УДК 004.4

Гроза П.М., к.т.н., с.н.с.
Сомов С.В., к.т.н., доцент,Петренко М.А, студент гр. 601-ТМм
Полтавський національний технічний університет
імені Юрія Кондратюка

ПОБУДОВА VPN КАНАЛУ ДЛЯ ІТ КОМПАНІЇ

У статті розглянуто питання створення віддаленого доступу до мережі ІТ компанії шляхом побудови VPN каналу. Розглянуто способи технічної реалізації VPN та схеми маршрутизації при побудові віддаленого доступу до мережі компанії.

Ключові слова: ІТ компанії, *VPN технологія, технічна реалізація VPN*, маршрутизація.

У сучасному світі розробка програмного забезпечення ІТ компаніями передбачає розміщення відділених офісів (філіал компаній), які територіально можуть знаходитися в іншій країні та віддалений доступ (роботу) співробітників компанії. Віддалена робота співробітників може бути передбачена договором або форс мажорними обставинами (відрядження, захворювання і т.д.).

Важливе завданням у цьому випадку є пошук не дорогого рішення для віддаленому доступу до БД та бібліотек компанії співробітником. При рішенні необхідно забезпечити захист комерційних даних та інтелектуальної власності компанії. Варіантом рішення є використання VPN технології.

Переваги каналів передачі даних на основі технології VPN:

– можлива побудова мереж будь-якого географічного масштабу;

– найоптимальніший варіант побудови корпоративної мережі, якщо не висуваються додаткові вимоги до гарантій пропускної здатності організованих за допомогою публічної мережі Інтернет каналів;

– невисока вартість.

VPN - «віртуальний захищений тунель», чи шлях, за допомогою якого можна організувати віддалений захищений доступ через відкриті канали Інтернету до серверів баз даних, FTP та поштових серверів. Фізична сутність технології VPN полягає у здатності захистити трафік будь-яких інформаційних, Інтранет та Екстранет-систем, аудіовідеоконференцій, систем електронної комерції та т. ін. [2].

Тунелювання (tunneling) або інкапсуляція (encapsulation) - це спосіб передачі інформації через проміжну мережу. Такою інформацією можуть бути кадри (або пакети) іншого протоколу. При інкапсуляції кадр не передається в згенерованому вузлом-відправником вигляді, а забезпечується додатковим заголовком, містить інформацію про маршрут, що дозволяє інкапсульованим пакетам проходити через проміжну мережу (Internet). На кінці тунелю кадри деінкапсулюються і передаються одержувачу.

VPN-пристрій розташовується між внутрішньою мережею і Internet на кожному кінці з'єднання. Під час передачі даних через VPN, вони зникають "з поверхні" в точці відправлення і знову з'являються тільки в точці призначення. Завдяки тунелюванню комерційна інформація стає невидимою для інших користувачів. Перш ніж потрапити в Internet-тунель дані шифруються, що забезпечує їх додатковий захист. Протоколи шифрування визначаються VPN-рішенням.

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

Конфігурація і характеристики віртуальної приватної мережі багато в чому визначаються типом застосовуваних VPN-пристроїв.

За способом технічної реалізації розрізняють VPN на основі [1]:

– маршрутизаторів;
– міжмережевих екранів;
– програмних рішень;
– спеціалізованих апаратних засобів з вбудованими шифропроцесорами.

VPN на основі маршрутизаторів. Даний спосіб побудови VPN передбачає застосування маршрутизаторів для створення захищених каналів. Оскільки вся інформація, яка виходить із локальної мережі, проходить через маршрутизатор, то цілком природно покласти на нього і завдання шифрування. Приклад обладнання для VPN на маршрутизаторах - пристрої компанії Cisco Systems.

VPN на основі міжмережевих екранів. Міжмережевий екран більшості виробників підтримують функції тунелювання і шифрування даних, наприклад продукт Fire Wall-1 компанії Check Point Software Technologies. При використанні мережевих екранів на базі ПК потрібно пам'ятати, що подібне рішення підходить тільки для невеликих мереж з невеликим обсягом переданої інформації. Недоліками цього методу є висока вартість рішення в перерахунку на одне робоче місце і залежність продуктивності від апаратного забезпечення, на якому працює мережевий екран.

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 в разі віддаленого доступу вимоги до необхідної смузі пропускання невеликі. Тому чисто програмні продукти легко забезпечують продуктивність, достатню для віддаленого доступу. Безсумнівним достоїнством 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 обумовлено тим, що шифрування в них здійснюється спеціалізованими мікросхемами. Спеціалізовані VPN-пристрої забезпечують високий рівень безпеки, однак вони є дорогими.

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 керуються самими компаніями. Проте, прийнято виділяти три основних види віртуальних приватних мереж: VPN з віддаленим доступом (Remote Access

VPN), внутрішньо корпоративні VPN (Intranet VPN) і міжкорпоративні VPN (Extranet VPN).

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

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

– можливість використання місцевих dial-in numbers замість міжміських дозволяє значно знизити витрати на міжміські телекомунікації;

– ефективна система встановлення автентичності віддалених і мобільних користувачів забезпечує надійне проведення процедури аутентифікації;

– висока масштабованість і простота розгортання для нових користувачів, що додаються до неї;

– зосередження уваги компанії на основних корпоративних бізнес-цілей замість відволікання на проблеми забезпечення роботи мережі.

