ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до бакалаврської роботи

на тему:

«ДОСЛІДЖЕННЯ ШЛЯХІВ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ПОБУДОВИ ЗАХИЩЕНОЇ ДИСТАНЦІЙНОЇ РОБОТИ ПРАЦІВНИКІВ ОРГАНІЗАЦІЇ НА БАЗІ РІШЕННЯ CISCO SECURE VPN»

Виконав студент 4 курсу, групи БСД-41
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»

(шифр і назва спеціальності)

Матвєєв О.А.

(прізвище та ініціали)

Керівник Довженко Н.М.

(прізвище та ініціали)

Рецензент

(прізвище та ініціали)

Нормоконтролер Чумак Н.С.

(прізвище та ініціали)

КИЇВ – 2023

ВСТУП

Актуальність дослідження. У великих компаніях все частіше використовують різні додатки для досягнення своїх цілей: різноманітні хмарні сервіси, служби онлайн банкінгу тощо, в той час як працівники цих компаній не завжди захищені, адже зараз майже всі працівники працюють віддалено, із власних домівок. Цей факт є причиною для хвилювання, адже не завжди працівники використовують VPN чи інші додатки для контролю мережевого трафіку, чим і наражають на небезпеку як себе, так і компанії у яких вони працюють.

Підприємствам як ніколи важливо дбати про безпеку в Інтернеті. Оскільки більше людей, ніж будь-коли, працюють з дому, конфіденційна інформація компанії та клієнтів піддається більшому ризику крадіжки.

Якщо працівник віддалено підключається до робочого комп'ютера в загальнодоступній мережі без використання VPN. Теоретично, будь-хто з цієї публічної мережі може отримати доступ до внутрішньої мережі компанії, оскільки працівник не зробив нічого, щоб приховати свою інформацію.

Необмежений доступ до файлів компанії та інформації про клієнтів може мати катастрофічні наслідки для бізнесу. Використання VPN для підключення до бізнес-мереж може допомогти гарантувати, що конфіденційні дані будуть приховані за фіктивною інформацією, що надається через VPN.

Об'єкт дослідження — процес забезпечення безпечної дистанційної роботи працівників організації.

Предмет дослідження — методи та засоби забезпечення безпечної дистанційної роботи працівників на базі рішення Cisco Secure VPN.

Мета роботи — розробити рекомендації щодо забезпечення безпечної дистанційної роботи користувачів на базі рішення Cisco Secure VPN.

Завдання бакалаврської роботи:

– дослідити методи та засоби боротьби з атаками за допомогою VPN

– проаналізувати вплив VPN на успішність атак, переваги та недоліки;

– розробити рекомендації щодо забезпечення безпеки даних користувачів під час дистанційної роботи на базі рішення Cisco Secure VPN;

Методи дослідження — опрацювання літератури за темою, теорія інформації, технології компанії Cisco, стандарти в сфері кібербезпеки.

1 АНАЛІЗ ВПЛИВУ АТАК З ГЛОБАЛЬНОЇ МЕРЕЖІ НА КОРИСТУВАЧІВ ПІД ЧАС ДИСТАНЦІЙНОЇ РОБОТИ

1.1 Аналіз дистанційної роботи та можливих ризиків

Дистанційна робота є чудовим варіантом для більшості професіоналів, але зростання популярності роботи з будь-якого місця призвело до відповідного зростання кількості інцидентів у сфері кібербезпеки.

Дистанційна робота під час пандемії COVID-19 призвела до збільшення кількості кібератак на 238%, згідно зі звітом Alliance Virtual Offices, який надає послуги віддаленої роботи, за березень 2022 року. Вони вважають, що розширення сфери атак пов'язано з віддаленою роботою та зростаючим використанням хмарних технологій, що є проблемою для фахівців кібербезпеки.

Такі тенденції призвели до того, що 78% IT-директорів, опитаних постачальником програмного забезпечення для забезпечення безпеки Lumu Technologies, назвали поліпшення безпеки для віддалених співробітників і управління вразливостями на основі оцінки ризиків найважливішими проектами у 2022 році.

1. *Вплив віддаленої роботи на кібербезпеку*. На думку багатьох експертів з кібербезпеки, віддалена робота може підвищити ризик витоку даних або інших кібератак. Дистанційна робота значно збільшує потенційну масштабність будь-якої атаки.

Компанія Gartner повідомила, що 60% інтелектуальних працівників працюють віддалено і щонайменше 18% не планують повертатись до офісу. Дистанційні працівники іноді ще більше розширюють простір для різних типів атак шляхом впровадження несанкціонованих технологій.

Дистанційна робота не лише розширила потенційну масштабність атак, але й вивела за межі традиційні засоби захисту систем, такі як брандмауери та системи виявлення вторгнень, які організації традиційно встановлювали та

налаштовували для запобігання атакам витоку даних та іншим видам кіберзлочинів.

Більше того, кіберзлочинці користуються переходом до віддаленої роботи, використовуючи вразливості в компаніях, які забезпечують віддалену роботу.

2. *Ризики які можуть виникати.* Ризики кібербезпеки, пов'язані з віддаленою роботою, численні та різноманітні, включаючи дефіцит навичок безпеки, вразливі мережі, хмарні технології та робочі звички співробітників.

Зі збільшенням кількості працівників, які працюють віддалено, в організаціях збільшується кількість кінцевих точок, мереж і програмного забезпечення, яке потрібно захищати, що значно збільшує навантаження на відділи кібербезпеки, які і так часто працюють на межі своїх можливостей.

Кадрові проблеми в деяких організаціях можуть призвести до затримок у забезпеченні належного захисту віддалених працівників.

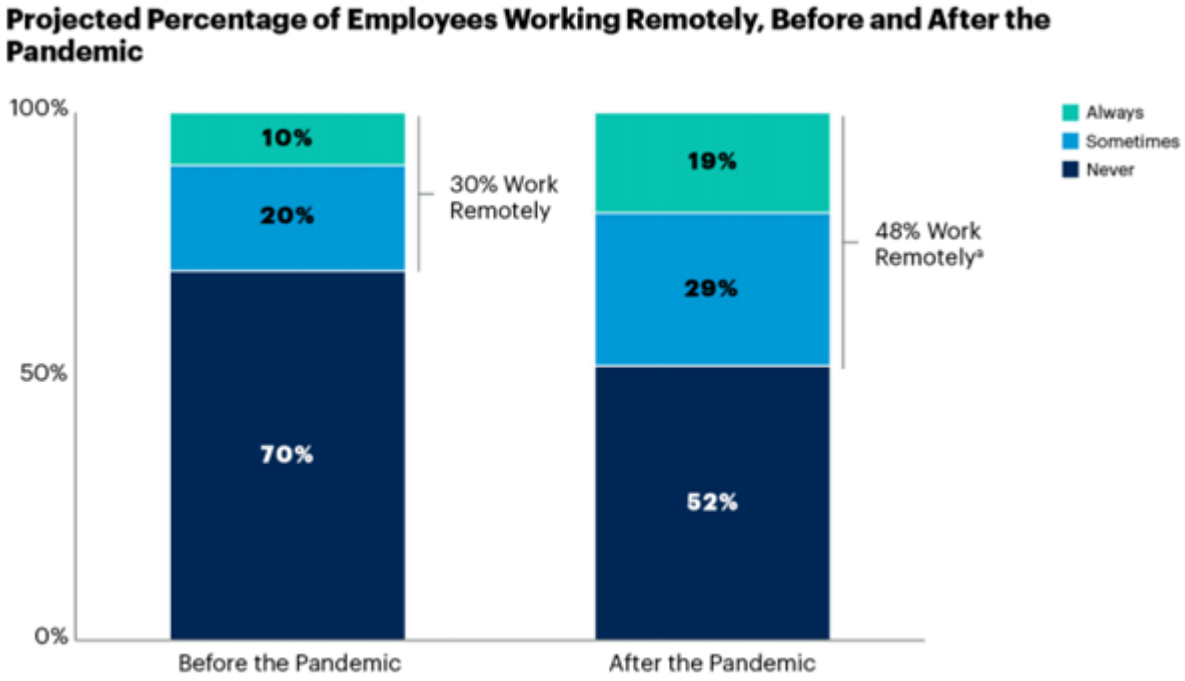

Рис.1.1. Статистика кількості віддалених працівників в компаніях до пандемії та після

У глобальному дослідженні про прогалини в навичках кібербезпеки за 2022 рік постачальник послуг мережевої безпеки Fortinet показав, що 60% з 1223 опитаних лідерів IT та кібербезпеки заявили, що їм важко наймати талановитих

фахівців з кібербезпеки, а 52% намагаються утримати кваліфікованих працівників, тоді як 67% визнали, що дефіцит кваліфікованих кандидатів у сфері кібербезпеки створює високі ризики для їхніх організацій.

За своєю природою віддалена робота виводить частину доступу до системи, мережевого трафіку і даних за межі традиційних периметрів корпоративного технологічного середовища і моніторингу безпеки в цьому середовищі. Компанії, як правило, не можуть поширити моніторинг на всі кінцеві точки і всі мережі, які підтримують віддалену роботу.

Працівники з різних причин можуть завантажувати конфіденційну інформацію на свої локальні пристрої, які можуть бути зашифровані, а можуть і не бути зашифрованими. Заради ефективності вони також можуть ділитися конфіденційними даними компанії незахищеними каналами, наприклад, незашифрованою електронною поштою або файлами, не усвідомлюючи ризиків[1].

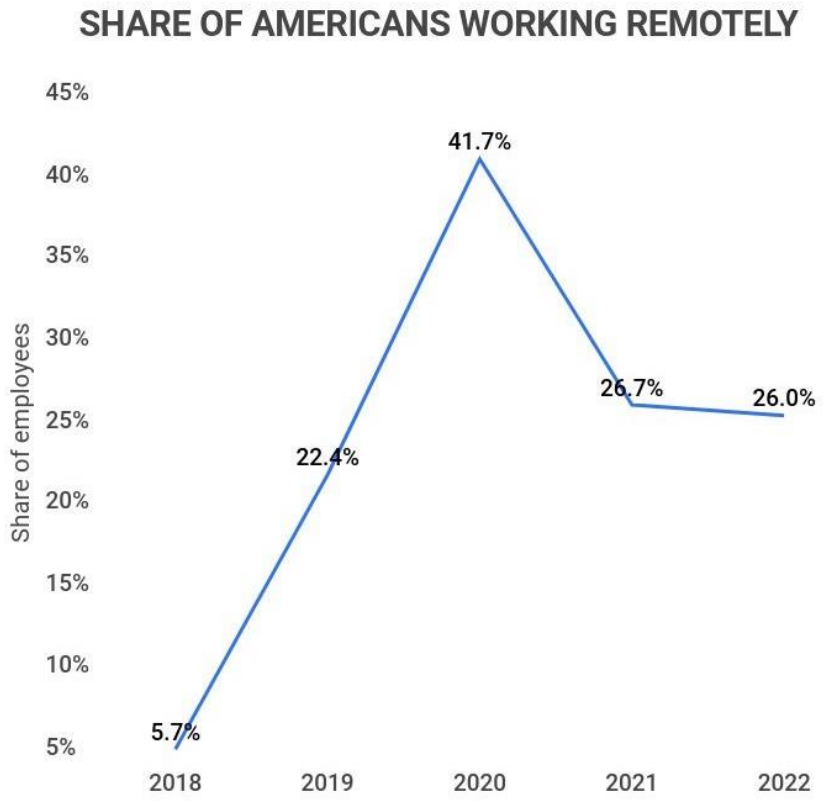

Рис.1.2. Статистика кількості працюючих віддалено американців з 2018 по 2022 рік

1.2 Вплив кібератак на підприємства та уряд

1. Вплив кібератак на бізнес. Кіберзлочинці частіше обирають своєю мішенню підприємства та компанії, оскільки вони, як правило, мають більше прогалин у системі безпеки, що робить їх більш вразливими до атак.

Хоча найчастіше атакують енергетичний, фінансовий та технологічний сектори, всі види бізнесу можуть стати мішенню і зазнати наступних короткострокових і довгострокових наслідків.

a) Втрата продуктивності. Коли шкідливе програмне забезпечення розгортається на підприємстві, воно часто може зупинити роботу на кілька годин, а то й днів.

Для прикладу буде розглянуто атаку віруса-вимагача на Colonial Pipeline у травні 2021 року. Хоча було зламано лише частину комп'ютерної системи, яка впливала на білінгову інфраструктуру, їм довелося вимкнути всю систему, що керувала трубопроводом, щоб зменшити збитки.

Хоча це один з найбільш екстремальних прикладів, майже кожна компанія, яка зазнає кібератаки, змушена частково або повністю припинити свою діяльність до усунення наслідків атаки, чи то шляхом виплати викупу, видалення шкідливого програмного забезпечення з пристрою, мережі або системи, чи то відновлення резервної копії системи.

b) Втрата доходів. Витрати на кібератаку можуть завдати шкоди бізнесу. Незалежно від того, чи доведеться зупинити роботу на кілька днів, сплатити викуп, втратити дані, замінити пристрої або заплатити експерту з безпеки за видалення шкідливого програмного забезпечення з системи чи мережі, середня вартість витоку даних для малого та середнього бізнесу становить значну частку від їх доходів. Це не охоплюючи подальші витрати, включаючи оплату повідомлень клієнтам, кредитний моніторинг і навіть регуляторні штрафи.

c) Втрата репутації. Найсерйознішим наслідком кібератаки для бізнесу є втрата репутації. Наприклад, витоки даних, від яких постраждали Equifax, Target і J.P. Morgan Chase - кожна з цих компаній втратила персональні дані своїх

клієнтів, включно з номерами соціального страхування, інформацією про банківські рахунки та номери кредитних карток. Хоча вони мали ресурси для відновлення, більшість компаній не оговтуються від порушень безпеки, оскільки втрачають довіру клієнтів, а отже, втрачають бізнес.

