається "*Peer-to-Peer VPN*" або "*site-to-site VPN*". Між двома мережами встановлюється режим "прозорого шифрування". Для шифрування і передачі трафіку в *IP*-мережах найбільш часто використовують протокол *IPSec*.

Для організації *VPN*-з'єднань (*VPN*-тунелів) між центральним офісом і філіями невеликих компаній рекомендуємо використовувати апаратні інтернет-шлюзи (*firewall*) з вбудованою підтримкою *VPN*. Прикладом таких шлюзів можуть бути *ZyXEL ZyWALL, Netgear Firewall, Check Point Safe @ Office,* і т.п. Даний клас продуктів розрахований на застосування в невеликих компаніях із середньою чисельністю персоналу від 5 до 100 чоловік. Ці пристрої прості в налаштуванні, мають високу надійність і достатньою продуктивністю.

У головному офісі організації часто встановлюють програмні інтегровані рішення щодо захисту мережі, такі як "*Microsoft Internet Security and Acceleration Server*" (*Microsoft ISA*), *CheckPoint Express, CheckPoint VPN*-1 *Edge* і інші. Для управління цими засобами захисту необхідна наявність висококваліфікованого персоналу, який, як правило, або є в головному офісі або запозичується у компанії-аутсорсера.

Незалежно від застосовуваного обладнання, загальна схема побудови *Peer-to-Peer VPN* для безпечного об'єднання локальних мереж віддалених офісів в єдину мережу, наступна:

Слід також зауважити, що існують спеціалізовані апаратні крипто-шлюзи, такі як *Cisco VPN Concentrator* та ін. Їх область застосування - мережі середніх і великих компаній, де необхідно забезпечити високу продуктивність при шифруванні мережевого трафіку, а також спеціальні можливості.

При роботі віддалених філіалів необхідно забезпечити балансування навантаження на сервери та саму комп'ютерну мережу. У термінології комп'ютерних мереж балансування (вирівнювання) навантаження – це розподіл процесу виконання завдань між декількома серверами мережі з метою оптимізації використання ресурсів і скорочення часу обчислення.

Типи серверів, які можуть бути збалансовані:

– серверні кластери;

– міжмережеві екрани;

– сервери інспектування змісту (такі як *AntiVirus* – або *AntiSpam* – сервери).

Зазвичай системи балансування завантаження серверів використовують можливості рівня *L*4 (*UDP*/*TCP*). При цьому контролюється доступність сервера за *IP* -адресою і номером порту і приймається рішення: якому з доступних серверів слід переслати запит. Найбільш часто для вибору сервера використовується карусельний алгоритм (*round-robin*). У цьому варіанті передбачається, що всі запити створюють однакову завантаження і тривалість виконання. У більш просунутих варіантах алгоритму використовується рівень зайнятості сервера і число активних сполук.

Раніше можливості балансування навантаження убудовувалися в саму прикладну програму або операційну систему. Сучасні системи балансування навантаження повинні задовольняти наступним вимогам:

– забезпечувати управління трафіком, щоб гарантувати доступність додатка і розподіл навантаження в умовах ферми серверів (група серверів, з'єднаних мережею передачі даних і працюють як єдине ціле);

– прискорювати виконання додатків в кілька разів;

– гарантувати захист додатків, збереження даних і забезпечення моніторингу трафіку.

Тут важливо враховувати, що доступність *IP*-адреси і порту ще не гарантує доступу до додатка.

Останнім часом для вирішення завдання балансування навантаження все частіше використовується прикладний рівень. При цьому в процесі прийняття рішення враховується тип клієнта, запитуваний *URL*, інформація з *cookie*, можливості конкретного сервера і тип прикладної програми, що дозволяє оптимізувати використання ресурсів системи.

Досить істотні переваги може надати система *GSLB* (*Global Server Load Balancing*), яка здатна вирішувати завдання балансування для довільно розташованих ферм серверів з урахуванням їх віддаленості від клієнта. Ця система може підтримувати кілька різних алгоритмів розподілу навантаження і забезпечувати оптимальне обслуговування клієнтів, розкиданих по всьому світу. Для адміністраторів система дає можливість формування гнучкої політики управління ресурсами.

Одним із способів прискорення обслуговування є кешування. У разі добре сконфигурированного кеша частка запитів, що задовольняються кешем, може досягати 40%. При цьому прискорення обслуговування може бути покращено в 30 разів.

Ще одним методом прискорення обслуговування може служити архівація даних, так як в цьому варіанті знижується рівень перевантаження каналів мережі.

Управління балансуванням навантаження можна поєднати з функцією прикладного мережевого доступу (70% успішних вторгнень використовує уразливості додатків) і з використанням *SSL* по *VPN*-туннелю. *SSL – Secure Sockets Layer* – криптографічний протокол, який забезпечує встановлення безпечного з’єднання між клієнтом і сервером.

З збільшенням кількості користувачів проблема доставки об’ємного контенту в інтернеті стає все більш актуальною. Виникає необхідність

розташовувати сервера з даними як можна ближче до користувачам, для зменшення затримок і зниження навантаження на магістральні канали. Особливо це актуально для контенту, який потрібно одночасно роздати великим кількістю користувачів. Таким чином великим постачальникам контенту потрібно розподілена мережа серверів, звана Мережею Доставки Контенту (англ. *Content Delivery Network – CDN*). При побудові *CDN* можуть виникати різні проблеми – оптимізація трафіку всередині *CDN,* оптимізація розподілу контенту по серверам.

Зазвичай балансування називають маршрутизацією з двома *WAN* або мультихомінгами) – це можливість збалансувати трафік через два або більше *WAN*-каналів без використання складних протоколів маршрутизації, таких як *BGP*.

Цей баланс можливостей – це мережеві сеанси, такі як Інтернет, електронна пошта тощо за декількома підключеннями з метою розповсюдження кількості пропускної здатності, використовуваного кожним користувачем локальної мережі, таким чином збільшуючи загальну кількість доступної пропускної здатності. Наприклад, користувач має єдине *WAN*-з'єднання з Інтернетом, що працює на швидкості 1,5 Мбіт/с. Вони хочуть додати друге широкосмугове (кабельне, *DSL*, бездротове тощо), що працює на швидкості 2,5 Мбіт/с. Це забезпечить їм загальну пропускну здатність 4 Мбіт/с при балансуванні сеансів.

Мета дипломного дослідження – розробити та налаштувати мережа підприємства з віддаленими філіями. Об'єкт дипломного дослідження – розподілені корпоративні комп'ютерні мережі. Предмет дипломного дослідження – мережа підприємства з віддаленими філіями.

РОЗДІЛ 1

ПРИНЦИПИ НАЛАШТУВАННЯ КОМП'ЮТЕРНОЇ МЕРЕЖІ ДЛЯ ВІДДАЛЕНОЇ РОБОТИ

Сьогодні головна проблема компаній, особливо великих, полягає в тому, що відправка декількох тисяч співробітників на віддалену роботу - це важке завдання як для ІБ, так і для ІТ-служби в цілому. Ви можете відправити людей додому, зробити *VPN*, але підключення до корпоративної мережі великої кількості не надто контрольованих вами пристроїв - дійсно непроста робота. Очевидно, що не вийде кожному віддаленого співробітнику видати антивірус і систему запобігання витоків.

Ще одна проблема - як забезпечити роботу всього набору корпоративних додатків з дому на різношерстому парку обладнання: від старенького ПК на *Windows* 7 до *iPad*'а.

У цьому пості ми розповімо про декілька прикладних задачах і проблемах, які виникли у величезної кількості компаній у зв'язку з переведенням співробітників на удалёнку.

1.1. Аналіз можливостей *VDI*-доступу

Суть створення інфраструктури віртуальних робочих столів (*VDI*) - перенесення користувацьких ІТ-потужностей на серверну інфраструктуру / в хмару. При такому підході, робочі місця користувачів стають *Enterprise*-рішенням, для якого доступний весь той функціонал, який доступний для бізнес-критичних ІТ-систем: відмовостійкість, безпеку, централізоване управління, оновлення, резервне копіювання і відновлення. До такої системи найпростіше організувати безпечний віддалений доступ.

Можливості впровадження *VDI*:

– більшості компаній потрібно впровадити технологію дуже терміново. Тобто, фактично, віддалений доступ був потрібен їм «вже вчора».

– як правило, на проект по впровадженню *VDI* ні у кого не закладено будь-якого бюджету, всім доводиться знаходити кошти, що ще більше ускладнює ситуацію.

– система *VDI* передбачає наявність досить продуктивних серверів і СГД, і мало у кого з компаній вони є в наявності, а закупівля, крім певної вартості, передбачає ще й тимчасові витрати на узгодження, логістику і т.д.

– брак кваліфікованих фахівців усередині компаній - «робочих рук і голів».

Специфіка при виборі засобів організації віддаленого доступу:

– для багатьох компаній мало зробити безпечний віддалений доступ до своєї IT-інфраструктури: *VPN* або безпечна публікація сервісів захищають від зовнішніх негативних факторів, але не захищають від ризиків передачі інформації, що становить корпоративну таємницю недобросовісними співробітниками, або банального зараження вірусами при підключенні співробітників через *VPN* зі своїх домашніх робочих станцій / ноутбуків. Вкрай бажано організувати безпечний периметр для співробітників, що підключаються віддалено.

– при масовому віддаленому підключенні співробітників очевидно зростає навантаження на мережеві канали ЦОД, де розташовуються IT-системи компанії. Важливо передбачити, щоб ширини наявних каналів вистачило, а самі вони були організовані в відмовостійкої конфігурації.

1.2. Типи віддаленого доступу

Зіткнувшись із збільшеним потоком запитів на організацію віддаленого доступу, для себе ми придумали таку класифікацію типів віддаленого доступу:

– рівень 0. Всі IT-системи повністю ізольовані в периметрі організації, віддалений доступ відсутній. Звичайно ж, така інфраструктура є максимально безпечною, але поточна ситуація змушує більшість замовників переходити на інші рівні;

– рівень 1. Це найпоширеніший зараз тип віддаленого доступу, у кого він вже організований: або підключення відбувається через *VPN*, або частина сервісів може просто публікуватися (найпоширеніше - корпоративна пошта, сервіс ВКС). Подібних технологій не один десяток років. Додаткове обладнання зазвичай не потрібно, компанія може порівняно швидко налаштувати більшу частину функціональності для віддалених співробітників. Однак у такого підходу чимало недоліків. Робота користувачів зазвичай нічим функціонально не обмежується, доступ можливий з будь-яких пристроїв, що у випадку з *VPN* загрожує вірусними атаками, а в разі публікації сервісів назовні, ІТ-служба не зможе контролювати, куди переміщуються корпоративні дані, які залишають межі периметра мережі. Ніщо не завадить недобросовісному співробітникові відправити якусь поштове повідомлення / вкладення через *WhatsApp* або *Telegram* того, кому не варто було б. Чим більше додатків ми публікуємо, тим більше створюємо потенційно уразливих місць у зовнішній мережі для хакерських атак. Складно спрогнозувати навантаження на мережеві канали, тому що різні ІТ-системи вимагають різної пропускної здатності мережі. Для користувачів таке віддалене робоче оточення виглядає не завжди зручно: не у всіх є достатньо продуктивні особисті ноутбуки, може не діставати будь-яких клієнтів корпоративного ПЗ і т.д.

– рівень 2. Так званий «швидкий старт» - перехідний варіант до повноцінного *VDI* за допомогою використання компонентів *VDI,* але підключення здійснюється не до віртуальних робочих столів на виділених серверах віртуалізації, а до фізичних робочих станцій (АРМ) співробітників. При такому варіанті вимоги до додаткових серверних ресурсів мінімальні, тому що мова йде про розгортання 6-8 не сильно вимогливих до ресурсів віртуальних машин, терміни розгортання теж мінімальні, протоколи і політики підключень при цьому використовуються найпоширеніші - на базі *Citrix Virtual Apps and Desktops,* або *VMware Horizon*.

Основні переваги рівня 2:

– користувачі вже можуть працювати повністю віддалено в звичному їм оточенні: сидять за домашніми комп'ютерами, але бачать звичні екрани своїх офісних ПК.

– до користувачів йде лише один тип трафіку - відображення віддалених робочих столів. При необхідності *VMware* і *Citrix* дозволяють дуже тонко налаштовувати дозволу на кидок інших даних: мультимедіа-трафік від мікрофона і камери, смарт-карти і т.п.

– протоколи *VMware* і *Citrix* дуже добре оптимізовані. Протокол *Citrix* взагалі вважається найкращим варіантом для роботи на вузьких нестабільних каналах зв'язку.

– можна набагато краще спрогнозувати навантаження на мережевий канал: для передачі даних в *VDI* на призначену для користувача сесію досить в середньому 512 Кбіт / с.

– трафік будь-яких додатків залишається всередині периметра корпоративної мережі і не виходить назовні. Немає можливості щось скачати на домашній ПК, або навпаки завантажити в периметр мережі. Всі корпоративні дані набагато краще контролюються.

– висока швидкість розгортання такої інфраструктури - менш ніж через тиждень можна підключати перших користувачів.

Основні недоліки рівня 2:

– у порівнянні зі звичайною роботою користувачів в офісі з'являються додаткові точки відмови, тому що ми розгортається нові компоненти, нехай і в відмовостійкої конфігурації.

– в офісі повинні чергувати технічні фахівці для обслуговування корпоративних ПК, до яких підключаються співробітники: включити / перезавантажити / відновити роботу в разі стрибка напруги.

– рівень 3. Самий просунутий рівень, що представляє собою повноцінний *VDI*. До всього вищепереліченого у нас додаються цільові ресурси - віртуальні машини і окремі віртуалізовані застосування. Схема дуже схожа на рівень 2, але вже будуть потрібні окремі фізичні ресурси у вигляді серверів і систем зберігання даних, або гіперконвергентние кластери.

Основні переваги рівня 3:

– Додаткова перевага *VDI* в порівнянні з рівнем 2 полягає в повноцінному вилученому керуванні інфраструктурою. Аж до того, що технічні фахівці в офісі вже не потрібні (*VDI* в зовнішньому хмарі - стандартна історія).

– Робочі місця користувачів уніфіковані: віртуальні столи створюються на основі єдиного шаблону, розгортаються і управляються серійно, гарантовано оновлюються.

– Можна легко організувати резервне копіювання профілів. Тобто з'являється набагато більше свободи і сильно спрощується адміністрування. Автоматизуються багато рутинні завдання, завдяки цьому знижується навантаження на співробітників тих. підтримки і вплив людського фактора.

– *VDI* прекрасно інтегрується зі сторонніми системами безпеки: антивірусним захистом, *DLP, MDM*.

Але віддалений досту має низку недоліків:

– Чимала вартість реалізації. У звичайний час витрати окупалися в середньостроковій перспективі, приблизно за 5 років, а потім починалася економія. Сьогодні часи напружені, тому часто стоїть питання не окупності, а виживання компаній.

– Тривалість реалізації. Потрібно створити віртуальні робочі столи, віртуалізувати окремі додатки, все налаштувати, зробити переміщувані профілі, мігрувати користувачів. Мова йде про терміни від трьох тижнів і до двох-трьох місяців (без урахування термінів поставки обладнання).

– Буде потрібно досить продуктивне обладнання, тому що *VDI* досить сильно навантажує сервери і СГД.

Висновки до розділу

Підведемо підсумки можливостей віддаленого доступу на різних рівнях:

– рівень 0 - ніякого віддаленого доступу немає;

– рівень 1 - базовий віддалений доступ, який можна реалізувати за два-три дні, швидше за все, без закупівлі додаткового обладнання;

– рівень 2 - це перехідний варіант до повноцінного *VDI* - кидок сесії користувачів на технологіях *VDI* до фізичних робочих місць;

– рівень 3 - повноцінний *VDI* з шаблонами, автоматизацією, отказоустойчивостью та іншими *Enterprise*-можливостями.

Щоб якомога швидше організувати віддалену роботу співробітників компаніям без закладеного бюджету на впровадження *VDI*, можна почати розгортання з використанням тимчасових (*trial*) ліцензій і вже через тиждень почати підключати користувачів до їх робочих місць, не купуючи обладнання і ПЗ.

Термін дії тимчасової ліцензії залежить від технологій, зазвичай це 2-4 місяці при узгодженні з виробниками ПЗ. Паралельно можна переходити на рівень 2.

