Előkészületek:

Szükségünk lesz egy Windows Server 2016 virtuális szerverre!

A következő feltételeknek megfelelő pillanatkép hiányában telepítsen egy új szervert:

RAM: *min*. ***1024 MB***, ***HDD***: ***50 GB***, ***gépnév: srv1-dc***, a ***tűzfal kikapcsolva*** a virtuális gépen és ***nincsenek szerepkörök telepítve***, ***1 db hálókártya*** (vagy *NetTeaming-el összevont 2 db hálókártya* (belső hálózat!), IP: 192.168.10.1 /24)!

Feladatok:

Telepítse az Active Directory működéséhez szükséges szerepkört és hozza létre egy új tartomány első tartományvezérlőjét az új erdőben *(a DNS kiszolgálót az Active Directory telepítse)*! A tartomány neve ***TESZT.LOCAL*** legyen!

Biztosítsa, hogy a szerver elérhető legyen a ***vpn.teszt.local*** néven is! (DNS: ***ALIAS*** rekord: ***vpn***)

Telepítse és konfigurálja a ***DHCP szerepkört*** a kiszolgálóra! A hálózat számítógépei ***DHCP*** szervertől kapják meg a hálózati beállítás paramétereit! A kliens munkaállomás a DHCP kiszolgálótól kapjon automatikusan IP-címet!

A VPN kapcsolathoz telepítse fel és konfigurálja a távelérést biztosító szerepkör-szolgáltatást a szerverre!

A klienseknek az IP-címet -*VPN kapcsolaton keresztüli eléréskor is*- a **DHCP**-kiszolgáló biztosítsa!

- A VPN kapcsolatok engedélyezéséhez a hálózati házirend-kiszolgálón a megfelelő hálózati házirend szabályokat hozza létre! Hozzon létre egy ***Távelérés*** nevű szervezeti egységet, ebben vegyen fel egy ***PPTP*** nevű szervezeti egységet melynek legyen tagja egy ***vpn1*** nevű felhasználó! A felhasználónak engedélyezze a VPN kapcsolat használatát ***hálózati házirendben*** előírt szabály alapján, a szabály neve legyen ***Távelérés-PPTP***!

  Biztosítsa, hogy a felhasználó gépén -bejelentkezéskor- ***automatikusan*** létrejöjjön a VPN kapcsolat! (Az új kapcsolat neve legyen: ***VPN-PPTP***)

  A kapcsolat létrejöttét ellenőrizze a kliens gépen, tesztelésképpen **vpn*1*** felhasználó nevében lépjen be a kliens gépen és kapcsolódjon a VPN kiszolgálóhoz! A létrejött kapcsolat *állapot/részleteket* igazoló ablakot mentse el, ***pptp.jpg*** néven!

Hitelesítési módszer	*lehet* ***EAP-MSCHAPv2*** *vagy* ***MS-CHAPv2***
Alagút protokoll	***PPTP***
Felhasználó korlátozás	***csak a szervezeti egységgel egyező nevű csoport tagjai (pptp)***
Időkorlátozás	***hétköznap 6-22 óra között***

- A ***Távelérés*** nevű szervezeti egységben hozzon létre egy ***L2TP*** nevű szervezeti egységet, melynek legyen tagja egy ***vpn2*** nevű felhasználó! A felhasználónak engedélyezze a VPN kapcsolat használatát ***hálózati házirendben*** előírt szabály alapján, az új szabály neve legyen: ***Távelérés-L2TP***!

  A kapcsolat teszteléséhez kapcsolódjon a kliens gépről a VPN kiszolgálóhoz ***vpn2*** felhasználó nevében! (Az új kapcsolat neve: ***VPN-L2TP***)

  A létrejött kapcsolat *állapot/részleteket* igazoló ablakot mentse el, ***l2tp.jpg*** néven!

Hitelesítési módszer	***csak EAP-MSCHAPv2***
Alagút protokoll	***csak L2TP használatával, előre megosztott kulccsal***
Előmegosztott kulcs	***Qwe123***
Felhasználó korlátozás	***csak a szervezeti egységgel egyező nevű csoport tagjai (l2tp)***
Időkorlátozás	***a hét minden napján***

Szervezeti felépítés:

- **Távelérés** *OU*
  - **PPTP** *OU*
    - **pptp** *csoport*
      - **vpn1** *felhasználó*
  - **L2TP** **OU**
    - **l2tp** **csoport**
      - **vpn2** **felhasználó**