**MonkeBricks**

**Hálózati Dokumentáció**

Nagy-Raffay Barnabás

Sölét Tamás

Tartalom

[1. A projekt leírása 4](#_Toc193398807)

[1.1 A cég bemutatása és tervei 4](#_Toc193398808)

[1.2 A csapatmunka leírása 4](#_Toc193398809)

[2. A hálózat felépítése 4](#_Toc193398810)

[2.1 Logikai felépítés 4](#_Toc193398811)

[2.2 Telephelyek 4](#_Toc193398812)

[2.2.1 Központi iroda 4](#_Toc193398813)

[2.2.2 Markotabödögei telephely 5](#_Toc193398814)

[2.2.3 Taktaharkányi telephely 5](#_Toc193398815)

[2.3 IP címzés 5](#_Toc193398816)

[2.3.1 Központ IP címzés 6](#_Toc193398817)

[2.3.2 Markotabödöge IP címzés 7](#_Toc193398818)

[2.3.3 Taktaharkány IP címzés 8](#_Toc193398819)

[2.4 VLAN felosztás 9](#_Toc193398820)

[2.5 Redundancia 10](#_Toc193398821)

[2.5.1 Második rétegbeli 10](#_Toc193398822)

[2.5.2 Harmadik rétegbeli 10](#_Toc193398823)

[2.5.3 Szolgáltatásredundancia 10](#_Toc193398824)

[2.6 Forgalomirányítás 11](#_Toc193398825)

[2.6.1 Statikus 11](#_Toc193398826)

[2.6.2 Dinamikus 11](#_Toc193398827)

[2.6.3 VPN 12](#_Toc193398828)

[2.7 Biztonság 14](#_Toc193398829)

[2.7.1 Statikus NAT 14](#_Toc193398830)

[2.7.2 PAT 14](#_Toc193398831)

[2.7.3 Tűzfal szabályok 14](#_Toc193398832)

[2.7.4 Jelszavak 14](#_Toc193398833)

[3. Szerverek 14](#_Toc193398834)

[3.1 A szerverek leírása 14](#_Toc193398835)

[3.2 Szolgáltatások 14](#_Toc193398836)

[3.2.1 Hyper-V 14](#_Toc193398837)

[3.2.2 AD 15](#_Toc193398838)

[3.2.3 DNS 16](#_Toc193398839)

[3.2.4 DHCP 16](#_Toc193398840)

[3.2.5 Fájl szerver 16](#_Toc193398841)

[3.2.6 VSS 17](#_Toc193398842)

[3.2.7 WEB 17](#_Toc193398843)

[3.2.8 NTP 17](#_Toc193398844)

[3.2.9 Zabbix 17](#_Toc193398845)

[3.2.9 Hálózatautomatizálás 18](#_Toc193398846)

[4. Felhasznált eszközök 18](#_Toc193398847)

[4.1 Hálózati eszközök 18](#_Toc193398848)

[4.1.1 Routerek, tűzfalak 19](#_Toc193398849)

[4.1.2 Switchek 19](#_Toc193398850)

[4.1.3 Szerverek 20](#_Toc193398851)

[4.1.4 AP-k 20](#_Toc193398852)

[4.1.5 Szünetmentes tápegységek 21](#_Toc193398853)

[4.2 Egyéb eszközök 21](#_Toc193398854)

[4.2.1 PC-k, Laptopok 21](#_Toc193398855)

[4.2.2 Nyomtatók 21](#_Toc193398856)

[4.2.3 Telefonok 21](#_Toc193398857)

[4.2.4 Kamerák 21](#_Toc193398858)

[4.3 Eszközök összeköttetése 21](#_Toc193398859)

[4.3.1 Kábelek (UTP, optika, DAC) 21](#_Toc193398860)

[4.3.2 SFP modulok, Média konverter 21](#_Toc193398861)

[4.3.3 DAC kábelek 21](#_Toc193398862)

[5. Árkalkuláció 22](#_Toc193398863)

[5.1 Eszközök költsége 22](#_Toc193398864)

[5.1.1 Hálózati eszközök (Juniper partner) 22](#_Toc193398865)

[5.1.2 Egyéb eszközök 22](#_Toc193398866)

[5.2 Licenszek, eszköztámogatás 22](#_Toc193398867)

[5.2.1 Microsoft 22](#_Toc193398868)

[5.2.2 Eszközök támogatása, egyedi garancia 22](#_Toc193398869)

[5.3 Internet előfizetés 22](#_Toc193398870)

[5.3.1 Központi iroda intenet csomag 22](#_Toc193398871)

[5.3.2 Telephelyi internet csomag 22](#_Toc193398872)

[6. Összegzés 22](#_Toc193398873)

# 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 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 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 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 mindketten a lehető legtöbb szakmai gyakorlatot sajátítottuk el.

# 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 switchet 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 IP címzés

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 x. táblázatban láthatóak.

