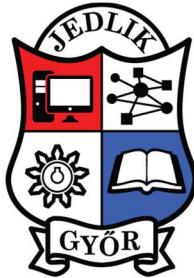




győri szakképzési centrum

Jedlik Ányos
Gépipari és Informatikai
Technikum és Kollégium



9021 Győr, Szent István út 7.

tel: +36 (96) 529-480

fax: +36 (96) 529-448

OM: 203037/003

e-mail: jedlik@jedlik.eu

web: www.jedlik.eu

Záródolgozat feladatkiírás

Tanuló(k) neve: Nagy-Raffay Barnabás, Sölét Tamás
Képzés: nappali munkarend
Szak: 5 0612 12 02 Informatikai rendszer- és alkalmazás-üzemeltető
technikus

A záródolgozat címe: MonkeBricks hálózat

Konzulens: Czita Zsuzsanna
Beadási határidő: 2025. 04. 15.

Győr, 2025. 02. 01

Módos Gábor

igazgató



győri szakképzési centrum

Jedlik Ányos
Gépipari és Informatikai
Technikum és Kollégium



9021 Győr, Szent István út 7.

tel: +36 (96) 529-480

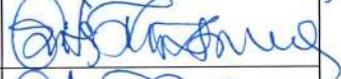
fax: +36 (96) 529-448

OM: 203037/003

e-mail: jedlik@jedlik.eu

www.jedlik.eu

Konzultációs lap

	A konzultáció		Konzulens aláírása
	ideje	témája	
1.	2025.02.15.	Témaválasztás és specifikáció	
2.	2025.03.14.	Záródolgozat készültségi fokának értékelése	
3.	2025.04.15.	Dokumentáció véglegesítése	

Tulajdonosi nyilatkozat

Ez a dolgozat a saját munkánk eredménye. Dolgozatunk azon részeit, melyeket más szerzők munkájából vettünk át, egyértelműen megjelöltük.

Ha kiderülne, hogy ez a nyilatkozat valóltan, tudomásul vesszük, hogy a szakmai vizsgabizottság a szakmai vizsgáról kizárt minket és szakmai vizsgát csak új záródolgozat készítése után tehetünk.

Győr, 2025. április 15.



tanuló aláírása



tanuló aláírása



MonkeBricks

Hálózati Dokumentáció

Nagy-Raffay Barnabás

Sölét Tamás

TARTALOM

1. A projekt leírása.....	1
1.1 A cég bemutatása és tervei	1
1.2 A csapatmunka leírása	1
2. A hálózat felépítése.....	5
2.1 Logikai felépítés	5
2.2 Fizikai topológia.....	6
2.2.1 Központ	6
2.2.2 Gyártási telephelyek	7
2.2 Telephelyek.....	10
2.2.1 Központi iroda.....	10
2.2.2 Markotabödögei telephely	12
2.2.3 Taktaharkányi telephely.....	13
2.3 IP címzés	15
2.3.1 IPv4	15
2.3.2 IPv6	16
2.4 VLAN felosztás.....	16
2.5 Redundancia	17
2.5.1 Második rétegbeli redundancia	17
2.5.2 Harmadik rétegbeli redundancia	18
2.5.3 Szolgáltatásredundancia	19
2.6 Forgalomirányítás.....	21
2.6.1 VPN	21
2.6.2 Statikus forgalomirányítás.....	27
2.6.3 Dinamikus forgalomirányítás	27
2.7 BIZTONSÁG	28
2.7.1 Statikus NAT	28

2.7.2 PAT	30
2.7.3 Tűzfal szabályok.....	31
2.8 VEZETÉKNÉLKÜLI HÁLÓZATOK.....	32
3. Szerverek.....	33
3.1 A szerverek leírása.....	33
3.2 Szolgáltatások.....	33
3.2.1 Hyper-V.....	33
3.2.2 AD	34
3.2.3 DNS	36
3.2.4 DHCP	38
3.2.5 Fájl szerver	38
3.2.6 VSS.....	39
3.2.7 Nyomtatószerver	40
3.2.8 WEB	41
3.2.9 NTP	45
3.2.10 Zabbix.....	45
3.2.11 Microsoft Exchange Server	48
3.2.11 Hálózatautomatizálás.....	50
4. Felhasznált eszközök.....	54
4.1 HÁLÓZATI ESZKÖZÖK	54
4.1.1 Routerek, tűzfalak	54
4.1.2 Switchek	55
4.1.3 Szerverek	55
4.1.4 AP-k.....	56
4.1.5 Szünetmentes tápegységek	56
4.2 Egyéb eszközök.....	57
4.2.1 PC-k, Laptopok	57

4.2.2 Nyomtatók	58
4.2.3 Telefonok	59
4.2.4 Kamerák	59
4.2.5 Kábelek (UTP, optika).....	60
4.2.6 SFP modulok	61
5. Árajánlat	62
5.1 Internet előfizetés	63
5.1.1 Központi iroda internet csomag	63
5.1.2 Telephelyi internet csomag.....	63
6. Tesztelés	64
6.1 Ping tesztelés	64
6.2 Active Directory tesztelés.....	65
6.3 Juniper Mist tesztelés	66
6.4 Hálózati tesztek	68
6.5 WiFi tesztelés	68

1. A PROJEKT LEÍRÁSA

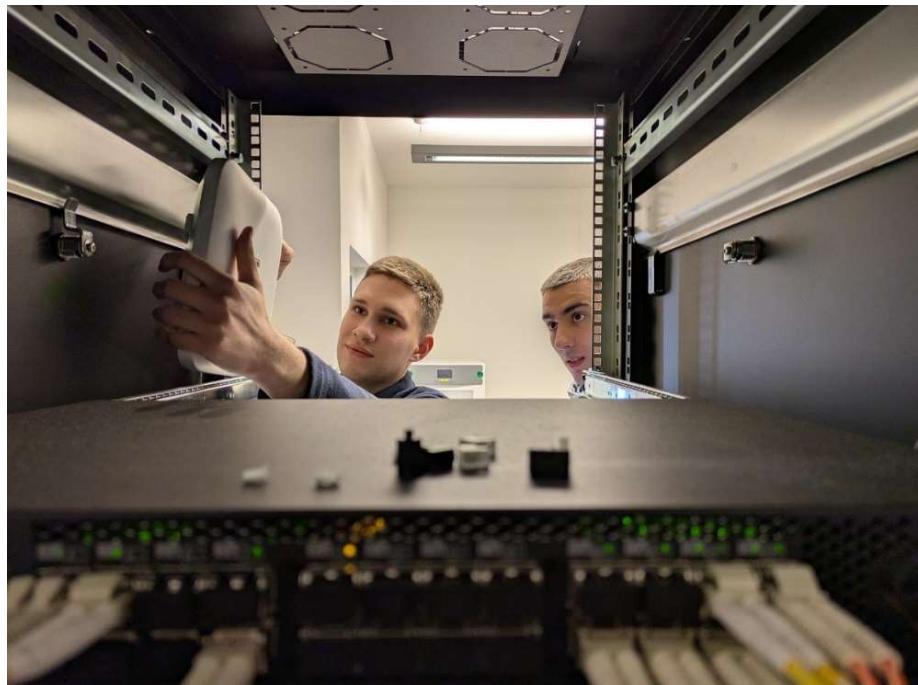
1.1 A CÉG BEMUTATÁSA ÉS TERVEI

A MonkeBricks Kft. Magyarország legnagyobb és legsikeresebb építőipari cége, melynek fő profilja az építőelemek gyártása. A vállalat 3 telephellyel rendelkezik: Győrben található egy irodaépület, a cég székhelye, Markotabödögén és Taktaharkányban pedig egy-egy téglagyár található. Csapatunkat azzal a feladattal bízták meg, hogy egy olyan hibatűrő hálózatot hozzon létre, amely összeköttetést biztosít a telephelyek között.

1.2 A CSAPATMUNKA LEÍRÁSA

Az egész projektet a Leier-nél töltött duális képzés keretében terveztük és valósítottuk meg. A cég szakemberei végig segítették csapatunkat megfelelő tanácsokkal, illetve megosztották tapasztalataikat, így még valósághűbb szempontoknak kellett megfelelnie a végeredménynek. Külön köszönet illeti Varga Bálintot, Varga Bencét és Szabó Rolandot, akik kiemelkedően sokat segítettek. Emellett fontos megemlíteni Czita Zsuzsanna nélkülözhetetlen szerepét a projektben, aki az informatikai osztály vezetőjeként biztosította a több, mint megfelelő körülményeket és eszközöket csapatunk számára.

A csapatunk munka közben az alábbi ábrán látható. (1. ábra)



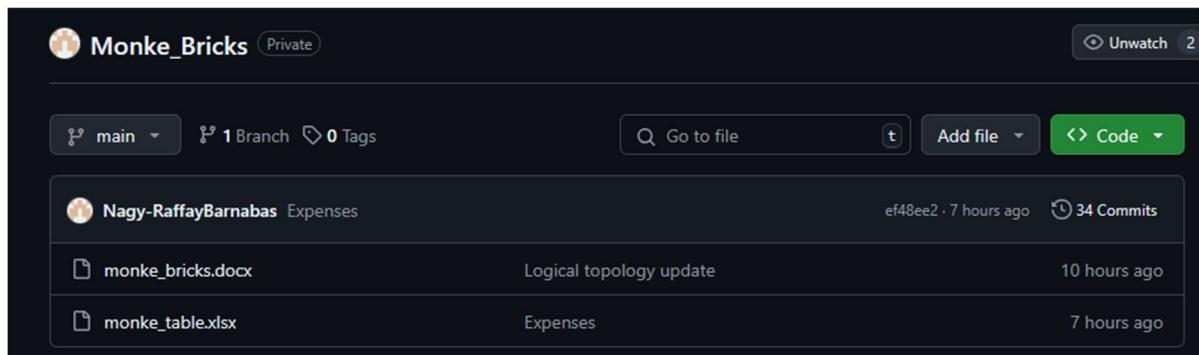
1. ábra: A csapat munka közben

A projekt alatt, amikor nem voltunk jelen az irodában, a Slack nevű kommunikációs platformot használtuk. A fő előnyei közé tartozik a könnyű csoportos üzenetküldés, fájlmegosztás, valamint a különböző alkalmazásokkal való integráció, amelyek megkönnyítik a munkafolyamatokat. Ezen kívül lehetőséget ad a különböző csatornák létrehozására, így a projektek és témák egyszerűen kezelhetők. A Slack felülete az alábbi ábrán látható. (2. ábra)



2. ábra: Slack szakmai kommunikáció

A munka során a fájlokat a GitHub-on tároltuk, így volt lehetőségünk távolról is folyamatosan hozzájuk férni, és nyomon követni a projekt aktuális állását. A tervezést, megvalósítást és a dokumentálást közösen végeztük el, így mindenki a lehető legtöbb szakmai gyakorlatot sajátítottuk el. A GitHub repository a 3. ábra látható.

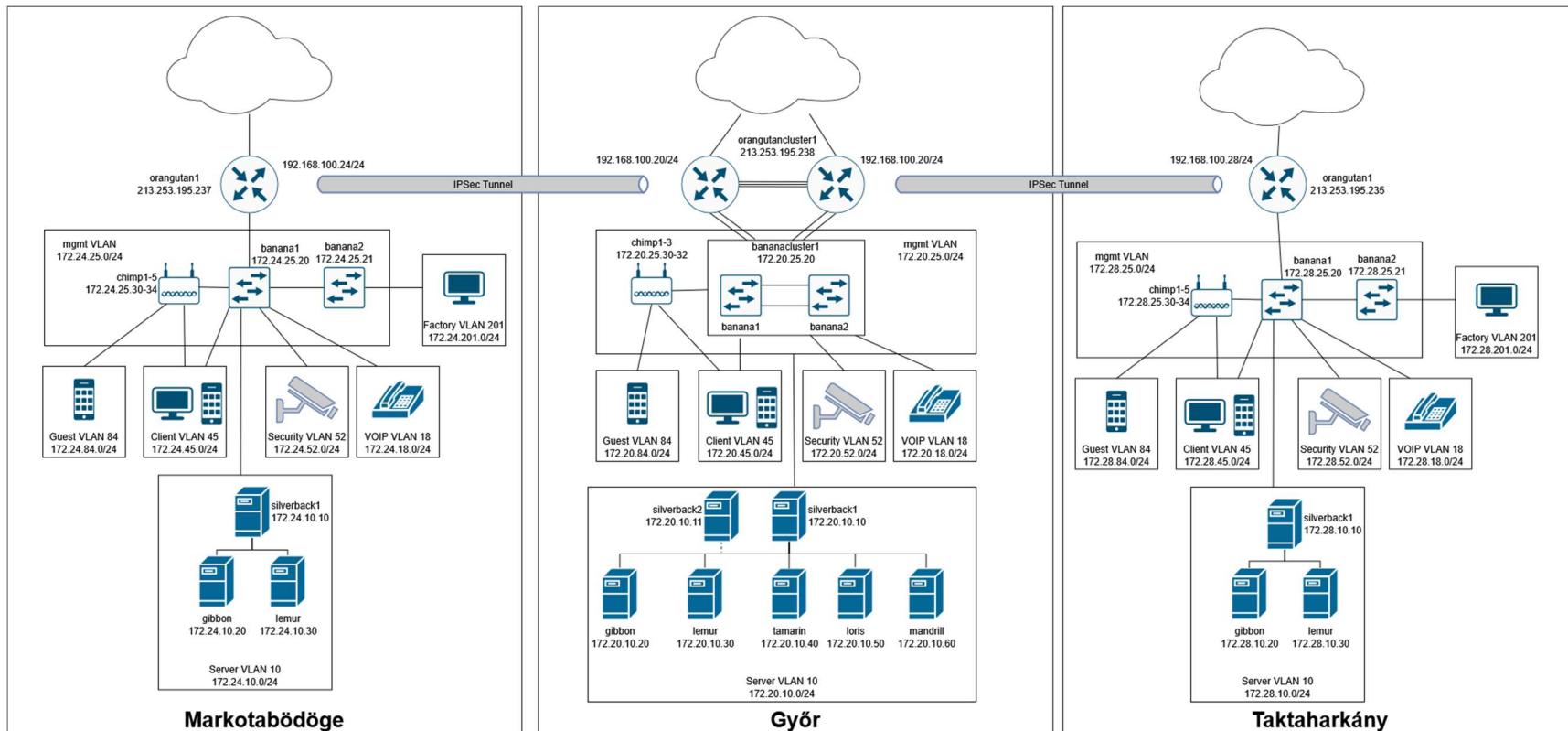


3. ábra: GitHub repo

2. A HÁLÓZAT FELÉPÍTÉSE

2.1 LOGIKAI FELÉPÍTÉS

A teljes hálózat logikai topológiája az alábbi ábrán látható. (4. ábra)

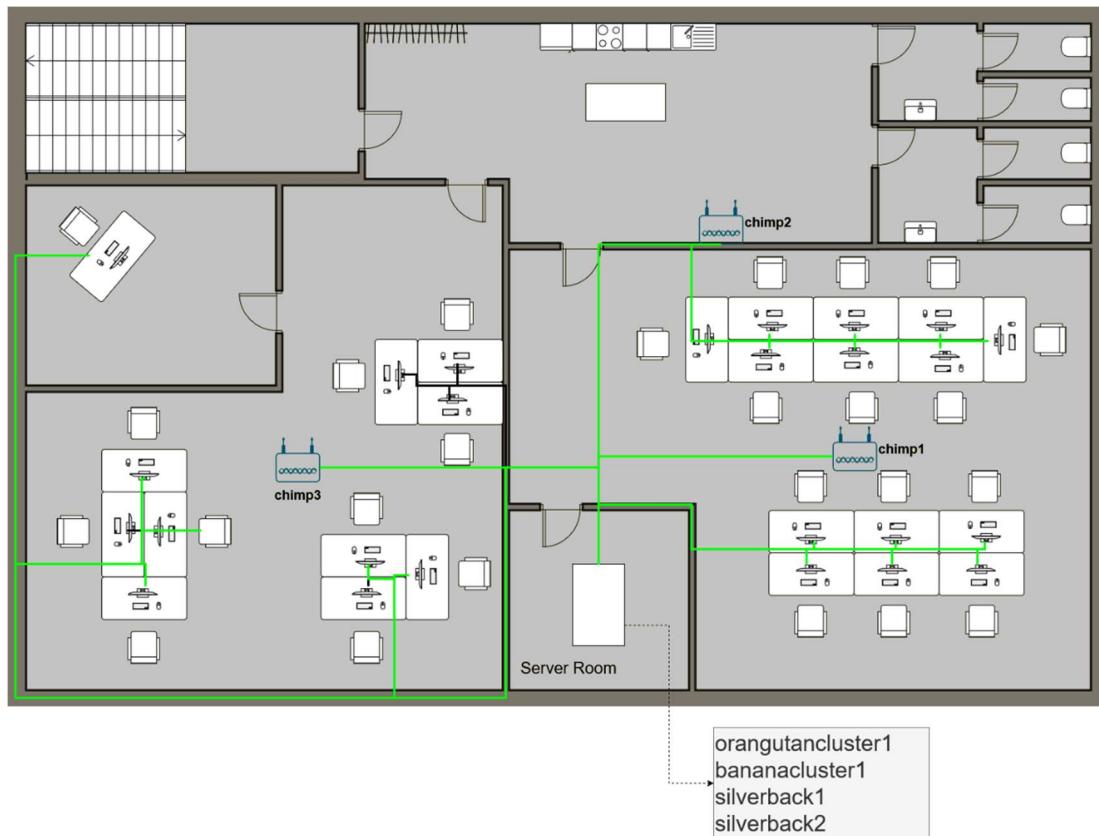


4. ábra: Teljes hálózat logikai topológia

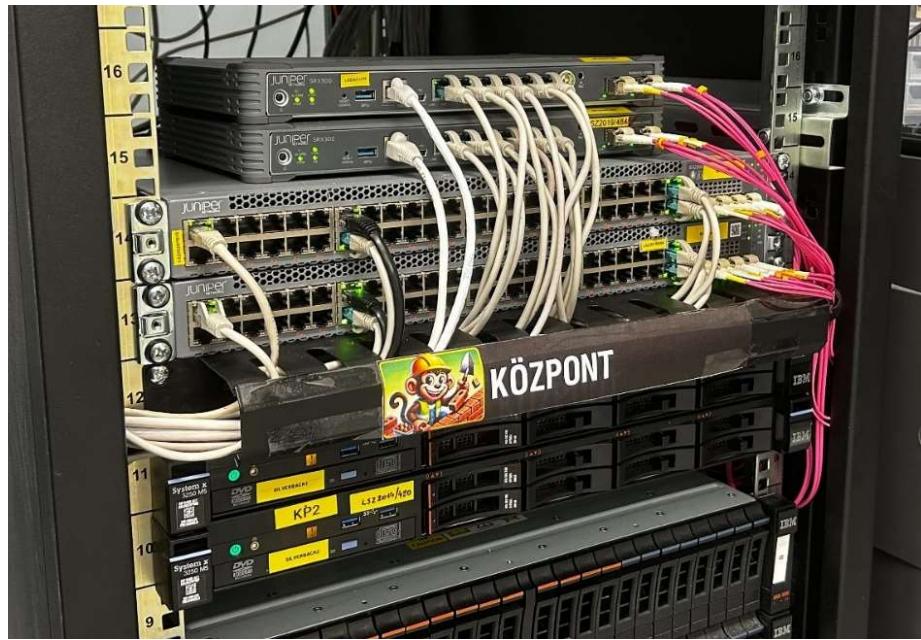
2.2 FIZIKAI TOPOLÓGIA

2.2.1 Központ

A központ fizikai topológiája és megvalósítása az alábbi képeken látható. (5. ábra, 6. ábra)



