KKK hálózati dokumentációja

Csete Ádám

Nagy Barnabás

Téringer Gergő

Tartalomjegyzék

[1. Projekt ismertetése 1](#_Toc191308354)

[1.1 A projekt célja 1](#_Toc191308355)

[1.2 A Kihagyhatatlan Kincsek Kiadó 1](#_Toc191308356)

[1.3 A cég felépítése 1](#_Toc191308357)

[1.3.1 Központ – Budapest 1](#_Toc191308358)

[1.3.2 Fiók – Debrecen 2](#_Toc191308359)

[1.3.3 Fiók – Szeged 2](#_Toc191308360)

[1.4 A cég igénye 2](#_Toc191308361)

[1.5 Csapatunk 3](#_Toc191308362)

[1.6 Csapatmunka 4](#_Toc191308363)

[2. Hálózat 5](#_Toc191308364)

[2.1 LAN 5](#_Toc191308365)

[2.1.1 Logikai topológia 5](#_Toc191308366)

[2.1.2 Fizikai topológia 8](#_Toc191308367)

[2.1.2.1 Épületek paraméterei 8](#_Toc191308368)

[2.1.2.2 Topológia 9](#_Toc191308369)

[2.1.3 VLAN-ok 14](#_Toc191308370)

[2.1.4 Kapcsolók 15](#_Toc191308371)

[2.1.5 IPv4 és IPv6 címzés 15](#_Toc191308372)

[2.1.6 VTP 25](#_Toc191308373)

[2.1.7 STP 25](#_Toc191308374)

[2.1.8 Második rétegbeli redundancia 25](#_Toc191308375)

[2.1.8.1 LACP 25](#_Toc191308376)

[2.1.9 Harmadik rétegbeli redundancia 25](#_Toc191308377)

[2.1.9.1 Redundáns kapcsolatok 25](#_Toc191308378)

[2.1.9.2 HSRP 25](#_Toc191308379)

[2.1.10 OSPFv2, OSPFv3 25](#_Toc191308380)

[2.1.11 Biztonság 25](#_Toc191308381)

[2.1.11.1 Fizikai biztonság 25](#_Toc191308382)

[2.1.11.2 Hitelesítés 26](#_Toc191308383)

[2.1.11.3 Belépés próbálkozások száma 26](#_Toc191308384)

[2.1.11.4 Inaktív időkorlát 26](#_Toc191308385)

[2.1.11.5 Webes felület 26](#_Toc191308386)

[2.1.11.6 SSH 27](#_Toc191308387)

[2.1.11.7 Management VLAN 29](#_Toc191308388)

[2.1.11.8 VLAN 30](#_Toc191308389)

[2.1.11.9 Nem használt portok 30](#_Toc191308390)

[2.1.11.10 Portbiztonság 30](#_Toc191308391)

[2.1.11.11 Trunk portok 30](#_Toc191308392)

[2.1.11.12 DHCP Snooping 30](#_Toc191308393)

[2.1.11.13 Dinamikus ARP-ellenőrzés 30](#_Toc191308394)

[2.1.11.14 BPDU Guard 31](#_Toc191308395)

[2.1.11.15 Root guard 31](#_Toc191308396)

[2.1.11.16 CDP letiltása 31](#_Toc191308397)

[2.1.11.17 ACL-ek 31](#_Toc191308398)

[2.1.11.18 unicast Reverse Path Forwarding (uRPF) 34](#_Toc191308399)

[2.1.11.19 WLAN 34](#_Toc191308400)

[2.1.11.20 OSPFv2 és OSPFv3 hitelesítés 34](#_Toc191308401)

[2.1.11.21 EIGRP hitelesítés 35](#_Toc191308402)

[2.1.11.22 BGP hitelesítés 36](#_Toc191308403)

[2.1.11.23 Passzív interfész 36](#_Toc191308404)

[2.1.11.24 HSRP hitelesítés 36](#_Toc191308405)

[2.1.11.25 Direkt kulcsok 37](#_Toc191308406)

[2.1.11.26 Hardveres tűzfal: ASA 37](#_Toc191308407)

[2.1.12 WIFI 37](#_Toc191308408)

[2.1.13 Bannerek 37](#_Toc191308409)

[2.2 WAN 37](#_Toc191308410)

[2.2.1 Internetszolgáltató 37](#_Toc191308411)

[2.2.2 BGP, statikus forgalomirányítás 38](#_Toc191308412)

[2.2.3 PPPoE 39](#_Toc191308413)

[2.2.4 PAT, SNAT 40](#_Toc191308414)

[2.2.5 DMVPN 41](#_Toc191308415)

[2.2.6 EIGRP 41](#_Toc191308416)

[3. Szerverek 41](#_Toc191308417)

[3.1 Windows szerverek 41](#_Toc191308418)

[3.1.1 ADDS, RODC, Sub domain 41](#_Toc191308419)

[3.1.2 Group Policy 41](#_Toc191308420)

[3.1.3 WDS 41](#_Toc191308421)

[3.1.4 Radius 41](#_Toc191308422)

[3.2 Linux szerverek 41](#_Toc191308423)

[3.2.1 KKK-LIN 41](#_Toc191308424)

[3.2.1.1 Ansible 41](#_Toc191308425)

[3.2.1.2 LibreNMS 41](#_Toc191308426)

[3.2.1.3 Webszerver 41](#_Toc191308427)

[3.2.1.4 Email 41](#_Toc191308428)

[3.2.1.5 Rsyslog 41](#_Toc191308429)

[3.2.2 KKK-VPN 41](#_Toc191308430)

[3.2.2.1 Wireguard 41](#_Toc191308431)

[3.2.3 Rsyslog kliens 41](#_Toc191308432)

[3.3 Felhő 41](#_Toc191308433)

[3.3.1 Amazon Web Services 42](#_Toc191308434)

[3.3.2 A felhő 42](#_Toc191308435)

[3.3.3 Webkiszolgáló 42](#_Toc191308436)

[3.3.4 Fájlkiszolgáló szolgáltatás 43](#_Toc191308437)

[3.3.5 Adatbázis szolgáltatás 44](#_Toc191308438)

[3.3.6 A weboldal 45](#_Toc191308439)

[4.Automatizáció 46](#_Toc191308440)

[4.1 Ansible kódok 47](#_Toc191308441)

[4.1.1 ADDS 47](#_Toc191308442)

[4.1.2 DNS 49](#_Toc191308443)

[4.1.3 DHCP 53](#_Toc191308444)

[4.1.4 ADDFS 57](#_Toc191308445)

[4.1.5 FSRM 62](#_Toc191308446)

[4.2 PowerShell 64](#_Toc191308447)

[5. Árkalkuláció 64](#_Toc191308448)

[6. Tesztelés 67](#_Toc191308449)

[6.1 Hálózat 67](#_Toc191308450)

[6.2 Szerverek 67](#_Toc191308451)

[7. Összegzés 67](#_Toc191308452)

1. Projekt ismertetése

1.1 A projekt célja

A projekt célja, hogy csapatunk elkészítse a Kihagyhatatlan Kincsek Kiadó zenei kiadó számára a cég teljes hálózatát. A projekt keretében meg kell terveznünk és ki kell alakítanunk a központi és a fiókirodák hálózatát és a közöttük lévő kapcsolódásokat. Emellett figyelembe kell venni a biztonsági intézkedéseket, hogy a zenei anyagok védelme és az elérhetősége megfelelően biztosított legyen. A célunk az, hogy egy stabil és megbízható hálózatot hozzunk létre, amely támogatja a cég napi működését, és lehetővé teszi a jövőbeni bővítéseket és innovációkat.

1.2 A Kihagyhatatlan Kincsek Kiadó

A Kihagyhatatlan Kincsek Kiadó egy zenei kiadó, amely egy új cég. A kiadó magyar zenei élet egyik meghatározó szereplője szeretne lenni. A cég célja, hogy támogassa a haza zenei tehetségeket, valamint elősegítse a zenei műfajok sokszínűségét. A kiadó különböző zenei stílusok széles spektrumát képviseli, beleértve a popot, rockot, jazz-t és klasszikus zenét.

Elkötelezett amellett, hogy lehetőséget biztosítson a feltörekvő művészek számára, miközben innovatív marketing- és promóciós megoldásokat kínál. A Kihagyhatatlan Kincsek Kiadó célja, hogy a legjobb zenei anyagokat juttassa el a közönséghez, valamint támogassa a zenei közösséget különféle projektek és események révén.

1.3 A cég felépítése

1.3.1 Központ – Budapest

A Kihagyhatatlan Kincsek Kiadó központja Budapesten található, ahol a cég főbb zenei tevékenységei zajlanak. A kiadói részleg keretében a szerződéskezelők felelősek a szerződések kezeléséért és a jogi dokumentumok nyomon követéséért. Emellett a digitális tartalomkezelő gondoskodik a zenei tartalmak online elérhetőségéről és menedzseléséről, míg zenei elemzők dolgoznak azon, hogy a legfrissebb zenei trendek figyelembevételével támogassák a kiadási döntéseket. A kiadói asszisztens pedig segíti a kiadási folyamatokat és elvégzi az adminisztratív feladatokat.

