

1. sz. melléklet

DEBRECENI SZAKKÉPZÉSI CENTRUM BRASSAI SÁMUEL



MŰSZAKI TECHNIKUM

4029 Debrecen, Víztorony u. 3.

OM: 203033/099



PROJEKTMUNKA DOKUMENTÁCIÓ

Kozma Csaba, Motocz Edward Alexander - 13/B

Az ágazat megnevezése: **Informatikai rendszer- és alkalmazás-üzemeltető
technikus** szakma megnevezése: **Informatika és távközlés**
A szakma azonosító száma: **5 0612 12 02**

Debrecen

2025

Tartalomjegyzék

Cégbemutató	3
Telephelyek bemutatása	5
Telephelyek eszközeinek listája	8
Alkalmazott technológiák	9
Címzési terv és táblázat	12
Hálózati infrastruktúra	14
Szerverek konfigurációja	24
Tesztelés és dokumentáció	48
Feladatmegosztás	50
Összegzés	51
Irodalmi jegyzék	52
Eszközbe írt konfigurációk	53
Nyilatkozatok és melléletek	65

Dokumentáció a Vállalati Hálózatról

Ez a dokumentáció bemutatja egy komplex vállalati hálózat tervezését, implementálását és tesztelését. A projekt célja egy olyan működő prototípus kialakítása, amely megfelel az előírt követelményeknek, és a valós hálózati infrastruktúra alapelveit tükrözi.

Cégbemutató

Cég neve:

NetSys Solutions Kft.

Székhely:

Budapest, Magyarország

Telephelyek:

- Központi iroda – Budapest
- Regionális iroda 1 – Debrecen
- Regionális iroda 2 – Szeged

Cég profilja:

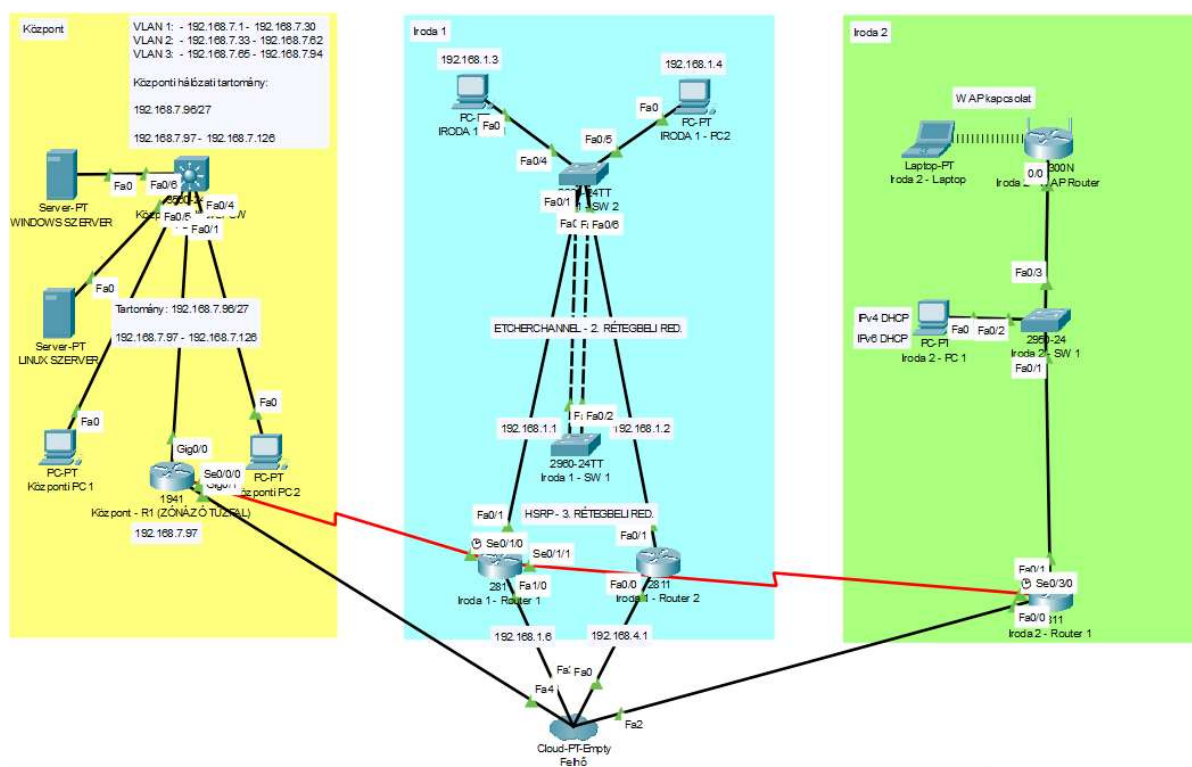
A NetSys Solutions Kft. egy informatikai szolgáltatásokat nyújtó vállalat, amely elsősorban kis- és középvállalkozásoknak kínál IT megoldásokat. A cég fő tevékenységi körei közé tartozik:

- Hálózati rendszerek tervezése és kivitelezése
- Szerverüzemeltetés (Linux, Windows)
- Felhőalapú szolgáltatások bevezetése és üzemeltetése
- IT biztonsági rendszerek kiépítése
- Távfelügyeleti és karbantartási szolgáltatások biztosítása

A projekt célja egy korszerű, biztonságos és skálázható vállalati hálózat megtervezése és megvalósítása, amely megfelel a NetSys Solutions Kft. jelenlegi és jövőbeli igényeinek.

A rendszernek biztosítania kell:

- Megbízható hálózati infrastruktúrát
- Magas szintű biztonságot (tűzfal, ACL, VPN)
- Központi menedzsmentet és felügyeletet
- Hatékony adatkezelést és biztonsági mentéseket



1. ábra – A vizsgaremek projektünk hálózati topológiája a Cisco Packet Tracer alkalmazásban

Telephelyek bemutatása

1. Központi Iroda – Budapest

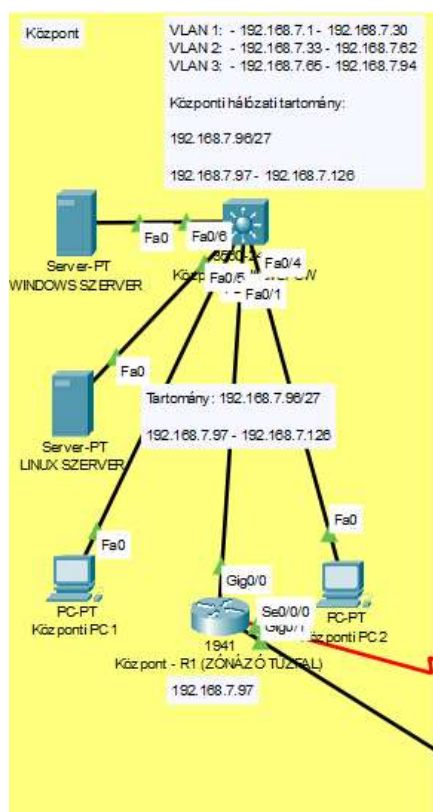
- Ez a vállalat elsődleges székhelye, ahol az itt tartózkodó Admin, vezetőségi, valamint IT-infrastruktúra menedzsment feladatokat látják el.

- Ez a telephely a legnagyobb forgalmat bonyolítja le, és itt helyezkednek el a kulcsfontosságú szerverek és központi hálózati eszközök.

- A központi iroda biztosítja a hálózat gerincét, valamint innen történik a rendszerfelügyelet és a szolgáltatások koordinálása.

- Hálózati infrastruktúra:

- Windows és Linux szerverek
- Hardveres tűzfal és ACL szabályok alkalmazása
- VPN szerver a távoli irodák kapcsolatához



2. ábra – Központi telephely



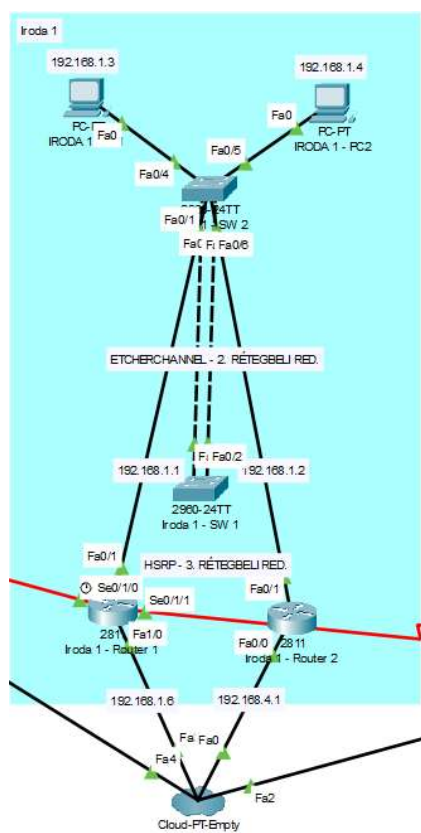
3. ábra – Központi telephely valós eszközökön megvalósítása

2. Iroda 1 – Debrecen

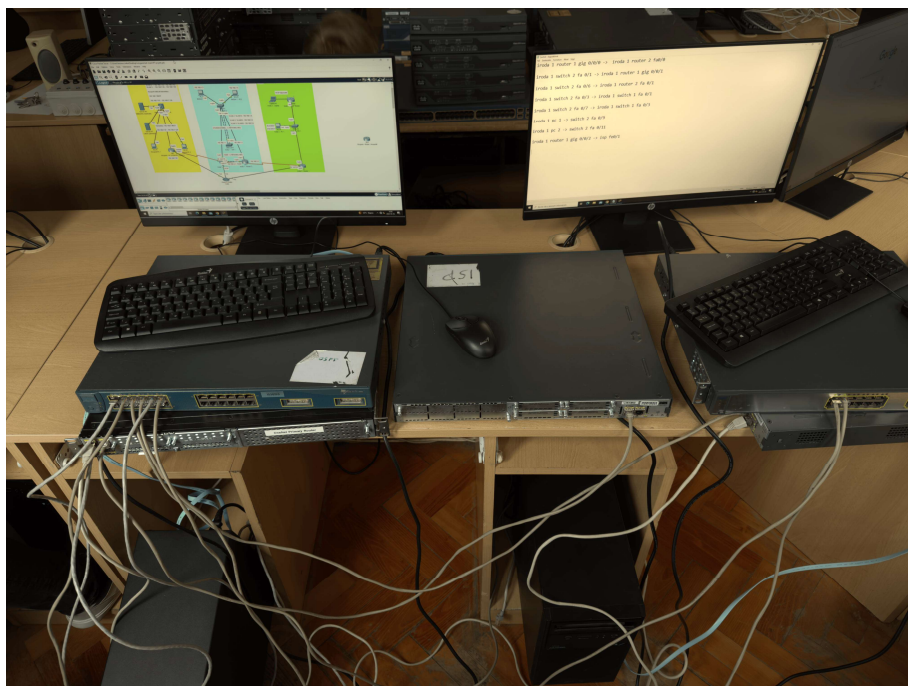
- Debreceni telephelyünk a keleti régió egyik kulcsfontosságú pontján található.
- Ez az iroda az ügyfélszolgálati és értékesítési részlegek, valamint egy kisebb fejlesztői csapat otthona.
- A helyi hálózat redundáns eszközökkel van kialakítva, biztosítva a folyamatos működést és a zökkenőmentes adatkapcsolatot a központi rendszerrel.

Hálózati infrastruktúra:

- Redundáns kapcsolatok és eszközök (EtherChannel – LACP protokoll, HSRP)
- OSPF protokoll a WAN kapcsolat miatt
- VPN kapcsolat a központtal



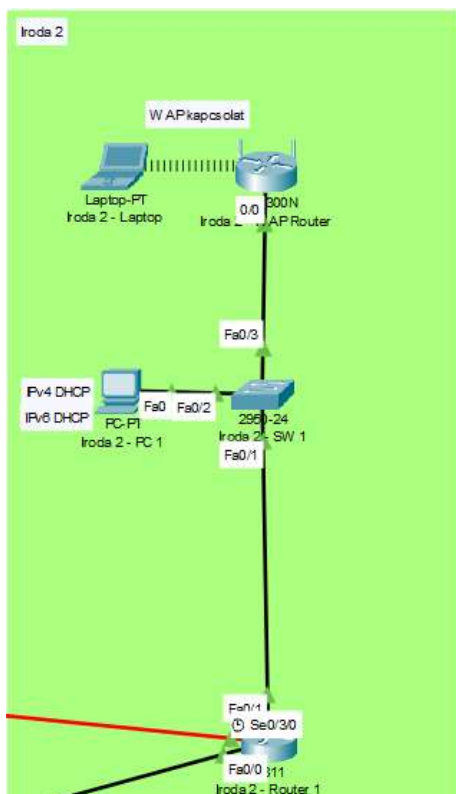
4. ábra – PT topológia az Iroda 1-ről



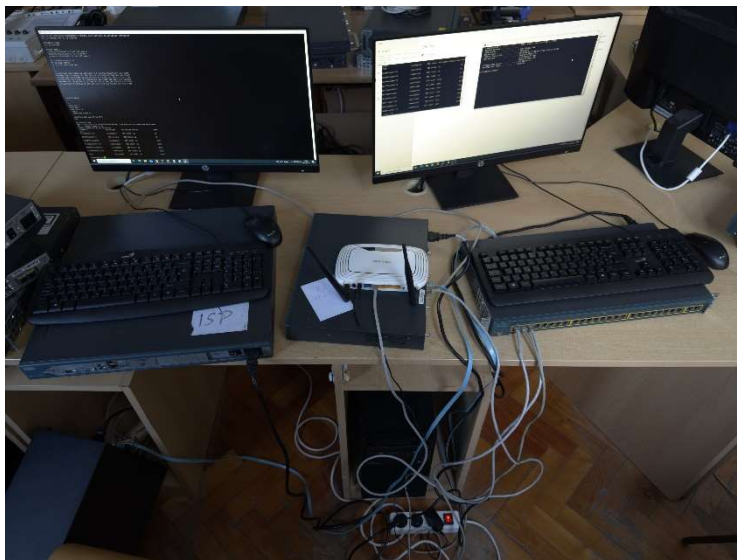
5. ábra – Az Iroda 1 valós eszközön megvalósítása

Iroda 2 - Szeged

- A szegedi telephely a vállalat nyugat-délkeleti régióját szolgálja ki, és elsősorban az ügyfélkapcsolatok és a helyszíni támogatás központjaként funkcionál.
- Ez az iroda kisebb, de fontos része a cég hálózatának, itt is kiépítésre került a megfelelő szintű hálózati infrastruktúra, amely biztosítja az összeköttetést a központi rendszerrel.
- Hálózati infrastruktúra:
 - Egyszerűbb VLAN struktúra (irodai, vendég)
 - Vezetékes és vezeték nélküli hálózat (Wi-Fi router és AP)
 - IPv4 és IPv6 címezés
 - VPN kapcsolat a központi telephelyhez
 - DHCP kiosztás helyben



6. ábra – PT topológia az Iroda 2-ről



7. ábra – Az Iroda 2 valós eszközökön megvalósítása

Telephelyek eszközeinek listája

Központi Iroda eszközeinek listája:

- 2db PC
- Router: 1db 2851 - A nagyobb teljesítmény és a több interfész támogatása miatt választottuk. Alkalmas nagy forgalom kezelésére, valamint VPN kapcsolatok létrehozására.
- Switch:
 - ME3400 1db - Metro Ethernet switch, amely vállalati szintű forgalomkezelést és biztonságos VLAN támogatást biztosít.