5. ábra: Központ fizikai topológlia



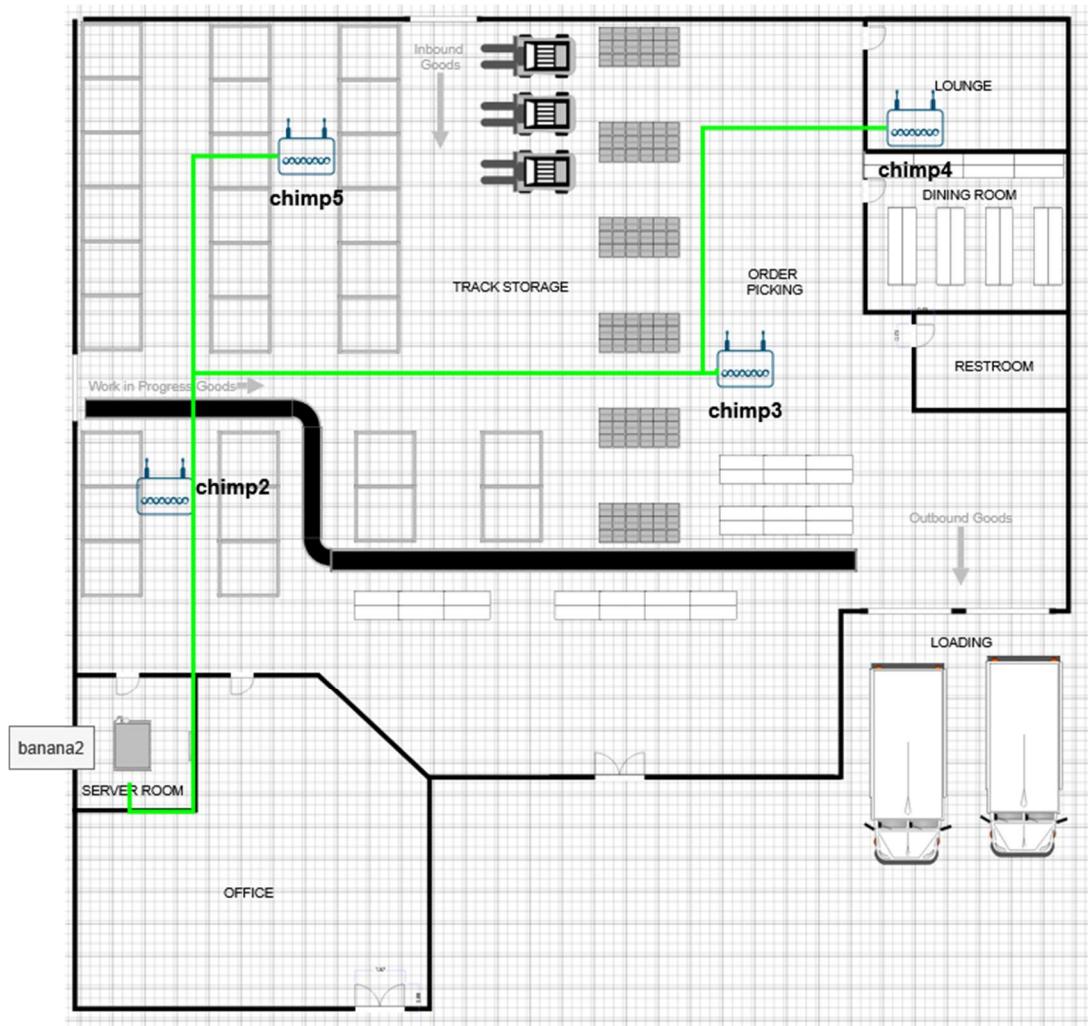
6. ábra: Központi telephely megépítve

2.2.2 Gyártási telephelyek

A két gyártási telephelyen, Markotabödögén és Taktaharkányban megegyező tervek alapján épültek az egységek. A telephely irodai része a 7. ábraán, a gyár része a 8. ábraán látható. A két telephely megvalósítása a 9. ábraán és a 10. ábraán látható.



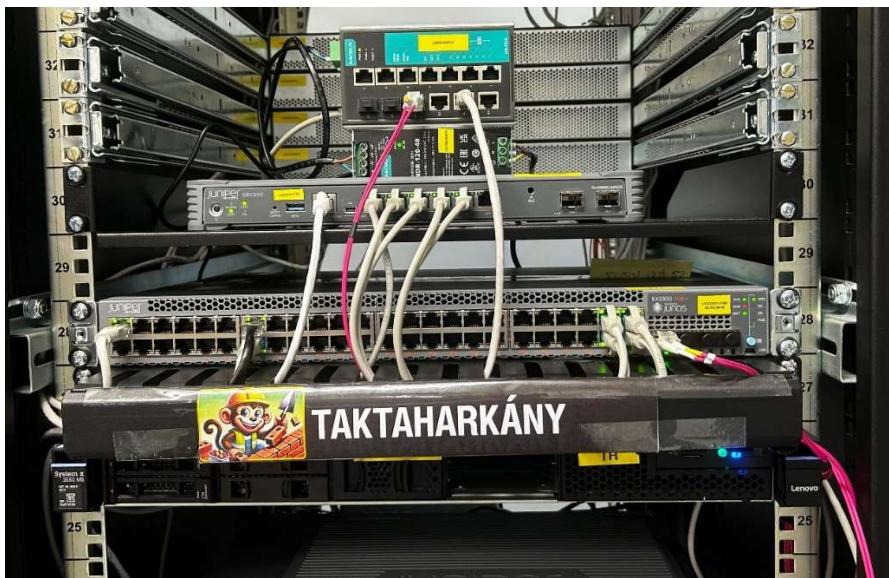
7. ábra: Gyártási telephely iroda fizikai topológia



8. ábra: Gyártási telephely gyár fizikai topológia



9. ábra: Markotabödögei telephely megépítve



10. ábra: Taktaharkányi telephely megépítve

2.2 TELEPHELYEK

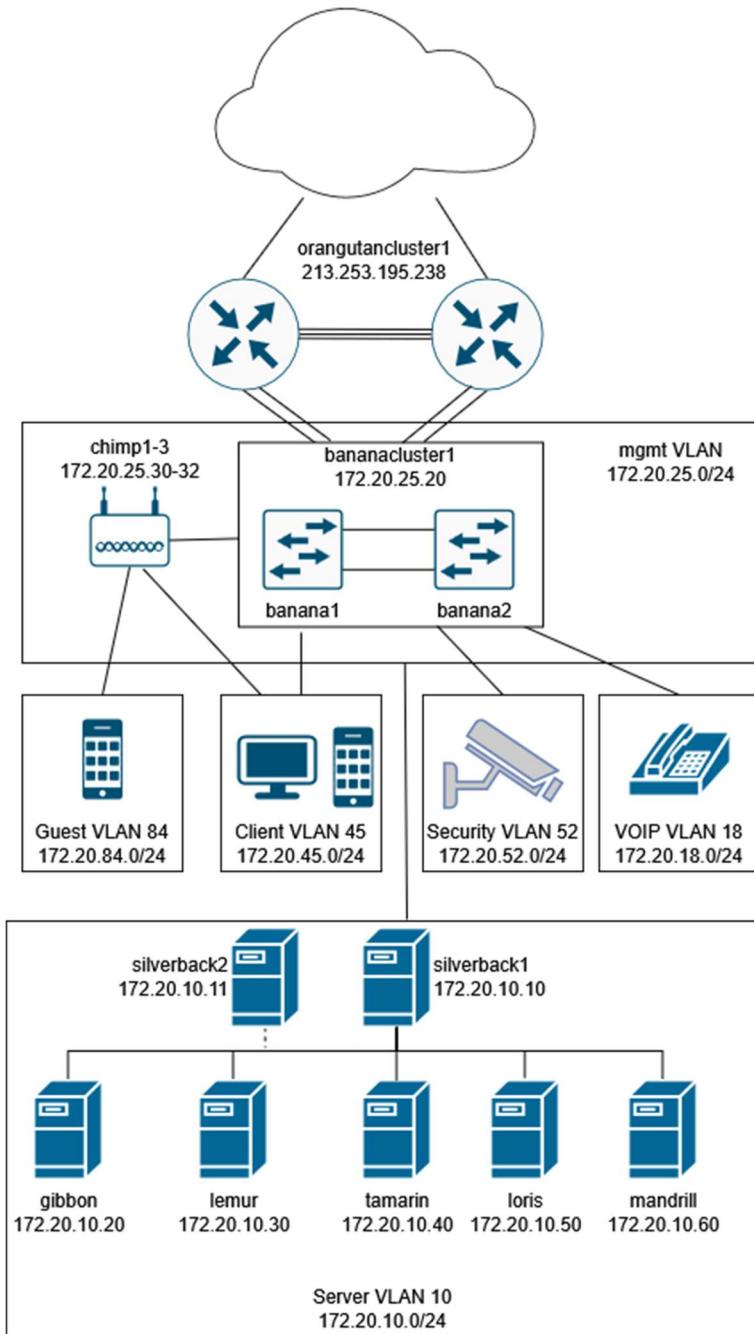
2.2.1 Központi iroda

A cég központi telephelye Győrben helyezkedik el. Innen történik az egész vállalat irányítása és minden részleg koordinálása. Emiatt ezen a helyszínen dolgoznak a legtöbb, a projekt kivitelezése alatt 25-en, azonban ez a szám biztosan bővülni fog a közeljövőben, így a hálózat hatékony bővíthetőségét előre biztosítottuk. Már a tervezési folyamatok alatt különös figyelmet szántunk arra, hogy minél hibatűrőbb és redundánsabb hálózatot és szolgáltatásstruktúrát biztosítsunk a cégvezetés és a dolgozók számára, de az elsődleges szempont egy olyan hálózat felépítése volt, ami a lehető legbiztonságosabb akár külső vagy belső informatikai támadások ellen. A hálózati eszközöket a korábbi munkatapasztalataink alapján válogattuk össze, és a számunkra legjobb ár-érték arányú informatikai berendezéseket biztosítottuk a telephelyre. Az épületben teljes Wifi lefedettséget biztosítottunk nem csak a vendégek számára, de a megfelelő hozzáféréssel rendelkező dolgozóknak teljes elérést nyújt a munkájukhoz. A további biztonság érdekében kamerákat is szereltünk fel az irodába, amelyeknek a felvételei központilag kezelhetőek. Emellett olyan szerződést kötöttünk az energia- és internetszolgáltatóval, hogy a lehető legkisebb kímaradást biztosítsák a nap 24 órájában.

A központi telephelyen felhasznált eszközök:

- 2 Juniper SRX300 tűzfal
- 2 Juniper EX2300 switch
- 3 Juniper AP45 access point
- 2 IBM System x3250 M5 szerver

A központi hálózat logikai topológiája az alábbi képen látható. (11. ábra)



11. ábra: Központi logikai topológia

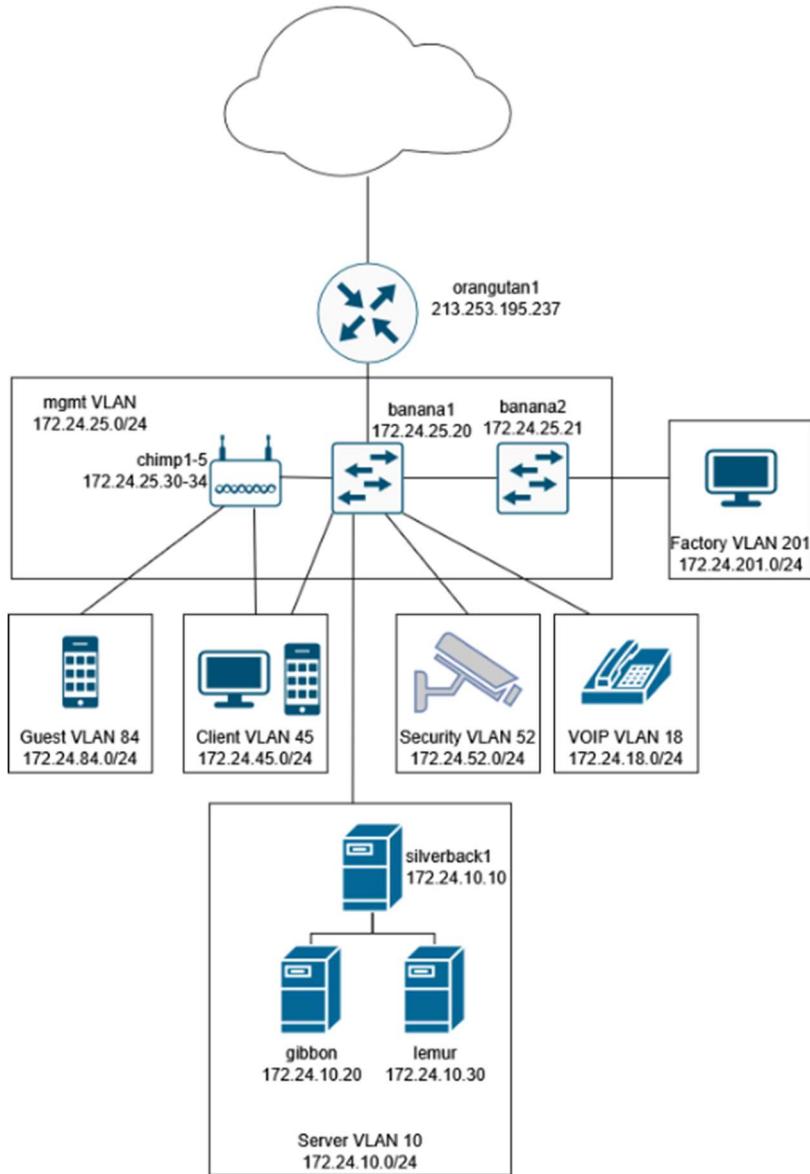
2.2.2 Markotabödögei telephely

A cég markotabödögei telephelyén elsősorban ipari tevékenység zajlik, így az itt foglalkoztatott emberek jelentős része a gyártásban dolgozik. Ettől függetlenül szükség van irodai munkát végző kollegáakra is, így számukra biztosítottunk az összes szerverszolgáltatást, akár csak a központban, azonban a kisebb terhelés miatt kevesebb végponttal és kisebb internetsávszélességgel is tudjuk a megfelelő informatikai környezetet biztosítani. Mivel a gyártásban ipari körülmények között is biztosítanunk kell a hálózati elérhetőséget, például a PLC-nek, így ipari switchekkel és ezek tárolására megfelelő rack szekrényekkel láttuk el a gyári csarnokokat. Az ilyen környezetbe szánt hálózati eszközöknek számos tényezőnek kell ellenállniuk, például a pornak vagy a magas páratartalmú levegőnek. Erre a célra mi a Moxa EDS-508a ipari switchet választottuk, ami az egyik legmegalázóbb eszköz indusztriális környezetben.

A markotabödögei telephelyen felhasznált eszközök:

- 1 Juniper SRX300 tűzfal
- 1 Juniper EX4100 switch
- 5 Juniper AP45 access point
- 1 IBM System x3250 M5 szerver

A markotabödögei telephely logikai topológiája az alábbi képen látható. (12. ábra)



12. ábra: Markotabödöge logikai topológia

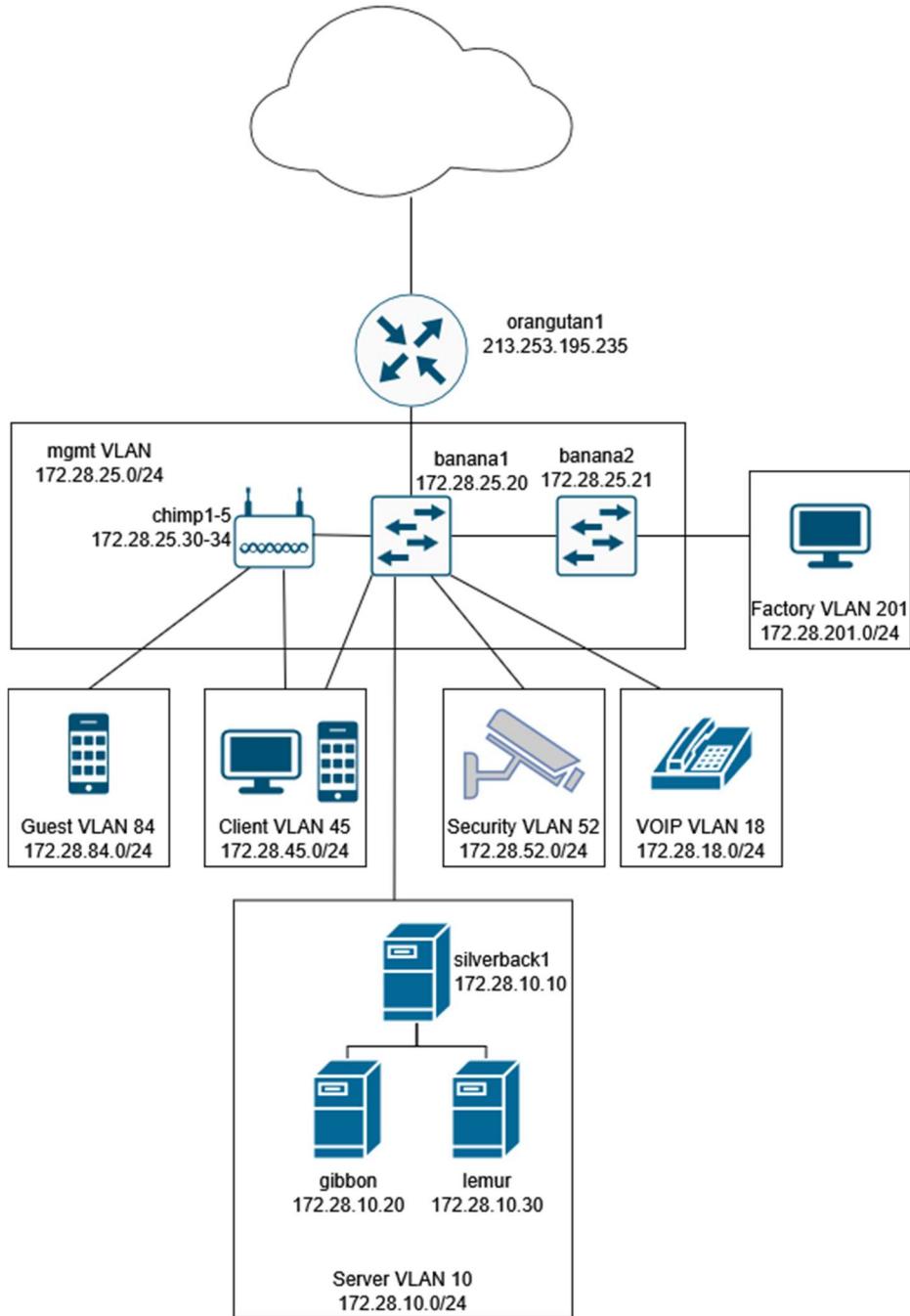
2.2.3 Taktaharkányi telephely

Hasonlóan a vállalat markotabödögei telephelyéhez Taktaharkányban is elsősorban gyártás, illetve annak üzemeltetése és feldolgozása történik. Informatikai oldalról nem olyan jelentős a különbség a gyártó telephelyek között, inkább a gyártási technológiákban és az előállított termék típusában van eltérés. Ebben az üzemben a cég külön mérnököket és technikusokat alkalmazott, hogy minél hatékonyabban tudják automatizálni és ezzel költséghatékonyabbá, illetve ezzel csökkenteni a hibaarányt a gyártási folyamatokban. Ennek érdekében biztosítottuk a szakembereknek a megfelelő hálózatot, de a további folyamatok már nem a mi munkakörünk része.