А якщо ситуація з віддаленої роботою затягнеться, то непогано б організувати повноцінний *VDI*. У *Citrix* в цьому році з'явилася нова схема ліцензування локальної версії - по щорічній підписці. Її вартість приблизно в 2,5 рази нижче постійної ліцензії. *VMware* пропонує послугу швидкого запуску *VDI*, але вона доступна тільки тим клієнтам, які можуть розплачуватися кредитами - це коштує 212 кредитів. В рамках цієї послуги пропонується один шаблон *VDI* до 25 користувачів.

РОЗДІЛ 2

ІНСТРУМЕНТИ БАЛАНСУВАННЯ НАВАНТАЖЕННЯ КОМП'ЮТЕРНИХ МЕРЕЖ

2.1. Типи топології балансування навантаження

Кожна з наступних топологій може бути застосована як для балансувальник навантаження *L*4, так і для *L*7.

2.1.1. Балансування навантаження через проксі по середині

Топологія проксі по середині, показана на рис. 1.1 (у розділі 1.1, вище за текстом), ймовірно, є найбільш відомим способом отримання балансування навантаження для більшості користувачів. Ця категорія включає апаратні пристрої від *Cisco, Juniper, F5* і т.д.; хмарні програмні рішення, такі як *Amazon ALB* і *NLB* і C*loud Load Balancer*; і чисті програмні рішення, такі як *HAProxy, NGINX* і *Envoy*. Переваги подібної топології – простота застосування для користувачів. У загальному випадку користувачі підключаються до балансувальника навантаження через *DNS* і не повинні турбуватися ні про що інше. Угодою рішення проксі по середині є той факт, що проксі (навіть в разі кластеризації) є єдиною точкою відмови, а також вузьким місцем масштабування. Проксі по середині також часто є чорним ящиком, що ускладнює роботу.

2.1.2. Балансування навантаження через крайовий проксі

Топологія крайового проксі, показана на рис. 2.1, на самому ділі є лише варіантом топології проксі по середині, в якій балансувальник навантаження доступний через Інтернет.

Всі плюси і мінуси крайового проксі-сервера такі ж, як і проксі по середині. Клієнтам зазвичай потрібно доступ до системи через DNS з використанням довільних мереже

Залежно від підключення, транспортних протоколів та від того, чи є носій приватним чи загальнодоступним, у грі можуть бути кілька різних різновидів WAN. Чотири основних типи глобальної мережі:

Агрегація мережевих / приватних мереж WAN

Інтернет-краю

Взаємозв'язок центру обробки даних

Велике відділення WAN

Роль агрегування WAN також можна розділити на наступні три категорії, виходячи з того, що зазвичай можна знайти в корпоративних мережах:

Основне агрегування глобальної мережі (пояснення в наступному розділі)

Безпечне агрегування WAN (надбудова з рішеннями на основі IPsec або Secure Sockets Layer віртуальної приватної мережі [SSL VPN])

Оптимізоване агрегування WAN (надбудова з рішеннями, заснованими на оптимізації WAN з протоколом зв'язку Web Cache Версії 2 / Маршрутизація на основі політики [WCCPv2 / PBR] та Служби додатків для широкої області [WAAS])

Роль агрегації філій / приватних WAN

Агрегація глобальної мережі WAN - це спосіб з'єднати та об'єднати всі гілки підприємства в основний маршрутизатор WAN або головну станцію. На стороні хмари, інтерфейси маршрутизатора використовують різні варіанти фізичного транспорту (як зазначено в таблиці 1-1), тоді як на стороні ядра кампусу підключенням є Gigabit Ethernet (GE) або 10 Gigabit Ethernet (10 GigE), що діє оскільки висхідна лінія для ядра кампуса перемикається на глобальну мережу. Орендовані лінії - один із найпоширеніших способів (зараз більше Ethernet) взаємодії з хмарою WAN. Функції припинення тунелю IPsec та функції брандмауера зазвичай не згортаються в маршрутизаторі агрегації / краю WAN. Зазвичай це реалізується як класичний дизайн з концентратором і спицями з традиційним підключенням рівня 2.

У таблиці 1-1 показані різні варіанти, що використовуються для підключення до глобальної мережі.

Таблиця 1-1 Параметри підключення до WAN

Типи	Фізичний транспорт	Плюси	Мінуси	Типова пропускна здатність	Інкапсуляції протоколів
Виділена лінія	T1 / E1, T3 / E3	Приватна	Дорого	Від 1,544 до 45 Мбіт / с	Контроль даних високого рівня (HDLC), PPP
Перемикання ланцюга	Пакет через SONET / SDH OC3 / OC12 / OC192	Доступний	Менш захищений	155 Мбіт / с до 10 Гбіт / с	HDLC, PPP
Комутація пакетів	T1 / E1, T3 / E3 (ПВХ)	Доступний	Спільна пропускна здатність	До 45 Мбіт / с	Кадрове реле

Кліти нне реле	ОС 3 / ОС12 / ОС48	При ватна	Ви ща вартість порту	До 620 Мбіт / с	Банко мат
Метро Ethernet	Eth ernet, GE, 10 GigE	Дост упний	Не вистачає властиво ї надійнос ті	Д о 10 Гбіт / с	Ethernet (Frac-GE, Frac-10 GigE)

ПРИМІТКА

Metro Ethernet набирає великих обертів для об’єднання сайтів, розташованих у певній географічній зоні. Це також добре масштабується сьогодні з дробовим GE та 10 GigE, і ще більше масштабуватиметься за допомогою нових стандартів 40 і 100 Гбіт / с, які вже працюють в IEEE як P802.3ba, і перші чернетки вже вийшли

Основні вимоги до функцій

У таблиці 1-2 викладено основні вимоги, яким повинен відповідати маршрутизатор, щоб бути позиціонованим як платформа агрегування WAN. Масштаб та продуктивність цих служб визначаються залежно від того, наскільки великою є концентрація відділення для даного розгортання. Платформа з окремим управлінням, даними та площиною введення / виведення є найбільш переважною із зрозумілих причин.

Таблиця 1-2 Матриця функцій для ролі агрегації WAN

Характеристика / Сервіс	Детальна інформація про функцію / послугу
Маршрутизація IP (v4 / v6)	Протокол внутрішніх шлюзів (IGP) та Протокол прикордонних

	шлюзів (BGP) з швидкою конвергенцією, наприклад, двонаправлене виявлення відмов (BFD) Маршрутизація на основі політики (PBR)
IP одноадресне та багатоадресне	Незалежний від протоколу багатоадресний (PIM) розріджений, розріджений щільний режим, точка автоматичного побачення (RP), Anycast-RP, багатоадресна передача, специфічна для джерела, двонаправлений PIM, переадресація зворотного шляху одноадресної передачі (uRPF)
NetFlow	v5, v9 Експорт даних NetFlow
Якість обслуговування (QoS)	Класифікація на основі трафіку додатків, протоколу / порту, списків контролю доступу (ACL) Маркування Ієрархічне QoS Класові зважені чесні черги (WFQ), чесні черги, низька затримка (LLQ), зважені випадкові раннє виявлення (WRED) ДАІ Формування дорожнього руху Фрагментація та чергування посилань (LFI)

Стиснення	Стиснення заголовка протоколу реального часу (RTP) для голосового трафіку
WCCP (протокол управління веб-кешем)	WCCPv2 для механізму веб-кешування та оптимізації WAN для передачі даних та відео
Мультилінк ППС (MLPPP)	MLPPP з LFI
Багатопротокольне перемикання етикеток (MPLS)	VPN на базі 2547, VPN рівня 2
Висока доступність (HA)	Інтра- та Interbox HA

~ Вимоги до базового рівня обслуговування

У таблиці 1-3 викладені звичайні вимоги до угоди про рівень обслуговування (SLA), яким потрібно відповідати для конвергентної глобальної мережі для типів голосового, відео та трафіку даних.

Таблиця 1-3 Типова ціль SLA

Тип трафіку / Застосування	Ціль SLA
VoIP	Інтерактивне відео Відеоконференція
Затримка <= 50 мс	Джиттер <= 5 мс Втрати <= 1% Голосовий MOS (середній бал думки)> = 3,8
Відеотрансляція Відео на вимогу (VoD)	Затримка <= 50 мс Втрати <= 1%

Критично важливий трафік WWW Голосова сигналізація	Час відгуку <= 3 сек
Втрата обслуговування (конвергенція RP)	IGP <= 3 хв

Традиційні глобальні мережі (такі як ті, що базуються на Frame Relay) вважаються за своєю суттю безпечними, що не так (оскільки постачальники використовують спільну фізичну інфраструктуру для перенесення цього трафіку). MPLS VPN - ще один приклад, коли трафік ізольований (через екземпляри та мітки віртуальної маршрутизації / переадресації [VRF]), але при цьому використовує ту саму фізичну інфраструктуру під час обходу хмари постачальника послуг.

Не рідко можна побачити певну форму шифрування, що використовується для досягнення конфіденційності, рушіями якої можуть бути політика компанії (наприклад, будь-який трафік, що виходить із приміщення, має бути зашифрована) або відповідність нормативним документам (наприклад, HIPAA або SOX).

У таблиці 1-4 викладено загальновживані технології для захисту трафіку глобальної мережі. Розділ 14, “Випадки використання служб безпеки”, містить додаткові подробиці.

Таблиця 1-4 Деталі високого рівня про безпечні технології WAN

Безпечна технологія WAN	Деталі
Власний IPsec (одноадресний та багатоадресний)	IPsec використовує як шифрування, так і алгоритм хешування. Інтерфейс віртуального тунелю може бути використаний для підтримки багатоадресного трафіку.

Інкапсуляція загальної маршрутизації (GRE) від точки до точки (p2p) через IPsec (або p2p GRE всередині IPsec)	IPsec з підтримкою багатоадресної передачі та протоколу маршрутизації.
Динамічна багатоточкова VPN (DM VPN)	Зазвичай розгортається через загальнодоступну Інтернет-інфраструктуру.
VPN з віддаленим доступом	M'які клієнти IPsec / SSL VPN та агрегація тунелів маршрутизатора малого офісу / домашнього офісу (SOHO; 8xx / 18xx).
Груповий зашифрований транспорт (GET VPN)	Безтунельне шифрування, найкраще підходить для приватних хмар IP або MPLS.

ПРИМІТКА

У більшості випадків транспортним середовищем для безпечних рішень зв’язку (як зазначено в таблиці) є загальнодоступна мережа глобальної мережі.

Роль Інтернет-краю

Край Інтернету - це межа, де приватна мережа підприємства підключається до загальнодоступної мережі Інтернет. У найпростішому сенсі пристрій Інтернет-краю виконує роль шлюзу для внутрішньої мережі. На відміну від загальноприйнятого розуміння, край Інтернету - це не лише доступ до Інтернету для веб-трафіку для користувачів кампусу.

Мережа Інтернету виконує різні функції, включаючи ті, що описані в Таблиці 1-5.

Таблиця 1-5 Функціональність Internet Edge Router

Функція	Деталі

Корпоративний інтернет-шлюз для кампусу та центру обробки даних	Користувачі в кампусі отримують доступ до Інтернету для перегляду, надсилання електронної пошти та використання обміну миттєвими повідомленнями тощо.
Корпоративний інтернет-шлюз для філій	Користувачі філій отримують доступ до Інтернету для перегляду, надсилання електронної пошти та використання обміну повідомленнями екземплярів тощо. Це для забезпечення загального набору
	політика на всьому підприємстві під тягарем приведення всього трафіку до головної дошки.
Послуги демілітаризованої зони (DMZ)	Традиційні служби FTP, Система доменних імен (DNS) та Мережевий протокол часу (NTP), розташовані на DMZ.
Телеробітник (віддалені користувачі)	Телеробітники або дорожні воїни підключаються до корпоративних ресурсів через Інтернет за допомогою зашифрованих технологій VPN, таких як IPsec або SSL VPN, м'які або жорсткі клієнти (наприклад, маршрутизатори Cisco 800).

Резервне копіювання глобальної мережі WAN	Це служить резервним або альтернативним підключенням для маршрутизаторів філій для підключення до головної корпоративної мережі через загальнодоступний Інтернет. У цьому сценарії найчастіше використовуються технології DM VPN, GRE через IPsec або віддалений доступ на основі динамічного інтерфейсу віртуального тунелю (VTI).
Мульти-самонаведення	Тут мережевий маршрутизатор краю підключається безпосередньо до декількох ІП. Це забезпечує вищу толерантність до відмов і простір вибору шляху за допомогою передових технологій маршрутизації. Це вимагає, щоб маршрутизатор міг підтримувати одну або кілька копій таблиці маршрутизації в Інтернеті.

~ Основні вимоги до функцій

Основна функція пристрою на межі Інтернету - діяти як розмежування між приватною (кампус чи центр обробки даних) та загальнодоступною мережею (тобто Інтернетом). Функції, необхідні для одного пристрою, залежать від того, як розроблений край Інтернету, хоча, як правило, основними функціями є ті, що описані в Таблиці 1-6.

Таблиця 1-6 Вимоги до функцій мережевого пристрою Internet Edge

Характеристика / Сервіс	Деталі

Маршрутизація IP (v4 / v6)	IGP та BGP з швидкою конвергенцією, такі як BFD PBR Великий масштаб маршрутизації (таблиця маршрутизації в Інтернеті)
NetFlow	v5, v9 Експорт даних NetFlow
QoS	Класифікація на основі трафіку додатків, протоколу / порту, ACL Маркування Ієрархічне QoS Клас WFQ, чесні черги, LLQ, WRED ДАІ Формування дорожнього руху LFI
Пом'якшення розподіленої відмови в обслуговуванні (DDoS)	Дистанційно спрацьовані чорні діри (RTBH), rACL, брандмауер
WCCP	WCCPv2 для механізму веб-кешування
Брандмауер	Брандмауер L4 – L7
Переклад адреси	Переклад адреси мережі / порту (NAT / PAT) із шлюзом прикладного рівня (ALG)
Висока доступність	Внутрішньо- та міжповерховий HA

НА від коробки до коробки	Протокол маршрутизатора гарячого режиму очікування (HSRP), протокол резервування віртуального маршрутизатора (VRRP), протокол балансування навантаження шлюзу (GLBP)
Глибока перевірка пакетів	Розпізнавання додатків на основі мережі (NBAR), гнучке узгодження пакетів (FPM)
Безпечне підключення до WAN	DMVPN, GRE через IPsec, IPsec

Центр обробки даних

Взаємозв'язок центру обробки даних (DCI) - це ще одна функція WAN, коли хтось намагається з'єднати два центри обробки даних за допомогою посилань рівня 2 або 3. Розширення рівня 2 набагато частіше через їх здатність приймати всі кадри Ethernet (або навіть dot1Q або QinQ [IEEE 802.1Q-in-Q VLAN]), як і в центрах обробки даних. Зазвичай це робиться з якоюсь псевдопроводом (наприклад, Ethernet через MPLS [EoMPLS] для двох центрів обробки даних, і Служба віртуальної приватної локальної мережі [VPLS] для підключення до багатоцентрового центру обробки даних). Основними драйверами DCI є наступні:

Консолідація та віртуалізація ЦОД (VMWare VMotion)

Відновлення після катастрофи або центр обробки даних НА

Гео-кластеризація, де кластери пов’язані між собою за географічними регіонами

Розширення рівня 2 з будь-якої причини

Майже всі архітектури кластерів VMWare та IBM або Microsoft вимагають підключення до локальної мережі як базову вимогу. Отже, емуляція послуги

локальної мережі, коли вона все ще підключена через глобальну мережу, створює багато проблем для конвергенції (в ідеалі - за кілька секунд).

Вимоги до рішення, наведені в Таблиці 1-7, вимагають інфраструктури, яка має функції, наведені в Таблиці 1-8.

Таблиця 1-7 Вимоги до функції DCI

Особливість	Деталі
Розширення 2-го рівня	Зазвичай використовують псевдопроводи.
Ізоляція протоколу обширного дерева (STP)	Ізоляція розгалужуючого дерева є одним з обов'язкових моментів, коли кожен DCI не розширює STP, щоб уникнути будь-якого циклу. Маючи зайві посилання, що функціонують одночасно без STP в ядрі.
HA	Край DCI повинен мати справу з несправностями вузлів і каналів.
Швидша конвергенція	Це повинно бути якомога меншим на випадок відмови вузла або каналу. В ідеалі - що завгодно менше кількох секунд.
Безпечне спілкування	Шифрування, наприклад рішення на основі IPsec.
QoS	Ієрархічне QoS для DCI.
Оптимізація глобальної мережі	Оптимізація DCI WAN з використанням технологій WAAS.

