УДК 621.39

ПОБУДОВА ВІРТУАЛЬНИХ ПРИВАТНИХ МЕРЕЖ НА ОСНОВІ ОБЛАДНАННЯ ФІРМИ CISCO

Волік Д. В., Григоренко О.Г.
Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: stormfall927@gmail.com, olenagri@ukr.net

Наведено термінологію, статистичні дані, методи налаштування віртуальних приватних мереж та їх реалізація. Зображено класифікацію, а також порівняння різних типів віртуальних приватних мереж (VPN).

Design of virtual private networks based on CISCO equipment

Theoretical base, statistics, methods for setting up and implementing virtual private networks are given. The classification and comparison of different types of virtual private networks (VPNs) are also shown.

Віртуальні приватні мережі (VPN) використовуються у всьому світі, щоб забезпечити зашифровані підключення до Інтернету. Це надає можливість користуватися мережею Інтернет з підвищеною конфіденційністю. Більше того, VPN може замінити справжню IP-адресу на іншу з іншого регіону, що дозволяє отримувати інформацію, доступ до якої раніше був заблокований.

Ринок VPN невпинно зростає. Згідно з дослідженнями компанії Knowledge Sourcing Intelligence LLP, ринок VPN буде зростати з темпами 6,39% на рік протягом наступних п'яти років [1]. У 2018 році ринок охоплював близько 34,6 мільярда доларів, тож, враховуючи цей темп, до 2024 року його обсяг сягне понад 50 мільярдів доларів. У звіті основною причиною зростання попиту зазначаються проблеми кібербезпеки. Однак, оскільки VPN направляє дані на інший сервер перед тим, як перенести користувача на потрібну веб-сторінку, з’являються певні проблеми із продуктивністю та швидкістю, що частково стримує попит на ці послуги протягом прогнозованого періоду.

Віртуальні приватні мережі також можуть слугувати і для організації мереж без шифрування, тобто загальнодоступних. Існує низка способів реалізації VPN з використанням таких технологій, як GRE, SSL, IPsec та ін. Побудова віртуальних приватних мереж включає в себе створення тунелів, що являють собою канали, які сполучають два пристрої. Цими каналами і передаються дані. Налаштування тунелів - обов’язкова задача мережевого інженера при реалізації VPN. Тунелі поділяються на два типи [2]:

1. **Remote Access VPN** – тунель сполучає комп’ютер користувача з відповідним програмним забезпеченням та будь-який пристрій, що виконує роль сервера і реалізує підключення клієнтів. Ним може бути маршрутизатор, VPN-концентратор, Cisco ASA і т. п.
2. **Site-to-Site VPN** – передбачає постійний тунель між двома пристроями (наприклад, маршрутизаторами). Користувачі ж знаходяться у локальних мережах (LAN) і даний спосіб тунелювання не потребує завантаження спеціалізованого програмного забезпечення.

Нижче наведено приклади використання цих технологій.

Перший тип застосовується, коли необхідно забезпечити підключення віддалених співробітників до корпоративної мережі за допомогою захищеного каналу. В даному випадку, якщо користувач має стабільне інтернет-з'єднання та завантажив відповідне програмне забезпечення, комп'ютер самостійно побудує даний тунель до маршрутизатора компанії.

Другий тип часто використовується за необхідності з'єднання віддалених мереж, наприклад, філіалів або філіалу з центральним офісом. Роботу зі створення тунелю виконує сам граничний маршрутизатор. Він будує віддалене з'єднання від маршрутизатора з локальної мережі користувача – тунель, отже, співробітник без спеціалізованого програмного забезпечення здатний працювати у локальній мережі офісу.

З точки зору мережевого інженера, більших знань та навичок потребує реалізація Site-to-Site VPN. Два способи налаштування захищеного доступу між двома офісами, а саме алгоритми, полягають у наступному [3].

Перший спосіб – *використання тунельних інтерфейсів*. Він доречний у випадку створення тунелю між двома маршрутизаторами Cisco.