A taktharkányi telephelyen felhasznált eszközök:

- 1 Juniper SRX300 tűzfal
- 1 Juniper EX2300 switch
- 5 Juniper AP45 access point
- 1 IBM System x3250 M5 szerver

A taktharkányi telephely logikai topológiája az alábbi képen látható. (13. ábra)



13. ábra: Taktharkány logikai topológia

2.3 IP CÍMZÉS

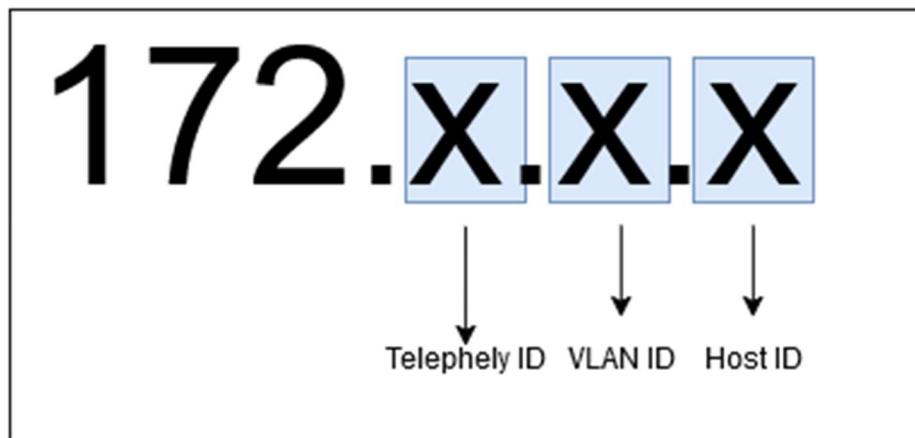
2.3.1 IPv4

A helyi címzéshez a 172.16.0.0/12 tartományt választottuk, amelyet tovább osztottunk számunkra megfelelő alhálózatokra. A három telephelynek egyenként egy /16 hosszúságú tartományt különítettünk el. A telephelyeknek szánt címzés az 1. táblázatban látható.

KP	172.20.0.0/16
MB	172.24.0.0/16
TH	172.28.0.0/16

1. táblázat: IP címzés

A telephelyeken belül, VLAN-ok szerint bontottuk tovább a címeket egységesen. Így, minden VLAN-nak egy /24-es tartomány áll rendelkezésre. A felosztási séma az alábbi ábrán. (14. ábra)



14. ábra: VLAN felosztási séma

Az eszközök címzése a dokumentációhoz csatolt monke_table táblázatban található.

2.3.2 IPv6

Az IPv6-os címzéssel érkező kérések kiszolgálását valódi IPv6-os cím hiányában egy IPv6-over-IPv4 tunnel segítségével oldottuk meg. Ennek konfigurációja az alábbi ábrán látható. (15. ábra)

```
{primary:node0}
solett@orangutancluster1> show configuration interfaces ip-0/0/0
unit 0 {
    tunnel {
        source 213.253.195.238;
        destination 216.66.87.14;
    }
    family inet6 {
        address 2001:470:1f1a:368::2/64;
    }
}
```

15. ábra: IPv6-over-IPv4 tunnel konfiguráció

Ezt az IPv6-os tartományt a Hurricane Electric weboldalán (ipv6.he.net) szereztük, amely tunnelek segítségével teszi elérhetővé az IPv6 címzést ingyen.

A 2001:470:1f1a:368::/64 tartományt használhattuk fel a saját hálózatunkban.

2.4 VLAN FELOSZTÁS

A VLAN felosztás megegyezik az összes telephelyen, azzal a kivétellel, hogy a központban nincs factory VLAN.

- **srv**: A szerverek által használt VLAN, amely a szerverszolgáltatások forgalmát foglalja magában.
- **mgmt**: A menedzsment VLAN, ami a hálózati eszközökhöz való adminisztratív forgalom elkülönítésére szolgál, biztosítja a hálózati eszközök biztonságos és zavartalan kezelését.
- **client**: A client VLAN, amely a felhasználói eszközök forgalmát elkülöníti, így biztonságosabb működést biztosít a végpontok számára.
- **security**: A security VLAN-ban a biztonsági kamerák vannak.
- **guest**: A cégez érkező vendégek a vezetéknélküli kapcsolaton keresztül, a vendég VLAN-ba kerülnek.
- **voip**: A cég által használt IP telefonok alhálózata.
- **factory**: A két telephelyen, ahol a gyártás történik, az IP hálózatra kötött gyártássegítő eszközök forgalmát különíti el.

A virtuális hálózatok a 2. táblázatban láthatóak.

VLAN szám	Név	IP tartomány
10	srv	172.x.10.0/24
25	mgmt	172.x.25.0/24
45	client	172.x.45.0/24
52	security	172.x.52.0/24
84	guest	172.x.84.0/24
18	voip	172.x.18.0/24
201	factory	172.x.201.0/24

2. táblázat: *VLAN* táblázat

2.5 REDUNDANCIA

A redundancia biztosítása rendkívül fontos szempont volt a hálózat megtervezése, illetve megvalósítása közben. Bizonyos helyzetekben ezt többszörös összeköttetéssel, máskor tartalék eszközök konfigurálásával is megvalósítottuk arra az esetre, ha hiba lépne fel az eszközökben.

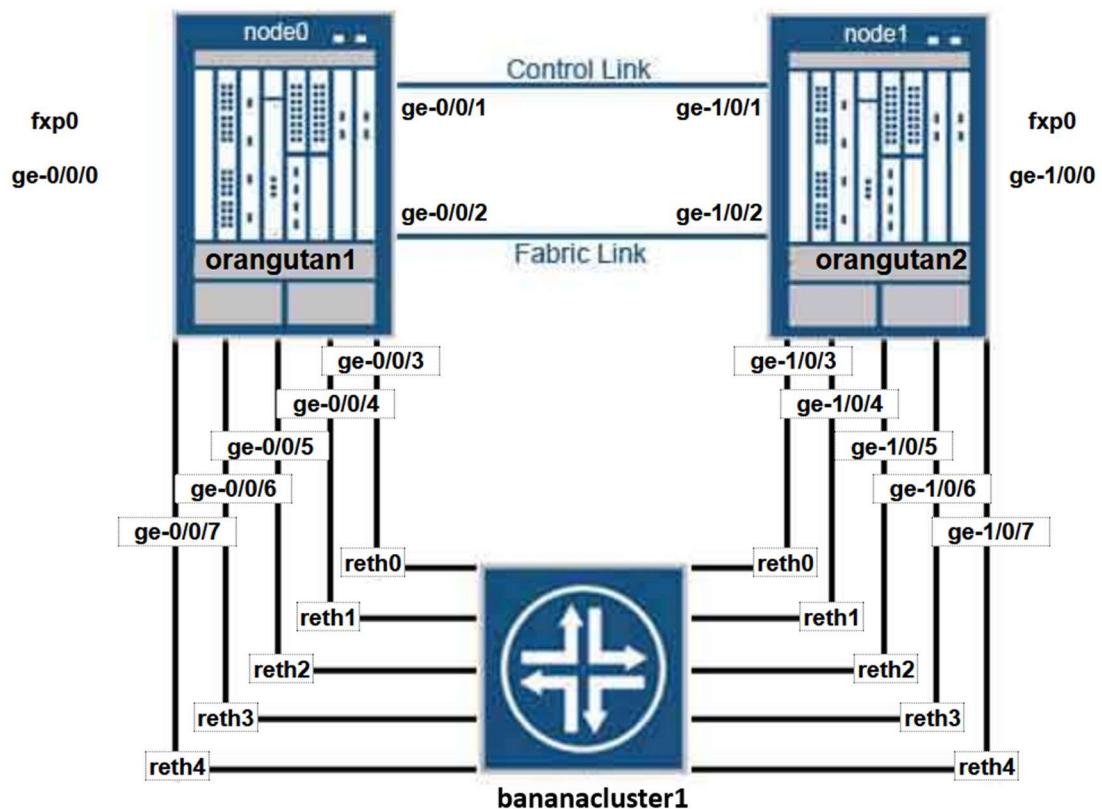
2.5.1 Második rétegbeli redundancia

A switchek hibatűrésének érdekében a Juniper szabványosított megoldását, a Virtual Chassis-t választottuk, amely nem csupán egy redundáns összeköttetést biztosít, hanem szoftveresen is integráltan felügyeli és optimalizálja a hálózati forgalmat, ezzel folyamatos hozzáférést és skálázhatóságot garantál. A Virtual Chassis technológia ráadásul egyesíti a különálló eszközöket egy közös logikai egységbe, lehetővé téve a központosított menedzsmentet és az intelligens önjavító mechanizmusokat, amelyek csökkentik az állásidőt és elősegítik a zökkenőmentes bővíthetőséget.

Emellett RSTP-t (Rapid Spanning Tree Protocol) konfiguráltunk annak érdekében, hogy a redundáns kapcsolatokat helyesen kezelje a switch. Erre azért van szükség, hogy ha az egyik tűzfal meghibásodna és a másik tűzfal venné át az elsődleges szerepet, akkor sem alakulhasson ki szórási vihar.

2.5.2 Harmadik rétegbeli redundancia

Az általunk választott SRX300-as tűzfalak támogatják a Chassis Cluster üzemmódját, amivel egy pár eszköz összekapcsolható, és úgy konfigurálható, hogy egyetlen eszközként működjön a magas rendelkezésre állás biztosítása érdekében. Ha Chassis Cluster van konfigurálva, a két tag (node) egymást támogatja, az egyik tag az elsődleges, a másik pedig a másodlagos eszközként működik, így biztosítva a folyamatok és szolgáltatások kimaradásmentes átállását rendszer- vagy hardverhiba esetén. Ha az elsődleges eszköz mehibásodik, a másodlagos eszköz veszi át a forgalom feldolgozását. Ennek a felépítése az alábbi ábrán látható. (16. ábra)



16. ábra: Chassis cluster felépítés

A Chassis Cluster csoportosítja a redundáns portokat, és ezekből egy logikai interfészt hoz létre Redundant Ethernet (reth) néven. Ezek az alábbi ábrán láthatóak. (17. ábra)

Logical Interfaces (IFL)			
IFD.IFL	vlan-id	IP/mask	Security Zone
reth0.0		213.253.195.238/28	untrust
reth1.18	18	172.20.18.254/24	voip
reth1.25	25	172.20.25.254/24	mgmt
reth1.84	84	172.20.81.254/24	guest
reth2.10	10	172.20.10.254/24	srv
reth3.45	45	172.20.45.254/24	client
reth4.52	52	172.20.52.254/24	security

17. ábra: Redundant ethernet portok

2.5.3 Szolgáltatásredundancia

A szerverszolgáltatások redundáns megoldásához három megoldás közül választottunk. A három lehetőség:

- **Megosztott tárhely:** ennek során egy különálló eszközön lehetne tárolni az összes adatot, amikhez hozzáférnek az engedélyezett szerverek. Az egyik szerver meghibásodása esetén a másik szerver adatvesztéség és kímaradás nélkül átveszi a szerepet.
- **Virtuális gép replikálása szerverek között:** A virtuális gépek replikálása a Hyper-V olyan szolgáltatása, ami kettő vagy több szerver között átmásolja a virtuális gépek állapotát adott időtartamonként, ezzel biztosítva a folyamatos működést hiba esetén. Ennél a megoldásnál érdemes figyelembe venni a replikációs időt, ami két mentés között történik (pár perc).
- **Harmadik féltől származó replikáló szoftver:** Az előző megoldáshoz hasonló, azonban ez nem az adott rendszerbe beépített funkció, hanem egy külső féltől származó szolgáltatás, ami adott esetben egyedi igényekre szabott.

Mi ebben a projektben a **Hyper-V** beépített replikáló funkcióját választottuk, mert ez a legköltséghatékonyabb megoldás, illetve mivel ez a Windows szerver saját szolgáltatása, ez a megoldás a legmegbízhatóbb lehetőség.

Ez a fajta redundancia a központban lett megvalósítva, mivel ez a legfontosabb telephely, hiszen a többi által használt szolgáltatások is megtalálhatóak itt. Ehhez két fizikai szervert telepítettünk, ezek a **silverback1** és a **silverback2**. Ennek segítségével az összes virtuális számítógép legfrissebb állapota megtalálható minden szerveren, ezzel akár az egyik fizikai szerver teljes kiesését is pótolni tudjuk. A replikációs felület az 18. képen látható.

The screenshot shows the Hyper-V Manager interface with the following details:

- Virtual Machines** list:

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuratio...
baboon	Running	0%	4096 MB	5.12:57:01		12.0
gibbon	Running	0%	8096 MB	5.12:34:30		12.0
lemur	Running	0%	4096 MB	5.12:57:01		12.0
loris	Off					12.0
mandrill	Running	0%	4096 MB	5.12:56:58		12.0
tamarin	Off					12.0
- Checkpoints** section: The selected virtual machine has no checkpoints.
- gibbon** details:

Replication Mode: Primary	Primary Server: silverback.monke.eu
Replication State: Replication enabled	Replica Server: SILVERBACK2.monke.eu
Replication Health: Normal	Last synchronized at: 2025. 03. 19. 21:15:56
- Bottom navigation: Summary, Memory, Networking, Replication.

18. ábra: Hyper-V replikáció

2.6 FORGALOMIRÁNYÍTÁS

2.6.1 VPN

2.6.1.1 Site-to-site VPN

A telephelyek közti kommunikáció titkosítására szükség volt, mivel a vállalatnak és a felhasználóknak is biztosítani akartuk a teljeskörű adatvédelmet. Ennek érdekében IPSEC site-to-site VPN-t konfiguráltunk a telephelyek között. Az IPSEC egy megbízható protokoll, amely titkosítással és hitelesítéssel védi az adatokat a nyilvános hálózatokon keresztül. Az IKE (Internet Key Exchange) automatizálja a titkosítási kulcsok cseréjét és kezelését, így növeli a biztonságot és csökkenti az emberi hibák lehetőségét. Együtt alkalmazva az IPSEC és az IKE egy skálázható, rugalmas és hatékony VPN megoldás. Úgy terveztük az alagutak kialakítását, hogy a 2 gyártással foglalkozó telephelyet a központi iroda köti össze, ezzel egy sokkal átláthatóbb rendszert kialakítva.

IKE beállítások

```
proposal kpsrx {  
    authentication-method pre-shared-keys;  
    dh-group group2;  
    authentication-algorithm sha-256;  
    encryption-algorithm aes-256-cbc;  
}
```

- **Pre-shared key autentikáció:** Egyszerű és hatékony hitelesítési módszer.
- **DH Group 2:** 1024-bites Diffie-Hellman kulccsere, amely kiegysúlyozott kompromisszumot biztosít a biztonság és teljesíteny között.
- **SHA-256 autentikációs algoritmus:** Ellenőrzi az adatok hitelességét és biztosítja, hogy azok ne módosuljanak az átvitel során.
- **AES-256-CBC titkosítás:** Erős, ipari szabványú titkosítás az érzékeny adatok védelmére.

```
policy kpsrx {
    mode main;
    proposals kpsrx;
    pre-shared-key ascii-text "SECRET";
}
```

Main mode: Biztonságosabb, mert több lépéses az IKE kapcsolatfelvétel.

VPN Gateway konfiguráció (Központ-Markotabödöge)

```
gateway kp-mb {
    ike-policy kpsrx;
    address 213.253.195.237;
    no-nat-traversal;
    local-identity inet 213.253.195.238;
    external-interface reth0.0;
}
```

- **No NAT traversal:** Mivel a kapcsolatban nincs NAT, az ESP csomagok továbbítása nem igényel UDP réteget.
- **Local identity:** Az IP-cím egyértelműen azonosítja a helyi eszközt.
- **External interface:** A kapcsolat a reth0.0 interfészen keresztül valósul meg.

Multipoint konfiguráció

A **st0** logikai interfészek között épül fel a VPN alagút. A multipoint üzemmód használata a központban az átjáró porton szükséges, mivel lehetővé teszi több VPN kapcsolat egyidejű kezelését egyetlen interfészen keresztül.

IPSEC beállítások

```
proposal kpsrx {  
    protocol esp;  
    authentication-algorithm hmac-sha-256-128;  
    encryption-algorithm aes-256-cbc;  
}
```

- **ESP protokoll:** Biztonságos adattitkosítást és hitelesítést biztosít.
- **HMAC-SHA-256-128:** A csomagok titkosítását végző algoritmus.

```
policy kpsrx {  
    perfect-forward-secrecy {  
        keys group2;  
    }  
    proposals kpsrx;  
}
```

- **Perfect Forward Secrecy (PFS):** Növeli a biztonságot azzal, hogy minden munkamenetnél új kulcsokat generál.

VPN kapcsolat létrehozása

```
vpn kp-mb {  
    bind-interface st0.0;  
    ike {  
        gateway kp-mb;  
        ipsec-policy kpsrx;  
    }  
    establish-tunnels immediately;  
}
```

- **Bind-interface st0.0:** Az IPSEC alagutat a virtuális interfészhez csatolja.
- **Establish-tunnels immediately:** Az alagút folyamatosan aktív marad, nem vár bejövő forgalomra.

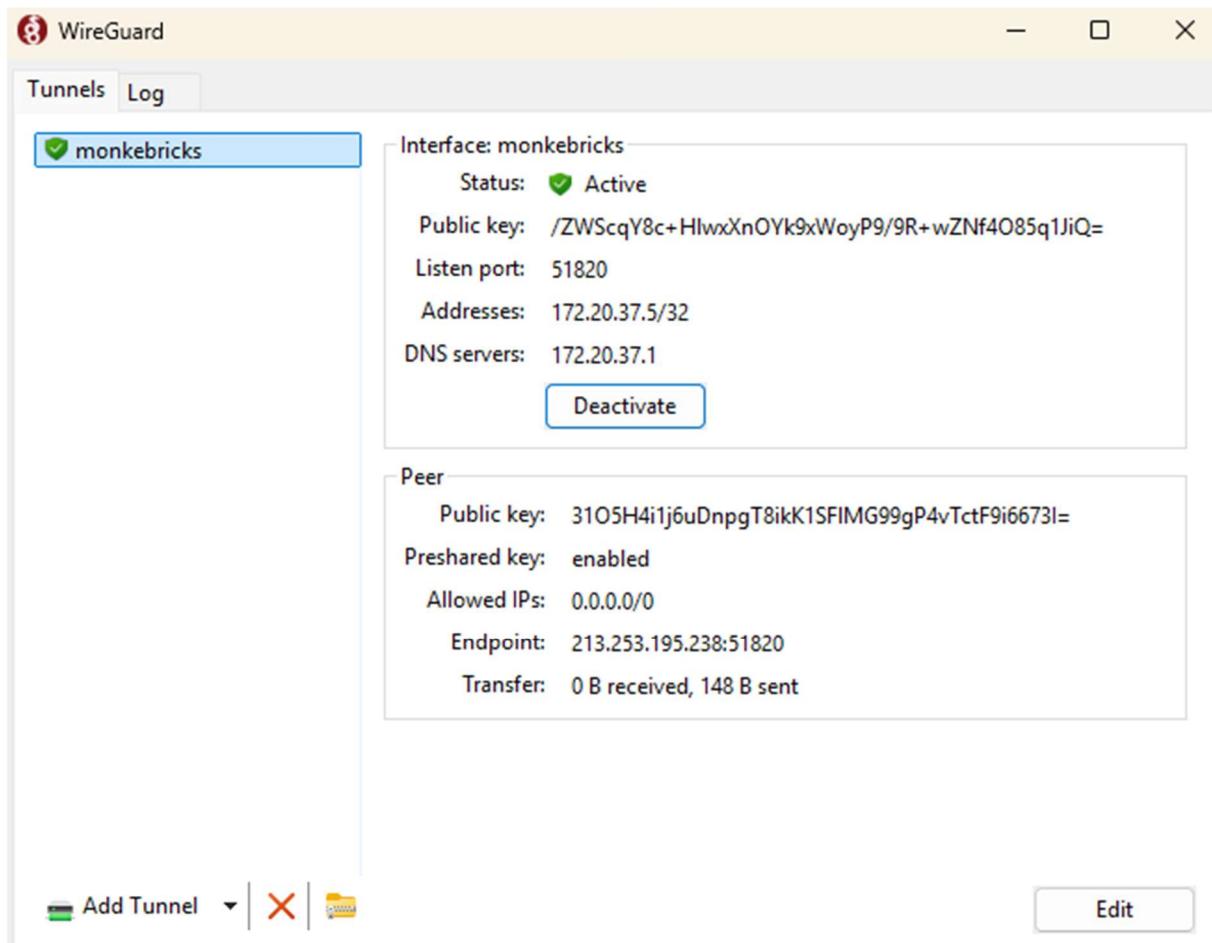
VPN zóna készítése

A VPN zóna bevezetése lehetővé teszi, hogy pontosan meghatározott szabályokat állítsunk be a telephelyek közti forgalmak szűrésére, biztosítva ezzel a hálózat biztonsági előírások betartását.

