

Minggu 9 – IP Security

TIS13534P

KOMUNIKASI DAN KEAMANAN DATA

Ingat IP yang kamu pakai itu Publik!

- Ketika kamu terhubung dengan internet, IP address adalah identitas dari computer/perangkat yang kamu pakai. Dan orang lain bisa menggunakan IP computer/perangkat untuk mencari di mana kamu berasal.
- IP statik juga berbahaya karena sifatnya yang tetap dan tidak berubah-ubah.

Dial-Up vs ADSL

- Kalau kamu masih memakai koneksi Dial-Up, IP yang akan kamu dapatkan pasti berbeda setiap kali kamu terhubung ke Internet.
- Tapi jika kamu berlangganan Internet Kabel ADSL, kemungkinan kamu mendapatkan IP yang sama adalah besar
- Terlebih lagi jika kamu langganan dedicated static IP untuk web server, serangan IP menjadi 100%

ipleak.net tanpa VPN

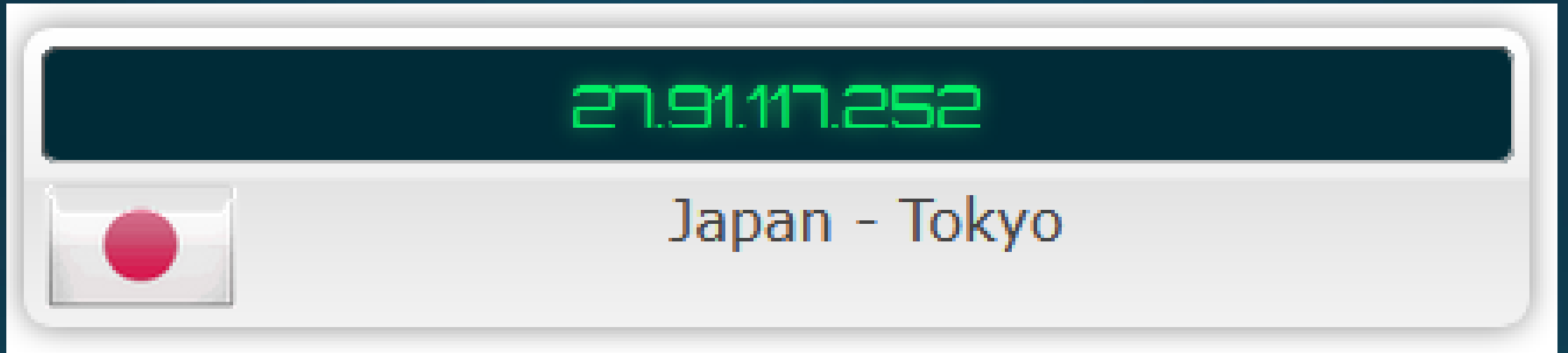


IP Komputer yang saya gunakan adalah 158.140.17.21

Pengamanan IP dengan VPN

- Seperti yang sudah dibahas sebelumnya, VPN adalah satu-satunya cara mengamankan IP kita dari orang lain
- Selain menyembunyikan IP, VPN juga melakukan enkripsi koneksi sehingga aman dari serangan Sniffer

ipleak.net dengan VPN

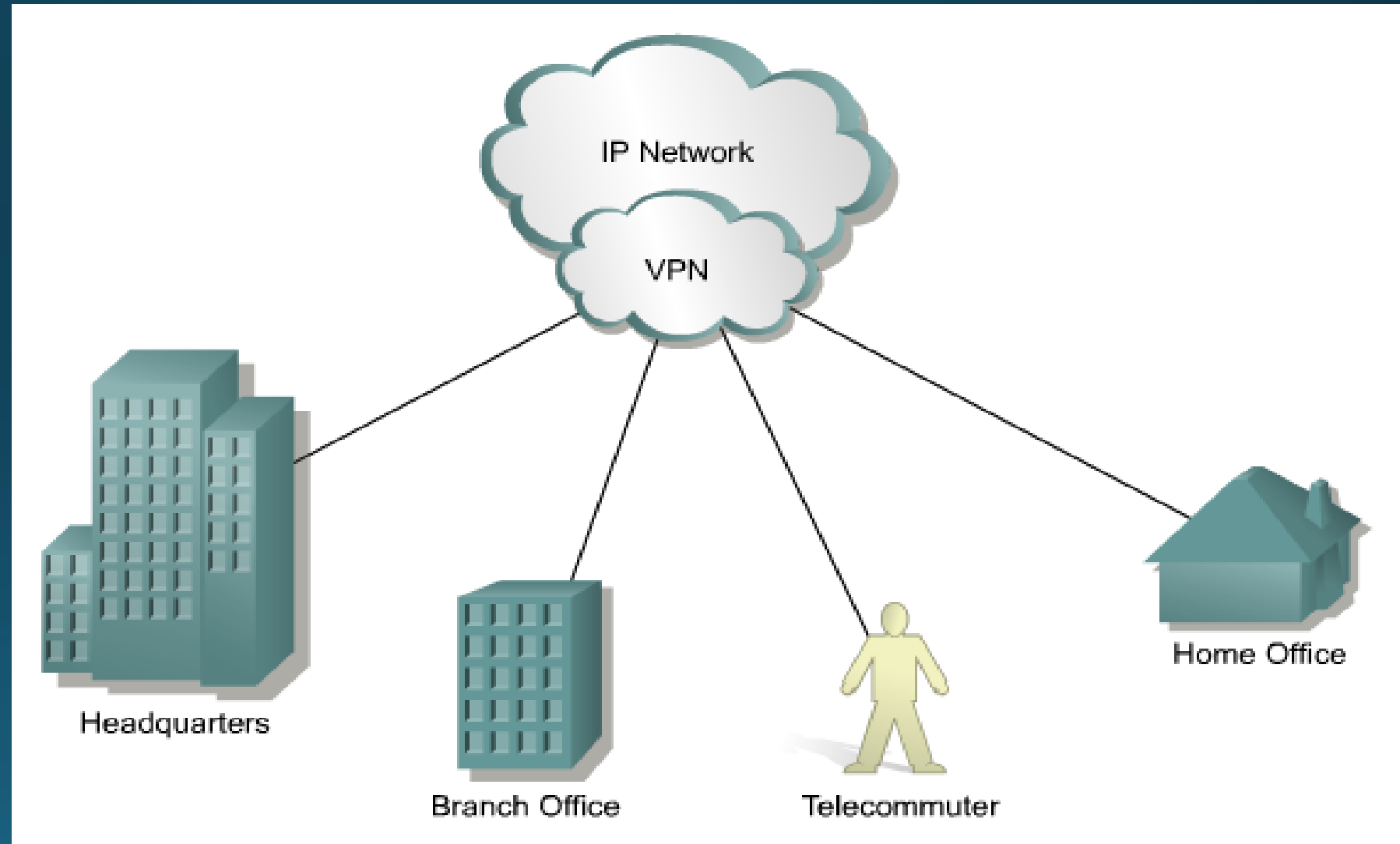


IP yang saya pakai adalah 27.91.117.252

Virtual Private Network

- Apa itu VPN?
 - Sebuah jaringan pribadi virtual yang di mana remote user dapat bergabung, dan dapat mengakses internet tanpa batasan dan tetap aman dari serangan internet
- Seperti yang sudah dijelaskan sebelumnya
 - VPN memerlukan username dan password untuk masuk ke dalam jaringannya