Вимоги до максимального блоку передачі (MTU)	Підтримка Jumbo frame.

Вимоги до рішення, наведені в Таблиці 1-7, вимагають інфраструктури, яка має функції, наведені в Таблиці 1-8.

Таблиця 1-8 Вимоги до функції маршрутизатора / комутатора, необхідні для задоволення вимог рішення DCI

Особливість	Деталі
Розширення 2-го рівня	Використання EoMPLS (p2p) або VPLS (від точки до багатоточок).
Ізоляція STP для кожного центру обробки даних	Можливість припинення STP у самому даному центрі обробки даних. Надлишкові посилання, що функціонують на одному і тому ж рівні, можуть бути забезпечені за допомогою віртуальних комутаційних систем Cat 6500 / багатокасісного Ethernet-каналу (VSS / MEC) та / або Nexus 7K vPC (віртуального портового каналу).
HA	Використання резервних маршрутизаторів (ASR 1000, наприклад) або комутаторів (6500 / Nexus 7K).
Швидша конвергенція	Існує два ширших підходи: віддалене вимкнення порту EoMPLS за допомогою вимкненого лазера (підтримується на ASR 1000). Використання вбудованого диспетчера подій (EEM) або виявлення неспрямованого зв’язку (UDLD) на 6500, Nexus 7K або ASR 1000.

Безпечне спілкування	Рішення GRE через IPsec або Nexus TrustSec (Cisco TrustSec на основі шифрування рівня посилання IEEE 802.1AE).
QoS	Ієрархічне QoS на краю DCI.
Оптимізація глобальної мережі	Оптимізація глобальної мережі за допомогою WCCPv2 або PBR з використанням існуючих пристроїв Cisco WAAS.
Вимоги до MTU	Джамбо-кадри підтримуються на посиланнях Cat 6500, Nexus 7K та ASR 1000 GE / 10 GigE.

~ Велика гілка WAN

Як загальновідомо, не всі гілки рівні. Це стосується не лише розміру філії (як, наприклад, кількості користувачів або, можливо, серверів додатків, що проживають у філії), а й того, наскільки критично важлива філія для загальної ділової функції. Наприклад, розглянемо відділення банків. Не всі філії надають весь портфель послуг. У реальному світі одні надають лише основні банківські послуги, тоді як інші надають повномасштабні послуги, включаючи заставу вдома, позики для малого бізнесу та інвестиційні послуги для комерційних клієнтів.

Великі філії (ті, що надають більше послуг чи послуг, що є критично важливими для бізнесу, або в більшості випадків обидва), як правило, мають дещо інші вимоги до інфраструктури глобальної мережі, яка зв’язує їх із корпоративною магістраллю. У таблиці 1-9 викладено основні вимоги до глобальної мережі.

Таблиця 1-9 Вимоги до розгортання великої філії

Вимоги	Деталі

Більша пропускна здатність висхідної лінії зв'язку	OC3, або навіть Metro Ethernet.
Можливість обробляти як WAN, так і Інтернет-трафік	Через обсяг трафіку великі філії підключені безпосередньо до Інтернету.
Багатоквартирність	Можливість підтримувати кілька відділів або навіть клієнтів або партнерів, які використовують спільну фізичну інфраструктуру разом із працівниками.
QoS	Ієрархічне QoS для підтримки декількох рівнів класів обслуговування.
	WFQ на основі класів, чесні черги, LLQ, WRED формування трафіку.
Вимоги до послуг	Такі послуги, як NAT, брандмауер та NetFlow на високій швидкості та масштабі.
HA	Внутрішня та внутрішня скринька HA підтримує основну переадресацію трафіку та послуги.

Таблиця 1-10 відображає вимоги до інфраструктури, необхідної для підтримки таких вимог.

Таблиця 1-10 Вимоги / особливості великого відділення

Вимоги	Риси інфраструктури для зустрічі з ними

Більша пропускна здатність висхідної лінії зв'язку	Різноманітність інтерфейсу
Можливість обробляти як WAN, так і Інтернет-трафік	Модульні дані та площина управління для вирішення зростаючого набору вимог
Багатоквартирність	Можливість підтримки віртуалізації інтерфейсів, служб та таблиць маршрутизації / переадресації
QoS	Гнучка архітектура, яка може адаптуватись до мінливих вимог QoS за допомогою оновлення програмного забезпечення
Вимоги до послуг	Можливість підтримувати існуючі та новіші служби за допомогою наявного обладнання за допомогою оновлення програмного забезпечення
HA	По суті високодоступна система

2.2. Центр Інтернет-безпеки: 18 необхідних засобів контролю безпеки

Центр безпеки в Інтернеті оновив свій набір запобіжних заходів для запобігання п’яти найпоширенішим типам атак, які стикаються з корпоративними мережами - злому веб-додатків, зловживанням інсайдерами та привілеями, зловмисним програмним забезпеченням, вимогами та цільовими вторгненнями.

При видачі йогоЕлементи управління СНД V8цього місяця організація прагнула представити практичні та конкретні дії, які бізнес може вжити для захисту своїх мереж та даних. Вони варіюються від проведення інвентаризації активів підприємства до управління рахунками до аудиту журналів.

Частково нова версія була потрібна для вирішення змін у роботі підприємств, починаючи з випуску V7 три роки тому, і ці зміни керували роботою. "Перехід до хмарних обчислень, віртуалізації, мобільності, аутсорсингу, роботи вдома та зміна тактики зловмисників були головними у кожному обговоренні", - йдеться в новому документі про управління.

Уроки резервного копіювання від катастрофи в хмарному сховищі

СНД трохи змінив формат елементів управління, описуючи дії, які слід вжити для усунення загроз та слабких місць, не сказавши, хто повинен виконувати ці завдання. Це зосереджує увагу на завданнях, не прив’язуючи їх до певних команд на підприємстві.

Кожен елемент управління містить детальні процедури їх реалізації, а також посилання на відповідний ресурс. Ось короткий опис 18 елементів управління.

Контроль 1: Інвентаризація та контроль активів підприємства

Це вимагає активного управління запасами, відстеження та виправлення всіх пристроїв кінцевих користувачів, включаючи портативні та мобільні; мережеві пристрої; необчислювальні пристрої / Інтернет речей (IoT); і сервери, які підключаються до інфраструктури фізично, віртуально, віддалено, а також ті, що знаходяться в хмарних середовищах. Інвентаризація допоможе визначити пристрої для видалення або усунення.

Контроль 2: Інвентаризація та контроль програмних активів

Підприємства повинні активно інвентаризувати, відстежувати та виправляти всі операційні системи та додатки в мережі для виявлення та блокування несанкціонованого та некерованого програмного забезпечення, щоб було встановлено та могло виконуватись лише дозволене програмне забезпечення.

Контроль 3: Захист даних

Потрібно запровадити процеси обробки даних та технічний контроль для ідентифікації, класифікації, надійної обробки, збереження та розпорядження даними.

Ідеальним для цього є розміщення даних однакового рівня чутливості в одній мережі та ізольованих від даних з іншими рівнями чутливості. Брандмауери контролюватимуть доступ до кожного сегмента, і доступ буде надаватися лише тим користувачам, яким комерційна діяльність потребує доступу до них.

Контроль 4: Безпечна конфігурація активів та програмного забезпечення

Безпечна конфігурація пристроїв кінцевих користувачів, включаючи портативні та мобільні; мережеві пристрої; не обчислювальні пристрої / пристрої IoT; сервери; операційні системи та додатки слід створювати, зберігати та підтримувати. Рекомендується встановлювати VPN перед серверами та використовувати DNS-сервери, які контролюються підприємством.

Контроль 5: Управління рахунками

Це рекомендує використовувати процеси та інструменти для управління авторизацією корпоративних активів та програмного забезпечення. Сюди входять облікові записи адміністратора та служби. Одна з рекомендацій передбачає обмеження прав адміністратора на спеціальні облікові записи адміністраторів та надання цих прав лише тим, хто фактично адмініструє мережеві активи. Ці адміністратори також повинні мати окремі облікові записи, які вони використовують для доступу до електронної пошти, веб-перегляду та додатків для підвищення продуктивності.

Контроль 6: Управління контролем доступу

Підприємства повинні використовувати процеси та інструменти для створення, призначення, управління та анулювання облікових даних та привілеїв доступу для облікових записів користувачів, адміністраторів та служб для активів та програмного забезпечення підприємства. Рольовий доступ повинен бути призначений кожному обліковому запису на основі необхідності знати, найменших привілеїв, вимог щодо конфіденційності та розподілу обов'язків.

Елемент управління 7: Постійне управління вразливістю

Вразливості слід постійно оцінювати та відстежувати в корпоративній інфраструктурі, щоб їх можна було своєчасно усувати, щоб мінімізувати можливість для зловмисників використовувати їх. Для сприяння цьому процесу слід використовувати державні та приватні галузеві джерела інформації про нові загрози та вразливість.

Контроль 8: Управління журналом аудиту

Журнали аудиту слід збирати, переглядати та зберігати для документування подій та допомагати виявляти, розуміти та відновлювати атаки. Журнали можуть показувати, коли і як відбуваються атаки, до якої інформації здійснювався доступ, а також якщо дані були вилучені. Зберігання журналів є критичним для подальших розслідувань або для розуміння атак, які залишаються невизначеними протягом тривалого періоду часу.

Управління 9: Захист електронної пошти та веб-браузера

Цей контроль закликає покращити захист та виявлення електронної пошти та веб-загроз, які можуть маніпулювати поведінкою людини шляхом прямого залучення; це головні цілі як для зловмисного коду, так і для соціальної інженерії. Запобіжні заходи включають використання служб DNS-фільтрації для зменшення впливу та застосування мережевих URL-фільтрів>

Елемент управління 10: Захист від зловмисного програмного забезпечення

Підприємства повинні запобігати встановленню, розповсюдженню та виконанню програмного забезпечення на корпоративних активах або контролювати його, використовуючи методи, що включають антивірусне програмне забезпечення на всіх корпоративних активах, скануючи наявність шкідливого програмного забезпечення на змінних носіях, таких як флеш-

накопичувачі, та дозволяючи анти-експлуатаційні функції, "такі як як Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG) або Apple® System Integrity Protection (SIP) та Gatekeeper ™ ".

Елемент управління 11: Відновлення даних

Повинні бути застосовані практики відновлення даних, достатні для відновлення масштабів корпоративних активів до попереднього інциденту та довіреного стану. Оскільки зміни конфігурації можуть створювати уразливості для зловмисників, важливо мати нещодавні резервні копії для відновлення корпоративних активів та даних у відомий надійний стан.

Контроль 12: Управління мережевою інфраструктурою

Підприємства повинні відстежувати, звітувати та коригувати мережеві пристрої, щоб запобігти зловмисникам використання мережевих послуг та точок доступу. Інфраструктура включає фізичні та віртуальні шлюзи, брандмауери, бездротові точки доступу, маршрутизатори та комутатори. Ці заходи повинні розглядати уразливі місця, які можна ввести за допомогою налаштувань за замовчуванням, контролю за змінами та переоцінки поточних конфігурацій. Одним із прикладів є запуск останнього стабільного випуску програмного забезпечення або використання підтримуваних в даний час пропозицій мережі як послуги (NaaS).

Крім того, підприємства повинні підтримувати схеми мережі та іншу системну документацію, а також щороку переглядати та оновлювати їх. Обчислювальні ресурси, що використовуються для адміністративних завдань, повинні бути фізично або логічно відокремлені від первинної корпоративної мережі та ізольовані від доступу до Інтернету.

Контроль 13: Моніторинг та захист мережі

Слід встановити комплексний моніторинг мережі та захист від загроз, включаючи виявлення вторгнень, фільтрацію трафіку між сегментами мережі та розгортання засобів контролю на рівні порту, таких як ті, що підтримуються автентифікацією 802.1x.

Контроль 14: Поінформованість про безпеку та навчання навичкам

Повинна бути розроблена програма підвищення обізнаності щодо безпеки, яка створює свідомість безпеки серед робочої сили та надає їм навички зменшення ризиків кібербезпеки.

Контроль 15: Управління постачальником послуг

Слід встановити процес оцінки постачальників послуг, які зберігають конфіденційні дані або відповідають за критичні IT-платформи або процеси, щоб забезпечити належний захист. Підприємства повинні встановлювати вимоги до постачальників послуг, які можуть включати мінімальні програми безпеки, повідомлення про порушення та повідомлення про порушення даних, вимоги щодо шифрування даних та зобов'язання щодо розпорядження даними. Підприємства повинні щороку переглядати контракти на надання послуг, щоб переконатися, що вони включають вимоги.

Керування 16: Захист програмного забезпечення

Підприємства повинні керувати життєвим циклом безпеки власного розробленого, розміщеного або придбаного програмного забезпечення для запобігання, виявлення та усунення слабких місць безпеки, перш ніж вони вплинуть на підприємство. Організації також повинні використовувати стандартні, рекомендовані галуззю шаблони конфігурації, щоб зміцнити базові сервери, бази даних та веб-сервери. Це також стосується хмарних контейнерів, компонентів платформи як послуги та компонентів SaaS.

Контроль 17: Управління реакцією на аварії

Ключові ролі та обов'язки повинні бути призначені для реагування на інциденти, включаючи співробітників юридичних, IT, інформаційної безпеки, служб, зв'язків з громадськістю, людських ресурсів, реагуючих на аварії та аналітиків, залежно від ситуації. План слід переглядати щороку або коли відбуваються суттєві зміни на підприємстві, які можуть вплинути на реакцію на інциденти.

Контроль 18: Випробування на проникнення

Програма тестування на проникнення повинна імітувати дії зловмисника з метою виявлення та використання слабких місць серед людей, процесів та технологій. Програма повинна відповідати розміру, складності та зрілості

підприємства. Вразливі місця слід усунути, виходячи з політики підприємства щодо масштабу виправлення та встановлення пріоритетів.

2.3. Прискорення бізнес-мережі Wi-Fi

Перешкоди, занадто багато SSID, трафік управління ключами та мала ширина каналу можуть уповільнити мережі Wi-Fi. Ось як їх пришвидшити.

Правильне обстеження та обслуговування сайтів є вирішальним для бездротових мереж, особливо для мереж з великим трафіком, таких якWi-Fiгарячих точок у громадських місцях. Те саме стосується ситуації, коли швидкість життєво необхідна, як при потоковому передаванні відео чи голосу через Wi-Fi.

Перешкоди, затори, поганий дизайн, неправильна конфігурація та відсутність технічного обслуговування - це лише кілька факторів, які можуть негативно вплинути на роботу Wi-Fi. На щастя, для боротьби з цими проблемами можна використати кілька методів.

Але спочатку примітка про ефірний час Wi-Fi, тобто час, який передає бездротовий пристрій або точка доступу (AP). Чим повільніше швидкість передачі, тим більше ефірного часу займає пристрій і тим менше часу доступно для інших пристроїв. Це важливо, оскільки не всі пристрої можуть передавати одночасно по даному каналу; бездротові клієнти та точки доступу повинні спільно використовувати ефір.

Як розгорнути 802.1x для Wi-Fi за допомогою WPA3 для підприємств

Старі пристрої, такі якWi-Fi 4 (802.11n)може говорити лише по одній. Пристрої Wi-Fi 5 (802.11ac) дозволяють підключення внизбагатокористувацький MIMO, тому точка доступу дійсно може одночасно передавати на кілька бездротових пристроїв на одному каналі. Крім того, Wi-Fi 6 (802.1ax) додає лінію зв'язку, тому одночасне спілкування може відбуватися в обидві сторони. Однак, ймовірно, не всі пристрої підтримуватимуть ці два стандарти, тому ефірний час все ще викликає занепокоєння.

Якщо на вашому робочому місці є зони, в яких повністю відсутній покриття Wi-Fi, додавання або переміщення існуючих бездротових точок

доступу, мабуть, найкраще місце для початку. Однак, якщо у покритті немає великих дір, а головна проблема полягає у повільних швидкостях, спробуйте скористатися описаними тут методами, перш ніж переміщувати або додавати точки доступу.

Якщо у вашій мережі є бездротовий контролер або ваші точки доступу мають вбудовану функціональність контролера, тоді ви можете налаштувати параметри з центрального інтерфейсу. В іншому випадку вам, швидше за все, доведеться входити в кожну точку доступу, щоб внести рекомендовані зміни.

