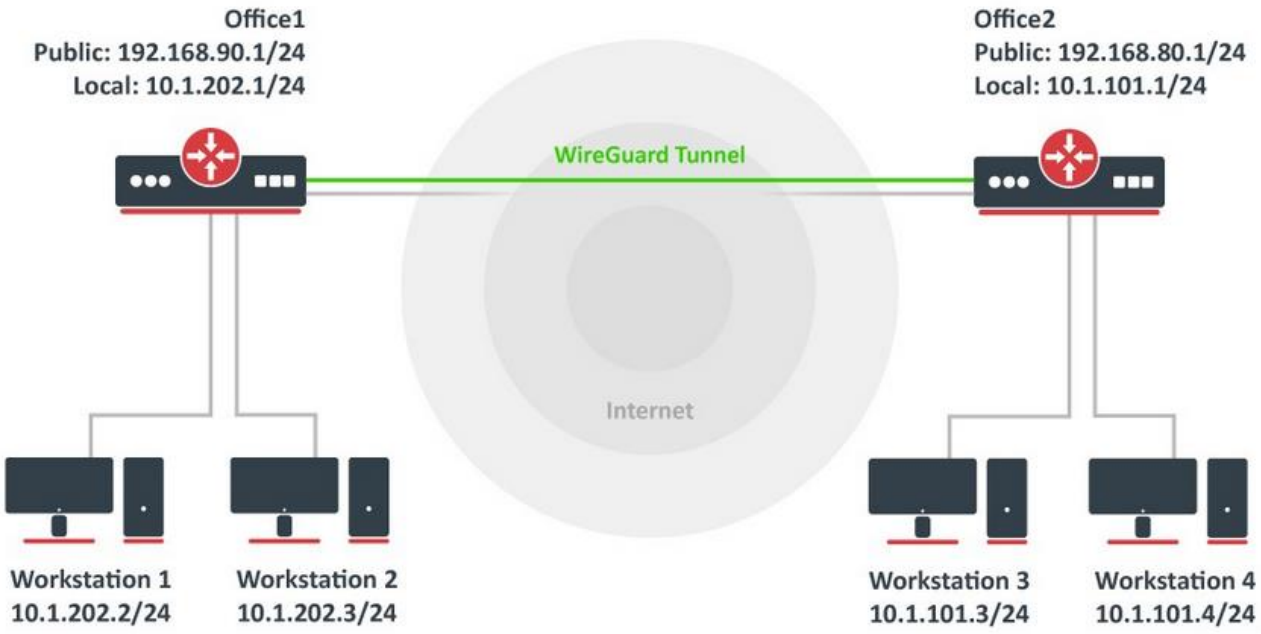
Лабораторна робота № 6. Налаштування Site to Site WireGuard VPN

Метою даної лабораторної роботи є отримання базових навичок по налаштуванню WireGuard VPN пристроях під керуванням операційній системі RouterOS.

Завдання на лабораторну роботу

- Зібрати схему і провести попереднє налаштування роутера через консоль в GNS3
- Налаштувати site to site wireguard тунель між пристроями.
- Перевірити досяжність мереж.

Розглянемо налаштування схеми на рис. 1. Два віддалені офісні маршрутизатори підключені до Інтернету, а офісні робочі станції знаходяться за NAT. Кожен офіс має власну локальну підмережу, 10.1.202.0/24 для Office1 і 10.1.101.0/24 для Office2. Обидва віддалені офіси потребують безпечних тунелях до локальних мереж за маршрутизаторами.



Конфігурація інтерфейсу WireGuard

Перш за все, інтерфейси WireGuard повинні бути налаштовані на обох сайтах, щоб дозволити автоматичне генерування приватних і відкритих ключів. Команда однакова для обох маршрутизаторів:

```
/interface/wireguard
add listen-port=13231 name=wireguard1
```

Тепер під час друку деталей інтерфейсу повинні бути видимі як приватні, так і відкриті ключі, щоб дозволити обмін.