A marketing és PR osztály feladata, hogy a cég arculatát kialakítsa és a zenei kampányokat lebonyolítsa. A digitális marketing szakemberek online kampányokat terveznek és valósítanak meg különböző platformokon, beleértve a közösségi médiát és a hirdetéseket. A webfejlesztő a cég weboldalának karbantartásáért és frissítéséért felel, míg a grafikai tervezők a kiadványok borítóit és promóciós anyagait készítik. A szociális média menedzser kezeli a cég közösségi média platformjait, interakcióba lép a követőkkel, míg a PR szakértők kapcsolatot tartanak a sajtóval és a közönséggel.

A zenei produkció területén a hangmérnök a hangfelvételek készítésével és szerkesztésével foglalkozik professzionális szoftverek segítségével. A zenei producerek a zenei projektek digitális irányításáért felelnek, míg a zenei szerkesztők a zenei anyagok szerkesztését végzik. A zenei asszisztensek segítenek a stúdióban a felvételek előkészítésében és lebonyolításában.

Az adminisztrációs osztály pénzügyi elemzője pénzügyi kimutatásokat készít és elemzéseket végez, míg a HR menedzser a munkavállalók nyilvántartásait vezeti és a toborzási folyamatokat irányít. A titkárok adminisztratív támogatást nyújtanak a vezetőség számára, és az IT szakember felelős a számítógépes rendszerek és szoftverek működéséért és karbantartásáért.

A vezetői osztály magában foglalja a kiadói, a marketing és PR, a zenei produkciós és az adminisztrációs osztály vezetőit. Ezen szakemberek együttműködése biztosítja a cég tevékenységének hatékony irányítását és zökkenőmentes működését.

1.3.2 Fiók – Debrecen

A debreceni fiók a tehetségkutatásra specializálódott, és célja, hogy felfedezze és támogassa a helyi művészeket, valamint megvalósítsa a zenei közösség által megálmodott projekteket. A tehetségkutató szakember a helyi zenészek adatbázisának nyilvántartásáért felel, és szervezi a helyi zenészek audícióit. A zenei mentor támogatja a feltörekvő zenészeket, és tanácsokat ad a fejlődésükhöz.

A kiadói szolgáltatások területén a zenei marketing asszisztens kampányokat támogat a helyi zenekarok számára, míg a piackutató piaci elemzéseket és trendek kutatását végzi.

A debreceni fiókvezető koordinálja a fiók tevékenységeit, biztosítja a csapat hatékony együttműködését, és felügyeli a tehetségkutatás, zenei mentorálás, valamint a kiadói szolgáltatások projektjeit. Emellett kapcsolatot tart a helyi zenei közösséggel és stratégiai döntéseket hoz a fiók célkitűzéseinek elérése érdekében.

1.3.3 Fiók – Szeged

A szegedi fiók az eseményszervezésre és a helyi rendezvények lebonyolítására összpontosít. A csapat célja, hogy minél több zenei eseményt hozzon létre, amelyek bemutatják a helyi tehetségeket és erősítik a zenei közösséget. Az eseményszervező tervezi és koordinálja az eseményeket. A logisztikai szakember a rendezvényekhez szükséges eszközök és erőforrások tervezéséért és nyilvántartásáért felel, míg a színpadi technikus gondoskodik a technikai háttérről az események során, beleértve a világítást és a hangosítást.

A közönségkapcsolati menedzser digitális platformokon tartja a kapcsolatot a közönséggel, például e-mailek és közösségi média segítségével. A hírlevél szerkesztő készíti a cég hírlevelét, amely informálja a közönséget az újdonságokról és eseményekről. A visszajelzés-elemző gyűjti és elemzi a közönségi visszajelzéseket az események után, hogy javítsa a jövőbeli rendezvényeket.

A szegedi fiókvezető felel a fiók tevékenységeinek irányításáért, az események zökkenőmentes lebonyolításáért és a csapat munkájának összehangolásáért. Emellett biztosítja, hogy a rendezvények stratégiai célokat szolgáljanak, és erősítsék a helyi zenei közösséget.

1.4 A cég igénye

A **Kihagyhatatlan Kincsek Kiadó** egy dinamikusan fejlődő zenei kiadó. A cég célja, hogy a zenei iparban kiemelkedő szerepet töltsön be, és ennek érdekében fontos, hogy a digitális jelenlétüket is megfelelően támogassák.

A cég számára elengedhetetlen egy korszerű hálózat kialakítása, amely összeköti a központot és a fiókirodákat. Az alábbi speciális igények merültek fel a cég részéről, amelyeket a csapatunktól mindenképpen elvárnak a hálózat kialakítása során:

* **Zavartalan Hálózati Kapcsolatok**: A központ és a fiókirodák közötti stabil és gyors internetkapcsolat kialakítása alapvető fontosságú. Ez lehetővé teszi a munkatársak számára, hogy valós időben osszanak meg zenei fájlokat és projektinformációkat, így a zenei produkciók gördülékenyebbé válnak.
* **Adatbiztonság Megteremtése**: A cég hangsúlyt fektet a szerzői jogok védelmére és a zenei anyagok biztonságos tárolására. Olyan hálózati megoldásokat keresnek, amelyek lehetővé teszik a felhő alapú adattárolást, miközben biztosítják az adatok titkosítását és a hozzáférési jogosultságok szigorú ellenőrzését.
* **Hálózati Monitoring**: A cég elvárja, hogy az IT csapat a kezdeti időszakban folyamatosan figyelje a hálózat teljesítményét és biztonságát. A hálózati forgalom elemzése segít az esetleges problémák korai észlelésében, valamint a megelőző intézkedések megtételében.
* **VPN Hozzáférés**: A fiókirodák munkatársai számára biztosítani kell a távoli elérést a központi hálózathoz. A VPN rendszer kiépítése segít abban, hogy a dolgozók biztonságosan csatlakozhassanak a cég hálózatához.
* **Hálózati Eszközök Telepítése és Beállítása**: A cég elkötelezett amellett, hogy a legmodernebb hálózati eszközöket alkalmazza. A routerek, switch-ek és egyéb eszközök rendszeres frissítése és karbantartása elengedhetetlen a hálózat zökkenőmentes működéséhez.
* **Maga**s **erőforrás-igényű gépek**: A számára a munkájukból adódóan következő részlegek számára nagy teljesítményű gépeket kell elhelyezni: Grafikai Tervező, Webfejlesztő, Hangmérnök, Zenei Producer, Zenei Szerkesztő, IT szakember

A **Kihagyhatatlan Kincsek Kiadó** célja, hogy egy erős és biztonságos hálózatot alakítson ki, amely segíti a zenei produkciók hatékony lebonyolítását és a cég működésének zökkenőmentességét. A csapatunk feladata, hogy ezeket az igényeket teljesítse, és olyan hálózati megoldásokat kínáljon, amelyek hozzájárulnak a cég sikeréhez.

1.5 Csapatunk

A hálózat kiépítésével csapatunkat, Csete Ádámot, Nagy Barnabást és Téringer Gergőt bízták meg. A csapatunk által elvégzendő feladatok listája:

* Közös feladatok:
  + Logikai-, fizikai topológia elkészítése
  + Hardveres eszközök kiválasztása
  + A munka dokumentálása
  + Funkcionális tesztelés
* Nagy Barnabás:
  + Felhőszolgáltatások alkalmazása
* Csete Ádám:
  + Hálózati eszközök konfigurálása
* Téringer Gergő:
  + Szerverek szolgáltatásainak telepítése és konfigurálása
  + Automatizált folyamatok megvalósítása

A feladatok felosztása, közös megbeszélést követően kerülnek kiosztásra, és mindig egy másik tag fogja tesztelni, annak a működését. A fent említett, feladatkörökön kívül, a csapattársak, segítenek egymásnak, tehát mindenki részt vesz a hálózat minden részének konfigurálásában.

A csoportmunka során a csapatunk Messengeren, Discordon keresztül kommunikál, a feladatok kiosztása, pedig a Trello szoftvermenedzsment szoftveren keresztül végezzük, mivel kis csapat létszámra, ingyenes működése mellett rengeteg bővítése lehetőséget tartalmaz. A file-ok megosztására a Google Drive SaaS felhőszolgáltatást használjuk, illetve GitHub-ra mentjük a konfigurációs file-okat és Ansible scripteket.