Ilustrasi



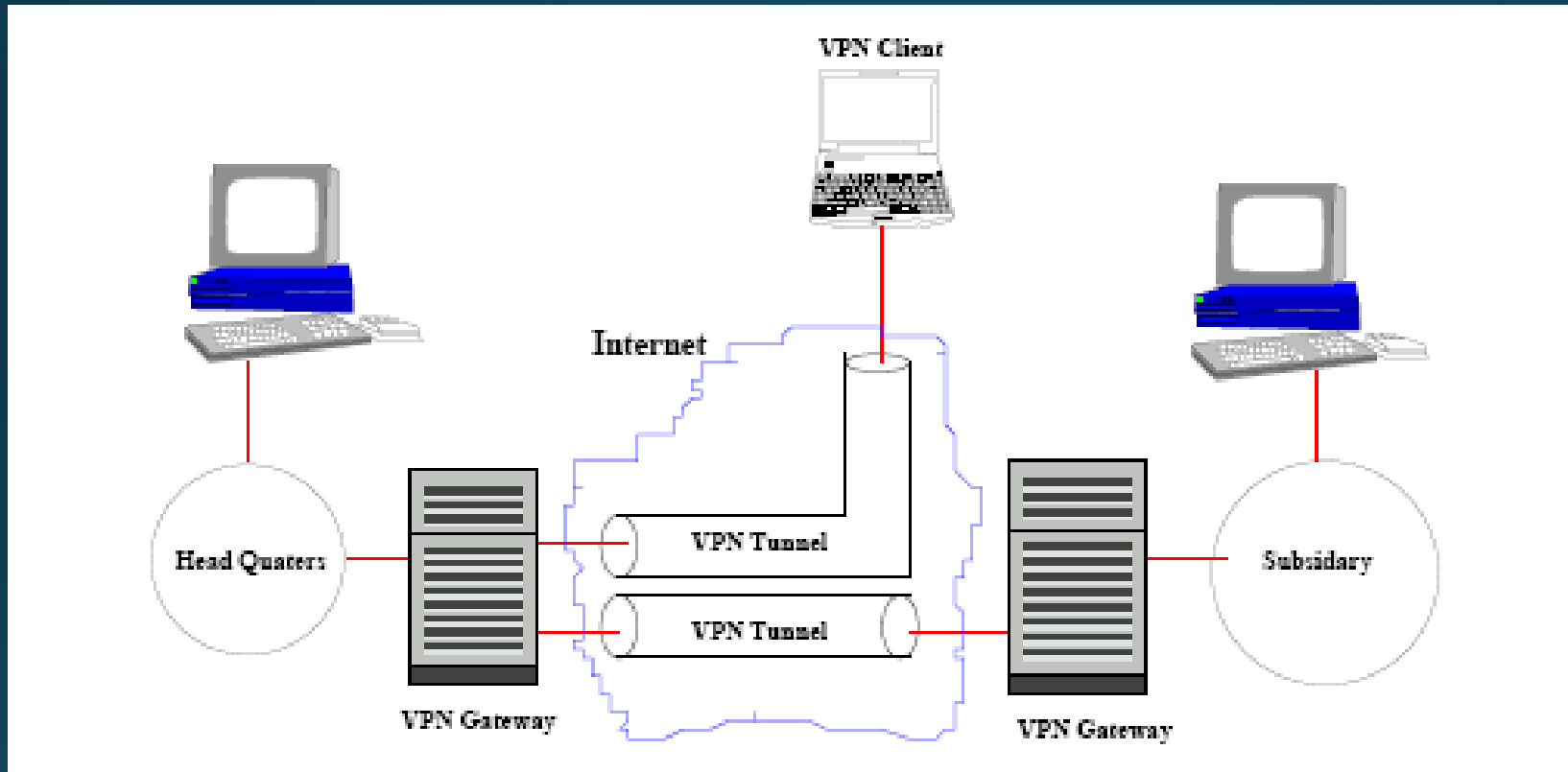
Protokol-Protokol VPN

1. *Point-to-point tunneling protocol (PPTP)*
2. *Layer-2 forwarding (L2F)*
3. *Layer-2 tunneling protocol (L2TP)*
4. *IP security protocol (IPSec)*

IP Security (IPSec)

- IPSec adalah sekumpulan ekstensi dari keluarga protokol IP yang menyediakan layanan kriptografi untuk keamanan transmisi data.
- IPSec bekerja dengan tiga jalan, yaitu:
 - 1. *Network-to-network*
 - 2. *Host-to-network*
 - 3. *host-to-host*

Ilustrasi



- Komunikasi antar gateway yang akan melakukan verifikasi otentifikasi pengirim dan penerima dan mengenkripsi semua lalu lintas

Protokol IPSec - Keamanan

1. AH (*Authentication header*), AH menyediakan layanan *authentication, integrity*, dan *replay protection*, namun tidak dengan *confidentiality*. AH juga melakukan pengamanan terhadap header IP
2. ESP (*Encapsulated security payload*), ESP menyediakan layanan *authentication, integrity, replay protection*, dan *confidentiality* terhadap data (ESP melakukan pengamanan terhadap segala sesuatu dalam paket data setelah header)

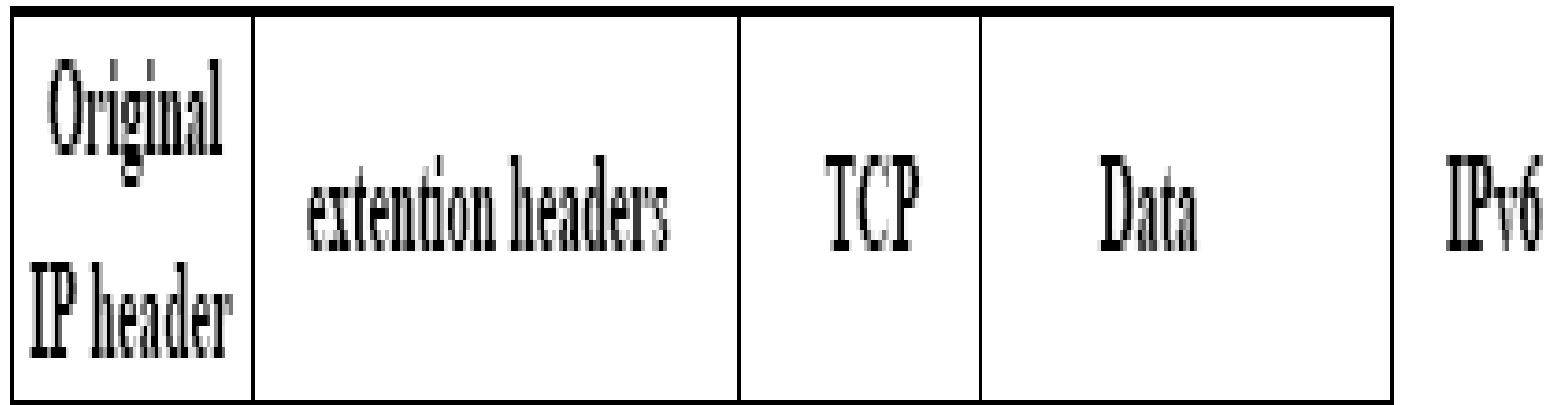
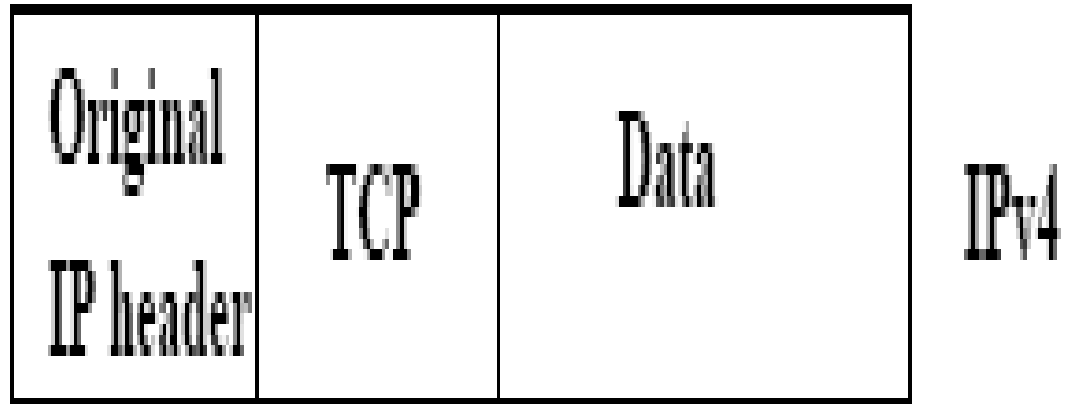
Security Association