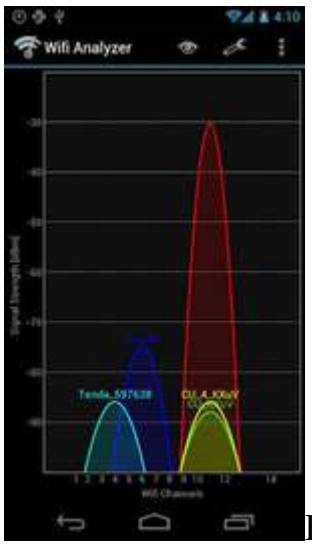
РЕКОМЕНДОВАНІ КЛІПАТИ

Безпека та відповідність: Пташиний погляд на трансформацію

Як управління ідентифікацією та доступом надає бізнесу можливість безпечно працювати з будь-якого місця

MIT Technology Review Insights - планування до 2021 року: нові бізнес-моделі, великі можливості

1. Мінімізуйте перешкоди



Ерік Гейєр / IDG

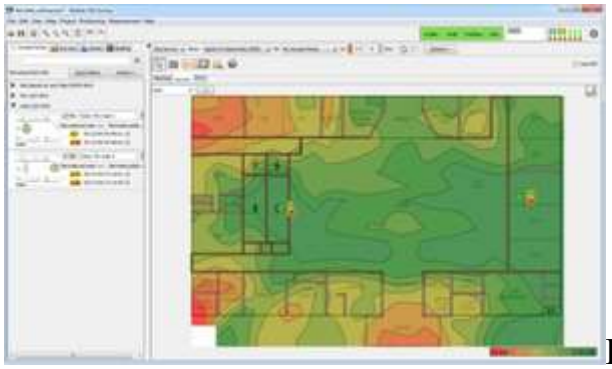
Додаток спотикача Wifi Analyzer для Android показує перешкоди спільного каналу.

Одним із перших речей, які потрібно зробити при оптимізації Wi-Fi, є зменшення або усунення перешкод. На відміну від роботи з кабелями в дротових мережах, ви не можете легко керувати транспортним середовищем Wi-Fi, ефіром. Ймовірно, існуватиме якийсь тип перешкод, з якими можна боротися, чи то з інших сусідніх мереж Wi-Fi, чи перешкод спільного каналу з вашої власної мережі, чи сигналів, що не належать до Wi-Fi, в тому ж радіочастотному спектрі.

Почніть з того, що є найбільш контрольованим, перешкодами для спільного каналу, тобто перешкодами, спричиненими наявністю двох або більше точок доступу Wi-Fi, що використовують однакові або перекриваються канали. Хоча більшість точок доступу мають функцію автоматичного каналу, яка повинна вибрати найкращий канал, перевірте їх вибір.

Перешкоди спільного каналу є більшою проблемою в діапазоні 2,4 ГГц, ніж у діапазоні 5 ГГц. У діапазоні 2,4 ГГц є 11 каналів, але лише три канали не перекриваються: 1, 6 і 11. У діапазоні 5 ГГц є до 24 каналів, і вони не перекриваються, якщо застарілі ширини каналів 20 МГц використовується. Хоча деякі точки доступу не підтримують всі канали, і більша ширина каналів спричиняє певне перекриття, діапазон 5 ГГц все ще більший.

Перевіряючи канали в менших мережах, таких як ті, що мають шість або менше точок доступу, ви можете скористатися безкоштовнимКамінник Wi-Fінаноутбукабо Пристрій Android. Ці прості програми сканують ефір та перелічують основні відомості про сусідні бездротові маршрутизатори та точки доступу, включаючи використання каналів.



Ерік Гейєр / IDG

Огляд сайту Ekahau та подібні інструменти можуть показати теплову карту перешкод спільного каналу.

Для великих мереж розгляньте можливість використання інструменту геодезичного Wi-Fi на основі карт, наприклад, відAirMagnet, Ekahau або TamoGraphпід час розгортання та для періодичних перевірок. Поряд із захопленням сигналів Wi-Fi, ці інструменти дозволяють виконати повне сканування радіочастотного спектру для пошуку перешкод, що не стосуються Wi-Fi.

Для постійного моніторингу перешкод використовуйте будь-яку функціональність, вбудовану в точки доступу, яка буде попереджати вас про неправдиві точки доступу та / або інші перешкоди.

Інструменти зйомки Wi-Fi на основі карт зазвичай пропонують деякі функції автоматизованого аналізу каналів та планування. Однак, якщо ви проводите опитування в меншій мережі за допомогою простого спотикача Wi-Fi, вам доведеться вручну створити план каналу. Почніть спочатку призначати канали точкам доступу на зовнішніх краях зони покриття, оскільки саме там найімовірніше будуть перешкоди від сусідніх бездротових мереж. Потім просуньтеся посередині, де, швидше за все, проблемою є втручання від власних точок доступу.

Детальніше про виправлення перешкодтут, а інформація про перекриття та методи роумінгу єтут.

2. Використовуйте 5 ГГц та діапазон рульового управління

Тдіапазон 5 ГГц пропонує набагато більше каналів, ніж 2,4 ГГц, тому має сенс використовувати двосмугові точки доступу, які також підтримують 5 ГГц. Це дозволяє старішим пристроям Wi-Fi підключатися в нижньому діапазоні, а новішим двосмуговим пристроям - через верхній діапазон. Менша перевантаження в нижній смузі зазвичай означає швидше з'єднання, а пристрої у верхній смузі зазвичай підтримують більш високу швидкість передачі даних, обидва з яких допомагають зменшити час роботи пристроїв. Незважаючи на те, що не всі нові пристрої Wi-Fi є двосмуговими, в наш час їх стає все більше, особливо смартфонів та планшетів вищого класу.

На додаток до підтримки 5 ГГц, розгляньте можливість використання будь-яких функцій управління смугами, передбачених точками доступу. Це може спонукати або змусити двосмугові пристрої підключатися до вищого діапазону, а не залишати це за пристроєм або користувачем.

Багато точок доступу дозволяють лише вмикати або вимикати смугове управління, тоді як деякі також дозволяють налаштовувати порогові значення сигналу, тому двосмугові пристрої, які мали б сильніший сигнал на 2,4 ГГц, не змушені використовувати 5 ГГц. Це корисно, оскільки 5 ГГц забезпечує менший діапазон, ніж нижній діапазон. Якщо ваш AP підтримує це, спробуйте скористатися налаштуванням порогу сигналу, який забезпечує хороший компроміс між зменшенням перевантажень на 2,4 ГГц, пропонуючи користувачам найкращий сигнал.

3. Використовуйте WPA2 та / або WPA3

Не секрет, що безпека WEP небезпечна, навіть якщо її підтримують практично всі точки доступу. Захищений доступ до Wi-Fi (WPA) є більш безпечним, але це залежить від використовуваної версії. Майте на увазі, що при використанні першої версії WPA швидкість передачі даних у бездротовій мережі обмежена 54 Мбіт / с, що є максимальною швидкістю за старими стандартами 802.11a та 802.11g. Щоб ви могли скористатися вищою швидкістю передачі даних, пропонованою новішими пристроями, використовуйте лише захист WPA2 та / або WPA3.

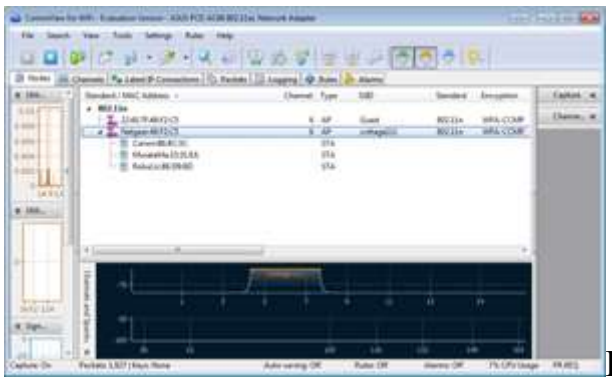
4. Зменште кількість SSID

Якщо на точках доступу у вас налаштовано більше одного ідентифікатора SSID, майте на увазі, що кожна віртуальна бездротова мережа повинна транслювати окремі маяки та пакети управління. Це споживає більше ефірного часу, тому економно використовуйте кілька SSID. Один приватний SSID та один загальнодоступний SSID, безумовно, є прийнятним, але намагайтеся уникати використання віртуальних SSID для таких речей, як відокремлений бездротовий доступ між департаментами.

Якщо потрібна сегрегація мережі, розгляньте можливість використанняАутентифікація 802.1Xдинамічно призначати користувачів VLAN

при підключенні до SSID. Таким чином ви можете мати лише один приватний SSID, але в той же час практично розділити бездротовий трафік.

5. Не приховуйте SSID


Ерік Гейєр / IDG

Цей аналізатор Wi-Fi показав прихований SSID "cottage111" після підключення пристрою до мережі.

Можливо, ви чули, що приховування імені мережі, вимкнувши SSID у радіомовній передачі, може допомогти у забезпеченні безпеки. Однак це лише приховує назву мережі від випадкових користувачів; більшість пристроїв показуватимуть, що поблизу є неназвана мережа. Крім того, кожен, хто має аналізатор Wi-Fi, зазвичай може виявити SSID, оскільки він все одно буде присутнім у деякому управлінському трафіку.

Приховування SSID також спричиняє додатковий трафік управління в мережі, наприклад запити зонду та відповіді, які займають більше ефірного часу. Крім того, приховані ідентифікатори SSID можуть заплутати та зайняти багато часу для користувачів, оскільки їм доводиться вручну вводити ім'я мережі при підключенні до Wi-Fi. Таким чином, такий підхід до безпеки насправді може принести більше шкоди, ніж користі.

Більш вигідним методом захисту є використання корпоративного режиму WPA2 та / або WPA3. Якщо ви виявите, що не всі пристрої в мережі підтримують корпоративний режим або його занадто важко налаштувати, обов’язково використовуйте довгу і міцну парольну фразу із змішаними регістрами та символами. Також розгляньте можливість періодичної зміни парольної фрази і, звичайно, після того, як будь-який користувач вийде з організації або втратить пристрій Wi-Fi.

6. Вимкніть нижчі швидкості передачі даних та стандарти

Хоча сучасні пристрої Wi-Fi можуть підтримувати швидкість вище 1 Гбіт / с, точки доступу можуть передавати лише 1 Мбіт / с на 2,4 ГГц та 6 Мбіт / с на 5 ГГц для певного трафіку. Як правило, чим далі ви їдете від точки доступу, тим нижчий сигнал і нижча швидкість передачі даних.

Однак, навіть якщо покриття мережі та сигнали відмінні, більшість точок доступу за замовчуванням надсилають управління або багатоадресний трафік, такі як маяки SSID, на дуже низьких швидкостях замість максимальних швидкостей передачі даних, як це відбувається при надсиланні регулярного трафіку даних. Збільшення мінімальної або багатоадресної швидкості передачі даних AP може змусити керуючий трафік надсилати швидше, ефективно зменшуючи загальний ефірний час.

Цей метод також може допомогти пристроям швидше автоматично підключатися до кращих точок доступу. Наприклад, деякі пристрої за замовчуванням можуть не шукати іншу точку доступу, на яку можна блукати, доки вони повністю не втратять зв’язок з точкою доступу, до якої вони наразі підключені. Це може статися, поки пристрій не пройде так далеко, що швидкість передачі сигналу та даних буде мінімальною, що підтримується точкою доступу. Отже, якщо ви збільшите мінімальну швидкість передачі даних, ви в основному скоротите максимальну зону покриття кожної точки доступу, але одночасно збільшите загальну продуктивність мережі.

Не пропонується мінімальна швидкість передачі даних, яку повинні використовувати всі мережі. Це рішення, зокрема, залежить від унікального покриття мережі та можливостей клієнта. Однак майте на увазі, що, вимкнувши нижчу швидкість передачі даних, ви можете ефективно відключити підтримку старих стандартів бездротового зв'язку. Наприклад, якщо ви вимкнете всі швидкості передачі даних зі швидкістю 11 Мбіт / с і нижче, це перешкоджає використанню пристроїв 802.11b, оскільки максимальна швидкість передачі даних цього стандарту становить 11 Мбіт / с.

Для більшості мереж вимкнення підтримки 802.11b є прийнятним, але ви можете не захотіти повністю вимикати наступні стандарти: 802.11a та 802.11g, які досягають 54 Мбіт / с. Отже, найвищі швидкості передачі даних, які ви

повинні розглянути, - це швидкість до 48 Мбіт / с, що все ще дозволяє використовувати застарілі стандарти 802.11a / g / n.

7. Правильно налаштуйте ширину каналів

Як зазначалося раніше, Wi-Fi може використовувати різну ширину каналу. Як правило, чим більша ширина каналу, тим більше даних можна надсилати одночасно і тим менше ефірного часу буде використано. Стандарти 802.11b / g підтримують лише застарілу ширину каналу 20 МГц, 802.11n додає підтримку 40 МГц, а 802.11ac і 802.11ax - ширину каналів 80 МГц і 160 МГц.

Враховуючи, наскільки мала смуга 2,4 ГГц, і щоб підтримувати 802,11 г, ви хотіли б зберегти застарілу ширину каналу 20 МГц у цій смузі. Для 5 ГГц розгляньте можливість використання параметра автоматичної ширини каналу. Хоча примусове використання каналів 80 МГц або 160 МГц дозволило б збільшити швидкість передачі даних із пристроями 802.11ac та 802.11ax, це не є хорошим підходом для більшості мереж, оскільки це завадить двосмуговим пристроям 802.11n підключатися в цій смузі.

8. Скоротіть розміри пакетів та час передачі

Існують розміри пакетів і час передачі для певного трафіку, які можна зменшити, щоб сприяти збільшенню швидкості та зменшенню ефірного часу. Якщо вони доступні у ваших точках доступу, їх можна змінити в розширених налаштуваннях бездротової мережі / радіо. Хоча ви можете побачити лише незначний приріст продуктивності для кожного окремого налаштування, ви можете помітити помітну різницю в поєднанні.

Якщо у вас немає клієнтів 802.11b, ви можете ввімкнути коротку довжину преамбули, щоб скоротити інформацію заголовка на пакетах.

Увімкнення короткого часу слоту може зменшити час будь-яких повторних передач.

Короткий інтервал охорони скорочує час, необхідний для передачі пакетів, що може збільшити швидкість передачі даних.

Агрегація кадрів дозволяє надсилати кілька кадрів за одну передачу, але використовуйте з обережністю: це може спричинити проблеми сумісності з продуктами Apple.

9. Оновіть до Wi-Fi 6 (802.11ax)

Вимкнення підтримки застарілих бездротових стандартів може допомогти збільшити швидкість керування трафіком та допомогти примусити повільні пристрої покращити AP. Але використання старих стандартів також уповільнює швидкість передачі даних для всього трафіку, навіть для пристроїв, що використовують новіші стандарти.

Якщо у вас є будь-які пристрої у вашій мережі, які підтримують лише 802.11b, g або n (Wi-Fi 4), розгляньте можливість оновлення принаймні до двосмугового Wi-Fi 5 (802.11ac) або, бажано, до Wi-Fi 6. Хоча як правило, можливо оновлення внутрішнього Wi-Fi ноутбука або настільного комп’ютера, швидший і простіший спосіб - це додати бездротовий адаптер USB.

Якщо ваші точки доступу старші за Wi-Fi 5, ви дотепер дотримувались порад і все ще боретеся зі швидкістю, спробуйте оновити точки доступу. Якщо ви розглядаєте точки доступу Wi-Fi 6, можливо, вам доведеться внести зміни до мережевих компонентів, тож ви захочетеперевірити специфікаціїінших мережевих передач, таких як маршрутизатор, комутатори та PoE-інфраструктура.

Завжди пам’ятайте, що ефірний час має вирішальне значення для бездротових мереж. Хоча вам не обов'язково потрібен надзвичайно швидкий Wi-Fi, для підтримки мереж з інтенсивним або щільним використанням може знадобитися скорочення ефіру та збільшення швидкості.

Якщо покриття прийнятне у вашій мережі, спершу спробуйте описані тут методи перед додаванням або зміною розташування точок доступу. Може бути причина низької продуктивності, яку слід вирішити, або інші способи підвищення продуктивності за допомогою простих змін налаштувань.

