ЛЬВІВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
БЕЗПЕКИ ЖИТТЄДІЯЛЬНОСТІ

Кафедра управління інформаційною безпекою

Освітня компонента “Інструменти кібербезпеки”

Л Е К Ц І Я

DMZ. VPN-мережі

План лекції:

1. Інтранет і екстранет.
2. Принципи побудови DMZ-мережі.
3. Різні архітектури DMZ-мережі.
4. Service Leg конфігурація.
5. Віртуальні приватні мережі і їх підключення.
6. Розміщення DNS-, SMTP-, VPN- серверів.

Інформаційні джерела

Основні

1. Курс дисципліни у віртуальному університеті

Додаткові

1. Chris Sanders. PRACTICAL PACKET ANALYSIS. 3-RD EDITION. Usng Wireshark to Solve Real-World Problems.San Francisco. 2017. 450 p.
2. James D. Miller Implementing Splunk 7. Third Edition. Effective operational intelligence to transform machine-generated data into valuable business insightr. Packt Publishing. 2018. 490 p.
3. Левин М. Библия хакера 2. Книга 1. - М.: Майор, 2003. - 640 с. 4. Левин М. Библия хакера 2. Книга 2. - М.: Майор, 2003. - 688 с.
Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ.: BHV, 2009. – 607 с.

Завдання створення комп'ютерної мережі підприємства в межах однієї будівлі може бути вирішене відносно легко. Проте сучасна інфраструктура корпорацій включає географічно розподілені підрозділи самої корпорації, її партнерів, клієнтів і постачальників. Тому створення корпоративної мережі стало істотно складнішим завданням.

З бурхливим розвитком Internet і мереж колективного доступу стався якісний стрибок в поширенні і доступності інформації. Користувачі отримали дешеві і доступні канали Internet. Підприємства прагнуть використати такі канали для передачі критичної комерційної і управлінської інформації.

Для ефективної протидії мережевим атакам і забезпечення можливості активного і безпечного використання у бізнесі відкритих мереж на початку 1990х рр. народилася і активно розвивається концепція побудови віртуальних приватних мереж — VPN (Virtual Private Network).

1. Концепція побудови віртуальних захищених мереж VPN

У основі концепції побудови віртуальних мереж VPN лежить досить проста ідея: якщо в глобальній мережі є два вузли, якими треба обмінятися інформацією, то між цими двома вузлами необхідно побудувати віртуальний захищений тунель для забезпечення конфіденційності і цілісності інформації, що передається через відкриті мережі; доступ до цього віртуального тунелю має бути надзвичайно ускладнений усім можливим активним і пасивним зовнішнім спостерігачам.

Переваги, що отримуються компанією від створення таких віртуальних тунелів, полягають передусім в значній економії фінансових коштів, оскільки в цьому випадку компанія може відмовитися від побудови або оренди дорогих виділених каналів зв'язку для створення власних intranet/extranet мереж і використати для цього дешеві Інтернет канали, надійність і швидкість передачі яких у більшості своєму вже не поступається виділеним лініям. Очевидна економічна ефективність від впровадження VPN технологій стимулює підприємства до активного їх впровадження.

1.1. Основні поняття і функції мережі VPN

При підключенні корпоративної локальної мережі до відкритої мережі виникають загрози безпеки двох основних типів:

- НСД до внутрішніх ресурсів корпоративної локальної мережі, отримуваний зловмисником в результаті несанкціонованого входу в цю мережу;
- НСД до корпоративних даних в процесі їх передачі по відкритій мережі.

Забезпечення безпеки інформаційної взаємодії локальних мереж і окремих комп'ютерів через відкриті мережі, зокрема через мережу Інтернет, можливо шляхом ефективного рішення наступних завдань:

- захист підключених до відкритих каналів зв'язку локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища;

- захист інформації в процесі її передачі по відкритих каналах зв'язку.

Як вже відзначалося вище, для захисту локальних мереж і окремих комп'ютерів від несанкціонованих дій з боку зовнішнього середовища зазвичай використовують МЕ, що підтримують безпеку інформаційної взаємодії шляхом фільтрації двостороннього потоку повідомлень, а також виконання функцій посередництва при обміні інформацією. МЕ розташовують на стику між локальною і відкритою мережею. Для захисту окремого віддаленого комп'ютера, підключеного до відкритої мережі, на цьому комп'ютері встановлюють ПЗ мережевого екрану, і такий мережевий екран називається персональним.

Захист інформації в процесі її передачі по відкритих каналах заснований на використанні віртуальних захищених мереж VPN. Віртуальною захищеною мережею VPN (Virtual Private Network) називають об'єднання локальних мереж і окремих комп'ютерів через відкрите зовнішнє середовище передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних. Віртуальна захищена мережа VPN формується шляхом побудови віртуальних захищених каналів зв'язку, що створюються на базі відкритих каналів зв'язку загальнодоступної мережі. Ці віртуальні захищені канали зв'язку називаються тунелями VPN. Мережа VPN дозволяє за допомогою тунелів VPN з'єднати центральний офіс, офіси філій, офіси бізнес партнерів і видалених користувачів і безпечно передавати інформацію через Інтернет (Рис. 1).

Тунель VPN є з'єднанням, проведеним через відкриту мережу, по якому передаються криптографічно захищені пакети даних віртуальної мережі. Захист інформації в процесі її передачі по тунелю VPN заснований:

- на аутентифікації взаємодіючих сторін;
- криптографічному закритті (шифруванні) передаваних даних;
- перевірці достовірності і цілісності інформації, що доставляється.

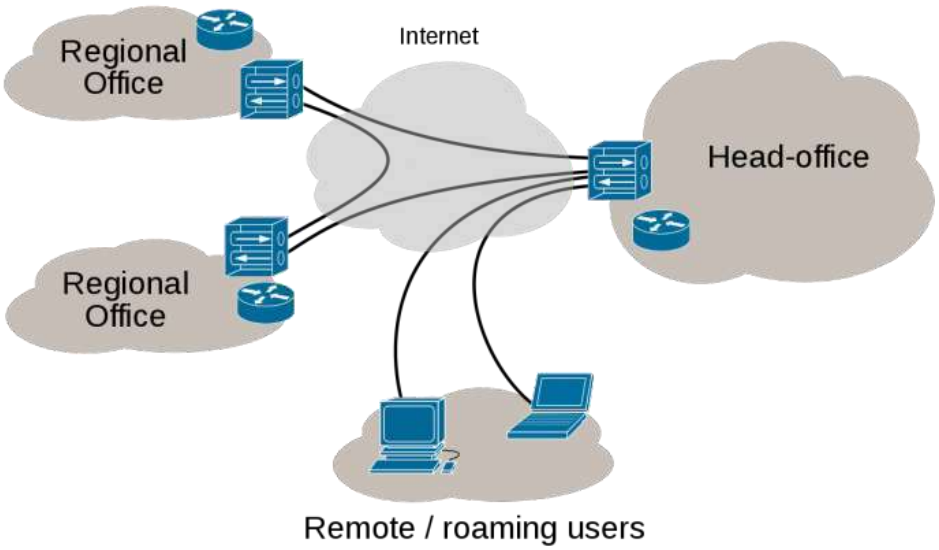

Рис. 1. Віртуальна захищена мережа VPN

Для цих функцій характерний взаємозв'язок сторін. При їх реалізації використовуються криптографічні методи захисту інформації. Ефективність такого захисту забезпечується за рахунок спільного використання симетричних і

асиметричних криптографічних систем. Тунель VPN, що формується облаштуваннями VPN, має властивості захищеної виділеної лінії, яка розгортається у рамках загальнодоступної мережі, наприклад Інтернету. Пристрої VPN можуть грати у віртуальних приватних мережах роль VPN клієнта, VPN сервера або шлюзу безпеки VPN.