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

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 x. képen látható.

A képen szöveg, Betűtípus, képernyőkép, Grafika látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### 2.3.1 Központ IP címzés

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Eszköz neve** | **Port** | **logikai port** | **VLAN** | **IP cím** | **Csatlakozó eszköz** | **Csatlakozó port** |
| orangutancluster1  (orangutan1;orangutan2) | ge-0/0/3 | reth0 | - | 213.253.195.238/24 | ISP | - |
| ge-1/0/3 |
| ge-0/0/4 | reth1.18 reth1.25 reth1.84 | 18 25 84 | 172.20.18.254/24 172.20.25.254/24 172.20.84.254/24 | bananacluster1 | ge-0/0/46 |
| ge-1/0/4 | ge-1/0/46 |
| ge-0/0/5 | reth2.10 | 10 | 172.20.10.254/24 | ge-0/0/47 |
| ge-1/0/5 | ge-1/0/47 |
| ge-0/0/6 | reth3.45 | 45 | 172.20.45.254/24 | ge-0/1/2 |
| ge-1/0/6 | ge-1/1/2 |
| ge-0/0/7 | reth4.52 | 52 | 172.20.52.254/24 | ge-0/1/3 |
| ge-1/0/7 | ge-1/1/3 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Eszköz neve** | **Port** | **logikai port** | **VLAN** | **IP cím** | **Csatlakozó eszköz** | **Csatlakozó port** |
| bananacluster1 (banana1; banana2) | - | irb.0 | 25 | 172.20.25.20/24 | - | |
| ge-0/0/12 | ge-0/0/12.0 | 25 | - | silverback1 | IMM |
| ge-0/0/13 | ge-0/0/13.0 | 10 | Data |
| ge-1/0/12 | ge-1/0/12.0 | 25 | silverback2 | IMM |
| ge-1/0/13 | ge-1/0/13.0 | 10 | Data |
| ge-0/1/0 | ge-0/1/0.0 | 10;18;25;45;52;84 | banana2 | ge-1/1/0 |
| ge-0/1/1 | ge-0/1/1.0 | ge-1/1/1 |
| ge-1/1/0 | ge-1/1/0.0 | banana1 | ge-0/1/0 |
| ge-1/1/1 | ge-1/1/1.0 | ge-0/1/1 |
| ge-0/0/46 | ge-0/0/46.0 | 18;25;84 | orangutancluster1 | ge-0/0/4 |
| ge-1/0/46 | ge-1/0/46.0 | ge-1/0/4 |
| ge-0/0/47 | ge-0/0/47.0 | 10 | ge-0/0/5 |
| ge-1/0/47 | ge-1/0/47.0 | ge-1/0/5 |
| ge-0/1/2 | ge-0/1/2.0 | 45 | ge-0/0/6 |
| ge-1/1/2 | ge-1/1/2.0 | ge-1/0/6 |
| ge-0/1/3 | ge-0/1/3.0 | 52 | ge-0/0/7 |
| ge-1/1/3 | ge-1/1/3.0 | ge-1/0/7 |

### 2.3.2 Markotabödöge IP címzés

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Eszköz neve** | **Port** | **logikai port** | **VLAN** | **IP cím** | **Csatlakozó eszköz** | **Csatlakozó port** |
| orangutan1 | ge-0/0/0 | ge-0/0/0.0 | - | 213.253.195.237/24 | ISP | - |
| ge-0/0/1 | ge-0/0/1.18 | 18 | 172.24.18.254/24 | banana1 | ge-0/0/20 |
| ge-0/0/1.25 | 25 | 172.24.25.254/24 |
| ge-0/0/1.84 | 84 | 172.24.84.254/24 |
| ge-0/0/2 | ge-0/0/2.10 | 10 | 172.24.10.254/24 | ge-0/0/21 |
| ge-0/0/3 | ge-0/0/3.45 | 45 | 172.24.45.254/24 | ge-0/0/22 |
| ge-0/0/4 | ge-0/0/4.52 | 52 | 172.24.52.254/24 | ge-0/0/23 |
| banana1 | - | irb.0 | 25 | 172.24.25.20/24 | - | |
| ge-0/0/12 | ge-0/0/12.0 | 25 | - | silverback1 | IMM |
| ge-0/0/13 | ge-0/0/13.0 | 10 | Data |
| ge-0/1/0 | ge-0/1/0.0 | ? | banana2 | G1 |
| ge-0/0/20 | ge-0/0/20.0 | 18;25;84 | orangutan1 | ge-0/0/1 |
| ge-0/0/21 | ge-0/0/21.0 | 10 | ge-0/0/2 |
| ge-0/0/22 | ge-0/0/22.0 | 45 | ge-0/0/3 |
| ge-0/0/23 | ge-0/0/23.0 | 52 | ge-0/0/4 |
| banana2 | G1 | - | 201;25 | banana1 | ge-0/1/0 |
| - | Management | 25 | 172.24.25.21/24 | - | |