A feladat elkészítése során a következő operációs rendszereket fogjuk használni:

* Debian 12.7
* Windows 10
* Windows Server 2022

1.6 Csapatmunka

A csapaton belüli kommunikáció fő platformjaként a Messengert használtuk, amely lehetővé tette a gyors és hatékony információcserét. A feladatok kiosztását és nyomon követését a Trello segítségével végeztük, biztosítva a projekt szervezettségét és átláthatóságát. A fájlok megosztására és verziókezelésére pedig a GitHubot alkalmaztuk, amely hozzájárult az egységes és rendezett munkafolyamathoz. Az *1. képen* látható a GitHub, *2. képen* pedig a Trello. A képek 2025.02.22.-én készültek.

A képen szöveg, képernyőkép, szám, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

. kép - GitHub: 2025.02.22

A képen szöveg, képernyőkép, szoftver, Számítógépes ikon látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

. kép - Trello: 2025.02.22

A képen szöveg, Emberi arc, képernyőkép, ember látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

. kép - Messenger

1. Hálózat

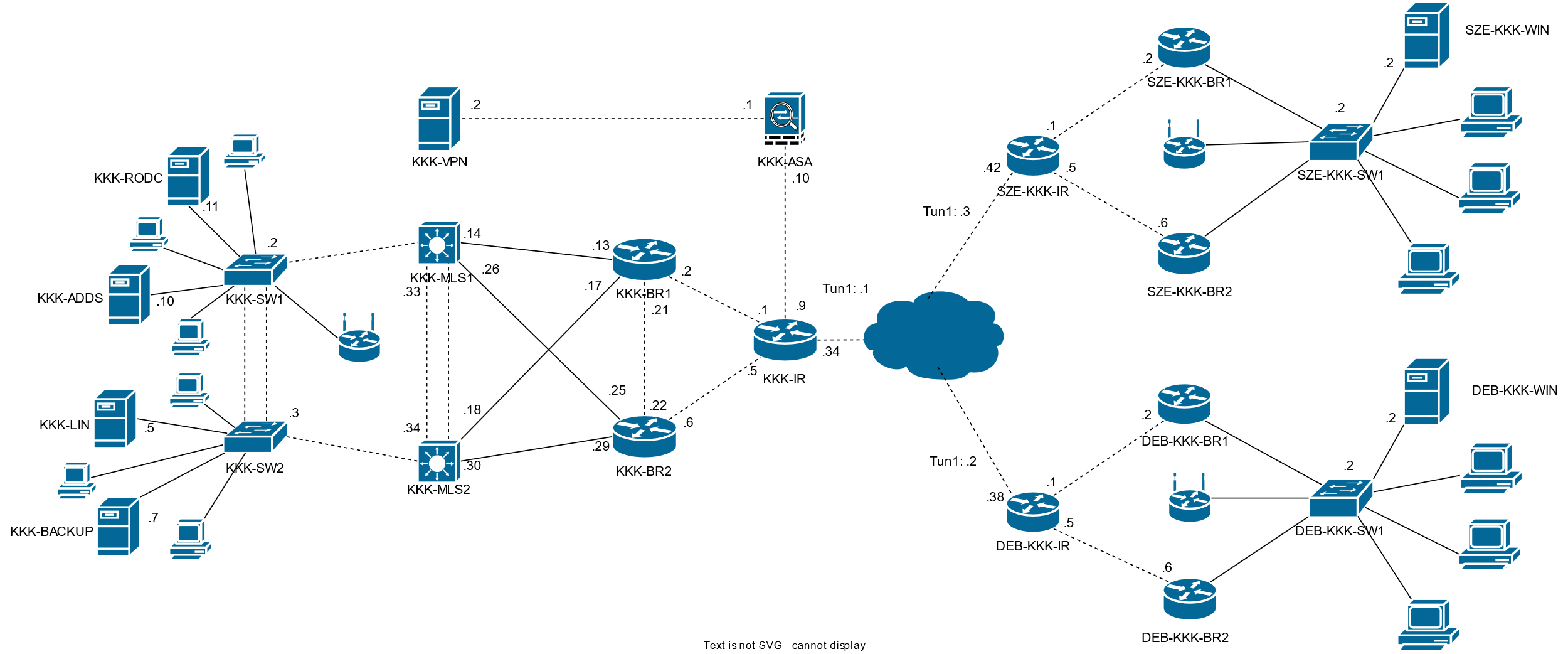
A Kihagyhatatlan Kincsek Kiadó hálózatát a következő rész mutatja be.

2.1 LAN

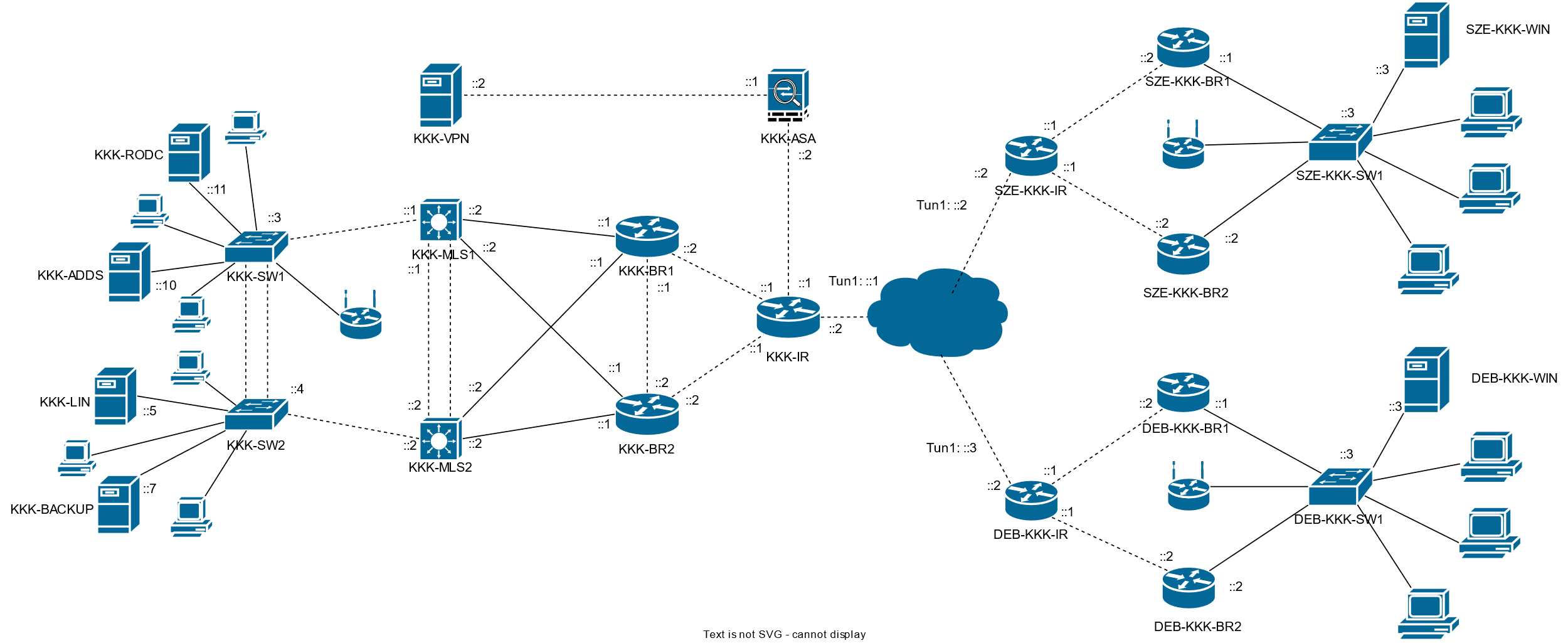
A következő alcímek alatt találhatók információk mind a három telephely helyi hálózatáról.

2.1.1 Logikai topológia

A *4. képen* az IPv4-es, a *5. képen* pedig az IPV6-os címek hoszt részeit tartalmazó logikai topológia látható, amiken mind a három telephely rajta van.



4. kép - Logikai topológia: IPv4 címek



. kép - Logikai topológia: IPv6 címe

2.1.2 Fizikai topológia

2.1.2.1 Épületek paraméterei

A központi épület négy szintből áll, míg a két fiókirodában csak földszint található. A központi épület közepén helyezkedik el a lépcső, és szintjeinek belső elosztása (a legfelső, harmadik szint kivételével) azonos. Ezért a földszint paraméterei megegyeznek a többi szint paramétereivel. A harmadik szint annyiban tér el, hogy néhány ajtó más helyre került, valamint a bal felső helyiségben egy válaszfal található, ami a 3,36 méter hosszú fallal párhuzamos és a mellette lévő két helyiség falával egy vonalban van. A dupla ajtók az épületek bejáratait jelölik. A budapesti épület paraméterei az *6. képen*, a szegedié az *7. képen*, a debrecenié pedig az *8. képen* láthatók.