Iroda 1 eszközeinek listája:

- 2db 2960 switch - Gigabites portokkal rendelkező switch, amely gyors és stabil kapcsolatot nyújt a helyi hálózat számára.
- 2db 2811 router - Kisebb irodai hálózatokhoz ideális, megfelelő teljesítményt és bővíthetőséget biztosít a stabil működés érdekében.
- 2db PC

Iroda 2 eszközeinek listája:

- 1db wifi router - Vezeték nélküli hálózat biztosítására a mobil eszközök számára.
- 1db 2811 router
- 1db 2950 switch - Megbízható Layer 2 switch, amely biztosítja a szükséges hálózati kapcsolódást az eszközök számára.
- 1db telefon
- 1db PC

Alkalmazott technológiák

A hálózati infrastruktúránk három telephelyet foglal magában: a központi iroda, valamint az Iroda 1 és Iroda 2. Az infrastruktúra tervezése során a redundancia, a biztonság és a skálázhatóság kiemelt szempontok voltak. Az alábbi technológiákat alkalmaztuk a hálózat kiépítése során:

Hálózati réteg és forgalomirányítás

- **Statikus és dinamikus útvonalválasztás:** A központi router támogatja mind statikus útvonalak konfigurálását, mind pedig dinamikus forgalomirányítási protokollokat (pl. OSPF, EIGRP) a hatékony útvonalválasztás érdekében.

```
Iroda-1-R1(config)#do sh ip ospf interface

FastEthernet0/1 is up, line protocol is up
  Internet address is 192.168.1.2/24, Area 0
  Process ID 1, Router ID 192.168.20.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.20.1, Interface address 192.168.1.2
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:03
  Index 1/1, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
    Suppress hello for 0 neighbor(s)
Serial10/1/1 is up, line protocol is up
  Internet address is 192.168.20.1/30, Area 0
  Process ID 1, Router ID 192.168.20.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.20.2
    Suppress hello for 0 neighbor(s)
Serial10/1/0 is up, line protocol is up
  Internet address is 192.168.10.2/30, Area 0
  Process ID 1, Router ID 192.168.20.1, Network Type POINT-TO-POINT, Cost: 64
  Transmit Delay is 1 sec, State POINT-TO-POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:09
  Index 3/3, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 0 msec
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.10.1
    Suppress hello for 0 neighbor(s)
```

8. ábra OSPF az Iroda 1 Router 1-ben

- **IPv4 és IPv6 címzés:** A hálózat mindkét címzési rendszert támogatja, biztosítva ezzel a jövőbeli kompatibilitást.
- **NAT/PAT:** A központi telephelyen implementáltuk a NAT és PAT technológiákat a belső hálózat és az internet közötti címfordítás céljából.

- **WAN-összeköttetések:** A telephelyek közötti kapcsolatot megbízható WAN-kapcsolatok biztosítják.
- **VPN:** Virtuális magánhálózatot valósítottunk meg a biztonságos távoli hozzáférés és telephelyek közötti titkosított kommunikáció érdekében.

Hálózati redundancia és teljesítménynövelés

- **HSRP (Hot Standby Router Protocol):** Az Iroda 1 területén két router között implementáltuk az elsődleges és tartalék router kialakítására, ezzel biztosítva a magas rendelkezésre állást.
- **EtherChannel:** Az Iroda 1-ben található két switch közötti redundáns kapcsolat biztosítására EtherChannel technológiát alkalmaztunk.
- **VLAN szegmentáció:** A központi telephelyen több VLAN-t hoztunk létre, elkülönítve az egyes részlegek hálózati forgalmát és növelve a biztonságot.
- **ACL-ek:** A forgalomirányító eszközökön és a tűzfalon hozzáférési listákat konfiguráltunk a biztonsági házirendek betartásának érdekében.

Biztonsági megoldások

- **Tűzfal és zónázás:** A központi router egyben egy zónázó tűzfallal is konfigurált, amely szabályozza a be- és kimenő forgalmat.

Vezeték nélküli hálózat

- **WLAN:** Az Iroda 2 területén egy vezeték nélküli hálózatot is üzemeltetünk a mobil eszközök és vendéghozzáférések biztosítására.

Szerver infrastruktúra

A központi irodában két szerver üzemel, egy Linux és egy Windows alapú rendszer, melyek az alábbi szolgáltatásokat biztosítják:

- **Windows szerver:**
 - Active Directory címtárszolgáltatás
 - Kliens számítógépekre automatizált szoftvertelepítés
 - Fájl- és nyomtatómegosztás
 - DHCP szerver
 - DNS kiszolgáló
- **Linux szerver:**
 - HTTP/HTTPS webkiszolgálás
 - Automatizált mentési szolgáltatás

Automatizált konfiguráció

- **Programozott hálózatkezelés:** A hálózat konfigurációját automatizált scriptekkel és eszközökkel (Python) menedzseljük.
- **Megvalósítás:** Az általunk benyújtott videó alapján a script pythonban lett írva, bejelentkezik a megadott felhasználói adatokkal a routerbe és kilistáztatja nekünk az interfészeket, a kiosztott ip-ket, és a vlan struktúrát, a könnyebb átláthatóság jegyében.

Címzési terv

Központi iroda - Budapest		
Eszköz	ipv4 cím	ipv4 maszk
Windows Szerver	192.168.7.100	/27
Linux Szerver	192.168.7.101	/27
ME switch VLAN10	192.168.7.1	/27
ME switch VLAN 20	192.168.7.33	/27
ME switch VLAN 30	192.168.7.65	/27
Router 1	192.168.7.97	/27
PC 1	192.168.7.123	/27
PC 2	192.168.7.124	/24

Iroda 1 - Debrecen		
Eszköz	ipv4 cím	ipv4 maszk
PC 1	192.168.1.3	/24
PC 2	192.168.1.4	/24
Router 2 fa 0/0 (ISP felé)	192.168.1.5	/24
Router 2 fa 0/1 (SW2 felé)	192.168.1.2	/24
Router 1 fa0/1 (SW2 felé)	192.168.1.1	/24
Router 1 fa0/0 (ISP felé)	192.168.1.6	/24

Iroda 2 - Szeged			
Eszköz	ipv4 cím	ipv4 maszk	ipv6 cím
Router	192.168.4.1	/24	2001:db8:4::1/64

PC	192.168.4.2	/24	2001:db8:4:0:202:4AFF:FE7E:2895/64
W AP	192.168.4.3	/24	
Laptop	192.168.4.4	/24	

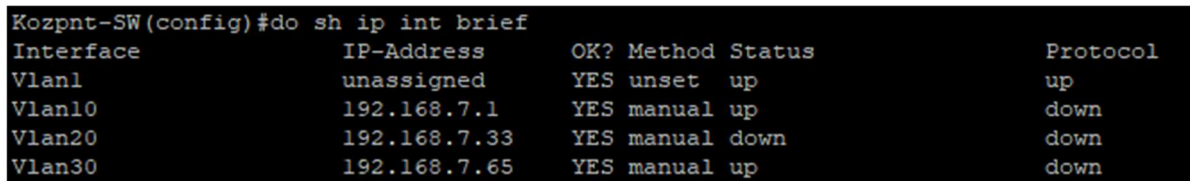
Hálózati Infrastruktúra Tervezése

1. Telephelyek

- Telephelyek száma: 3
- Főbb elemek:
 - Központ
 - Iroda 1
 - Iroda 2

2. VLAN Struktúra

- Az Központ nevű telephelyen 3 VLAN kerül kialakításra.
 - VLAN1: 192.168.7.1 – 192.168.7.30
 - VLAN2: 192.168.7.33 – 192.168.7.62
 - VLAN3: 192.168.7.65 – 192.168.7.94



Interface	IP-Address	OK?	Method	Status	Protocol
Vlan1	unassigned	YES	unset	up	up
Vlan10	192.168.7.1	YES	manual	up	down
Vlan20	192.168.7.33	YES	manual	down	down
Vlan30	192.168.7.65	YES	manual	up	down

9. ábra – Valós eszközön létrehozott virtuális LAN-ok a Központi telephelyen

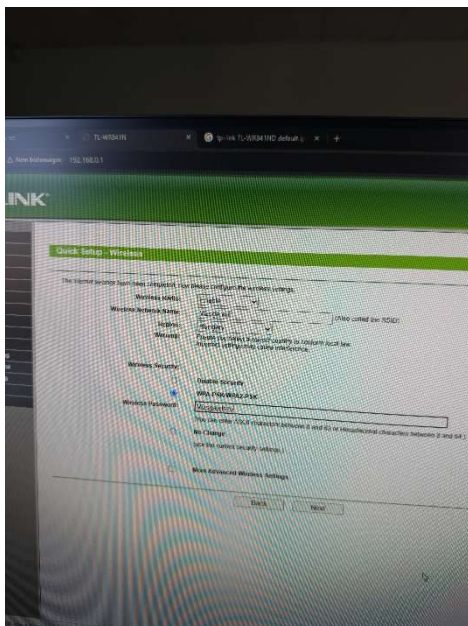
3. IPv4 és IPv6 címzési terv

- IPv4:
 - Privát címeket használunk
 - A Központi irodában a hálózati cím 192.168.7.0/27
 - A routerből az ISP felé történő kommunikáció külön hálózaton történik, a 192.168.6.0/24 hálózati címen.

- Az Iroda 1 három alhálózattal rendelkezik, mind különböző hálózati címen fut, melyet a projektdokumentáció 2-es pontjában határoztunk meg.
- Az Iroda 2 a 192.168.4.0/24 hálózati címet használja.
 - Alhálózati maszk az egyes címekhez /24-es prefixnek megfelelően 255.255.255.0 – kivétel a központi iroda, ami a 255.255.255.224 maszkot használja a /27-es prefixnek megfelelően.
- **IPv6:**
 - Globális prefix: 2001:db8:x::/64
 - Az IPv6 létrehozatala az Iroda 2 PC1 ben került megvalósításra DHCP-vel. A cím az 2001:db8:4:0::/64

4. Vezeték nélküli hálózat

Az Access Point kialakítása az Iroda 2 telephelyen kerül kialakításra, amely az ott elhelyezett mobiltelefonnal és az Iroda 2 switch-el kommunikál.



10. ábra – az Access Point alapkonfigurációja

5. WAN – telephelyek kommunikációja

A megadott konfigurációval három telephelyet kötöttünk össze egy központi OSPF alapú irányítással működő WAN hálózaton keresztül. A hálózat célja, hogy a központi telephely (R1) és a két iroda (Iroda 1 és Iroda 2) közötti adatforgalmat hatékonyan és dinamikusan kezelje, valamint biztosítsa az egyes irodák belső hálózatainak elérhetőségét az egész rendszerben.

Központi Router (R1)

- WAN kapcsolat Iroda 1-hez:
 - IP: 192.168.10.1/30 (Serial 0/0/0 interfész)
 - OSPF beállítás:
192.168.7.0/27 hálózat hirdetése (helyi LAN)
192.168.10.0/30 (WAN link Iroda 1 felé)
192.168.20.0/30 (WAN link Iroda 2 felé Iroda 1-en keresztül)

Iroda 1 Router

- Kapcsolat a központhoz:
 - IP: 192.168.10.2/30 (Serial 0/1/0 interfész)
- Kapcsolat Iroda 2-höz:
 - IP: 192.168.20.1/30 (Serial 0/1/1 interfész)
 - OSPF beállítás:

Hirdeti az iroda saját LAN hálózatait:

192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24

Továbbítja a WAN linkeket:

192.168.10.0/24 (kapcsolat a központhoz)

192.168.20.0/24 (kapcsolat Iroda 2-höz)

Iroda 2 Router

- Kapcsolat Iroda 1 routerhez:

IP: 192.168.20.2/30 (Serial 0/3/0 interfész)

OSPF beállítás:

Hirdeti az Iroda 2 helyi hálózatát:

192.168.4.0/24

Továbbítja a WAN linkeket:

192.168.20.0/24 (kapcsolat Iroda 1 felé)

192.168.10.0/30 (bár ez redundánsan lett hirdetve itt, valószínűleg routing szempontból nincs jelentősége)

Mit értünk el ezzel?

Teljes hálózati összeköttetés: A központi iroda, Iroda 1 és Iroda 2 között biztosítottuk az elérést, mind WAN, mind LAN szinten.

OSPF dinamikus routing protokoll: Az OSPF 1-es processz használatával a routing dinamikusan alkalmazkodik a hálózati topológiához és hirdeti a helyi hálózatokat a többi router felé.

