* + 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**

Cégbemutatás 3

Telephelyek bemutatása 5

Telephelyek eszközeinek listája 8

Alkalmazott technológiák 9

Címzési terv és táblázat 11

Hálózati infrastruktúra 13

Hálózat műszaki megvalósítása 16

Szerverek konfigurációja 20

Tesztelés és dokumentáció 33

Feladatmegosztás 34

Összegzés 35

📄 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.

Cégbemutatás

### **Cég neve:**

**NetSys Solutions Kft.**

### **Székhely:**

Budapest, Magyarország

### **Telephelyek:**

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

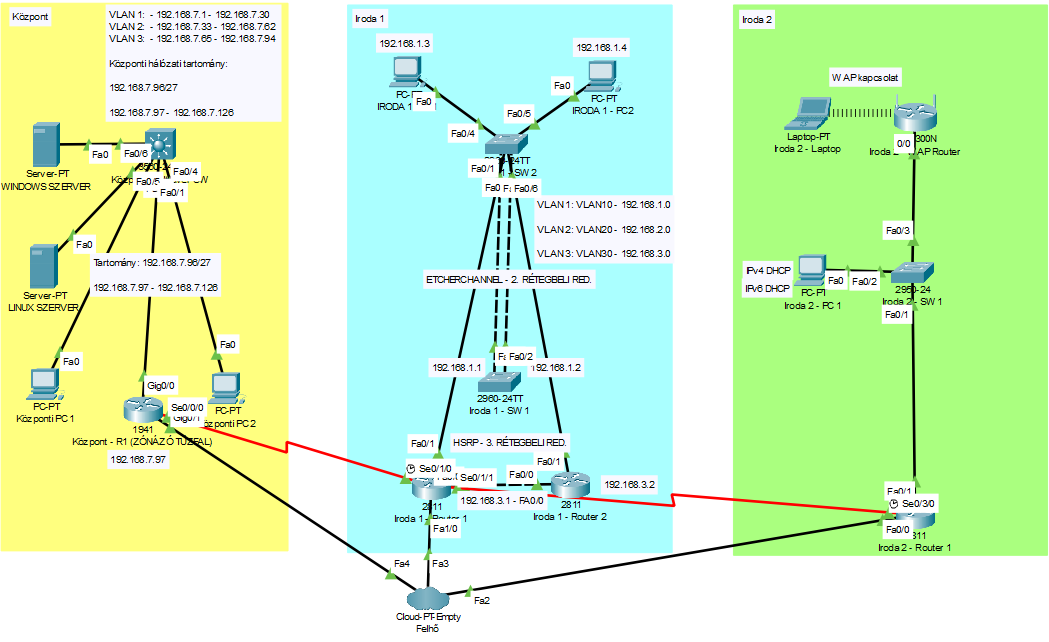
### **Cég profilja:**

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

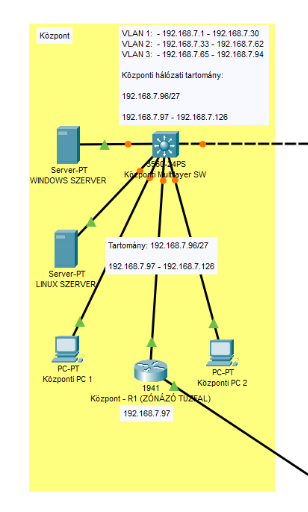
### ****Projekt célja:****

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

****

**2**. ábra – Központi telephely

1. **Központi Iroda – Budapest**

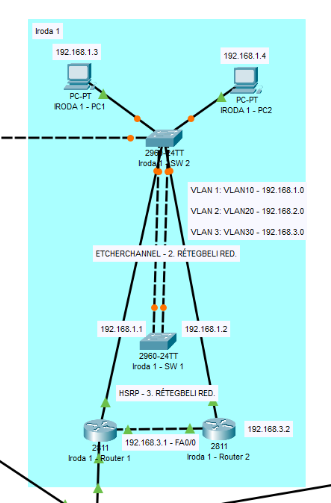
- Ez a vállalat elsődleges székhelye, ahol az itt tartózkodó rendszergazdák, vezetőségi, valamint IT-infrastruktúra menedzsment feladatokat látják el.

