УДК 004.056.5 **Гордієнко С.Б.**

ВІРТУАЛЬНІ ПРИВАТНІ МЕРЕЖІ: ІСТОРІЯ, КЛАСИФІКАЦІЯ, ЗАСТОСУВАННЯ

У статті розглянуто історію формування віртуальних приватних мереж, стан питань на сьогодні та найпростіший приклад їх розгортання на базі OpenVPN.

Ключові слова: віртуальна приватна мережа, безпечний канал зв'язку, інтернет, середовище передачі, фактор безпеки, статичні ключі, віддалений доступ, локальна мережа.

У час розвитку інформоційно-коммунікаційних систем, одне з важливіших місць для бізнесу займає доступність та безпека інформації. Головним чинником у цій справі є використання безпечних потоків для її передачі. Використання віртуальних приватних мереж (ВПМ) є стандартом для безпечного віддаленого доступу та об'єднання мереж через незахищений простір, наприклад Інтернет, та надання віддаленого доступу до приватної мережі організації. ВПМ - це логічна мережа, створена поверх інших мереж, на базі загальнодоступних або віртуальних каналів інших мереж (Інтернет). Безпека передавання пакетів через загальнодоступні мережі може реалізуватися за допомогою шифрування, внаслідок чого створюється закритий для сторонніх канал обміну інформацією. ВПМ дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Термін "приватна мережа" з'явився у 60-ті роки минулого століття. У той час фахівцями нью-йоркської телефонної компанії було розроблено систему автоматичного встановлення з'єднань абонентів АТС - Centrex.

З початком впровадження в Північний Америці станцій з програмним управлінням термін набув інший зміст і став означати спосіб надання додаткових послуг телефонного зв'язку абонентам, еквівалентних послуг PBX (Private Branch Exchange), на базі АТС загального користування.

Хоча для зв'язку між собою абоненти Centrex використовували ресурси і обладнання мережі загального користування, самі вони утворювали так звані замкнуті групи користувачів CUG (Closed Users Group) з обмеженим доступом ззовні, для яких у станціях мережі реалізувались віртуальні PBX.

В даний час Centrex замінюється більш сучасним її аналогом - IP-Centrex.

Термін Віртуальна Приватна Мережа у минулому був пов'язаний з телефонною системою, але зараз асоціюється з IP мережами. Ще до того часу як була розроблена концепція ВПМ великі корпорації вклади значні ресурси для побудови приватних мереж на технологіях видалених ліній (Leased line), Frame Relay та ATM для віддаленого доступу користувачів.

У той час малі та середні компанії не мали можливості використовувати видалені лінії. З приходом Інтернету у повсякденне життя з'являються сервіси для об'єднання роботи локальних та віддалених користувачів у єдиний простір -Extranet. Але дешеві та прості рішення навколо Інтернет мали фундаментальну проблему - безпека.

Сьогодні ВПМ-рішення подолали фактор безпеки. Використовуючи спеціальні тунельні протоколи і складні процедури шифрування, цілісності і конфіденційності даних досягається надійне та безпечне рішення для об'єднання двох віддалених вузлів точка-точка (point-to-point). І, оскільки ці операції відбуваються через загальнодоступні мережі, ВПМ може коштувати значно менше, ніж для реалізації приватних або орендованих послуг.

Зараз ВПМ досягнув такого рівня, що робить впровадження простим і доступним рішенням для підприємств усіх розмірів та сфер управління, в тому числі малого і середнього бізнесу, які раніше були виключеними з «електронної революції».

Використовуючи Інтернет, компанії можуть підключити їх віддалені філії та ділових партнерів до спільної роботи. Мобільні чи віддалені працівники можуть отримувати безпечне

з'єднання з офісом через провайдера послуг Інтернет. Для великих корпорацій ВПМ є можливістю скоротити витрати на підтримку видалених ліній та їх обладнанні.

Класифікувати ВПМ рішення можна за багатьма параметрами.

1. За рівнем у моделі OSI.

Існують протоколи ВПМ, які будується на 2-ому чи 3-ому рівні моделі OSI, але частіше використовуються гібридні моделі, які охоплюють канальний, мережний та транспортний рівні.

2. За ступенем захищеності використовуваного середовища:

Захищені. Створення захищеної приватної мережі через не захищену, наприклад, Інтернет. Приклади: IPSec, OpenVPN, PPTP.

Довірчі. Коли середовище передачі вважається надійним, задача зводиться лише до побудови підмережі. Приклади: MPLS, L2TP.

3. За способом реалізації:

- Програмно-апаратні рішення
- Програмні рішення.
- Інтегроване рішення

4. За призначенням

- *Internet VPN.* Використовується для об'єднання локальних мереж через незахищені канали зв'язку.
- *Remote Access VPN.* Має на меті під'єднання до локальної мережі та її сервісів віддалених працівників компанії.
- *Екстранет VPN*. На відміну від Remote Access VPN слугує за для підключення клієнтів, чий рівень довіри є нижчим чим у працівників компанії. У такому випадку будується віртуальна мережа, на яку накладається обмеження на доступ до особливо цінної інформації.