Для прикладу буде розглянуто атаку віруса-вимагача на Colonial Pipeline - ця компанія транспортує бензин, дизель і авіаційне паливо з Техасу до Нью-Йорку, і на її трубопровід припадає майже 45% палива, що використовується на Східному узбережжі.

Коли трубопровід було зупинено, мільйони людей відчули нестачу пального, і навіть авіакомпанії були змушені скасовувати і перенаправляти рейси, щоб компенсувати дефіцит.

2. Вплив кібератак на уряд. Найбільше занепокоєння при кібератаці на державну установу викликає величезний обсяг даних, які можуть бути втрачені, починаючи від інформації про окремих громадян, яка може бути продана і закінчуючи питаннями національної безпеки та військовими даними, які можуть бути використані терористичними організаціями.

1.3 Основні різновиди кібератак

а) Атаки на основі шкідливого програмного забезпечення (програми вимагачі, трояни тощо).

Шкідливе програмне забезпечення - це програмне забезпечення, яке призначене для порушення роботи або викрадення даних з комп'ютера, мережі або сервера. Хакери обманом змушують користувачів встановити шкідливе програмне забезпечення на ваші пристрої. Після встановлення шкідливий скрипт запускається у фоновому режимі і обходить систему безпеки, надаючи хакерам доступ до ваших конфіденційних даних і можливість навіть перехопити управління. Шкідливе програмне забезпечення - один з найпоширеніших способів кібератак. Існує кілька його різновидів:

- Програми-вимагачі. Цей тип шкідливого програмного забезпечення шифрує файли у вашій системі, щоб ви не могли отримати до них доступ, поки не заплатите (зазвичай у криптовалюті). Нещодавній звіт з 2023 року показав, що 75% з 1400 опитаних організацій зазнали атак з використанням програм-вимагачів, що свідчить про їхню постійну поширеність у діловому світі[2].
- Шпигунські програми. Як випливає з назви, цей тип шкідливого програмного забезпечення шпигує за вашими діями та надсилає дані назад хакеру. Це можуть бути банківські реквізити, логіни та паролі.
- Кейлоггери. Клавіатурні шпигуни схожі на шпигунські програми, за винятком того, що вони відстежують дії користувача. Все, що вводить користувач (і сайт, на якому він це робить), надсилається хакеру і може бути використане для шантажу або крадіжки особистих даних.
- Трояни. Названі на честь відомого троянського коня, ці типи шкідливих програм маскуються всередині легітимного програмного забезпечення. Наприклад, користувач може завантажити те, що вважає антивірусним програмним забезпеченням, але насправді його пристрій буде інфіковано.
- Віруси. Віруси приєднуються до програм і файлів і запускаються, коли їх відкривають. Ставши активним, вірус може самовідтворюватися без вашого відома і сповільнювати роботу вашого пристрою або знищувати дані. Існують також хробаки - віруси, які переміщуються мережею від одного зараженого комп'ютера до іншого, надаючи хакерам віддалений доступ до всієї вашої системи.

Атаки на основі шкідливого програмного забезпечення можуть використовуватись для атак як на окремимих користувачів, так і для атак на різні підприємства та організації.

У травні 2021 року компанія JBS USA, найбільший у світі постачальник м'яса, зазнала атаки програми-вимагача, який зупинив виробництво на багатьох її заводах. Зрештою, компанія заплатила викуп у розмірі 11 мільйонів доларів у біткоїнах, щоб запобігти подальшим збиткам.

b) Фішингові атаки (фішинг зі списом, китобійний фішинг тощо)

Фішингова атака відбувається, коли кіберзлочинець надсилає шахрайський електронний лист, текст (так званий смішинг) або телефонний дзвінок (так званий вішинг). Ці повідомлення виглядають так, ніби вони від офіційної особи або компанії, якій довіряє користувач - наприклад, від банку або компанії Microsoft, Apple чи Netflix.

Насправді ці повідомлення надсилаються від самозванців. Якщо користувач на них відповість, вказавши конфіденційну інформацію, наприклад, свій пароль, шахраї можуть використати її, щоб заволодіти його акаунтами, банківськими рахунками тощо[3].

Фішингові та смішингові повідомлення також можуть містити вказівки натиснути на посилання або відкрити вкладення електронної пошти, які або завантажать шкідливе програмне забезпечення на пристрій користувача, або перенаправлять його на фішинговий сайт, призначений для крадіжки конфіденційної інформації.

У багатьох випадках фішингові атаки не націлені на конкретних осіб (це полегшує їх виявлення). Однак з'явилося кілька нових видів фішингових кібератак, які є більш цілеспрямованими і їх важче виявити. До них відносяться:

- Фішингові атаки зі списом.Ці атаки зазвичай надсилаються електронною поштою і націлені на конкретну особу. Хакер використовує особисту інформацію користувача, яку він купив у Dark Web (або знайшов у соціальних мережах тощо), щоб зробити її більш правдоподібною і змусити користувача натиснути на посилання.
- Китобійний фішинг. Китова фішингова атака відбувається, коли хакер націлюється на високопоставлених осіб, наприклад, на керівників та менеджерів. Мета - викрасти їхні облікові дані та отримати доступ до мережі їхньої компанії..
- Фішингові атаки Angler. Атака Angler - це новий тип фішингового шахрайства, в якому хакер заманює користувачів у соціальних мережах, прикидаючись акаунтом служби підтримки клієнтів відомої компанії. Шахраї створюють акаунти на кшталт @AmazonHelp$, а потім автоматично відповідають на відповідні повідомлення, надаючи посилання для зв'язку з представником

певної компанії, але насправді це шахрайство, спрямоване на крадіжку інформації.

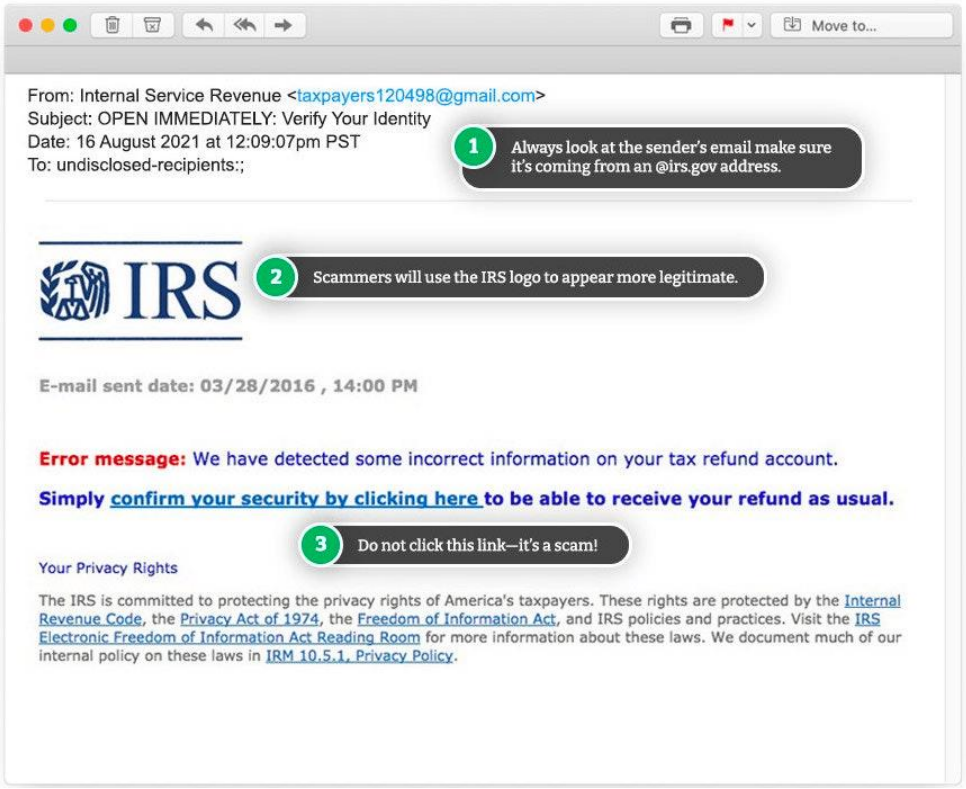

Рис.1.3. Фішингова атака

c) Атаки типу людина посередині.

Атака людина посередині (MitM) відбувається, коли зловмисники перехоплюють дані або компрометують мережу, щоб "підслуховувати" користувачів. Ці атаки особливо поширені при використанні публічних мереж Wi-Fi, які можна легко зламати.

Наприклад, користувач користується Wi-Fi у кав'ярні Starbucks і хоче перевірити баланс свого банківського рахунку, він буде заходити у систему, хакер в цей час може перехопити його дані та отримати ім'я користувача і пароль (а потім зняти кошти з його рахунку).

MitM-атаки також можуть використовуватися для "підміни" розмов. Хакери втручаються у розмову і видають себе за іншу людину, співрозмовника.

d) Атаки на відмову в обслуговуванні (DoS і DDoS)

Відмова в обслуговуванні (DoS-атака) відбувається, коли комп'ютер надсилає на сервер або ресурс велику кількість запитів даних, перевантажує його можливості і робить його недоступним для інших користувачів.

Розподілена атака на відмову в обслуговуванні (DDoS-атака) є розширеною версією DoS-атаки. Ця атака також передбачає порушення нормального потоку трафіку на сервер шляхом перевантаження його фіктивними запитами. Однак, на відміну від DoS-атаки, DDoS-атака передбачає надсилання цих запитів з декількох комп'ютерів у різних місцях[4].

Під час типової DDoS-атаки зловмисник обирає вразливу комп'ютерну систему. Зловмисник через свій комп'ютер запускає подальші атаки на інші системи. Він робить це, знаходячи інші вразливі системи та отримуючи доступ до них за допомогою шкідливого програмного забезпечення. Зрештою, кількість заражених комп'ютерних систем (ботів), множиться і створює ефект доміно. Ця мережа ботів називається ботнетом і контролюється зловмисником через командно-контрольний сервер. Боти засипають цільовий сервер численними запитами і роблять його недоступним для обслуговування справжніх користувачів. Ботнети можуть бути неймовірно складними і містити сотні тисяч окремих ботів.

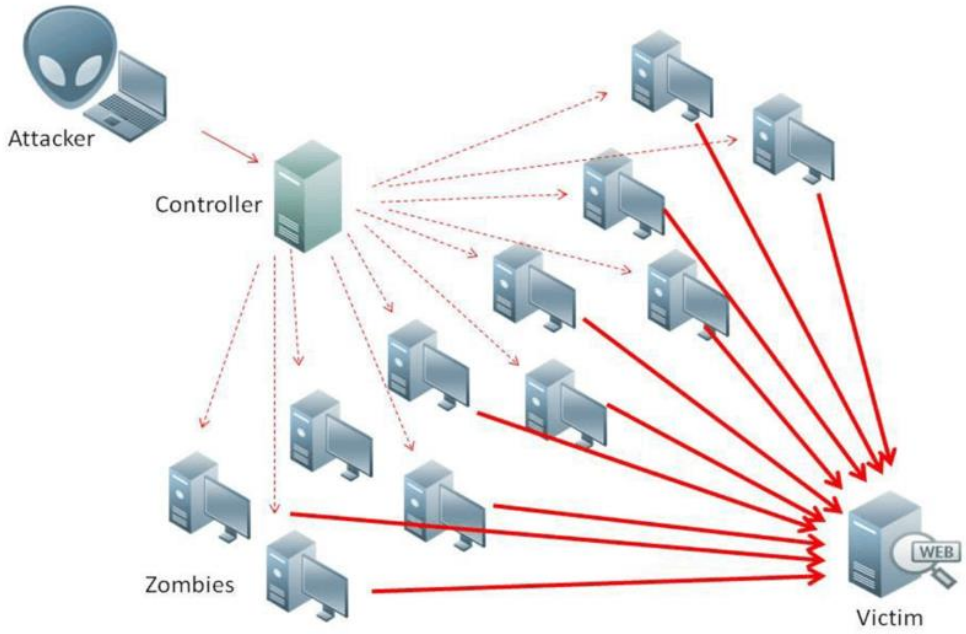

Рис.1.4. DDoS атака

1.4 Тенденції розвитку кібератак

Звіт Check Point про кібербезпеку за 2023 рік озирається на 2022 рік, коли кількість кібератак досягла історичного максимуму. Освіта та наука залишаються найбільш націленими секторами, але кількість атак на сектор охорони здоров'я зросла на 74% у порівнянні з минулим роком. Загалом, глобальні кібератаки зросли на 38% у 2022 році порівняно з 2021 роком[5].

Основні моменти Звіту з кібербезпеки за 2022 рік включають:

- Вимагання викупу - Атрибуція операцій з використанням програм-вимагачів та відстеження суб'єктів загрози може стати ще складнішою, а існуючі механізми захисту, які базуються на виявленні активності шифрування, можуть виявитися менш ефективними. Замість цього основна увага буде зосереджена на знищенні даних та виявленні витоків інформації.
- Хактивізм - Межі між державними кібероперaціями і хактивізмом були розмиті, оскільки національні держави діяли з певним ступенем анонімності. Недержавні хактивістські групи в сучасному світі краще організовані та ефективніші, ніж будь-коли раніше.
- Хмара - Загроза з боку третіх осіб - кількість атак на хмарні мережі на одну організацію значно зросла - на 48% у 2022 році порівняно з 2021 роком, що свідчить про те, що зловмисники надають перевагу скануванню діапазону IP-адрес хмарних провайдерів, отримуючи легший доступ до конфіденційної інформації або критично важливих сервісів.
- Озброєння законних інструментів - Для боротьби з сучасними рішеннями кібербезпеки зловмисники розробляють і вдосконалюють свої методи атак, які все менше покладаються на використання особистого шкідливого програмного забезпечення, натомість цього переходять до використання інструментів без підписів[6].