VPN клієнт є програмним або програмно-апаратним комплексом, що виконується зазвичай на базі персонального комп'ютера. Його мережеве ПЗ модифікується для виконання шифрування і аутентифікації трафіку, яким цей пристрій обмінюється з іншими VPN клієнтами, VPN серверами або шлюзами безпеки VPN. Зазвичай реалізація VPN клієнта є програмним рішенням, що доповнює стандартну ОС, — Windows 2000/XP/7 або Unix.

VPN сервер є програмним або програмно-апаратним комплексом, що встановлюється на комп'ютері, що виконує функції сервера. VPN сервер забезпечує захист серверів від НСД із зовнішніх мереж, а також організацію захищених з'єднань (асоціацій) з окремими комп'ютерами і з комп'ютерами з сегментів локальних мереж, захищених відповідними VPN продуктами. VPN сервер є функціональним аналогом продукту VPN клієнт для серверних платформ. Він відрізняється передусім розширеними ресурсами для підтримки множинних з'єднань з VPN клієнтами. VPN сервер може підтримувати захищені з'єднання з мобільними користувачами.

Шлюз безпеки VPN (security gateway) — цей мережевий пристрій, що підключається до двох мереж і виконує функції шифрування і аутентифікації для численних хостів, розташованих за ним. Розміщений шлюз безпеки VPN так, щоб через нього проходив увесь трафік, призначений для внутрішньої корпоративної мережі. Мережеве з'єднання шлюзу VPN прозоро для користувачів позаду шлюзу, представляється ним виділеною лінією, хоча насправді прокладається через відкриту мережу з комутацією пакетів. Адреса шлюзу безпеки VPN вказується як зовнішню адресу тунелює пакет, що входить, а внутрішня адреса пакету є адресою конкретного хоста позаду шлюзу. Шлюз безпеки VPN може бути реалізований у вигляді окремого програмного рішення, окремого апаратного пристрою, а також у вигляді маршрутизатора або МЕ, доповнених функціями VPN.

Відкрите зовнішнє середовище передачі інформації включає як канали швидкісної передачі даних, як яка використовується мережа Інтернет, так і повільніші загальнодоступні канали зв'язки, в якості яких зазвичай застосовуються канали телефонної мережі. Ефективність віртуальної приватної мережі VPN визначається мірою захищеності інформації, циркулюючої по відкритих каналах зв'язку. Для безпечної передачі даних через відкриті мережі широко використовують інкапсуляцію і тунелювання. За допомогою методики тунелювання пакети даних передаються через загальнодоступну мережу, як по звичайному двоточковому з'єднанню. Між кожною парою «посилач — одержувач даних» встановлюється своєрідний тунель — логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

Суть тунелювання полягає в тому, щоб інкапсулювати, «упакувати», передавану порцію даних, разом із службовими полями, в новий «конверт». При цьому пакет протоколу нижчого рівня поміщається в поле даних пакету протоколу більш високого або такого ж рівня. Слід зазначити, що тунелювання саме по собі не захищає дані від НСД або спотворення, але завдяки тунелюванню з'являється

можливість повного криптографічного захисту початкових пакетів, що інкапсулюються. Щоб забезпечити конфіденційність передаваних даних, посилач шифрує початкові пакети, упаковує їх в зовнішній пакет з новим IP заголовком і відправляє по транзитній мережі (Рис. 2).

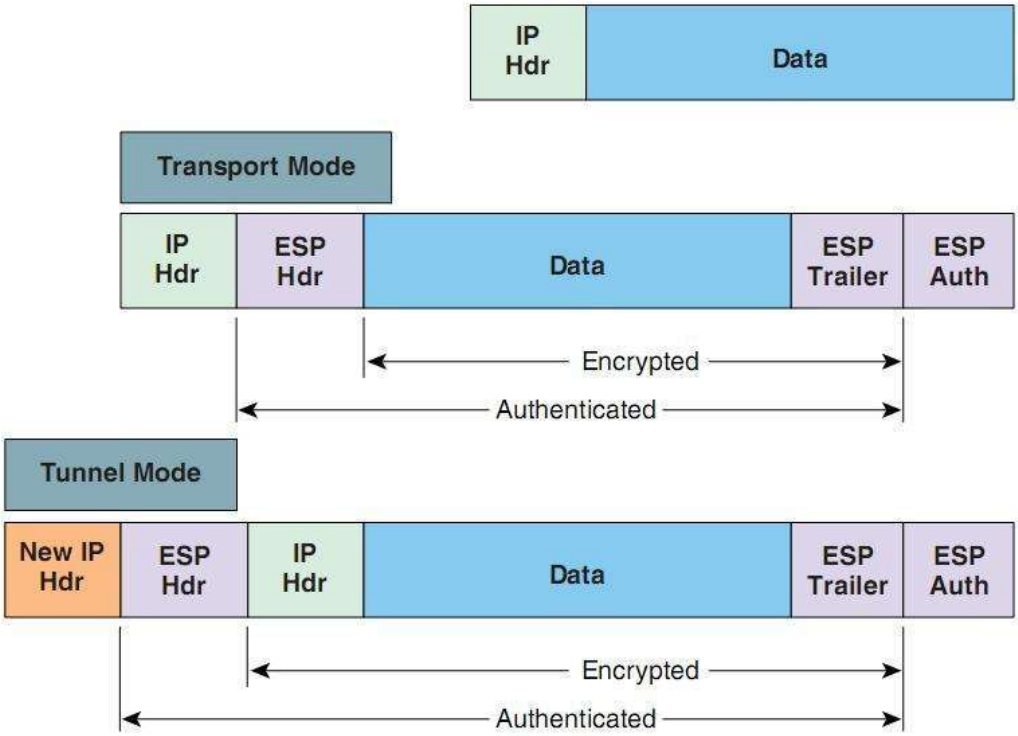

Рис. 2. Приклад пакету, підготовленого для тунелювання

Особливість технології тунелювання в тому, що вона дозволяє зашифровувати початковий пакет цілком, разом із заголовком, а не тільки його поле даних. Це важливо, оскільки деякі поля заголовка містять інформацію, яка може бути використана зловмисником. Зокрема, із заголовка початкового пакету можна витягнути відомості про внутрішню структуру мережі — дані про кількість підмереж і вузлів і їх IP адресах. Зловмисник може використати таку інформацію при організації атак на корпоративну мережу. Початковий пакет із зашифрованим заголовком не може бути використаний для організації транспортування по мережі. Тому для захисту початкового пакету застосовують його інкапсуляцію і тунелювання. Початковий пакет зашифровують повністю, разом із заголовком, і потім цей зашифрований пакет поміщають в інший зовнішній пакет з відкритим заголовком. Для транспортування даних по відкритій мережі використовуються відкриті поля заголовка зовнішнього пакету.