Інтернет-VPN. Слугує для надання провайдерами доступу користувачам до інтернету через єдиний фізичний канал. Наприклад, PPPoE, що є стандартом для ADSL та L2TP для користувачів локальних мереж у державах колишнього СРСР.

Client / Server VPN. Цей тип слугує для логічного розмежування трафіку у внутрішній мережі. Він схожий з технологією VLAN.

5. За типом протоколу

Існують реалізації ВПМ під TCP/IP, IPX і AppleTalk.

За приведеною класифікацією побудуємо ВПМ з'єднання для доступу до локальної веб-сторінки компанії, яка знаходиться на тому ж комп'ютері, що і ВПМ-сервер.

Для цього налаштовуємо на нашому шлюзі ВПМ-сервер на базі OpenVPN.

OpenVPN - вільна реалізація технології віртуальної приватної мережі з відкритим вихідним кодом для створення зашифрованих каналів типу точка-точка або сервер-клієнти між комп'ютерами. Вона дозволяє встановлювати з'єднання між комп'ютерами, що знаходяться за NAT-firewall, без необхідності зміни їх налаштувань. OpenVPN була створена Джеймсом Йонаном (James Yonan) і розповсюджується під ліцензією GNU GPL. Стандарт порт - 1194.

Припустимо, що OpenVPN сервер встановлений, а веб-сервер налаштований.

Маємо таку конфігурації:

	VPN сервер	VPN клієнт
Зовнішня ip-адреса чи dns-ім'я	server.example.com	client.example.net
Локальна ip-адреса(за NAT)	192.168.0.1	192.168.100.101
ОС	Linux	Linux

Тестування OpenVPN. Задля тестування ВПМ з'єднання протестуємо просте незахищене з'єднання. Запускаємо на OpenVPN сервері таку команду:

```
# openvpn --remote client.example.net --dev tun1 --ifconfig 10.9.8.1 10.9.8.2
```

На стороні клієнта:

```
# openvpn --remote server.example.com --dev tun1 --ifconfig 10.9.8.2 10.9.8.1
```

Після цього тестуємо ping у будь-який кінець:

```
$ ping 10.9.8.1
PING 10.9.8.1 (10.9.8.1) 56(84) bytes of data.
64 bytes from 10.9.8.1: icmp_seq=1 ttl=64 time=6.57 ms
64 bytes from 10.9.8.1: icmp_seq=2 ttl=64 time=1.92 ms
```

Бачимо, що ping працює - з'єднання встановлено.

Створення сертифікатів і ключів для OpenVPN. Для функціювання OpenVPN необхідний сертифікат сервера і сертифікати клієнтів, випущені одним Центром Сертифікації (Certification Authority, CA), тобто потрібна інфраструктура відкритих ключів (Public Key Infrastructure, PKI). Для нашого прикладу ми використаємо статичний ключ, що буде як на сервері, так і на стороні клієнта за шляхом /etc/openvpn/. Вводимо команду генерації ключа:

```
# openvpn --genkey --secret static.key
```

На боці сервера створюємо файл налаштувань /etc/openvpn/tun0.conf для нашого ВПМ з'єднання:

```
dev tun0
ifconfig 10.9.8.1 10.9.8.2
secret /etc/openvpn/static.key
```

де dev tun0 - мережний тунель, ifconfig 10.9.8.1 10.9.8.2 - налаштування для тунелю точка-точка(point-to-point), secret /etc/openvpn/static.key - шлях до ключа автентифікації.

На боці клієнта створюємо файл налаштувань /etc/openvpn/tun0.conf:

```
remote server.example.com
dev tun0
ifconfig 10.9.8.2 10.9.8.1
secret /etc/openvpn/static.key
```

де remote server.example.com - dns ім'я ВПМ-сервера.

Тепер запускаємо на обох кінцях однаковою командою ВПМ з'єднання:

```
openvpn --config /etc/openvpn/tun0.conf
```

та перевіряємо пінг:

```
$ ping 10.9.8.1
PING 10.9.8.1 (10.9.8.1) 56(84) bytes of data.
64 bytes from 10.9.8.1: icmp_seq=1 ttl=64 time=2.24 ms
64 bytes from 10.9.8.1: icmp_seq=2 ttl=64 time=2.04 ms
```

Перевіримо доступність веб-серверу:

```
$ telnet 10.9.8.1 80
Trying 10.9.8.1...
Connected to 10.9.8.1.
Escape character is '^]'.
<html>
<body>
<h1>It works!</h1>
</body>
</html>
```

Все працює!

ЛІТЕРАТУРА

1. Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: учеб. для вузов. - СПб.: Питер, 2001. - 672 с.
2. Сторінка з wikipedia - http://en.wikipedia.org/wiki/VPN
3. http://www.articlesbase.com/networks-articles/a-brief-history-of-vpn-virtual-private-network-5646054.html
4. Сторінка з wiki проекту debian про OpenVPN - http://wiki.debian.org/OpenVPN

Надійшла: 30.03.2013 р.

Рецензент: д.т.н., проф. Козловський