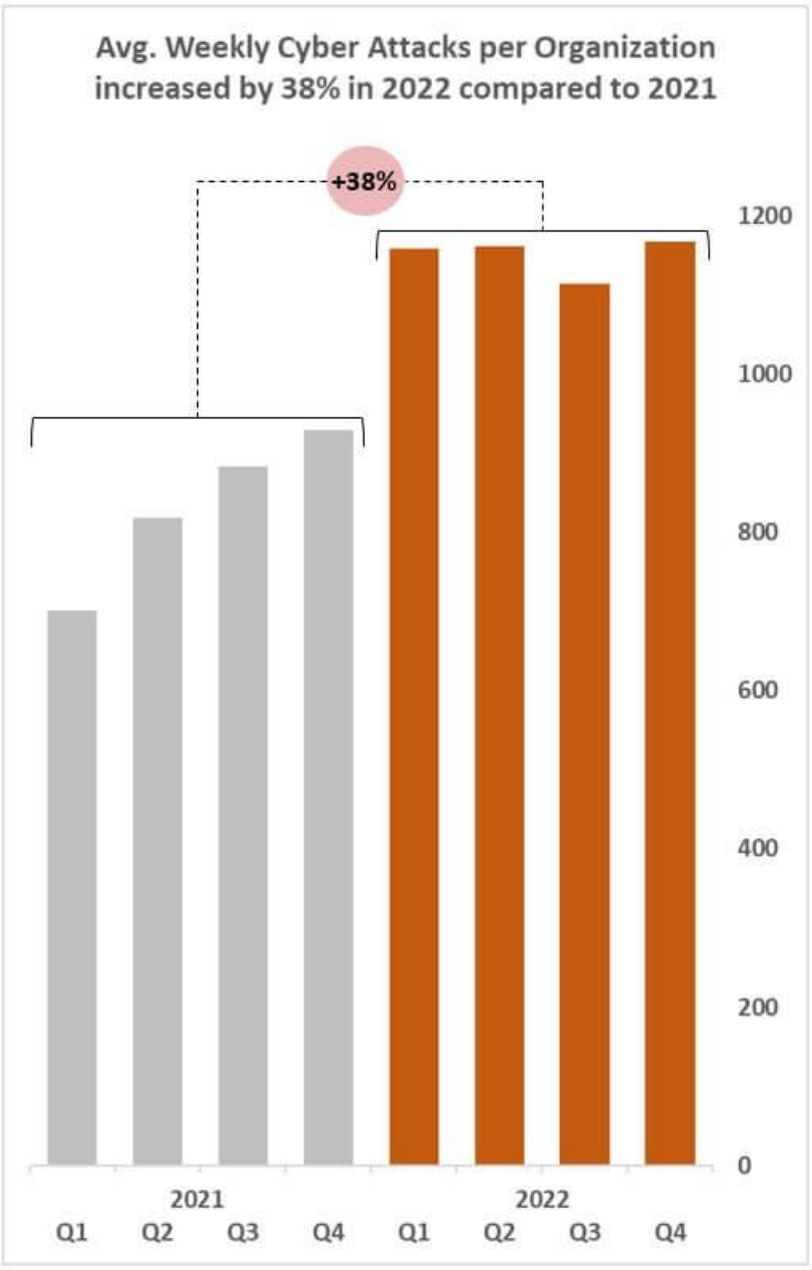

Рис.1.5. Звіт щотижневих кібератак на одну організацію у 2022 році порівняно з 2021 роком

Сектор освіти/досліджень посів перше місце за кількістю атак у світі: у 2022 році кількість атак зросла на 43% порівняно з 2021 роком, при цьому щотижня на одну організацію припадало в середньому 2 314 атак. Багато навчальних закладів виявилися погано підготовленими до несподіваного переходу на онлайн-навчання, що створило широкі можливості для хакерів проникати в мережі будь-якими способами[7].

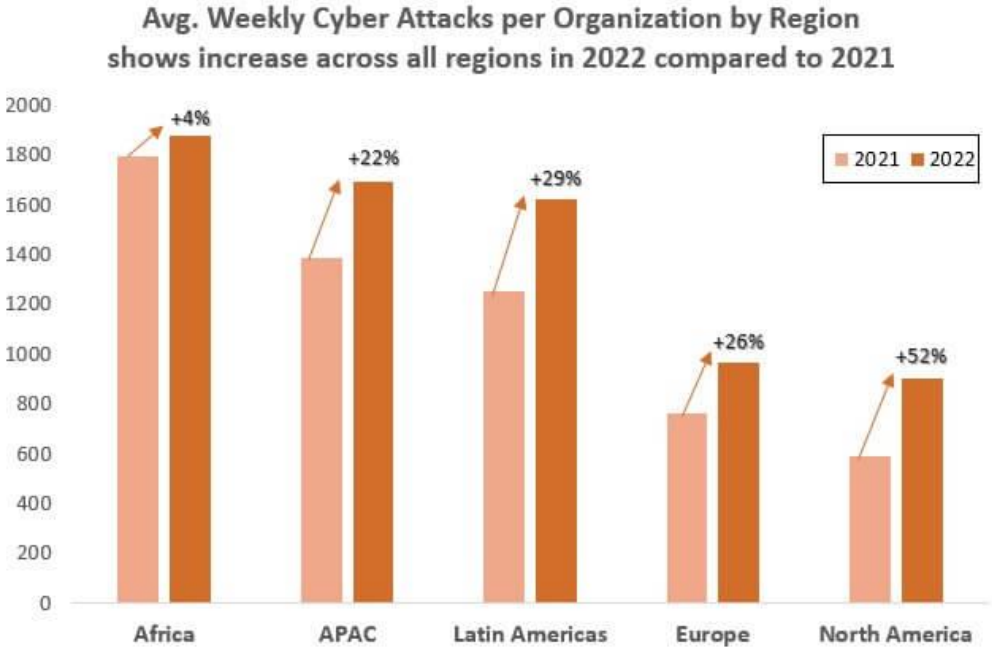

Рис.1.6. Звіт щотижневих кібератак на кожну організацію за регіонами у 2022 році порівняно з 2021 роком

1.5 Наслідки дій зловмисників

Наслідки кібератак можуть бути різними, починаючи від зупинення функціонування компації, та закінчуючи витоком всіх данних. В найгіршому випадку компанія може втратити репутацію, а це своєю чергою призведе до втрати довіри користувачів до компанії, що означає її знищення[8]. Далі буде розглянуто детальніше інформація про витоки даних:

- Витік даних це несанкціонована передача даних з організації до будь-якого зовнішнього джерела відома як витік даних. Ці дані можуть витікати фізично або в електронному вигляді через жорсткі диски, USB-пристрої, мобільні телефони тощо, а також можуть бути оприлюднені публічно або потрапити до рук кіберзлочинців.
- Витрати на витік даних. IBM виявила, що середня світова вартість витоку даних у 2022 році була найвищою за всю історію проведення цих звітів. Вартість витоку даних у 2022 році склала $4,35 млн - на 12,7% більше, ніж у 2020 році, коли вона становила $3,86 млн[9].

Рис.1.7. Середня вартість витоку даних за галузями, Звіт про вартість витоку даних за 2022 рік, IBM Security

- Галузі в яких найбільше зростає вартість витоку даних. Вже 12-й рік поспіль галузь охорони здоров'я демонструє найвищі витрати, пов'язані з порушеннями. Охорона здоров'я є однією з найбільш регульованих галузей і вважається урядом США критично важливою інфраструктурою.

Середня вартість порушення у сфері охорони здоров'я у 2022 році становила $10,1 млн, що на 9,4% більше, ніж у 2021 році, коли середня вартість становила $9,23 млн. Ці витрати також приблизно в два-п'ять разів перевищують витрати в інших галузях.

Витрати фінансової галузі також зросли у 2022 році порівняно з 2021 роком. Зростання на 4,4% призвело до того, що загальна середня вартість склала $5,97 млн порівняно з $5,72 млн у 2021 році.

У 2022 році до п'ятірки найдорожчих галузей увійшли охорона здоров'я, фінанси, фармацевтика, технології та енергетика - та ж п'ятірка, що й у 2021 році. Промислова галузь, до якої входять хімічні, інженерні та виробничі організації, і яка посідає сьоме місце в списку витрат на витоки даних, продемонструвала зростання витрат на 5,4% порівняно з 2021 роком, в результаті чого вартість витоку для цієї галузі в середньому склала 4,47 млн доларів США.

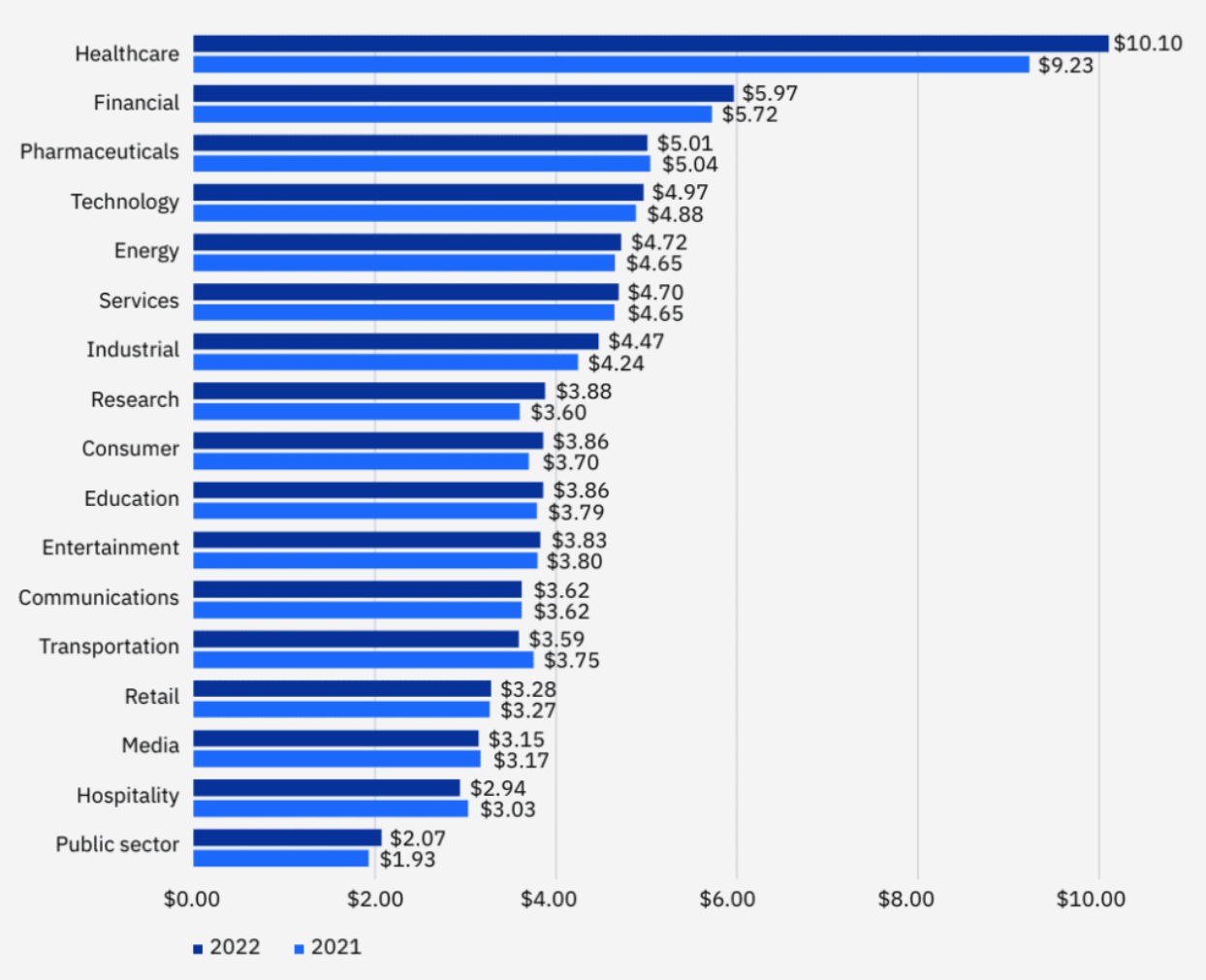

Рис.1.8. Середня вартість витоку даних за галузями, Звіт про вартість витоку даних за 2022 рік, IBM Security

Наслідки кібератак у Європі та Північній Америці. 5 лютого 2023 року Національне агентство з кібербезпеки Італії (ACN) попередило про поширення програм-вимагачів на тисячах комп’ютерних серверів у Європі та Північній Америці. У Європі наразі найбільше постраждали Франція, Фінляндія та Італія. Вразливими залишаються США і Канада.

Атака спрямована на вразливості в технології VMware ESXi, які були виявлені раніше. Ці типи серверів у минулому були мішенню хакерів через їх уразливість. Однак ця вразливість сервера не була повністю виправлена, залишаючи відкритими двері для нових хакерських атак.[10]

Франція була першою країною, яка виявила атаку. Французьке агентство з кібербезпеки ANSSI у п'ятницю випустило сповіщення, щоб попередити організації про необхідність виправлення вразливості.

За оцінками, тисячі комп'ютерних серверів були скомпрометовані по всьому світу, і ця кількість, ймовірно, зросте. Слід звернути увагу організацій на те, що слід вжити заходів, щоб уникнути блокування доступу до своїх систем.