Hatékony IP-címtartomány kezelés: A WAN kapcsolatokhoz szűk IP-tartományokat (point-to-point /30 hálózatokat) alkalmaztunk, így gazdaságosan kezeltük az IP-címeket.

Skálázhatóság: Az OSPF és a kialakított struktúra lehetőséget biztosít a hálózat későbbi bővítésére (új irodák, új hálózatok integrálása).

- **Access Point konfiguráció:**
 - SSID: Céges hálózat (titkosított hozzáférés WPA2-vel)
 - Vendégálózat (külön VLAN-hoz kötve, internet eléréssel)

Hálózat műszaki megvalósítása

1. Hálózati Redundancia

- **Második és harmadik rétegbeli redundancia:**
 - **Helyi redundancia:**
 - Redundancia: Ha az egyik fizikai link meghibásodik (pl. fa0/2 vagy fa0/3), a másik továbbra is biztosítja a kapcsolatot. Ezzel elkerüljük az egyetlen ponton történő meghibásodást (Single Point of Failure).
 - Sáv szélesség-növelés: A több link egyesítésével összesített sáv szélességet kapunk (pl. két 100 Mbps link esetén akár 200 Mbps-ot).
 - Terheléelosztás (Load Balancing): Az adatforgalmat a protokoll automatikusan elosztja a rendelkezésre álló linkek között.
 - Hurokmentes hálózat: Az EtherChannel logikai linkként jelenik meg a Spanning-Tree Protocol számára, így elkerülhetjük a hurokképződést anélkül, hogy portokat kellene blokkolni.
 - **Miért LACP?**
 - Az LACP (IEEE 802.3ad) szabványos protokoll, amely automatikusan kezeli

a taglinkek állapotát.

- Active módban mindkét eszköz aktívan küld LACP üzeneteket, így biztos a linkek együttműködése és stabil működése.
- **Routerek redundanciája:**
- Redundáns alapértelmezett gateway biztosítása a kliensek számára az 192.168.3.254 címen. Ez a cím mindig az aktuálisan aktív router IP-jére mutat.
- Folyamatos elérhetőség: Ha az elsődleges router (R1) meghibásodik, azonnal észleli a rendszer, és a tartalék router (R2) veszi át a forgalom továbbítását. A kliensek ebből semmit nem vesznek észre, hiszen a gateway IP nem változik.
- Automatikus visszaállás (Preemption): Ha az elsődleges router helyreáll, az automatikusan visszaveszi az aktív szerepet, így a tervezett elsődleges-fő és másodlagos-tartalék szerepek mindig fenntarthatók.

- **Miért HSRP?**

- Cisco saját fejlesztésű protokoll, széles körben elterjedt Cisco eszközökön.
- Gyors failover (jellemzően néhány másodperc alatt).
- Egyszerű konfiguráció, és nagyfokú megbízhatóság.

2. Forgalomirányítás

- **Statikus útvonalak:**

- Az Iroda 1-ben statikus útvonalakat alkalmaztunk, mivel itt az eszközök közötti forgalom viszonylag kiszámítható, és az iroda hálózati struktúrája nem változik

gyakran. A statikus útvonalak egyszerűek, könnyen konfigurálhatók, és alacsony overheadet eredményeznek, mivel nem igényelnek folyamatos protokoll-alkalmazást.

- **Dinamikus forgalomirányítás:**

- A Központban dinamikus forgalomirányítást választottunk, EIGRP protokollal, hogy a hálózaton belüli változások, például új eszközök csatlakozása vagy hálózati hibák gyorsan és automatikusan kezelhetők legyenek. Az EIGRP gyors konvergenciát biztosít, ami kritikus a nagyobb és dinamikusabb hálózatok esetén, mint amilyen a Központ.

3. Címfordítás

- **Statikus címfordítás:**

- A Központban alkalmazott statikus címfordítás biztosítja, hogy az internetről érkező kérések mindig a megfelelő, fix IP-című szerverekhez irányuljanak. Ez a megoldás biztosítja az erőforrások állandóságát és elősegíti a biztonságos, kontrollált forgalmat.

- **Dinamikus címfordítás (NAT):**

- A Központban dinamikus NAT-ot alkalmaztunk, hogy a belső hálózaton elhelyezkedő eszközök internetelérése rugalmas legyen, miközben a belső IP-címek védve maradnak. A dinamikus NAT biztosítja, hogy a belső hálózati eszközök egyedi IP-címet kapjanak az internetes forgalom számára, miközben csökkenti a külső támadási felületet és javítja a hálózat biztonságát.

```
Kozpont-R1(config)#do sh ip nat translations
Pro Inside global      Inside local      Outside local      Outside global
--- 203.0.113.10        192.168.7.20      ---                ---
--- 203.0.113.11        192.168.7.21      ---                ---
--- 200.200.200.10       192.168.7.66      ---                ---
--- 200.200.200.11       192.168.7.67      ---                ---
Kozpont-R1(config)#
```

11. ábra – NAT a központi routerben

4. Virtuális Magánhálózat (VPN)

- **IPsec VPN:**

- A projekt során az IPsec VPN (Virtual Private Network) technológia alkalmazása mellett döntöttünk a hálózati biztonság garantálása érdekében, mivel az IPsec kiváló védelmet nyújt az adatforgalom titkosításában és hitelesítésében, miközben lehetővé teszi a távoli hálózatok közötti biztonságos kommunikációt. Az IPsec VPN alapvetően az adatok védelmét biztosítja azáltal, hogy titkosítja a hálózaton keresztül továbbított információkat, megakadályozva ezzel a lehallgatást és az adatok manipulálását, amely kritikus a vállalati adatvédelmi előírásoknak való megfelelés szempontjából.
- A projektünkben minden egyes routert VPN-kapcsolaton keresztül kapcsoltunk össze, biztosítva, hogy a topológia minden pontján biztonságos, titkosított adatátvitel történjen. Ezen keresztül a különböző helyszínek közötti kommunikáció védetté vált, minimalizálva a potenciális támadási felületeket és megakadályozva, hogy illetéktelenek hozzáférjenek a hálózati forgalomhoz.
- Az engedélyezéseket ACL-ek (Access Control Lists) segítségével oldottuk meg, amelyek lehetővé tették a hálózati hozzáférések szigorú ellenőrzését. Az ACL-ek alkalmazásával pontosan meghatározhatjuk, hogy mely eszközök és felhasználók férhetnek hozzá a VPN-alapú kapcsolatokhoz, és így biztosíthatjuk, hogy csak a jogosult eszközök és felhasználók számára legyen elérhető a titkosított kommunikációs csatorna. Ez növeli a hálózat biztonságát, mivel lehetővé teszi a hozzáférések finomhangolását, és csökkenti a nem kívánt hozzáférési kísérletek lehetőségét.

- Összességében az IPsec VPN és az ACL-ek alkalmazása biztosította számunkra a megfelelő védelmet, miközben biztosította a hálózati erőforrások közötti biztonságos, zökkenőmentes kommunikációt. Az ilyen típusú megoldás nemcsak a jelenlegi biztonsági igényeket elégíti ki, hanem a jövőbeli hálózati bővítésekhez is kellő rugalmasságot biztosít.

- **GRE Tunnel**

- A GRE (Generic Routing Encapsulation) alagút egy hálózati protokoll, amely lehetővé teszi különböző típusú adatsomagok kapszulázását egy másik adatsomagba, és azok biztonságos továbbítását az interneten vagy más, nem megbízható hálózatokon keresztül. Az általunk létrehozott GRE alagút az ISP (Internet Szolgáltató) hálózatán keresztül biztosít egy privát, titkosított kapcsolatot két irodai hálózat között.
- A GRE alagút előnye, hogy lehetővé teszi a két iroda közötti forgalom egyszerű továbbítását, miközben titkosítást nem alkalmazunk a protokoll szintjén, így kisebb a hálózati overhead és könnyen implementálható. Az alagút két végpontja között egy közvetlen IP kapcsolat jön létre, amely mintha egy fizikai összeköttetés lenne, bár valójában az ISP által biztosított internetkapcsolaton keresztül zajlik a forgalom.
- A GRE alagút konfigurálása az irodák közötti adatkommunikáció szempontjából gyors és hatékony megoldást jelent, mivel az alagútba csomagolt forgalom nem igényel különböző hálózati protokollok kezelését, és a hálózati infrastruktúra is viszonylag egyszerű marad. Az alagútban küldött adatokat az ISP nem módosítja, így az irodák közötti kommunikáció biztonságosnak tekinthető, ha a megfelelő biztonsági intézkedéseket is alkalmazzuk, például VPN-ek vagy titkosított alkalmazások használatával.

Ez a megoldás ideális lehetőséget biztosít a távoli irodák közötti gyors és megbízható adatátvitelhez, miközben minimalizálja a bonyolult infrastruktúra fenntartását és biztosítja a folyamatos adatkommunikációt az ISP hálózatán keresztül.

5. Biztonsági Funkciók

- **ACL-ek:**

- A külső hálózatokból érkező forgalom szűrésére ACL-t alkalmaztunk az összes irodában a vpn megfelelő működése érdekében. Az ACL minden beérkező forgalmat eldob, kivételt képez a hálózaton belül történő forgalom.

```
Kozpont-R1(config)#do sh access-list
Standard IP access list 1
 10 permit 192.168.1.0, wildcard bits 0.0.0.255
 20 permit 192.168.4.0, wildcard bits 0.0.0.255
 30 permit 192.168.7.0, wildcard bits 0.0.0.127
Extended IP access list 100
 10 permit ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255
 20 permit ip 192.168.7.0 0.0.0.255 192.168.6.0 0.0.0.255
 30 permit ip 192.168.7.0 0.0.0.255 192.168.4.0 0.0.0.255
 40 permit ip 192.168.7.0 0.0.0.255 192.168.3.0 0.0.0.255
 50 permit ip 192.168.7.0 0.0.0.255 192.168.2.0 0.0.0.255
 60 permit ip 192.168.7.0 0.0.0.255 192.168.5.0 0.0.0.255
Extended IP access list VPN_ACL
Kozpont-R1(config)#
```

12. ábra – ACL a Központi routerben

- **Hardveres tűzfal:**

- Eszközhiány lévén szoftveres tűzfalat hoztunk létre a Központban, az ott lévő „Központ R1” rendelkezik az ott kialakított Zónázó tűzfallal, amely szűri a kívülről érkező csomagokat.

```
zone outside
  Member Interfaces: ISP
  FastEthernet0/1
zone inside
  Member Interfaces: SW
  FastEthernet0/0
```

13. ábra – Zónázó tűzfal a Központi telephelyen

Szerverek és Szolgáltatások

A projektünkben két különböző típusú szervert alkalmazunk: egy Ubuntu alapú Linux szervert és egy Windows alapú szervert. A két rendszer különböző szolgáltatásokat lát el, amelyek célja a hatékony működés és a Admin adminisztráció egyszerűsítése. Az alábbiakban részletesen bemutatjuk, miért és hogyan alakítottuk ki a szolgáltatásokat a két szerveren.

1. Ubuntu Szerver

Az Ubuntu Linux szerver három fő szolgáltatást biztosít, amelyek a következő célt szolgálják:

a) HTTP/HTTPS – Webszerver

Az Ubuntu szerver HTTP/HTTPS szolgáltatásokat biztosít, amelyek a weboldalak és webalkalmazások futtatásáért felelősek. Az Apache és Nginx webszerverek rendkívül népszerűek az Ubuntu rendszerekben, és biztosítják a magas rendelkezésre állást, valamint a biztonságos adatforgalmat az SSL/TLS titkosítással. Az Ubuntu kiváló teljesítményű és erőforrás-hatékony rendszert biztosít a webszolgáltatások skálázásához.

b) Automatizált mentés – Cron használatával

Az Ubuntu rendszerek egyik legnagyobb előnye, hogy a cron eszközzel könnyen beállíthatók időzített feladatok. Automatizált mentéseket végezhetünk, amelyek biztosítják, hogy a fontos adataink rendszeres időközönként mentésre kerüljenek. A cron segítségével napi, heti vagy havi mentéseket konfigurálhatunk, így a rendszer folyamatos adatvédelmet nyújt.