- 1. Destination IP address*
- 2. Security parameter index*
- 3. Security protocol.*

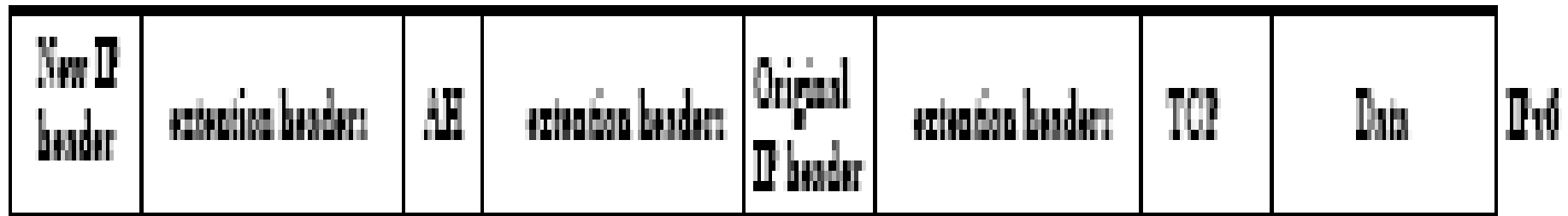
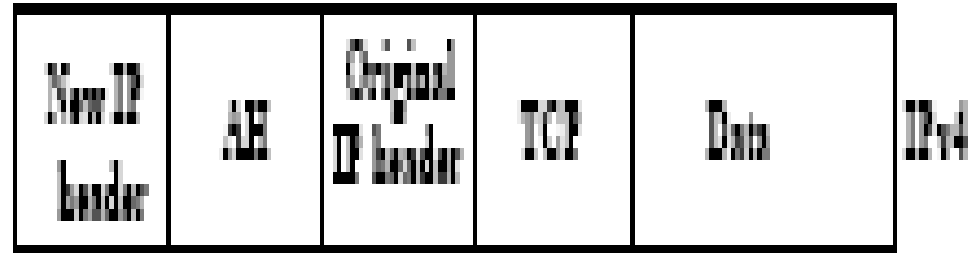
Model IPSec

- ***Transport mode***. *Transport mode* digunakan untuk mengenkripsi dan mengotentifikasi *optional* data IP (*transport layer*).
- ***Tunnel mode***. *Tunnel mode* mengenkripsi seluruh paket IP.