Окрім цього, хакерам вдалося зламати акаунти армії Великої Британії в твіттері та на ютубі. Також, члени кібергрупи Anonymous зламали сайт російської державної корпорації з атомної енергії «Росатом». За даними звіту Microsoft, який було опубліковано минулого року, російські хакери займаються «стратегічним шпигунством» проти урядів, аналітичних центрів, бізнесу та груп допомоги, що належать країнам-союзникам України.

2,4 ТБ витоку даних Microsoft. Нещодавно компанія Microsoft підтвердила, що через неправильну конфігурацію сервера Microsoft в Інтернет потрапила велика кількість конфіденційної інформації про деяких клієнтів компанії[11].

Загалом SOCRadar виявив понад 65 000 витоків інформації, які стали надбанням громадськості.

Дослідники безпеки з SOCRadar, компанії, яка спеціалізується на розвідці загроз, попередили Microsoft 24 вересня 2022 року, що на сервері стався витік.

Перелік інформації, що піддався ризику наданий компанією Microsoft, включає наступну інформацію:

1.Імена

2.Адреси електронної пошти

3.Вміст електронної пошти

4.Назви компаній

5.Номери телефонів

6.Бізнес-файли

На кінцевій точці, де було виявлено витік, ненавмисно було зроблено неправильну конфігурацію, що призвело до витоку. Витік не стався внаслідок вразливості системи безпеки, тому не може бути звинувачений у цьому.

Аналітики з кібербезпеки ідентифікували інформацію для більш ніж 150 000 компаній з 123 країн у шести великих публічних ресурсах.

Крім того, в результаті витоків було виявлено велику кількість даних, в тому числі:

1.Понад 335 000 електронних листів;

2.Понад 133 000 проектів;

3.Понад 548 000 вразливих користувачів.

Висновки до першого розділу

Проаналізовано ризики під час дистанційної роботи працівників, різновиди кібератак, їх вплив на наш світ та тенденції їх розвитку.

Розглянуто наслідки дій зловмисників на різні компанії з урахуванням їх витрат на усунення проблем по звіту IBM Security, які можуть досягати мільйонів доларів США.

Зазначено, що при зупиненні функціонування компанії вона втрачає значну частину своїх доходів за кожну годину зупинки, після чого втрачає власні кошти на усунення проблеми яка власне і спричинила цю зупинку функціонування.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ТА ЗАСОБІВ БОРОТЬБИ З АТАКАМИ ЗА ДОПОМОГОЮ VPN

2.1 Методи та засоби боротьби з кібератаками

1. Першим і найголовнішим кроком у підтримці кібербезпеки є створення унікального та оригінального пароля для кожного облікового запису. Користувачі також повинні пам'ятати про оновлення паролів кожні три місяці.

2. Важливо стежити за оновленням програмного забезпечення, оскільки кіберзлочинці часто використовують відомі недоліки в програмному забезпеченні, щоб отримати доступ до системи користувача.

3. Кіберзлочинці можуть переглядати публікації в соціальних мережах у пошуках інформації, яка зазвичай використовується в питаннях безпеки, наприклад, ім'я домашнього улюбленця або дівоче прізвище матері. Щоб протистояти цьому ризику, користувачі соціальних мереж повинні зробити свій обліковий запис приватним або уникати розкриття конфіденційної інформації в публікаціях.

4. Віртуальна приватна мережа (VPN) це чудовий спосіб захистити конфіденційні дані, особливо під час доступу до публічної мережі Wi-Fi. VPN шифрує всю інформацію, що передається пристроєм користувача, і допомагає запобігти багатьом видам кібератак[12].

Для захисту бізнес-процесів та даних, потрібно в першу чергу:

1. Захищати обладнання;

2. Створювати резервні копії;

3. Шифрувати дані;

4. Інвестувати в кібербезпеку;

5. Використовувати надійне програмне забезпечення.

Ці кроки допоможуть знизити ризики та забезпечити безперебійну роботу бізнесу.

2.2 Принцип дії VPN та його типи

VPN - це послуга, яка маскує IP-адресу користувача. Це дозволяє йому користуватися інтернетом анонімно, оскільки ніхто не може пов'язати його дані з IP-адресою.

VPN - узагальнена назва технологій, що дають змогу забезпечити одне або кілька мережевих з'єднань поверх іншої мережі[13].

Далі буде розглянуто приклад користування VPN у пару кроків:

Крок 1. Підключення до VPN-сервера. Спочатку потрібно вімкнути програму VPN. Програма підключить комп'ютер до VPN-сервера, який виступатиме посередником між комп'ютером користувача і будь-якими серверами, до яких він хоче отримати доступ. Багато VPN-провайдерів дозволяють вибрати країну або місто сервера, щоб користувач міг переглядати місцевий контент.

Крок 2. Тунелювання VPN. Після підключення до VPN-сервера, він зашифрує всі дані, які користувач завантажує або надсилає, і відправить їх туди і назад через тунель.

Тунель VPN - це захищене з'єднання, за допомогою якого VPN-сервер отримує доступ до будь-яких серверів і використовує наскрізне шифрування для доставки або отримання даних від вашого VPN-клієнта.

Після цього, клієнт користувача розшифровує дані і показує йому веб-сайт або вміст, до якого він отримав доступ.

Ці дані все одно проходять через провайдера користувача, але провайдер їх не бачить, оскільки вони зашифровані. Провайдер бачить лише те, що користувач передає дані на VPN-сервер і з нього.

Більшість VPN мають політику працювати без журналів, тому вони також не зберігають жодних даних про веб-серфінг користувача.

Не існує єдиного способу шифрування даних, оскільки VPN використовують різні протоколи безпеки. Деякі з найпопулярніших VPN-протоколів у 2023 році включають: OpenVPN, Internet Key Exchange Version 2

(IKEv2), PPTP, протокол тунелювання захищених сокетів (SSTP), протокол тунелювання другого рівня (L2TP), Wireguard

Крок 3. Шифрування, інкапсуляція та дешифрування VPN. Коли користувач отримує доступ до сайту або онлайн-сервісу, VPN-сервер спочатку завантажує призначені для користувача дані і шифрує їх. Потім він передає зашифровані дані назад на його комп'ютер. Після цього, комп'ютер користувача розшифровує дані за допомогою VPN-клієнта або розширення, яке він використовує.

Багато VPN також використовують інкапсуляцію для обгортання окремих «пакетів даних» у пакети, створені VPN, тому провайдер не може зробити жодних здогадок про те, що робить користувач.

Цей процес може здатися трудомістким, але насправді він займає лише частку секунди. Комп'ютер і VPN-сервер виконуватимуть цей триступеневий процес незліченну кількість разів, поки користувач будете переглядати сторінки в мережі.

VPN поділяються на три основні категорії:

1. VPN віддаленного доступу. Віддалені працівники, мобільні працівники та віддалені офіси з мінімальною пропускною здатністю глобальної мережі можуть скористатися перевагами віддаленого доступу до VPN. Віддалений доступ VPN розширює корпоративну мережу для цих користувачів через загальнодоступну інфраструктуру, зберігаючи при цьому політику корпоративної мережі на всьому шляху до користувача. Віддалений доступ до VPN є основним типом VPN, який використовується сьогодні. Вони забезпечують безпечний доступ до корпоративних додатків для віддалених працівників, мобільних користувачів, філій та ділових партнерів. Ці VPN реалізуються через загальнодоступні інфраструктури з використанням ISDN, комутованих, аналогових, мобільних IP, DSL і кабельних технологій. Ці VPN вважаються загальними, оскільки вони можуть бути створені в будь-який час практично з будь-якого місця в Інтернеті. Електронна пошта є основним додатком, що використовується цими з'єднаннями, за нею йдуть додатки для роботи з базами даних та автоматизації офісу.

Деякі з переваг, які можна отримати від переходу від приватних мереж до VPN з віддаленим доступом, є наступними:

- Можна відмовитися від модемів і термінальних серверів та пов'язаних з ними капітальних витрат.

- Витрати на міжміський зв'язок та номери 1-800 можуть бути значно зменшені, оскільки користувачі VPN телефонують на місцеві номери провайдерів або підключаються безпосередньо через свої постійні широкосмугові з'єднання.

-Розгортання нових користувачів спрощується, а підвищена масштабованість VPN дозволяє додавати нових користувачів без збільшення витрат на інфраструктуру.

- Передача управління та обслуговування комутованої мережі третім особам дозволяє корпорації зосередитися на своїх бізнес-цілях, а не на обслуговуванні мережі.

Незважаючи на безліч переваг, не слід забувати про недоліки при впровадженні VPN-рішень:

- IPSec має невеликі накладні витрати, оскільки йому доводиться шифрувати дані, коли вони залишають комп'ютер, і розшифровувати дані, коли вони входять в комп'ютер через тунель. Хоча накладні витрати невеликі, вони можуть вплинути на роботу деяких програм.

- Для користувачів з аналоговим модемним підключенням до Інтернету зі швидкістю 40 кбіт/с або менше, VPN може спричинити незначне зниження швидкості передачі даних, оскільки IPSec вимагає часу на обробку даних.

- IPSec чутливий до затримок. Оскільки використовується загальнодоступна інфраструктура Інтернету, немає ніяких гарантій щодо розміру затримки, яка може виникнути на кожній ділянці з'єднання під час проходження тунельних даних через Інтернет. Це не повинно викликати серйозних проблем, але про це слід пам'ятати. Користувачам може знадобитися періодично відновлювати з'єднання, якщо пороги затримки перевищено. VPN з віддаленим доступом можуть ініціювати тунелювання і шифрування або на комутованому клієнті, або

на сервері мережевого доступу (NAS). У таблиці 2.1 наведено деякі відмінності між цими двома підходами.

Таблиця 2.1.

Відмінності між Client-initiated model та NAS-initiated model

Тип моделі	Характеристики
Ініційована клієнтом модель	Використовує IPSec, протокол тунелювання другого рівня (L2TP) або протокол тунелювання «Point-to-Point» (PPTP) для створення зашифрованого тунелю на стороні клієнта. Повсюдний. Мережа провайдера використовується лише як транспортний засіб для передачі зашифрованих даних, що дозволяє використовувати декілька провайдерів. Дані захищені наскрізно від точки відправлення (клієнта) до точки призначення, що дозволяє створювати VPN через будь-яку інфраструктуру, не боячись компрометації. Сторонні програмні пакети безпеки, такі як Cisco VPN Client, можуть бути використані для для забезпечення більш високого рівня безпеки, ніж вбудоване в систему програмне забезпечення, таке як PPTP. Недоліком є те, що користувач повинний встановити VPN-клієнт на кожну систему. Початкова конфігурація і подальше обслуговування вимагають додаткових ресурсів від організації.
Ініційована сервером мережевого доступу модель	VPN ініціюються в точці присутності постачальника послуг (POP) за допомогою L2TP або переадресації другого рівня (L2F). Усуває потребу в клієнтському програмному забезпеченні VPN, спрощуючи встановлення та зменшуючи адміністративні витрати. Недоліком є те, що канали передачі даних від POP до клієнта залишаються незахищеними.

Продовження Таблиці 2.1.

	Іншим недоліком є те, що користувач повинний використовувати одного і того ж постачальника послуг від початку до кінця, що виключає використання Інтернету як транспортного засобу.

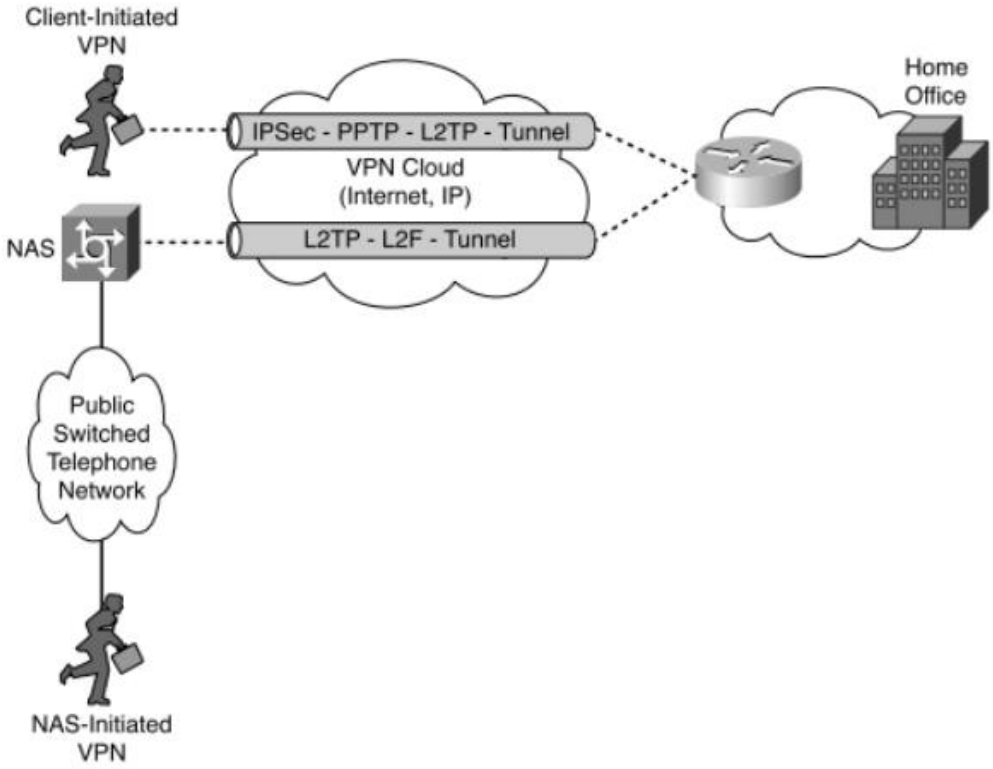

Рис.2.2. Типи VPN для віддаленого доступу

2. Інтрамережеві (Site-to-Site) VPN. Користувачі можуть використовувати інтранет-мережі VPN для підключення віддалених офісів і філій до внутрішньої мережі штаб-квартири через спільну інфраструктуру. Ці з'єднання зазвичай використовують виділені канали, щоб забезпечити доступ лише для співробітників. Ці VPN все ще забезпечують характеристики глобальної мережі, такі як масштабованість, надійність і підтримка різноманітних протоколів, за меншу вартість і в гнучкий спосіб. Інтранет-мережі VPN, як правило, будуються на основі мережевої інфраструктури, що спільно використовується постачальниками послуг, таких як Frame Relay, асинхронний режим передачі (ATM) або схеми P2P.