A képen diagram, Tervrajz, Műszaki rajz, sematikus rajz látható

Automatikusan generált leírás

6. kép - A budapesti épület paraméterei

A képen diagram, Tervrajz, sor, Műszaki rajz látható

Automatikusan generált leírás

7. kép - A szegedi épület paraméterei

A képen diagram, Tervrajz, sor, képernyőkép látható

Automatikusan generált leírás

8. kép - A debreceni épület paraméterei

2.1.2.2 Topológia

A hálózat fizikai kialakítása során a cég kérésére nem helyeztünk el kábelt a mellékhelyiségek falában, hogy megóvjuk az ott lévő burkolatot. Ennek következtében bizonyos esetekben szinte az egész épületet meg kellett kerülni. Mindegyik épület minden szintjének belmagassága 3 méter. A központban a legtávolabbi PC is csak körülbelül 50 méter hosszú kábellel csatlakozik a kapcsolóhoz, ami bőven megfelel az Ethernet-szabvány által előírt 100 méteres maximális kábelhossznak. Ezáltal nem kell aggódni amiatt, hogy a földszinten lévő végpontok hálózati elérése jelentősen romlana a nagy távolság miatt. A kábelek minden épületben a falban futnak. A központi épületben minden szinten a jobb felső helyiség sarkában kerültek felvezetésre a legfelső emeleten található kapcsolókhoz. A fizikai topológiákon szürke vonal jelzi, hogy hol fut a kábel a falban. Minden helyiségbe dupla kábel lett vezetve és ezáltal dupla fali aljzat lett elhelyezve, hogy később, ha szükséges, rendelkezésre álljon tartalék. Így a fizikai topológiákon a zöld vonalak két UTP kábelt jelölnek. A fizikai topológiák a felsorolásban megadott képeken tekinthetők meg.

* budapesti épület földszintje a *9. képen*
* budapesti épület első emelete a *10. képen*
* budapesti épület második emelete a *11. képen*
* budapesti épület harmadik emelete a *12. képen*
* debreceni épület földszintje a *13. képen*
* szegedi épület földszintje a *14. képen*

látható.

A képen szöveg, diagram, képernyőkép, Tervrajz látható

Automatikusan generált leírás

9. kép - Fizikai topológia: budapesti épület földszintje

A képen szöveg, diagram, képernyőkép, Tervrajz látható

Automatikusan generált leírás

10. kép - Fizikai topológia: budapesti épület első emelete

A képen diagram, szöveg, képernyőkép, Tervrajz látható

Automatikusan generált leírás

11. kép - Fizikai topológia: budapesti épület második emelete

A képen szöveg, képernyőkép, diagram, Tervrajz látható

Automatikusan generált leírás

12. kép - Fizikai topológia: budapesti épület harmadik emelete

A képen szöveg, diagram, képernyőkép, Tervrajz látható

Automatikusan generált leírás

13. kép - Fizikai topológia: debreceni épület

A képen diagram, képernyőkép, sor, Tervrajz látható

Automatikusan generált leírás

14. kép - Fizikai topológia: szegedi épüle

2.1.3 VLAN-ok

A vállalatnál dolgozók foglalkozási köre alapján is kerültek kialakításra a VLAN-ok. Erre elsősorban azért volt szükség, hogy a dolgozók hálózati forgalma jól elkülönüljön, és ezáltal a későbbi vállalati irányelvek könnyebben érvényesíthetők legyenek. Emellett ez a megoldás biztosította a hálózat hatékony szegmentálását, valamint a szórási tartományok méretének csökkentését. Mivel a különböző telephelyeken eltérő szakmák képviseltetik magukat, a VLAN-ok is ennek megfelelően, telephelyenként kerültek kialakításra. A VLAN-ok azonosítását az adott telephely privát IP-címtartományának második oktettje segíti, amely megegyezik a VLAN-ok első két számjegyével. Az *1. táblázatban* látható a debreceni, a *2. táblázatban* a szegedi, a *3. táblázatban* pedig a központi telephely VLAN-jai.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  | | --- | --- | | **Debrecen VLAN** | | | **VLAN neve** | **VLAN száma** | | FIOKVEZETO | 3741 | | TEHETSEG | 3779 | | KIADO | 3737 | | |  |  | | --- | --- | | **Szeged VLAN** | | | **VLAN neve** | **VLAN száma** | | FIOKVEZETO | 2319 | | KOZONSEG | 2323 | | ESEMENY | 2341 | |
| . táblázat - VLAN: Debrecen | 2. táblázat - VLAN: Debrecen |

|  |  |
| --- | --- |
| **Központ VLAN** | |
| **VLAN neve** | **VLAN száma** |
| ADMINISZTRACIO | 1147 |
| MARKETING | 1173 |
| VEZETO | 1171 |
| KIADO | 1197 |
| ZENE | 1119 |

3. táblázat - VLAN: Központ

Emellett vannak olyan VLAN-ok, amik mind a három telephelyen megjelennek. Ez a MANAGEMENT, NATIVE VLAN. A fizikai biztonságot nyújtó Patent Cégcsoport számára lett létrehozva a BIZTONSAG VLAN. Az IT VLAN a rendszergazdáé, az SRV VLAN a szervereké, a WIFI VLAN pedig a AP-ké. A BLACKHOLE VLAN pedig a nem használt kapcsoló portoknak lett létrehozva. Ezek számai a *4. táblázatban* láthatóak.

|  |  |
| --- | --- |
| **Közös VLAN** | |
| **VLAN neve** | **VLAN száma** |
| MANAGEMENT | 37 |
| BLACKHOLE | 29 |
| **VLAN neve** | **VLAN száma** |
| NATIVE | 11 |
| WIFI | 41 |
| SRV | 13 |
| BIZTONSAG | 20 |
| IT | 69 |

4. táblázat - VLAN: Közös

2.1.4 Kapcsolók

A központban mindegyik második rétegbeli kapcsoló a G1/1/1-es interfészével kapcsolódik az adott MLS kapcsolóhoz, vagyis a KKK-SW1 a KKK-MLS1-hez a KKK-SW2 a KKK-MLS2-höz. A harmadik rétegbeli kapcsolók pedig a G1/1/3-as interfészeivel kapcsolódnak. Mindkét második rétegbeli kapcsolón a kettő közötti port-channel-ben a G1/1/2 és a G1/1/3 interfésze van benne. A KKK-SW1 G1/0/1 interfészéhez a KKK-RODC, a G1/0/2 porthoz pedig a KKK-ADDS szerver csatlakozik. A KKK-SW2 G1/0/1 interfészéhez a KKK-LIN, a G1/0/2-hőz a KKK-BACKUP kapcsolódik. A földszint és az első emelet AP-ja a KKK-SW1 G1/0/3 és G1/0/4 interfészéhez, a többi AP pedig lentről-felfelé a KKK-SW2 G1/0/3 és G1/0/4 portjaihoz kapcsolódik. A KKK-SW1 G1/0/5-as portjától a G1/0/36-os portjáig csatlakozik az első 16 kliens. Fentről lefele, illetve minden szinten a szerver teremnek megfelelő helyiség az első és utána a fizikai topológián balra haladva van a kliensek sorrendje. Ez alapján KKK-SW1 kapcsolón a Kiadói vezető az első és a Hangmérnök az utolsó. A port kiosztás ugyanígy folytatódik a KKK-SW2 kapcsolón. Mindkét kapcsolón lett hagyva 8-8 port az esetleges későbbi bővítéshez.

Mind a debreceni, mind pedig a szegedi telephelyen is a kapcsoló G1/1/1 interfésze az ottani BR1 forgalomirányítóhoz kapcsolódik, a G1/1/2 interfésze pedig a BR2-höz. Mindkét telephelyen a szerverek a G1/0/40 interfészhez kapcsolódnak, az AP-k pedig a G1/0/35 porthoz kapcsolódnak. A fizikai topológián a debreceni telepen balra indulva, a szegedin pedig jobbra indulva lettek kiosztva a portok a G1/0/1-től.