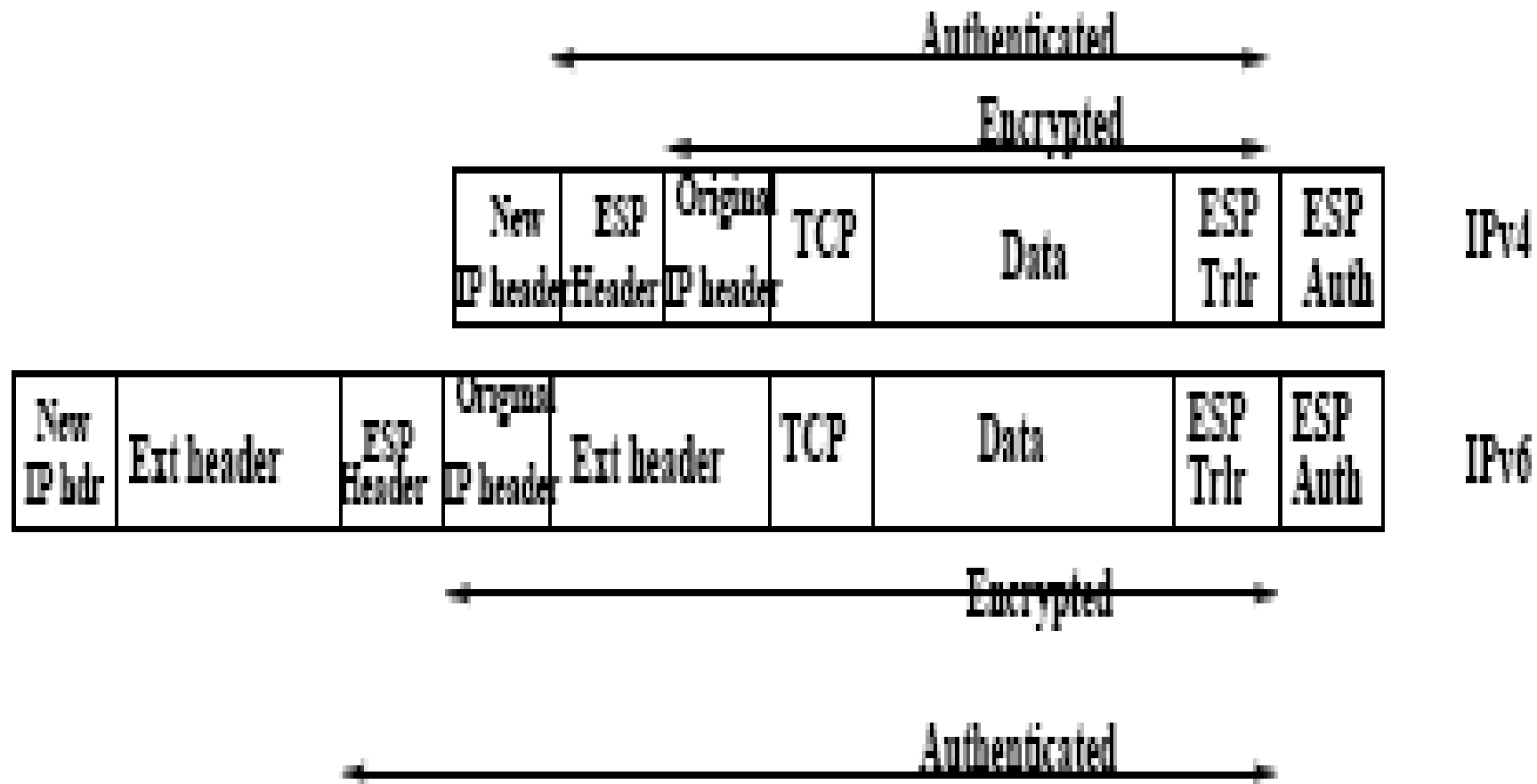
Paket IP tanpa IPSec



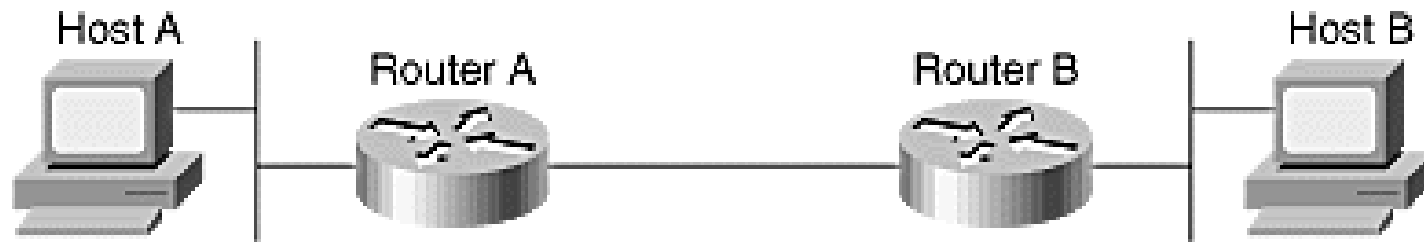
Tunnel Mode + AH Header



Tunnel Mode + ESP



Cara Kerja IPSec



1. Host A sends interesting traffic to Host B.
2. Routers A and B negotiate an IKE phase one session.



3. Routers A and B negotiate an IKE phase two session.



4. Information is exchanged via IPSec tunnel.



5. IPSec tunnel is terminated.

Internet Key Exchange (IKE) berguna untuk otentifikasi antar peer dengan mengirimkan pesan.

IKE juga dapat digunakan untuk berbagai macam jenis otentifikasi

Internet Key Exchange

- IKE ini akan melakukan pertukaran berbagai jenis kunci tergantung konfigurasi. Pada umumnya menggunakan:
 - Pre-shared key yang disediakan oleh penyedia VPN server
 - RSA signatures: menggunakan sertifikat digital yang diotentifikasikan oleh RSA signature
 - RSA encrypted nonces: Menggunakan enkripsi RSA untuk mengenkripsi nilai nonce (nomor acak yang dibuat oleh peer) dan nilai lain

L2TP+IP Sec

VPN yang menggunakan protocol L2TP pasti menggunakan IPSec.

Sebagai Contoh: VPN Gate menggunakan L2TP + IPSec dengan pre-shared key.