Деякі з переваг використання інтрамережевих VPN:

- Зменшення витрат на глобальну мережу, особливо при використанні через Інтернет.

- Можна створювати частково або повністю об'єднані мережі, забезпечуючи надлишковість мережі через одного або декількох постачальників послуг.

- Простота підключення нових сайтів до існуючої інфраструктури.

На рисунку 2.3 показано схему типової інтранет-мережі VPN. Корпорація управляє пограничними маршрутизаторами, забезпечуючи гнучкі можливості управління та обслуговування VPN в інтрамережі.

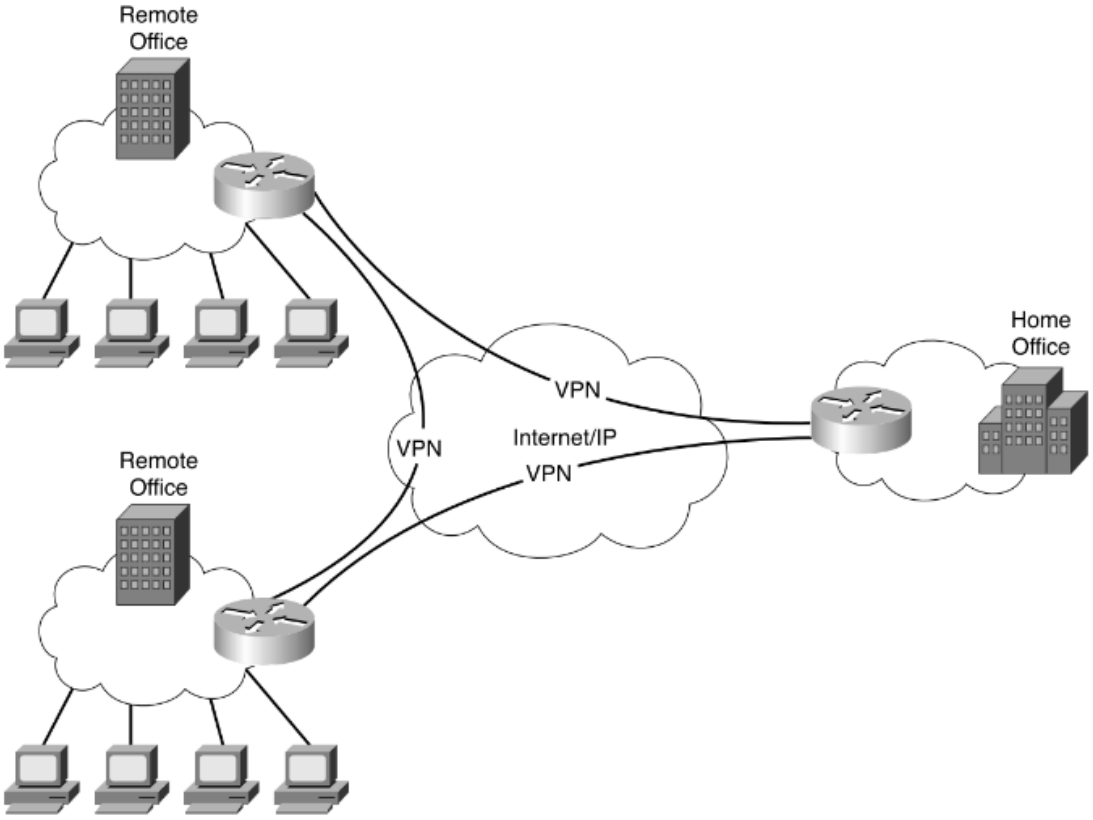

Рис.2.3. Інтрамережевий VPN

3. Екстранет-мережі VPN. Екстранет VPN - це VPN, який надає доступ до корпоративної мережі клієнтам, постачальникам, діловим партнерам або іншим зацікавленим особам, які не є співробітниками корпорації. Екстранет-мережі VPN використовують комбінацію тих самих інфраструктур, які використовуються для віддаленого доступу та інтранет-мереж. Різниця полягає у привілеях, які

надаються користувачам екстранету. Політика безпеки може обмежувати доступ за протоколом, портами, ідентифікацією користувача, часом дня, адресою джерела або призначення, або іншими контрольованими факторами.

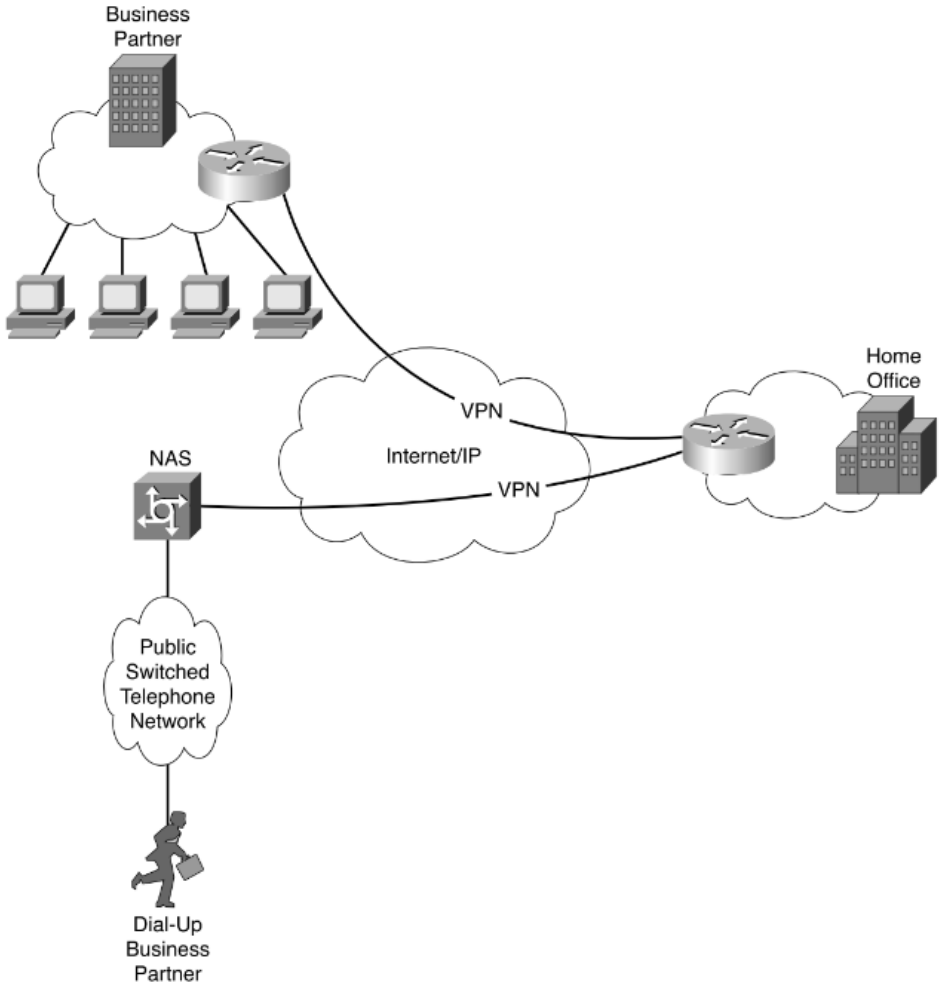

Рис.2.4. Екстранет VPN

2.3 Переваги використання VPN для користувача

1. VPN захищає користувача від крадіжки особистих даних. Крадіжка персональних даних стає все більш значущою проблемою. У 2020 році збитки від крадіжки особистих даних зросли на 42% до $712,4 млрд - порівняно з $502,5 млрд у 2019 році[14].

VPN захищає від крадіжки особистих даних, не дозволяючи кіберзлочинцям використовувати інтернет-звички користувача для крадіжки його банківських, фінансових, трудових та ідентифікаційних даних (наприклад, вашої адреси).

2. VPN зупиняє цінову дискримінацію. Багато веб-сайтів електронної комерції відстежують поведінку користувача в Інтернеті за допомогою файлів cookie, щоб змінювати ціни залежно від його місцезнаходження та статі в Інтернеті. Цінова дискримінація стосується багатьох речей, включаючи авіаквитки, підручники, технології та готелі.

Використання VPN приховує поведінку користувача в Інтернеті та його місцезнаходження, таким чином не даючи йому стати жертвою цінової дискримінації.

3. VPN захищає вас від DDoS атак. Щоб бути впевненим у тому, що розподілена атака на відмову в обслуговуванні (DDoS) не зруйнує мережеве з'єднання, VPN - це найкращий вибір, адже якщо ніхто не знатиме справжньої IP-адреси користувача, його не зможуть атакувати.

Але VPN допомагає захистити лише персональний комп'ютер і з'єднання, а не веб-сервер або хост. Безпечний веб-сайт - це перший крок до повного запобігання шахрайству в електронній комерції.

4. VPN допомагає безпечно працювати з дому. VPN дає змогу використовувати мережу організації під час віддаленої роботи, забезпечуючи доступ до робочих матеріалів і залишаючись захищеними завдяки функціям безпеки вашої організації.

5. Допомагає отримати доступ до контенту з географічними обмеженнями. Оскільки VPN дає змогу переглядати інтернет-сторінки з сервера за межами країни, користувач зможе отримати доступ до контенту, який в іншому випадку був би географічно обмеженим (обмежений IP-адресою). Це стосується географічно обмеженого контенту на потокових відеосервісах, веб-сайтах і платформах соціальних мереж.

6. VPN допомагає обійти інтернет-цензуру. VPN дозволяє отримувати доступ до веб-сайтів і веб-сторінок, заблокованих навчальним закладом, роботодавцем, інтернет-провайдером або урядом. Ці блокування зазвичай застосовуються у локальній мережі або в певній місцевості, тому зміна місцезнаходження користувача за допомогою VPN дозволяє їх обійти.

2.4 Захист даних за допомогою VPN

VPN потрібні не лише організаціям, які хочуть захистити комерційну таємницю, або мандрівникам, які хочуть спокійно користуватися Wi-Fi в аеропортах. VPN можуть бути корисними для всіх, хто користується інтернетом[15].

Ось кілька речей, які може зробити VPN:

1. Приховувати активність користувача в Інтернеті. Інтернет-провайдер і пошукові системи відстежують, що користувач шукає в Інтернеті, щоб надавати персоналізовану рекламу, пропонувати локалізований досвід тощо. Оскільки VPN дозволяє переглядати сторінки через іншу IP-адресу, пошукові системи не можуть націлитися на користувача, оскільки дані прив'язані до VPN, а не до нього.

Однак, якщо користувач все ще зареєстрований в таких сервісах, як Google, Facebook та інші, вони всерівно будуть відстежувати все, що робить користувач, якщо він не заблокував рекламні трекери.

2. Блокувати шкідливе програмне забезпечення та трекери. Багато кіберзлочинців використовують вразливі публічні мережі WiFi для зараження комп'ютерів користувачів шкідливим програмним забезпеченням, такими як кейлоггери. Зокрема, кіберзлочинці перехоплюють трафік, що проходить через загальнодоступні сервери, і використовують ці дані для пошуку потенційних жертв.

Під час використання програми VPN, VPN-провайдер шифрує зв'язок комп'ютера користувача з сервером призначення. Таке наскрізне шифрування запобігає доступу кіберзлочинців і хакерів до даних користувача.

3. Шифрування даних. Служби VPN шифрують будь-які дані, які користувач надсилає під час поточної веб-активності. Шифрування цих даних запобігає доступу корпоративних шпигунів до будь-якої конфіденційної інформації або даних[16].

2.5 Порівняння ефективності VPN від різних розробників

1. Surfshark може похвалитися вражаючим набором функцій конфіденційності та безпеки, необмеженою кількістю одночасних з'єднань, простим у використанні інтерфейсом і широкою глобальною мережею. І це все ще значно дешевше, ніж у більшості конкурентів. Саме це допомогло Surfshark отримати нагороду Вибір редакторів CNET за найкращу VPN-платформу у 2022 році.

Поряд зі стандартними функціями VPN, такими як вимикач і захист від витоку DNS, деякі з найбільш помітних функцій Surfshark включають режим маскування (який приховує той факт, що ви використовуєте VPN), роздільне тунелювання, режим NoBorders (який дозволяє використовувати Surfshark в регіонах з обмеженим доступом до VPN).

Станом на лютий 2022 року і Surfshark, і NordVPN мають одну материнську компанію (Tesonet).