- 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



3. ábra – Iroda 1

# 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:

# Több VLAN (irodai, vendég, fejlesztői)

# Redundáns kapcsolatok és eszközök (EtherChannel, HSRP)

# IPv4 és IPv6 címzés

# VPN kapcsolat a központtal

# Központi router és switch redundáns kialakításban

# 

4. ábra – Iroda 2

# 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 címzés

# VPN kapcsolat a központi telephelyhez

# DHCP kiosztás helyben

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 eszközeninek 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 laptop

# 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.
* **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, hogy csökkentsük az emberi hibák lehetőségét és egyszerűsítsük a karbantartást.

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 |
| SW1-2 VLAN 10 | 192.168.1.0 | /24 |
| SW1-2 VLAN 20 | 192.168.2.0 | /24 |
| SW1-2 VLAN 30 | 192.168.3.0 | /24 |
| Router 1 fa0/1 | 192.168.1.2 | /24 |
| Router 1 fa 0/ | 192.168.3.1 | /24 |
| Router 2 fa 0/0 | 192.168.3.2 | /24 |
| Router 2 fa 0/1 | 192.168.2.1 | /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

## Telephelyek

### Telephelyek száma: 3

* + **Főbb elemek:**
    - Központ
    - Iroda 1
    - Iroda 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
* Az Iroda 1 nevű telephelyen 2 VLAN kerül kialakításra.
  + VLAN1: VLAN10 – 192.168.1.0
  + VLAN2: VLAN20 – 192.168.2.0
  + VLAN3: VLAN30 – 192.168.3.0

## 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

## Vezeték nélküli hálózat

Az AP (WAN) kialakítása az Iroda 2 telephelyen kerül kialakításra amely az ott elhelyezett Laptoppal és az Iroda 2 switch-el kommunikál.

1. **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)
    - Vendéghálózat (külön VLAN-hoz kötve, internet eléréssel)

Hálózat műszaki megvalósítása

## 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).

### Sávszélesség-növelés: A több link egyesítésével összesített sávszélességet kapunk (pl. két 100 Mbps link esetén akár 200 Mbps-ot).

### Terheléselosztás (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.

## 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.

## 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.

## 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.

## 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.

### 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.

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 az Rendszergazdákisztráció 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 rendszerRendszergazdákisztrációt 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 Rendszergazdák adminisztrációs terheket, miközben biztosítja a hálózat zökkenőmentes működését.

**d) Fájlszerver – Központi fájlmegosztás**

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

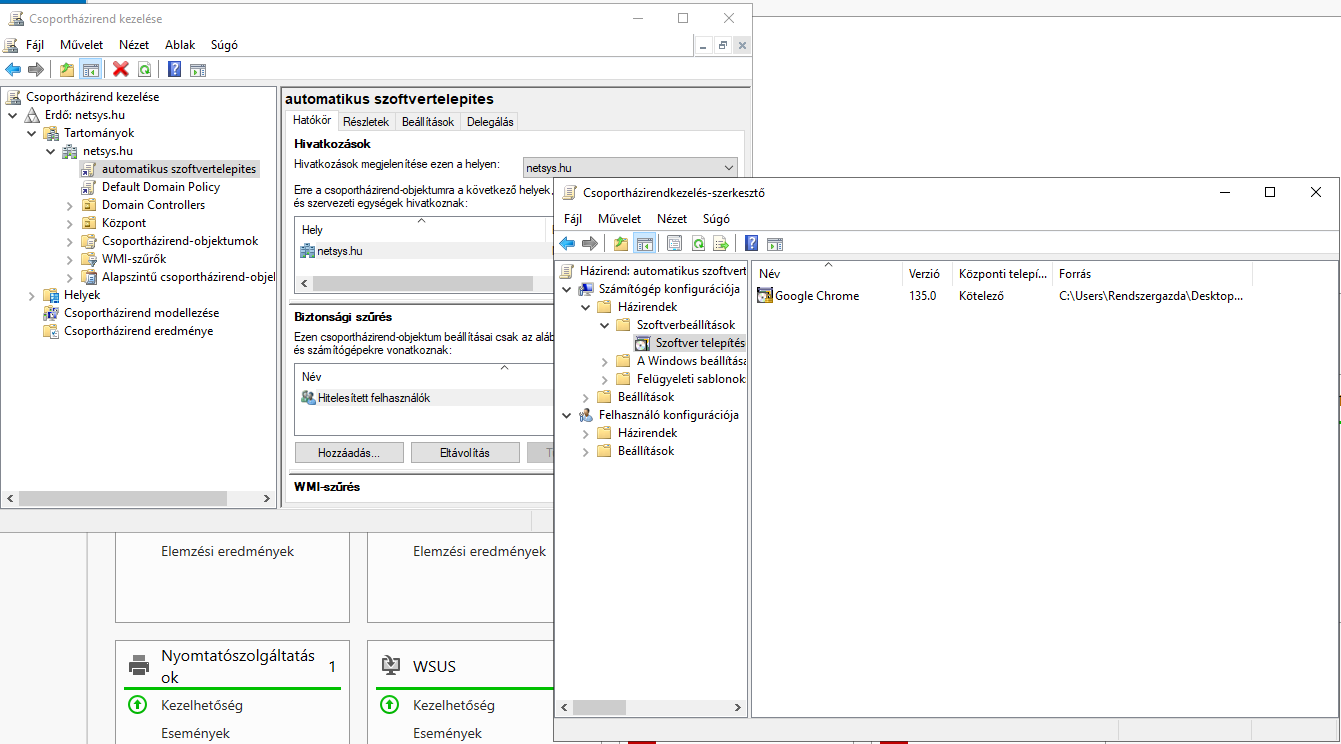
**e) Nyomtatómegosztás – Nyomtatók központi kezelése**