### 2.3.3 Taktaharkány IP címzés

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Eszköz neve** | **Port** | **logikai port** | **VLAN** | **IP cím** | **Csatlakozó eszköz** | **Csatlakozó port** |
| orangutan1 | ge-0/0/0 | ge-0/0/0.0 | - | 213.253.195.235/24 | ISP | - |
| ge-0/0/1 | ge-0/0/1.18 | 18 | 172.28.18.254/24 | banana1 | ge-0/0/44 |
| ge-0/0/1.25 | 25 | 172.28.25.254/24 |
| ge-0/0/1.84 | 84 | 172.28.84.254/24 |
| ge-0/0/2 | ge-0/0/2.10 | 10 | 172.28.10.254/24 | ge-0/0/45 |
| ge-0/0/3 | ge-0/0/3.45 | 45 | 172.28.45.254/24 | ge-0/0/46 |
| ge-0/0/4 | ge-0/0/4.52 | 52 | 172.28.52.254/24 | ge-0/0/47 |
| banana1 | - | irb.0 | 25 | 172.28.25.20/24 | - | |
| ge-0/0/12 | ge-0/0/12.0 | 25 | - | silverback1 | IMM |
| ge-0/0/13 | ge-0/0/13.0 | 10 | Data |
| ge-0/1/0 | ge-0/1/0.0 | 201 | banana2 | G1 |
| ge-0/0/44 | ge-0/0/44.0 | 18;25;84 | orangutan1 | ge-0/0/1 |
| ge-0/0/45 | ge-0/0/45.0 | 10 | ge-0/0/2 |
| ge-0/0/46 | ge-0/0/46.0 | 45 | ge-0/0/3 |
| ge-0/0/47 | ge-0/0/47.0 | 52 | ge-0/0/4 |
| banana2 | G1 | - | 201;25 | banana1 | ge-0/1/0 |
| - | Management | 25 | 172.28.25.21/24 | - | |

## 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 céghez érkező vendégek a vezetéknélküli kapcsolaton keresztül, a vendég VLAN-ba kerülnek.
* **voip**: A cég által használt IP telefonok alhálózata.
* **factory**: A két telephelyen, ahol az előállítás történik, az IP hálózatra kötött gyártássegítő eszközök forgalmát különíti el.

A VLAN táblázat az x. képen látható.

|  |  |  |
| --- | --- | --- |
| 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 |

## 2.5 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

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.

### 2.5.2 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.

### 2.5.3 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 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.

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 mindkét szerveren, ezzel akár az egyik fizikai szerver teljes kiesését is pótolni tudjuk. A replikációs felület az x. képen látható.

A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

## 2.6 Forgalomirányítás

### 2.6.1 Statikus

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

### 2.6.2 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.

### 2.6.3 VPN

#### 2.6.3.1 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.

## 2.7 Biztonság

### 2.7.1 Statikus NAT

### 2.7.2 PAT

### 2.7.3 Tűzfal szabályok

### 2.7.4 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.

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 x. képen látható.

A képen szöveg, képernyőkép, szoftver, Weblap látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

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 (Taktaharkány)

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



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 x. képen láthatóak.

A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

### 3.2.3 DNS

### 3.2.4 DHCP

### 3.2.5 Fájl szerver

A fájl szerverünk a lemur Windows szerven 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 naplózási 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 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

A hálózati konfigurációk beállítása, illetve a problémák feltárása gyakran túl sok időt vesznek igénybe. Ez akár a cég számára hálózati kimaradást vagy limitációt is eredményezhet, amit minden eszközzel igyekezetünk 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 hibákból származó tervezési és konfigurálási problémák.

**A Mist AI előnyei:**

1. **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 szükségességét, gyorsítva ezzel a problémák elhárítását.

1. **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.

1. **Önvezető hálózat**

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

1. **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.

1. **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.

1. **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.

# 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

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

A képen fal, Háztartási eszköz, fedett pályás, hűtőszekrény látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.A képen szöveg, monitor, multimédia, Megjelenítőeszköz látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.A szerverszobában nagy teljesítményű szünetmentes tápegységeket telepítettünk, ami áramszünet esetén képes közel fél óráig biztosít áramellátást. Azonban egy hosszabb kimaradás esetén sem állhat le a rendszerünk, ezért amint kimaradás lép fel elindul a telephelyen lévő ipari dízel aggregátor, aminek várhatóan 10 percre van szüksége, mire elegendő mennyiségű energiát képes kitermelni. 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.

## 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

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 mb/s-os (letöltés/feltöltés) sávszélességet biztosító szolgáltatásra szerződtünk. Természetesen ebbe beleszámoltuk a jövőbeli bővülési lehetőségeket.

### 5.3.2 Telephelyi internet csomag

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

# 6. Összegzés