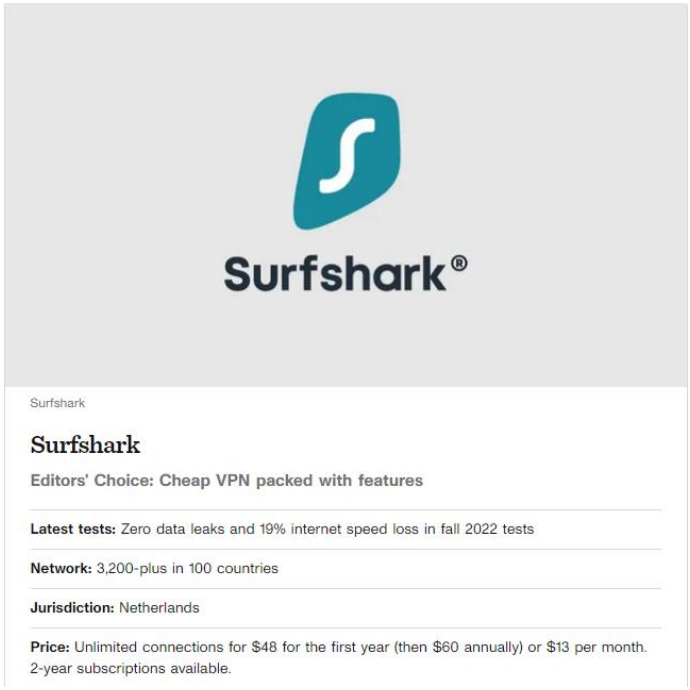

Рис.2.5. Surfshark VPN

2. NordVPN - один з найвідоміших брендів у сфері VPN. Він пропонує велику кількість одночасних з'єднань, з шістьма одночасними з'єднаннями через

свою мережу, тоді як майже всі інші провайдери пропонують п'ять або менше. NordVPN також пропонує опцію виділеної IP-адреси для тих, хто шукає VPN-з'єднання іншого рівня, і можливість VPN-з'єднання з Tor.

Під час тестування було помічено кілька затримок у роботі Nord при використанні його додатку для iOS, що може викликати занепокоєння у користувачів. У останніх тестах швидкості, продуктивність NordVPN відновилася з середніх показників 2021 року і повернулася до числа найшвидших VPN, які тестувались, втративши лише 13% від базової швидкості інтернету.

Рис.2.6. NordVPN

3. Proton VPN є це надійним вибором для досвідчених користувачів VPN і всіх, кому критично важлива безпека, але він також відмінно підходить для звичайних користувачів VPN, які просто хочуть підвищити рівень конфіденційності в Інтернеті або отримати доступ до географічно обмеженого контенту. Він швидкий, простий у використанні на всіх платформах і може

розблокувати такі потокові сервіси, як Netflix, Disney Plus, HBO Max і Amazon Prime Video.

Proton VPN існує не так давно, як деякі з його аналогів, такі як ExpressVPN і NordVPN, але за кілька коротких років він завоював міцну репутацію безпечного і прозорого сервісу. Значною мірою ця репутація ґрунтується на вже існуючій репутації Proton Mail як безпечного рішення для електронної пошти, але з моменту запуску в 2017 році Proton VPN стала самостійним продуктом.

Proton VPN має всі стандартні функції безпеки, які користувач може очікувати від будь-якого VPN-провайдера, що заслуговує на довіру, включаючи захист від витоку DNS і 256-бітне шифрування AES. Провайдер також пропонує додаткові засоби захисту, такі як блокування реклами та шкідливого програмного забезпечення, Tor через VPN і стелс-протокол, який допомагає маскувати VPN-з'єднання і обходити брандмауери.

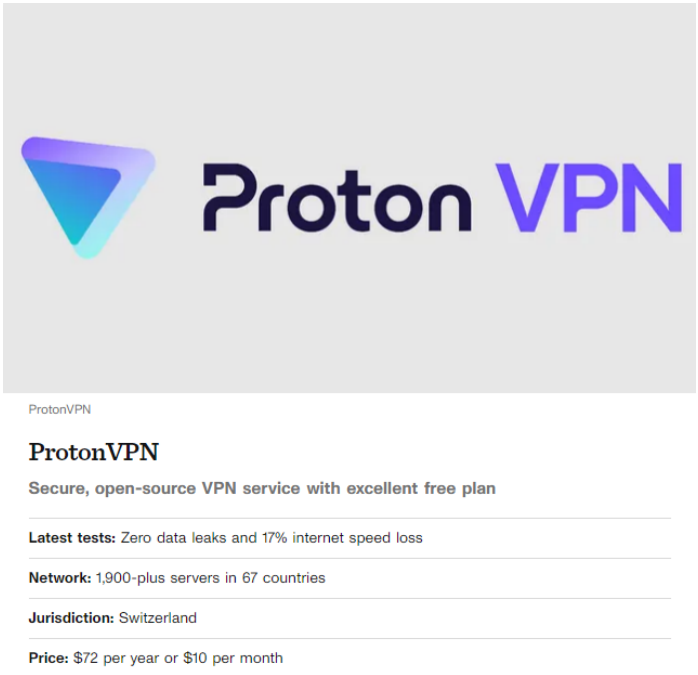

Рис.2.7. Proton VPN

4. CyberGhost VPN. Оскільки підвищились вимоги до перевірки VPN, CyberGhost викликав певні занепокоєння. Історія його материнської компанії викликає скептицизм. Попередні тести показали, що він розкриває використання VPN вашому провайдеру, його трекери веб-сайтів і додатків є більш численними,

ніж це виправдано, а його блокувальник реклами використовує ненадійний метод маніпулювання трафіком, про який жодна VPN не повинна навіть думати. Його низька ціна раніше робила його вартим уваги, якщо користувачу потрібно було змінити його місцезнаходження в Інтернеті, але не в тому випадку, якщо він хоче отримати найкращий у своєму класі захист.

З іншого боку, CyberGhost все ще швидший, ніж Norton Secure VPN, і менш обтяжливий для обчислювальних потужностей пристроїв. Він також пропонує роздільне тунелювання у своєму клієнті для Windows, а його сервери чітко організовані за категоріями: NoSpy сервери, сервери для торрентування, сервери для потокового мовлення, і сервери що найкраще підходять для використання зі статичною IP-адресою. CyberGhost не встановлює обмежень на обсяг даних, дозволяє необмежену кількість перемикань між серверами і пропонує 45-денну гарантію повернення коштів за річну або більше підписку.

CyberGhost

CyberGhost VPN

- Number of servers: Over 8,000 worldwide in 91 countries
- Number of server locations: 111
- Jurisdiction: Romania, with UK parent company
- Number of simultaneous connections: 7
- $2.03 a month or $60 for a two year plan (plus four free months). Month-to-month plan at $13.

Рис.2.8. CyberGhost VPN

5. Norton Secure VPN не підтримує P2P або BitTorrent, Linux, роутери або телевізійні приставки. Його сумісність з Netflix і стрімінгом дещо обмежена. Також, під час тестування було помічено витоки даних, що порушує конфіденційність.

Під час тестування CNET швидкість Norton Secure VPN була порівнянною з іншими VPN середнього рівня, але не конкурентоспроможною. Хоча VPN доступна лише на чотирьох платформах - Mac, iOS, Windows і Android - Norton має цілодобову телефонну підтримку клієнтів.

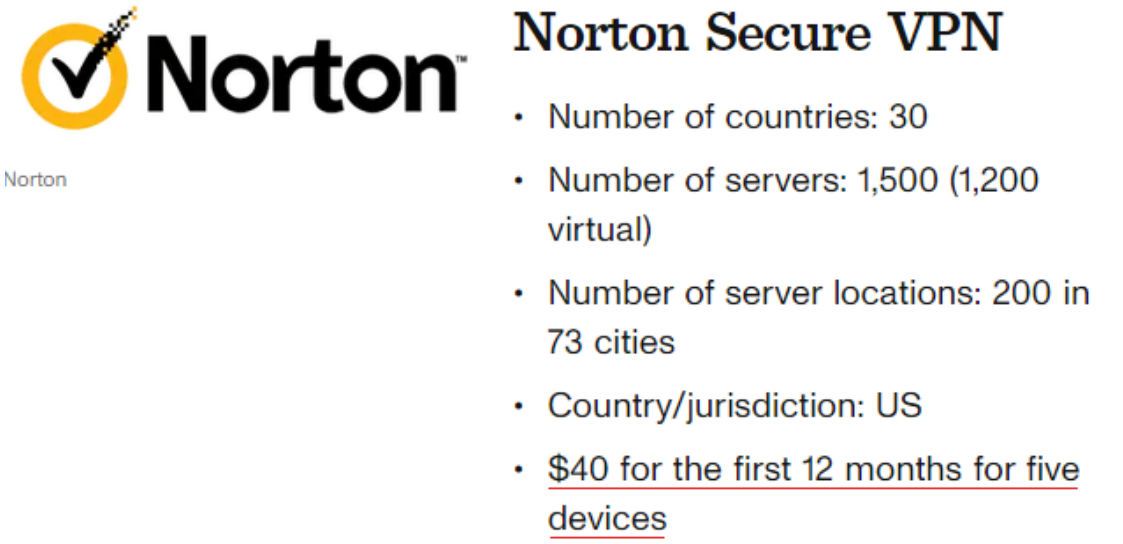

Рис.2.9. Norton Secure VPN

6. Cisco AnyConnect VPN підтримує надійну уніфіковану відповідність кінцевих точок. Він захищає цілісність корпоративної мережі, обмежуючи VPN-доступ Cisco Adaptive Security Appliance (ASA) на основі стану безпеки кінцевої точки. Оцінка та виправлення стану безпеки кінцевих точок у дротових і бездротових середовищах підтверджує статус різних антивірусів, персональних брандмауерів і антишпигунських продуктів. Примусовий захист кінцевих точок, що не відповідають вимогам надає можливості для виправлення ситуації та впровадження додаткових перевірок системи перед наданням доступу[17].

Cisco AnyConnect Solution має вбудовані засоби захисту від веб-загроз і шкідливого програмного забезпечення. При цьому, користувач може обрати один із наступних варіантів захисту:

1.Cisco® Web Security Appliance (WSA) рішення для приміщень;

2.Cisco Cloud Web Security (CWS) хмарне рішення для надійного і високозахищенного доступу співробітників до корпоративних ресурсів.

Веб-безпека, захист від зловмисних програм і віддалений доступ об'єднані в комплексному та високозахищеному рішенні для корпоративної мобільності. Послідовні контекстно-залежні політики безпеки допомагають забезпечити захищене та продуктивне робоче середовище[18].

На додаток до провідних в галузі можливостей VPN, Cisco AnyConnect в якості складової рішення Cisco Secure VPN допомагає реалізувати можливості IEEE 802.1X, забезпечуючи єдину систему автентифікації для управління ідентифікацією користувачів і пристроїв, а також протоколи доступу до мережі, необхідні для плавного переходу від дротових до бездротових мереж. Відповідно до своєї VPN-функціональності Cisco AnyConnect підтримує стандарт IEEE 802.1AE (MACsec) для забезпечення конфіденційності, цілісності даних та автентифікації походження даних у дротових мережах, захищаючи зв'язок між довіреними компонентами мережі[19].

Cisco AnyConnect не зможе захистити усіх співробітників компанії під час віддаленої роботи, проте якщо використовувати Cisco AnyConnect як складову рішення Cisco Secure VPN, це максимально знизить ризики несподіваних атак на компанію або її працівників.

Рис.2.10. Cisco AnyConnect

Висновки до другого розділу

Проаналізовано методи та засоби боротьби з кібератаками, кроки які потрібно виконувати для захисту бізнес-процесів та даних

Досліджено, що жодна система не є цілком безпечною - проте знизити ризики проникнення в систему шкідливого програмного забезпечення все ж таки можливо, для цього потрібно проводити консультації з працівниками, оновлювати програми та користуватись різними рішеннями пов’язаними з безпекою, такими як VPN, системи для аналізу мережевого трафіку тощо.

Зазначено, що VPN це не ідеальний спосіб уникнення від атак, адже захистити від усього це рішення аж ніяк не зможе, проте якщо використовувати його як частину засобів захисту - це знизить ймовірність того що будь-які бізнес-процеси будуть зупинені.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ КОРИСТУВАЧІВ ПІД ЧАС ДИСТАНЦІЙНОЇ РОБОТИ НА БАЗІ РІШЕННЯ CISCO SECURE VPN

3.1 Огляд Cisco Secure VPN Client

Cisco Secure VPN Client - це програмний компонент, який дозволяє користувачеві комп'ютера створювати зашифрований тунель з використанням IPSec та/або IKE до віддаленого сайту для наскрізного екстранет VPN-рішення. Технологія шифрування IP Security Protocol (IPSec) - це розробка IETF, яка є загальноприйнятою в усій індустрії. Internet Key Exchange (IKE) - це гібридний протокол, який реалізує обмін ключами Oakley і Skeme.[20]

Skeme в рамках протоколу Internet Security Association and Key Management Protocol (ISAKMP). (ISAKMP, Oakley і Skeme - це протоколи безпеки, реалізовані IKE.) IPSec можна налаштувати і без IKE, але IKE розширює можливості IPSec, надаючи додаткові функції, гнучкість і простоту налаштування для стандарту IPSec. Мережеві пристрої Cisco IOS використовують IPSec для створення захищених, зашифрованих тунелів між мережевими пристроями Cisco. Це створює безпечний зв'язок між клієнтом і сервером через IP-мережу 3-го рівня. У всіх наступних прикладах мережевий пристрій Cisco IOS з підтримкою IPSec виступає в ролі сервера, а Cisco Secure VPN Client виконує завдання як клієнт.