Після прибуття в кінцеву точку захищеного каналу із зовнішнього пакету витягають внутрішній початковий пакет, розшифровують його і використовують його відновлений заголовок для подальшої передачі по внутрішній мережі (Рис. 3).

Тунелювання може бути використане для захисту не лише конфіденційності вмісту пакету, але і його цілісності і автентичності, при цьому електронний цифровий підпис можна розповсюдити на усі поля пакету.

На додаток до приховання мережевої структури між двома точками, тунелювання може також запобігти можливий конфлікт адрес між двома

локальними мережами. При створенні локальної мережі, не пов'язаної з Internet, компанія може використати будь-які IP адреси для своїх мережевих пристроїв і комп'ютерів. При об'єднанні раніше ізольованих мереж ці адреси можуть почати конфліктувати один з одним і з адресами, які вже використовуються в Internet. Інкапсуляція пакетів вирішує цю проблему, оскільки дозволяє приховати первинні адреси і додати нові, унікальні в просторі IP адресів Internet, які потім використовуються для пересилки даних по мережах, що розділяються. Сюди ж входить завдання налаштування IP адреса і інших параметрів для мобільних користувачів, що підключаються до локальної мережі.

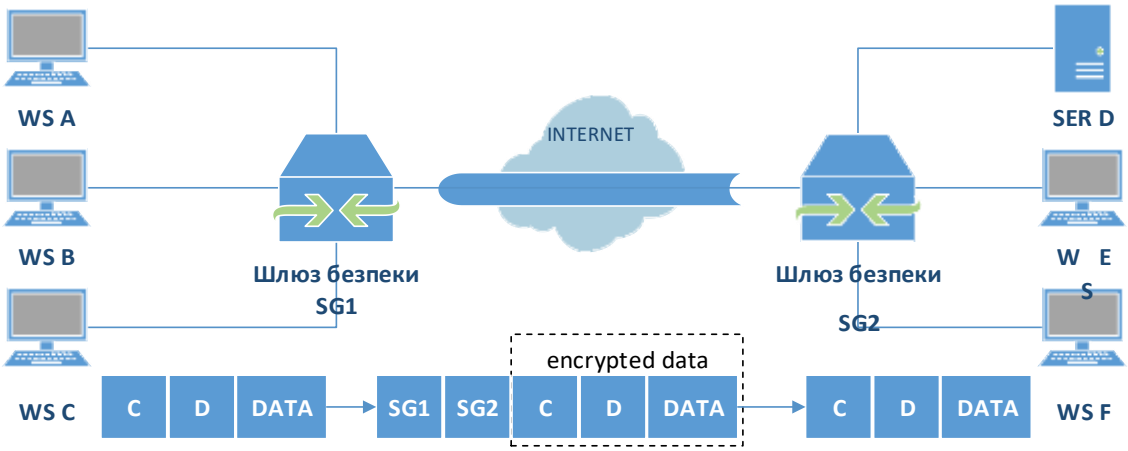

Рис. 3. Схема віртуального захищеного тунеля

Механізм тунелювання широко застосовується в різних протоколах формування захищеного каналу. Зазвичай тунель створюється тільки на ділянці відкритої мережі, де існує загроза порушення конфіденційності і цілісності даних, наприклад між точкою входу у відкритий Інтернет і точкою входу в корпоративну мережу. При цьому для зовнішніх пакетів використовуються адреси пограничних маршрутизаторів, встановлених в цих двох точках, а внутрішні адреси кінцевих вузлів містяться у внутрішніх початкових пакетах в захищеному виді. Слід зазначити, що сам механізм тунелювання не залежить від того, з якою метою застосовується тунелювання. Тунелювання може застосовуватися не лише для забезпечення конфіденційності і цілісності усієї передаваної порції даних, але і для організації переходу між мережами з різними протоколами (наприклад, IPv4 і IPv6). Тунелювання дозволяє організувати передачу пакетів одного протоколу в логічному середовищі, що використовує інший протокол. В результаті з'являється можливість вирішити проблеми взаємодії декількох різнотипних мереж, починаючи з необхідності забезпечення цілісності і конфіденційності передаваних даних і закінчуючи подоланням невідповідностей зовнішніх протоколів або схем адресації.

Реалізацію механізму тунелювання можна представити як результат роботи протоколів трьох типів: протоколу «пасажира», протоколу, що несе, і протоколу тунелювання. Наприклад, в якості протоколу «пасажира» може бути використаний транспортний протокол IPX, що переносить дані в локальних мережах філій одного підприємства. Найбільш поширеним варіантом протоколу, що несе, є протокол IP мережі Інтернет. В якості протоколів тунелювання можуть бути використані протоколи канального рівня PPTP і L2TP, а також протокол мережевого рівня

IPSec. Завдяки тунелюванню стає можливим приховання інфраструктури Internet від VPN додатків.

Тунелі VPN можуть створюватися для різних типів кінцевих користувачів — або це локальна мережа LAN (local area network) з шлюзом безпеки, або окремі комп'ютери видалених і мобільних користувачів. Для створення віртуальної приватної мережі великого підприємства потрібні VPN шлюзи, VPN сервери і VPN клієнти. VPN шлюзи доцільно використати для захисту локальних мереж підприємства, VPN сервери і VPN клієнти використовують для організації захищених з'єднань видалених і мобільних користувачів з корпоративною мережею через Інтернет.

1.2. Варіанти побудови віртуальних захищених каналів

Безпеку інформаційного обміну необхідно забезпечувати як у разі об'єднання локальних мереж, так і у разі доступу до локальних мереж видалених або мобільних користувачів [62]. При проектуванні VPN зазвичай розглядаються дві основні схеми:

1) віртуальний захищений канал між локальними мережами (канал ЛВС-ЛВС);

2) віртуальний захищений канал між вузлом і локальною мережею (Рис. 4).