2. Windows Szerver

A Windows szerver a következő kulcsfontosságú szolgáltatásokat biztosítja a hálózati környezetben:

a) DNS – Névszerver-szolgáltatás

A DNS (Domain Name System) szolgáltatás a Windows szerveren biztosítja a domain nevek IP-címekre való lefordítását. A Windows Server DNS szerepköre lehetővé teszi a helyi hálózatban történő gyors és megbízható címfeloldást. A DNS szolgáltatás konfigurálása a Windows Server környezetében egyszerű, és a rendszer megfelelő működéséhez nélkülözhetetlen a hálózaton belüli kommunikációhoz.

b) Active Directory – Felhasználók és csoportok kezelése

Az Active Directory (AD) központi adatbázisként tárolja a felhasználói fiókokat, csoportokat és más hálózati erőforrásokat. Az AD segítségével könnyen kezelhetjük a felhasználói engedélyeket és jogosultságokat. Az Active Directory integrációja lehetővé teszi, hogy központosítva tároljuk a hálózati fiókokat és biztonsági beállításokat, így megkönnyítve a Admin adminisztrációt és növelve a hálózat biztonságát.

c) DHCP – Dinamikus IP címek kiosztása

A DHCP szolgáltatás automatikusan kiosztja az IP-címeket a hálózati eszközöknek. Ez lehetővé teszi a gyors és hatékony IP-cím-kezelést, csökkentve az Admin adminisztrációs terheket, miközben biztosítja a hálózat zökkenőmentes működését.

d) Fájlszerver – Központi fájlmegosztás

A Windows szerver fájlszerverként működik, amely lehetővé teszi a központi fájlmegosztást a vállalatban belül. A SMB (Server Message Block) protokoll segítségével biztonságos és gyors fájlmegosztást biztosítunk a felhasználók számára.

e) Nyomtatómegosztás – Nyomtatók központi kezelése

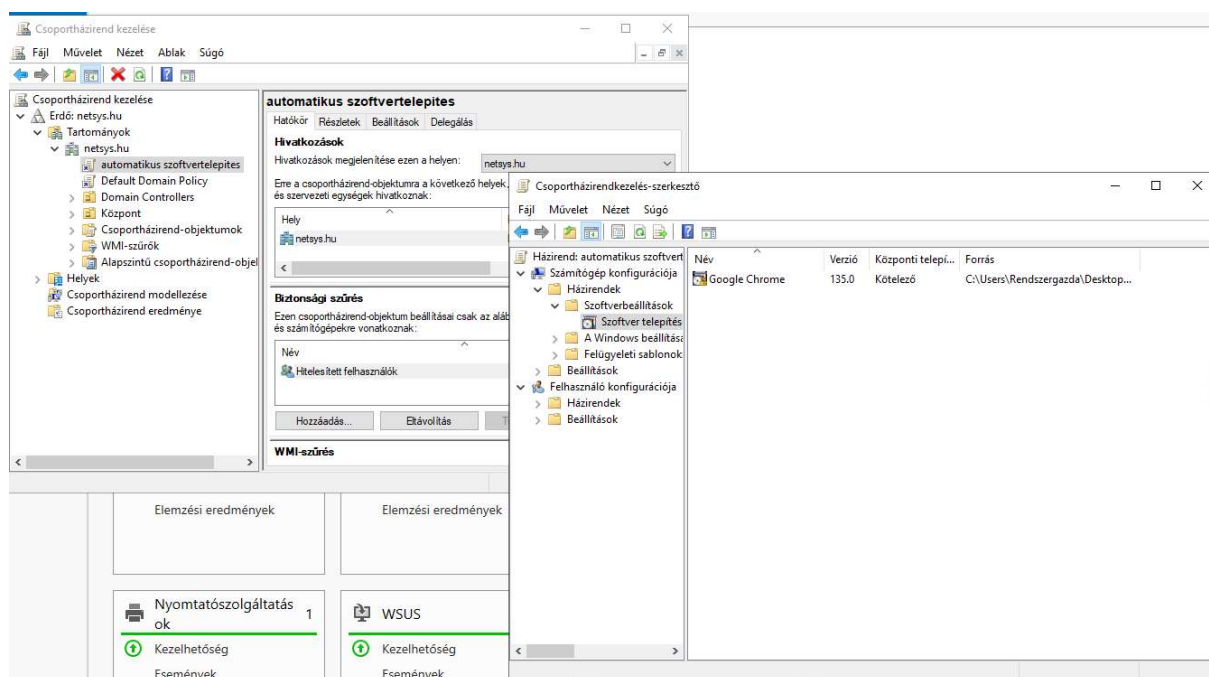
A Windows szerveren a nyomtatók központilag kezelhetők, és a felhasználók számára könnyen elérhetővé válik a központi nyomtatási szolgáltatás.

f) Szoftvertelepítés

A telepítési fájlokat a NetSys Fájlszerver megosztott mappájában tárolom, a gépekre automatikusan a tartományi beállítások alapján települ a Google Chrome böngésző a könnyebb hálózati hozzáférés érdekében.

A csoportházirend-kezelőbe belépve csatlakozunk a netsys.hu tartományra, és létrehoztunk egy új csoportházirend-objektumot „automatikus szoftvertelepites” néven. Ebben az objektumban fogjuk kialakítani az egész tartományra kiterjedően a Google Chrome böngésző automatikus települését.

A felhasználók a szoftvert majd a megosztott fájlszerveren érhetik el és telepíthetik a saját számítógépükre.



14. ábra – Automatikus szoftvertelepítés

Hogyan hoztuk létre ezeket a szolgáltatásokat?

A szolgáltatások kialakítása során az a célunk, hogy a Linux és Windows szerverek zökkenőmentesen együtt működjenek, miközben mindkét rendszer a legmegfelelőbb szolgáltatásokat biztosítja. A következő lépéseken mentünk végig:

1. Szerverek előkészítése

- **Ubuntu szerver:** Az Ubuntu operációs rendszert választottuk, mivel rendkívül megbízható és széles körben támogatott. Az alap telepítés után telepítettük a szükséges csomagokat és szolgáltatásokat: Apache (HTTP/HTTPS), valamint a cron-t a rendszeres mentésekhez.
- **Windows szerver:** A Windows Server operációs rendszer telepítése után a DNS, Active Directory, DHCP, fájlszolgáltatás állítottunk be. A DNS szerepkört a Windows Server integrált szolgáltatásaként konfiguráltuk, az SMB protokollt használtuk a fájlmegosztáshoz, és egyszerűen konfiguráltuk a nyomtatómegosztást.

2. Szolgáltatások konfigurálása

- **Ubuntu szerver:** Az Apache webservert konfigurációját az /etc/apache2/sites-available könyvtárban végeztük el, és SSL tanúsítványt telepítettünk a HTTPS működéséhez. A cron segítségével automatizált mentéseket állítottunk be, napi fájlmentéseket végezve.
- **Windows szerver:** A DNS szolgáltatást a Windows Server DNS szerepkörével állítottuk be, konfigurálva a kívánt domain neveket. Az Active Directory beállításakor létrehoztuk a szükséges tartományokat és szervezeti egységeket, valamint beállítottuk a felhasználói fiókokat. A DHCP szerepkört úgy konfiguráltuk, hogy a hálózaton lévő eszközök automatikusan IP-címet kapjanak. A fájlszolgáltatásokat SMB protokollon keresztül, a nyomtatómegosztást egyszerűen konfiguráltuk. A WSUS telepítésével biztosítottuk, hogy a rendszerek folyamatosan frissüljenek.
- **DNS Konfiguráció - Windows Server**
 - A DNS (Domain Name System) szolgáltatás kulcsfontosságú szerepet játszik a hálózati kommunikációban, mivel lehetővé teszi a számítógépek számára, hogy név alapján azonosítsák egymást. A Windows Server rendszeren belül a DNS szolgáltatást a rendszer integrált szerepköre biztosítja, ami jelentősen megkönnyíti a beállításokat. A DNS konfigurációját az alábbiakban részletezett módon hajtottuk végre.

- **DNS Rekordok Beállítása**

- **A rekord (Host Record)**

Az A rekordok segítségével a domain nevekhez rendelhetjük az IP-címeket. Ez biztosítja, hogy a hálózaton lévő szolgáltatások elérhetőek legyenek a domain név alapján.

- **Hozzáadott A rekordok:**

- **Domain név:** www.netsys.hu ! Tisztában vagyunk azzal, hogy ez éles környezetben regisztráció kötelező, így csak tesztelés jelleggel használtuk fel a munkánk során.

- **IP cím:**

- 192.168.7.170

Az A rekordot sikeresen hozzáadtuk a Windows DNS szolgáltatásában a "Forward Lookup Zones" menüpont alatt. Az "Új Host (A vagy AAAA)" lehetőséget választva megadtuk a domain nevet és az IP címet.

- **Miért szükséges?**

Az A rekord biztosítja, hogy a felhasználók a domain név használatával elérjék a kívánt szolgáltatást, és a DNS szerver az IP címre irányítja a kéréseket.

- **MX rekord (Mail Exchanger Record)**

Az MX rekordokat a levelezőszerverek konfigurálására használjuk, amelyek az e-mailek kézbesítését végzik.

- **Hozzáadott MX rekord:**

- **Domain név:** www.netsys.hu
- **Mail szerver:** mail.netsys.hu
- **Prioritás:**10

Az MX rekordot is hozzáadtuk a DNS rendszerhez, így biztosítva, hogy a beérkező e-mailek a megfelelő levelezőszerverre kerüljenek.

- **Miért szükséges?**

Az MX rekordok szükségesek a levelezési forgalom irányításához, és segítenek biztosítani, hogy a levelek a helyes szerverre kerüljenek.

- **CNAME rekord (Canonical Name Record)**

A CNAME rekordok segítségével egy domain nevet alias névként használhatunk egy másik domain névhez.

- **Hozzáadott CNAME rekord:**

- **Alias név:** mail.netsys.hu

- **Hivatkozott domain:**

- mailserver.netsys.hu

A CNAME rekordot létrehoztuk, így a mail.netsys.hu domain név a mailserver.netsys.hu-ra mutat.

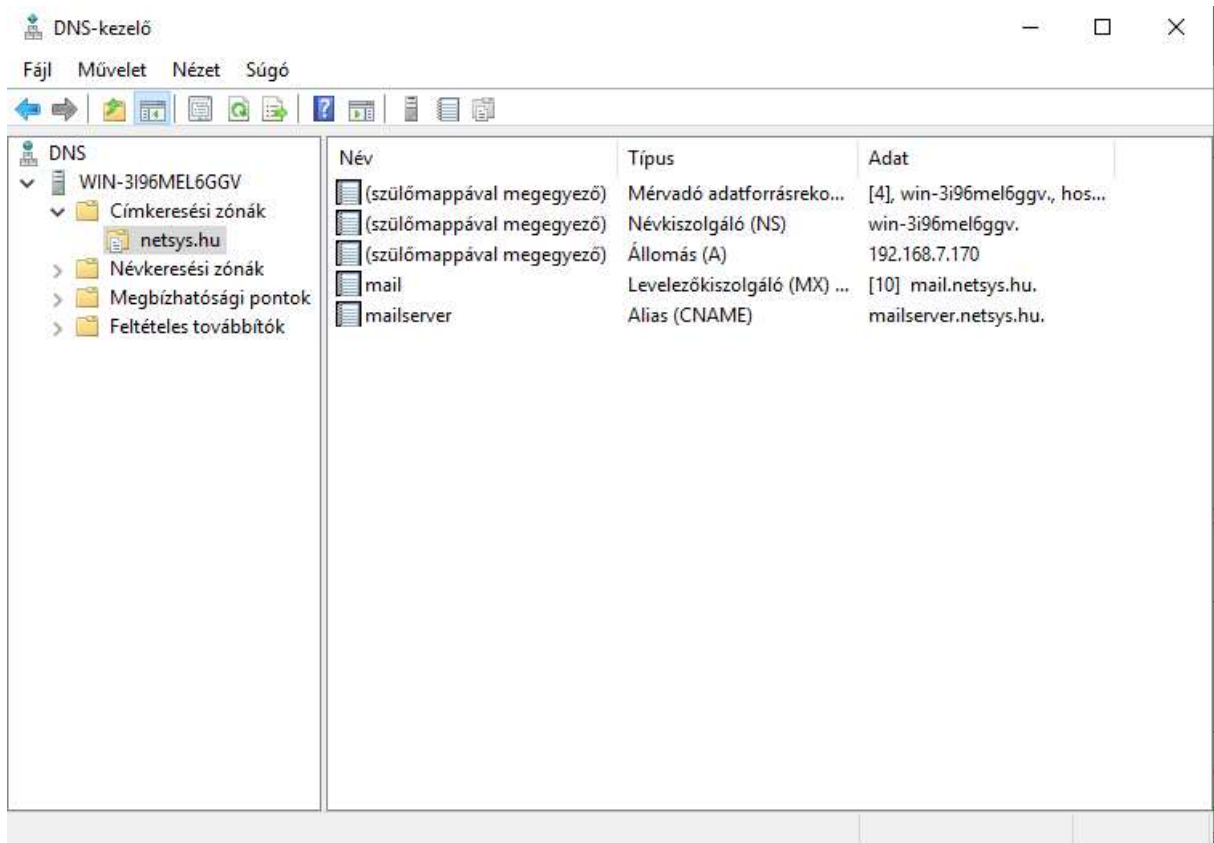
- **Miért szükséges?**

A CNAME rekordok segítenek az egyszerűbb és rugalmasabb domain névkezelésben,

mivel nem szükséges külön IP címeket rendelni minden szolgáltatáshoz.

- **DNS Szerver Konfigurációja**

- A DNS szerver beállításait a Windows Serveren a "Server Manager"-en belül végeztük el. A konfiguráció során a "DNS" szerepkör alatt hozzáadtuk az új rekordokat:
- A DNS konzolon belépve hozzáadtuk a szükséges A, MX és CNAME rekordokat a megfelelő zónákhoz.
- Az összes szükséges domain nevet és IP címet pontosan konfiguráltuk a megfelelő szolgáltatásokhoz, így biztosítva, hogy a hálózati kommunikáció zökkenőmentesen működjön.
- **Miért fontos a DNS megfelelő beállítása?**
- A DNS helyes konfigurálása kulcsfontosságú, mivel a legtöbb szolgáltatás és alkalmazás DNS-t használ a másik rendszerhez való kapcsolódáshoz. Ha a DNS nincs megfelelően beállítva, a szolgáltatások nem működnek megfelelően, vagy teljesen elérhetetlenné válhatnak. A DNS rekordok pontos beállításával biztosítjuk a zavartalan működést és a rendszerek közötti kommunikációt.



15. ábra – DNS tartományok

- **Active Directory Beállítása - Windows Server**
- Az Active Directory (AD) szolgáltatásának beállítása után sikeresen létrehoztuk a szükséges csoportokat és felhasználói fiókokat, amelyek biztosítják a rendszer hatékony és biztonságos működését. Az alábbiakban részletezzük a végrehajtott konfigurációkat.
- Ezeket a beállításokat a netsys-erdo erdőben végezzük, NetSys tartományban létrehozva, így konfiguráljuk azokat.
- **Felhasználói csoportok létrehozása**
 - **Admin Csoport Létrehozása:**

Az Admin csoportja olyan felhasználókat tartalmaz, akik teljes hozzáféréssel rendelkeznek a rendszerhez. Ezen a csoporton keresztül biztosítottuk a rendszer felügyeletét és a jogosultságok kezelhetőségét.

- **Admin csoport és felhasználók:**

- **Csoport neve:**

- Admin

A csoportot sikeresen létrehoztuk az Active Directory-ban, és minden Rendszergazdánk hozzá lett adva.

