

## 1. Upravte následující tvrzení tak, aby jejich znění byla pravdivá.

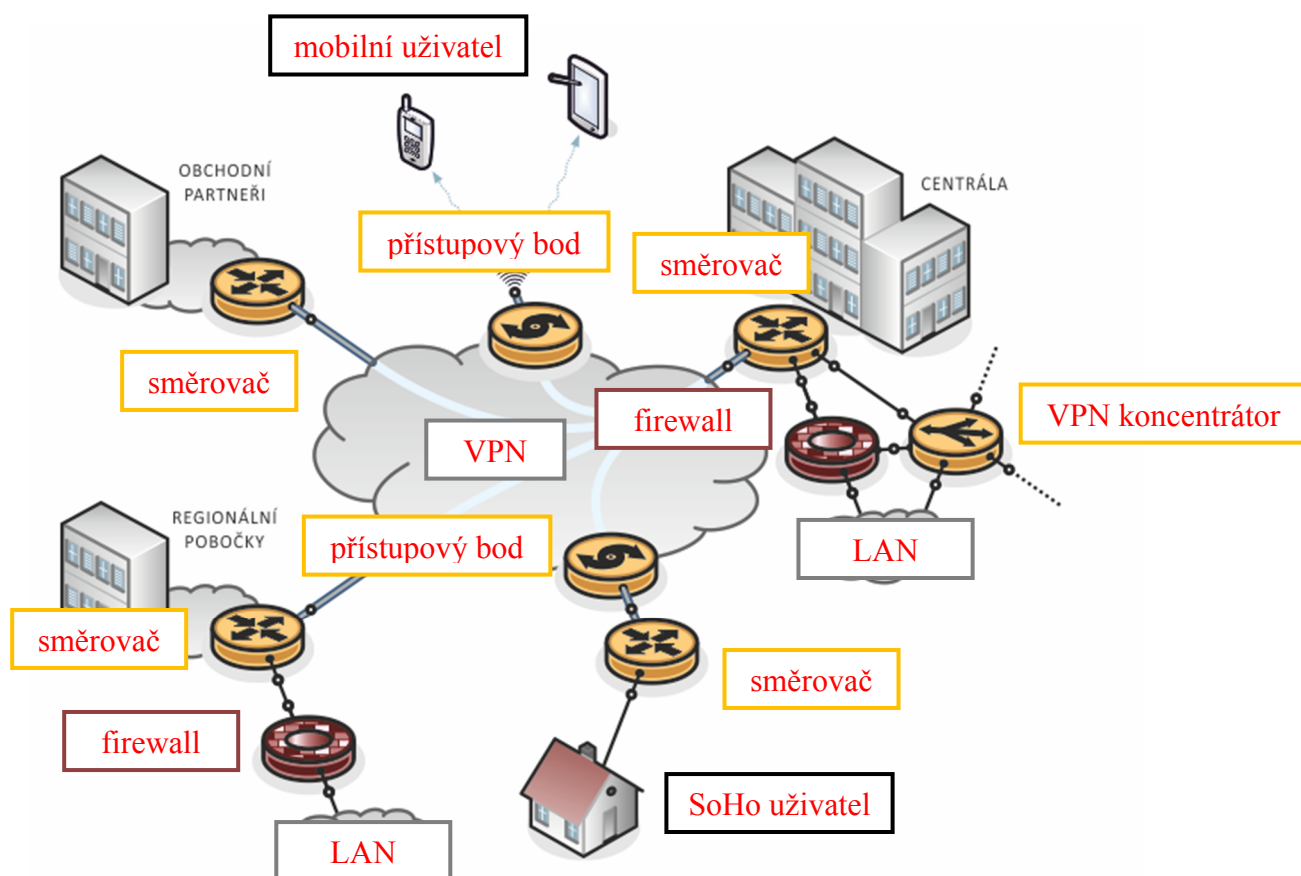
Virtuální privátní síť VPN je (neveřejná / veřejná) (počítačová) síť, vybudovaná v rámci (neveřejné / veřejné) síťové infrastruktury, jakou je např. Internet.

Pojmem šifrování rozumíme u sítí VPN proces pro zajištění (důvěrnosti / autentizace) i (integrity / šifrování) dat.

## 2. Požadavky na bezpečnost se z hlediska návrhu VPN řeší pomocí:

1. tunelování
2. šifrování
3. autentizace
4. řízení přístupu

## 3. Doplněte do následujícího obrázku správné popisky k jeho jednotlivým částem:



Erasmus+

Tento projekt byl realizován za finanční podpory Evropské unie.  
Za obsah publikací (sdělení) odpovídá výlučně autor. Publikace (sdělení) nereprezentují názory Evropské komise a Evropská komise neodpovídá za použití informací, jež jsou jejich obsahem.

#### 4. Vyberte z následujících možností správná tvrzení.

- ☐ Protokol IPSec není komplexním souborem protokolů řešící šifrování, autentizaci, integritu dat a proces tunelování.
- ☐ Protokol IPSec umožňuje dva pracovní režimy – transportní a tunelovací.
- ☐ Protokol IKE má k dispozici pro sestavení tunelu dva režimy – hlavní a jednoduchý režim.
- ☐ Výhodou agresivního režimu je úspora přenosového pásma a času nutných pro přenos zpráv.
- ☐ Nevýhodou agresivního režimu je výměna důležitých informací ještě před sestavením šifrovaného spojení, což je náchylné na odposlech, tzv. Sniffing.
- ☐ Diffie-Hellmanův algoritmus (D-H algoritmus) je kryptografický protokol, který však neumožňuje vytvořit mezi komunikujícími stranami šifrované spojení přes nezabezpečený kanál, je totiž nutné si nejprve dopředu dohodnout šifrovací klíč.
- ☐ Kvalifikovaný elektronický podpis zajišťuje právní akceptovatelnost podepsaných dokumentů.
- ☐ Elektronický podpis používá výhradně právnická osoba nebo organizační složkou státu, elektronická pečeť může být využita výlučně fyzickou osobou.

---

#### 5. Upravte následující tvrzení tak, aby jeho znění bylo pravdivé.

Kvalifikovaná pečeť je založena na (kvalifikovaném zaručeném) elektronickém podpisu, resp. je jeho ekvivalentem s ohledem na oblast jejího využití (výlučně pro (právníkové fyzické) osoby).

---

#### 6. Elektronicky podepsaná struktura časového razítka mimo jiné obsahuje:

1. jméno vydavatele
2. jedinečné sériové číslo razítka
3. kontrolní součet (tzv. HASH) odvozený z dokumentu
4. čas