2.6.1.2 Remote Acces VPN

A cég alkalmazottai, illetve a hálózat üzemeltetői munkáját jelentősen megkönnyíti, ha a vállalati hálózaton kívülről is rendelkeznek biztonságos körülmények között a megfelelő elérésekkel. Ezt azonban szigorú adatvédelmi szabályozások és titkosítások mellett lehet csak kivitelezni.

A Wireguard VPN-re esett a választásunk, mivel egyszerűen konfigurálható, mégis gyors és modern VPN megoldás, amely megfelelő titkosítási technológiákat használ hatékony teljesítmény mellett. Fontos szempont volt még, hogy platformfüggetlen, vagyis támogatja a legnépszerűbb operációs rendszereket (Linux, Windows, macOS, iOS, Android), és könnyen telepíthető és konfigurálható az eszközökön. A WireGuard kliens felülete az 19. ábrán látható.



19. ábra: WireGuard kliens

A Wireguard működése

Minden Wireguard eszköznek van egy egyedi privát és publikus kulcsa, amelyet az eszközök közötti titkosított kapcsolat létrehozásához használnak. A rendszer peer-to-peer módon működik, tehát nem szükséges központi szerver, ami közvetlenül irányítja az adatforgalmat. A kapcsolatokat közvetlenül a peer-ek (eszközök) között hozzák létre. Mégis érdemes egy szerverre telepített központi peer-t létrehozni, hiszen azon keresztül tudják elérni a szolgáltatásokat az eszközök. A Wireguard nem tárol állapotinformációt (stateless), így kevesebb erőforrást igényel, mint az állapotot kezelő VPN protokollok.

Wireguard dockerban

Annak érdekében, hogy a lehető legjobb teljesítményt érjük el egy izolált környezetben, docker containerben futtatjuk a Wireguard szerver oldali állomását, ami a **tamarin** Debian 12 szerveren található. A rendszer felépítését és a konténerek létrehozását egy docker-compose fájl vezéreljük, illetve a kulcsok biztonságos kezelése érdekében minden induláskor mountoljuk megfelelő elérési úton a szükséges fájlokat tartalmazó könyvtárat. A docker további előnyeit részletesebben kifejtjük a 3.2.8 bekezdésben.

A Docker compose fájl az alábbi ábrán látható. (20. ábra)

```
---
services:
  wireguard:
    image: lscr.io/linuxserver/wireguard:latest
    container_name: wireguard
    cap_add:
      - NET_ADMIN
      - SYS_MODULE #optional
    environment:
      - PUID=0
      - PGID=0
      - TZ=Etc/CET
      - SERVERURL=kp.monkebricks.eu #optional
      - SERVERPORT=51820 #optional
      - PEERS=barni,solett,phoenix #optional
      - PEERDNS=auto #optional
      - INTERNAL_SUBNET=172.20.37.0 #optional
      - ALLOWEDIPS=0.0.0.0/0 #optional
      - PERSISTENTKEEPALIVE_PEERS=all #optional
      - LOG_CONFS=true #optional
    volumes:
      - /root/config:/config
      - /lib/modules:/lib/modules #optional
    ports:
      - 51820:51820/udp
    sysctls:
      - net.ipv4.conf.all.src_valid_mark=1
  restart: unless-stopped
```

20. ábra: WireGuard compose fájl

2.6.2 Statikus forgalomirányítás

Statikus forgalomirányítást alkalmazunk minden telephelynél az alapértelmezett útvonal céljából. Erre a szolgáltató IP-címe van beállítva, mint következő ugrás cím. A központban lévő konfiguráció az alábbi képen látható. (21. ábra)

```
{primary:node1}
solett@orangutancluster1> show configuration routing-options
static {
    route 0.0.0.0/0 next-hop 213.253.195.225;
}
```

21. ábra: Statikus forgalomirányítás konfiguráció

2.6.3 Dinamikus forgalomirányítás

A telephelyeket az **OSPF dinamikus forgalomirányító** protokoll köti össze. Ennek segítségével a helyi alhálózatok hirdetésre kerülnek a három tűzfal között így biztosítva az átjárhatóságot a telephelyek között. A helyi alhálózatok interfészei passzív módon vannak konfigurálva, így az azokon lévő alhálózatok hirdetésre kerülnek, azonban OSPF csomagok nem továbbítódnak rájuk. Az összes hálózat az area 0-ba kerül hirdetésre. A dinamikus forgalomirányítást az IPSEC alagútba ágyaztuk bele.

A forgalom kiesésének elkerülése érdekében, konfiguráltuk a graceful-restart funkciót, amely segítségével az OSPF folyamat újraindítása esetén a tűzfal továbbra is fenntartja a forgalomirányítást. Ez lehetővé teszi, hogy a szomszédos eszközök ideiglenesen megtartsák az útvonal-információkat, így elkerülhető a felesleges konvergencia és a hálózati instabilitás.

A konfigurációban szereplő restart-duration megadja, hogy mennyi ideje van a tűzfalnak, hogy végrehajtsa a graceful-restart folyamatot. Amennyiben nem sikerül neki, a többi tűzfal lekapcsolnak nyilvánítja a kapcsolatot. A másik, notify-duration opció, azt szabályozza, hogy a sikeres folyamat után, mennyi ideig értesítse arról a szomszédait. A no-strict-lsa-checking opció segít elkerülni a graceful-restart felesleges megszakítását, így csökkenti a hálózati kímaradásokat és növeli a stabilitást kisebb LSA-változások esetén.

Az OSPF konfiguráció az alábbi ábrám látható. (22. ábra)

```
{primary:node1}
solett@orangutancluster1> show configuration protocols ospf
graceful-restart {
    restart-duration 300;
    notify-duration 1000;
    no-strict-lsa-checking;
}
area 0.0.0.0 {
    interface lo0.0 {
        passive;
    }
    interface reth2.10 {
        passive;
    }
    interface st0.0 {
        interface-type p2mp;
        dynamic-neighbors;
    }
    interface reth1.18 {
        passive;
    }
    interface reth1.84 {
        passive;
    }
    interface reth1.25 {
        passive;
    }
    interface reth3.45 {
        passive;
    }
    interface reth4.52 {
        passive;
    }
}
```

22. ábra: Dinamikus forgalomirányítás konfiguráció

2.7 BIZTONSÁG

2.7.1 Statikus NAT

A projekt tervezése során a statikus NAT konfiguráció igénye, habár fenn állt, mi egy ennél logikusabb megoldást választottunk, mivel úgy gondoljuk, hogy a port forwarding segítségével jobban ki tudjuk használni a rendelkezésre álló IP-címeket. Ahelyett, hogy teljesen elhasználnánk egy publikus címet, mi a tűzfalunk külső IP-jére érkező kéréseket, mérlegelés után, a célportszám alapján fordítjuk a megfelelő belső címre, ezáltal a megfelelő szerverhez érkezik a kérés. Például, a központban a 443-as portra érkező kéréseket átfordítjuk a 172.20.10.40-re, ezáltal a tamarin nevű szerverünk kapja meg a csomagokat. Ennek a konfigurációja az alábbi képen látható. (23. ábra)

```

rule majomweb_ssl {
    match {
        source-address 0.0.0.0/0;
        destination-address 213.253.195.238/32;
        destination-port {
            443;
        }
        protocol tcp;
    }
    then {
        destination-nat {
            pool {
                majomweb_ssl;
            }
        }
    }
}

```

23. ábra: Port forwarding konfiguráció

Amennyiben statikus NAT-ot alkalmaztunk volna, így kellene konfigurálni:

```

set security nat static rule-set monkeruleset from zone untrust

set security nat static rule-set monkeruleset rule monkeweb match destination-address
213.253.195.238/32

set security nat static rule-set monkeruleset rule monkeweb then static-nat prefix
172.20.10.40/32

```

2.7.2 PAT

Annak érdekében, hogy a felhasználóinknak internetelérést biztosítsunk PAT-ot (Port Address Translation) használtunk. Ennek segítségével a belső címeket egyetlen külső IP-re fordítjuk. Ezeket a fordításokat portszámokkal jelöli meg a tűzfal és tartja számon. Ennek köszönhetően egyetlen publikus címmel biztosítunk kijárást az internetre. minden telephelyen a szerverek és a felhasználók tartománya kerül fordításra a tűzfal külső címére. Ennek a konfigurációja az alábbi képen látható. (24. ábra)

```
{primary:node1}
solett@orangutancluster1> show configuration security nat source
rule-set server-to-untrust {
    from zone server;
    to zone untrust;
    rule source-nat-rule-servers {
        match {
            source-address 172.20.10.0/24;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
rule-set client-to-untrust {
    from zone client;
    to zone untrust;
    rule source-nat-rule-clients {
        match {
            source-address 172.20.45.0/24;
        }
        then {
            source-nat {
                interface;
            }
        }
    }
}
```

24. ábra: PAT konfiguráció

2.7.3 Tűzfal szabályok

A Juniper tűzfalakon a forgalomvezérlés alapja a zónák rendszere. A zónák logikai csoportok, amelyekbe a hálózati interfések tartoznak. minden bejövő és kimenő forgalmat a zónák közti szabályok (security policies) határoznak meg. minden VLAN-nak, illetve a telephelyek közti szegmenseknek létrehoztunk egy-egy zónát, továbbá a „külső”, a belső hálózaton kívüli hálózatnak is létrehoztuk az untrust zónát. Az összes zóna alább látható. (25. ábra)

```
{primary:node1}
solett@orangutancluster1> show security zones terse
node1:
-----
Zone          Type
client        Security
guest         Security
mgmt          Security
security      Security
server        Security
untrust       Security
voip          Security
vpn           Security
junos-host    Security
```

25. ábra: Security zónák

Alapértelmezés szerint semmilyen forgalom nem haladhat át a zónák között. A biztonság megtervezése során törekedtünk arra, hogy a lehető legkevesebb forgalmat engedélyezzük, ezzel növelve a biztonságot egy esetleges behatolás során. A legszigorúbb szabályok a kinről (untrust) érkező forgalomra vannak állítva, mivel elsődleges szempont megelőzni a külső behatolásokat. Az untrust zónából csak a kívülről elérhető szolgáltatásokat (e-mail, web) tettük elérhetővé. A belső zónák között mindenhol megengedtük a pinget és az ssh-t a hatékony hibakeresés érdekében. További szempont volt, hogy a kliensek működéséhez elérést kellett biztosítanunk a szerverek zónájába. Ezek mellett, hogy a különböző telephelyek szerverei és kliensei tudjanak kommunikálni egymással, így a vpn zónából engedélyeztük azok elérését. Végül, hogy a szervereknek és klienseknek internetelérést biztosítsunk engedélyeztük a forgalmat az untrust zónába. A biztonsági szabályok beállítása az alábbi képen látható. (26. ábra)

```
from-zone client to-zone server {
    policy client-global-ANY-server-global-PERMIT {
        match {
            source-address client-global;
            destination-address server-global;
            application any;
        }
        then {
            permit;
        }
    }
}
```

26. ábra: Biztonsági szabály konfiguráció

2.8 VEZETÉKNÉLKÜLI HÁLÓZATOK

Minden telephelyen kettő vezetéknélküli hálózat (WLAN) lett konfigurálva. A Monke_Client azoknak a dolgozóknak lett kialakítva, akik vezetéknélküli kapcsolaton keresztül szeretnének teljes eléréssel rendelkezni.

A Monke_Guest az irodához érkező vendégeknek lett létrehozva.

3. SZERVEREK

3.1 A SZERVEREK LEÍRÁSA

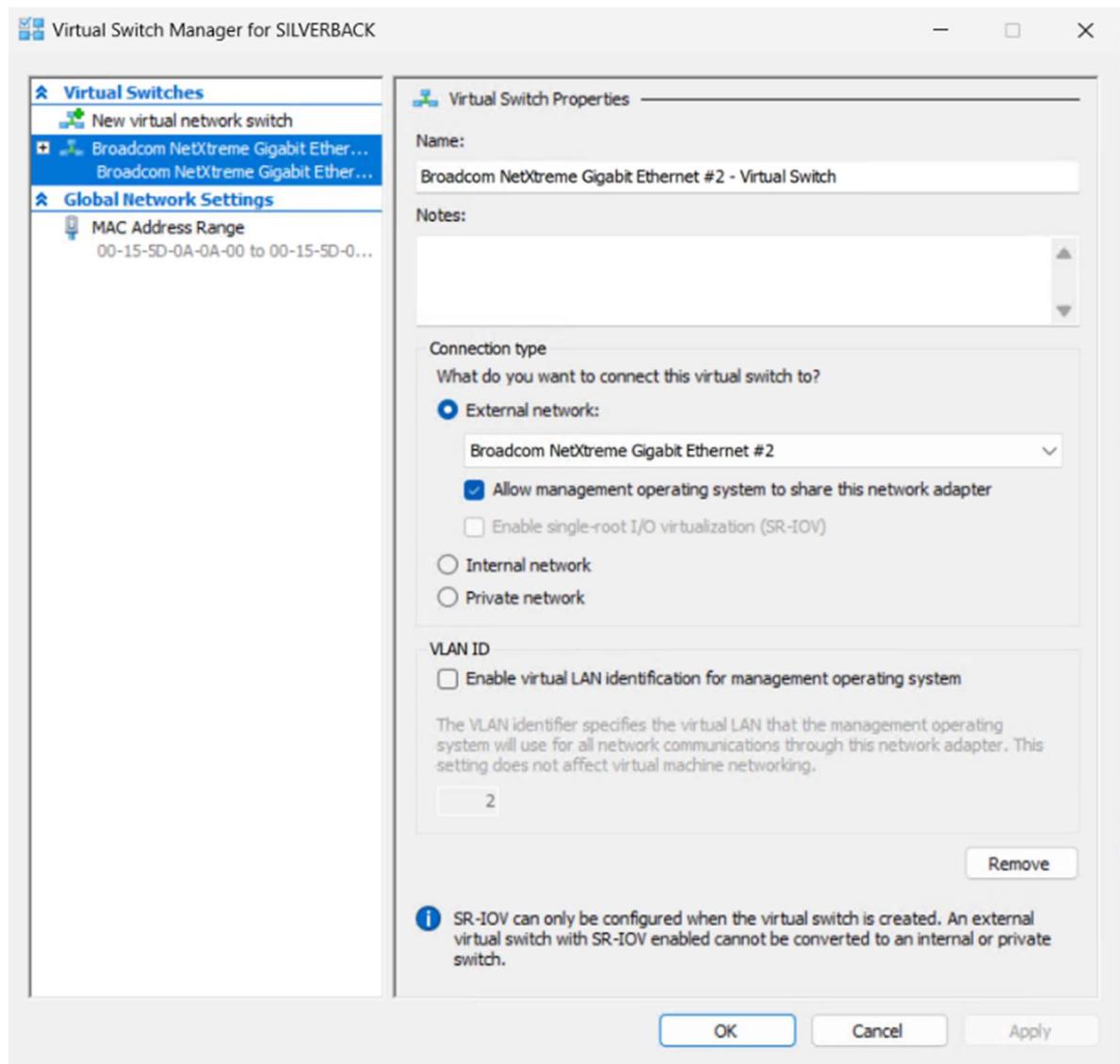
Minden telephelyen a fizikai szerverek Hypervisor-ként működnek, tehát virtuális számítógépeket futtatnak. Ezekben a VM-eken futnak valójában az általunk telepített szerverszolgáltatások.

3.2 SZOLGÁLTATÁSOK

3.2.1 Hyper-V

A szervereken használt virtualizációs szoftvernek a Microsoft Hyper-V szolgáltatását választottuk, mivel megfelel az igényeinknek, továbbá része a Windows szerverekhez járó licencnek. Ennek a segítségével virtuális szervereket tudunk létrehozni, így nincs szükség különálló fizikai eszközökre, és jobban ki tudjuk használni a szerverünk kapacitását. A Silverback nevű szervereken található a szolgáltatás.

A hálózat és a virtuális számítógépek közti kommunikáció érdekében egy virtuális switch-et konfiguráltunk, amely az „external” beállítás miatt úgy működik, mintha a VM-ek a teljes mértékben a valódi hálózaton lennének. Ezen beállítási felület az alábbi képen látható (27. ábra).



27. ábra: Hyper-V virtual switch

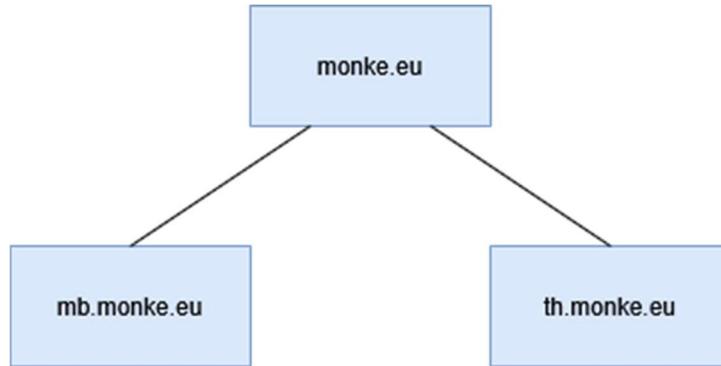
A központban a redundancia mellett terheléselosztást is alkalmaztunk. A két fizikai szerveren megosztva vannak a virtuális gépek, azonban, ha valamilyen probléma miatt szükséges lenne, az egyik szerver is át tudná venni az összes VM-et és tovább futtatni azokat.