- **Felhasználók az Admin csoportban:**

- **Felhasználónév:** kpista

- **Teljes név:** Kiss Pista

- **E-mail cím:** kpista@netsys.hu

- **Beállítások:** Pista Admin jogosultságokkal rendelkezik, így teljes hozzáférése van a szerverekhez és a hálózati erőforrásokhoz.

- **Felhasználónév:** nzsofia

- **Teljes név:** Nagy Zsófia

- **E-mail cím:** nzsofia@netsys.hu

- **Beállítások:** Zsófia szintén Admin jogosultságokkal rendelkezik, így ő is képes a teljes rendszer konfigurálására és karbantartására.

- **Felhasználónév:** fkristóf

- **Teljes név:** Fekete Kristóf

- **E-mail cím:** fkristof@netsys.hu

- **Beállítások:** Kristóf teljes hozzáféréssel rendelkezik, beleértve az összes Admin

feladatot is.

- **Alkalmazott Csoport Létrehozása:**

Az általános felhasználói csoportot azoknak a felhasználóknak hoztuk létre, akik nem rendelkeznek Admin jogosultságokkal, de szükségük van a vállalat erőforrásainak használatára.

- **Felhasználói csoport és felhasználók:**

- **Csoport neve:**

- Alkalmazott

Ezt a csoportot létrehoztuk, és minden nem rendszargazdai felhasználót hozzáadtuk.

- **Felhasználók a Felhasználók csoportban:**

- **Felhasználónév:** gjakab
- **Teljes név:** Gipsz Jakab
- **E-mail cím:** gjakab@netsys.hu

- **Beállítások:** Jakab hozzáférést kapott az alapvető vállalati erőforrásokhoz, például a fájlmegosztásokhoz és a nyomtatókhöz.

- **Felhasználónév:** fanna
- **Teljes név:** Fehér Anna
- **E-mail cím:** fanna@netsys.hu

- **Beállítások:** Anna alapvető felhasználói jogosultságokkal rendelkezik, hozzáférést

kapott a vállalati fájlokhoz és a közös nyomtatókhoz.

- **Felhasználónév:** ppeter
- **Teljes név:** Pici Péter
- **E-mail cím:** ppeter@netsys.hu
- **Beállítások:** Péter is alapfelhasználói jogosultságokkal rendelkezik, biztosítva számára a napi munkavégzéshez szükséges hozzáféréseket.

- **Felhasználók és Csoportok Kezelése**

- Az Active Directory Users and Computers konzolon keresztül sikeresen létrehoztuk és konfiguráltuk a felhasználókat és csoportokat. Az egyes felhasználók jogosultságait és beállításait pontosan a vállalati igényeknek megfelelően alakítottuk ki, így biztosítva a megfelelő szintű hozzáférést és biztonságot.

- **Miért fontos az Active Directory megfelelő konfigurálása?**

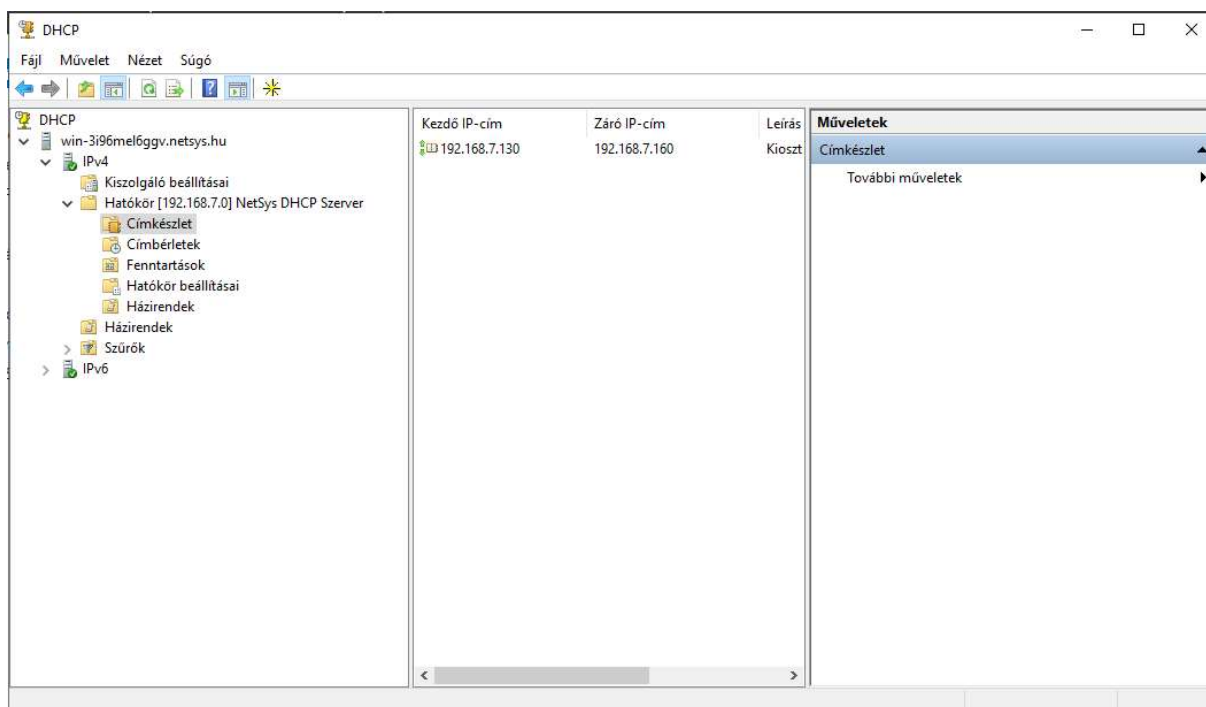
- Az Active Directory alapvető fontosságú az informatikai infrastruktúra kezelésében, mivel lehetővé teszi a központi felhasználókezelést és a hálózati erőforrásokhoz való hozzáférést. A megfelelően beállított Active Directory biztosítja a rendszer biztonságát, az erőforrások hatékony kezelését és a felhasználói jogosultságok pontos meghatározását.

- **DHCP Szerver konfigurálás**

A DHCP hatókör a Windows Szerveren jött létre. A kezdő cím 192.168.7.130 és a záró 192.168.7.160 - /24 -es maszkkal.

Az alapértelmezett átjáró a Központban elhelyezkedő ME Switch ip címe, a 192.168.7.1

A DNS címe 192.168.7.170



16. ábra – DHCP Hatókör

Fájl- és nyomtatómegosztás

A Windows Szerveren elérhető a fájlmegosztás is, amely a „NetSys Fájlszerver” néven érnek el a dolgozók, ide kerülnek a közös fájlok a munka gördülékeny előrehaladásának segítése érdekében. Mindemellett innen tudják a munkatársak a számukra elérhető Google Chrome – Automatikus szoftvertelepítésben hozzáadott fájlt is telepíteni a gépükre.

Nyomtatómegosztás:

A nyomtatómegosztás célja, hogy a NetSys vállalat alkalmazottai – mind adminisztrátorok, mind általános felhasználók – központilag hozzáférhessenek a cég által biztosított nyomtatási szolgáltatáshoz. A központi nyomtatót a tartományi szerverhez csatlakoztattam, majd hálózaton keresztül megosztottam az Active Directory környezetben belül.

1. Nyomtató hozzáadása a szerverhez

A nyomtatót IP-cím alapján adtam hozzá, majd a megfelelő illesztőprogramot kiválasztottam és telepítettem.

2. Megosztási beállítások

A nyomtatót a következő megosztási névvel láttam el:
NetSys központi nyomtató.

A *nyomtató megosztása* opciót bejelöltem, és megadtam, hogy a nyomtató jelenjen meg a tartományban, így Active Directory-n keresztül is könnyen kereshető és elérhető legyen.

Jogosultságok és hozzáférések beállítása

A jogosultságokat a Printer Properties > Security fülön állítottam be:

- **Admin csoport:**

- Nyomtatás – Igen
- Nyomtató kezelése – Igen
- Dokumentumok kezelése – Igen
Így az adminok nemcsak használhatják, hanem konfigurálhatják is a nyomtatót, valamint beavatkozhatnak a dokumentumok sorba állításába, törlésébe is.

- **Domain felhasználók csoport:**

- Nyomtatás – Igen
- Nyomtató kezelése – Nem
- Dokumentumok kezelése – Nem
Az alap felhasználók nyomtatni tudnak, de nincs jogosultságuk a nyomtató konfigurálásához vagy más felhasználók dokumentumainak kezeléséhez.

Active Directory integráció

A listázás opció bekapcsolásával a nyomtató elérhető lett a tartományi felhasználók számára, kereshető módon. Ez megkönnyíti az új kliensek nyomtatóhoz való csatlakozását. A nyomtató automatikusan regisztrálódott az Active Directory-ba, így csoportházirenden keresztül is telepíthető a klienseken.

Csoportházirend (GPO) beállítás (opcionális)

Az egyszerűbb hozzáférés érdekében a Group Policy Management konzolon keresztül létrehoztam egy új GPO-t NetSys Default Printing néven, és a következőket állítottam be:

- Felhasználók > Preferenciák > Nyomtatók alatt egy megosztott nyomtató beállítással automatikusan hozzáadódik a nyomtató minden Domain felhasználó taghoz bejelentkezéskor.

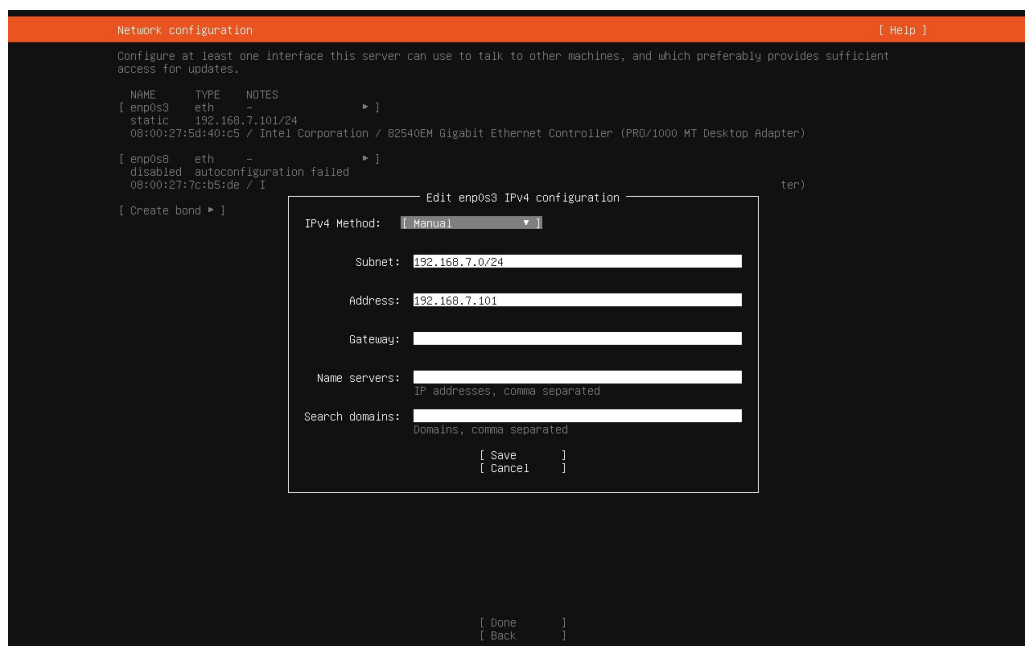
Tesztelés és ellenőrzés

A végleges beállítás után több tesztet is végeztem:

- Admin felhasználó sikeresen telepítette és tesztoldalt nyomtatott.
- Általános domain user gjakab csatlakozott a nyomtatóhoz és sikeresen küldött nyomtatási feladatot.
- Nyomtatás figyelése, sor kezelése és jogosultság-ellenőrzés is megtörtént.

Linux szerver telepítése

- Létrehozunk egy új virtuális gépet, aminek a neve az az, hogy NetSys. **Típusa:** Linux a **verziója** pedig Ubuntu (64-bit)
- **Alap memóriája:** 4096MB
- **Processzorra:** 2
- Csinálunk egy új Virtual Hard Disket aminek a mérete 20GB, ezután pedig a befejezésre nyomunk.
- Ezután megnyitjuk a konfigurálást és becsatoljuk a Vezérlő: IDE-be az ISO fájlt, aminek a típusa: ubuntu-24-04-live-server-amd64. Bezárjuk a konfigurációs fület és elindítjuk az Ubuntu szervert.
- Beállítjuk a következőket:
- **Nyelv:** Magyar
- **Billentyűzet:** Magyar
- A telepítés módja az normál telepítés (Install Ubuntu Server)
- Beállítunk egy hálózati csatolót, amelyeken a kiszolgáló más gépekhez csatlakozhat, és amely lehetőleg alkalmas a frissítések elérésére: kiválasztjuk az enp0s3 eth -> rámegyünk, hogy ipv4 szerkesztés kézikézzel és beállítjuk a következő alhálózatot: 192.168.7.0/24, címet: 192.168.7.101, ipv6 címet nem adtunk neki.



17. ábra - Kézikézzel beállított ipv4 alhálózat

- Proxy beállítását kihagytuk, üresen hagytuk, mivel a rendszer közvetlenül kapcsolódik az internetre és nem igényel köztes proxy szerveret.

- **Tükör (mirror) kiválasztása:** Alapértelmezett Ubuntu mirror használata (nem változtattunk rajta)

- **Tárhely beállítása: lemez:** 20GB Virtual Hard Disk, felhasználói beavatkozás nélkül hagytuk az alap automatikus particionálást, így **felhasználói beavatkozás nélkül** történt a lemez felosztása. Ez gyors, biztonságos

- Aztán létrehozunk egy **felhasználói profilt**, aminek a következő beállításokat adtuk meg:

neve: NetSys

szerver neve: netsysszerver

felhasználónév: netsys

jelszó: projekt

- Az OpenSSH szerver telepítését **kihagytuk**, mivel a szerverhez közvetlenül a VirtualBox konzolon keresztül férünk hozzá, és nem volt szükség távoli bejelentkezésre SSH-n keresztül

- Kiegészítő csomagok és szolgáltatások kiválasztásánál semmit nem választottunk ki.