Схема 1 з'єднання дозволяє замінити дорогі виділені лінії між окремими офісами і створити постійно доступні захищені канали між ними. В цьому випадку шлюз безпеки служить інтерфейсом між тунелем і локальною мережею, при цьому користувачі локальних мереж використовують тунель для спілкування один з одним. Багато компаній використовують цей вид VPN як заміну або доповнення до наявних з'єднань глобальної мережі, таким як frame relay.

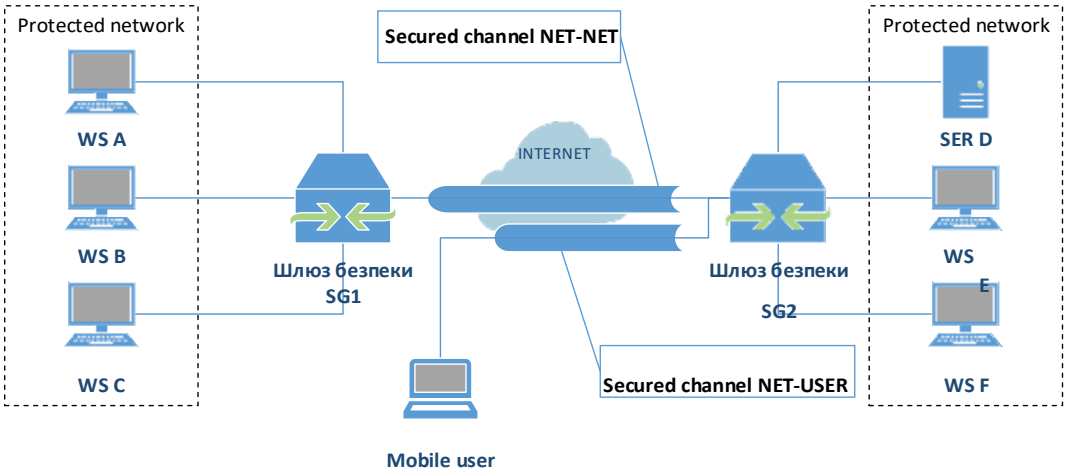

Рис. 4. Віртуальні захищені канали типу Мережа – Мережа, і Клієнт - Мережа

Схема 2 захищені канали VPN призначена для встановлення з'єднань з віддаленими або мобільними користувачами. Створення тунеля ініціює клієнт (видалений користувач). Для зв'язку з шлюзом, що захищає видалену мережу, він запускає на своєму комп'ютері спеціальне клієнтське ПЗ.

Цей вид VPN замінює собою комутовані з'єднання і може використовуватися разом з традиційними методами віддаленого доступу.

Існують варіанти схем віртуальних захищених каналів. В принципі будь-який з двох вузлів віртуальної корпоративної мережі, між якими формується віртуальний захищений канал, може належати кінцевій або проміжній точці потоку повідомлень, що захищається.

З точки зору забезпечення інформаційної безпеки кращим є варіант, при якому кінцеві точки захищеного тунеля співпадають з кінцевими точками потоку повідомлень, що захищається. В цьому випадку забезпечується захищеність каналу уздовж усього шляху дотримання пакетів повідомлень. Проте такий варіант веде до децентралізації управління і надмірності ресурсних витрат. В цьому випадку потрібна установка засобів створення VPN на кожному клієнтському комп'ютері локальної мережі. Це ускладнює централізоване управління доступом до комп'ютерних ресурсів і не завжди виправдано економічно. Окреме адміністрування кожного клієнтського комп'ютера з метою конфігурації в нім засобів захисту є досить трудомісткою процедурою у великій мережі.

Якщо усередині локальної мережі, що входить у віртуальну мережу, не потрібно захист трафіку, тоді в якості кінцевої точки захищеного тунеля можна вибрати МЕ або пограничний маршрутизатор цієї локальної мережі. Якщо ж потік повідомлень усередині локальної мережі має бути захищений, тоді в якості кінцевої точки тунеля в цій мережі повинен виступати комп'ютер, який бере участь в захищеній взаємодії. При доступі до локальної мережі віддаленого користувача комп'ютер цього користувача має бути кінцевою точкою віртуального захищеного каналу.

Досить поширеним є варіант, коли захищений тунель прокладається тільки усередині відкритої мережі з комутацією пакетів, наприклад усередині Інтернету. Цей варіант відрізняється зручністю застосування, але має порівняно низьку безпеку. Кінцевими точками такого тунеля зазвичай виступають провайдери Інтернету або пограничні маршрутизатори (міжмережеві екрани) локальної мережі.

При об'єднанні локальних мереж тунель формується тільки між пограничними провайдерами Інтернету, або маршрутизаторами (міжмережевими екранами) локальної мережі. При віддаленому доступі до локальної мережі тунель створюється між сервером віддаленого доступу провайдера Інтернету, а також пограничним провайдером Інтернету або маршрутизатором (міжмережевим екраном) локальної мережі. Побудовані по цьому варіанту віртуальні корпоративні мережі мають хорошу масштабованість і керованість. Сформовані захищені тунелі повністю прозорі для клієнтських комп'ютерів і серверів локальної мережі, що входить в таку віртуальну мережу. ПЗ цих вузлів залишається без змін. Проте цей варіант характеризується порівняно низькою безпекою інформаційної взаємодії, оскільки частково трафік проходить по відкритих каналах зв'язку в незахищеному виді. Якщо створення і експлуатацію такої VPN бере на себе провайдер ISP, тоді уся віртуальна приватна мережа може бути побудована на його шлюзах прозоро для локальних мереж і видалених користувачів підприємства. Але в цьому випадку виникають проблеми довіри до провайдера і постійної оплати його послуг.

Захищений тунель створюється компонентами віртуальної мережі, що функціонують на вузлах, між якими формується тунель. Ці компоненти прийнято називати **ініціатором тунеля** і **термінатором тунеля**.

Ініціатор тунеля інкапсулює початковий пакет в новий пакет, що містить новий заголовок з інформацією про відправники і одержувачі. Пакети, що

інкапсулюються, можуть належати до протоколу будь-якого типу, включаючи пакети протоколів, що не маршрутизуються, наприклад NetBEUI. Усі передавані по тунелю пакети є пакетами IP. Маршрут між ініціатором і термінатором тунеля визначає звичайна мережа IP, що маршрутизується, яка може бути мережею, відмінною від Інтернету.

Ініціювати і розривати тунель можуть різні мережеві пристрої і ПЗ. Наприклад, тунель може бути ініційований ноутбуком мобільного користувача, обладнаним модемом і відповідним ПЗ для встановлення з'єднань віддаленого доступу. В якості ініціатора може виступити також маршрутизатор локальної мережі, наділений відповідними функціональними можливостями. Тунель зазвичай завершується комутатором мережі або шлюзом провайдера послуг.

Термінатор тунеля виконує процес, зворотний інкапсуляції. Термінатор видаляє нові заголовки і направляє кожен початковий пакет адресатові в локальній мережі.