Жоден секретний ключ ніколи не знадобиться на віддаленому пристрої - звідси й назва приватний.

Office1

```
/interface/wireguard print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-key="yKt9NJ4e5qlaSgh48WnPCDCEkDmq+VsBTt/DDEBWfEo="
      public-key="u7gYAg5tkioJDcm3hyS7pm79eADKPs/ZUGON6/fF3iI="
```

Office2

```
/interface/wireguard/print
Flags: X - disabled; R - running
 0  R name="wireguard1" mtu=1420 listen-port=13231 private-key="KMwxqe/iXAU8Jn9dd1o5pPdHep2blGxNWm9I944/I24="
      public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+Tb5e601M="
```

Однорангова конфігурація

Конфігурація однорангового зв’язку визначає, хто може використовувати інтерфейс WireGuard і який тип трафіку можна передавати через нього. Щоб ідентифікувати віддалений одноранговий вузол, його відкритий ключ необхідно вказати разом із створеним інтерфейсом WireGuard.

Office1

```
/interface/wireguard/peers
add allowed-address=10.1.101.0/24 endpoint-address=192.168.80.1 endpoint-port=13231 interface=wireguard1 \
public-key="v/oIzPyFm1FPHrqhytZgsKjU7mUToQHLrW+Tb5e601M="
```

Office2

```
/interface/wireguard/peers
add allowed-address=10.1.202.0/24 endpoint-address=192.168.90.1 endpoint-port=13231 interface=wireguard1 \
public-key="u7gYAg5tkioJDcm3hyS7pm79eADKPs/ZUGON6/fF3iI="
```

IP і конфігурація маршрутизації

Нарешті, IP-адреса та інформація про маршрути повинні бути налаштовані, щоб дозволити надсилання трафіку через тунель.

Office1

```
/ip/address
add address=10.255.255.1/30 interface=wireguard1
/ip/route
add dst-address=10.1.101.0/24 gateway=wireguard1
```

Office2

```
/ip/address
add address=10.255.255.2/30 interface=wireguard1
/ip/route
add dst-address=10.1.202.0/24 gateway=wireguard1
```

Налаштування Firewall

Firewall RouterOS за замовчуванням блокує належне встановлення тунелю. Трафік має прийматися у ланцюжку "input" перед будь-якими правилами відкидання на обох сайтах.

Office1

```
/ip/firewall/filter
add action=accept chain=input dst-port=13231 protocol=udp src-address=192.168.80.1
```

Office2

```
/ip/firewall/filter
add action=accept chain=input dst-port=13231 protocol=udp src-address=192.168.90.1
```

Крім того, можливо, що "input" ланцюжок також обмежує зв'язок між підмережами, тому такий трафік також слід приймати до будь-яких правил відкидання.

Office1

```
/ip/firewall/filter
add action=accept chain=forward dst-address=10.1.202.0/24 src-address=10.1.101.0/24
add action=accept chain=forward dst-address=10.1.101.0/24 src-address=10.1.202.0/24
```

Office2

```
/ip/firewall/filter
add action=accept chain=forward dst-address=10.1.101.0/24 src-address=10.1.202.0/24
add action=accept chain=forward dst-address=10.1.202.0/24 src-address=10.1.101.0/24
```

Завдання на лабораторну роботу

1. Провести базове налаштування роутерів і IP-адрес інтерфейсів відповідно до Таблиці 1

Таблиця 1

Дані для адресації підмереж

Office 1		Office 2	
IP-адреса (Public)	Префікс	IP-адреса (Public)	Префікс
193.G.N.0	/24	193.G.N.0	/24
IP-адреса (Local)	Префікс	IP-адреса (Local)	Префікс
100.G.N+3.0	/24	100.G.N+4.0	/24

2. Провести налаштування wireguard site to site VPN.
3. Перевірити досяжність хостів у мережі
4. Запишіть висновки по виконаній роботі.