1. Upravte nasledujúce tvrdenia tak, aby ich znenie bolo pravdivé.

Virtuálna privátna sieť VPN je (neverejná / verejná) (počítačová) sieť vybudovaná v rámci (neverejnej / verejnej) sieťovej infraštruktúry, akou je napr. Internet.

Pod pojmom šifrovanie rozumieme v sieťach VPN proces pre zabezpečenie (dôvernosti / autentizácie) aj (integrity / šifrovania) dát.

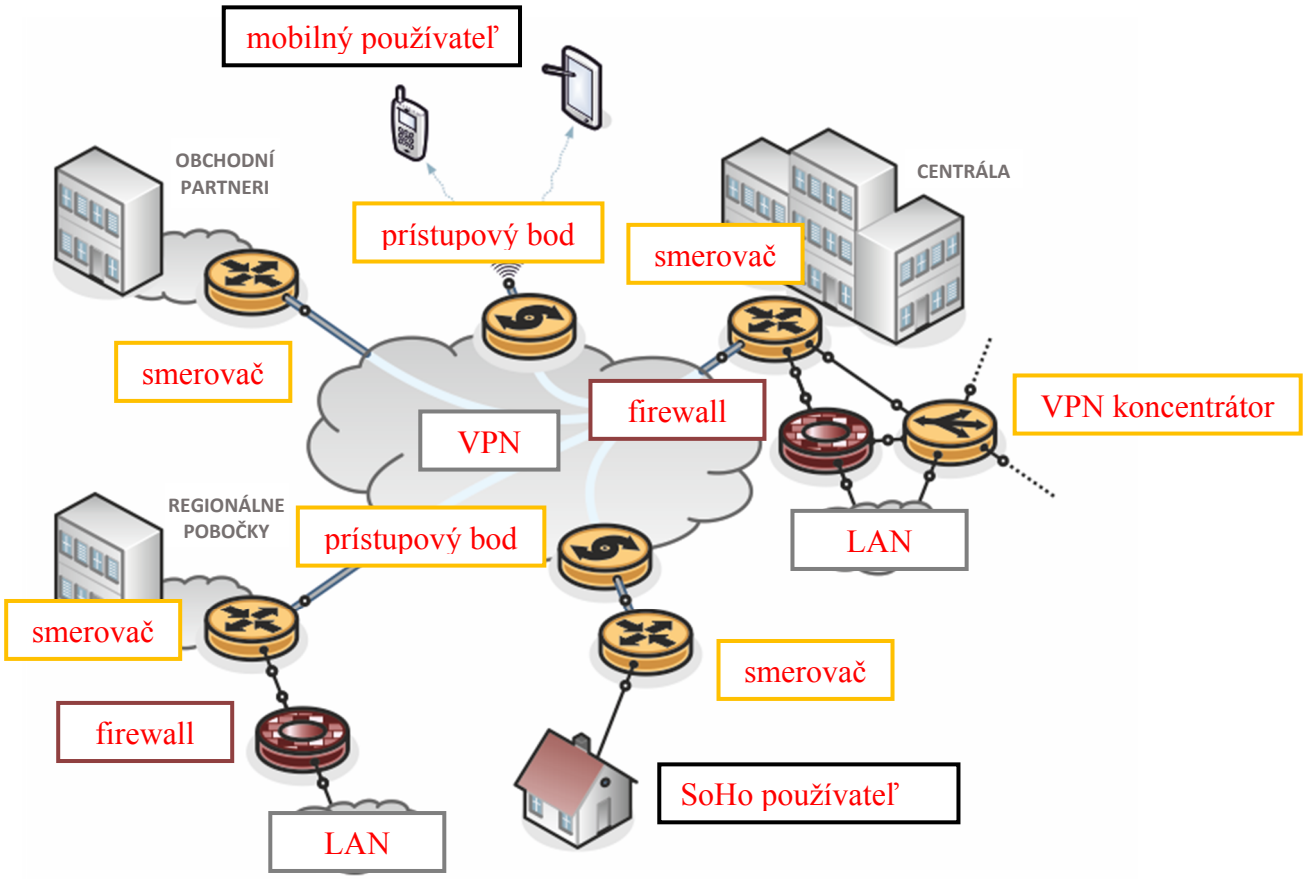
---

2. Požiadavky na bezpečnosť sa z hľadiska návrhu VPN riešia pomocou:

1. tunelovania
2. šifrovania
3. autentizácie
4. riadenia prístupu

---

3. Doplňte do nasledujúceho obrázku správne popisy k jeho jednotlivým častiam:



Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).

4. Vyberte správne tvrdenia z nasledujúcich možností.

- ☐ Protokol IPsec nie je komplexným súborom protokolov riešiacich šifrovanie, autentizáciu, integritu dát a proces tunelovania.
- ☐ Protokol IPsec umožňuje dva pracovné režimy – transportný a tunelovací.
- ☐ Protokol IKE má k dispozícii pre postavenie tunelu dva režimy – hlavný a jednoduchý režim.
- ☐ Výhodou agresívneho režimu je úspora prenosového pásma a času potrebného pre prenos správ.
- ☐ Nevýhodou agresívneho režimu je výmena dôležitých informácií ešte pred zostavením šifrovaného spojenia, čo je náchylné na odpočúvanie, tzv. Sniffing.
- ☐ Diffie-Hellmanov algoritmus (D-H algoritmus) je kryptografický protokol, ktorý ale neumožňuje vytvoriť medzi komunikujúcimi stranami šifrované spojenie cez nezabezpečený kanál, je totiž nutné si najskôr dopredu dohodnúť šifrovací kľúč.
- ☐ Kvalifikovaný elektronický podpis poskytuje právnu akceptovateľnosť podpísaných dokumentov.
- ☐ Elektronický podpis používa výhradne právnická osoba alebo organizačná zložka štátu, elektronická pečať môže byť využitá výlučne fyzickou osobou.

---

5. Upravte nasledujúce tvrdenia tak, aby ich znenie bolo pravdivé.

Kvalifikovaná pečať je založená na (kvalifikovanom / zaručenom) elektronickom podpise, resp. je jeho ekvivalentom s ohľadom na oblasť jej využitia (výlučne pre (právnické / fyzické) osoby).

---

6. Elektronicky podpísaná štruktúra časovej pečiatky okrem iného obsahuje:

1. meno vydavateľa
2. jedinečné sériové číslo pečiatky
3. kontrolný súčet (tzv. HASH) odvodený z dokumentu
4. čas

Erasmus+
Tento projekt bol financovaný s podporou Európskej Komisie.
Táto publikácia (dokument) reprezentuje výlučne názor autora a Komisia nezodpovedá za akékoľvek použitie informácií obsiahnutých v tejto publikácii (dokumente).