Конфіденційність пакетів, що інкапсулюються, забезпечується шляхом їх шифрування, а цілісність і достовірність — шляхом формування електронного цифрового підпису. Існує безліч методів і алгоритмів криптографічного захисту даних, тому необхідно, щоб ініціатор і термінатор тунеля своєчасно погоджували один з одним і використали одні і ті ж методи і алгоритми захисту. Для забезпечення можливості розшифровки даних і перевірки цифрового підпису при прийомі ініціатор і термінатор тунеля повинні також підтримувати функції безпечного обміну ключами. Крім того, кінцеві сторони інформаційної взаємодії повинні пройти аутентифікацію, щоб гарантувати створення тунелів VPN тільки між уповноваженими користувачами.

Існуюча мережева інфраструктура корпорації може бути підготовлена до використання VPN як за допомогою програмного, так і за допомогою апаратного забезпечення.

1.3. Засоби забезпечення безпеки VPN

При побудові захищеної віртуальної мережі VPN первинне значення має завдання забезпечення інформаційної безпеки. Згідно із загальноприйнятим визначенням, під безпекою даних розуміють їх конфіденційність, цілісність і доступність. Стосовно завдань VPN критерії безпеки даних можуть бути визначені таким чином:

- конфіденційність — гарантія того, що в процесі передачі даних по захищених каналах VPN ці дані можуть бути відомі тільки легальному відправнику і одержувачеві;
- цілісність — гарантія збереження передаваних даних під час проходження по захищеному каналу VPN. Будь-які спроби зміни, модифицикації, руйнування або створення нових даних будуть виявлені і стануть відомі легальним користувачам;
- доступність — гарантія того, що засоби, що виконують функції VPN, постійно доступні легальним користувачам. Доступність засобів VPN є комплексним показником, який залежить від надійності реалізації, якості обслуговування і міри захищеності самого засобу від зовнішніх атак.

Конфіденційність забезпечується за допомогою різних методів і алгоритмів симетричного і асиметричного шифрування. Цілісність передаваних даних зазвичай досягається за допомогою різних варіантів технології електронного підпису, заснованих на асиметричних методах шифрування і односторонніх функціях.

Аутентифікація здійснюється на основі багаторазових і одноразових паролів, цифрових сертифікатів, смарткарт, протоколів строгої аутентифікації, забезпечує встановлення VPN з'єднань тільки між легальними користувачами і запобігає доступу до засобів VPN небажаних осіб.

Авторизація має на увазі надання абонентам, що довели свою легальність (автентичність), різних видів обслуговування, зокрема різних способів шифрування їх трафіку. Авторизація і управління доступом часто реалізуються одними і тими ж засобами.

Для забезпечення безпеки передаваних даних у віртуальних захищених мережах мають бути вирішені наступні основні завдання мережевої безпеки:

- взаємна аутентифікація абонентів при встановленні з'єднання;
- забезпечення конфіденційності, цілісності і автентичності передаваної інформації;
- авторизація і управління доступом;
- безпека периметра мережі і виявлення вторгнень;
- управління безпекою мережі.

Аутентифікація абонентів. Процедура аутентифікації (встановлення достовірності) дозволяє вхід для легальних користувачів і запобігає доступу до мережі небажаних осіб.

Методи, алгоритми і ряд протоколів аутентифікації детально розглянуті в л. 7; протоколи і системи аутентифікації видалених користувачів приведені в л. 13.

Забезпечення конфіденційності, цілісності і автентичності інформації. Завдання забезпечення конфіденційності інформації полягає в захисті передаваних даних від несанкціонованого читання і копіювання. Основним засобом забезпечення конфіденційності інформації є шифрування.

Алгоритми шифрування і електронного цифрового підпису розглянуті в л. 6.

Авторизація і управління доступом. Ключовим компонентом безпеки VPN є гарантія того, що доступ до комп'ютерних ресурсів дістають авторизовані користувачі, тоді як для неавторизованих користувачів мережа повністю закрита.

При побудові програмних засобів авторизації застосовуються:

- централізована схема авторизації;
- децентралізована схема авторизації.

Основне призначення централізованої системи авторизації — реалізувати принцип єдиного входу. Управління процесом надання ресурсів користувачеві здійснюється сервером. Централізований підхід до процесу авторизації реалізований в системах Kerberos, RADIUS і TACACS.

Останнім часом активно розвивається так зване ролеве управління доступом. Воно вирішує не стільки проблеми безпеки, скільки покращує керованість систем. Суть ролевого управління доступом полягає в тому, що між користувачами і їх привілеями поміщають проміжні сутності - ролі. Для кожного користувача одночасно можуть бути активними декілька ролей, кожна з яких надає йому цілком певні права.

Оскільки ролей багато менше, ніж користувачів і привілеїв, використання ролей сприяє пониженню складності і, отже, поліпшенню керованості системи. Крім того, на підставі ролевої моделі управління доступом можна реалізувати такий важливий принцип, як розділення обов'язків (наприклад, неможливість самостійно скомпрометувати критично важливий процес).

Безпека периметра мережі і виявлення вторгнень. Суворий контроль доступу до додатків, сервісів і ресурсів мережі, що захищається, є важливою функцією правильно побудованої мережі. Використання таких засобів безпеки, як МЕ, системи виявлення вторгнень, системи аудиту безпеки, антивірусні комплекси забезпечує системний захист переміщуваних по мережі даних.

Важливою частиною загального рішення безпеки мережі є МЕ, які контролюють трафік, що перетинає периметр мережі, що захищається, і накладають обмеження на пропуск трафіку відповідно до політики безпеки організації.

Додатковим елементом гарантії безпеки периметра мережі є система виявлення вторгнень IDS (Intrusion Detection System), працююча в реальному часі і призначена для виявлення, фіксації і припинення неавторизованої мережевої активності як від зовнішніх, так і від внутрішніх джерел.

Системи аналізу захищеності сканують корпоративну мережу з метою виявлення потенційних уразливостей безпеці, даючи можливість адміністраторам мережі краще захистити мережу від атак.

Управління безпекою мережі. Мережі VPN інтегрують як самі мережеві пристрої, так і численні сервіси управління безпекою і пропускною спроможністю. Компаніям потрібне цілісне управління цими пристроями і сервісами через інфраструктуру VPN, включаючи користувачів віддаленого доступу і засобів extranet. У зв'язку з цим управління засобами VPN стає одному з найважливіших завдань забезпечення ефективного функціонування VPN. Система управління корпоративною мережею повинна включати необхідний набір засобів для управління політиками безпеки, пристроями і сервісами VPN будь-якого масштабу.

Система управління безпекою мережі є наріжним каменем сімейства продуктів, що забезпечують наскрізну безпеку VPN. Для забезпечення високого рівня безпеки і керованості VPN, і зокрема системи розподілу криптографічних ключів і сертифікатів, необхідно забезпечити централізоване скоординоване управління безпекою усієї корпоративної мережі, що захищається.