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.



5. 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 és WSUS szolgáltatásokat állítottuk 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 webszerver 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](http://www.netsys.hu)
* **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.

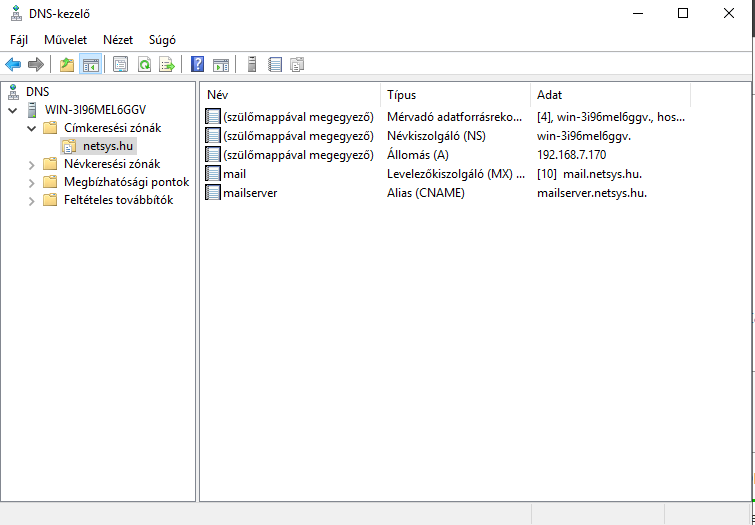
* **CNAME rekord (Canonical Name Record)**

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.example.com domain név a mailserver.example.com-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.



6. 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.
* **Felhasználói csoportok létrehozása**
  + **Rendszergazdák Csoport Létrehozása:**

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

* **Rendszergazdák 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](mailto:kpista@netsys.hu)
* **Beállítások:** Pista rendszergazdai jogosultságokkal rendelkezik, így teljes hozzáférése van a szerverekhez és a hálózati erőforrásokhoz.
  + **Felhasználónév:** nzsofia
  + **Teljes név:** Nagy Zsófia
  + **E-mail cím:** [nzsofia@netsys.hu](mailto:nzsofia@netsys.hu)
* **Beállítások:** Zsófia szintén rendszergazdai 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 rendszergazdai feladatot is.
* **Alkalmazott Csoport Létrehozása:**

