**Monkebricks**

**Hálózati Dokumentáció**

Nagy-Raffay Barnabás

Sölét Tamás

Tartalom

[1. A projekt leírása 4](#_Toc191815423)

[1.1 A cég bemutatása és tervei 4](#_Toc191815424)

[1.2 A csapatmunka leírása 4](#_Toc191815425)

[2. A hálózat felépítése 4](#_Toc191815426)

[2.1 Logikai felépítés 4](#_Toc191815427)

[2.2 Telephelyek 4](#_Toc191815428)

[2.2.1 Központi iroda 4](#_Toc191815429)

[2.2.2 Markotabödögei telephely 4](#_Toc191815430)

[2.2.3 Taktaharkányi telephely 5](#_Toc191815431)

[2.3 VLAN felosztás 5](#_Toc191815432)

[2.4 Redundancia 5](#_Toc191815433)

[2.4.1 Második rétegbeli 5](#_Toc191815434)

[2.4.2 Harmadik rétegbeli 5](#_Toc191815435)

[2.4.3 Szolgáltatásredundancia 5](#_Toc191815436)

[2.5 Forgalomirányítás 6](#_Toc191815437)

[2.5.1 Statikus 6](#_Toc191815438)

[2.5.2 Dinamikus 6](#_Toc191815439)

[2.5.3 VPN 6](#_Toc191815440)

[2.6 Biztonság 6](#_Toc191815441)

[2.6.1 Statikus NAT 6](#_Toc191815442)

[2.6.2 PAT 6](#_Toc191815443)

[2.6.3 Tűzfal szabályok 6](#_Toc191815444)

[2.6.4 Jelszavak 6](#_Toc191815445)

[3. Szerverek 6](#_Toc191815446)

[3.1 A szerverek leírása 6](#_Toc191815447)

[3.2 Szolgáltatások 6](#_Toc191815448)

[3.2.1 Hyper-V 6](#_Toc191815449)

[3.2.2 AD 6](#_Toc191815450)

[3.2.3 DNS 7](#_Toc191815451)

[3.2.4 DHCP 7](#_Toc191815452)

[3.2.5 Fájl szerver 7](#_Toc191815453)

[3.2.6 VSS 7](#_Toc191815454)

[3.2.7 WEB 7](#_Toc191815455)

[3.2.8 NTP 7](#_Toc191815456)

[3.2.9 Zabbix 7](#_Toc191815457)

[3.2.9 Hálózatautomatizálás 8](#_Toc191815458)

[4. Felhasznált eszközök 8](#_Toc191815459)

[4.1 Hálózati eszközök 8](#_Toc191815460)

[4.1.1 Routerek, tűzfalak 8](#_Toc191815461)

[4.1.2 Switchek 9](#_Toc191815462)

[4.1.3 Szerverek 9](#_Toc191815463)

[4.1.4 AP-k 10](#_Toc191815464)

[4.1.5 Szünetmentes tápegységek 10](#_Toc191815465)

[4.2 Egyéb eszközök 10](#_Toc191815466)

[4.2.1 PC-k, Laptopok 10](#_Toc191815467)

[4.2.2 Nyomtatók 10](#_Toc191815468)

[4.2.3 Telefonok 10](#_Toc191815469)

[4.2.4 Kamerák 10](#_Toc191815470)

[4.3 Eszközök összeköttetése 11](#_Toc191815471)

[4.3.1 Kábelek (UTP, optika, DAC) 11](#_Toc191815472)

[4.3.2 SFP modulok, Média konverter 11](#_Toc191815473)

[4.3.3 DAC kábelek 11](#_Toc191815474)

[5. Árkalkuláció 11](#_Toc191815475)

[5.1 Eszközök költsége 11](#_Toc191815476)

[5.1.1 Hálózati eszközök (Juniper partner) 11](#_Toc191815477)

[5.1.2 Egyéb eszközök 11](#_Toc191815478)

[5.2 Licenszek, eszköztámogatás 11](#_Toc191815479)

[5.2.1 Microsoft 11](#_Toc191815480)

[5.2.2 Eszközök támogatása, egyedi garancia 11](#_Toc191815481)

[5.3 Internet előfizetés 11](#_Toc191815482)

[5.3.1 Központi iroda intenet csomag 11](#_Toc191815483)

[5.3.2 Telephelyi intenet csomag 11](#_Toc191815484)

[6. Összegzés 11](#_Toc191815485)

# 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

# 2. A hálózat felépítése

## 2.1 Logikai felépítés

## 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 legtöbben, 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. A legfontosabb eszközök a Juniper SRX300-as tűzfal, a Juniper EX2300-as switch, a Ruckus R750-es access point és az IBM \*\* szerver. 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 kimaradást biztosítják a nap 24 órájában.