2. VPN рішення для побудови захищених мереж

Сьогодні технології побудови віртуальних захищених приватних мереж (VPN) привертають все більше уваги з боку великих компаній (банків, відомств, великих державних структур і т. д.). Причина такого інтересу полягає в тому, що VPN технології дійсно дають можливість не лише істотно скоротити витрати на

утримування виділених каналів зв'язку з віддаленими підрозділами (філіями), але і підвищити конфіденційність обміну інформацією.

VPN технології дозволяють організовувати захищені тунелі як між офісами компанії, так і до окремих робітників станціям і серверам. Потенційним клієнтам пропонується широкий спектр устаткування і ПЗ для створення віртуальних захищених мереж — від інтегрованих багатофункціональних і спеціалізованих пристроїв до чисто програмних продуктів.

2.1. Класифікація мереж VPN

Завдяки технології VPN багато компаній починають будувати свою стратегію з урахуванням використання Інтернету як головного засобу передачі інформації, причому навіть тій, яка є уразливою або життєво важливою.

Існують різні ознаки класифікації VPN. Найчастіше використовуються:

- «робочий« рівень моделі OSI;
- архітектура технічного рішення VPN;
- спосіб технічної реалізації VPN.

Класифікація VPN за «робочим» рівнем моделі OSI

Для технологій безпечної передачі даних по загальнодоступній (незахищеною) мережі застосовують узагальнену назву — захищений канал (secure channel). Термін «канал» підкреслює той факт, що захист даних забезпечується між двома вузлами мережі (хостами або шлюзами) уздовж деякого віртуального шляху, прокладеного в мережі з комутацією пакетів.

Захищений канал можна побудувати за допомогою системних засобів, реалізованих на різних рівнях моделі взаємодії відкритих систем OSI (Рис. 5).

Рис. 5. Рівні протоколів захищеного каналу

Класифікація VPN по «робочому» рівню моделі OSI представляє значний інтерес, оскільки від вибраного рівня OSI багато в чому залежить функціональність VPN, що реалізовується, і її сумісність з додатками, а також з іншими засобами захисту.

За ознакою «робочого» рівня моделі OSI розрізняють наступні групи VPN:

- VPN канального рівня;
- VPN мережевого рівня;
- VPN сеансового рівня.

VPN канального рівня. Засоби VPN, використовувані на канальному рівні моделі OSI, дозволяють забезпечити інкапсуляцію різних видів трафіку третього рівня (і вище) і побудову віртуальних тунелів типу «точка-точка» (від

маршрутизатора до маршрутизатора або від персонального комп'ютера до шлюзу ЛВС). До цієї групи відносяться VPN продукти, які використовують протоколи L2F (Layer 2 Forwarding) і PPTP (PointtoPoint Tunneling Protocol), а також стандарт L2TP (Layer 2 Tunneling Protocol), розроблений спільно фірмами Cisco Systems і Microsoft.

VPN мережевого рівня. VPN продукти мережевого рівня виконують інкапсуляцію IP в IP. Одним з широко відомих протоколів на цьому рівні є протокол IPSec (IP Security), призначеним для аутентифікації, тунелювання і шифрування IP пакетів. Стандартизованний консорціумом Internet Engineering Task Force (IETF) протокол IPSec увібрав в себе усі кращі рішення по шифруванню пакетів і повинен увійти в якості обов'язкового компонента в протокол IPv6.

З протоколом IPSec пов'язаний протокол IKE (Internet Key Exchange), вирішальний завдання безпечного управління і обміну криптографічними ключами між віддаленими пристроями. Протокол IKE автоматизує обмін ключами і встановлює захищене з'єднання, тоді як IPSec кодує і «підписує» пакети. Крім того, IKE дозволяє змінювати ключ для вже встановленого з'єднання, що підвищує конфіденційність передаваної інформації.

VPN сеансового рівня. Деякі VPN використовують інший підхід під назвою «посередники каналів» (circuit proxy). Цей метод функціонує над транспортним рівнем і ретранслює трафік із захищеної мережі в загальнодоступну мережу Internet для кожного сокета окремо. (Сокет IP ідентифікується комбінацією TCP з’єднання і конкретного порту або заданим портом UDP. Стек TCP/IP не має п'ятого — сеансового — рівня, проте орієнтовані на сокети операції часто називають операціями сеансового рівня.)

Шифрування інформації, що передається між ініціатором і термінатором тунеля, часто здійснюється за допомогою захисту транспортного рівня TLS (Transport Layer Security). Для стандартизації аутентифікованного проходу через МЕ консорціум IETF визначив протокол під назвою SOCKS, і в теперішній час протокол SOCKS v.5 застосовується для стандартизованої реалізації посередників каналів.

Протоколи захисту на канальному, транспортному і сеансовому рівнях детально розглядаються в л. 11. Особливості захисту на мережевому рівні за допомогою протоколів IPSec і IKE розбираються в л. 12.

Класифікація VPN за архітектурою технічного рішення

По архітектурі технічного рішення прийнято виділяти три основні види віртуальних приватних мереж:

- внутрішньокорпоративні VPN (Intranet VPN);
- VPN з віддаленим доступом (Remote Access VPN);
- міжкорпоративні VPN (Extranet VPN).

Внутрішньокорпоративні мережі VPN призначені для забезпечення захищеної взаємодії між підрозділами усередині підприємства або між групою підприємств, об'єднаних корпоративними мережами зв'язку, включаючи виділені лінії.

VPN з віддаленим доступом призначені для забезпечення захищеного віддаленого доступу до корпоративних інформаційних ресурсів мобільним і/або віддаленим (homeoffice) співробітникам компанії.

Міжкорпоративні мережі VPN призначені для забезпечення захищеного обміну інформацією із стратегічними партнерами по бізнесу, постачальниками, великими замовниками, користувачами, клієнтами і т. д. Extranet VPN забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і тим самим сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці.

Слід зазначити, що останнім часом спостерігається тенденція до конвергенції різних конфігурацій VPN.

Класифікація VPN за способом технічної реалізації

Конфігурація і характеристики віртуальної приватної мережі багато в чому визначаються типом вживаних VPNпристроїв.

За способом технічної реалізації розрізняють VPN на основі:

- маршрутизаторів;
- міжмережевих екранів;
- програмних рішень;
- спеціалізованих апаратних засобів зі вбудованими шифропроцесорами.

VPN на основі маршрутизаторів. Цей спосіб побудови VPN припускає застосування маршрутизаторів для створення захищених каналів. Оскільки уся інформація, що виходить з локальної мережі, проходить через маршрутизатор, то цілком природно покласти на нього і завдання шифрування. Приклад устаткування для VPN на маршрутизаторах — облаштування компанії Cisco Systems.