Програмне забезпечення Cisco Secure VPN Client дозволяє виконувати наступні завдання безпосередньо з робочого столу:

1. Генерація публічного/приватного ключа. За допомогою IKE користувач може налаштувати клієнт Cisco Secure VPN на використання системи відкритих/закритих ключів для шифрування. Система відкритих/закритих ключів - це метод шифрування і дешифрування інтернет-трафіку для безпечного з'єднання без попереднього повідомлення. Технологія відкритого/закритого ключа використовує алгоритм шифрування алгоритм шифрування (наприклад, DES) і

ключ шифрування, який дві сторони - одержувач і відправник - використовують для передачі даних між собою. Одержувач володіє приватним ключем, тоді як відкритий ключ належить центру сертифікації (ЦС) або серверу каталогів для розповсюдження.

2. Отримання цифрового сертифікату. За допомогою IPSec користувач може налаштувати клієнт Cisco Secure VPN Client на використання цифрових сертифікатів для автентифікації. Щоб підтвердити особу відправника, ЦС видає цифровий сертифікат - електронний файл, який ЦС затверджує підписуючи його після перевірки особи відправника. Після того, як відправник отримає цифровий сертифікат від ЦС, що його видав (а також цифровий сертифікат відправника), відправник повинен створити політику безпеки.

3. Створення політики безпеки. Політика безпеки надає інформацію про те, як перевірити особу користувача, забезпечити цілісність для запобігання цілісності для запобігання фальсифікації даних, а також активний аудит для виявлення вторгнень. Кожна корпоративна мережа повинна мати політику безпеки, яка визначає, як мережа підтримується для автентифікованих користувачів і контролюється на предмет несанкціонованого доступу[21].

Підтримувані конфігурації Cisco Secure VPN:

Наразі Cisco підтримує використання Cisco Secure VPN Client з IPSec та IKE. Для сумісності між Cisco Secure VPN Client та мережевими пристроями Cisco, Cisco підтримує наступні конфігурації:

1. Використання попередньо наданих ключів. Користувач може генерувати попередньо надані ключі для автентифікації користувачів між VPN-клієнтом і шлюзом.

2. Використання цифрової сертифікації. Користувач може попросити центр сертифікації (ЦС) призначити цифровий сертифікат кожному клієнту VPN для автентифікації пристрою. Цифрові сертифікати забезпечують більшу масштабованість, ніж попередньо надані ключі, і зазвичай застосовуються у великих мережах (понад 10 клієнтів).

Cisco Secure VPN Client підтримується мережевими пристроями Cisco, що використовують цифрові сертифікати Entrust, Microsoft та VeriSign.

Cisco Secure VPN забезпечує безпечне з'єднання для віддаленого доступу для окремих осіб (наприклад, мобільних користувачів або віддалених працівників), корпоративної інтрамережі або екстрамережі через спільну мережу постачальника послуг з тими ж політиками, що і в приватній мережі.

Cisco Secure VPN Client підтримує два типи VPN доступу:

1.Доступ ініційований клієнтом до мережі VPN

Доступ до VPN за ініціативою клієнта дозволяє віддаленим користувачам використовувати клієнти для створення зашифрованого IP-тунелю через загальну мережу інтернет-провайдера (ISP) до мережі корпоративного клієнта. Основна перевага VPN з доступом за ініціативою клієнта над VPN з доступом за ініціативою NAS полягає в тому, що вони використовують тунельний режим IPSec для захисту з'єднання між клієнтом і провайдером через телефонну мережу загального користування.

На Рис.3.1 показано клієнт Cisco Secure VPN в топології VPN з доступом, ініційованим клієнтом. Клієнт встановлює захищене PPP-з'єднання з мережевим сховищем провайдера, після чого встановлюється тунель IPSec через телефонну мережу загального користування. Клієнти VPN можуть використовувати або статичну IP-адресацію з ручним налаштуванням, або динамічну IP-адресацію з налаштуванням режиму IKE.

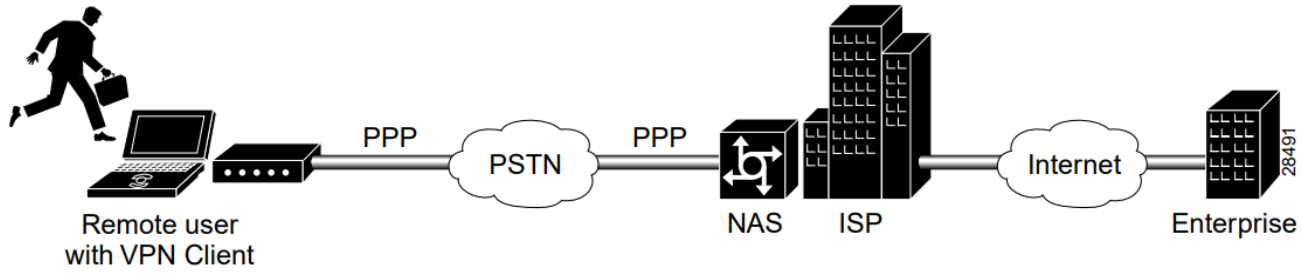

Рис.3.1. Cisco Secure VPN в топології VPN з доступом, ініційованим клієнтом

2.Доступ ініційований NAS до мережі VPN

Доступ ініційований NAS до VPN дозволяє віддаленим користувачам підключатися до мережевого сховища провайдера. Мережеве сховище встановлює зашифрований тунель до приватної мережі підприємства. VPN-мережі, ініційовані NAS, дають змогу віддаленим користувачам підключатися до кількох мереж за допомогою кількох тунелів. VPN-мережі, ініційовані NAS, не шифрують з'єднання між клієнтом і провайдером, а покладаються на безпеку PSTN.

На рис.3.2 показано топологію VPN з доступом за допомогою NAS. Оскільки клієнт Cisco Secure VPN не потрібен для рішення VPN з доступом до мережевого сховища, він не є компонентом цієї мережі. Недоліком доступу ініційованого NAS до мережі VPN є те, що PSTN не є захищеною.

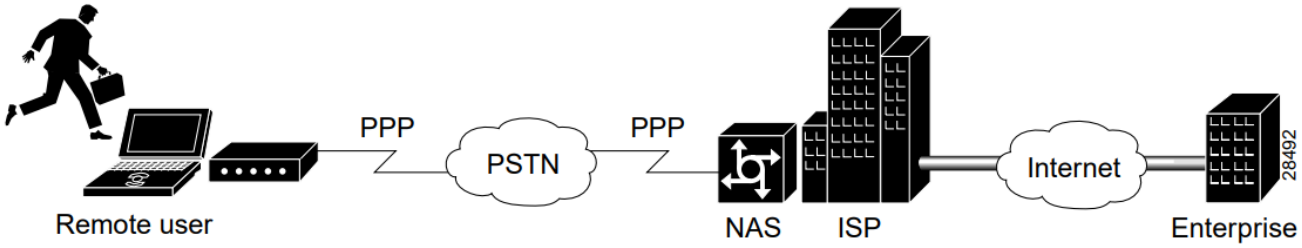

Рис.3.2. Cisco Secure VPN в топології VPN з доступом за допомогою NAS

3.2 Побудова доступу до Cisco Secure VPN

1. Мережеве обладнання підприємства. На рисунку 3.1 показано конкретні мережеві пристрої, які використовуються на підприємстві для побудови VPN доступу.

- Програмне забезпечення VPN-клієнта, яке мережевий адміністратор може попередньо налаштувати з одноразовою статичною IP-адресою або налаштувати на динамічну IP-адресу.

- Домашній шлюз (наприклад, маршрутизатор Cisco IOS або брандмауер Cisco Secure PIX Firewall), налаштований за допомогою IPSec з підтримуваного випуску програмного забезпечення Cisco IOS.

- Загальнодоступний веб-сервер і приватний корпоративний сервер.

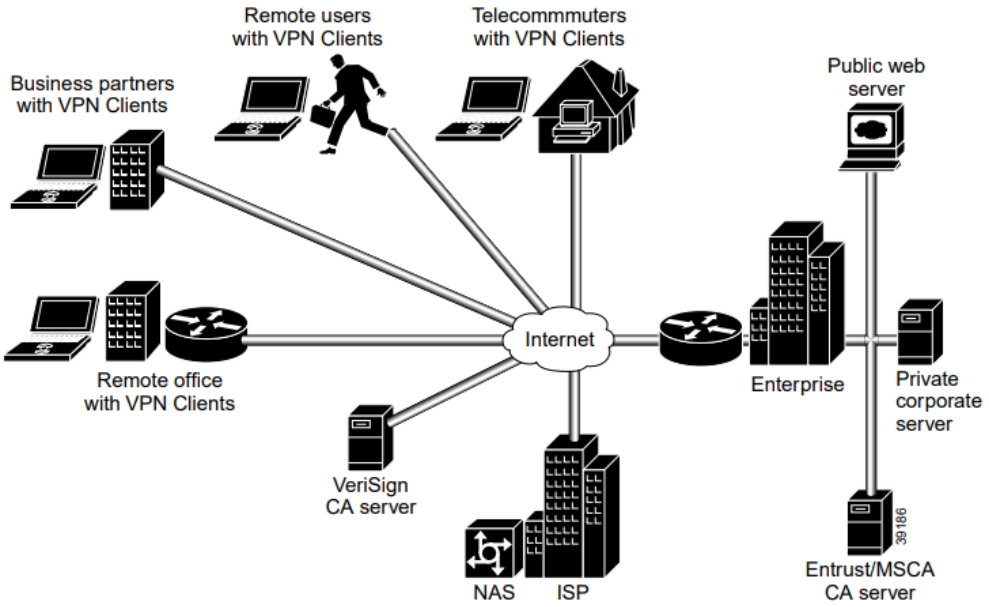

Рис.3.3. Мережеві пристрої, які використовуються на підприємстві для побудови VPN доступу

2. Опис VPN для корпоративного доступу. Клієнти VPN ініціюють тунелі IPSec, запитуючи автентифікацію на одноранговому IPSec-шлюзі, домашньому шлюзі. Як тільки домашній шлюз підтверджує автентичність з'єднання, VPN-клієнти створюють зашифрований тунель до домашнього шлюзу. Для маршрутизації авторизованого трафіку до вказаного місця призначення на домашньому шлюзі налаштовується список доступу, який дозволяє або забороняє трафік в різні підмережі корпоративної мережі:

- Для співробітників компанії дозволений доступ до приватного корпоративного сервера, де вони можуть отримати доступ до конфіденційних даних віддалено. Співробітники компанії також можуть переглядати інформацію на загальнодоступному веб-сервері.

- Для екстранет-партнерів доступ обмежений загальнодоступним веб-сервером, де вони виконують різні мережеві завдання на основі IP-адреси, такі як розміщення та управління замовленнями на продукцію. Бізнес-партнерам заборонено доступ до всіх приватних внутрішньокорпоративних серверів.

3.3 Налаштування конфігурації Cisco Secure VPN

Для налаштування конфігурації Cisco Secure VPN, потрібно винонати 2 основних завдання:

1. Налаштування конфігурації на VPN-клієнті
2. Налаштування конфігурації на шлюзі

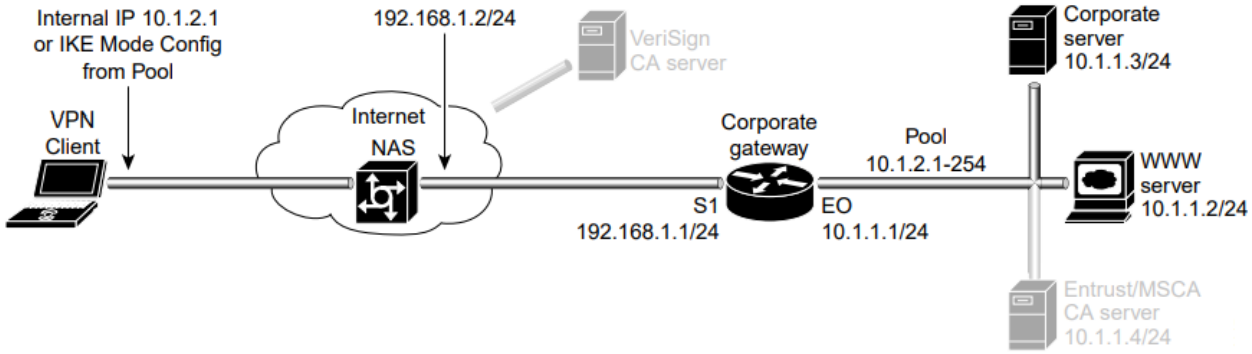

Рис.3.4. Топологія ручної конфігурації Cisco Secure VPN

1. Налаштування конфігурації на VPN-клієнті

1.1 Задання внутрішньої мережевої адреси на VPN-клієнті:

Пуск>Програми>Cisco Secure VPN Client>Security Policy Editor.

З'явиться вікно Редактор політики безпеки SafeNet/Soft-PK, як показано на рис.3.3.

Рис.3.5. Редактор політики безпеки SafeNet/Soft-PK

У меню Параметри потрібно обрати пункт Налаштування глобальної політики.

З'явиться вікно Налаштування глобальної політики, як показано на рис.3.4.

Далі слід встановити прапорець Дозволити вказувати внутрішню мережеву адресу і натиснути кнопку OK.

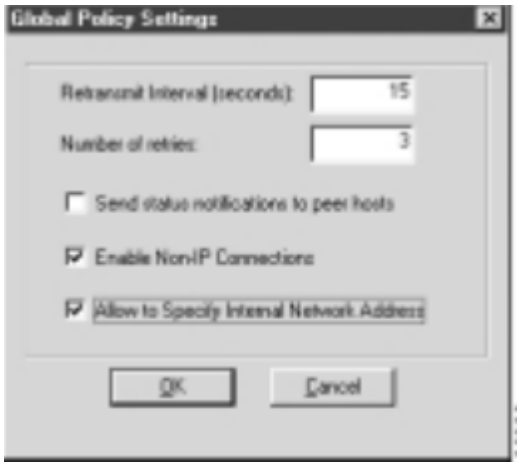

Рис.3.6. Вікно налаштувань глобальних політик

1.2 Налаштування нового шлюзу для політики безпеки:

На лівій панелі потрібно натиснути Інші підключення.