### 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 kollegákra 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 swichekkel és ezek tárolására megfelelő rack szekrényekkel láttuk el a gyári csarnokokat. Az ilyen környezetbe szánt hálózati eszközöknek számos tényezőnek ellen kell állniuk, például a pornak vagy a magas páratartalmú levegőnek. Erre a célra mi a Moxa EDS-508a ipari swichet választottuk, ami az egyik legmegbízhatóbb eszköz indusztriális környezetben.

### 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 rejlik a különbség. 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.

## 2.3 VLAN felosztás

## 2.4 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.

### 2.4.1 Második rétegbeli

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.

### 2.4.2 Harmadik rétegbeli

Az általunk választott SRX300-as tűzfalak támogatják a Chassis Cluster üzemmódot, 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 meghibásodik, a másodlagos eszköz veszi át a forgalom feldolgozását.

### 2.4.3 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 adatveszteség és kimaradás nélkül átveszi a szerepét.
* 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.

## 2.5 Forgalomirányítás

### 2.5.1 Statikus

Statikus forgalomirányítást alkalmazunk minden telephelynél az alapértelmezett útvonal céljából. Erre a szolgáltató IP-címe van beállítva, mint következő ugrás cím.

### 2.5.2 Dinamikus

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 közt. 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 lekapcsoltnak 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 kimaradásokat és növeli a stabilitást kisebb LSA-változások esetén.

### 2.5.3 VPN

#### 2.5.3.1 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 kulcscsere, amely kiegyensúlyozott kompromisszumot biztosít a biztonság és teljesítény 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 Biztonság

### 2.6.1 Statikus NAT

### 2.6.2 PAT

### 2.6.3 Tűzfal szabályok

### 2.6.4 Jelszavak

# 3. Szerverek

## 3.1 A szerverek leírása

## 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.

### 3.2.2 AD

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

* monke.eu (Győr központ)
* mb.monke.eu (Markotabödöge)
* th.monke.eu (Taktaharkány)

Különböző Group Policy-kat állítottunk be, melyekkel például hálózati meghajtókhoz való hozzáférést tudjuk szabályozni.

A 3 tartomány fa struktúrát alkot, ez az xy képen látható.



### 3.2.3 DNS

### 3.2.4 DHCP

### 3.2.5 Fájl szerver

### 3.2.6 VSS

A VSS a lemur Windows szerveren fut, aminek feladata összehangolni azokat a műveleteket, amelyek szükségesek egy konzisztens árnyékmásolat (más néven pillanatkép vagy időpillanat-másolat) létrehozásához a biztonsági mentéshez. A biztonsági mentések minden hétköznap este 19:00-kor jönnek létre.

### 3.2.7 WEB

### 3.2.8 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.

### 3.2.9 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 előnyei:**

* Skálázhatóság – Könnyedén bővíthető, több ezer eszköz monitorozására is képes.
* Valós idejű megfigyelés – Azonnali értesítések és riasztások biztosítása.
* Automatizált felderítés – Új eszközök automatikus felismerése és hozzáadása.
* SNMP támogatás – Hálózati eszközök, például Juniper routerek és switchek SNMP protokoll segítségével történő felvétele.
* Részletes riportok és vizualizáció – Grafikonok, jelentések és teljesítményelemzések segítik az üzemeltetést.

**Zabbix automatizálás**

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.

**Hálózati eszközök monitorozása**

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.

### 3.2.9 Hálózatautomatizálás

# 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 tehettünk 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 feladatokat egy eszköz látja el, ami az SRX300. Ebből minden telephelyen 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.



### 4.1.2 Switchek

Switcheknek a Juniper EX2300 típusú, 48 portos eszközét választottuk. Ezekből telephelyenként szintén kettő található, melyek összhangban működnek egymással. A kapcsoló 1Gbps sebességet biztosít, és el van látva PoE+ minősítéssel, aminek segítségével képes árammal ellátni a cégnél használt telefonokat és kamerákat.



### 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.

A képen elektronika, Számítógép-alkatrész, Elektronikus eszköz, meghajtó látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### 4.1.4 AP-k

Az általunk választott, Ruckus R750 egy nagy teljesítményű Wi-Fi 6 (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.

A képen meghajtó, elektronika látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### 4.1.5 Szünetmentes tápegységek

## 4.2 Egyéb eszközök

### 4.2.1 PC-k, Laptopok

### 4.2.2 Nyomtatók

### 4.2.3 Telefonok

### 4.2.4 Kamerák

## 4.3 Eszközök összeköttetése

### 4.3.1 Kábelek (UTP, optika, DAC)

### 4.3.2 SFP modulok, Média konverter

### 4.3.3 DAC kábelek

# 5. Árkalkuláció

## 5.1 Eszközök költsége

### 5.1.1 Hálózati eszközök (Juniper partner)

### 5.1.2 Egyéb eszközök

## 5.2 Licenszek, eszköztámogatás

### 5.2.1 Microsoft

### 5.2.2 Eszközök támogatása, egyedi garancia

## 5.3 Internet előfizetés

### 5.3.1 Központi iroda intenet csomag

### 5.3.2 Telephelyi intenet csomag

# 6. Összegzés