Оскільки у Wi-Fi так багато змінних, іноді легко звинуватити її в проблемах, які насправді пов'язані із загальними проблемами мережі. Наприклад, якщо бездротовий зв'язок повільний, реальна проблема може бути в підключенні до Інтернету або, можливо, навіть у неправильній конфігурації, як-от низька межа смуги пропускання на точках доступу.

Висновки до розділу

Цей розділ висвітлив основні будівельні блоки архітектур глобальної мережі:

- Агрегація філій
- Інтернет-краю
- Взаємозв'язок центру обробки даних
- Велике відділення

Незважаючи на те, що основні вимоги є загальними для різних ролей, вони досить суттєво відрізняються, щоб вам потрібно було зрозуміти, як вони створюються, розгортаються та вирішують проблеми. Якби одне слово описувало обладнання, необхідне для задоволення цих потреб, це слово було б гнучкістю. Інфраструктура повинна бути дуже гнучкою з точки зору подачі та швидкості, масштабу та продуктивності, багатства послуг та різноманітності інтерфейсу (якщо назвати декілька).

РОЗДІЛ 3

РЕАЛІЗАЦІЯ ПРОЕКТУ ОБ'ЄДНАННЮ ЛОКАЛЬНИХ МЕРЕЖ ОФІСІВ

Перш ніж прісупити до вибору обладнання та програмного забезпечення (далі - ПЗ) для реалізації проекту по об'єднанню локальних мереж офісів в єдину мережу через *VPN*, необхідно мати у своєму розпорядженні наступними відомостями:

1. Визначити топологію:

– *Meshed* (повнозв'язні) - кожен сайт може автоматично організувати шифрування з'єднання з будь-яким іншим сайтом;

– *Star* (зірка) - філії можуть організувати захищене з'єднання із центральним сайтом;

– *Hub and Spoke* (зв'язок через концентратор) - філії можуть з'єднуватися між собою через концентратор центрального сайту;

– *Remote Access* (віддалений доступ) - користувачі і групи можуть організувати безпечні з'єднання з одним або декількома сайтами;

– Комбінації перелічених вище методів (наприклад, топологія *Star with Meshed Center* - зірка з повнозв'язну центром, - в якій віддалені філії можуть обмінюватися інформацією з усіма членами центральної *VPN*, що має повнозв'язну топологію).

2. Визначити кількість філіалів (кількість одночасних *VPN*-з'єднань повинно підтримувати обладнання головного офісу);

3. Кількість користувачів в центральному офісі та в кожній філії;

4. Яке обладнання та / або ПЗ використовується в кожній філії (дані необхідні для врахування можливостей по використанню існуючого обладнання та / або ПЗ);

5. Дані по підключенню філій до Інтернет: призначення *IP* адреси - динамічне або статичне, швидкість каналу зв'язку;

6. Який підхід до управління інформаційною безпекою (захист периметра мережі, антивірусний безпеку) буде застосований: централізоване управління головним офісом і філіями одним адміністратором безпеки (системним адміністратором), або в кожній філії свій системний адміністратор.

Щоб мінімізувати загрози проникнення в мережу центрального офісу, необхідно приділити належну увагу захисту мереж філій організації. Використання *VPN* не гарантує надійний захист від проникнення, якщо мережі філій також не надійно захищені. Якщо зловмисник зможе отримати несанкціонований доступ до мережі філії, то він також зможе отримати доступ і до інформаційної системи головного офісу, оскільки мережі головного офісу та філії об'єднані в єдину мережу через *VPN*.

3.1. Встановити *Wireguard*-з'єднання між трьома інтернет-центрами

Таку схему підключення називають *Site-To-Site VPN* (межофісное з'єднання для зв'язку з метою розширення мережевої інфраструктури).

1. Необхідно переконатися, що зовнішній адресу одного з маршрутизаторів доступний з іншого. У разі, якщо *VPN*-тунель потрібно побудувати через Інтернет, це означає що у одного з роутерів повинен бути наданий провайдеромпублічний "білий" *IPv*4-адрес.

2. Встановіть компонент системи "*Wireguard VPN*". Зробити це можна ввеб-конфігураторі на сторінці "Загальні налаштування" в розділі "Оновлення та компоненти", натиснувши на "Змінити набір компонентів".

Встановити компонент "*Wireguard VPN*" потрібно на трьох роутерах *Keenetic*. Після цього налаштування зазначеного *VPN*-тунелю з'являться в веб-конфігураторі на сторінці "Інші підключення".

Розглянемо графічну схему мережі (рис. 3.1).

Маршрутизатору А провайдер видав публічний *IP*-адресу. На цю адресу, будуть встановлювати підключення Маршрутизатору Б і Маршрутизатору В.

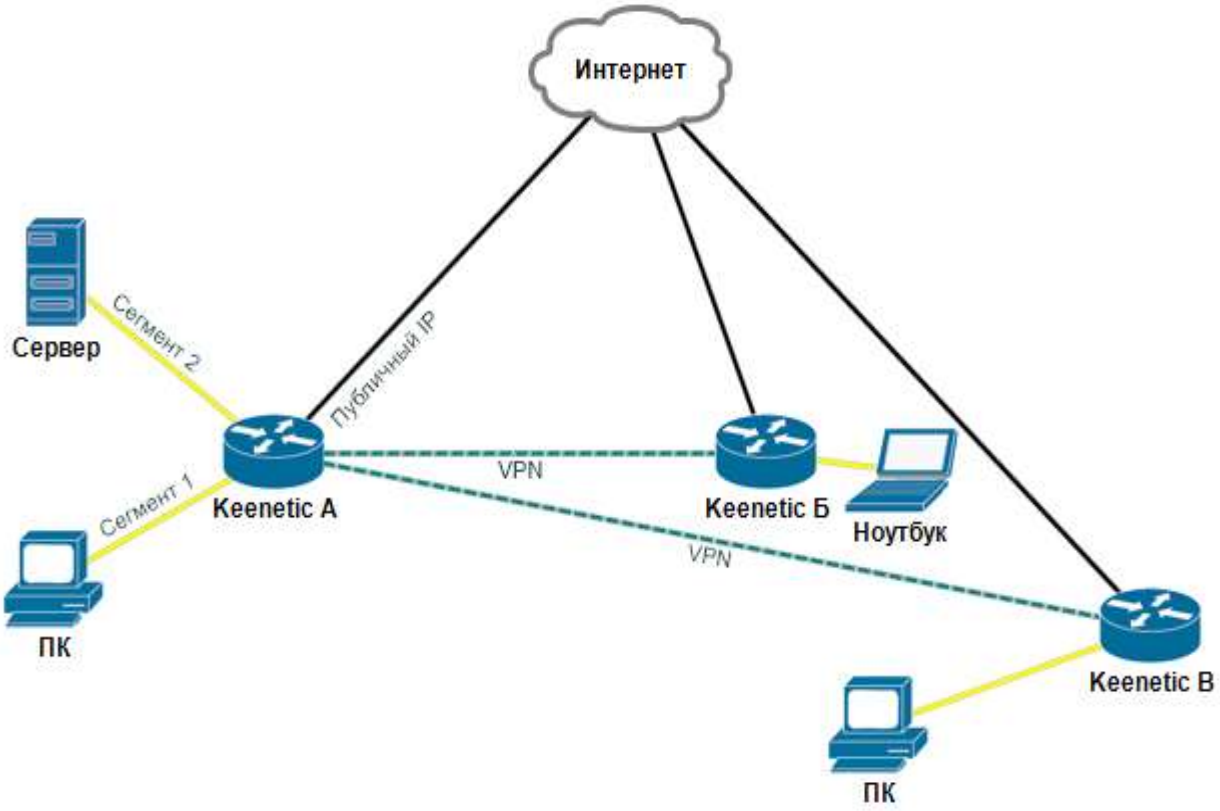


Рис. 3.1. Схема підключення віддалених філіалів

Іншими словами, інтерфейс *Wireguard* на маршрутизаторі *Keenetic* А виконуватиме роль сервера, до якого підключаються маршрутизатори віддалених офісів *Keenetic* Б і *Keenetic* В - клієнти.

У локальній мережі маршрутизатор А два локальних сегмента. До них потрібно забезпечити доступ з локальної мережі маршрутизатора Б. У зворотному напрямку, в локальну мережу Б, доступ також повинен бути забезпечений з цих двох сегментів.

Локальна мережа за *Keenetic* В повинна мати в мережі А доступ тільки до сегменту 1.

Хости в віддалених мережах Б і В, також, повинні мати можливість обмінюватися трафіком.

В якості публічного адреси, виданого провайдером на маршрутизатор А, ми використовуємо приватний *IP*-адреса 192.168.201.14. У загальному випадку, комутаційна середовище, в яке підключені всі три роутера (чорні лінії на ілюстрації) - не обов'язково глобальна мережа, це може бути і локальна мережа провайдера. На маршрутизаторі А (сервері, будемо вважати що це головний офіс

тоді як два віддалені мережі - філії Б і В) підмережа сегмента 1 має адресацію 192.168.111.1/24, сегмента 2 - 192.168.112.1/24. Локальна мережа філії Б - 192.168.15.1/24, локальна мережа філії В - 192.168.26.1.24 (табл. 3.1).

Таблиця 3.1

Таблиця адрес

Маршрутизатор	Локальна мережа	доступ Ксет	Адреса інтерфейсу тунелю
Keenetic А (головний офіс)	192.168.111.1/24	Б, В	172.16.82.1/24
	192.168.112.1/24	Б	
філія Б	192.168.15.1/24	А1, А2, В	172.16.82.2/24
філія В	192.168.26.1/24	А1, Б	172.16.82.3/24

3.1.1. Підключення *Wireguard VPN* на маршрутизаторах А і Б

В меню "Інтернет" - "Інші підключення", в розділі "*Wireguard*", потрібно натиснути кнопку "Додати підключення". Відкриється вікно налаштувань, в якому вкажіть назву тунелю - "*VPN* Б-А". За допомогою кнопки "Генерація ключів" потрібно створити пару ключів, приватний і публічний, які будуть використовуватися для захисту підключення.

В поле "Адреса" вказуємо *IP*-адреса в форматі *IP* / *bitmask* - 172.16.82.2/24 (це внутрішній адресу тунелю). Можна використовувати іншу підмережу, при цьому її слід вибрати ззарезервованих для приватного використання діапазоніві таким чином, щоб уникнути накладення з іншими налаштованими на даних пристроях подсетями. Далі потрібно натиснути кнопку "Зберегти публічний ключ в буфер обміну" (він буде потрібно на наступному кроці) і декілька разів натисніть "Зберегти" для застосування налаштувань (рис. 3.2).

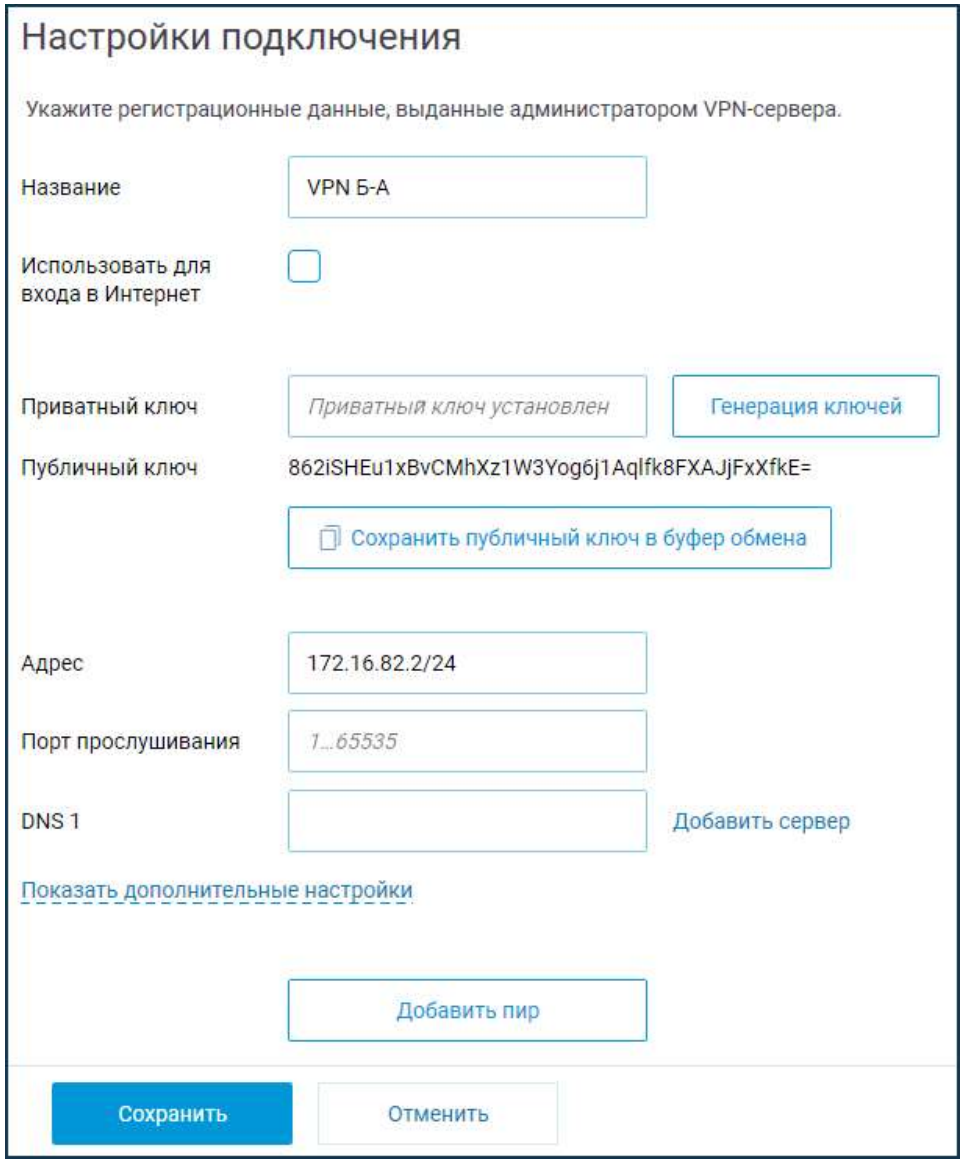


Рис. 3.2. Вікно налаштувань маршрутизатору А

На маршрутизаторі А аналогічно потрібно додати підключення, вказати назву і згенерувати пару ключів. Копіювати в буфер обміну публічний ключ А поки не треба.

Далі вкажемо адресу. Внутрішній, "технічний" адреса пристрою в тунелі має сенс вказати з уже обраної при налаштуванні інтерфейсу маршрутизатора Б підмережі - на ньому ми вказали адресу з мережі 172.16.82.2/24, на маршрутизаторі А адреса слід вказувати з цієї ж мережі. Зазначимо на кінці тунелю *Keenetic* А адреса 172.16.82.1 з маскою мережі 255.255.255.0.

Адресу можна вказати з маскою 32 біта, тобто не адреса мережі, а адреса хоста. При цьому доведеться додавати маршрут, який вказує на мережу інтерфейсу тунелю або індивідуально до кожного кінця тунелю. У разі

зазначення адреси таким чином, щоб маска охоплювала адреси всіх учасників в тунелі, що вибудовується автоматично маршрут позбавляє від необхідності вводити дані установки вручну.

Порт, вказаний в полі "Порт прослуховування", буде використаний при подальшій настройці маршрутизатора Б. На цей порт *Keenetic* Б (як і *Keenetic* В) буде звертатися при встановленні тунелю. У нашому прикладі використовуємо порт номер 16632. Цей порт маршрутизатор А автоматично відкриє на всіх інтерфейсах, щоб проходили вхідні підключення. Додатково додавати дозволяють правила мережевого екрану не потрібно.