3.2.2 AD

Active Directory címtárszolgáltatást használunk a felhasználók és hálózati erőforrások kezelésére. A Gibbon nevű szerverek futtatják a tartományvezérlőket. A három telephelynek három tartományt hoztunk létre:

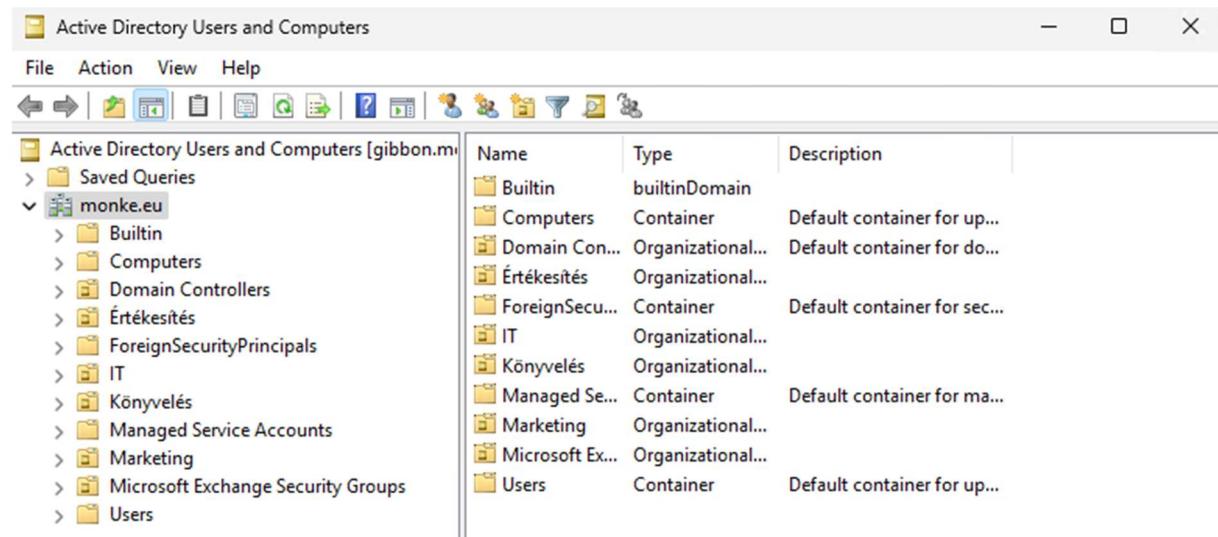
- monke.eu (Győr központ)
- mb.monke.eu (Markotabödöge)
- th.monke.eu (Taktharkány)

Ezek így együtt egy fa struktúrát alkotnak, melynek tetején a központi monke.eu domain áll. Ez az 28. ábrán látható.



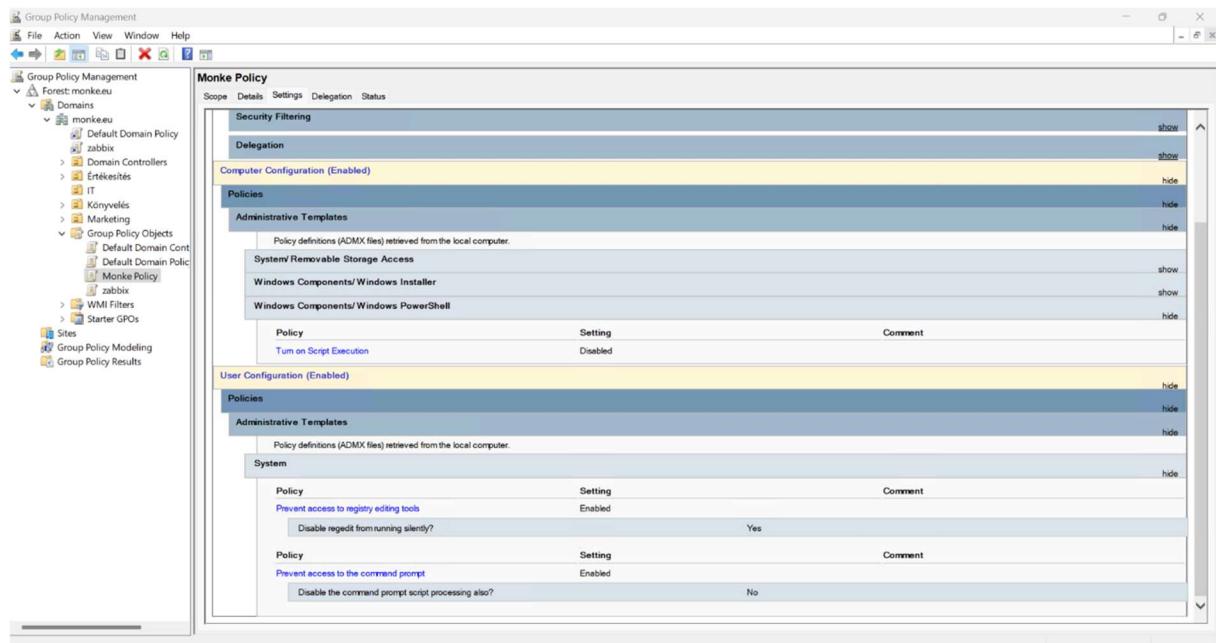
28. ábra: Active Directory domain struktúra

A cég különböző osztályainak megfelelően hoztunk létre különböző OU-kat, azonban a jövőben felmerülő igények szerint ezeket könnyedén bővíteni tudjuk. Ennek köszönhetően különböző szabályokat tudunk beállítani a felhasználó csoportoknak. A létrehozott szervezeti egységek az alábbi képen láthatóak. (29. ábra)



29. ábra: Active Directory OU

A felhasználók és számítógépek könnyebb kezelése érdekében Group Policy-kat hoztunk létre. Az egyik GPO lefuttat egy PowerShell scriptet a számítógépek indulásakor, ami feltelepíti az eszközök felügyeletéhez szükséges Zabbix Agentet. Továbbá, egy másik GPO-ban korlátoztuk a felhasználók hozzáférését olyan szoftverekhez, amelyekre nincs szükségük, azonban biztonsági rés lehet. Ilyen például a parancssor, vagy a registry szerkesztő. Ezek mellett letiltottuk, hogy a felhasználók külső adattárolókat használhassanak, ezzel is potenciális veszélynek kitéve a rendszert. A Group Policy beállítások az 30. ábrán láthatóak.



30. ábra: Group Policy beállítások

3.2.3 DNS

A DNS (Domain Name System) a hálózat egyik kulcsfontosságú eleme, amely a hosztneveket IP-címekre fordítja le, megkönnyítve ezzel a hálózati kommunikációt. A DNS szervert a gibbon nevű Windows 2025 szerverre konfiguráltuk, amin az Active Directory szolgáltatás is fut, mert Windows kliensek és szerverek automatikusan regisztrálódnak a DNS-ben, így csökkentve az adminisztrációs terheket. Csak a linux szervereket és a hálózati eszközöket kell regisztrálni az adatbázisba. Csak a hitelesített eszközök módosíthatják a DNS rekordokat, ami védelmet nyújt a nem kívánt változtatások ellen.

Minden telephely rendelkezik saját DNS szerverrel, így nem kell minden címfeloldást a központi szervernek kezelnie. Ha egy keresett név nincs a helyi DNS adatbázisban, a kérést továbbítják a központi DNS szerver felé, ami a nem helyi lekérdezéseket továbbítja a szolgáltatótól kapott külső DNS szerverhez, amely végül feloldja az internetes címeket. A DNS konfigurációs felület az alábbi ábrán látható. (31. ábra)

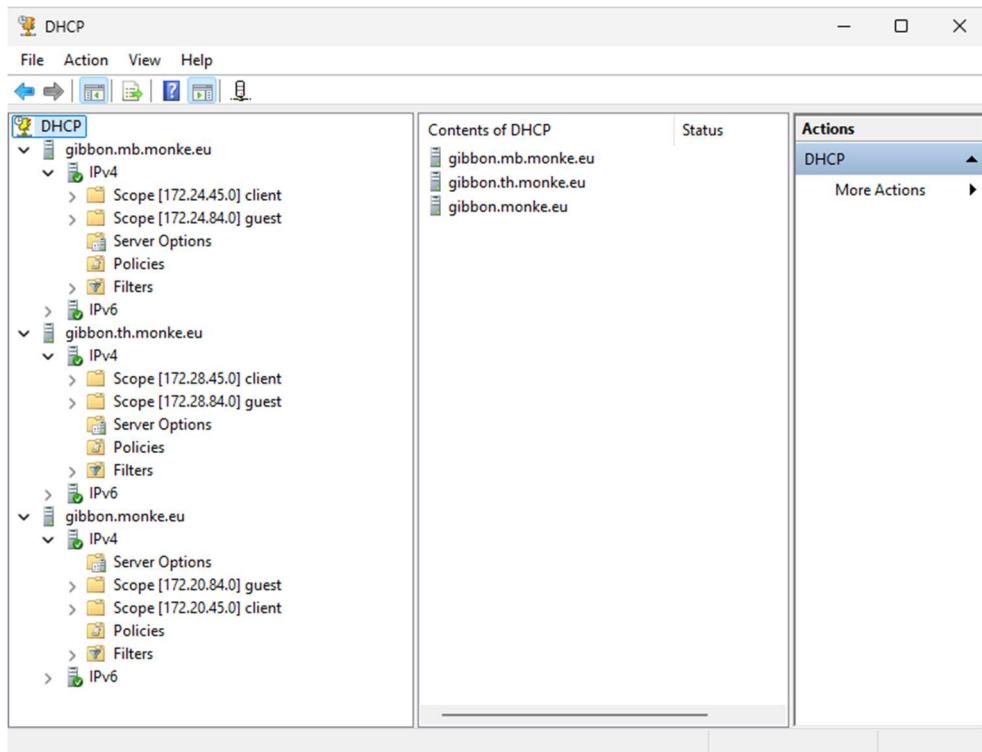
31. ábra: DNS konfigurációs felület

A külső elérés biztosításának érdekében a Rackhost domain szolgáltatótól megvásároltuk a monkebricks.eu domaint. A képen látható módon rekordokat hoztunk létre a telephelyeknek és az általunk telepített szolgáltatásoknak. (32. ábra)

32. ábra: Rackhost felület

3.2.4 DHCP

A gibbon szervereinkre telepítettük a DHCP szolgáltatást, aminek segítségével klienseink és vendégeink a hálózatra csatlakozva automatikusan megkapják hálózati konfigurációjukat. Ez magában foglalja az IP-címzést, az alapértelmezett átjárót, a DNS szerver IP címét és a tartomány nevét. Az access point-okon keresztül csatlakozó eszközök DHCP kérései is a szerverre futnak be, így központilag tudjuk kezelní az összes DHCP kölcsönzést. A kapott címzést óránként kell megújítani. A konfigurált Scope-ok az 33. ábrán láthatóak.



33. ábra: DHCP konfiguráció

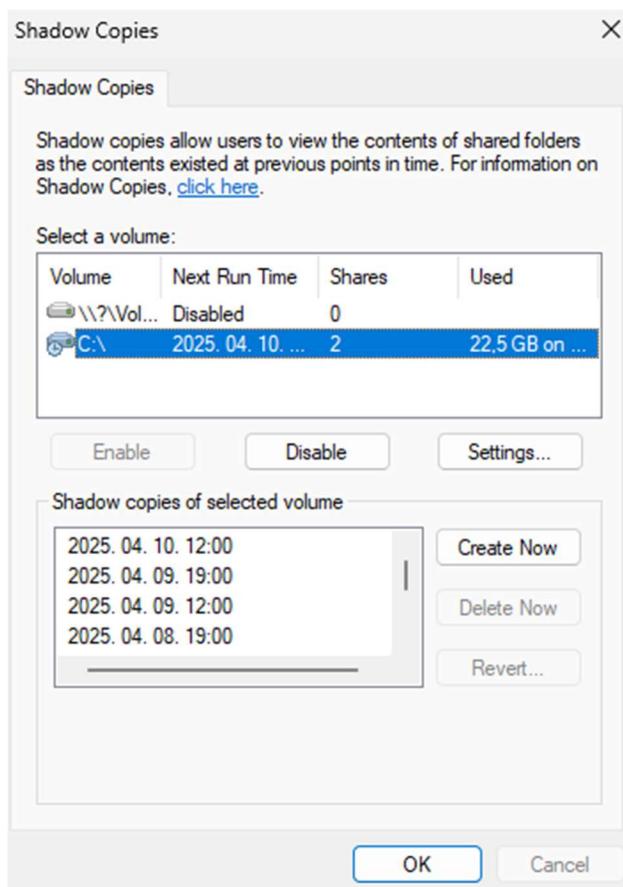
3.2.5 Fájl szerver

A fájl szerverünk a **lemur** Windows szerveren van. A Microsoft saját fejlesztésű szolgáltatását választottuk, mivel könnyen integrálható meglévő Windows infrastruktúrába, például Active Directory-val és csoportházirendekkel. A felhasználói jogosultságok és a megosztott mappák hatékonyan kezelhetőek. Az NTFS engedélyezési rendszer pedig pontosan szabályozza, hogy ki milyen hozzáféréssel rendelkezik. Emellett beépített redundancia és biztonsági funkciókkal rendelkezik, például árnyékmásolatokkal és BitLocker titkosítással. A naplázási lehetőségek révén könnyen nyomon követhető a fájlhasználat és a felhasználói tevékenységek.

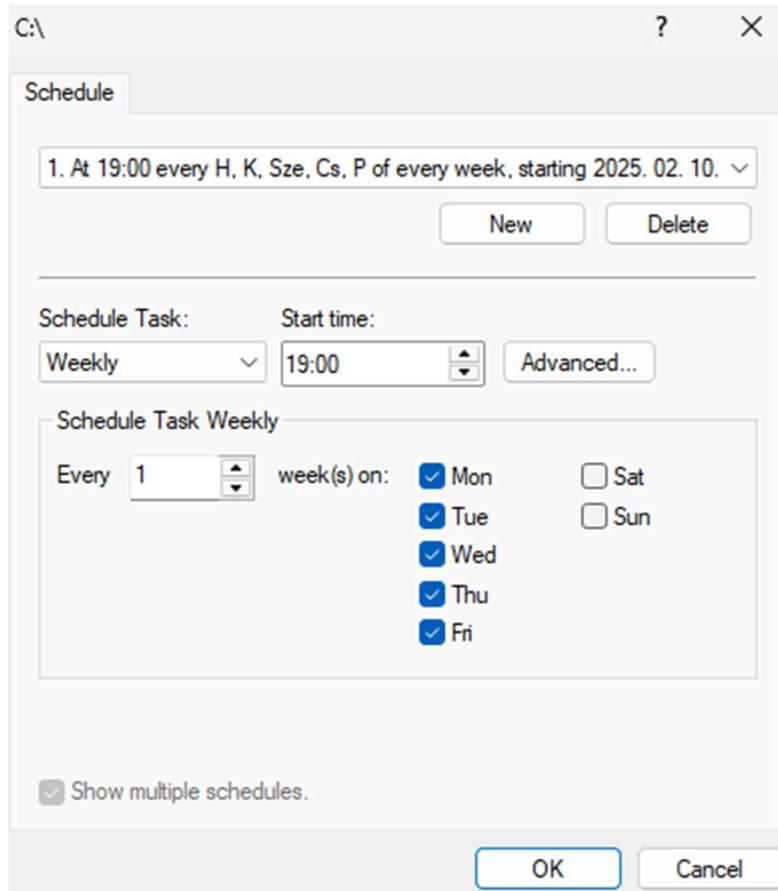
Kezdetnek minden telephelyen létrehoztunk egy közös nevű meghajtót, amit tartományba lépéskor a Group Policy automatikusan felcsatol minden Domain Users csoporttag számára, és teljes hozzáférést biztosít számukra. A jövőben felmerülő igények szerint mindegyik munkaosztály kaphat saját megosztott meghajtót, amit csak a megfelelő csoporttagsággal rendelkező felhasználók érhetnek el. Ezekről a hálózati meghajtókról ütemezett biztonsági mentések is készülnek.

3.2.6 VSS

A VSS is a **lemon** Windows szerveren fut, aminek feladata összehangolni azokat a műveleteket, amelyek szükségesek egy konzisztens árnyékmásolat (más néven pillanatkép vagy időpillanatmásolat) létrehozásához a biztonsági mentéshez. A szolgáltatás segítségével könnyedén visszaállítható egy törölt fájl. A biztonsági mentések minden hétköznap este 19:00-kor jönnek létre. A VSS konfigurációs felülete és a mentések idejének beállítása az alábbi képeken látható. (34. ábra, 35. ábra)



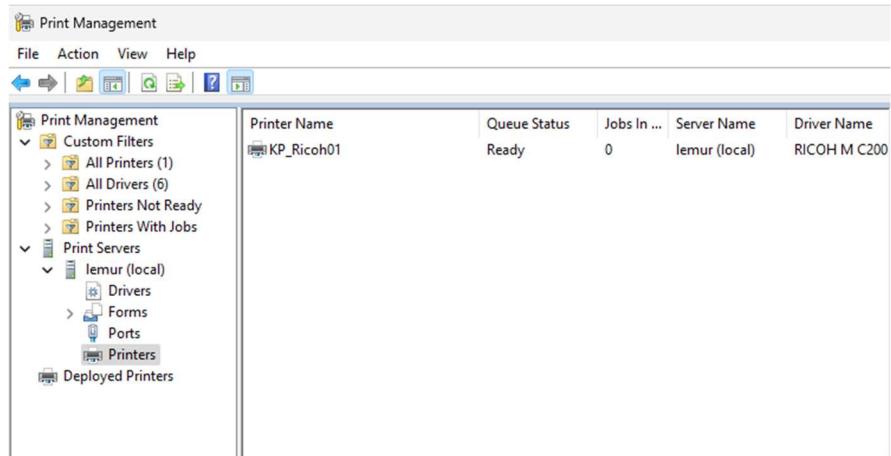
34. ábra: VSS konfiguráció



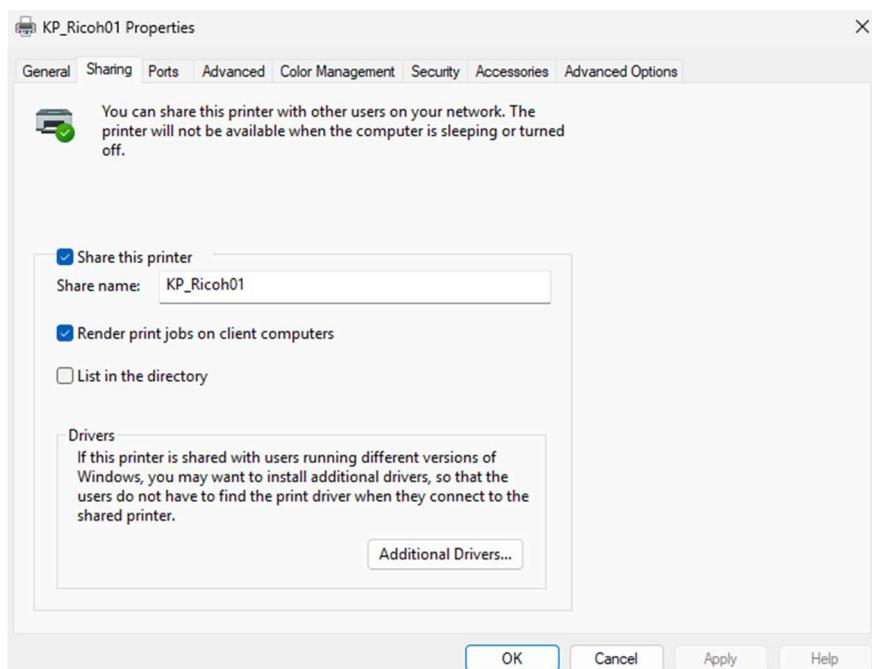
35. ábra: VSS mentés idő beállítás

3.2.7 Nyomtatószervert

A **lemur** Windows szerverre telepített nyomtatószervert központosított megoldást nyújt a vállalati nyomtatás kezelésére. Egyszerűsíti a nyomtatók adminisztrációját, a jogosultságkezelést és a nyomtatási forgalom felügyeletét. A rendszer megbízhatóságát az illesztőprogramok hatékony kezelése és biztonsági funkciók növelik. A Print Management konzol lehetővé teszi a nyomtatók gyors konfigurálását és hibaelhárítását, míg a csoportházirendekkel könnyedén kioszthatók a nyomtatók a felhasználóknak. A nyomtatószerver beállításai az alábbi (36. ábra, 37. ábra) képeken látható.