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

* **Felhasználói csoport és felhasználók:**
* **Csoport neve:**
  + Alkalmazott

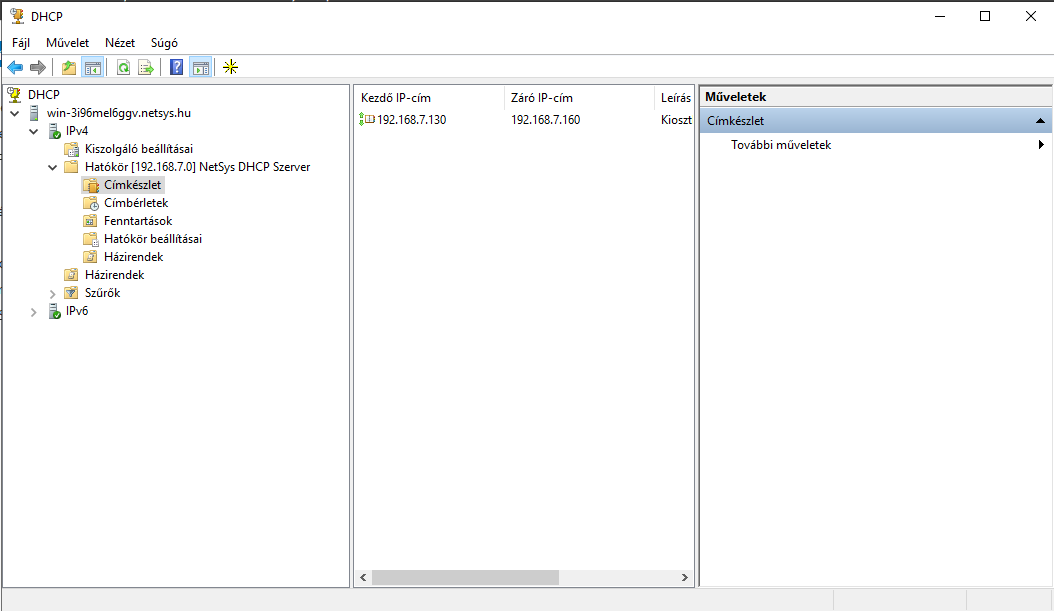
Ezt a csoportot létrehoztuk, és minden nem rendszargazdai felhasználót hozzáadtuk.

* **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 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



7. ábra – DHCP Hatókör

**Linux szerver telepítése**

- Először letöltjük az Ubuntu szerver ISO-t, majd VirtualBoxban az új gombra nyomunk és megadjuk a következőket:

**Felhasználónév**: NetSys

**Jelszó**: projekt

**Hostname**: NetSys

**Domain** **name**: netsys.hu

**Típus**: Linux

**Ubuntu** **ISO** **fájl** **csatolása**: Ubuntu 24.04 (64-bit)

- Majd beállítjuk a memóriát, ami 9670MB (szabványos memóriaméret, 2 hatványa legyen) és a processzort, ami 6 db. Létrehozunk egy virtuális merevlemezt, a formátumot meghagyjuk VDI-nak (Virtual Disk Image).

- Ezután elindítjuk a virtuális gépet és miután betöltötte az Ubuntu telepítőt az ISO fájl segítségével akkor megjelenik az Ubuntu telepítő képernyője és rányomunk arra, hogy Install Ubuntu, a telepítés nyelve English (angol), a billentyűzet nyelve pedig Hungary (magyar).

- Miután ezekkel végeztünk a telepítő elkezdi a fájlok másolását és a rendszer telepítését, ennek a végén kérni fogja, hogy indítsuk újra ezért rányomunk arra, hogy Restart Now.

- Amikor a rendszer újraindul, akkor bejelentkezhetünk a létrehozott felhasználó és jelszó segítségével.

**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**

1. **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.