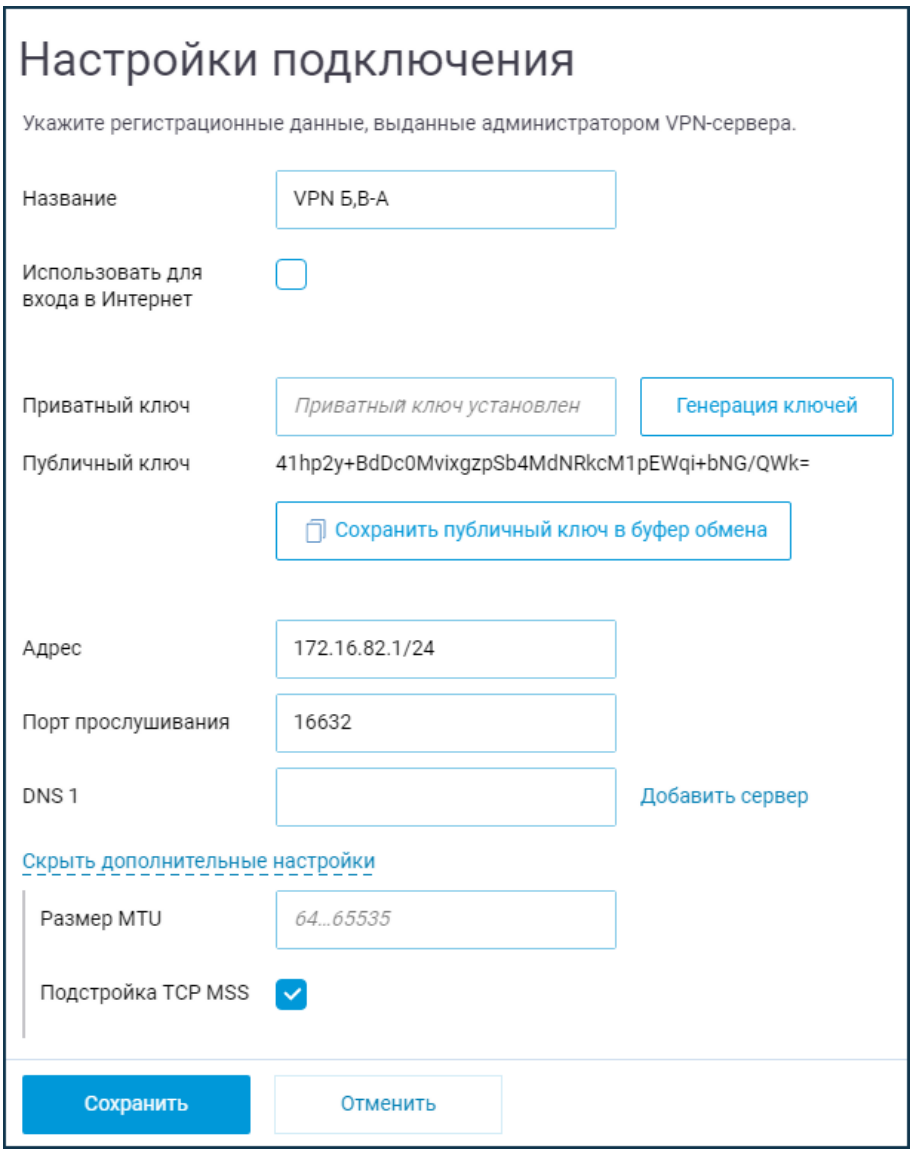


Рис. 3.2. Вікно налаштувань з’єднання маршрутизаторів А і Б

Додамо з'єднання за допомогою кнопки "Додати бенкет". Зазначимо відповідне ім'я з'єднання і публічний ключ тунелю з маршрутизатора Б. Оскільки

на попередньому кроці цей ключ був скопійований в буфер обміну, його можна зараз вставити в поле "Публічний ключ".

В полях "Дозволені підмережі" потрібно вказати адреси, трафік з яких повинен бути допущений від віддаленої сторони, і адреси, трафік до яких може бути відправлений віддаленої стороні. Це: технічний адреса віддаленого кінця тунелю - 172.16.82.2/32 (з боку бенкету Б трафік в тунелі буде йти з адресою джерела 172.16.82.2, і в нашому прикладі ми вказуємо тут явно адреса хоста, беручи до уваги що адресні простори дозволених підмереж на з'єднаннях в рамках одного інтерфейсу не повинні перекриватися), і віддалена мережа - локальна мережа маршрутизатора Б - 192.168.15.0/24 (до цієї мережі потрібно забезпечити доступ по тунелю).

В поле "Перевірка активності" необхідно вказати періодичність спроб зондування. Це внутрішня, вбудована в протокол перевірка доступності віддаленої сторони з'єднання. Зазвичай, достатньо 8-10-секундного інтервалу між перевірками.

Після чого, скопіюємо публічний ключ маршрутизатора А в буфер обміну і збережемо налаштування.

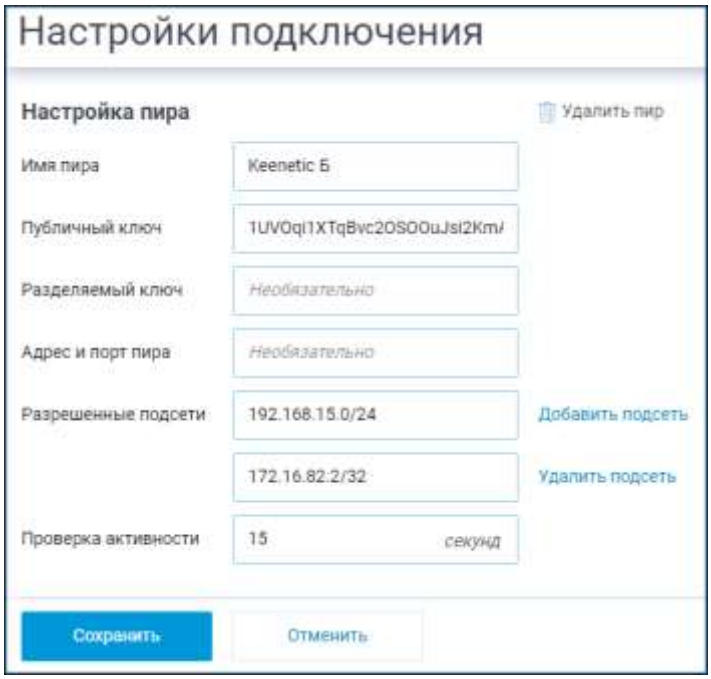


Рис. 3.3. Вікно налаштувань маршрутизатора *Keenetic* Б

Тепер, виконуємо донастройку підключення на маршрутизаторі *Keenetic* Б. Потрібно додати з'єднання, яке буде встановлюватися до маршрутизатора А.

Після клацання на рядку доданого тунелю, відкриваємо його налаштування і натискаємо кнопку "Додати бенкет" (рис. 3.4).

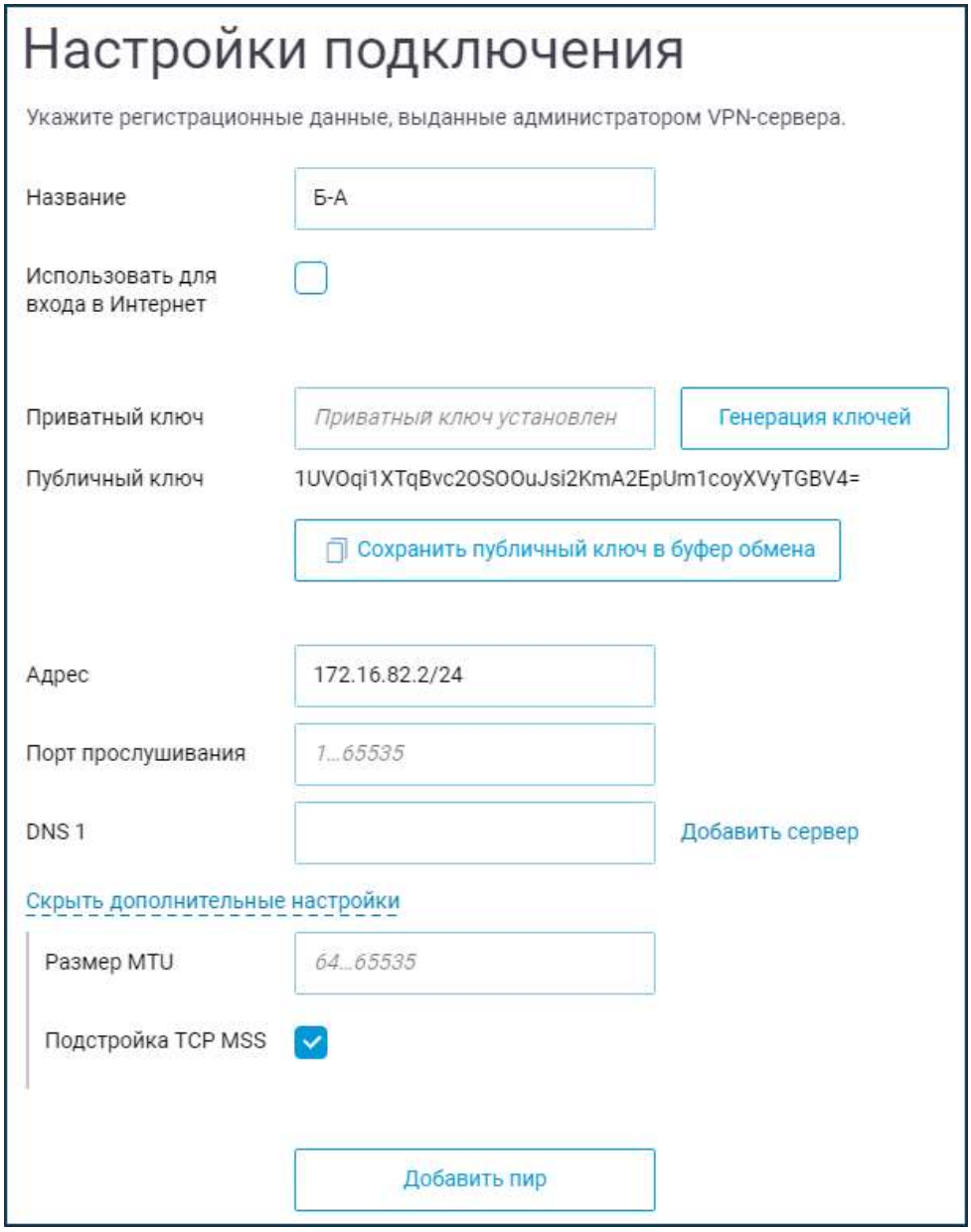


Рис. 3.4. Вікно налаштувань маршритзаторів з’єднання *Keenetic* Б і *Keenetic* А

В налаштуваннях бенкету вказуємо Ім'я бенкету (*Keenetic* А), Публічний ключ (на попередньому кроці він був скопійований в буфер обміну), адреса і порт бенкету в форматі *IP*: *port* (це публічний адресу маршрутизатора А і порт прослуховування, яка була вказана при конфігурації тунелю на маршрутизаторі А), тобто, в нашому прикладі 192.168.201.14:16632

В поле "Дозволені підмережі" потрібно внести адреси віддалених кінців тунелю, вказуємо 172.16.82.0/24, трафік з адрес цієї мережі буде прийнятий з тунелю. Додамо адреси мереж локальних сегментів 1 і 2 маршрутизатора А -

192.168.111.0/24 і 192.168.112.0/24. Вихідний трафік до цих двох мереж буде допущений до передачі по тунелю. Додамо адреси локальної мережі філії В, 192.168.26.0/24 - в цю мережу також потрібен доступ. Інтервал перевірки активності з цього боку виберемо 10 секунд. Зберігаємо установки.

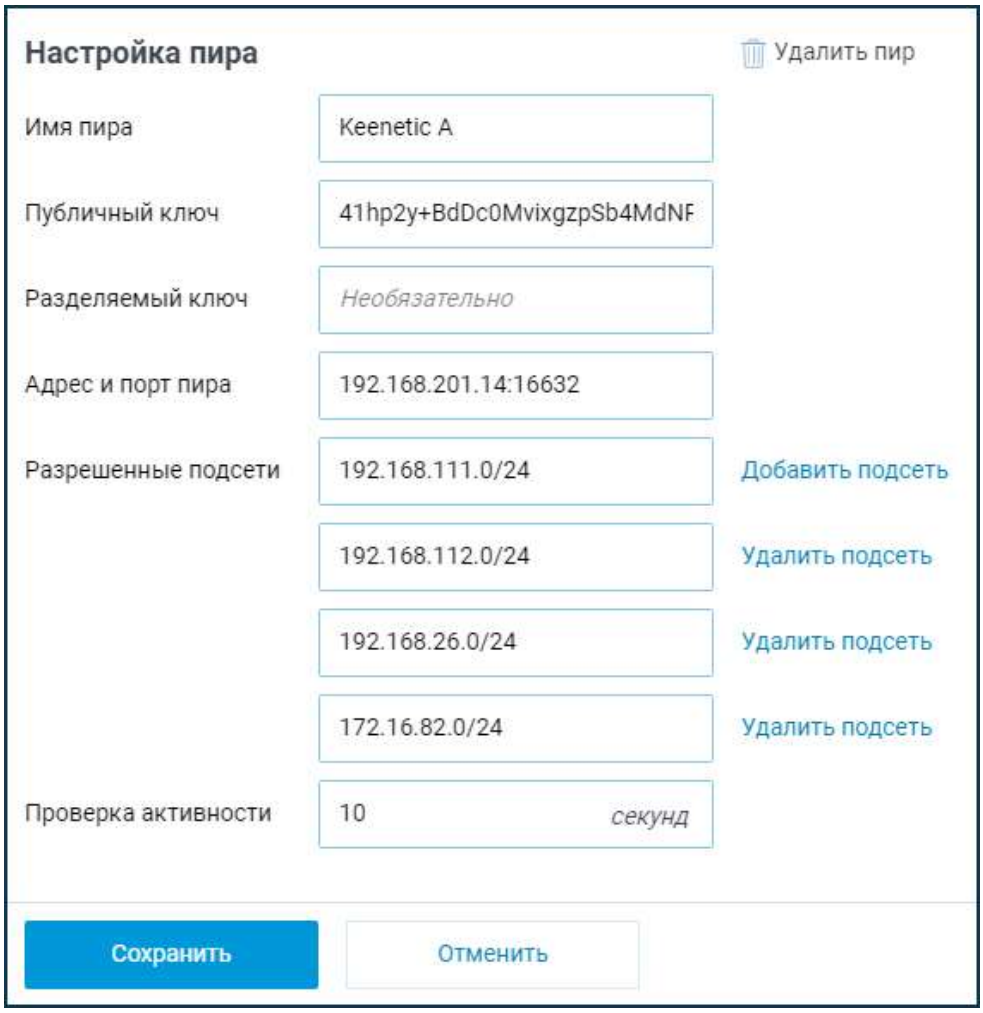


Рис. 3.5. Вікно налаштувань маршритзатора *Keenetic* A

Включимо налаштовані *VPN*-інтерфейси на маршрутизаторах А і Б. Якщо все налаштовано коректно, в полях по колонці "Бенкет" повинен відображатися зелений індикатор статусу (рис. 3.6 та 3.7).

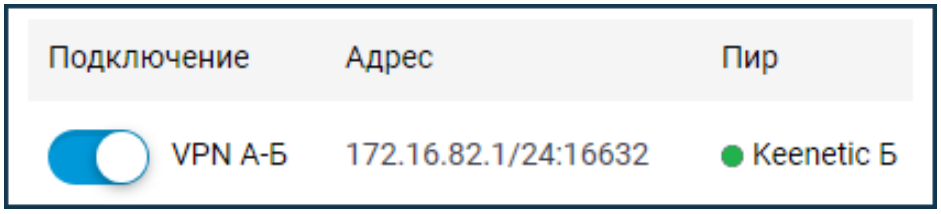


Рис. 3.6. Статус *Keenetic* A

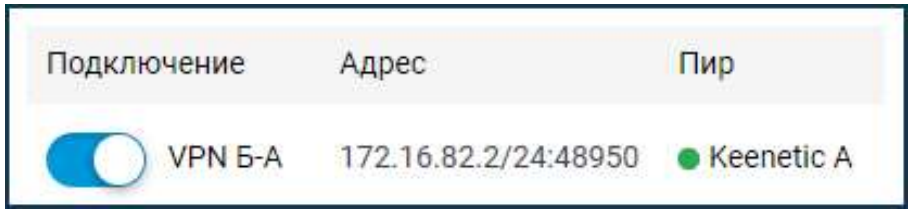


Рис. 3.7. Статус *Keenetic* Б

3.1.2. Налаштування мережевого екрану і маршрутизації.

Для роботи буде потрібно вказати маршрути і дозволити вхідний трафік на додані *VPN*-інтерфейси.

Дозволяємо входить в інтерфейс *Wireguard* трафік. Це потрібно, тому що за замовчуванням інтерфейсів тунелю встановлюєтьсяпублічний рівень безпекиі вхідний трафік заборонений. Щоб запити з віддалених мереж могли проходити по тунелю, додамо на обох роутерах відповідні налаштування в меню "Брандмауер" (рис. 3.8 та рис. 3.9).