VPN Gate Server Korea

Nama server: vpn419074312.opengw.net

IP Server: 121.140.156.131

Username: vpn, Password: vpn

Pre-shared Key (Secret): vpn

Cara Set Up L2TP+IPSec

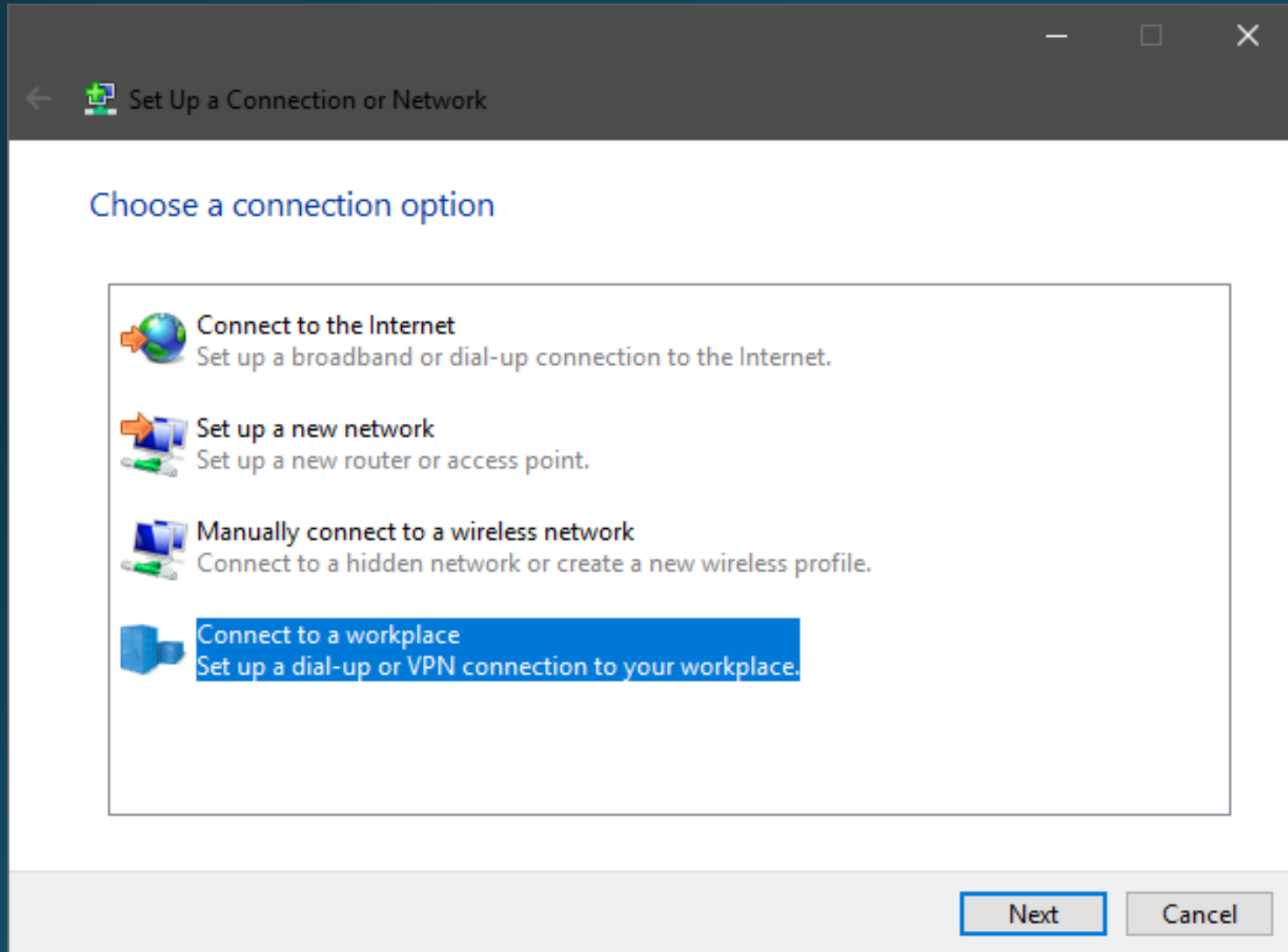


Set up a new connection or network

Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

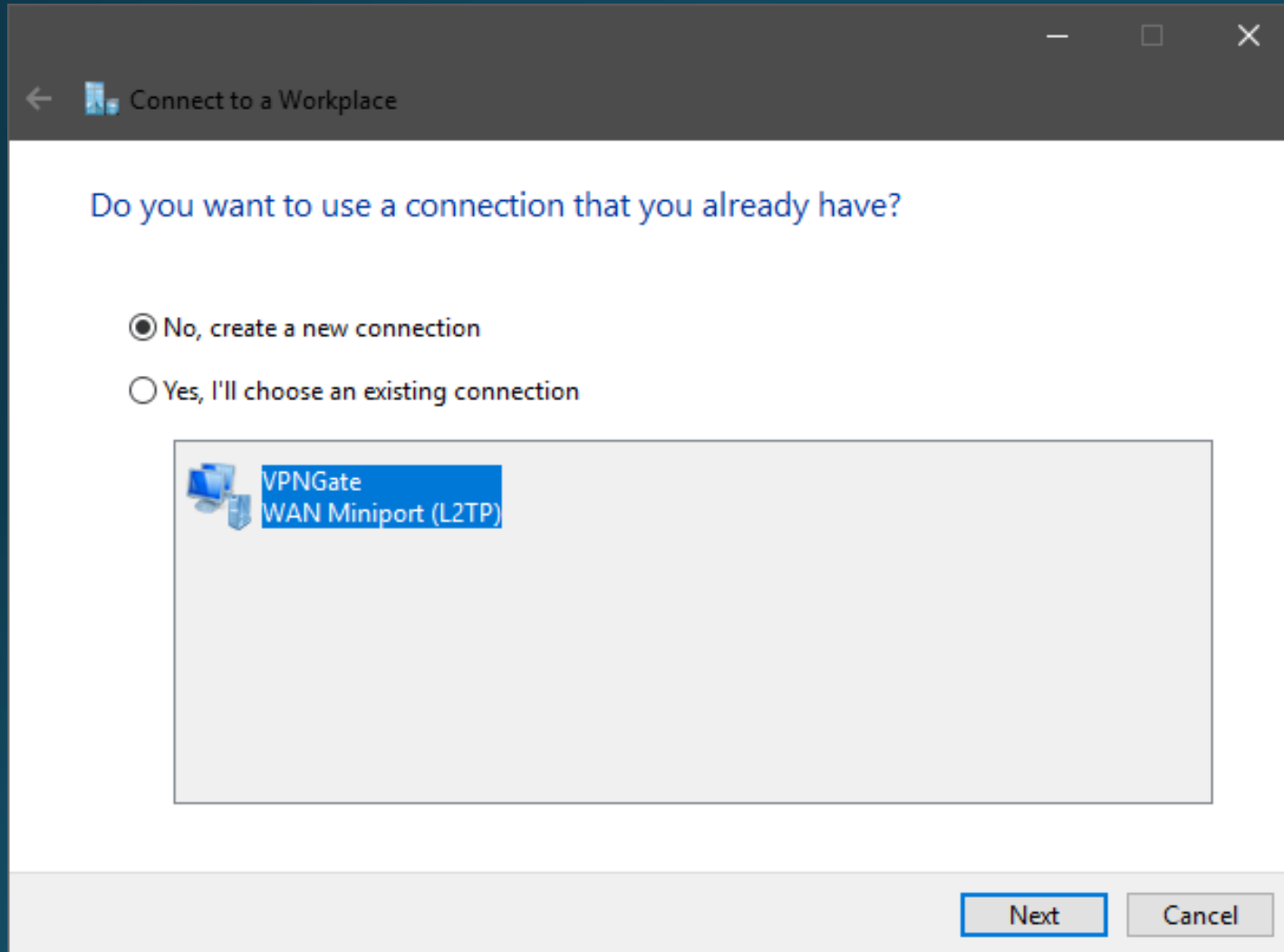
Lalu akan keluar window kecil

Cont'd