- Minden beállítás után a „**Telepítés elindítása**” opciót választottuk.

- **Ezután újra indítjuk a szervert.**

```
System information as of 2025. ápr. 11., péntek, 07:01:31 UTC

System load:  0.23      Processes:      124
Usage of /:   41.3% of 9.75GB  Users logged in:  0
Memory usage: 5%        IPv4 address for enp0s3: 192.168.7.101
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See 'man sudo_root' for details.

netsys@netsysszerver:~$ [ 51.465806] cloud-init[1221]: Cloud-init v. 24.1.3-0ubuntu3 running 'modules:final' at Fri, 11 Apr 2025 07:01:51 +0000. Up 51.43 seconds.
ci-info: no authorized SSH keys fingerprints found for user netsys.
<14>Apr 11 07:01:51 cloud-init: #####
<14>Apr 11 07:01:51 cloud-init: -----BEGIN SSH HOST KEY FINGERPRINTS-----
<14>Apr 11 07:01:51 cloud-init: 256 SHA256:BXvy60RM+omladPfrTcUyEugtTq45SDqzdM/e0RHccw root@netsysszerver (ECDSA)
<14>Apr 11 07:01:51 cloud-init: 256 SHA256:Bbvrs5PaJGrLPCpUSD57gDiVDauk0JqA71bWb7y/2AU root@netsysszerver (ED25519)
<14>Apr 11 07:01:51 cloud-init: 3072 SHA256:J2ID3uJ92rzSCV9mGFYJknuJked6YTEtBbUcw7bg1GM root@netsysszerver (RSA)
<14>Apr 11 07:01:51 cloud-init: -----END SSH HOST KEY FINGERPRINTS-----
<14>Apr 11 07:01:51 cloud-init: #####
-----BEGIN SSH HOST KEY KEYS-----
ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoVTIibmlzZDhAYNTAAABmLzdhYNTAAABBBG46kJffVG1oHG0P IUZEg0pG1TACSP3MHgJcug9kSSMx0+Y0uni11/XarKBxWUDyTD7Z++qrA0BVPVphbASqaQ=
root@netsysszerver
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDonts/LbNjoI0QSIx122A238vTt3Jw4w0YUX8tSKJ2SLHUV9KUhwa1fNUL0TnwlmrQR0RnEffFnAxdXEPwddlePQ05GvToYdyVu0J200Pg42Qn93Z+b1Laab
xHkFmaws5XSbdcvh0gcr6XGLG1+9u2uqCeryamQda5oIUXMY7UlyFKJb84u4nR50aek27FndvBRk00URKDCJ3FVS2egLt1xGUQtBhH5CM4d9Ix6pX0MBVNrXdpdx3U2D9tZpdkbQySgaHvd872bo0pV31duEP IgU
XyQz/76keqyb+Vyx207CZF1430Wn93JfRqeY5nfk7VbQ4gCm0uUgWhDBCFu0pMGcXhtIDntuVSMaK2ZF0BAGHubu90tynfm4tk3XfB7gqJkan6Jzu+Q8nqpd2BU/Stba0mwTdkrRSkvDXK1yxDurqLmgFvq125S
C00T0w+stHngTB6a016B16+4BY9q1E/ahPvtJukFUQu4T52Ik6GrsFgXc+gx1S1Sk/X0v= root@netsysszerver
-----END SSH HOST KEY KEYS-----
[ 51.609545] cloud-init[1221]: Cloud-init v. 24.1.3-0ubuntu3 finished at Fri, 11 Apr 2025 07:01:51 +0000. DataSource DataSourceNone. Up 51.60 seconds
[ 51.639912] cloud-init[1221]: 2025-04-11 07:01:51.884 - cc_final_message.py[WARNING]: Used fallback datasource
netsys@netsysszerver:~$
```

18. ábra – Sikeresen újra indított ubuntu szerver

Automatizált mentés – Linux Szerver

1. Rsync telepítése

- Először is le kell telepíteni a rsync (Remote Sync), ami egy egy hatékony és gyors fájlmásoló eszköz, amelyet fájlok és könyvtárak szinkronizálására használnak helyi vagy távoli rendszerek között.

Telepítése:

```
sudo apt update
```

```
sudo apt install rsync
```

2. Mentési szkript létrehozása

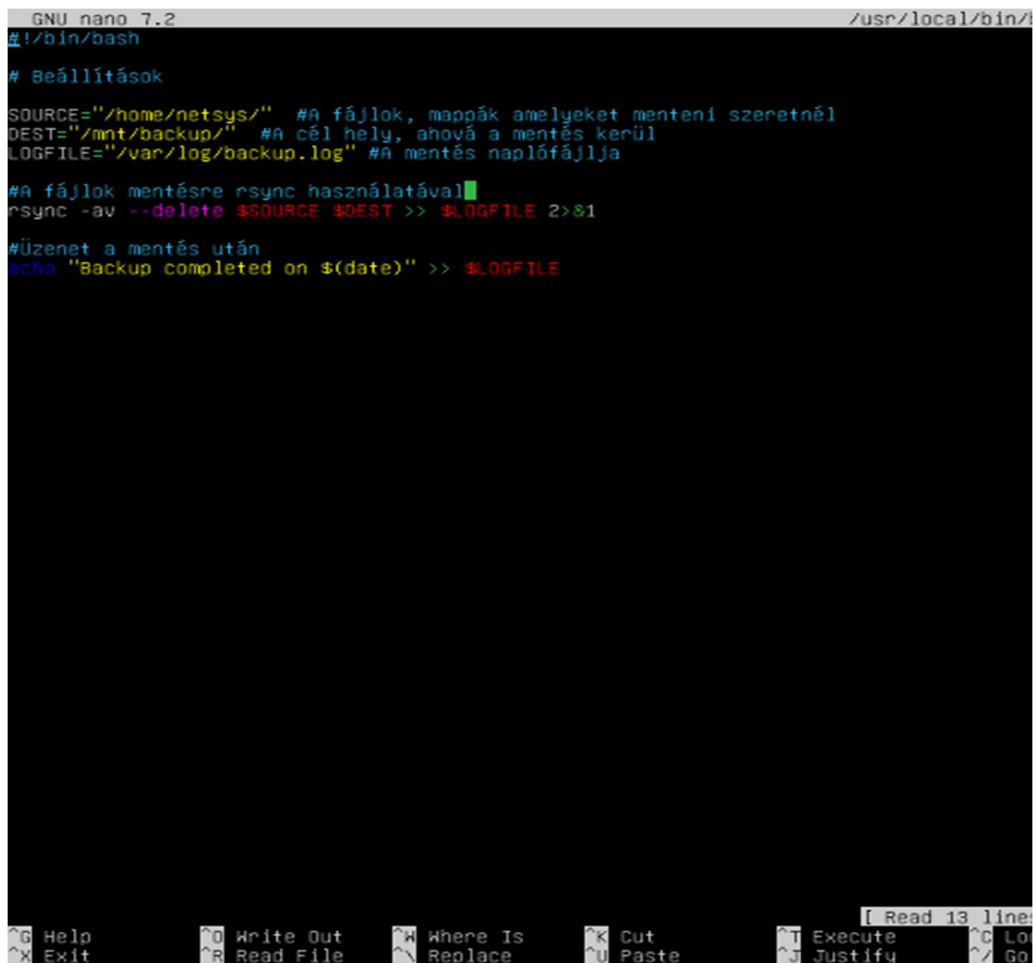
- Létrehoztunk egy szkriptet, amely a fájlokat menti egy másik helyre. Az rsync parancs használata előnyös, mivel hatékonyan másolja a fájlokat, és lehetőséget ad arra, hogy csak azokat a fájlokat másolja, amelyek változtak.

- Létrehoztunk egy egyszerű szkriptet, amely a fájlokat másolja egy biztonságos mentési helyre (pl. egy külső meghajtó vagy egy távoli szerver).

- Beléptünk a bin könyvtárba, és létrehoztunk egy szkriptet:

```
sudo nano /usr/local/bin/backup.sh – belépés a könyvtárba
```

- A következő tartalmat írtuk be a szkriptbe:

A screenshot of a terminal window with a dark background. At the top, it says 'GNU nano 7.2' on the left and '/usr/local/bin/' on the right. The script content is as follows:

```
#!/bin/bash

# Beállítások

SOURCE="/home/netsys/" #A fájlok, mappák amelyeket menteni szeretnénk
DEST="/mnt/backup/" #A cél hely, ahová a mentés kerül
LOGFILE="/var/log/backup.log" #A mentés naplófájlja

#A fájlok mentésre rsync használatával
rsync -av --delete $SOURCE $DEST >> $LOGFILE 2>&1

#Üzenet a mentés után
echo "Backup completed on $(date)" >> $LOGFILE
```

At the bottom, there is a status bar with various nano editor commands like 'Help', 'Exit', 'Write Out', 'Read File', 'Where Is', 'Replace', 'Cut', 'Paste', 'Execute', 'Justify', and 'Go'. On the right side of the status bar, it says '[Read 13 line'.

19. ábra – Mentési szkript

- **SOURCE:** Itt adtuk meg a mappát, amelyet menteni szeretnénk (pl. /home/netsys/).

- Azért a netsys felhasználó home könyvtárát menti mivel A **home** könyvtár tartalmazza minden felhasználó személyes adatait, beállításait, dokumentumait és egyéb fontos fájljait. Mivel a **netsys** felhasználó home könyvtára tartalmazza az ő személyes mappáját és fájljait, a mentés célja az, hogy biztosítsa a felhasználó adatainak védelmét és azok biztonságos helyre történő mentését. A /home/netsys/ könyvtárban található fájlok közvetlenül kapcsolódnak a felhasználó munkájához és napi használatához, így a mentési szkript célja, hogy ezt az adatokat védi.

- **DEST:** Itt adtuk meg a mentési helyet (pl. egy külső meghajtó elérési útja, például /mnt/backup/).

- A **/mnt/backup** könyvtár a rendszerben egy hagyományos hely, amelyet a Linux használ a csatolt eszközök számára. Mivel a rendszerben nem csatoltunk külső eszközt, így ezt a könyvtárat az automatizált mentés céljára manuálisan létrehoztuk. Amennyiben a jövőben külső meghajtót vagy hálózati tárolót csatolunk, ezt a könyvtárat használhatjuk a fájlok tárolására, de jelenleg egyszerűen egy hely a rendszerben, ahol a mentések elhelyezésére sor kerül.

- **LOGFILE:** A mentés naplózásához szükséges fájl (pl. /var/log/backup.log), ahová minden mentési művelet kimenete kerül.

- **rsync -av --delete:** hatékony mentés

- **"\$LOGFILE":** menti a naplófájlba a kimenetet

- **\$(date):** pontos idő a logban

3. A szkript futtatási jogainak beállítása

- A szkriptet futtatni kell, ezért adjunk neki futtatási jogokat:

sudo chmod +x /usr/local/bin/backup.sh

4. Automatikus mentés ütemezése cron segítségével

- Miután megvan a mentési szkript, beállítottuk, hogy a rendszer automatikusan futtassa egy bizonyos időpontban. Ehhez a cron használatával ütemezhetjük a szkriptet.

- Megnyitjuk cron ütemezőt:

crontab -e

- Ez megnyitja a cron fájlt, amelyben megadjuk az ütemezett feladatokat. A következő sorral beállítottuk, hogy a szkript napi egyszer fusson éjfélkor:

0 0 * * * /usr/local/bin/backup.sh

5. Létrehozunk egy mappát a mentendő fájlokkal, aminek netsys lesz a neve:

mkdir /home/netsys/netsys

echo "Ez a netsys " > /home/netsys/netsys/proba.txt

- Ezután újra futtatjuk a szkriptet:

sudo /usr/local/bin/backup.sh

- Majd ellenőrizzük:

ls /mnt/backup

ls /mnt/backup/teszt

- Mostmár látjuk, hogy valóban bemásolta a fájlt a célhelyre.

6. Ellenőrizzük a következőket:

- A mentendő fájlokat (ls /home/netsys/teszt)
- A mentési szkriptet (cat /usr/local/bin/backup.sh)
- A mentés futtatását (sudo /usr/local/bin/backup.sh)
- A célhelyen lévő fájlokat (ls /mnt/backup/teszt)
- A napló fájlt (cat /var/log/backup.log)

7. Naplózás és hibakeresés

- A naplófájl, amelyet a szkriptben beállítottunk, tartalmazza a mentés kimenetét és a hibákat.
- Ha valami nem működik, ezt a fájlt át lehet nézni.