2.1.5 IPv4 és IPv6 címzés

A hálózat dual-stack, vagyis minden eszköz rendelkezik IPv6-os és IPv4-es címmel. IPv4 esetén 10.0.0.0/8 privát IPv4 cím tartomány lett felosztva a telephelyek között. A központi telephelyen 10.11.0.0/16, debrecenin a 10.37.0.0/16, a szegedin pedig a 10.23.0.0/16 tartomány lett tovább osztva. Az *5. táblázatban* központi, a *6. táblázatban* a szegedi, a *7. táblázatban* pedig a debreceni tartomány tovább osztása láható.

|  |  |  |
| --- | --- | --- |
| **Központ - IPv4** | | |
| **IPv4 hálózatcím** | **Maszk** | **Megjegyzés** |
| 10.11.47.0 | /27 | ADMINISZTRACIO VLAN |
| 10.11.73.0 | /26 | MARKETING VLAN |
| 10.11.71.0 | /28 | VEZETO VLAN |
| 10.11.97.0 | /27 | KIADO VLAN |
| 10.11.19.0 | /26 | ZENE VLAN |
| **IPv4 hálózatcím** | **Maszk** | **Megjegyzés** |
| 10.11.208.0 | /20 | BIZTONSÁG |
| 10.11.137.0 | /26 | MANAGEMENT VLAN |
| 10.11.140.0 | /22 | WIFI VLAN |
| 10.11.113.0 | /28 | SRV VLAN |
| 10.11.169.0 | /28 | IT VLAN |
| 10.11.250.0 | /24 | PONT-PONT KAPCSOLATOK |
| 10.11.199.0 | /29 | ASA ALHÁLÓZAT |
| 10.11.255.0 | /24 | Loopback |

5. táblázat - IPv4 cím felosztás: Központ

|  |  |  |
| --- | --- | --- |
| **Szeged - IPv4** | | |
| **IPv4 hálózatcím** | **Maszk** | **Megjegyzés** |
| 10.23.19.0 | /29 | FIOKVEZETO VLAN |
| 10.23.23.0 | /28 | KOZONSEG VLAN |
| 10.23.41.0 | /28 | ESEMENY VLAN |
| 10.23.137.0 | /27 | MANAGEMENT VLAN |
| 10.23.140.0 | /23 | WIFI VLAN |
| 10.23.208.0 | /20 | BIZTONSÁG |
| 10.23.113.0 | /29 | SRV VLAN |
| 10.23.169.0 | /29 | IT VLAN |
| 10.23.250.0 | /24 | PONT-PONT KAPCSOLATOK |
| 10.23.255.0 | /24 | Loopback |

6. táblázat - IPv4 cím felosztás: Szeged

|  |  |  |
| --- | --- | --- |
| **Debrecen - IPv4** | | |
| **IPv4 hálózatcím** | **Maszk** | **Megjegyzés** |
| 10.37.41.0 | /29 | FIOKVEZETO VLAN |
| 10.37.79.0 | /28 | TEHETSEG VLAN |
| 10.37.37.0 | /28 | KIADO VLAN |
| 10.37.137.0 | /27 | MANAGEMENT VLAN |
| 10.37.140.0 | /23 | WIFI VLAN |
| 10.37.208.0 | /20 | BIZTONSÁG |
| 10.37.113.0 | /29 | SRV VLAN |
| 10.37.169.0 | /29 | IT VLAN |
| 10.37.250.0 | /24 | PONT-PONT KAPCSOLATOK |
| 10.37.255.0 | /24 | Loopback |

7. táblázat - IPv4 cím felosztás: Debrecen

IPv6 esetében a 2001:db8:c1c1::/48-as címtartomány lett szétosztva a telephelyek között. A központ kapta a 2001:db8:c1c1:ab00::/56-os, a szegedi telep a 2001:db8:c1c1:c100::/56-os, a debreceni telep pedig a 2001:db8:c1c1:ba00::/56-os tartomány kapta. Ezek lettek tovább osztva /64-es tartományokra. A pont-pont kapcsoltoknál csak link-local címek lettek használva. A 8*. táblázatban* központi, a *9. táblázatban* a szegedi, a *10. táblázatban* pedig a debreceni tartomány tovább osztása láható.

|  |  |
| --- | --- |
| **Központ - IPv6** | |
| **IPv6 alhálózat** | **Megjegyzés** |
| 2001:db8:c1c1:abb1::/64 | ADMINISZTRACIO VLAN |
| 2001:db8:c1c1:abf8::/64 | MARKETING VLAN |
| 2001:db8:c1c1:abba::/64 | VEZETO VLAN |
| 2001:db8:c1c1:abf6::/64 | KIADO VLAN |
| 2001:db8:c1c1:ab8d::/64 | ZENE VLAN |
| 2001:db8:c1c1:ab20::/64 | BIZTONSÁG |
| 2001:db8:c1c1:ab8a::/64 | MANAGEMENT VLAN |
| 2001:db8:c1c1:abda::/64 | WIFI VLAN |
| 2001:db8:c1c1:abfa::/64 | SRV VLAN |
| 2001:db8:c1c1:abb5::/64 | IT VLAN |
| 2001:db8:c1c1:ab22::/64 | ASA alhálózata |
| 2001:db8:c1c1:abfe::/64 | Loopback |

8. táblázat – IPv6 cím felosztás: Központ

|  |  |
| --- | --- |
| **Szeged - IPv6** | |
| **IPv6 alhálózat** | **Megjegyzés** |
| 2001:db8:c1c1:babf::/64 | FIOKVEZETO VLAN |
| 2001:db8:c1c1:ba85::/64 | KOZONSEG VLAN |
| 2001:db8:c1c1:babc::/64 | ESEMENY VLAN |
| 2001:db8:c1c1:ba38::/64 | MANAGEMENT VLAN |
| 2001:db8:c1c1:bac1::/64 | WIFI VLAN |
| 2001:db8:c1c1:ba20::/64 | BIZTONSÁG |
| 2001:db8:c1c1:baba::/64 | SRV VLAN |
| 2001:db8:c1c1:bab3::/64 | IT VLAN |
| 2001:db8:c1c1:ba48::/64 | Loopback |

9. táblázat – IPv6 cím felosztás: Szeged

|  |  |
| --- | --- |
| **Debrecen - IPv6** | |
| **IPv6 alhálózat** | **Megjegyzés** |
| 2001:db8:c1c1:c155::/64 | FIOKVEZETO VLAN |
| 2001:db8:c1c1:c1a5::/64 | TEHETSEG VLAN |
| 2001:db8:c1c1:c15a::/64 | KIADO VLAN |
| 2001:db8:c1c1:c1e3::/64 | MANAGEMENT VLAN |
| 2001:db8:c1c1:c1c1::/64 | WIFI VLAN |
| 2001:db8:c1c1:c120::/64 | BIZTONSÁG |
| 2001:db8:c1c1:c1ca::/64 | SRV VLAN |
| 2001:db8:c1c1:c1b5::/64 | IT VLAN |
| 2001:db8:c1c1:c1d2::/64 | Loopback |

10. táblázat – IPv6 cím felosztás: Debrecen

A DMVPN tunnel-ben a 10.255.255.0/28-as címtartomány lett felosztva.

A kliensek és az AP-k DHCP-vel kapnak IPv4 és IPv6 címeket. IPv6 esetén állapottartó DHCPv6 szerver lett konfigurálva. A következő parancsok lettek alkalmazva DHCP kliensek felé néző interfészeken a megfelelő működés érdekében. Ezek segítik a szórásos üzenetek célba érését, illetve az állapottartó DHCPv6 szerver működését:

ipv6 dhcp relay destination 2001:db8:c1c1:abfa::10

ipv6 nd managed-config-flag

ipv6 nd prefix default no-autoconfig

ip helper-address 10.11.113.10

A hálózati eszközök és a szerverek statikusan kaptak IPv4 és IPv6 címet. IPv4 címei a

* központi forgalomirányítóknak a *11. táblázatban*,
* debreceni forgalomirányítóknak a *12. táblázatban*,
* szegedi forgalomirányítóknak a *13. táblázatban*,
* kapcsolóknak a *14. táblázatban*,
* szervereknek a *15. táblázatban*

láthatóak.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Központ - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| KKK-IR | G0/0/0 | 10.11.250.1 | /30 | KKK-BR1 | G0/0/2 |
| G0/0/1 | 10.11.250.5 | /30 | KKK-BR2 | G0/0/2 |
| Lo0 | 10.11.255.1 | /32 | - | |
| Dialer1 (g0/1/0) | 203.5.100.34 | /30 | ISP | Virtual-Access (g0/0/0) |
| Tun1 | 10.255.255.1 | /28 | SZE-KKK-IR DEB-KKK-IR | Tun1 |
| G0/0/2 | 10.11.250.9 | /30 | KKK-ASA | G0/8 |
| KKK-BR1 | G0/0/2 | 10.11.250.2 | /30 | KKK-IR | G0/0/0 |
| G0/0/0 | 10.11.250.13 | /30 | KKK-MLS1 | G1/1/1 |
| G0/0/1 | 10.11.250.17 | /30 | KKK-MLS2 | G1/1/1 |
| G0/1/0 | 10.11.250.21 | /30 | KKK-BR2 | G0/1/0 |
| Lo0 | 10.11.255.2 | /32 | - | |
| KKK-BR2 | G0/0/2 | 10.11.250.6 | /30 | KKK-IR | G0/0/1 |
| G0/0/0 | 10.11.250.25 | /30 | KKK-MLS1 | G1/1/2 |
| G0/0/1 | 10.11.250.29 | /30 | KKK-MLS2 | G1/1/2 |
| G0/1/0 | 10.11.250.22 | /30 | KKK-BR1 | G0/1/0 |
| Lo0 | 10.11.255.3 | /32 | - | |
| KKK-ASA | G0/5 | 10.11.199.1 | /29 | KKK-VPN | ens33 |
| G0/8 | 10.11.250.10 | /30 | KKK-IR | G0/0/2 |
| Lo0 | 10.11.255.6 | /32 | - | |