VPN на основі міжмережевих екранів. МЕ більшості виробників підтримують функції тунелювання і шифрування даних, наприклад продукт Fire Wall1 компанії Check Point Software Technologies. При використанні МЕ на базі ПК треба пам'ятати, що подібне рішення підходить тільки для невеликих мереж з невеликим об'ємом передаваної інформації. Недоліками цього методу є висока вартість рішення в перерахунку на одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює МЕ.

VPN на основі програмного забезпечення. VPN продукти, реалізовані програмним способом, з точки зору продуктивності поступаються спеціалізованим пристроям, проте мають достатню потужність для реалізації VPN мереж. Слід зазначити, що у разі віддаленого доступу вимоги до необхідної смуги пропускання невеликі. Тому чисто програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Безперечною перевагою програмних продуктів є гнучкість і зручність в застосуванні, а також відносно невисока вартість.

VPN на основі спеціалізованих апаратних засобів. Головна перевага таких VPN — висока продуктивність, оскільки швидкодія обумовлена тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Спеціалізовані VPN пристроїв забезпечують високий рівень безпеки, проте вони дорогі.

2.2. Основні варіанти архітектури VPN

Існує безліч різновидів віртуальних приватних мереж. Їх спектр варіює від провайдерських мереж, що дозволяють управляти обслуговуванням клієнтів безпосередньо на їх площах, до корпоративних мереж VPN, що розгортаються і керованих самими компаніями. Проте, прийнято виділяти три основні види віртуальних приватних мереж:

1. VPN з віддаленим доступом (Remote Access VPN),

2. внутрішньокорпоративні VPN (Intranet VPN) і
3. міжкорпоративні VPN (Extranet VPN) [9].

VPN з віддаленим доступом (Рис. 6) дозволяють значно скоротити щомісячні витрати на використання комутованих і виділених ліній. Принцип їх роботи простий: користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі, після чого їх виклики тунелюють через Інтернет, що позбавляє від плати за міжміський і міжнародний зв'язок або виставляння рахунків власникам безкоштовних міжміських номерів; потім усі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі.

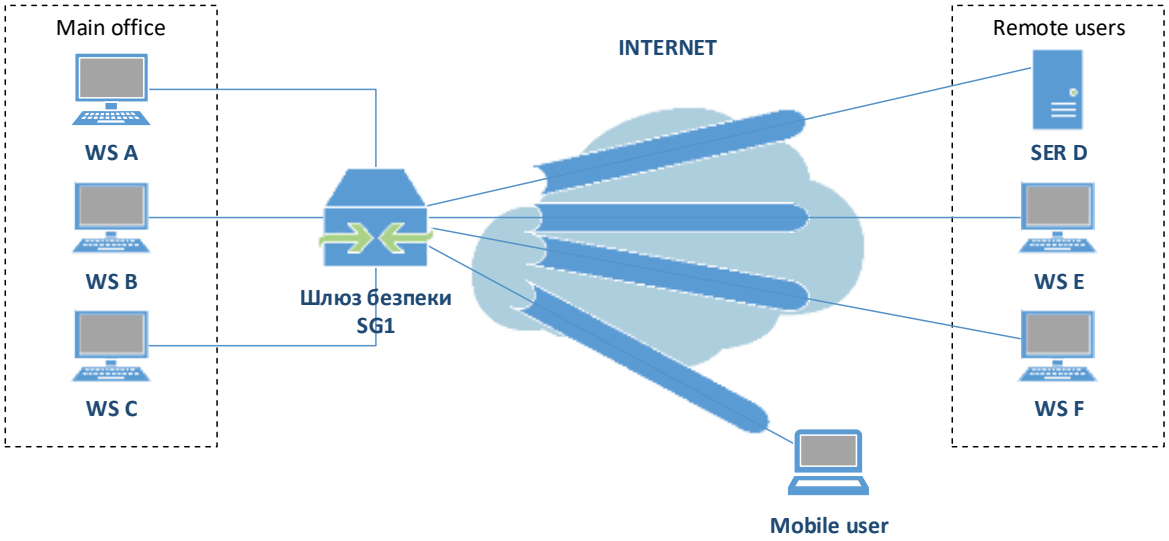

Рис. 6. Віртуальна приватна мережа з віддаленим доступом

Переваги переходу від приватно керованих dial networks до Remote Access VPN:

- можливість використання місцевих dialin numbers замість міжміських дозволяє значно понизити витрати на міжміські телекомунікації;
- ефективна система встановлення достовірності видалених і мобільних користувачів забезпечує надійне проведення процедури аутентифікації;
- висока масштабованість і простота розгортання для нових користувачів, що додаються до мережі;
- зосередження уваги компанії на основних корпоративних бизнесцілях замість відвернення на проблеми забезпечення роботи мережі.

Істотна економія при використанні Remote Access VPN є потужним стимулом, проте застосування відкритого Internet в якості об'єднуючої магістралі для транспорту чутливого корпоративного трафіку стає усе більш масштабним, що робить механізми захисту інформації життєво важливими елементами цієї технології.

Внутрішньокорпоративні мережі VPN (Рис. 7) будуються з використанням Internet або мережевих інфраструктур, що розділяються, сервіс провайдерами, що надаються. Компанії досить відмовитися від використання дорогих виділених ліній, замінивши їх дешевшим зв'язком через Internet. Це істотно скорочує витрати на використання смуги пропускання, оскільки в Internet відстань ніяк не впливає на вартість з'єднання.

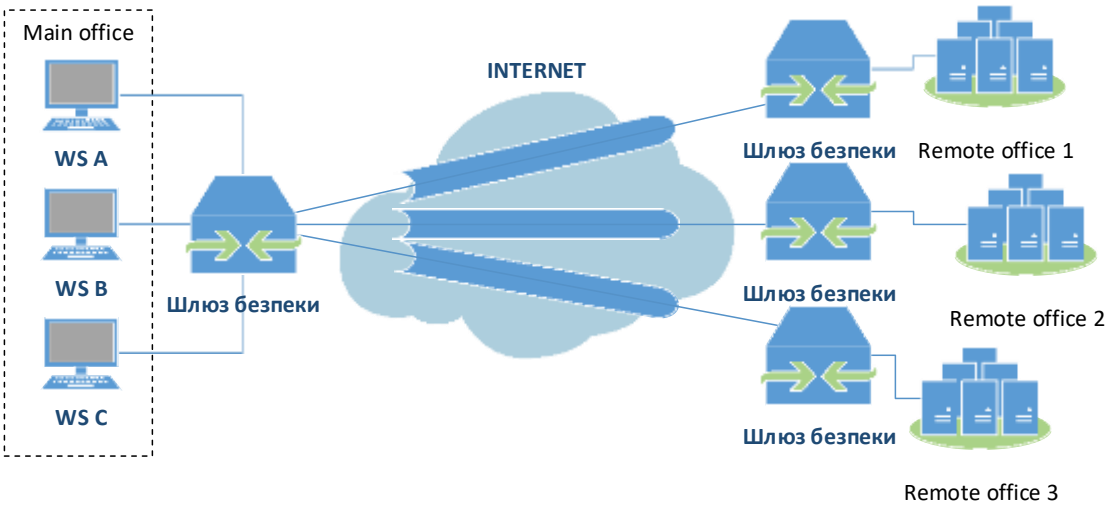

Рис. 7. З'єднання вузлів мережі за допомогою технології Intranet VPN

Переваги Intranet VPN:

- застосування потужних криптографічних протоколів шифрування даних для захисту конфіденційної інформації;
- надійність функціонування при виконанні таких критичних застосувань, як системи автоматизованого продажу і системи управління базами даних;
- гнучкість управління ефективним розміщенням швидко зростаючого числа нових користувачів, нових офісів і нових програмних застосувань.