Кроки реалізації:

1. Вибір параметрів шифрування для тунелю;
2. Ключі шифрування. Вони мають бути спільними на обох маршрутизаторах. Рекомендовано зробити їх довшими за 50 символів та використовувати букви різного регістру, цифри та спеціальні символи для більшої безпеки;
3. Створення віртуальних тунельних інтерфейсів для кожного офісу. Якщо їх налаштування виконано правильно, стан інтерфейсів буде показаний як "up";
4. Перевірка роботи VPN-тунелю за допомогою команди ping;
5. Налаштування маршрутизації, для того, щоб мережі мали доступ одна до одної.

Другий спосіб – *універсальний*. Він підходить, коли тунель встановлюється між маршрутизатором та Cisco ASA або іншим пристроєм, що підтримує технологію IPsec VPN, не обов'язково виробництва Cisco.

Кроки реалізації:

1. Вибір параметрів шифрування для тунелю;
2. Ключі шифрування. Вимоги як для першого способу;
3. Об'єкти шифрування. Зазначається трафік, що має бути зашифрований;
4. Політика шифрування. Для кожної з мереж створюється політика crypto map, у якій надаються правила та параметри шифрування;
5. Налаштування маршрутизації, для того, щоб мережі мали доступ одна до одної;
6. Перевірка роботи VPN-тунелю за допомогою команди ping.

В таблиці 1 надано порівняння двох часто використовуваних типів VPN: Cisco GRE VPN та Традиційних IP Sec VPN.

Таблиця 1.

Назва	Cisco GRE VPN	Традиційні IP Sec VPN
Переваги	- Забезпечує передачу широкомовного і маршрутизаційного трафіку через тунелі IPSec VPN - Підтримка протоколів відмінних від IP - підтримка QoS	- Функції захисту переданого між двома точками трафіку - підтримка QoS
Причини застосування	- При необхідності маршрутизації в мережі VPN - Реалізує функції аналогічні топології зірка DMVPN, але вимагає більш об'ємної і детальної конфігурації	- При побудові мережі з обладнання різних виробників
Сумісність обладнання	Тільки маршрутизатори Cisco	Повна, у тому числі від різних виробників
Масштабування	Тисячі пристроїв у мережі	Тисячі пристроїв у мережі
Управління та контроль	Cisco Security Manager, Cisco Router and Security Device Manager	Cisco Security Manager, Cisco Router and Security Device Manager
Топологія	Зірка, невеликі повнозв’язні мережі VPN	Зірка, невеликі повнозв’язні мережі VPN
Динамічна маршрутизація	Підтримується	Підтримується
Якість обслуговування	Підтримується	Підтримується
Широкомовний трафік	Через тунель VPN	Ні
Підтримка протоколів, відмінних від IP	Так	Ні
Резервування	Засобами протоколів маршрутизації	Можливість активізації резервного каналу

Таким чином, зі збільшенням кіберзагроз у сучасному світі впровадження віртуальних приватних мереж є і буде залишатися актуальним. Шифрування трафіку та ізольованість VPN є основними рисами, що забезпечують конфіденційність даних в телекомунікаційних мережах.

Література

1. Aimee O'Driscoll / VPN statistics: What the numbers tell us about VPNs // UPDATED: February 25, 2020 [Електронний ресурс] – Режим доступу: https://www.comparitech.com/vpn/vpn-statistics/
2. Bacek / Принципы организации VPN // [Електронний ресурс] – Режим доступу: http://ciscotips.ru/vpn
3. Nevidimkastd / VPN между двумя маршрутизаторами Cisco // Март 15, 2015 // [Електронний ресурс] – Режим доступу: https://deltaconfig.ru/router-site-to-site-vpn/
4. «Технориум» - интеграция / Развертывание виртуальных частных сетей VPN // Сравнение технологий построения VPN [Електронний ресурс] – Режим доступу: http://www.technorium.ru/vpn/compare-vpn-cisco.shtml.