- A naplófájl megtekintéséhez a következő parancsot használjuk:

cat /var/log/backup.log

```

#Üzenet a mentés után
echo "Backup completed on $(date)" >> $LOGFILE
netsys@netsysserver:~$ sudo /usr/local/bin/backup.sh
netsys@netsysserver:~$ ls /mnt/backup/netsys
proba.txt
netsys@netsysserver:~$ cat /var/log/backup.log
sending incremental file list
created directory /mnt/backup
./
.bash_logout
.bashrc
.profile
.selected_editor
.sudo_as_admin_successful
.cache/
.cache/motd.legal-displayed
.local/
.local/share/
.local/share/nano/
.ssh/
.ssh/authorized_keys

sent 5,600 bytes  received 210 bytes  11.636,00 bytes/sec
total size is 4,864  speedup is 0,84
sending incremental file list
./
LOGFILE

sent 577 bytes  received 43 bytes  1.240,00 bytes/sec
total size is 4,923  speedup is 7,94
sending incremental file list
LOGFILE

sent 632 bytes  received 40 bytes  1.344,00 bytes/sec
total size is 4,982  speedup is 7,41
Backup completed on 2025. ápr. 11., péntek, 07:40:34 UTC
sending incremental file list
./
netsys/
netsys/proba.txt

sent 606 bytes  received 51 bytes  1.314,00 bytes/sec
total size is 5,003  speedup is 7,61
Backup completed on 2025. ápr. 11., péntek, 07:47:02 UTC
sending incremental file list

sent 528 bytes  received 18 bytes  1.092,00 bytes/sec
total size is 5,003  speedup is 9,16
Backup completed on 2025. ápr. 11., péntek, 07:49:31 UTC
netsys@netsysserver:~$

```

20. ábra - Ellenőrzés

Ez azt jelenti, hogy a mentés sikeresen lefutott, mert:

- ✅ **Az rsync működött → kis mennyiségű fájlt másolt, sikeres volt a művelet (pl. sent 606 bytes, sent 3,895 bytes, stb.)**
- ✅ **A mentett fájl megjelent a célmappában → /mnt/backup/netsys/proba.txt fájl ott van, tehát sikeresen átmásolta**
- ✅ **A mentés időbélyegzője is megjelent a naplóban → Backup completed on 2025. ápr. 11., péntek, 07:47:02 UTC, vagyis pontosan dokumentálva van, mikor történt a mentés**
- ✅ **A naplófájl frissül minden futásnál → a /var/log/backup.log fájl szépen naplózza a mentési művelet részleteit és időpontját**
- ✅ **A mentés célhelyén most már nem csak egy fájl van (LOGFILE), hanem a valódi tartalom is → pl. netsys/proba.txt, ez bizonyítja, hogy a mentés valóban megtörtént**

HTTP/HTTPS – Linux szerver

- A vállalati webszerver biztonságos eléréséhez HTTPS kapcsolatot konfiguráltunk az Apache2 segítségével. A HTTPS titkosítja az adatforgalmat, így megvédi az érzékeny adatokat a lehallgatástól vagy módosítástól.

- A webszerver az Apache2 alapértelmezett kezdőoldalát szolgálja ki, amely megjelenik, ha a böngészőbe beírjuk a szerver IP-címét (pl. `https://10.0.2.15`). Ez az oldal azt jelzi, hogy az Apache webszerver sikeresen működik – az üzenete: „**It works!**”.

- A célja a webszervernek ebben a projektben az, hogy:

- bemutassa a **HTTPS kapcsolat működését** (titkosított webelérés),
- demonstrálja a **self-signed tanúsítvány használatát**,
- és szemlélteti, hogyan lehet **biztonságosan hostolni** (kiszolgálni) egy weboldalt Linux szerverről.

1, Elsőnek letelepítjük az Apache2 webszervert

```
sudo apt update
```

```
sudo apt install apache2 -y
```

2, A HTTPS támogatásához szükséges SSL modul aktiválása

- Ez a parancs engedélyezi az Apache SSL modult, ami szükséges a HTTPS működéséhez (ez teszi lehetővé a titkosított kapcsolatokat).

```
sudo a2enmod ssl
```

3, Self-signed SSL tanúsítvány létrehozása

- Mivel nem rendelkezünk hivatalos tanúsítvánnyal, saját magunk által aláírt tanúsítványt hozunk létre.

- Valós, éles környezetben javasolt hitelesített (CA – Certificate Authority által kiadott) tanúsítványt használni, mivel ez megbízhatóbb és a böngészők sem figyelmeztetnek rá. A projekt során azonban a tanúsítványt egyszerűség és demonstrációs cél miatt **saját magunk** hoztuk létre.

```
sudo openssl req -x509 -new -nodes -keyout /etc/ssl/private/selfsigned.key -out
```

/etc/ssl/certs/selfsigned.crt -days 365

- x509:** X.509 szabványú tanúsítványt hoz létre.
- new:** új tanúsítványt generál.
- nodes:** nem titkosítja a kulcsot jelszóval (automatizálható).
- keyout:** megadja, hová kerüljön a privát kulcs fájl.
- out:** megadja, hová kerüljön maga a tanúsítvány.
- days 365:** a tanúsítvány 365 napig érvényes.

- Itt néhány adatot bekér, amik szükségesek a tanúsítványhoz:

Country Name: HU

State or Province Name: .

Locality Name: Debrecen

Organization Name: NetSys

Organizational Unit Name: .

Common Name: NetSyszserver

Email Address: netsys@netsyszserver

4, Az Apache SSL konfiguráció módosítása

- Megnyitjuk a HTTPS konfigurációs fájlt

sudo nano /etc/apache2/sites-available/default-ssl.conf

- És beállítjuk benne az alábbi sorokat:

SSLCertificateFile **/etc/ssl/certs/selfsigned.crt** – a tanúsítvány útvonala
SSLCertificateKeyFile **/etc/ssl/private/selfsigned.key** – a hozzá tartozó
privát kulcs útvonala

5, Ezután a HTTPS oldal engedélyezése következik

- Aktiváljuk az SSL beállításokat

sudo a2ensite default-ssl.conf

- Engedélyezi a default-ssl.conf konfigurációt, ami beállítja, hogy a szerver a HTTPS kapcsolatot használja.

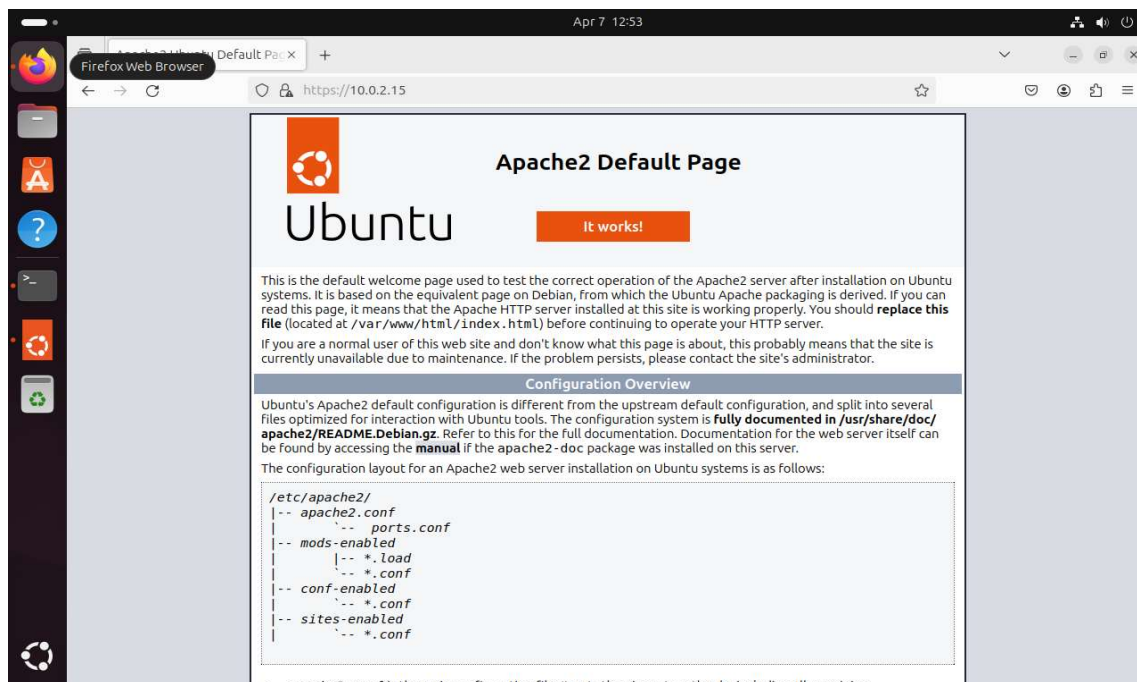
6, A módosítások érvényesítéséhez újra indítjuk az Apache szervert

sudo systemctl restart apache2

7, A szerver IP címének böngészőbe írásával tesztelhetjük a kapcsolatot

<https://10.0.2.15>

- A self-signed tanúsítvány miatt a böngésző figyelmeztethet, ezt jóváhagyva a HTTPS kapcsolat létrejön.



21. ábra – HTTPS szerver ellenőrzése

3.Tesztelés és finomhangolás

A telepítést és konfigurálást követően alapos tesztelést végeztünk, hogy biztosak legyünk abban, hogy minden szolgáltatás megfelelően működik. A DNS és HTTP/HTTPS szolgáltatásokat több különböző eszközzel teszteltük, míg a Windows szerver DNS, DHCP és Active Directory működését különböző felhasználói fiókokkal ellenőriztük.

Összegzés

A Linux (Ubuntu) és Windows szerverek szolgáltatásainak kialakításakor a stabilitás, biztonság és egyszerű kezelhetőség volt a fő szempont. A szolgáltatások konfigurálásával és finomhangolásával biztosítottuk, hogy minden rendszer optimálisan támogassa a projekt igényeit. A sikeres telepítés, konfigurálás és tesztelés után a szolgáltatások zökkenőmentesen integrálódtak a környezetbe, és elvégezték a rájuk bízott feladatokat.

Tesztelés és Dokumentáció

1. Tesztelési Terv

- A tesztelési terv célja a kialakított hálózat működésének ellenőrzése, az egyes eszközök közötti kommunikáció validálása és a biztonsági mechanizmusok megfelelőségének tesztelése. A tesztelési folyamat során az alábbi lépéseket hajtjuk végre:
- PC-k közötti kommunikáció ellenőrzése A telephelyeken elhelyezett PC-k közötti kommunikációt ping parancs segítségével ellenőrizzük. Ennek során megbizonyosodunk arról, hogy az eszközök képesek egymással kapcsolatba lépni, a csomagok sikeresen eljutnak egyik eszköztől a másikra. Továbbá, figyeljük a válaszidőt és az esetleges csomagvesztést, amely hálózati problémákra utalhat.
- Routers és switchek közötti forgalom tesztelése A routerek és switchek megfelelő konfigurációja kulcsfontosságú a hálózat zavartalan működése szempontjából. Ennek érdekében ellenőrizzük a forgalom irányítását, az eszközök által használt dinamikus vagy statikus routing beállításokat. Az adatok megfelelő átviteli sebességét is mérjük, és ellenőrizzük a csomagok torlódását.
- IPv4 és IPv6 címzések validálása Az eszközök címzésének helyességét ellenőrizzük mind IPv4, mind IPv6 protokollok esetében. Ezen belül vizsgáljuk, hogy az eszközök helyes IP-címet kaptak-e DHCP-n keresztül, illetve a statikusan beállított címek megfelelőek-e. A címtartományok helyes kiosztása biztosítja a hatékony forgalomkezelést és az eszközök zökkenőmentes kommunikációját.
- Vezeték nélküli hálózati csatlakozás tesztelése A vezeték nélküli kapcsolat ellenőrzésének célja, hogy biztosítsuk a Wi-Fi hálózat megfelelő működését. A teszt során egy vezeték nélküli eszköztől pingeljük a hálózat egy fizikális kapcsolattal rendelkező eszközét. Ezzel megerősítjük, hogy a vezeték nélküli és vezetékes

hálózatok közötti kommunikáció zökkenőmentes.

- Redundáns útvonalak kiesés esetén történő működésének tesztelése A hálózat megbízhatóságának érdekében redundáns útvonalakat alakítottunk ki. A teszt során szimuláljuk egy fő hálózati útvonal kiesését, majd megfigyeljük, hogy a forgalom automatikusan átvált-e a tartalék útvonalra. Ez biztosítja, hogy a hálózat egy esetleges meghibás esetén is folyamatosan működni tudjon.
- VPN működésének ellenőrzése A távoli kapcsolatok biztonságának garantálásához VPN kapcsolatot alkalmazunk. A teszt során egy távoli eszközről VPN-en keresztül csatlakozunk a hálózathoz, majd ellenőrizzük az elérhetőséget, az adatátvitel sebességét és a kapcsolat stabilitását.
- ACL-ek hatékonyságának vizsgálata Az Access Control List-ek (ACL) beállításai szabályozzák, hogy mely forgalmak haladhatnak át az eszközökön. A tesztelés során ellenőrizzük, hogy az ACL-ek megfelelően korlátozzák-e a nem engedélyezett forgalmat, valamint biztosítják-e a kritikus szolgáltatások zavartalan elérhetőségét.
- A fent leírt tesztelési lépések biztosítják, hogy a hálózat megfelelően működjön, stabil, biztonságos és hatékony legyen a mindennapi használat során.

Csapatmunka és Projektszervezés

1. Használt Eszközök

- Trello: Feladatkezelés.
- GitHub: Konfigurációk és dokumentáció verziókövetése.
- Google Drive: Közös fájlmegosztás és szerkesztés.

2. Munkamegosztás

A feladatmegosztás az alábbiakban került kiosztásra a csapatunkban:

Motocz Edward Alexander	Kozma Csaba
Infrastruktúra kialakítása	HSRP – Harmadik rétegbeli redundancia
VLAN kialakítása	EtherChannel – Második rétegbeli redundancia
IPv4 és IPv6 címzési rendszer	WAN összeköttetés
Statikus és dinamikus forgalomirányítás	VPN kapcsolat
Statikus és dinamikus címfordítás	Programozott hálózatkonfiguráció
ACL	Zónázó tűzfal
Linux (HTTP/HTTPS szerver, automatizált mentés)	Windows (Active Directory, DHCP szerver, DNS, Fájl és nyomtatómegosztás, Kliens számítógépekre automatizált szoftvertelepítés)
	Projektszervezési eszközkezelés (Git)
Közösen elkészített	
A projekt dokumentálása, videós dokumentáció elkészítése	

Összegzés

Ez a dokumentáció bemutatja a NetSys Solutions Kft. vállalati hálózatának tervezését, kiépítését és tesztelését. A projekt célja egy biztonságos, skálázható és megbízható infrastruktúra kialakítása, amely három telephelyet foglal magában: a központi iroda Budapesten, valamint a debreceni és szegedi regionális irodákat. A hálózat kialakítása során kiemelt figyelmet fordítottunk a biztonsági mechanizmusokra, a redundanciára¹ és a hatékony menedzsment lehetőségeire.

A központi telephely biztosítja a hálózat gerincét, ahol a kulcsfontosságú szerverek és menedzsment eszközök helyezkednek el. A telephelyek közötti kapcsolatok VPN-n keresztül valósulnak meg, garantálva a biztonságos adatáramlást. A hálózat VLAN szegmentációval² van ellátva, amely elkülöníti az egyes osztályok és részlegek forgalmát.