11. táblázat - IPv4 címek: Központ forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Debrecen - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| DEB-KKK-IR | G0/0/0 | 10.37.250.1 | /30 | DEB-KKK-BR1 | G0/0/2 |
| G0/0/1 | 10.37.250.5 | /30 | DEB-KKK-BR2 | G0/0/2 |
| Lo0 | 10.37.255.1 | /32 | - | |
| Dialer1 (G0/1/0) | 203.5.100.38 | /30 | ISP | Virtual-Access (G0/0/1) |
| Tun1 | 10.255.255.2 | /28 | SZE-KKK-IR KKK-IR | Tun1 |
| DEB-KKK-BR1 | G0/0/2 | 10.37.250.2 | /30 | DEB-KKK-IR | G0/0/0 |
| G0/0/0.41 | 10.37.41.5 | /29 | DEB-KKK-SW1 | G1/1/1 |
| G0/0/0.79 | 10.37.79.13 | /28 |
| G0/0/0.37 | 10.37.37.13 | /28 |
| G0/0/0.137 | 10.37.137.29 | /27 |
| G0/0/0.140 | 10.37.141.251 | /23 |
| G0/0/0.208 | 10.37.223.251 | /20 |
| G0/0/0.113 | 10.37.113.5 | /29 |
| G0/0/0.169 | 10.37.169.5 | /29 |
| Lo0 | 10.23.255.2 | /32 | - | |
| DEB-KKK-BR2 | G0/0/2 | 10.23.250.6 | /30 | DEB-KKK-IR | G0/0/1 |
| G0/0/0.41 | 10.37.41.6 | /29 | DEB-KKK-SW1 | G1/1/2 |
| G0/0/0.79 | 10.37.79.14 | /28 |
| G0/0/0.37 | 10.37.37.14 | /28 |
| G0/0/0.137 | 10.37.137.30 | /27 |
| G0/0/0.140 | 10.37.141.252 | /23 |
| G0/0/0.208 | 10.37.223.252 | /20 |
| G0/0/0.113 | 10.37.113.6 | /29 |
| G0/0/0.169 | 10.37.169.6 | /29 |
| Lo0 | 10.37.255.3 | /32 | - | |

12. táblázat - IPv4 címek: Debrecen forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Szeged - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| SZE-KKK-IR | G0/0/0 | 10.23.250.1 | /30 | SZE-KKK-BR1 | G0/0/2 |
| G0/0/1 | 10.23.250.5 | /30 | SZE-KKK-BR2 | G0/0/2 |
| Lo0 | 10.23.255.1 | /32 | - | |
| Dialer1 (G0/1/0) | 203.5.100.42 | /30 | ISP | Virtual-Access (G0/0/2) |
| Tun1 | 10.255.255.3 | /28 | DEB-KKK-IR KKK-IR | Tun1 |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| SZE-KKK-BR1 | G0/0/2 | 10.23.250.2 | /30 | SZE-KKK-IR | G0/0/0 |
| G0/0/0.19 | 10.23.19.5 | /29 | SZE-KKK-SW1 | G1/1/1 |
| G0/0/0.23 | 10.23.23.13 | /28 |
| G0/0/0.41 | 10.23.41.13 | /28 |
| G0/0/0.137 | 10.23.137.29 | /27 |
| G0/0/0.140 | 10.23.141.251 | /23 |
| G0/0/0.208 | 10.23.223.251 | /20 |
| G0/0/0.113 | 10.23.113.5 | /29 |
| G0/0/0.169 | 10.23.169.5 | /29 |
| Lo0 | 10.23.255.2 | /32 | - | |
| SZE-KKK-BR2 | G0/0/2 | 10.23.250.6 | /30 | SZE-KKK-IR | G0/0/1 |
| G0/0/0.19 | 10.23.19.6 | /29 | SZE-KKK-SW1 | G1/1/2 |
| G0/0/0.23 | 10.23.23.14 | /28 |
| G0/0/0.41 | 10.23.41.14 | /28 |
| G0/0/0.137 | 10.23.137.30 | /27 |
| G0/0/0.140 | 10.23.141.252 | /23 |
| G0/0/0.208 | 10.23.223.252 | /20 |
| G0/0/0.113 | 10.23.113.6 | /29 |
| G0/0/0.169 | 10.23.169.6 | /29 |
| Lo0 | 10.23.255.3 | /32 | - | |

13. táblázat - IPv4 címek: Szeged forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Switch** | | | | | |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| KKK-MLS1 | G1/1/1 | 10.11.250.14 | /30 | KKK-BR1 | G0/0/0 |
| G1/1/2 | 10.11.250.26 | /30 | KKK-BR2 | G0/0/0 |
| Port1 (G1/0/1-G1/0/2) | 10.11.250.33 | /30 | KKK-MLS2 | Port1 (G1/0/1-G1/0/2) |
| Lo0 | 10.11.255.4 | /32 | - | |
| Vlan 1147 | 10.11.47.29 | /27 | - | |
| Vlan 1173 | 10.11.73.59 | /26 |
| Vlan 1171 | 10.11.71.13 | /28 |
| Vlan 1197 | 10.11.97.29 | /27 |
| Vlan 1119 | 10.11.19.59 | /26 |
| Vlan 208 | 10.11.223.251 | /20 |
| Vlan 137 | 10.11.137.59 | /26 |
| Vlan 140 | 10.11.143.251 | /22 |
| Vlan 113 | 10.11.113.13 | /28 |
| Vlan 169 | 10.11.169.13 | /28 |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| KKK-MLS2 | G1/1/1 | 10.11.250.18 | /30 | KKK-BR1 | G0/0/1 |
| G1/1/2 | 10.11.250.30 | /30 | KKK-BR2 | G0/0/1 |
| Port1 (G1/0/1-G1/0/2) | 10.11.250.34 | /30 | KKK-MLS1 | Port1 (G1/0/1-G1/0/2) |
| Lo0 | 10.11.255.5 | /32 | - | |
| Vlan 1147 | 10.11.47.30 | /27 | - | |
| Vlan 1173 | 10.11.73.60 | /26 |
| Vlan 1171 | 10.11.71.14 | /28 |
| Vlan 1197 | 10.11.97.30 | /27 |
| Vlan 1119 | 10.11.19.60 | /26 |
| Vlan 208 | 10.11.223.252 | /20 |
| Vlan 137 | 10.11.137.60 | /26 |
| Vlan 140 | 10.11.143.252 | /22 |
| Vlan 113 | 10.11.113.14 | /28 |
| Vlan 169 | 10.11.169.14 | /28 |
| KKK-SW1 | Vlan 137 | 10.11.137.2 | /26 | - | |
| KKK-SW2 | Vlan 137 | 10.11.137.3 | /26 | - | |
| DEB-KKK-SW1 | Vlan 137 | 10.37.137.2 | /27 | - | |
| SZE-KKK-SW1 | Vlan 137 | 10.23.137.2 | /27 | - | |

14. táblázat - IPv4 címek: kapcsolók

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hosztok** | | | | | |
| **Eszköz** | **Interfész** | **IPv4 cím** | **Maszk** | **Másik eszköz** | **Interfész** |
| KKK-LIN | ens33 | 10.11.113.5 | /28 | KKK-SW2 | G1/0/1 |
| KKK-ADDS | Ethernet1 | 10.11.113.10 | KKK-SW1 | G1/0/2 |
| KKK-RODC | Ethernet1 | 10.11.113.11 | KKK-SW1 | G1/0/1 |
| KKK-VPN | ens33 | 10.11.199.2 | /29 | KKK-ASA | G0/5 |
| KKK-BACKUP | Ethernet1 | 10.11.113.7 | /28 | KKK-SW2 | G1/0/2 |
| DEB-KKK-WIN | Ethernet1 | 10.37.113.2 | /29 | DEB-KKK-SW1 | G1/0/40 |
| SZE-KKK-WIN | Ethernet1 | 10.23.113.2 | /29 | SZE-KKK-SW1 | G1/0/40 |