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

Таким чином, Remote Access VPN дає:

– криптографічний захист трафіку;

– засіб комутації з гарантією захисту доступу до внутрішніх ресурсів з будь-якої точки світу, що дозволяє розвивати віддалений доступ;

– розвиток комунікаційних систем компанії без вкладання значних коштів у будівництво власних виділених ліній.

При побудові Remote Access VPN необхідно виконати налаштування маршрутів, що б пакет визначив, що йому треба саме через тунель потрапити в вашу корпоративну мережу.

Розглянемо різні схеми маршрутизації при побудові віддаленого доступу до мережі компанії [3].

1) Клієнти отримують адреси в діапазоні локальної мережі. Цей варіант вимагає підтримки з боку сервера Proxy ARP, який дозволяє об'єднати дві не зв'язані на канальному рівні мережі в одну. Всі хости будуть "вважати", що знаходяться в одній фізичній мережі і обмінюватися трафіком без будь-якої додаткової маршрутизації.

До переваг такого варіанту відноситься простота реалізації і повний доступ віддалених клієнтів до ресурсів мережі. Але безпека цього рішення є вкрай низькою і вимагає високого рівня довіри до віддалених клієнтів, тому що практично неможливо розмежувати доступ до ресурсів між клієнтами локальної мережі і VPN клієнтами.

2) Клієнти отримують адреси в діапазоні який не є частиною локальної мережі, але маршрутизується з неї. Цей варіант передбачає виділення віддалених клієнтів в окрему підмережу. Обидві підмережі можуть бути частиною загальної мережі. Ми можемо управляти структурою мережі двома способами: за допомогою маски підмережі або маршрутизації. Перший варіант дозволяє перемістивши клієнта в мережу змінивши маску і дати йому доступ до обох підмереж. Другий варіант дозволяє направляти пакети з однієї підмережі через шлюз в іншу. Це забезпечує гнучкість налаштування за допомогою правил для різних підмереж з різним рівнем довіри.

Для доступу клієнтських ПК з однієї підмережі в іншу нам потрібно прописати на них статичні маршрути.

Дана схема дозволяє для віддаленої підмережі встановити свої правила, які обмежують права і можливості віддалених клієнтів в локальній мережі.

3) Клієнти отримують адреси в діапазоні, які не маршрутизуються з локальної мережі. Ця схема зазвичай не передбачає маршрутизацію з локальної мережі в віддалену і застосовується для підключення клієнтів з низьким ступенем довіри (замовники, дилери і т.п.). При такій реалізації віддаленим клієнтам доступні тільки ресурси опубліковані в VPN. Для доступу до локальної мережі вказати маршрут (як в попередньому випадку) буде недостатньо, потрібно виконати настройку сервера на трансляцію пакетів (NAT) з локальної мережі в віддалену і навпаки.

Опублікувати ресурс в VPN можна кількома способами: розмістити його на VPN сервері і дозволити доступ до нього з віддаленої мережі, прокинути у віддалену мережу потрібний порт або підключити потрібний ресурс в якості клієнта віддаленої мережі.

4) Об'єднання двох підмереж. Ця схема застосовується для об'єднання декількох підмереж (центрального офісу і філій) в єдину мережу, структура такої мережі складніша. Необхідно розуміння того, які пакети і через які інтерфейси необхідно направляти.

Висновок. У статті проведений аналіз VPN технології при побудові віддаленого доступу до мережі IT компанії і запропоновані схеми маршрутизації при створення підключення.

Список літератури

1. *VPN-решения для построения защищенных сетей) [Електронний ресурс] – Режим доступу: http://ypn.ru/342/vpn-solutions-for-secured-networking/*
2. *Побудова VPN-каналів передачі даних. [Електронний ресурс] – Режим доступу: http://old.best.com.ua/ua/poslugi-dlya-juridichnih-osib/korporativni-kanali-peredachi-danih/pobudova-vpnkanaliv-peredachi-danih*
3. *Настраиваем VPN сервер.) [Електронний ресурс] – Режим доступу: http://www.suli.odatrya.org.ua/it/seti/928-nastraivaem-vpn-server.html*

Гроза П.М., кандидат технических наук, старший научный сотрудник,
Сомов С.В., кандидат технических наук, доцент,
Петренко М.А, студент гр. 601-ТМм
Полтавский национальный технический университет
имени Юрия Кондратюка

ПОСТРОЕНИЕ VPN КАНАЛА ДЛЯ ИТ КОМПАНИИ

В статье рассмотрены вопросы создания удаленного доступа к сети ИТ компании путем построения VPN канала. Рассмотрены способы технической реализации VPN и схемы маршрутизации при построении удаленного доступа к сети компании.

Ключевые слова: *ИТ компании, VPN технология, техническая реализация VPN, маршрутизация.*

M. Petrenko, student,
P.Groza, Ph.D,
S.Somov, Ph.D
Poltava National Technical Yuri Kondratyuk University

BUILDING VPN CHANNEL FOR IT COMPANY

The paper deals with the creation of remote access to the company's IT network by constructing a VPN channel. The methods of the technical implementation of VPN and routing schemes when building remote access to the company network.

Keywords*: IT companies, VPN technology, the technical realization of the VPN, routing***.**