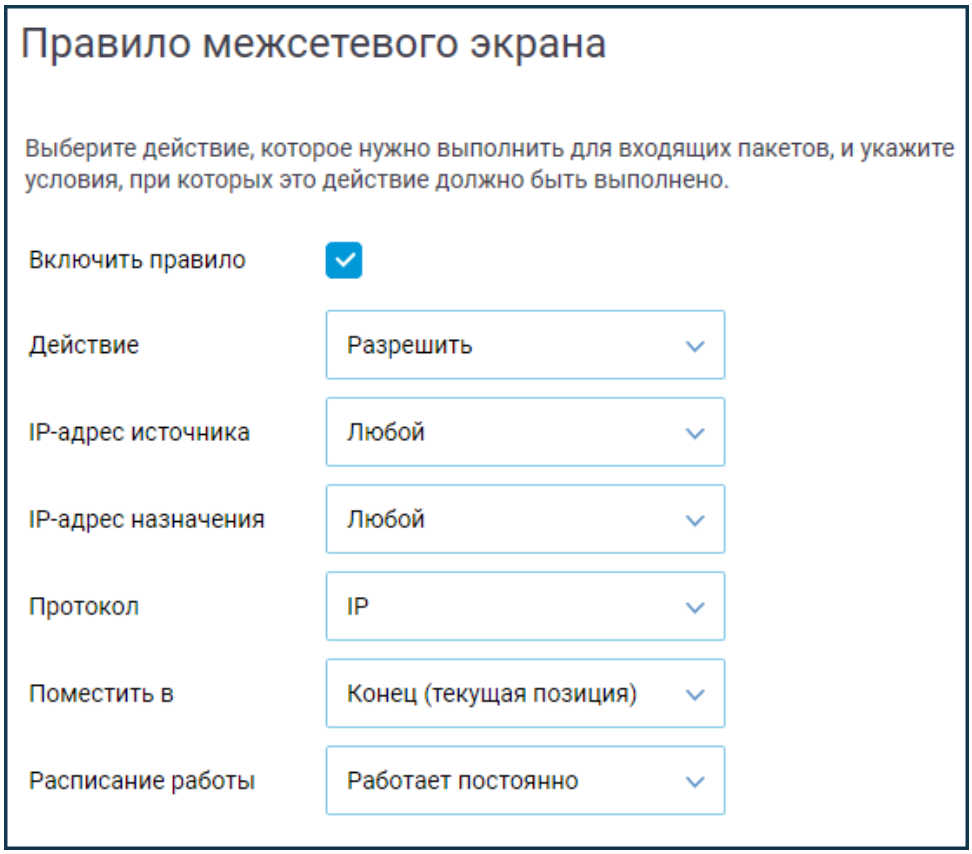


Рис. 3.8. Правила мережевого екрану

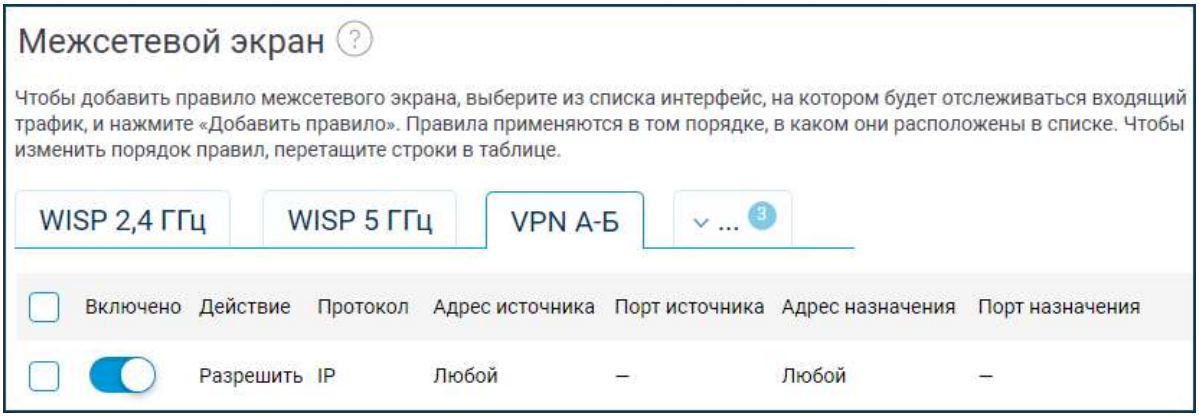


Рис. 3.9. Мережевий екран *VPN* А-Б

Технічні адреси мережі, позначеної на кінцях тунелю: 172.168.82.1 і 172.16.82.2, вже можуть на цьому етапі обмінюватися даними. Щоб по тунелю вирушав трафік в віддалені мережі, необхідні за схемою, на пристроях необхідно додати маршрути (меню "Маршрутизація" - кнопка "Додати маршрут").

Keenetic А - маршрут до мережі 192.168.15.0/24 через тунель (рис. 3.10):

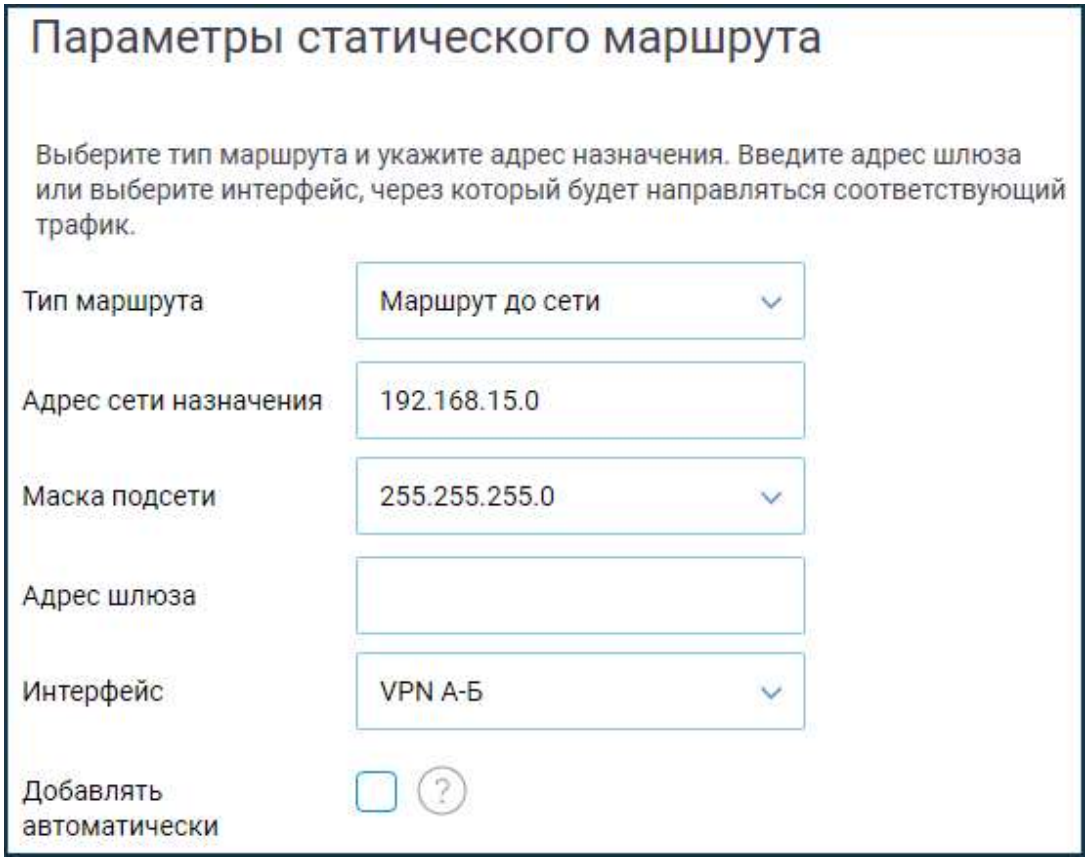
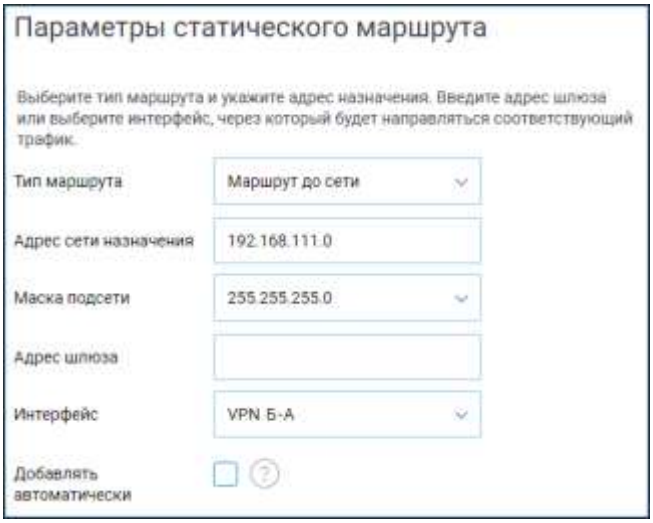
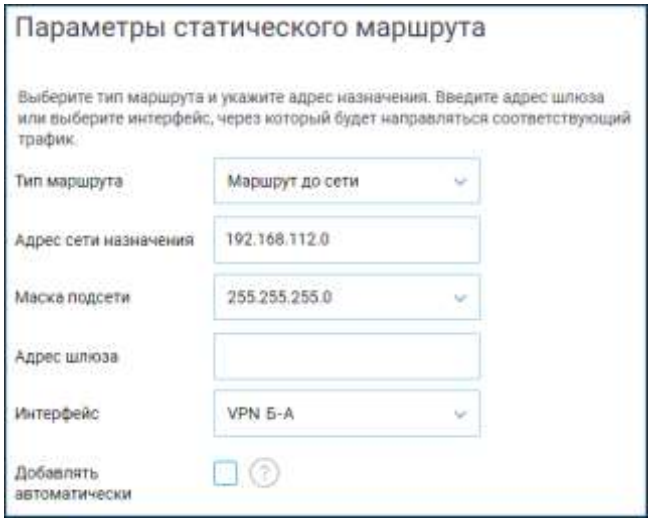


Рис. 3.10. Вікно налаштування тунелю

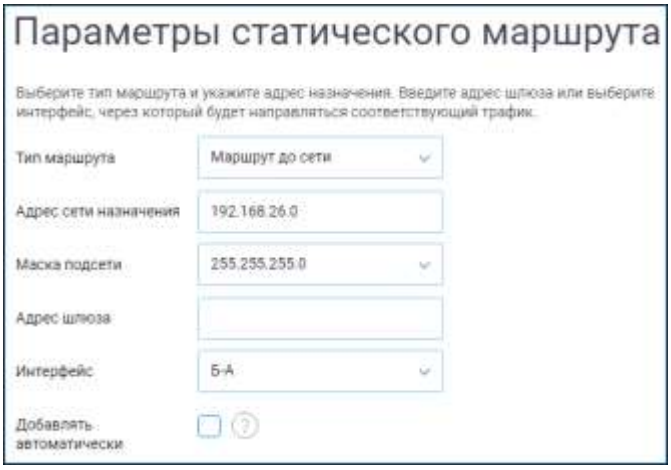
Keenetic Б - маршрути до мереж 192.168.111.0/24 і 192.168.112.0/24 і 192.168.26.0/24 через тунель (рис. 3.11):



а)



б)



в)

Рис. 3.11. Параметри налаштування тунелів: а) *VPN* Б-А для адреси 192.168.111.0, б) *VPN* Б-А для адреси 192.168.112.0, в) Б-А

Даний останній маршрут поки не може працювати, так як з'єднання третього філії не налаштоване. Завершимо настройку.

5. Налаштування з'єднання між роутерами А і В. Процедура аналогічна наведеної в пунктах 3 і 4. Публічний ключ одного з бенкетів (маршрутизатора в офісі А) у нас вже є. Скопіюємо його в буфер обміну і налаштуємо інтерфейс *Wireguard* маршрутизатора в офісі В.

3.2. Налаштування мережі на стороні віддалених філіалів

3.2.1. Налаштування мережі філіалу В

Параметри інтерфейсу *Wireguard* (рис. 3.12).

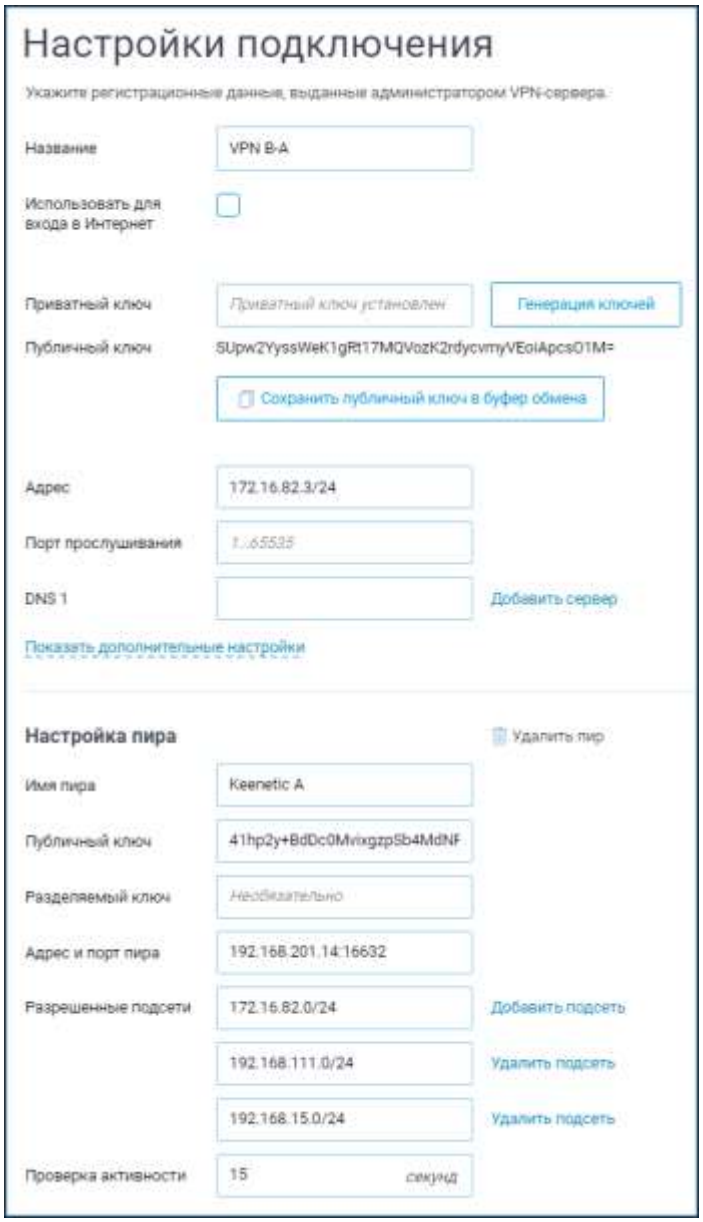


Рис. 3.12. Налаштування *Wireguard*

Налаштування мережевого екрану для інтерфейсу *Wireguard* (рис. 3.13).