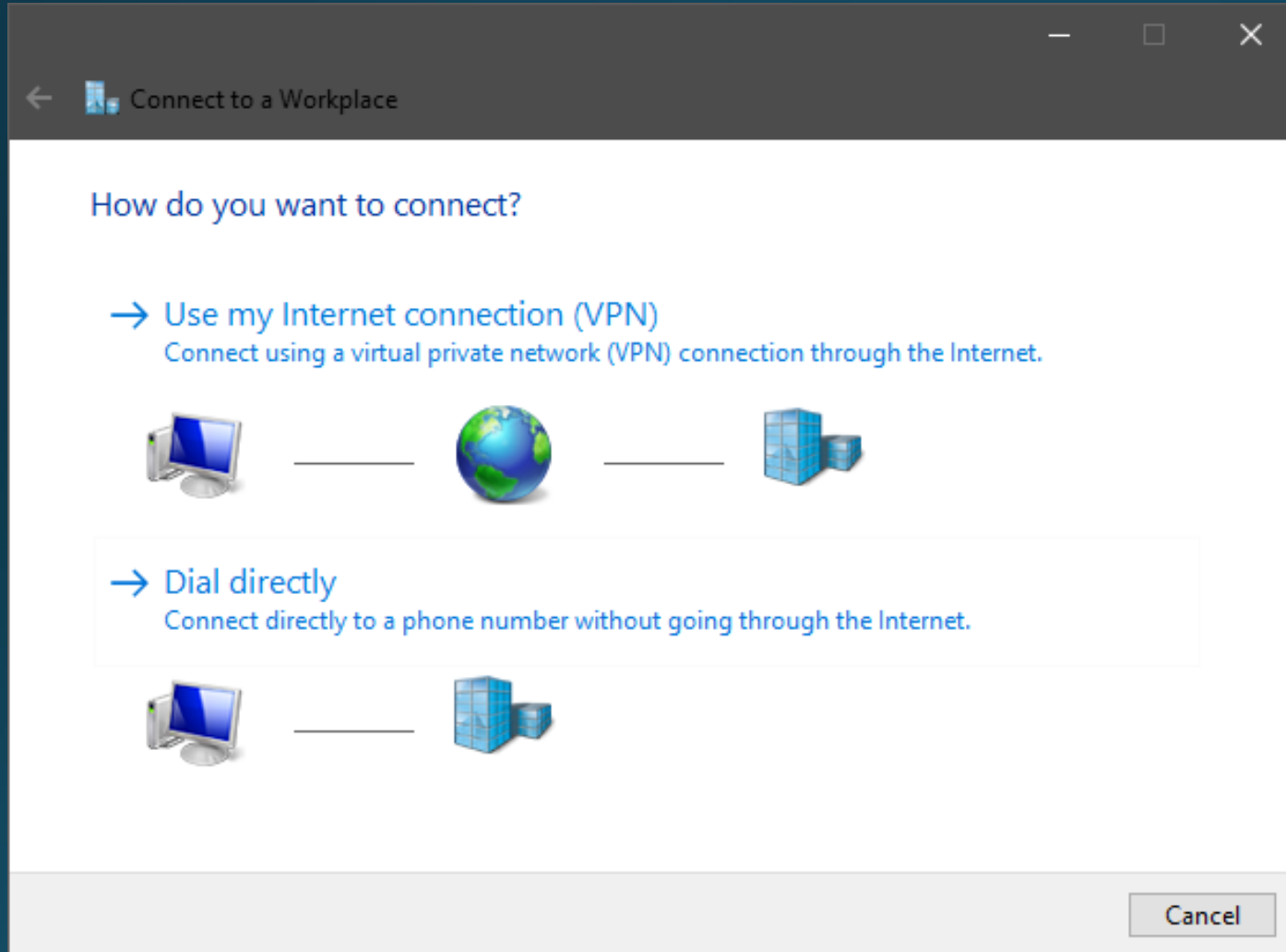
Pilih Connect to a workplace, lalu Next

Cont'd



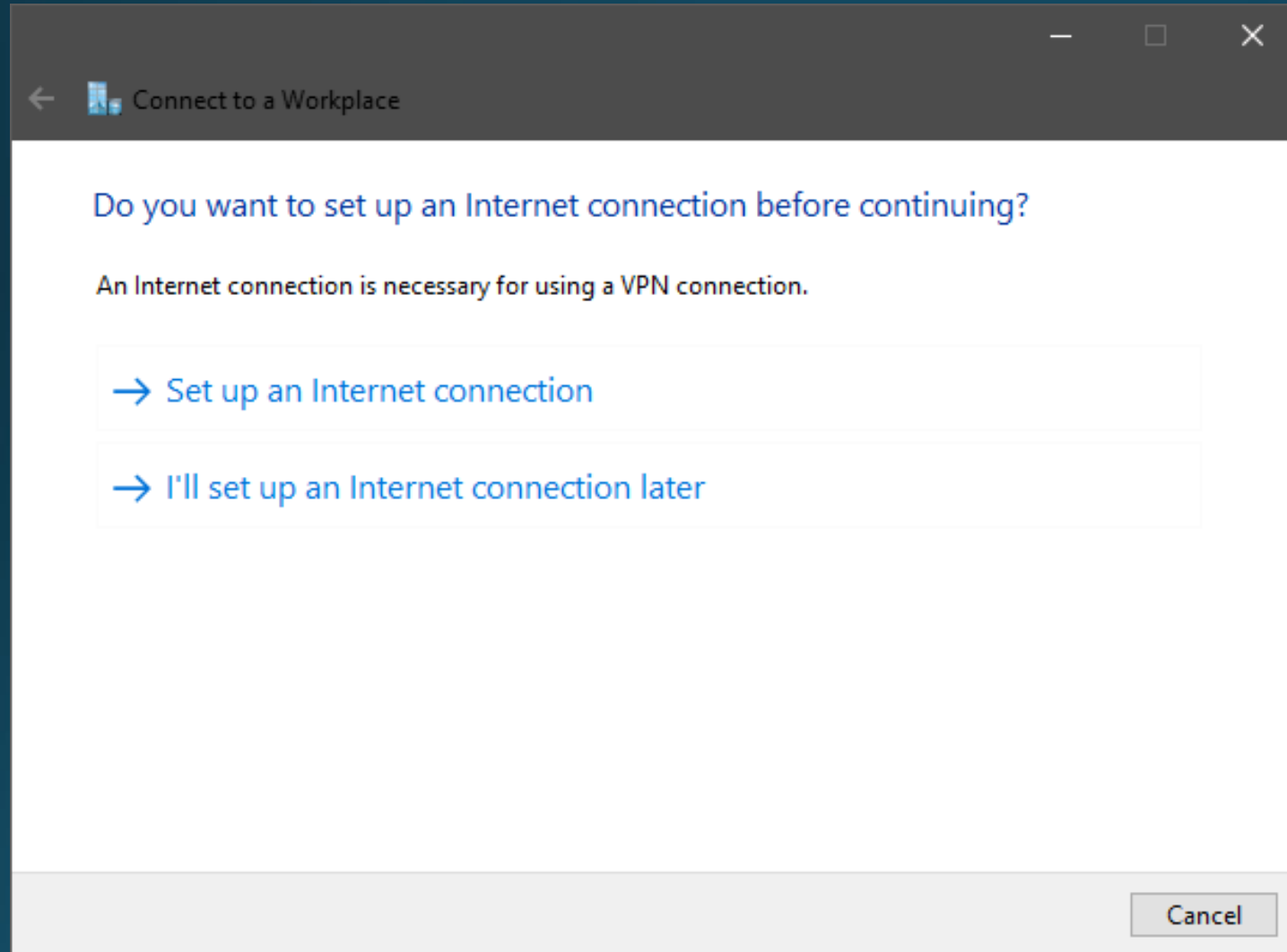
Lanjut klik Next

Cont'd



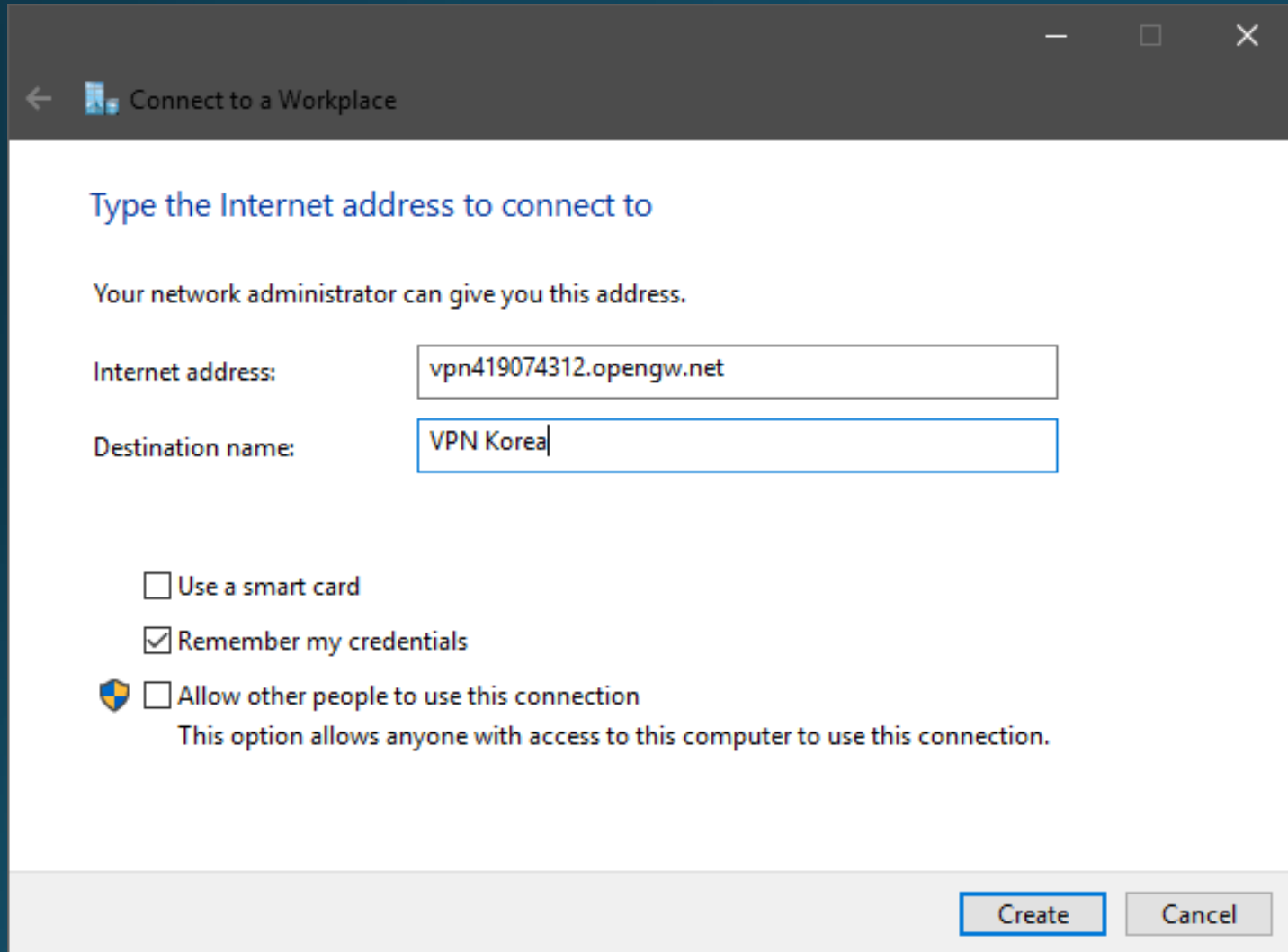
Klik "Use my Internet Connection (VPN)"


Cont'd



Pilih Set Up Internet
Connection Later

Cont'd



←  Connect to a Workplace

Type the Internet address to connect to


Your network administrator can give you this address.