15. táblázat - IPv4 címek: hosztok

IPv6 címei a

* központi forgalomirányítóknak a *16. táblázatban*,
* debreceni forgalomirányítóknak a *17. táblázatban*,
* szegedi forgalomirányítóknak a *18. táblázatban*,
* kapcsolóknak a *19. táblázatban*,
* szervereknek a *20. táblázatban*

láthatóak.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Központ - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| KKK-IR | G0/0/0 | fe80:1::1 | | KKK-BR1 | G0/0/2 |
| G0/0/1 | fe80:2::1 | | KKK-BR2 | G0/0/2 |
| Lo0 | 2001:db8:c1c1:abfe::1/128 | fe80:abfe::1 | - | |
| Dialer1 (g0/1/0) | 2001:db8:baba:ab12::2/64 | fe80:ab12::2 | ISP | Virtual-Access (g0/0/0) |
| Tun1 | fe80:255::1 | | SZE-KKK-IR DEB-KKK-IR | Tun1 |
| G0/0/2 | fe80:9::1 | | KKK-ASA | G0/8 |
| KKK-BR1 | G0/0/2 | fe80:1::2 | | KKK-IR | G0/0/0 |
| G0/0/0 | fe80:3::1 | | KKK-MLS1 | G1/1/1 |
| G0/0/1 | fe80:4::1 | | KKK-MLS2 | G1/1/1 |
| G0/1/0 | fe80:5::1 | | KKK-BR2 | G0/1/0 |
| Lo0 | 2001:db8:c1c1:abfe::2/128 | fe80:abfe::2 | - | |
| KKK-BR2 | G0/0/2 | fe80:2::2 | | KKK-IR | G0/0/1 |
| G0/0/0 | fe80:6::1 | | KKK-MLS1 | G1/1/2 |
| G0/0/1 | fe80:7::1 | | KKK-MLS2 | G1/1/2 |
| G0/1/0 | fe80:5::2 | | KKK-BR1 | G0/1/0 |
| Lo0 | 2001:db8:c1c1:abfe::3/128 | fe80:abfe::3 | - | |
| KKK-ASA | G0/5 | 2001:db8:c1c1:ab22::1/64 | fe80:ab22::1 | KKK-VPN | ens33 |
| G0/8 | fe80:9::2 | | KKK-IR | G0/0/2 |
| Lo0 | 2001:db8:c1c1:abfe::4/128 | fe80:abfe::4 | - | |

16. táblázat – IPv6 címek: Központ forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Debrecen - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| DEB-KKK-IR | G0/0/0 | fe80:1::1 | | DEB-KKK-BR1 | G0/0/2 |
| G0/0/1 | fe80:2::1 | | DEB-KKK-BR2 | G0/0/2 |
| Lo0 | 2001:db8:c1c1:c1d2::1/128 | fe80:c1d2::1 | - | |
| Dialer1 (G0/1/0) | 2001:db8:baba:c112::2/64 | fe80:c112::2 | ISP | Virtual-Access (G0/0/1) |
| Tun1 | fe80:255::2 | | SZE-KKK-IR KKK-IR | Tun1 |
| DEB-KKK-BR1 | G0/0/2 | fe80:1::2 | | DEB-KKK-IR | G0/0/0 |
| G0/0/0.41 | 2001:db8:c1c1:c155::1/64 | fe80:c155::1 | DEB-KKK-SW1 | G1/1/1 |
| G0/0/0.79 | 2001:db8:c1c1:c1a5::1/64 | fe80:c1a5::1 |
| G0/0/0.37 | 2001:db8:c1c1:c15a::1/64 | fe80:c15a::1 |
| G0/0/0.137 | 2001:db8:c1c1:c1e3::1/64 | fe80:c1e3::1 |
| G0/0/0.140 | 2001:db8:c1c1:c1c1::1/64 | fe80:c1c1::1 |
| G0/0/0.208 | 2001:db8:c1c1:c120::1/64 | fe80:c1a20::1 |
| G0/0/0.113 | 2001:db8:c1c1:c1ca::1/64 | fe80:c1ca::1 |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| DEB-KKK-BR1 | G0/0/0.169 | 2001:db8:c1c1:c1b5::1/64 | fe80:c1b5::1 | DEB-KKK-SW1 | G1/1/1 |
| Lo0 | 2001:db8:c1c1:c1d2::2/128 | fe80:c1d2::2 | - | |
| DEB-KKK-BR2 | G0/0/2 | fe80:2::2 | | DEB-KKK-IR | G0/0/1 |
| G0/0/0.41 | 2001:db8:c1c1:c155::2/64 | fe80:c155::2 | DEB-KKK-SW1 | G1/1/2 |
| G0/0/0.79 | 2001:db8:c1c1:c1a5::2/64 | fe80:c1a5::2 |
| G0/0/0.37 | 2001:db8:c1c1:c15a::2/64 | fe80:c15a::2 |
| G0/0/0.137 | 2001:db8:c1c1:c1e3::2/64 | fe80:c1e3::2 |
| G0/0/0.140 | 2001:db8:c1c1:c1c1::2/64 | fe80:c1c1::2 |
| G0/0/0.208 | 2001:db8:c1c1:c120::2/64 | fe80:c1a20::2 |
| G0/0/0.113 | 2001:db8:c1c1:c1ca::2/64 | fe80:c1ca::2 |
| G0/0/0.169 | 2001:db8:c1c1:c1b5::2/64 | fe80:c1b5::2 |
| Lo0 | 2001:db8:c1c1:c1d2::3/128 | fe80:c1d2::3 | - | |

17. táblázat – IPv6 címek: Debrecen forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Szeged - Router** | | | | | |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| SZE-KKK-IR | G0/0/0 | fe80:1::1 | | SZE-KKK-BR1 | G0/0/2 |
| G0/0/1 | fe80:2::1 | | SZE-KKK-BR2 | G0/0/2 |
| Lo0 | 2001:db8:c1c1:ba48::1/128 | fe80:ba48::1 | - | |
| Dialer1 (G0/1/0) | 2001:db8:baba:ba12::2/64 | fe80:ba12::2 | ISP | Virtual-Access (G0/0/2) |
| Tun1 | fe80:255::3 | | DEB-KKK-IR KKK-IR | Tun1 |
| SZE-KKK-BR1 | G0/0/2 | fe80:1::2 | | SZE-KKK-IR | G0/0/0 |
| G0/0/0.19 | 2001:db8:c1c1:babf::1/64 | fe80:babf::1 | SZE-KKK-SW1 | G1/1/1 |
| G0/0/0.23 | 2001:db8:c1c1:ba85::1/64 | fe80:ba85::1 |
| G0/0/0.41 | 2001:db8:c1c1:babc::1/64 | fe80:babc::1 |
| G0/0/0.137 | 2001:db8:c1c1:ba38::1/64 | fe80:ba38::1 |
| G0/0/0.140 | 2001:db8:c1c1:bac1::1/64 | fe80:bac1::1 |
| G0/0/0.208 | 2001:db8:c1c1:ba20::1/64 | fe80:ba20::1 |
| G0/0/0.113 | 2001:db8:c1c1:baba::1/64 | fe80:baba::1 |
| G0/0/0.169 | 2001:db8:c1c1:bab3::1/64 | fe80:bab3::1 |
| Lo0 | 2001:db8:c1c1:ba48::2/128 | fe80:ba48::2 | - | |
| SZE-KKK-BR2 | G0/0/2 | fe80:2::2 | | SZE-KKK-IR | G0/0/1 |
| G0/0/0.19 | 2001:db8:c1c1:babf::2/64 | fe80:babf::2 | SZE-KKK-SW1 | G1/1/2 |
| G0/0/0.23 | 2001:db8:c1c1:ba85::2/64 | fe80:ba85::2 |
| G0/0/0.41 | 2001:db8:c1c1:babc::2/64 | fe80:babc::2 |
| G0/0/0.137 | 2001:db8:c1c1:ba38::2/64 | fe80:ba38::2 |
| G0/0/0.140 | 2001:db8:c1c1:bac1::2/64 | fe80:bac1::2 |
| G0/0/0.208 | 2001:db8:c1c1:ba20::2/64 | fe80:ba20::2 |
| G0/0/0.113 | 2001:db8:c1c1:baba::2/64 | fe80:baba::2 |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| SZE-KKK-BR2 | G0/0/0.169 | 2001:db8:c1c1:bab3::2/64 | fe80:bab3::2 | SZE-KKK-SW1 | G1/1/2 |
| Lo0 | 2001:db8:c1c1:ba48::3/128 | fe80:ba48::3 | - | |