Побудова Intranet VPN, використовуючи Internet, є найрентабельнішим способом реалізації VPNтехнології. Проте в Internet рівні сервісу взагалі не гарантуються. Компанії, яким потрібно гарантовані рівні сервісу, повинні розглянути можливість розгортання своїх VPN з використанням мережевих інфраструктур, що розділяються, сервіс провайдерами, що надаються.

Міжкорпоративна мережа VPN (Рис. 8) — це мережева технологія, яка забезпечує прямий доступ з мережі однієї компанії до мережі іншої компанії і, таким чином, сприяє підвищенню надійності зв'язку, підтримуваного в ході ділової співпраці.

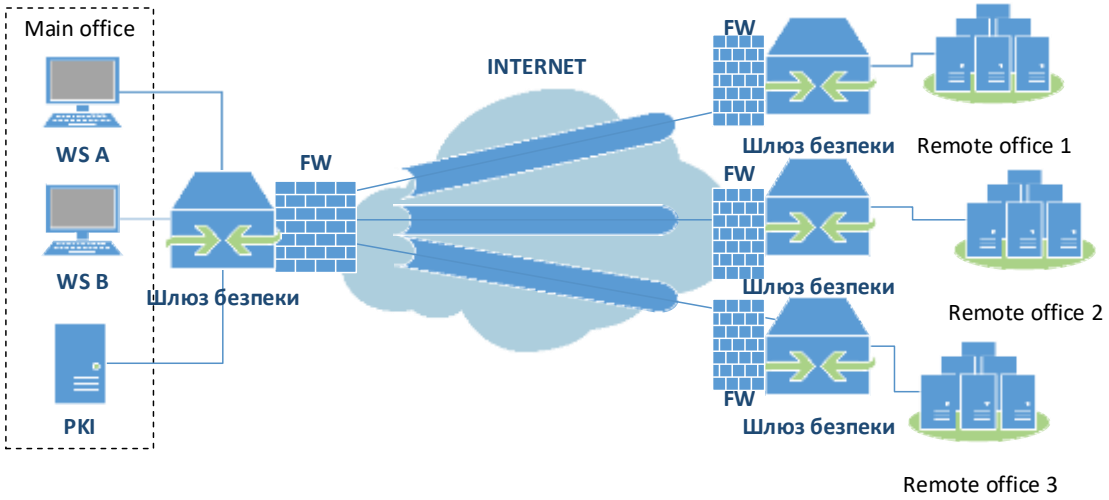

Рис. 8. Міжкорпоративна мережа Extranet VPN

Мережі Extranet VPN в цілому схожі на внутрішньокорпоративні віртуальні приватні мережі з тією лише різницею, що проблема захисту інформації є для них гострішою. Для Extranet VPN характерне використання стандартизованих VPN продуктів, що гарантують здатність до взаємодії з різними VPN рішеннями, які ділові партнери могли б застосовувати у своїх мережах.

Коли декілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні потурбуватися про те, щоб їх нові партнери мали доступ тільки до певної інформації. При цьому конфіденційна інформація має бути надійно захищена від несанкціонованого використання. Саме тому в міжкорпоративних мережах велике значення надається контролю доступу з відкритої мережі за допомогою МЕ. Важлива і аутентифікація користувачів, покликана гарантувати, що доступ до інформації дістають тільки ті, кому він дійсно дозволений. В той же час, розгорнута система захисту від несанкціонованого доступу не повинна залучати до себе уваги.

З'єднання Extranet VPN розгортаються, використовуючи ті ж архітектуру і протоколи, які застосовуються при реалізації Intranet VPN і Remote Access VPN. Основна відмінність полягає в тому, що дозвіл доступу, який дається користувачам Extranet VPN, пов'язаний з мережею їх партнера.

Іноді в окрему групу виділяють локальний варіант мережі VPN (Localnet VPN). Локальна мережа Localnet VPN забезпечує захист інформаційних потоків, циркулюючих усередині локальних мереж компанії (як правило, Центрального офісу), від НСД з боку «надмірно цікавих» співробітників самої компанії. Нині спостерігається тенденція до конвергенції різних способів реалізацій VPN [9, 65].

3. Переваги застосування технологій VPN

Ефективне застосування ИТ у поєднанні з технологіями в області інформаційної безпеки є найважливішим стратегічним чинником підвищення конкурентоспроможності сучасних підприємств і організацій. Технологія віртуальних приватних мереж VPN дозволяє вирішувати ці завдання, забезпечуючи зв'язок між мережами, а також між віддаленим користувачем і корпоративною мережею за допомогою захищеного каналу (тунеля), «прокладеного» в загальнодоступній мережі Інтернет.

Переваги використання VPN технологій для захисту інформації в розподілених мережевих ІС масштабу підприємства:

- можливість захисту усієї корпоративної мережі — від великих локальних мереж офісів до окремих робітників місць. Захист може бути поширений на усі ланки мережі — від сегментів локальних мереж до комунікаційних каналів глобальних мереж, у тому числі виділених і комутованих ліній;
- масштабованість системи захисту, т. е. для захисту об'єктів різної складності і продуктивності можна використати адекватні по рівню складнощі, продуктивності і вартості програмні або програмно апаратні засоби захисту;
- використання ресурсів відкритих мереж як окремих комунікаційних ланок корпоративної мережі; усі загрози, що виникають при використанні мереж загального користування, компенсуватимуться засобами захисту інформації;

- забезпечення підконтрольності роботи мережі і достовірна ідентифікація усіх джерел інформації. При необхідності може бути забезпечена аутентифікація трафіку на рівні окремих користувачів;
- сегментація ІС і організація безпечної експлуатації системи, оброблювальної інформацію різних рівнів конфіденційності, програмними і програмно апаратними засобами захисту інформації.

4. Технологія VPN входить до числа найважливіших технологій, які планують використати підприємства в найближчому майбутньому.