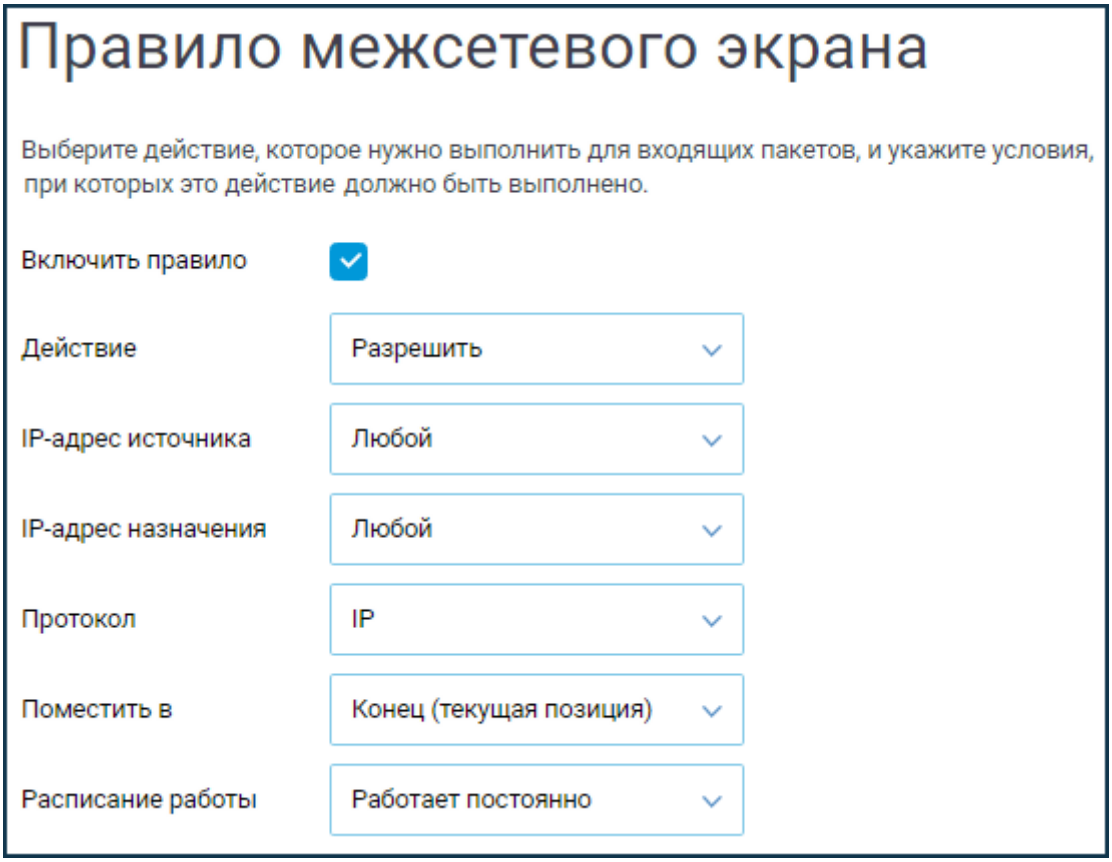


Рис. 3.13. Вікно мережевого екрану для інтерфейсу *Wireguard*

Правила маршрутизації (рис. 3.14).

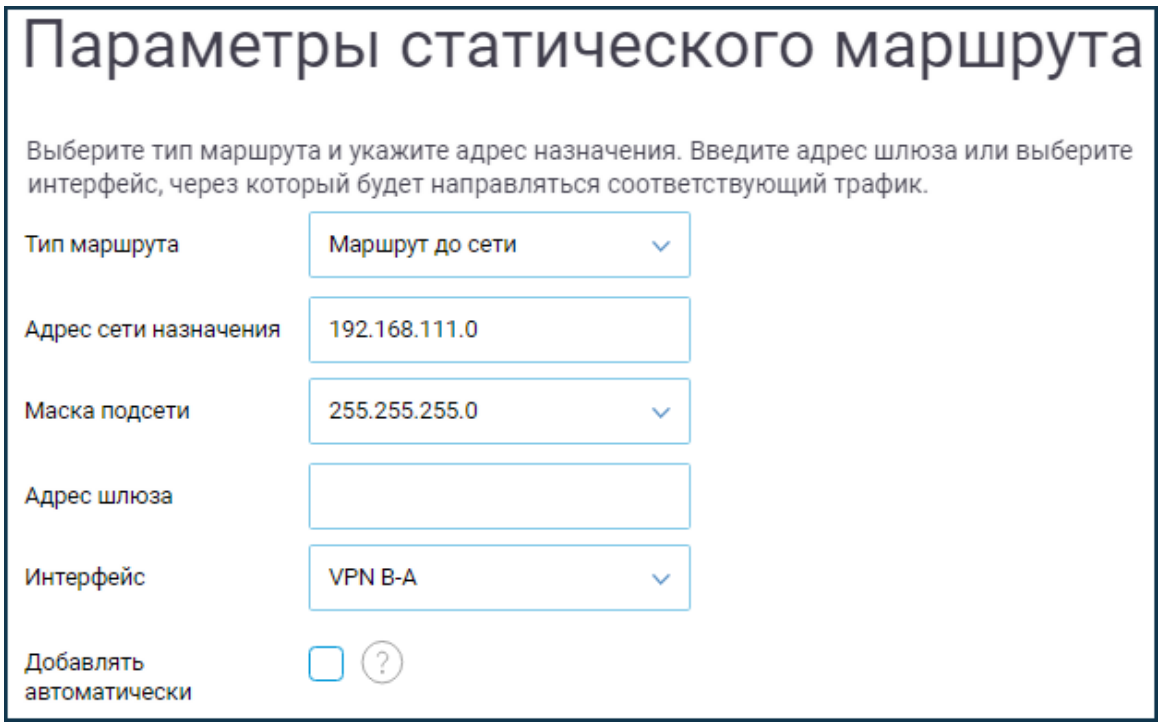


Рис. 3.14. Вікно налаштувань правил маршрутизації

3.2.2. Налаштування мережі філіалу А

Додаємо в налаштований інтерфейс *Wireguard* бенкет для офісу В.

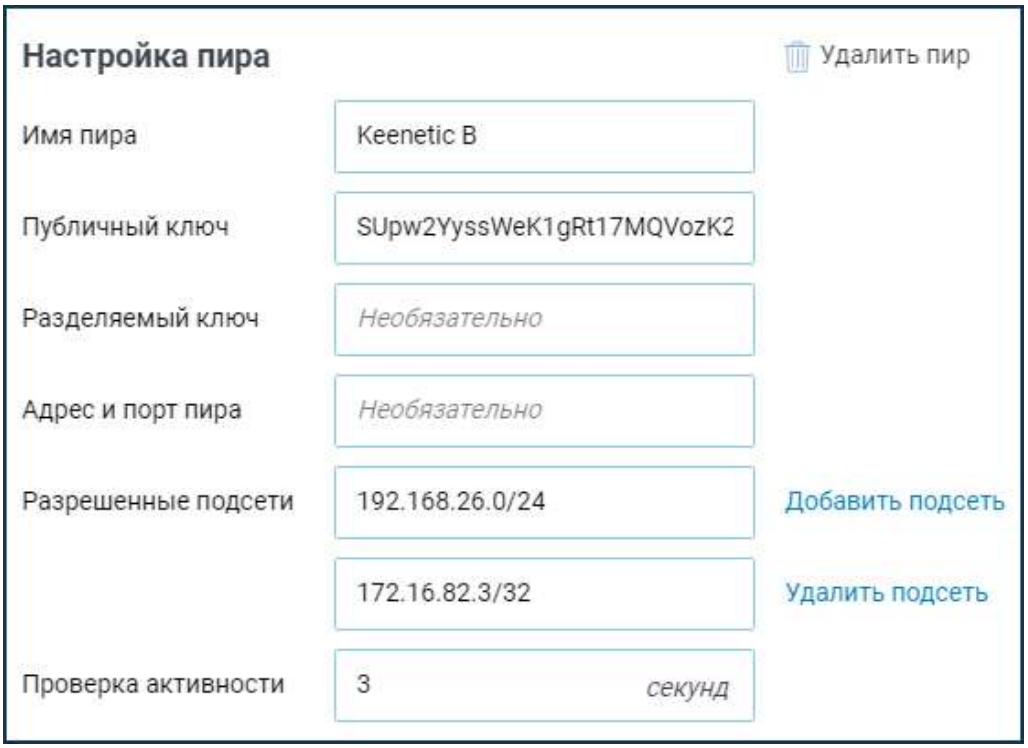


Рис. 3.15. Вікно налаштувань інтерфейсу *Wireguard* бенкет для офісу В

Також потрібно вказати маршрут до мережі 192.168.26.0/24 (рис. 3.16). На маршрутизаторі Б вже додавали цю настройку, тепер вона запрацює - після включення інтерфейсу в офісі В.

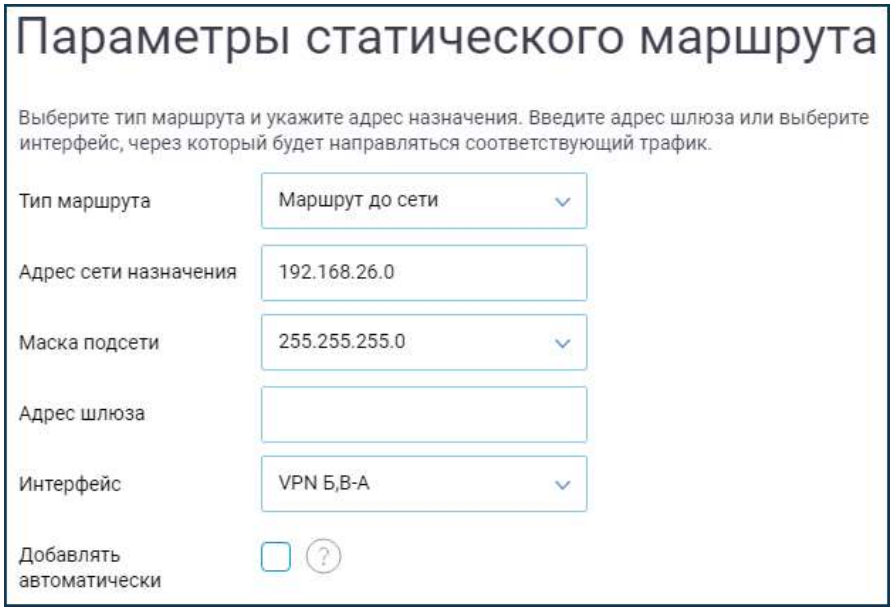


Рис. 3.16. Вікно налаштувань маршруту до мережі 192.168.26.0/24

Налаштування завершено. Його результати можна побачити у вікні на рисунку 3.17.

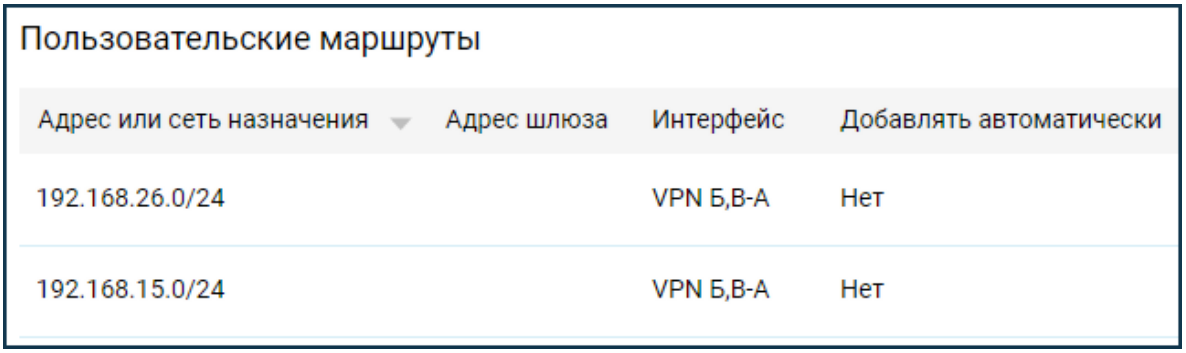


Рис. 3.17. Вікно результатів налаштування користувацьких маршрутів

Для перевірки можна виконати безпосередньо з пристроїв через меню "Діагностика" *ping* хостів в мережах, згідно з таблицею-завданням (пункт 2).

Конфігурації налаштувань наведено в додатку А.

Висновки до розділу

В даному розділі було проведено налаштування об’єднання мереж філіалів в єдину мережу через схему підключення *Site-To-Site VPN*.

Для цього було встановлено компонент "*Wireguard VPN*" на трьох роутерах *Keenetic*. Після цього проедене налаштування зазначеного *VPN*-тунелю.

Побудова єдиної захищеної корпоративної мережі для територіально розподілених об'єктів - складне комплексне завдання. При її вирішенні доводиться враховувати безліч факторів і ризиків. Про деякі з них розповідається нижче.

Більшість сучасних інформаційних систем носять розподілений характер і можуть функціонувати тільки при наявності високопродуктивної корпоративної мережі передачі даних, без якої сьогодні важко уявити роботу комерційних компаній і державних організацій.

Об'єднуючи в єдину систему всі офіси і підрозділи підприємства, корпоративна мережа дозволяє надати персоналу можливість одночасної роботи з розподіленими або централізованими програмами, базами даних та іншими сервісами.

При цьому територіально розподілені мережі повинні забезпечувати безпеку переданої інформації, володіти необхідною продуктивністю, бути зручними в адмініструванні і «прозорими» для користувачів і додатків. Це передбачає об'єднання віддалених офісів і філій в єдину інформаційно-комунікаційних структуру і формування на її базі захищеної корпоративної робочої середовища. Нерідко інфраструктурний рівень включає ще й бездротові сегменти мережі *Wi-Fi*, що забезпечують мобільність співробітників в офісі компанії

ВИСНОВКИ

В дипломному проекті було проведено налаштування об’єднання мереж філіалів в єдину мережу через схему підключення *Site-To-Site VPN*. Для цього було встановлено компонент "*Wireguard VPN*" на трьох роутерах *Keenetic* та налаштовано *VPN*-тунелі.

Вибираючи обладнання для організації віртуальної приватної мережі (*VPN*) було необхідно звернути увагу на наступні властивості:

– кількість одночасно-підтримуваних *vpn*-тунелів;

– продуктивність;

– можливість фільтрації мережевого трафіку всередині *vpn*-тунелю (ця функція реалізована далеко не у всіх інтернет-шлюзах);

– підтримка управління якістю *QoS* (дуже корисна при передачі голосового трафіку між мережами);

– сумісність з наявним обладнанням і застосовуваними технологіями.

– апаратні рішення

Переваги рішень, побудованих на недорогих апаратних інтернет-шлюзах:

– низька вартість;

– висока надійність (немає необхідності в резервному копіюванні, при відключенні харчування нічого не виходить з ладу);

– простота адміністрування;

– мале енергоспоживання;

– займає мало місця, можна встановити де завгодно;

– в залежності від обраної платформи для побудови *VPN*, є можливість для установки на *vpn*-шлюз додаткових сервісів: антивірусна перевірка інтернет-трафіку, виявлення атак і вторгнень, і ін, що істотно збільшує загальний рівень захищеності мережі і зменшує загальну вартість рішення з комплексного захисту мережі .

Недоліки рішень, побудованих на недорогих апаратних інтернет-шлюзах

– рішення не масштабується, збільшення продуктивності досягається повною заміною обладнання;

– менш гнучко в налаштуваннях;

– інтеграція з *Microsoft Active Directory* (або *LDAP*), як правило, не підтримується.

Переваги програмних рішень:

– гнучкість;

– масштабованість, тобто можливість збільшити продуктивність у міру необхідності;

– тісна інтеграція з *Microsoft Active Directory* (*Microsoft ISA* 2006, *CheckPoint*).

Недоліки програмних рішень:

– висока ціна;

– складність адміністрування.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Базові поняття мережевих технологій [Інтернет-ресурс] / Web-сайт: mobiz.com.ua; Режим доступу: https://mobiz.com.ua/bazovi-poniattia-merezhevykh-tekhnolohij.html, вільний.
2. Cisco Networking Academy Program CCNA / за ред. С.Н. Тригуба – Москва: Издательский дом «Вильямс», 2005.
3. Хилл Б. Полный справочник Cisco. / Брайан Хилл: Пер. С англ. – М. : Издательский дом «Вильямс», 2004. – 773 с.
4. Лісковський І. О. Узагальнюючий алгоритм аналізу працездатності фрагмента мережі тактової синхронізації довільної топології / І. О. Лісковський // Наукові записки Українського науково-дослідного інституту зв'язку. – 2013. – № 3. – С. 41-47.
5. Вентцель Е.С. Теория случайных процессов и ее инженерные приложения Учебное пособие для вузов. 5-е изд. / Е.С. Вентцель, Л.А. Овчаров – М : КноРус, 2013. – 441 с.
6. Беркман Л.Н., Лісковський І.О. Підвищення надійності функціонування мережі тактової синхронізації / Л.Н. Беркман, І.О. Лісковський // Збірник тез доповідей / Науково-технічний симпозіум "Нові технології в телекомунікаціях". – К.: ДУІКТ, – 2011. – С.72 – 75.
7. Филин Б.П. Методы анализа структурной надежности сетей связи. / Борис Филин. – М.: Радио и связь, 1988. – 204 с
8. Лісковський І.О. Внесення програмованої затримки в алгоритм обробки повідомлення про статус синхронізації / І.О. Лісковський // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка: зб. нукових праць. – Київ, 2008. – Вип. 11. – С. 46-50.
9. Сергееев А.П. Офисные локальные сети. Самоучитель. / Александр Сергеев. – М. : Издательский дом «Вильямс», 2003. – 320 с.
10. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов 5-е изд. / В.Г.Олифер, Н.А. Олифер. – СПб. : Питер, 2016. – 992 с.