36. ábra: Központi feltelepített nyomtató



37. ábra: A nyomtató megosztása

3.2.8 WEB

A vállalat igényei szerint saját weboldalt is fejlesztettünk, ami nem csak a cég munkásságát, de a termékpálettáját is részletesen bemutatja. A webszerver a **tamarin** nevű Debian 12 alapú Linux szerveren fut. A kiszolgálást egy nginx webszerver végzi, amely Docker konténerben működik. A weboldal elérhetőségét a monkebricks.eu domain biztosítja, amelyet a Rackhost szolgáltatótól vásároltunk. A megfelelő DNS-beállítások révén a forgalom a megfelelő szerverre irányul.

MonkeBricks - A Legjobb Téglák

Bricks Together Strong – Építsünk együtt!

Rólunk Termékek Kapcsolat

Rólunk

Üdvözölünk a MonkeBricks világában, ahol a téglák nem csak egy téglák, hanem **egy életérzés**. Mi nem csak téglát gyártunk – mi az álmaidat építjük fel. És ha valaki megkérdezi, hogy van-e közünk a Leier-hez... **NINCS!** Semmi, zérő, nulla!

MonkeBricks: ahol a téglák is nevetve tartja össze a falakat. 😊

Még egyszer, ha nem lenne világos: **semmi közünk a Leier-hez!**

Termékeink

A legjobb minőségű téglákat kínáljuk, amelyek olyan erősek, hogy még King Kong is elismerően csettintene!

Választhatsz a következő típusok közül:

- **MonkeBasic** – Az egyszerű, de nagyszerű téglák.
- **MonkeStrong** – Olyan erős, hogy a fal sem fog leesni.
- **MonkeLuxury** – Ha a falak is luxust érdemelnek.

És még minden, ha valaki megkérdezné: **semmi közünk a Leier-hez!**

Kapcsolat

Szeretnél téglát vásárolni, vagy csak beszélgetni a téglák csodálatos világáról? Írj nekünk!

38. ábra: Weblap

A Docker előnyei:

- **Izoláció:** A konténerek elkülönülnek a host operációs rendszertől, így minimalizálják az esetleges konfliktusokat és kompatibilitási problémákat.
- **Könnyű telepítés és skálázhatóság:** A docker-compose fájl segítségével gyorsan és egységesen lehet telepíteni és frissíteni a webszervert.

- **Hordozhatóság:** A konténer bármilyen Docker-képes környezetben könnyen futtatható, függetlenül az alaprendszeről.
- **Erőforrás-hatékonyság:** A konténerek kevesebb erőforrást igényelnek, mint a hagyományos virtuális gépek, mert közvetlenül a host OS kernelét használják.
- **Biztonság:** A konténerek korlátozott hozzáféréssel futnak, így egy esetleges biztonsági rést kevésbé lehet kihasználni a host rendszer ellen.
- **Egyszerű frissítés és rollback:** A verziókezelés és a frissítések egyszerűen kezelhetőek, valamint könnyen visszaállíthatók korábbi verziók, ha szükséges.

```
# File: docker-compose.yml
services:
  web:
    image: nginx
    container_name: web
    ports:
      - 80:80
      - 443:443
    volumes:
      - /opt/Monke/WEB_Monke/html:/usr/share/nginx/html
      - /opt/Monke/WEB_Monke/conf.d:/etc/nginx/conf.d/
      - /etc/letsencrypt:/etc/letsencrypt
```

39. ábra: Webes docker-compose.yml

A rendszer felépítését és a konténerek létrehozását egy docker-compose fájl segítségével végezzük. Az alábbi könyvtárat csatoljuk fel a docker containerbe amelyek a weblapot és a hozzátartozó CSS fájlokat, a default nginx configot és az SSL tanúsítványokat tartalmazzák. A weblap 80-as porton (HTTP), illetve 443-as porton (HTTPS) is elérhető, de mivel kiemelt figyelmet fordítottunk az oldal biztonságossá tételere így minden esetben HTTPS-en landol az oldal látogatója. Ezt a default.config fájlban a 80-as porton érkező kéréseket a „return 301 https:// monkebricks.eu\$uri;” parancsal érjük el.

Az TLS titkosítja a böngésző és a szerver közötti adatforgalmat. A Let’s Encrypt tanúsítványokat automatikusan generáljuk és megújítjuk a Certbot ACME protokolljával, amely a webroot hitelesítési módszert használja.

A megoldás előnyei:

- **Let's Encrypt + Certbot:** Ingynes, automatizált és megbízható tanúsítványkezelést biztosít.
- **Webroot módszer:** Biztonságos és egyszerű hitelesítési megoldás meglévő webszerver esetén, amivel igazoljuk, hogy mi vagyunk a domain adminisztrátorai.

A tanúsítványok láncot alkotnak:

1. Gyökértanúsítvány (Root CA): A megbízható hatóság által kibocsátott legfelső szintű tanúsítvány.
2. Köztes tanúsítványok (Intermediate CA): A gyökértanúsítvány és a végfelhasználói tanúsítvány közötti láncszemek, amelyek biztosítják a hitelesítési folyamatot.
3. Végfelhasználói tanúsítvány: A konkrét kiszolgálóhoz kiállított tanúsítvány.

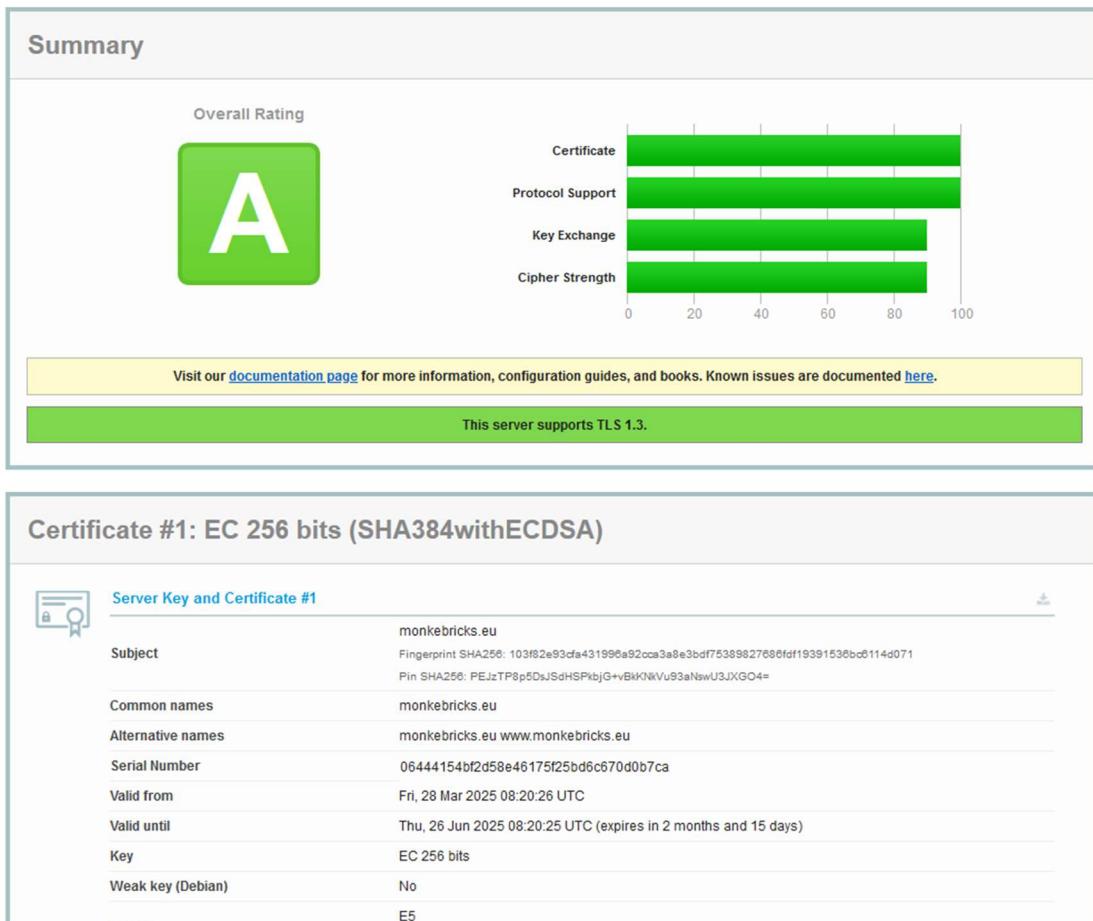
A teljes tanúsítvánnyláncot a fullchain.pem köztes tanúsítványokkal együtt tartalmazza, ezért ajánlott ezt használni az Nginx konfigurációban. Ez biztosítja, hogy minden böngésző és kliens gyorsan tudja ellenőrizni a tanúsítvány hitelességét anélkül, hogy külön kellene letölteniük a köztes tanúsítványokat.

A weboldalunk HTTPS (SSL/TLS) konfigurációját ellenőriztük a Qualys SSL Labs segítségével (40. ábra). Az oldal értékeli a tanúsítvány érvényességét, a titkosítás erősségét, a protokolltámogatást, valamint a konfiguráció biztonsági szintjét, és végül egy A-tól F-ig terjedő osztályzatot ad. Az értékelés az alábbi ábrán látható.

SSL Report: monkebricks.eu (213.253.195.238)

Assessed on: Thu, 10 Apr 2025 13:31:45 UTC | HIDDEN | [Clear cache](#)

[Scan Another »](#)



40. ábra: SSL értékelés

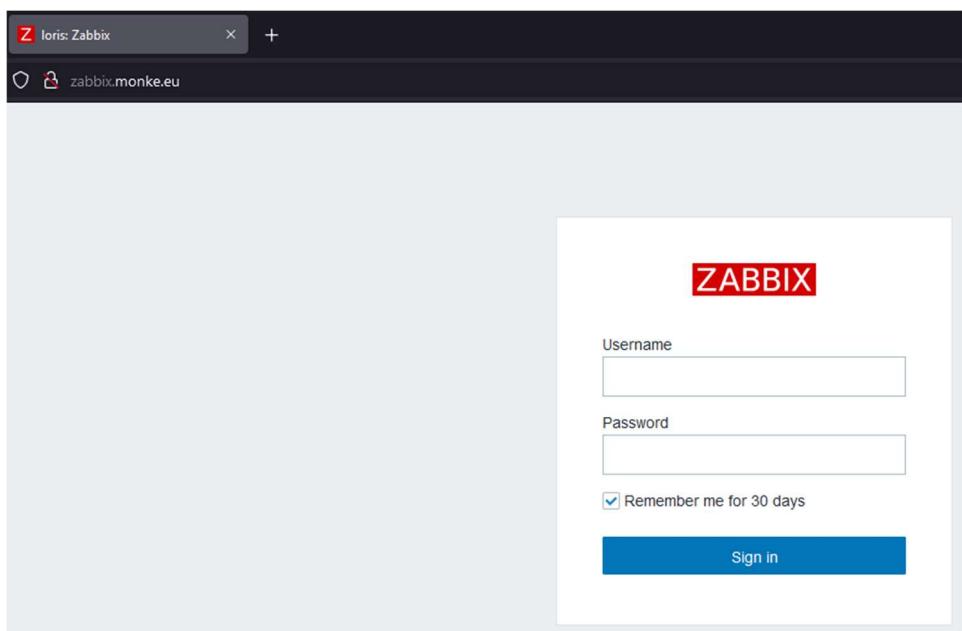
3.2.9 NTP

A **tamarin** szerveren fut a Chrony nevű szoftver, amely szinkronizálja az időt a szervereken és klienseken. Erre azért van szükség, hogy az egész cég azonos időbeállítással működjön, elkerülve ezzel az időkülönbségek okozta hibákat.

3.2.10 Zabbix

A Zabbix egy nyílt forráskódú, rugalmas és hatékony monitorozási megoldás, amelyet a **loris** szerverre telepítettünk Debian 12 operációs rendszeren. A monitorozó rendszerünk célja az összes tartományba léptetett gép és szerver megfigyelése, amelyet a Zabbix Agent segítségével valósítunk meg.

A Zabbix egy megbízható és jól skálázható monitorozó rendszer, amely akár több ezer eszköz felügyeletére is alkalmas. Valós idejű megfigyelést biztosít, azonnali értesítésekkel és riasztásokkal támogatva a gyors beavatkozást. Automatizált felderítési funkciója révén képes új eszközöket automatikusan felismerni és integrálni. Támogatja az SNMP protokollt is, így például hálózati eszközök, mint a Juniper routerek és switchek is könnyedén bevonhatók a megfigyelésbe. Emellett részletes riportokkal és vizuális elemzésekkel segíti az üzemeltetést és a teljesítmény nyomon követését. Az alábbi képen a Zabbix webes felülete látható. (41. ábra)

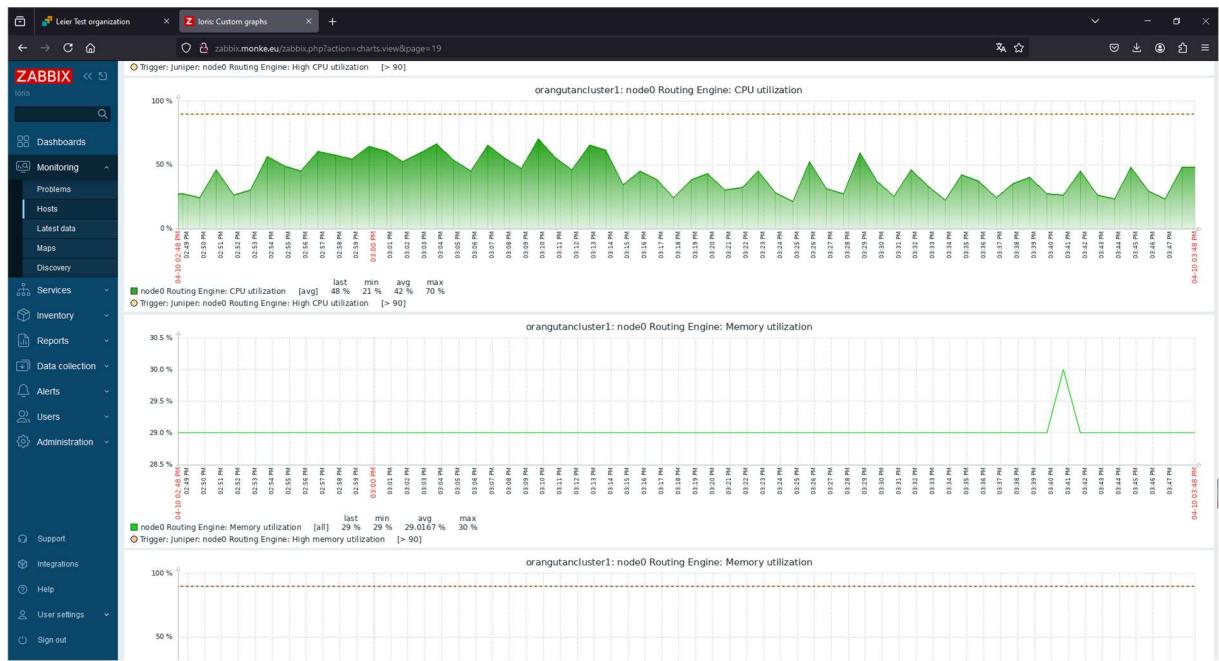


41. ábra: Zabbix webes kliens

Az agent szolgáltatás feltelepítését és a Windows kliensek és szerverek felvételét automatizáltuk. Group Policy (GPO) használatával és egy PowerShell script segítségével az agent szolgáltatás automatikusan települ, amikor egy eszköz csatlakozik a tartományhoz. Ezt követően a Zabbix szerver automatikusan felderíti és felveszi az adatbázisába az eszközöket.

A hálózatunkban található Juniper eszközöket az SNMP protokollon keresztül vettük fel a rendszerbe. Ez lehetővé teszi az eszközök állapotának folyamatos nyomon követését, a forgalmi adatok elemzését, valamint az esetleges hibák gyors észlelését és elhárítását.

42. ábra: Zabbix vezérlőpult



43. ábra: Zabbix grafikonok

3.2.11 Microsoft Exchange Server

Egy modern vállalat számára a megfelelő levelezőrendszer használata manapság szinte kötelezővé vált, hiszen a legtöbb irodai alkalmazott ezen keresztül képes munkáját hatékonyan elvégezni.

A projekt során igyekeztünk a szerverszolgáltatásokat is a lehető legjobban összehangolni, ezért esett a választásunk a Microsoft Exchange levelezőrendszer üzembe helyezésére, mivel jól optimalizált a Windows Active Directoryval, így lehetővé teszi a központi felhasználókezelést. Emellett titkosítás szempontjából biztonságosnak ítéltük az Exchanget, mivel többek közt a TLS hitelesítési protokollt is támogatja.

A levelezőszerver a **mandrill** nevű Windows 2025 szerverre telepítettük, amely során a Microsoft hivatalos dokumentációja által javasolt beállításokat használtuk, kivéve a levelezési címeknél. A szerver az Active Directory domainen belül működik, de a publikus elérhetőség miatt némi testreszabást végeztünk. Ez abból adódik, hogy a belső és a kívülről elérhető domainek neve különbözik. Az alap `user@monke.eu` email cím mellett automatikusan generálunk egy másodlagos címet a `vezeteknev@monkebricks.eu` (vezetéknév és a keresztnév első betűje) formában. Ezt az Exchange Email Address Policy segítségével állítottuk be.

Továbbá a Rackhost domain szolgáltatónk felületén egy MX (Mail Exchange) rekordot kellett felvennünk. Erre azért van szükség, mert segít az adott domainhez tartozó e-maileket a megfelelő levelezőszerver felé irányítani. A mi esetünkben a `monkebricks.eu` domainhez tartozó e-maileket a `kp.monkebricks.eu` DNS címre irányítja, ami a központi telephelyen lévő tűzfalra mutat, ami a 25-ös (SMTP) porton beérkező forgalmat a `mandrill` szerverre továbbítja.