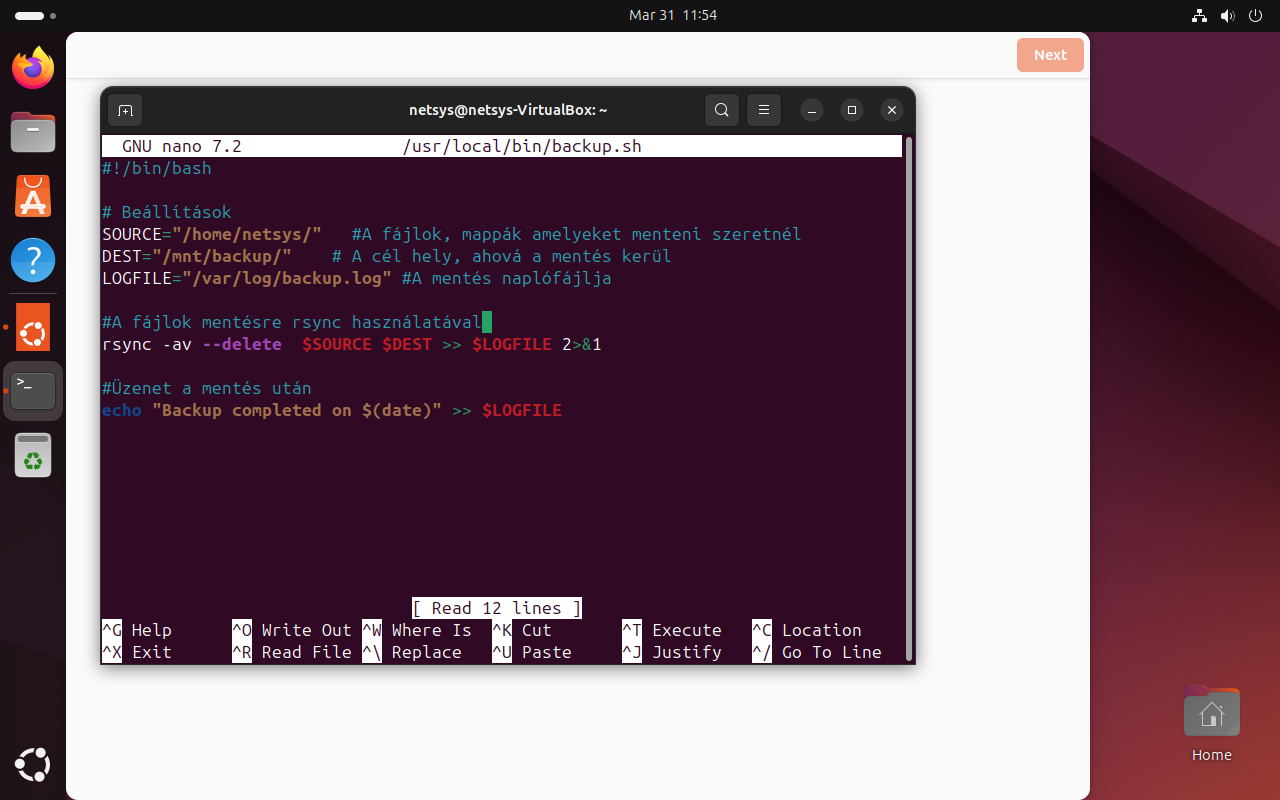
- Létrehoztunk egy egyszerű szkriptet, amely a fájlokat másolja egy biztonságos mentési helyre (pl. egy külső meghajtó vagy egy távoli szerver).

- Beléptünk a bin könyvtárba, és létrehoztunk egy szkriptet:

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

8. ábra – Mentési szkript

- A következő tartalmat írtuk be a szkriptbe:



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

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

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

**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. Mentés tesztelése**

- Manuálisan futtathatjuk a szkriptet, hogy ellenőrizzük, működik-e:

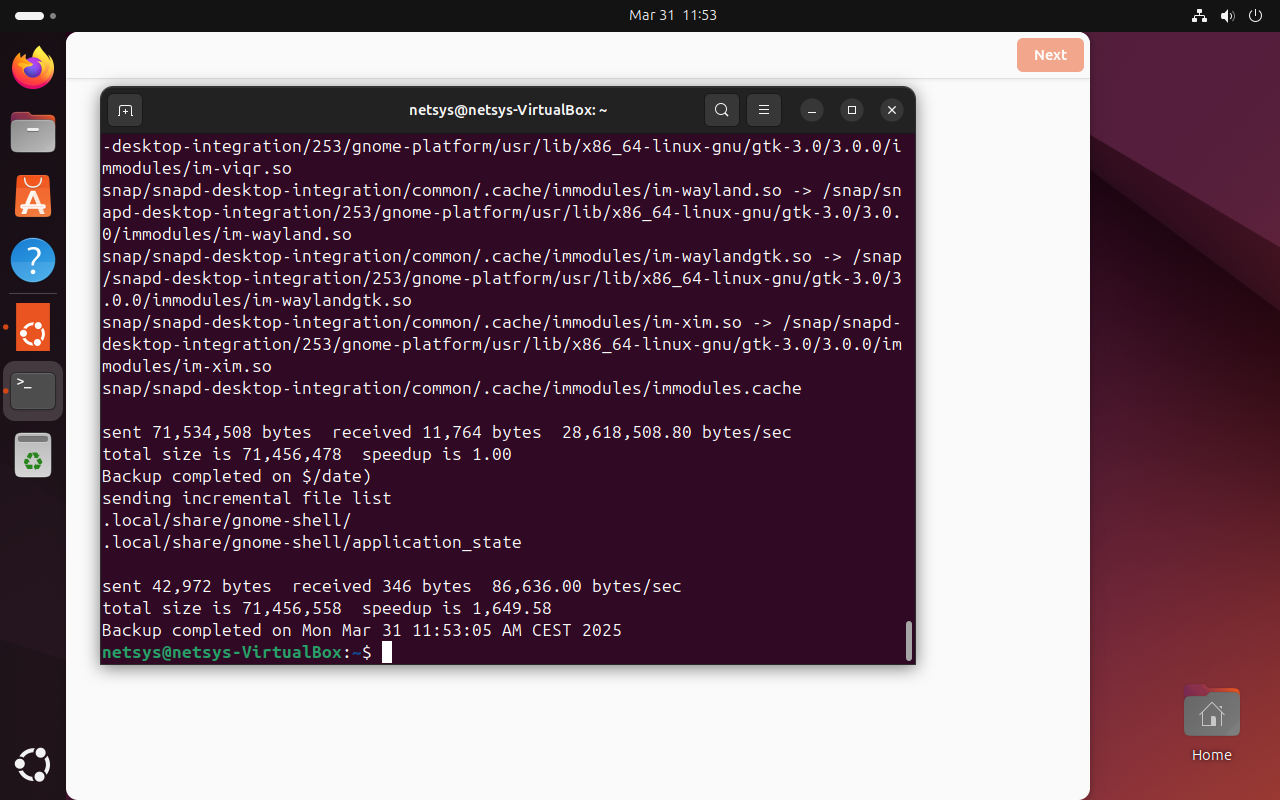
**sudo /usr/local/bin/backup.sh**

**6. 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**

****

**9**. ábra - Ellenőrzés

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

**✅ Az rsync működött → Nagy mennyiségű bájtot küldött (sent 71,534,508 bytes).**

**✅ A teljes méret rendben van → total size is 71,456,478.**

**✅ A sebesség is megfelelő → speedup is 1.00.**

**✅ A napló végén ott van a mentés befejezéséről szóló üzenet (Backup completed)**

**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

## 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 eszközről a másikra. Továbbá, figyeljük a válaszidőt és az esetleges csomagvesztést, amely hálózati problémákra utalhat.
  + Routerek 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 eszközről 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

## Használt Eszközök

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

1. **Munkamegosztás**

A feladatmegosztás az alábbiakban került kiosztásra a csapatunkban:

* Kozma Csaba a Központ és a Windows szerver kialakításáért, felkonfigurálásáért felelt.
* Motocz Edward az Iroda 1 és Linux szerver kialakításáért, felkonfigurálásért felelt.
* Az Iroda 2 kialakításában a WAN kapcsolat létrehozását, routerek konfigurációját közösen végeztük el.

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 redundanciára[[1]](#footnote-1) 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 szegmentációval[[2]](#footnote-2) 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 tesztelések 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](https://www.howtonetwork.com/technical/network-management/network-design/):

*OSPF-alapú dinamikus útvonalválasztás:*

[Step-by-Step VLAN Segmentation and OSPF Routing in Cisco Environment](https://www.youtube.com/watch?v=Lnw5tAaVt4o):

*NAT és PAT konfiguráció:*

[Introduction to NAT and PAT - NetworkLessons.com:](https://networklessons.com/ip-services/introduction-to-nat-and-pat?utm_source)

*ACL-ek és tűzfalhasználat:*

[Medium Enterprise Design Profile (MEDP)—Network Security Design:](https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/chap5sba.pdf?utm_source)

