1. Modify the following statements to make them true.

A Virtual Private Network (VPN) is a (non-public / ~~public~~) (computer) network, built within (~~non-public~~ / public) network infrastructure, such as the Internet.
The term "encryption" means the security process for VPNs with the goal to ensure (confidentiality / ~~authentication~~) and data (integrity / ~~encrypting~~).

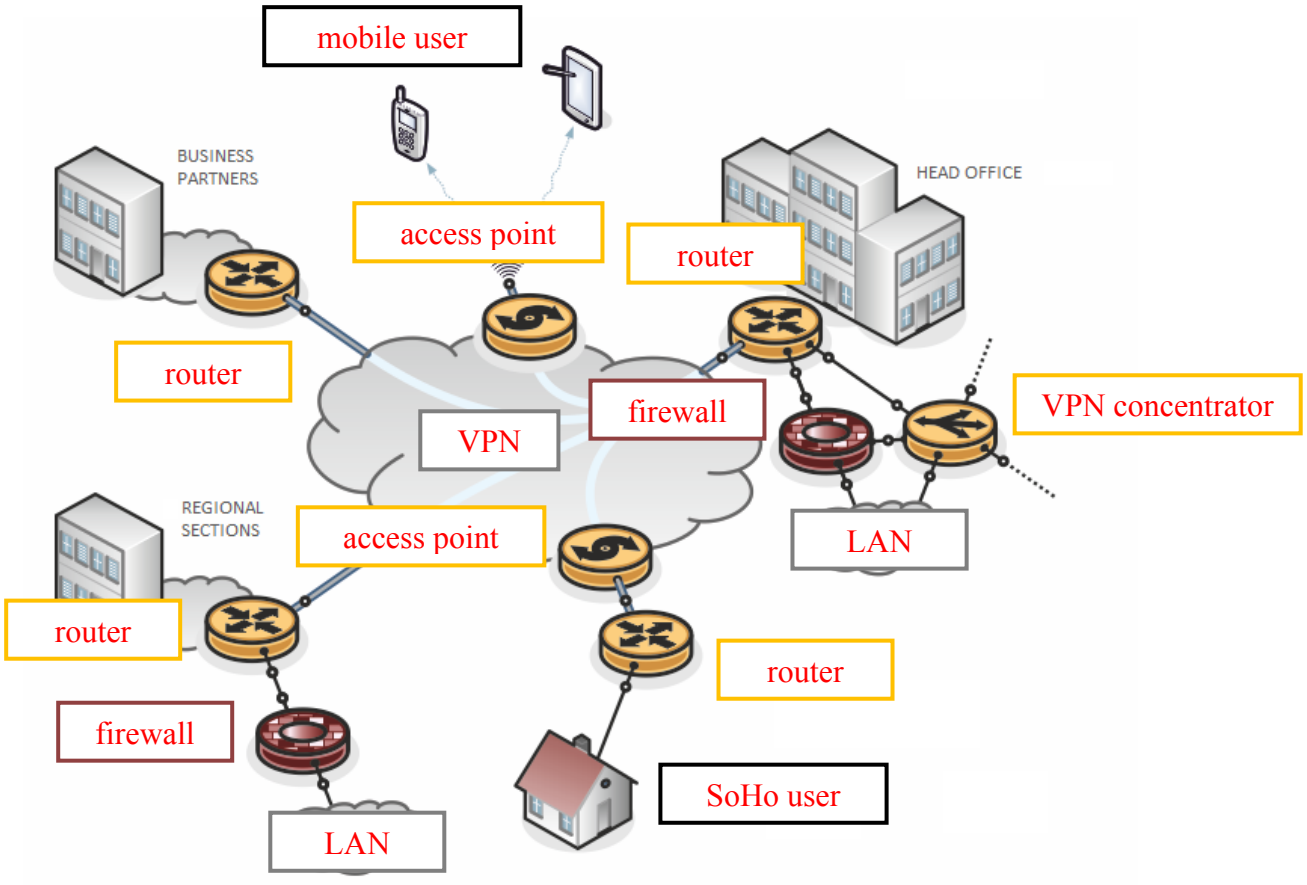
---

2. Requirements for security in terms of VPN design are solved by means of:

1. tunneling
2. encrypting
3. authentication
4. access control

---

3. Add the correct labels to their individual parts in the following figure:



Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

4. Choose the correct statements from the options below.

☐ IPSec is not a comprehensive set of protocols for encryption, authentication, data integrity, and tunneling.

X IPSec allows two working modes - transport and tunneling.

☐ The IKE protocol has two modes to set up the tunnel - main and simple mode.

X One advantage of aggressive mode is the bandwidth and time savings required for message transmission.

X One disadvantage of the aggressive mode is the exchange of important information before the encrypted connection is established, which is susceptible to interception, known as so-called Sniffing.

☐ Diffie-Hellman algorithm (D-H algorithm) is a cryptographic protocol that, however, does not allow for the creation of encrypted connections between the communicating parties over an unsecured channel; it is necessary to establish an encryption key in advance.

X A qualified electronic signature ensures legal acceptability of signed documents.

☐ An electronic signature is used exclusively by a legal person or a state organization; an electronic seal is exclusively used by a natural person.

---

5. Modify the following statements to make them true.

Qualified seal is based on (qualified / ~~guaranteed~~) electronic signature, it is its equivalent with regard to the area of its use (exclusively for a (legal / ~~natural~~) person).

---

6. An electronically signed timestamp structure includes, among others:

1. name of publisher
2. unique stamp serial number
3. checksum (HASH) derived from the document
4. time

Erasmus+
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.