MX rekordok <small>?</small>				<small>Új MX rekord</small>
HOSZTNÉV	LEVELEZŐ SZERVER	PRIORITÁS	TTL	
<code>monkebricks.eu</code>	<code>kp.monkebricks.eu</code>	10	3600	 

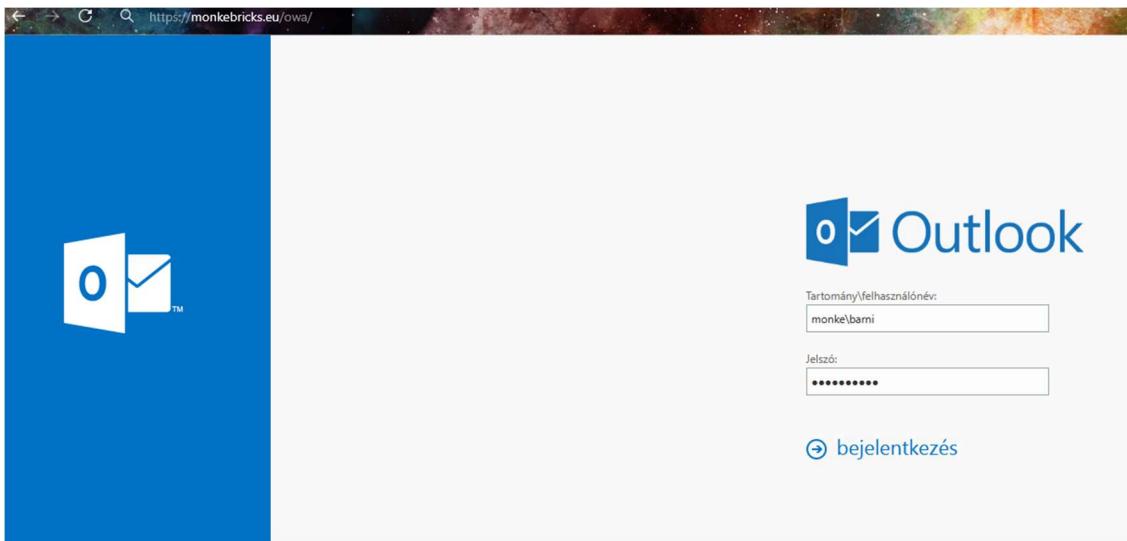
44. ábra: MX rekord

Outlook Web App

Előnyei:

Az Exchange 2019 webes felületét (45. ábra) a monkebricks.eu/owa címen külsőleg is az interneten elérhetővé tettük. Ez lehetővé teszi a felhasználók számára, hogy bármilyen böngészőből elérjék levelezésüket, naptárjaikat és kontaktjaikat.

- **Bárhonnan elérhető:** Nem szükséges helyi Outlook telepítés.
- **Biztonságos:** SSL titkosítással védett kapcsolat.
- **Platformfüggetlen:** Windows, macOS, Linux rendszereken egyaránt használható.
- **Mobilbarát felület:** Okostelefonokon és tableteken is zökkenőmentesen működik.



45. ábra: Webes Exchange felület

Exchange Admin Center

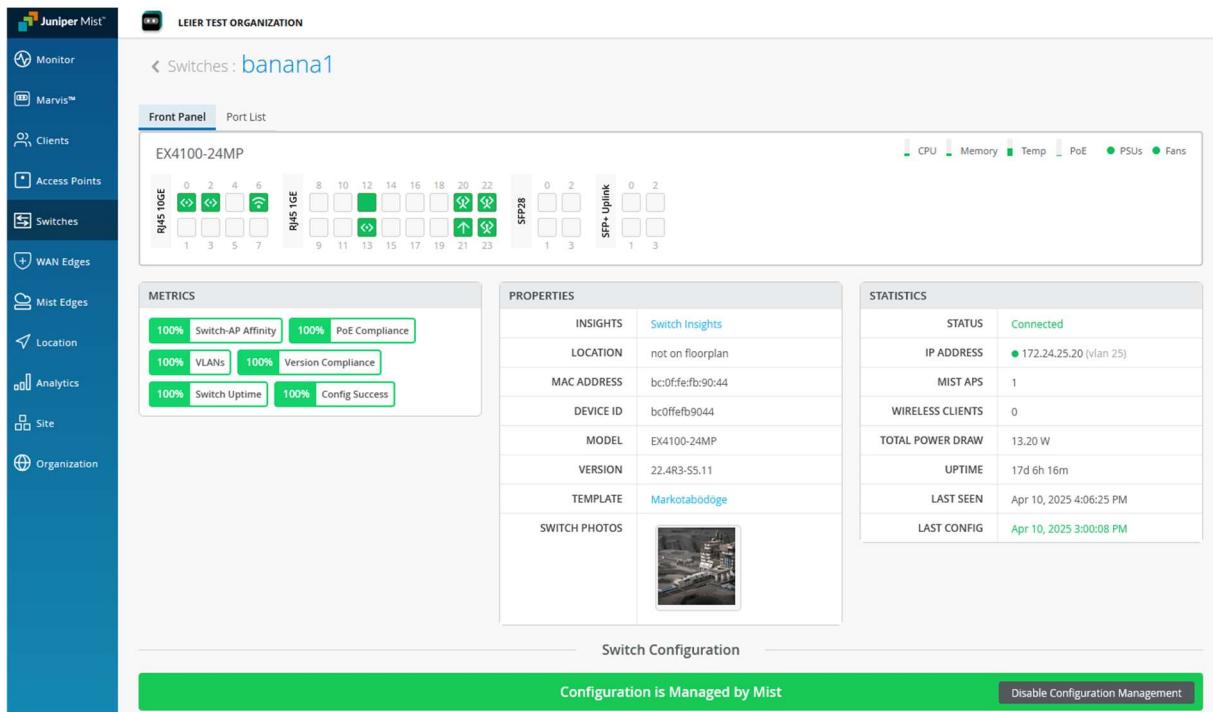
Az Exchange Admin Center (ECP) egy böngészőalapú rendszer (46. ábra), melynek nagy előnye, hogy webes felületen érhető el, így a rendszergazdák bárhonnan hozzáférhetnek a szerver adminisztrációs eszközeihez. Ehhez csak a megfelelő jogosultsággal rendelkező adminisztrátorok férnek hozzá a monkebricks.eu/ecp csak belsőleg elérhető címen.

46. ábra: Exchange Admin Center

3.2.11 Hálózatautomatizálás

A hálózati konfigurációk beállítása, illetve a problémák feltárása gyakran túl sok időt vesznek igénybe. Ez akár a cég számára hálózati kímaradást vagy limitációt is eredményezhet, amit minden eszközzel igyekezünk megelőzni.

A munkafolyamatok felgyorsítása és tökéletesítése miatt bevezettük a Mist AI-t a hálózatunkba. A Juniper Mist AI nevű technológiáját azért választottuk, mert képes a hálózati forgalom részletes megfigyelésével jelzéseket küldeni a működés közben fellépő anomáliákról, így kiküszöbölhető az emberi hibából származó tervezési és konfigurálási problémák. Az alábbi képen (47. ábra) egy switch konfigurációs felülete látható.



47. ábra: Mist AI switch konfigurációs felület

A Mist AI előnyei:

- Automatizált problémamegoldás**

A Juniper Mist AI képes automatikusan azonosítani a hálózati hibákat és azok forrását, valamint gyors javaslatokat adni a megoldásra. Ez jelentősen csökkenti az emberi beavatkozás szükségeségét, gyorsítva ezzel a problémák elhárítását.

- Anomália detektálás**

A rendszer folyamatosan figyeli a hálózati forgalmat észleli a potenciális problémákat, akár még azok kialakulása előtt. Így képesek vagyunk előre jelezni és megelőzni a lehetséges hálózati zavarokat, ami növeli a hálózat megbízhatóságát.

- Önvezető hálózat**

A Mist AI képes önállóan kezelní a hálózati beállításokat és műveleteket, például a switchek és routerek optimalizálását. Ez a funkció rendkívüli mértékben csökkenti a manuális beállítások szükségeségét, ezzel időt és erőforrást takarítva meg.

- **Mesterséges intelligencia – Marvis**

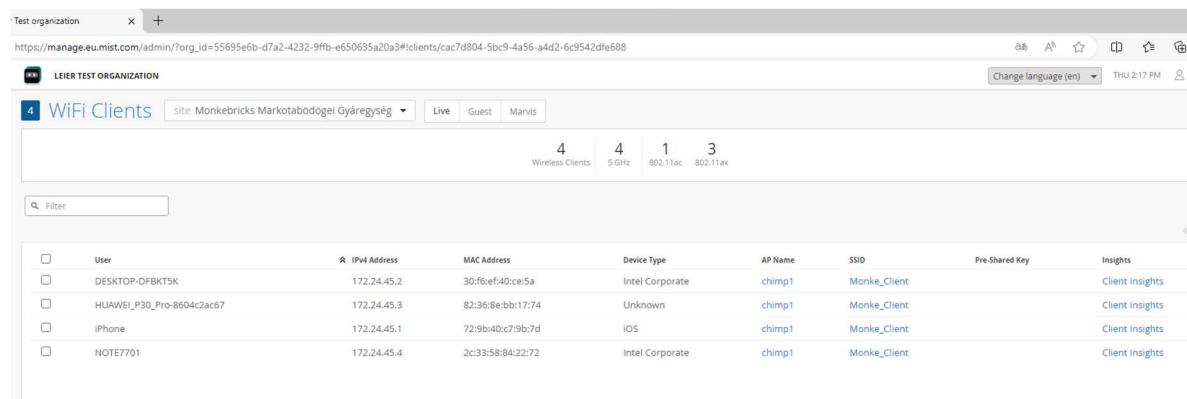
A Marvis, a Mist AI-al működő virtuális hálózati asszisztens, ami lehetővé teszi az IT személyzet számára, hogy gyorsan választ kapjon a hálózati problémákkal kapcsolatos kérdéseikre egy angol nyelvű chat felületen keresztül. Ez gyors és hatékony problémamegoldást eredményez.

- **Adat-vezérelt döntéshozatal**

A Juniper Mist AI nagy mennyiségű adatot gyűjt és elemez az összes hálózati eszközről (pl. kliensek, switchek és tűzfalak). Az adatok elemzése segít a hálózati teljesítmény maximalizálásában.

- **Egységes felület**

A szolgáltatás egy átlátható felületet biztosít a számunkra, ahol grafikusan hozzáférünk az összes eszközünk adataihoz és beállításaihoz, amiket egyszerűen bármikor megváltoztathatunk. A felülethez hozzáférők jogait is pontosan szabályozhatjuk, így megkülönböztetve egy teljes hálózathoz hozzáférő (super user-t), egy telephelyi adminisztrátort, vagy akár csak a hozzáférési pontok állapotát változtató technikust.



The screenshot shows a web-based management interface for a network organization. The top navigation bar includes 'Test organization', a search bar, and a URL 'https://manage.eu.mist.com/admin/?org_id=55695e6b-d7a2-4232-9ffb-e650635a20a3#clients/cac7d804-5bc9-4a56-a4d2-6c9542dfe688'. The main content area is titled 'LEIER TEST ORGANIZATION' and shows a 'WiFi Clients' dashboard. The dashboard displays the following statistics: 4 Wireless Clients, 4 5 GHz, 1 802.11ac, and 3 802.11ax. Below this, a table lists connected devices:

User	IPv4 Address	MAC Address	Device Type	AP Name	SSID	Pre-Shared Key	Insights
DESKTOP-DFBK75K	172.24.45.2	30:ef:ef:40:ce:5a	Intel Corporate	chimp1	Monke_Client		Client insights
HUAWEI_P30_Pro-8604c2ac67	172.24.45.3	82:36:8e:bb:17:74	Unknown	chimp1	Monke_Client		Client insights
iPhone	172.24.45.1	72:9b:40:c7:9b:7d	iOS	chimp1	Monke_Client		Client insights
NOTE7701	172.24.45.4	2c:33:58:84:22:72	Intel Corporate	chimp1	Monke_Client		Client insights

48. ábra: Mist AI WiFi kliensek

A VLAN-ok konfigurálását automatizáltuk, ezzel lecsökkentve az új eszközök üzembehozásának idejét. Amikor egy eszközöt csatlakoztatnak a kapcsolóhoz, az kiolvassa az állomás MAC-címét, és ha ez egyezik az általunk megengedett értékkel, a port automatikusan a megfelelő konfigurációt kapja. (49. ábra)

DYNAMIC PORT CONFIGURATION

Apply port profiles to ports based on properties of connected clients. First matching rule will be applied. Port range must have dynamic port configuration enabled.

Override Site/Template Settings

 Edit Rule  

Check MAC 

Select the 1st segment (separated by)

Start at character offset 0 (0 = first character)

If text starts with 50:9a:4c

comma-separated same length values, case-sensitive

Apply Configuration Profile

client client(45), access 

49. ábra: Dinkamikus VLAN-ba helyezés

4. FELHASZNÁLT ESZKÖZÖK

4.1 HÁLÓZATI ESZKÖZÖK

A hálózat tervezése során, a hálózati eszközök esetében Juniper eszközökre esett a választásunk, több okból is;

- a Juniper vállalattal korábban kialakított kapcsolattal rendelkezünk, emiatt bizonyos kedvezményekre tehetünk szert
- kiemelkedő ár-érték aránnyal rendelkeznek
- szükség esetén igénybe vehetjük az RMA (Return Material Authorization) szolgáltatást, amivel, ha bármilyen fizikai problémája lenne az eszköznek, azt pár napon belül cserélik

4.1.1 Routerek, tűzfalak

A forgalomirányító és tűzfal feladatakat egy eszköz látja el, ami a Juniper SRX300 (50. ábra). Ebből a gyártási telephelyeken egy-egy, a központban pedig kettő található, amelyek együttműködve biztosítják a magas rendelkezésre állást (erről a redundancia részben részletesen írunk). Ezek a tűzfalak beépített VPN képességgel rendelkeznek, és ezt kihasználva site-to-site VPN kapcsolatokat hoztunk létre.



50. ábra: SRX300 tűzfal

4.1.2 Switchek

Switcheknek a Juniper EX2300 típusú, 48 portos eszközöt választottuk. A kapcsoló 1Gbps sebességet biztosít, és el van látni PoE+ minősítéssel, aminek segítségével képes árammal ellátni a cégnél használt telefonokat és kamerákat. Az eszköz a 51. ábraán látható.



51. ábra: EX2300 switch

4.1.3 Szerverek

A szerverszolgáltatások az IBM System x3250 M5 eszközökön futnak. Ezek a szerverek Intel Xeon E3-1271 v3 típusú, 4 magos processzorral vannak felszerelve, amivel képesek futtatni a rajta létrehozott virtuális számítógépeket. Emellett 32 GB DDR3 típusú, ECC (Error Correcting Code) memóriával láttuk el őket, amivel bizonyos memóriahibákat képes kiszűrni, ezzel is javítva a rendszer stabilitását és megbízhatóságát, különösen a kritikus alkalmazások vagy szerverfeladatok esetén.



52. ábra: IBM System x3250 M5 szerver

4.1.4 AP-k

Az általunk választott, Juniper AP45 egy nagy teljesítményű Wi-Fi 6E (802.11ax) hozzáférési pont, amelyet nagy forgalmú és sűrűn használt környezetekhez terveztek. Fejlett antennatechnológiájának köszönhetően optimalizálja a jelerősséget és csökkenti az interferenciát, így stabilabb és gyorsabb kapcsolatot biztosít, ezáltal különösen ideális a vállalati környezetbe. Ennek köszönhetően a cégben dolgozók könnyen használhatják laptopjaikat munkára, és az irodába érkező vendégek is el vannak látva interneteléréssel.



53. ábra: Access point

4.1.5 Szünetmentes tápegységek

Nagy figyelmet fordítottunk a kímaradásmentes elektromos hálózat biztosítására, hiszen ennek hiányában túlságosan kiszolgáltatottá válik a rendszer. Emiatt a szolgáltatóval olyan szerződést kötöttünk, amiben éves szinten maximum 1 óra kímaradás engedélyezett.

A szerverszobában nagy teljesítményű szünetmentes tápegységeket telepítettünk (54. ábra), ami áramszünet esetén képes közel 45 percig biztosít áramellátást. Azonban egy hosszabb kímaradás esetén sem állhat le a rendszerünk, ezért amint kímaradás lép fel elindul a telephelyen lévő ipari dízel aggregátor, aminek várhatóan 10 percre van szüksége, mire elegendő mennyiségű energiát képes kitermeli. Addig a szünetmentesek akkumulátoráról működnek az eszközök, azonban amint elegendő a kitermelt energia a rendszer átáll az aggregátorok hálózatára. Ezekről az eseményekről minden esetben azonnal kapunk értesítést, így tudunk reagálni a vészhelyzetre.



54. ábra: UPS

4.2 EGYÉB ESZKÖZÖK

4.2.1 PC-k, Laptopok

Az irodai környezetben a Dell OptiPlex 7090 micro számítógépet választottuk, amelyekhez Windows 11 Pro operációs rendszer licenc jár. Elsősorban azért választottuk, mert megbízható, kompakt méretű és alacsony az energiafogyasztásuk. A PC az alábbi képen látható.



55. ábra: Dell irodai számítógép

Azoknak az alkalmazottaknak, akik gyakran mozognak telephelyek között laptopot biztosítottunk. A Dell Latitude 15 5540 egy kiváló választásnak bizonyult. A laptop az alábbi képen látható.



56. ábra: Dell Latitude 15 5540

4.2.2 Nyomtatók

A központi irodában kettő, míg a gyártási telephelyeken egy-egy nagyteljesítményű Ricoh IMC2010 nyomtatót telepítettünk. A nyomtató az alábbi képen látható. (57. ábra)



57. ábra: Ricoh nyomtató

4.2.3 Telefonok

A hálózatot felkészítettük az IP telefonok belső használatára, azonban már zajlanak a tárgyalások a külső kommunikációt lebonyolító szolgáltatóval. Ezeknek az eszközöknek a Yealink 1301110 készüléket választottuk, ami az alábbi képen látható.



58. ábra: IP telefon

4.2.4 Kamerák

A biztonság érdekében IP kamerákat is telepítettünk beltéren és kültéren egyaránt. A beltéri egységeknek a Hikvision DS-2CD2187G3-LIS2UY kamerát, míg kültéren a Hikvision DS-2CD2647G3T-LIZSY kamerákat választottuk. A kamerák az alábbi képen láthatóak.



59. ábra: Beltéri kamera



60. ábra: Kültéri kamera

4.2.5 Kábelek (UTP, optika)

A központban a tűzfalak és a switch-ek közti redundáns kapcsolatot, valamint a két kapcsoló összeköttetését is SC-SC, multimódusú optikai kábellel valósítottuk meg. Az összes többi kapcsódásnál Cat5e rézkábelt alkalmaztunk.

A gyártási telephelyeken csak a gyártásban lévő rack szekrényekhez vezet optikai szál, a nagyobb megbízhatóság, és a gyártási rendszerek okozta interferencia elkerülése végett.

4.2.6 SFP modulok

Az optikai kábeleknek megfelelően, 10Gb/s-os multimódusú Mikrotik SFP modulokat alkalmaztunk kivéve a Moxa switchekhez, mivel azokkal csak a saját gyártmányú modulok támogatottak. A Mikrotik modulok az alábbi képen láthatóak.



61. ábra: Mikrotik SFP modul



Michaela Monke

MonkeBricks Kft.

mailto: michaelam@monkebricks.eu

5. ÁRAJÁNLAT

Köszönettel vettük megkeresésüket. Az alábbiakban találják árajánlatunkat, amely reméljük, hogy elnyeri tetszésüket. Amennyiben bármilyen kérdésük lenne az ajánlat tartalmával kapcsolatban, állunk szíves rendelkezésükre.

Az ajánlat tárgya:

Hálózati eszközök, szerverek és licencek. A teljes árajánlat a monke_table táblázatban található.

Eszköz/Komponens	Mennyiség (db)	Egységár (EUR)	Összesen (EUR)
Juniper eszközök			
Juniper SRX300 tűzfal	4	900,00 €	3 600,00 €
Juniper EX2300 switch	3	1 725,00 €	5 175,00 €
Juniper EX4100 switch	1	7 900,00 €	7 900,00 €
Juniper AP45 access point	13	1 500,00 €	19 500,00 €
Juniper támogatás (next business day RMA)	–	–	5 800,00 €
Juniper eszközök összesen			41 975,00 €
IBM eszközök			
IBM System x3250 M5 szerver	4	650,00 €	2 600,00 €
Windows Server 2025 Standard Licenc	4	840,00 €	3 360,00 €
IBM támogatás (azonnali cserével)	–	–	1 200,00 €
IBM eszközök összesen			7 160,00 €
Végösszeg			49 135,00 €

Győr, 2025. április 8.