*Windows és Linux alapú szerver infrastruktúra:*

[Active Directory, DNS and DHCP Configuration on Windows Server:](https://www.linkedin.com/pulse/active-directory-dns-dhcp-configuration-windows-server-kawushika-v0k4c?utm_source)

[Zentyal: Best Linux Server with Active Directory Integration:](https://www.zentyal.com/news/integrating-linux-into-your-active-directory-environment-a-detailed-guide/?utm_source)

*Hálózati redundancia és menedzsment:*

[What is network redundancy, why it matters, and how to build it - Meter](https://www.meter.com/resources/network-redundancy?utm_source):

**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 udi pid CISCO1941/K9 sn FTX1524235A-

license boot module c1900 technology-package securityk9

interface GigabitEthernet0/0

ip address 192.168.6.1 255.255.255.0

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

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

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

crypto isakmp key projekt address 192.168.1.1

crypto isakmp key projekt address 192.168.4.1

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

mac-address 0001.631c.0b01

ip address 192.168.7.1 255.255.255.224

ex

interface Vlan20

mac-address 0001.631c.0b02

ip address 192.168.7.33 255.255.255.224

ex

interface Vlan30

mac-address 0001.631c.0b03

ip address 192.168.7.65 255.255.255.224

ex

do w

**Iroda 1 – R1:**

hostname Iroda-1-R1

interface FastEthernet0/0

ip address 192.168.3.1 255.255.255.0

duplex auto

speed auto

standby 1 ip 192.168.3.254

standby 1 priority 110

standby 1 preempt

ex

interface FastEthernet0/1

ip address 192.168.1.2 255.255.255.0

duplex auto

speed auto

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

no ip address

duplex auto

speed auto

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

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 192.168.3.2 255.255.255.0

standby 1 ip 192.168.3.254

ex

interface FastEthernet0/1

ip address 192.168.2.1 255.255.255.0

ex

interface Vlan1

no ip address

shutdown

ex

router ospf 1

log-adjacency-changes

network 192.168.2.0 0.0.0.255 area 0

network 192.168.3.0 0.0.0.255 area 0

ex

ip route 192.168.6.0 255.255.255.0 192.168.3.1

ip route 192.168.4.0 255.255.255.0 192.168.3.1

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 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 100 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 100 permit ip 192.168.3.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 100 permit ip 192.168.4.0 0.0.0.255 192.168.3.0 0.0.0.255

access-list 100 permit ip 192.168.6.0 0.0.0.255 192.168.3.0 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

crypto isakmp key projekt address 192.168.6.1

crypto ipsec transform-set VPN\_TRANS esp-aes 256 esp-sha-hmac

crypto map VPN\_MAP 10 ipsec-isakmp

set peer 192.168.7.1

set transform-set VPN\_TRANS

match address 100

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

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 w

2. sz. melléklet

**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 ……………………… hó ………..nap

…………………………………

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 ……………………… hó ………..nap

…………………………………

a vizsgázó aláírása

4. sz. melléklet

**Portfólió haladási lap**

|  |  |
| --- | --- |
| Név: |  |
| Osztályfőnök: |  |
| Ágazat: |  |
| Szakma: |  |
| Szakma kódja: |  |

Portfólió munkaanyagok:

1. **Kötelező tartalmi elemek bemutatása megtörtént:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sorszám | Osztály | Dokumentum | Dátum | Aláírás |
| 1. |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. **Választott tartalmi elemek bemutatása megtörtént:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sorszám | Osztály | Dokumentum | Dátum | Aláírás |
| 1. |  |  |  |  |
| 2. |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

5. melléklet

**Portfólió Értékelő Lap**

Konzultációs időpontok:

|  |  |  |
| --- | --- | --- |
| Dátum | Készültségi fok | Támogató oktató aláírása |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

A Támogató oktató értékelése:

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

………………………

aláírás

6. melléklet

**Tanuó-támogató összerendelés**

|  |  |
| --- | --- |
| Osztály: |  |
| Tanuló neve | Támogató/ elsődleges bíráló |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

1. [↑](#footnote-ref-1)
2. [↑](#footnote-ref-2)