Internet address:

Destination name:

☐ Use a smart card

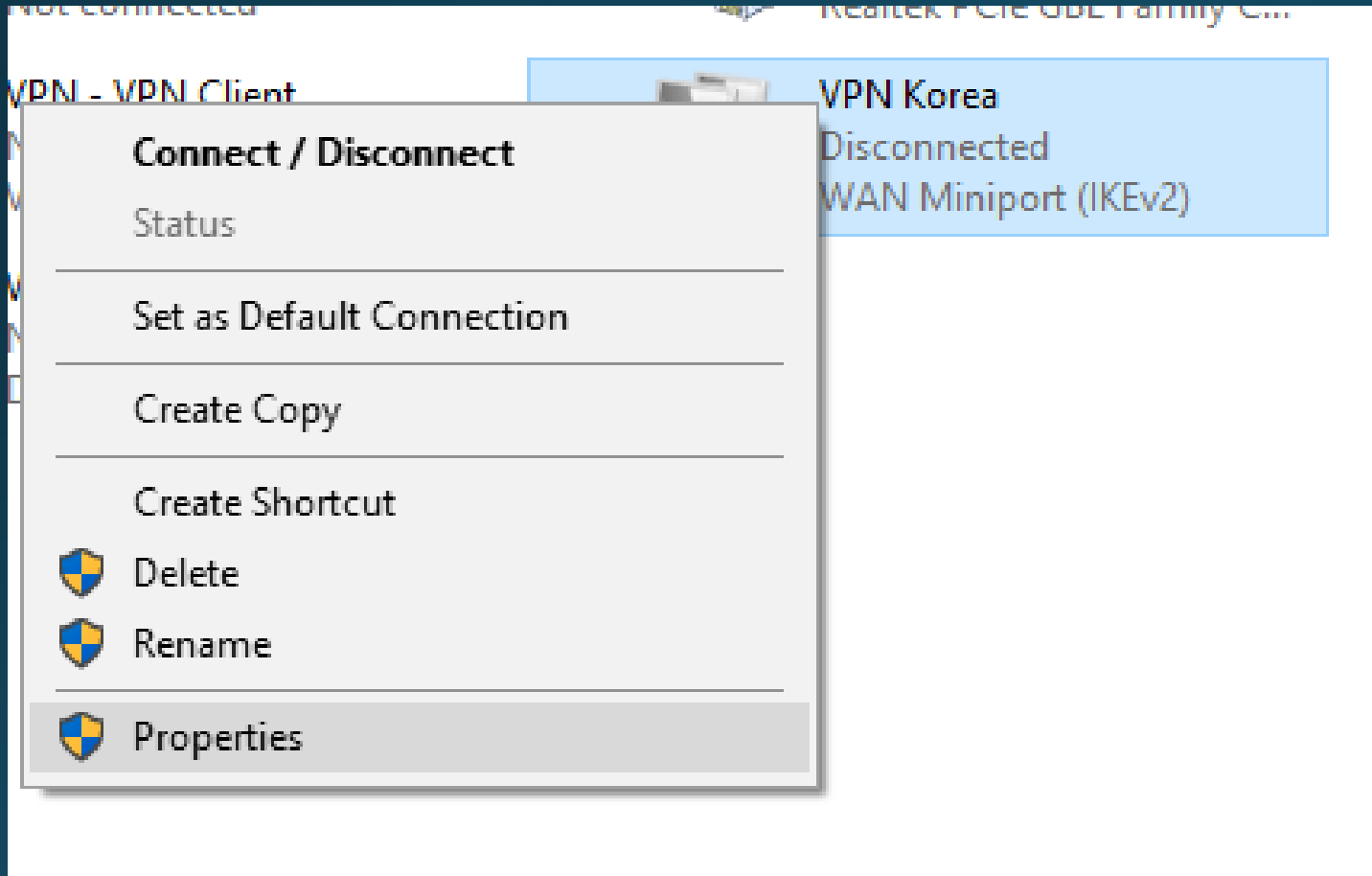
☒ Remember my credentials

 ☐ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

Isikan nama VPN/IP VPN di tempat kosongnya, serta berikan label VPN, lalu klik Create.

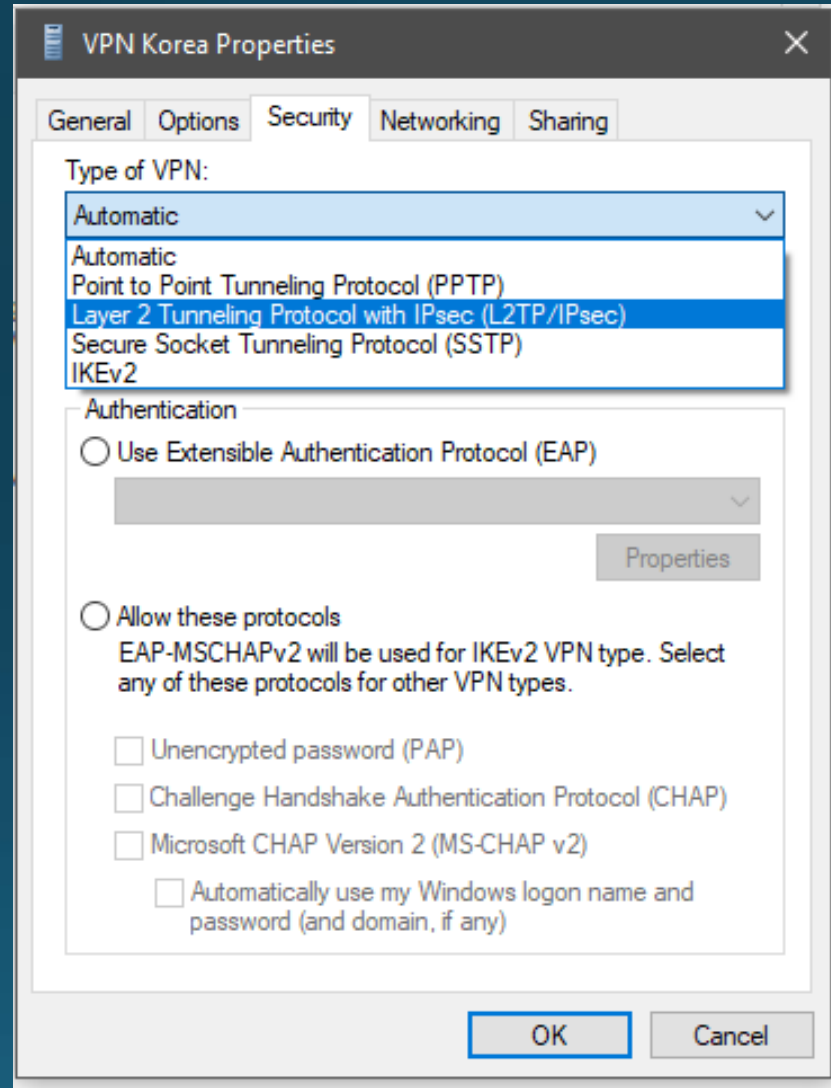
VPN sudah jadi tapi perlu dikonfigurasi

Cont'd



- Klik Change Adapter, untuk melihat daftar Adapter yang sudah dibuat. Klik kanan Adapter VPN korea lalu klik Properties