M. Monke
Michaela Monke
Cégtulajdonos

5.1 INTERNET ELŐFIZETÉS

5.1.1 Központi iroda internet csomag

Mivel a központi irodában lesz a legtöbb irodai alkalmazott, és számos informatikai folyamat itt központosul, ezért itt számoltunk a legnagyobb hálózati forgalommal. A Telekommal ezért egy vállalati csomag keretében 200/200 Mbit/s-os (letöltés/feltöltés) sávszélességet biztosító szolgáltatásra szerződtünk. Természetesen ebbe beleszámoltuk a jövőbeli bővülési lehetőségeket.

5.1.2 Telephelyi internet csomag

A gyártási telephelyekre jelentősen kisebb hálózati forgalom lesz, ezért itt csak 100/100 Mbit/s-os internetszolgáltatást biztosítanak a vállalatnak. A központtal ellentétben ezekre a településekre nagymértékben költségesebb volt a szolgáltatóval bevezettetni a megfelelő hálózati forráspontokat.

6. TESZTELÉS

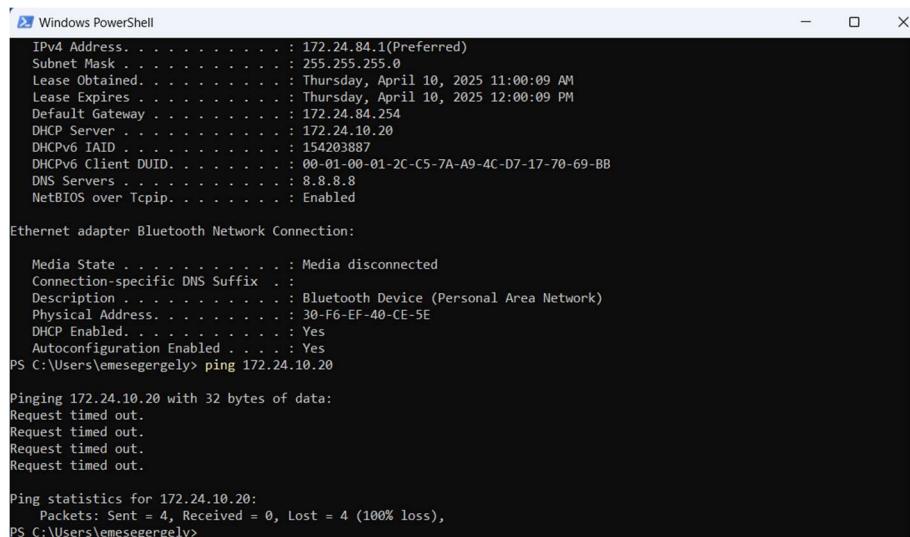
6.1 PING TESZTELÉS

Az alábbi képen (62. ábra) egy vezetéknélküli hálózaton lévő laptopról pingelünk egy, a központban lévő kliens számítógépet. Ezzel egyszerre vizsgáljuk a WiFi hálózatot, az IP címzést, a telephelyek közti IPSec tunnelt, valamint a dinamikus DNS-t, és a tűzfal szabályokat is.

```
Wireless LAN adapter Wi-Fi:  
  
  Connection-specific DNS Suffix  . : mb.monke.eu  
  Link-local IPv6 Address  . . . . . : fe80::64ed:e970:2507:a4cb%16  
  IPv4 Address. . . . . : 172.24.45.2  
  Subnet Mask . . . . . : 255.255.255.0  
  Default Gateway . . . . . : 172.24.45.254  
  
Ethernet adapter Bluetooth Network Connection:  
  
  Media State . . . . . : Media disconnected  
  Connection-specific DNS Suffix  . :  
  
C:\Users\emesegergely>ping pc001.monke.eu  
  
Pinging pc001.monke.eu [172.20.45.1] with 32 bytes of data:  
Reply from 172.20.45.1: bytes=32 time=3ms TTL=126  
Reply from 172.20.45.1: bytes=32 time=3ms TTL=126  
Reply from 172.20.45.1: bytes=32 time=4ms TTL=126  
Reply from 172.20.45.1: bytes=32 time=3ms TTL=126  
  
Ping statistics for 172.20.45.1:  
  Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
  Approximate round trip times in milli-seconds:  
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
```

62. ábra: Ping teszt 1

Az alábbi ábrán (63. ábra) a vendég WiFi hálózatra csatlakoztatott eszközről próbáljuk pingelni a gibbon szervert. A tűzfal szabályok megakadályozzák, hogy a céges belső hálózathoz hozzáférjenek a vendégek.



```

Windows PowerShell
IPv4 Address . . . . . : 172.24.84.1(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained . . . . . : Thursday, April 10, 2025 11:00:09 AM
Lease Expires . . . . . : Thursday, April 10, 2025 12:00:09 PM
Default Gateway . . . . . : 172.24.84.254
DHCP Server . . . . . : 172.24.10.20
DHCPv6 IAID . . . . . : 154203887
DHCPv6 Client DUID . . . . . : 00-01-00-01-2C-C5-7A-A9-4C-D7-17-70-69-B8
DNS Servers . . . . . : 8.8.8.8
NetBIOS over Tcpip . . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . .
    Description . . . . . : Bluetooth Device (Personal Area Network)
    Physical Address . . . . . : 30-F6-EF-40-CE-5E
    DHCP Enabled . . . . . : Yes
    Autoconfiguration Enabled . . . . . : Yes
PS C:\Users\emesegergely> ping 172.24.10.20

Pinging 172.24.10.20 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

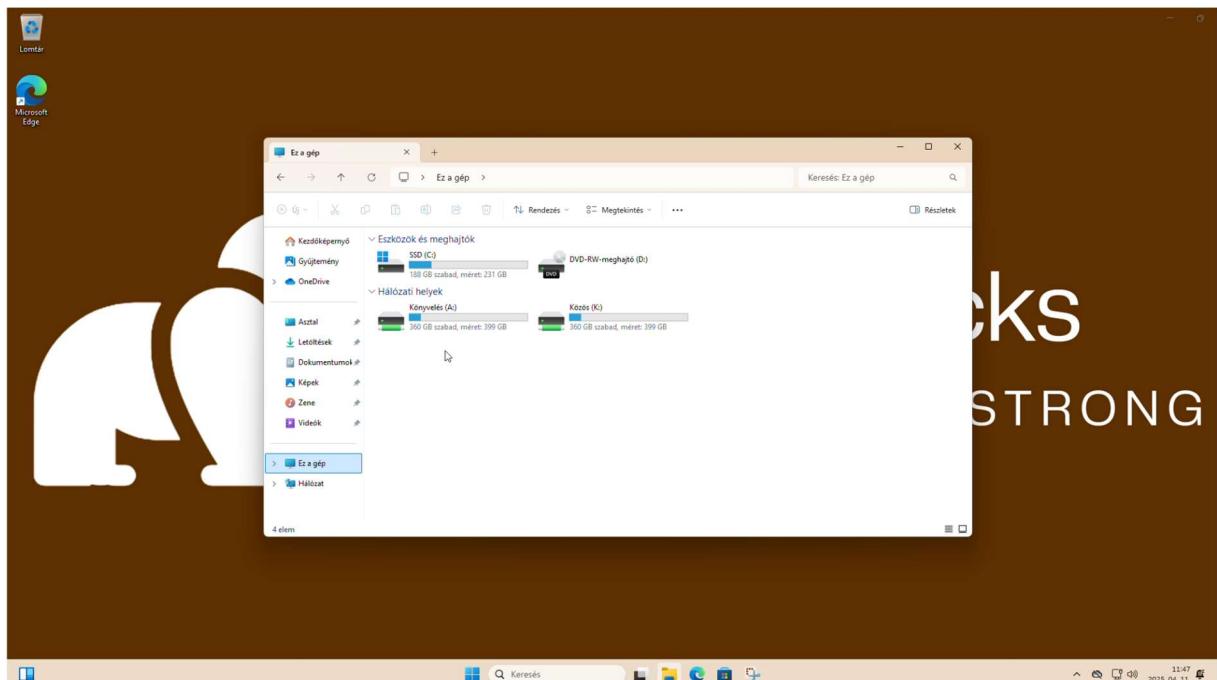
Ping statistics for 172.24.10.20:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
PS C:\Users\emesegergely>

```

63. ábra: Ping teszt 2

6.2 ACTIVE DIRECTORY TESZTELÉS

Az alábbi ábrán (64. ábra) több Group Policy beállítás tesztelése is látható. Érvényesül a háttérkép beállítás, valamint a felhasználónak megfelelő hálózati meghajtók is felcsatolásra kerülnek.



64. ábra: Háttérkép és meghajtók

Az alábbi képen (65. ábra) látható, hogy az egyik Group Policy beállítás megtiltja a felhasználóknak a parancssor használatát.

```
Parancssor
Microsoft Windows [Version 10.0.22631.4169]
(c) Microsoft Corporation. Minden jog fenntartva.

The command prompt has been disabled by your administrator.

Press any key to continue . . .
```

65. ábra: *CMD GPO*

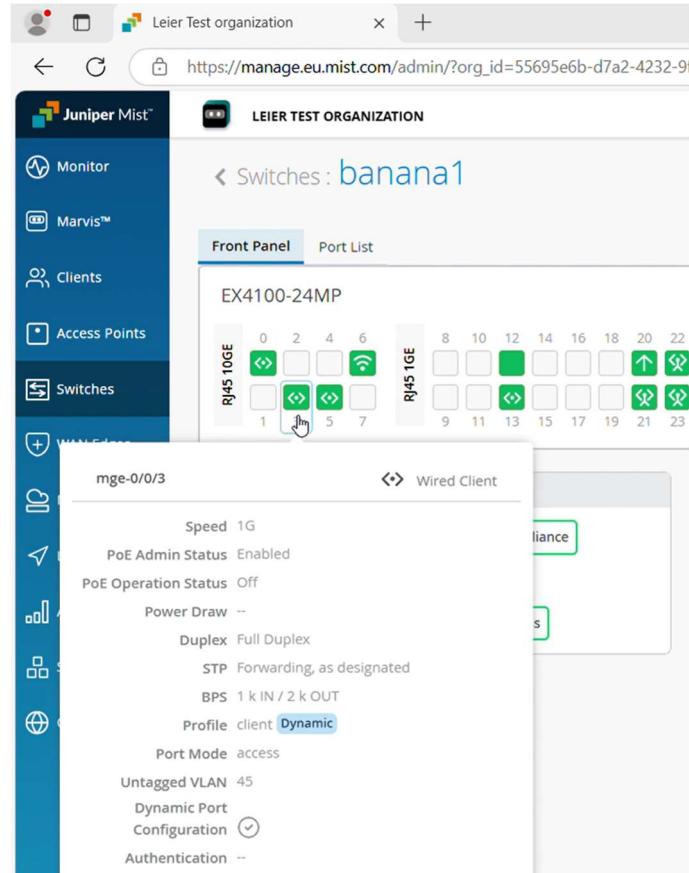
6.3 JUNIPER MIST TESZTELÉS

Az alábbi ábrán (66. ábra) a markotabödögei WiFi hálózatra csatlakozott kliensek láthatóak.

User	IPv4 Address	MAC Address	Device Type	AP Name	SSID	Pre-Shared Key	Insights
DESKTOP-DFBKT5K	172.24.45.2	30:96:ef:40:ce:5a	Intel Corporate	chimp1	Monike_Client		Client Insights
HUAWEI_P30_Pro-8604c2ac67	172.24.45.3	82:36:8e:cb:17:74	Unknown	chimp1	Monike_Client		Client Insights
iPhone	172.24.45.1	72:9b:40:c7:9b:7d	iOS	chimp1	Monike_Client		Client Insights
NOTE7701	172.24.45.4	2c:33:58:84:22:72	Intel Corporate	chimp1	Monike_Client		Client Insights

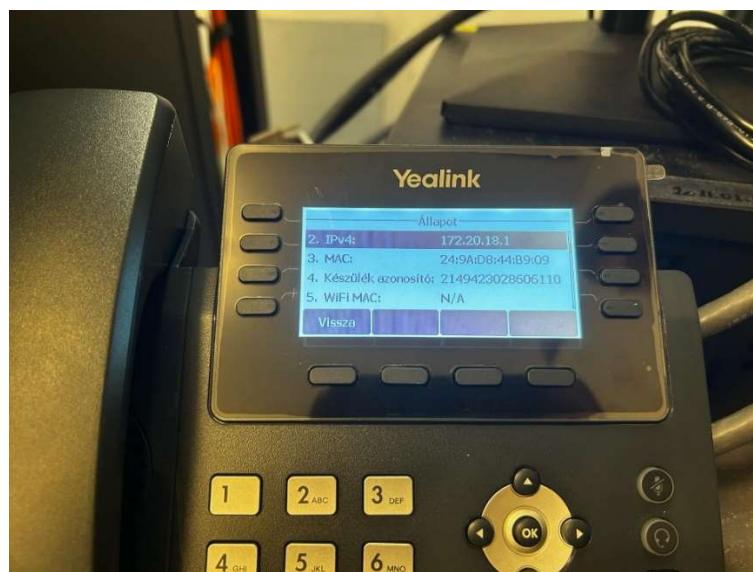
66. ábra: *Mist WiFi kliensek*

Az alábbi ábrán (67. ábra) látható, hogy az mge-0/0/3-as interfész dinamikusan módon konfigurálta magát a csatlakoztatott eszköznek megfelelő VLAN-ba.



67. ábra: Mist dinamikus VLAN konfiguráció

A dinamikus módon konfigurált porttal összekötött IP telefon kap IP címet a DHCP szervertől. (68. ábra)



68. ábra: IP telefon sikeresen kap DHCP-vel IP-t

6.4 HÁLÓZATI TESZTEK

Az alábbi képen (69. ábra) a központi tűzfalra konfigurált IPSec alagutak láthatóak.

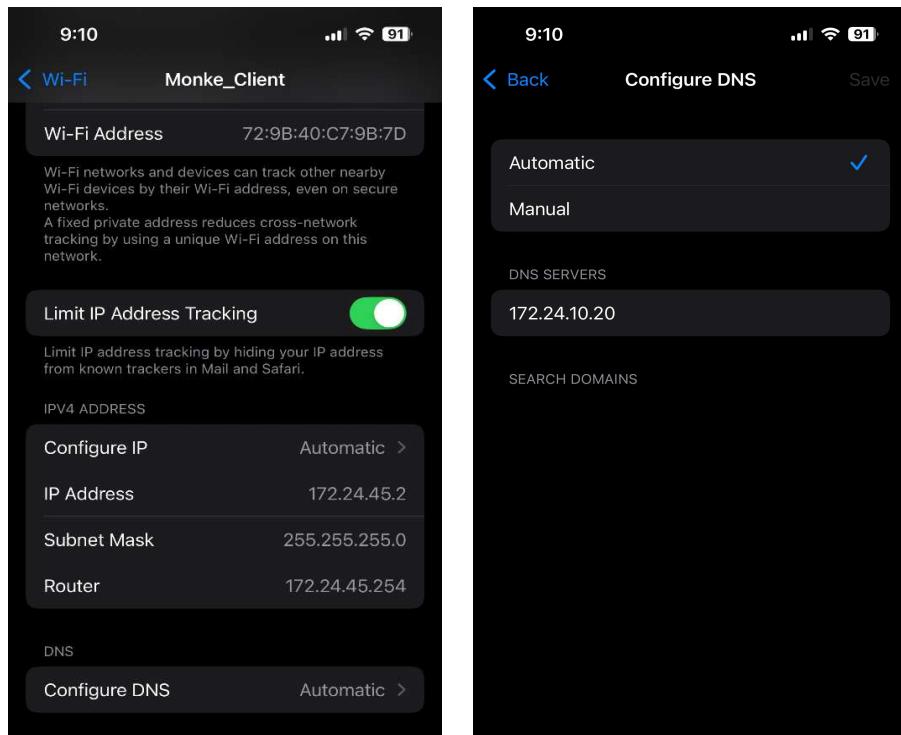
```
{primary:node0}
solett@orangutancluster1> show security ipsec security-associations
node0:
-----
Total active tunnels: 2      Total Ipsec sas: 3
ID  Algorithm      SPI      Life:sec/kb  Mon lsys Port  Gateway
<131073 ESP:aes-cbc-256/sha256 539e2052 2829/  unlim - root 500 213.253.195.237
>131073 ESP:aes-cbc-256/sha256 c732489d 2829/  unlim - root 500 213.253.195.237
<131074 ESP:aes-cbc-256/sha256 8c301f3e 2969/  unlim - root 500 213.253.195.235
>131074 ESP:aes-cbc-256/sha256 222fe0f5 2969/  unlim - root 500 213.253.195.235
<131074 ESP:aes-cbc-256/sha256 d1d814b7 2971/  unlim - root 500 213.253.195.235
>131074 ESP:aes-cbc-256/sha256 41dbc6c9 2971/  unlim - root 500 213.253.195.235

{primary:node0}
solett@orangutancluster1> show security ike security-associations
node0:
-----
Index  State  Initiator cookie  Responder cookie  Mode          Remote Address
5370354 UP    b75b4e2f8c124cd7  ba2ba6274c9ac3c0  Main          213.253.195.237
5370355 UP    3595828d06e651bd  8e05b6ae91241a7b  Main          213.253.195.235
```

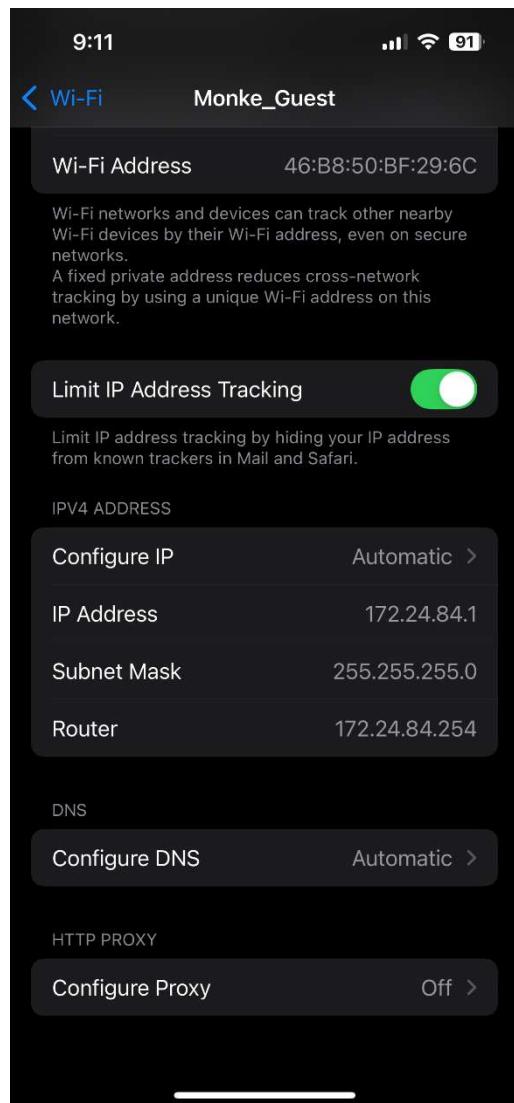
69. ábra: IPSec tunnel

6.5 WiFi TESZTELÉS

Az alábbi képeken (70. ábra, 71. ábra) mobilról csatlakoztunk a vezetéknélküli hálózatokra.



70. ábra: Monke_Client WiFi teszt



71. ábra: Monke_Guest WiFi teszt