У меню Файл обрати пункт Нове підключення.

На лівій панелі з'явиться заповнювач за замовчуванням Нове з'єднання для панелі Нове з'єднання.

Виділити Нове з'єднання і замість нього ввести унікальне ім'я для з'єднання з шлюзом.

Наприклад, якщо ім'я маршрутизатора hq_sanjose, його можна перейменувати на hq_sanjose, як показано на рисунку 3.4.

Рис.3.7. Перейменування нової панелі з'єднань

1.3 Визначення нового з'єднання:

На лівій панелі потрібно обрати Нове з'єднання. У прикладі буде обрано tohq_sanjose, після чого з'явиться панель нового з'єднання.

На правій панелі в розділі Безпека з'єднання слід обрати Безпечний.

На правій панелі в розділі Ідентифікація та адресація віддаленої сторони слід ввести такі дані:

a. У списку Тип ідентифікатора потрібно обрати IP-підмережу.

b. У полі Підмережа слід ввести IP-адресу корпоративної підмережі. У цьому прикладі IP-адреса корпоративної підмережі 10.1.1.0.

c. У полі Маска потрібно ввести маску підмережі для IP-адреси корпоративної підмережі. У цьому прикладі введено маску підмережі корпоративної підмережі 255.255.255.0.

d. Список і поле Порт за замовчуванням неактивні. У списку Протокол слід обрати Усі.

e. Необхідно встановити прапорець Підключитися за допомогою тунелю захищеного шлюзу.

f. У списку Тип_ідентифікатора потрібно обрати IP-адреса. У полі ID_Type необхідно ввести IP-адресу захищеного шлюзу. У цьому прикладі введено адресу захищеного шлюзу 192.168.1.1.

Рис.3.8. Нова панель з'єднань

1.4 Визначення ідентичності VPN-клієнта:

На лівій панелі потрібно двічі натиснути нове з'єднання. У цьому прикладі двічі натиснуто на tohq_sanjose. Нове з'єднання буде розгорнуто з даними про нього і політикою безпеки.

Слід Натиснути Моя особа. У правій частині вікна з'явиться панель Мої дані.

На правій панелі у розділі Мої дані потрібно ввести такі дані:

a. Якщо користувач використовує цифрові сертифікати, слід обрати свій цифровий сертифікат у списку Виберіть сертифікат. Якщо він не використовує цифрові сертифікати, йому слід залишити це поле без змін.

b. У списку ID_Type обрати IP-адреса.

c. У полі IP-адреса внутрішньої мережі ввести статичну IP-адресу VPN-клієнта. У цьому прикладі введено 10.1.2.1.

d. У списку Порт натиснути Усі.

e. У списку Ім'я слід обрати Будь-яке. Список IP-адреса за замовчуванням неактивний.

f. Якщо користувач використовує попередньо надані ключі, йому слід обрати Попередньо надані, після чого ввести ключ, який буде використано на етапі автентифікації. Далі слід натиснути ОК. Якщо користувач не використовує попередньо надані ключі, йому слід залишити це поле без змін.

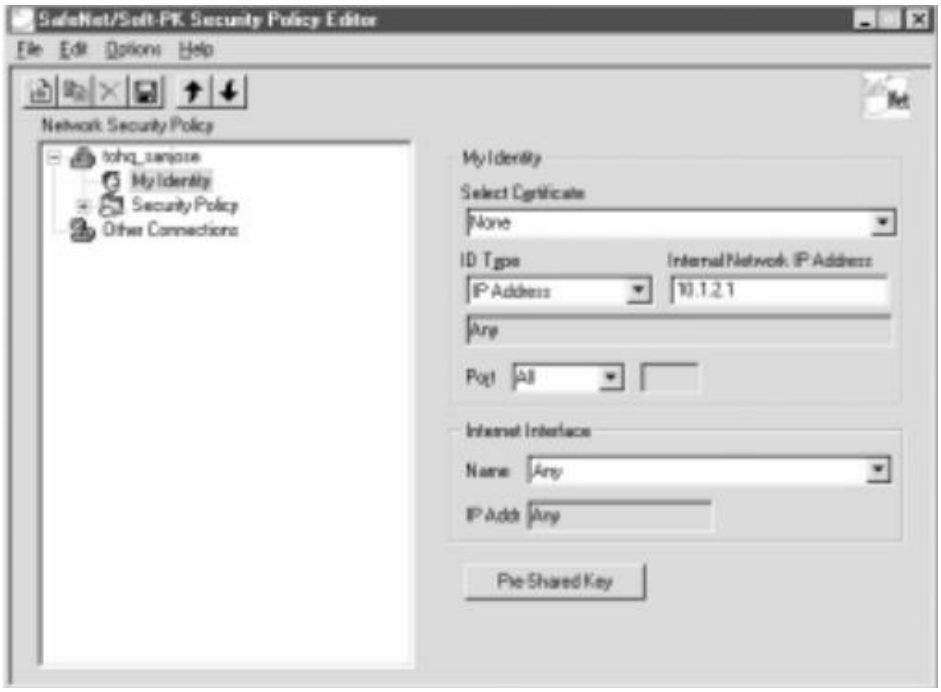

Рис.3.9. Панель ідентифікації

2. Налаштування конфігурації на шлюзі:

Налаштування конфігурацій у цьому пункті виконується за допомогою команд, які будуть представлені у підпунктах.

2.1 Налаштування шлюзу

router> enable

router# configure terminal Enter configuration commands, one per line.

End with CNTL/Z.

router(config)# ip domain-name example.com

router(config)# hostname hq_sanjose

hq_sanjose(config)# ip name-server 192.168.1.1

2.2 Визначення набору перетворень IPSec

hq-sanjose(config)# crypto ipsec transform-set vpn-transform esp-des ah-md5-hmac

hq-sanjose(cfg-crypto-trans)# mode tunnel

hq-sanjose(cfg-crypto-trans)# exit

2.3 Визначення динамічної криптографічної карти

hq_sanjose(config)# crypto dynamic-map vpn-dynamic 1

hq_sanjose(config-crypto-map)# set transform-set vpn-transform

hq_sanjose(config-crypto-map)# match address 101

hq_sanjose(config-crypto-map)# exit

2.4 Визначення статичної криптографічної карти

hq_sanjose(config)# crypto map vpnclient 1 ipsec-isakmp vpn-dynamic

hq_sanjose(config)# access-list 101 permit ip 192.168.1.1 255.255.255.0 host 10.1.2.1

hq_sanjose(config)# crypto map vpn-dynamic local-address loopback0

3.4 Переваги Cisco Secure VPN в порівнянні з конкурентами

Cisco Secure VPN Client є кращим за інші VPN з тунельним протоколом доступу, таким як L2F, через його здатність захищати передачу даних через телефонну мережу загального користування. При використанні попередньо наданих ключів це найпростіший метод захисту зашифрованого тунелювання між VPN-клієнтом віддаленого користувача і мережевим пристроєм. Cisco Secure VPN Client також масштабується до великих мереж при його використанні з цифровими сертифікатами

VPN зазвичай розгортаються для забезпечення покращеного доступу до корпоративних ресурсів, забезпечуючи при цьому жорсткіший контроль над безпекою при менших витратах на послуги WAN-інфраструктури.

Працівники, що працюють на дистанційно, мобільні користувачі, віддалені офіси, ділові партнери, клієнти та споживачі - всі отримують вигоду, тому що

корпорації розглядають VPN як безпечний і доступний метод відкриття доступу до корпоративної інформації.

Опитування Cisco показали, що більшість корпорацій, які впроваджують VPN, роблять це, щоб забезпечити доступ до корпоративної мережі з дому для працівників, які працюють віддалено. Вони називають безпеку і зниження витрат основними причинами вибору технології VPN і виділяють щомісячну плату за обслуговування як економічне обґрунтування свого рішення.

Технологія VPN була розроблена для забезпечення приватного спілкування будь-де і будь-коли, в будь-якому місці і в будь-який час, максимально нагадуючи традиційне приватне з'єднання з глобальною мережею (WAN) наскільки це можливо. Cisco пропонує різноманітні платформи та додатки, призначені для реалізації Cisco Secure VPN, вони будуть розглянуті у наступному пункті.

Cisco Secure VPN порівняно з іншими VPN-рішеннями:

Cisco Secure VPN є кращим за VPN з тунельним протоколом доступу, таким як L2F, завдяки своїй здатності захищати передачу даних через телефонну мережу загального користування (PSTN).

Також, Cisco Secure VPN підтримує використання попередньо наданих ключів, що є найпростішим методом захисту зашифрованого тунелювання між VPN-клієнтом віддаленого користувача та мережевим пристроєм.

Cisco Secure VPN Client також масштабується до великих мереж, якщо використовується з цифровими сертифікатами.

Доступність корпоративної мережі можна швидко масштабувати з мінімальними витратами. Єдина VPN-мережа може забезпечити безпечний зв'язок для різноманітних додатків на різних операційних системах, що надзвичайно актуально для кожного користувача.

3.5 Рекомендації щодо побудови захищеної дистанційної роботи

1. *Вибір надійного VPN провайдера.* Для корпоративних VPN не існує універсального рішення. Вибір відповідного програмного забезпечення залежить

від розміру компанії, можливостей сервера та IT-відділу, і це лише декілька факторів. Крім того, деякі багатофункціональні варіанти мають високу ціну, саме тому слід віднестись до вибору VPN дуже серйозно, це може зберегти як час користувачів, так і кошти компанії в майбутньому.

2.*Загальна конфігурація VPN*. Налаштування VPN для компанії складається з двох окремих частин. Перша - це налаштування мережі для прийняття VPN-з'єднань. Для початку компанії потрібен маршрутизатор з підтримкою VPN. Більшість таких маршрутизаторів постачаються з посібником щодо увімкнення цієї функції. Після запуску VPN слід змінити налаштування безпеки, включивши білий список.

Коли мережа увімкнена, потрібно налаштувати комп'ютери співробітників для безпечного віддаленого доступу. Цей процес починається зі встановлення VPN-клієнта, здатного спілкуватися з роутером. Після цього, співробітникам потрібно буде ввести IP-адресу мережі компанії.

3. *Налаштування статичної IP-адреси.* Якщо використовується функція білих списків для безпеки, потрібно, щоб комп'ютери співробітників виконали додатковий крок під час роботи з дому. Ця опція зазвичай знаходиться в розділі налаштувань VPN-клієнта на стороні клієну. IT-відділ повинен надіслати IP-адреси для введення на основі бажаного білого списку.

4. *Налаштування безпеки клієнту*. Під’єднання до VPN не захистить користувача від всіх загроз які можуть виникнути під час віддаленої роботи, саме тому слід дотримуватись і основних правил безпеки. Слід постійно оновлювати програмне забезпечення на пристрої та не переходити по підозрілим посиланням.

Найкращим варіантом для побудови захищеної дистанційної роботи працівників є використання різних технологій разом, у поєднанні вони будуть більш ефективними аніж будь-який самостійний додаток.

Не слід забувати і про контроль мережевого трафіку, це може захистити як конфіденційну інформацію працівника, так і компанії в якій він працює. Якщо ж не буде змоги уникнути атаки, подібні системи можуть завчасно помітити підозрілий трафік, що дозволить одразу відреагувати на атаку, і якщо вона не буде

усунена, то збитки які вона принесе компанії можуть бути зменшені у десятки разів.

Висновки до третього розділу

Проаналізовано особливості застосування Cisco Secure VPN та його налаштування для забезпечення безпечної дистанційної роботи працівників компанії.

Зазначено, що для побудови доступу до Cisco Secure VPN потрібно мати налаштоване мережеве обладнання, та надано опис корпоративного доступу до VPN.

Виокремлено, що Cisco Secure VPN Cisco Secure VPN є кращим за будь-який звичайний VPN з тунельним протоколом доступу, завдяки своїй здатності захищати передачу даних через телефонну мережу загального користування та використання попередньо наданих ключів.

ВИСНОВКИ

В бакалаврській роботі отримано наступні теоретичні та наукові результати:

1) Проаналізовано основні види атак та методи для запобігання та виявлення цих атак, також розглянуто методи забезпечення конфіденційності персональних даних.

2) Досліджено, що людські помилки провокують за собою більшість кіберпорушень, адже жодна система не може вважатись повністю захищеною, все що можливо - це знизити ймовірність винекнення атак, але для цього потрібно дотримуватись первних правил та перевіряти власну систему на наявність вразливостей.

3) Зазначено, що Cisco Secure VPN може знизити ризик нападу на систему та ризик виникнення певних видів атак, розглянуто принцип його роботи та надано повний опис цього рішення.

4) Виокремлено способи захисту даних користувачів за допомогою Cisco Secure VPN Client та надано опис налаштувань для цього рішення.

5) Зроблено висновок, що будь-який програмно-апаратний комплекс не зможе повністю захистити жодну систему, проте якщо проводити постійні перевірки наявності оновлень додатків на серверах чи комп’ютерах працівників, можна знизити ризик винекнення атак чи спроб проникнення в систему. Слід зазначити, що звичайний додаток який призначений для захисту системи користувача не може захистити його систему від усіх загроз, проте наявність налаштованного програмно-апаратного компелексу дозволяє не лише виявити загрозу на початковому етапі її винекнення, а й запобігти їй. Саме таким чином можна досягти високого рівня безпеки працівників під час дистанційної роботи з власних домівок.