A projekt során alkalmazott technológiák közé tartozik az OSPF-alapú dinamikus útvonalválasztás, NAT és PAT konfiguráció, valamint ACL-ek és tűzfalhasználat a forgalom biztonságos szabályozására. A szerver infrastruktúra Windows és Linux alapú kiszolgálókat tartalmaz, amelyek biztosítják az Active Directory szolgáltatásokat, DHCP és DNS konfigurációt, valamint web- és adatmentési szolgáltatásokat.

Az elkészített dokumentáció tartalmazza a telephelyek infrastruktúrájának részletes leírását, az alkalmazott eszközök listáját, a címzési tervet és a műszaki megvalósítás folyamatát. Az elvégzett tesztek megerősítették a hálózat stabilitását, megbízhatóságát és biztonsági megfelelőségét.

A projekt során megszerzett tapasztalatok megerősítették az informatikai rendszer- és alkalmazás-üzemeltetés területén szerzett ismereteket, amelyeket a jövőbeni projektek során is kamatoztatni lehet. Az elkészített infrastruktúra alapján a vállalat egy skálázható, fenntartható és biztonságos IT-környezetet kapott.

Irodalmi jegyzék

A projekt megvalósításához használt források

Hálózati tervezési alapelvek és VLAN szegmentáció:

[Network Design - Designing Advanced IP Addressing:](#)

OSPF-alapú dinamikus útvonalválasztás:

[Step-by-Step VLAN Segmentation and OSPF Routing in Cisco Environment:](#)

NAT és PAT konfiguráció:

[Introduction to NAT and PAT - NetworkLessons.com:](#)

ACL-ek és tűzfalhasználat:

[Medium Enterprise Design Profile \(MEDP\)—Network Security Design:](#)

Windows és Linux alapú szerver infrastruktúra:

[Active Directory, DNS and DHCP Configuration on Windows Server:](#)

[Zentyal: Best Linux Server with Active Directory Integration:](#)

Hálózati redundancia és menedzsment:

[What is network redundancy, why it matters, and how to build it - Meter:](#)

Eszközökbe írt konfigurációk

Különböző telephelyek eszközökre bontott konfigurációja

Központ – R1:

```
hostname Kozpont-R1
ip dhcp excluded-address 192.168.7.97
ip dhcp pool Kozpont
network 192.168.7.96 255.255.255.224
default-router 192.168.7.97
dns-server 0.0.0.0
ex
license boot module c1900 technology-package securityk9
```

```
interface GigabitEthernet0/0
ip address 192.168.7.2 255.255.255.0
ip nat outside
ex
interface GigabitEthernet0/1
ip address 192.168.7.97 255.255.255.224
ip nat inside
ex
interface GigabitEthernet0/1.10
encapsulation dot1Q 10
ip address 192.168.7.1 255.255.255.224
ex
interface GigabitEthernet0/1.20
encapsulation dot1Q 20
ip address 192.168.7.33 255.255.255.224
ex
interface GigabitEthernet0/1.30
encapsulation dot1Q 30
```

```
ip address 192.168.7.65 255.255.255.224
ex
interface Serial0/0/0
description WAN kapcsolat Iroda 1 hez
ip address 192.168.10.1 255.255.255.252
ex
interface Serial0/0/1
no ip address
clock rate 2000000
ex
interface Vlan1
no ip address
shutdown
ex
router ospf 1
log-adjacency-changes
network 192.168.7.0 0.0.0.31 area 0
network 192.168.10.0 0.0.0.3 area 0
network 192.168.20.0 0.0.0.3 area 0
ex
ip nat pool NAT_POOL 200.200.200.20 200.200.200.30 netmask 255.255.255.0
ip nat inside source list 1 pool NAT_POOL overload
ip nat inside source static 192.168.7.20 203.0.113.10
ip nat inside source static 192.168.7.21 203.0.113.11
ip nat inside source static 192.168.7.66 200.200.200.10
ip nat inside source static 192.168.7.67 200.200.200.11
ex
crypto isakmp key VPNKEY address 195.195.0.14
crypto ipsec transform-set TUNNEL esp-aes esp-sha-hmac
```

```
crypto map TUNNELMAP 10 ipsec-isakmp
set peer 195.195.0.14
set transform-set TSET
match address 101
ex
interface Tunnel0
ip address 172.16.0.1 255.255.255.252
ex
tunnel source g0/1
zone-member security outside
tunnel destination 195.195.0.14
ex
interface g0/1
ipv6 ospf 1 area 0
crypto map TUNNELMAP
router ospf 1
router-id 1.1.1.1
ex
passive-interface g0/1
network 192.168.1.0 0.0.0.255 area 0
network 172.16.0.0 0.0.0.3 area 0
router-id 1.1.1.1
access-list 101 permit gre host 195.195.0.2 host 195.195.0.14
ip route 192.168.1.0 255.255.255.0 192.168.7.2
ip route 192.168.4.0 255.255.255.0 192.168.7.2
class-map type inspect match-any tuzfal
match protocol icmp
policy-map type inspect tuzfal-policy
class type inspect tuzfal
inspect
```

```

ex
zone se
ex
zone security outside
ex
zone security inside
zone-pair security bentrol-kintre source inside destination outside
service-policy type inside tuzfal_policy
ex
int g0/0
zone-member security inside
int g0/1
zone-member security outside
ex
ip access-list extended VPN_ACL
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 permit 192.168.4.0 0.0.0.255
access-list 1 permit 192.168.7.0 0.0.0.127
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.6.0 0.0.0.255
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.4.0 0.0.0.255
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.3.0 0.0.0.255
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.2.0 0.0.0.255
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.5.0 0.0.0.255
ex
do w

```

Központ – ME Switch:

```

hostname Kozpont-SW
interface FastEthernet0/1

```



```
switchport access vlan 30
switchport trunk encapsulation dot1q
switchport mode trunk
```

ex

```
interface FastEthernet0/2
switchport access vlan 10
switchport trunk encapsulation dot1q
switchport mode trunk
```

ex

```
interface FastEthernet0/3
switchport access vlan 10
switchport mode access
```

ex

```
interface FastEthernet0/4
switchport access vlan 10
switchport mode access
```

ex

```
interface FastEthernet0/5
switchport access vlan 30
switchport mode access
```

ex

```
interface FastEthernet0/6
switchport access vlan 30
switchport mode access
```

ex

```
interface Vlan1
no ip address
shutdown
```

ex

```
interface Vlan10
```

```
ip address 192.168.7.1 255.255.255.224
```

```
ex
```

```
interface Vlan20
```

```
ip address 192.168.7.33 255.255.255.224
```

```
ex
```

```
interface Vlan30
```

```
ip address 192.168.7.65 255.255.255.224
```

```
ex
```

```
do w
```

Iroda 1 – R1:

```
hostname Iroda-1-R1
```

```
interface FastEthernet0/1
```

```
ip address 192.168.1.1 255.255.255.0
```

```
standby 1 ip 192.168.1.7
```

```
standby 1 priority 100
```

```
standby 1 preempt
```

```
ex
```

```
interface Serial0/1/0
```

```
description Kapcsolat a kozponti routerhez
```

```
ip address 192.168.10.2 255.255.255.252
```

```
clock rate 2000000
```

```
ex
```

```
interface Serial0/1/1
```

```
description Kapcsolat Iroda 2 routerhez
```

```
ip address 192.168.20.1 255.255.255.252
```

```
ex
```

```
interface FastEthernet1/0
```

```
ip address 192.168.1.6
```

ex

interface Vlan1

no ip address

shutdown

ex

crypto isakmp key VPNKEY address 195.195.0.14

crypto ipsec transform-set TUNNEL esp-aes esp-sha-hmac

crypto map TUNNELMAP 10 ipsec-isakmp

set peer 195.195.0.14

set transform-set TSET

match address 101

ex

interface Tunnel0

ip address 172.16.0.1 255.255.255.252

ex

tunnel source g0/1

tunnel destination 195.195.0.14

ex

interface fa0/0

crypto map TUNNELMAP

router ospf 1

router-id 1.1.1.1

router ospf 1

log-adjacency-changes

network 192.168.1.0 0.0.0.255 area 0

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

network 192.168.10.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

Iroda 1 – R2:

hostname Iroda-1-R2

interface FastEthernet0/0

ip address 192.168.1.5 255.255.255.0

standby 1 ip 192.168.1.7

standby 1 priority 110

standby 1 preempt

ex

interface FastEthernet0/1

ip address 192.168.1.2 255.255.255.0

ex

interface Vlan1

no ip address

shutdown

ex

router ospf 1

log-adjacency-changes

network 192.168.1.0 0.0.0.255 area 0

ex

ip route 192.168.7.0 255.255.255.0 192.168.1.1

ip route 192.168.4.0 255.255.255.0 192.168.1.1

access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.1.0 0.0.0.255

access-list 100 permit ip 192.168.6.0 0.0.0.255 192.168.1.0 0.0.0.255

do w

Iroda 1 – SW1:

hostname Iroda-1-SW1

ip dhcp excluded-address 192.168.1.1 192.168.1.2

interface Port-channel1

switchport access vlan 20

switchport mode trunk

switchport nonegotiate

ex

interface FastEthernet0/1

switchport mode access

switchport nonegotiate

ex

interface FastEthernet0/2

switchport access vlan 20

switchport mode trunk

switchport nonegotiate

channel-group 1 mode active

ex

interface FastEthernet0/3

switchport access vlan 20

switchport mode trunk

switchport nonegotiate

channel-group 1 mode active

ex

interface FastEthernet0/6

switchport mode trunk

ex

interface FastEthernet0/7

switchport mode trunk

ex

```
interface Vlan10
```

```
ip address 192.168.1.1 255.255.255.0
```

```
ex
```

```
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.1.0 0.0.0.255
```

```
access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.4.0 0.0.0.255
```

Iroda 1 – SW2:

```
hostname Iroda-1-SW2
```

```
interface Port-channel1
```

```
switchport mode trunk
```

```
ex
```

```
interface FastEthernet0/1
```

```
switchport mode trunk
```

```
channel-group 1 mode passive
```

```
ex
```

```
interface FastEthernet0/2
```

```
channel-group 1 mode passive
```

```
ex
```

```
do w
```

Iroda 2 – R1:

```
hostname Iroda-2-Router1
```

```
ip dhcp excluded-address 192.168.4.1
```

```
ip dhcp pool Iroda2-Gep
```

```
network 192.168.4.0 255.255.255.0
```

```
default-router 192.168.4.1
```

```
dns-server 0.0.0.0
```

```
ex
```

```
ipv6 unicast-routing
```

```
ipv6 dhcp pool Iroda2GepV6
  address prefix 2001:db8:4::/64 lifetime 172800 86400
  dns-server 2001:4860:4860::8888
ex
crypto isakmp policy 10
  encr aes
  authentication pre-share
  group 5
ex
interface FastEthernet0/0
  no ip address
ex
interface FastEthernet0/1
  ip address 192.168.4.1 255.255.255.0
  ipv6 address 2001:DB8:4::1/64
  ipv6 nd other-config-flag
  ipv6 dhcp server Iroda2GepV6
ex
interface Serial0/3/0
  description Kapcsolat Iroda 1 routerhez
  ip address 192.168.20.2 255.255.255.252
  clock rate 2000000
ex
interface Serial0/3/1
  no ip address
  clock rate 2000000
ex
interface Vlan1
  no ip address
  shutdown
```

ex

passive-interface fa0/1

network 192.168.4.0 0.0.0.255 area 0

network 172.16.0.0 0.0.0.3 area 0

access-list 101 permit gre host 195.195.0.14 host 195.195.0.2

router ospf 1

network 192.168.4.0 0.0.0.255 area 0

network 192.168.20.0 0.0.0.255 area 0

network 192.168.10.0 0.0.0.3 area 0

ex

access-list 100 permit ip 192.168.7.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.4.0 0.0.0.255

access-list 100 permit ip 192.168.6.0 0.0.0.255 192.168.4.0 0.0.0.255

do wr

ex

NYILATKOZAT

Alulírott

Név:

OM azonosító:

jelen nyilatkozat aláírásával kijelentem, hogy a portfólió önálló munkám eredménye, mások által írt részeket a megfelelő idézés nélkül nem használtam fel.

Debrecen, 20..... év hónap

.....

a vizsgázó aláírása

3. sz. melléklet

NYILATKOZAT

Alulírott

Név:

OM azonosító:

jelen nyilatkozat aláírásával kijelentem, hogy a portfólió a vizsgához kapcsolódó értékelésre a vizsgabizottság megtekintheti, valamint a vizsgaközpont, mint adatkezelő a portfólióban fellelhető személyes adataimat a vizsgadokumentáció őrzési idejéig, vagy visszavonásáig kezelheti és harmadik fél számára kizárólag az előzetes hozzájárulásommal adhatja át.

Az adatkezelés jogalapja: Az Európai Parlament és a Tanács (EU) 2016/679 számú a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/ EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR, általános adatvédelmi rendelet) rendelet 6. cikk (1) bekezdés a) pontja szerinti érintett hozzájárulás személyes adatok meghatározott céljából történő kezeléséhez.

Debrecen, 20..... év hónap

.....

a vizsgázó aláírása

Portfólió haladási lap

Név:	
Osztályfőnök:	
Ágazat:	
Szakma:	
Szakma kódja:	

Portfólió munkaanyagok:

1. Kötelező tartalmi elemek bemutatása megtörtént:

Sorszám	Osztály	Dokumentum	Dátum	Aláírás
1.				
2.				
3.				
4.				
5.				

2. Választott tartalmi elemek bemutatása megtörtént:

Sorszám	Osztály	Dokumentum	Dátum	Aláírás
1.				
2.				
3.				
4.				
5.				
6.				

Portfólió Értékelő Lap

Konzultációs időpontok:

Dátum	Készültségi fok	Támogató oktató aláírása

A Támogató oktató értékelése:

Dátum: Debrecen, 20..... . hó..... nap

.....
aláírás

Tanuló-támogató összerendelés

Osztály:

[illegible]