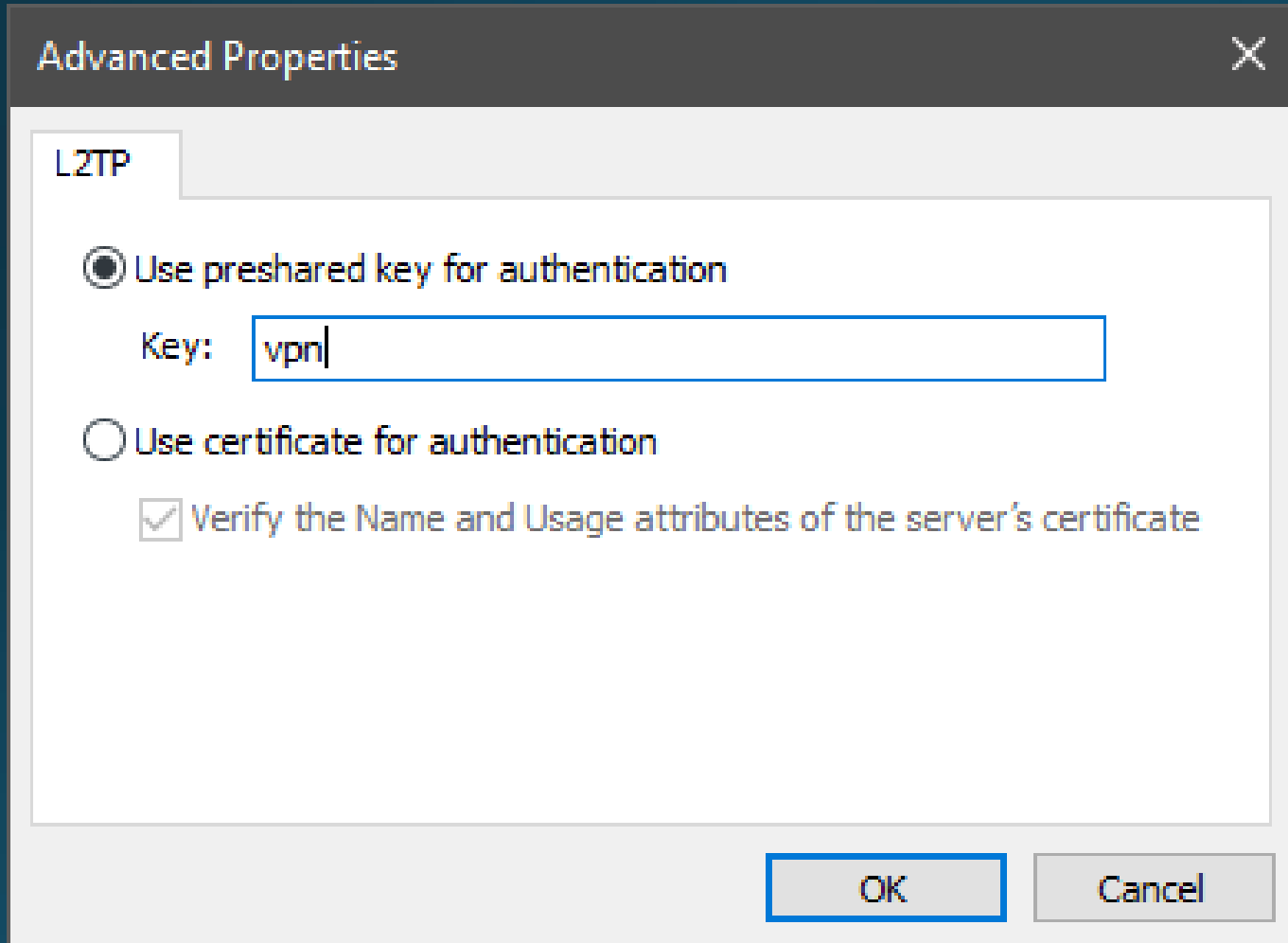
Cont'd



Pilih tab Security, lalu dari Automatic ganti ke Layer 2 Tunneling Protocol with IPsec.

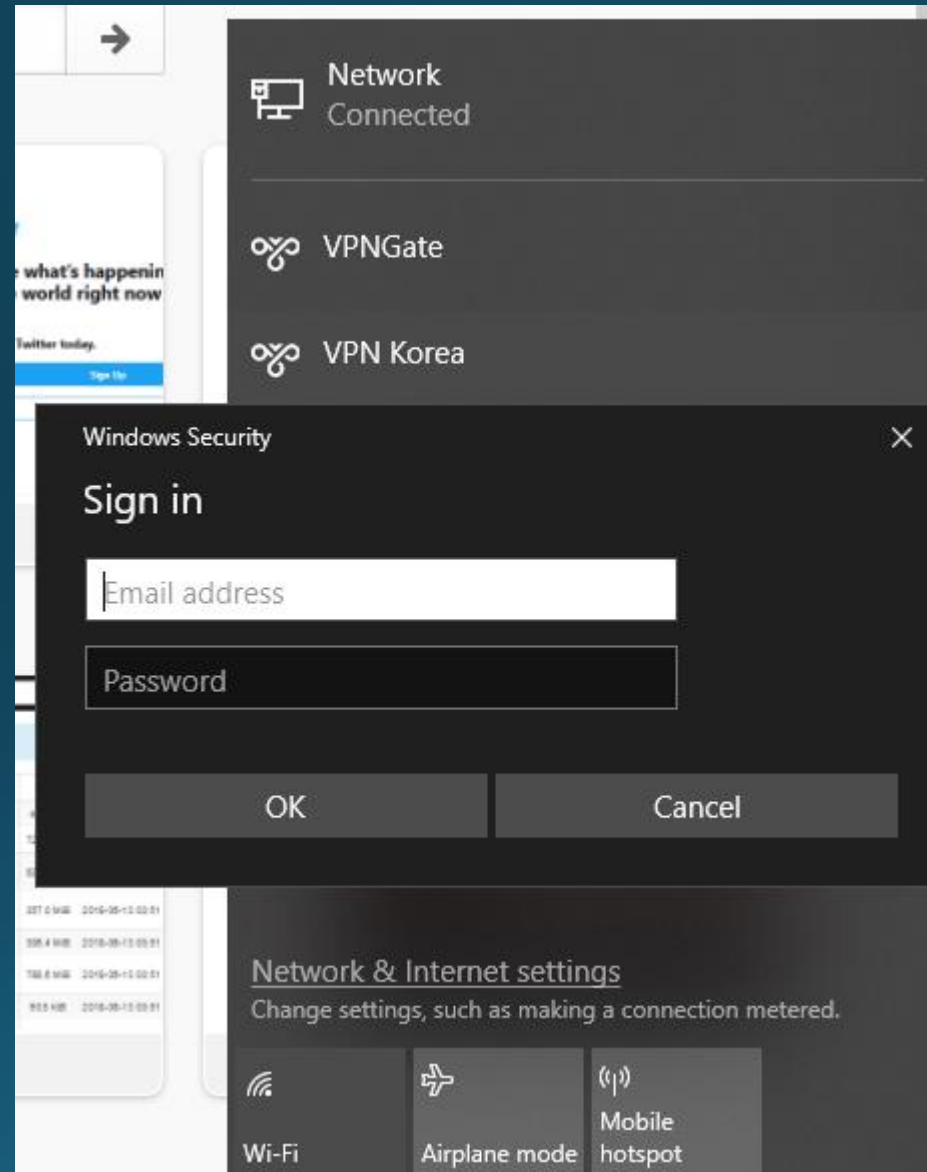
Lalu klik Advanced Settings untuk mengisi pre-shared key.

Cont'd



Klik Pre-shared Key,
lalu ketik "vpn"
tanpa petik. Lalu
klik OK

Cont'd



Untuk memulai koneksi, klik Network di Taskbar. Lalu klik VPN korea, lalu Connect. Akan muncul permintaan username dan password. Ketik vpn sebagai username dan password.

Cont'd

- Jika berhasil, maka ada tulisan Connected di sana
- Jika gagal, silahkan ganti IP server dengan IP lain