18. táblázat – IPv6 címek: Szeged forgalomirányítói

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Központ - Switch** | | | | | |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| KKK-MLS1 | G1/1/1 | fe80:3::2 | | KKK-BR1 | G0/0/0 |
| G1/1/2 | fe80:6::2 | | KKK-BR2 | G0/0/0 |
| Port1 (G1/0/1-G1/0/2) | fe80:10::1 | | KKK-MLS2 | Port1 (G1/0/1-G1/0/2) |
| Lo0 | 2001:db8:c1c1:abfe::5/128 | fe80:abfe::5 | - | |
| Vlan 1147 | 2001:db8:c1c1:abb1::1/64 | fe80:abb1::1 | - | |
| Vlan 1173 | 2001:db8:c1c1:abf8::1/64 | fe80:abf8::1 |
| Vlan 1171 | 2001:db8:c1c1:abba::1/64 | fe80:abba::1 |
| Vlan 1197 | 2001:db8:c1c1:abf6::1/64 | fe80:abf6::1 |
| Vlan 1119 | 2001:db8:c1c1:ab8d::1/64 | fe80:ab8d::1 |
| Vlan 208 | 2001:db8:c1c1:ab20::1/64 | fe80:ab20::1 |
| Vlan 137 | 2001:db8:c1c1:ab8a::1/64 | fe80:ab8a::1 |
| Vlan 140 | 2001:db8:c1c1:abda::1/64 | fe80:abda::1 |
| Vlan 113 | 2001:db8:c1c1:abfa::1/64 | fe80:abfa::1 |
| Vlan 169 | 2001:db8:c1c1:abb5::1/64 | fe80:aba5::1 |
| KKK-MLS2 | G1/1/1 | fe80:4::2 | | KKK-BR1 | G0/0/1 |
| G1/1/2 | fe80:7::2 | | KKK-BR2 | G0/0/1 |
| Port1 (G1/0/1-G1/0/2) | fe80:10::2 | | KKK-MLS1 | Port1 (G1/0/1-G1/0/2) |
| Lo0 | 2001:db8:c1c1:abfe::6/128 | fe80:abfe::6 | - | |
| Vlan 1147 | 2001:db8:c1c1:abb1::2/64 | fe80:abb1::2 | - | |
| Vlan 1173 | 2001:db8:c1c1:abf8::2/64 | fe80:abf8::2 |
| Vlan 1171 | 2001:db8:c1c1:abba::2/64 | fe80:abba::2 |
| Vlan 1197 | 2001:db8:c1c1:abf6::2/64 | fe80:abf6::2 |
| Vlan 1119 | 2001:db8:c1c1:ab8d::2/64 | fe80:ab8d::2 |
| Vlan 208 | 2001:db8:c1c1:ab20::2/64 | fe80:ab20::2 |
| Vlan 137 | 2001:db8:c1c1:ab8a::2/64 | fe80:ab8a::2 |
| Vlan 140 | 2001:db8:c1c1:abda::2/64 | fe80:abda::2 |
| Vlan 113 | 2001:db8:c1c1:abfa::2/64 | fe80:abfa::2 |
| Vlan 169 | 2001:db8:c1c1:abb5::2/64 | fe80:aba5::2 |
| KKK-SW1 | Vlan 137 | 2001:db8:c1c1:ab8a::3/64 | fe80:ab80::3 | - | |
| KKK-SW2 | Vlan 137 | 2001:db8:c1c1:ab8a::4/64 | fe80:ab80::4 | - | |
| DEB-KKK-SW1 | Vlan 137 | 2001:db8:c1c1:c1e3::3/64 | fe80:c1e3::3 | - | |
| SZE-KKK-SW1 | Vlan 137 | 2001:db8:c1c1:ba38::3/64 | fe80:ba38::3 | - | |

19. táblázat – IPv6 címek: kapcsolók

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Hosztok** | | | | | |
| **Eszköz** | **Interfész** | **IPv6 cím** | **Link local** | **Másik eszköz** | **Interfész** |
| KKK-LIN | ens33 | 2001:db8:c1c1:abfa::5/64 | fe80:abfa::5 | KKK-SW2 | G1/0/1 |
| KKK-ADDS | Ethernet1 | 2001:db8:c1c1:abfa::10/64 | fe80:abfa::10 | KKK-SW1 | G1/0/2 |
| KKK-RODC | Ethernet1 | 2001:db8:c1c1:abfa::11/64 | fe80:abfa::11 | KKK-SW1 | G1/0/1 |
| KKK-VPN | ens33 | 2001:db8:c1c1:ab22::2/64 | fe80:ab22::2 | KKK-ASA | G0/5 |
| KKK-BACKUP | Ethernet1 | 2001:db8:c1c1:abfa::7/64 | fe80:abfa::7 | KKK-SW2 | G1/0/2 |

20. táblázat – IPv6 címek: hosztok

2.1.6 VTP

2.1.7 STP

2.1.8 Második rétegbeli redundancia

2.1.8.1 LACP

2.1.9 Harmadik rétegbeli redundancia

2.1.9.1 Redundáns kapcsolatok

2.1.9.2 HSRP

2.1.10 OSPFv2, OSPFv3

2.1.11 Biztonság

2.1.11.1 Fizikai biztonság

A központban a helyiség, ahol a szerverek és a hálózati eszközök találhatóak, az épület legfelső szintjén van és csak az IT szakember irodáján keresztül lehet bemenni, hogy minél nehezebben elérhető és felfedezhető legyen egy támadó számára. Az épületbe csak a biztonsági őr által beengedett, ott dolgozó személyek mehetnek be munkaidőben. Beléptető rendszer nem üzemel, mivel az alacsony létszámú személyzet miatt feleslegesnek lett ítélve. Kamerák találhatóak az összes szinten. A szerverekhez és a hálózati eszközökhöz, valamint az IT szakember irodájába csak az ott dolgozó IT szakember mehet be arc- és ujjlenyomat azonosítás, és egy hetente változó, 20 karakter hosszú jelszó megadása után.

A többi fiókirodában csak a fiókvezetők irodáján keresztül lehet bemenni a szerverekhez és a hálózati eszközökhöz. Hasonló biztonsági intézkedések vannak, mint a központban. A különbség, hogy nincs biometrikus azonosítás, mivel nincs helyi IT szakember. Csak egyszer használható, 20 karakter hosszú jelszavak vannak, amelyet a központban lévő IT szakember mondhat meg a fiókvezetőnek egyszerű hibák megoldására. Nagyobb hiba esetén az IT szakember személyes megjelenése szükséges. Ezeket egy másik cég (Patent Cégcsoport**)** telepítette és üzemelteti.

2.1.11.2 Hitelesítés

A hálózati eszközök kis száma miatt, valamint azért, mert csak egyetlen ember, az IT szakember férhet hozzá ezekhez, ezért ezeken a helyi adatbázis alapú hitelesítés lett választva egy központi AAA szerver helyett. Mindegyik eszközön jelszó került konfigurálásra a privilegizált EXEC módba való belépéshez. A felhasználónév minden eszköz konzol és VTY vonalán azonos. A jelszavak és a felhasználónevek minden eszközön megegyeznek, és a jelszavak mindegyiken titkosítva vannak tárolva. Mindegyik eszközön létre lett hozva egy kosa nevű felhasználó arra az esetre, ha távolról valamiért nem lehetne elérni az adott eszközt. Mivel ezzel a felhasználóval is be lehet jelentkezni a VTY vonalon, ezért a biztonság érdekében ez a felhasználó a 10-es privilege szintet kapta. A kosa felhasználóval privilegizált exec módban a configure terminal, globális konfigurációs módban az interface, valamint interfész konfigurációs módban a shutdown, a no shutdown, és az ip address parancsot lehet kiadni. Illetve még a kapcsolóknál a portokat lehet access típusúra állítani, valamint hozzárendelni a 37-es, management VLAN-hoz. Erre azért volt szükség, hogy ha a trunk port romlik el, akkor is el lehessen érni a management VLAN-t. Tehát ezzel a felhasználóval helyre lehet állítani egy meghibásodott interfészt, hogy után el lehessen érni az eszközt VTY vonalon. A jelszó és a felhasználónév a *x. táblázatban* látható.

|  |  |  |
| --- | --- | --- |
| **Jelszavak** | | |
| **Típus** | **Felhasználónév** | **Jelszó** |
| enable | **-** | 9@PqZ$7sRfT!1a |
| konzol | kosa | bxJ<5EMJegS;U+O]4={T |
| VTY |
| admin | **-** |

x. táblázat - Jelszavak

2.1.11.3 Belépés próbálkozások száma

A brute force támadások elleni védelem érdekében korlátozva lett egy megadott időn belüli belépés próbálkozások száma. A konfigurálás alapján 1 percen belüli 3 helytelen bejelentkezés után 10 percig nem lehet bejelentkezni.

2.1.11.4 Inaktív időkorlát

Ha a hitelesített felhasználók inaktívak, akkor egy idő után automatikusan ki lesznek jelentkeztetve. Erre azért van szükség, hogy illetéktelen felhasználók ne tudják használni ezeket a nyitva maradt bejelentkezéseket. A beállítások szerint egy bejelentkezés nyolc percig lehet inaktív.

2.1.11.5 Webes felület

Az ip http server és az ip http secure-server szolgáltatások kikapcsolásával megszűnt a forgalomirányítók és kapcsolók web-alapú kezelésének lehetősége. Mivel a parancssori kezelés kerül alkalmazásra a hálózati eszközök konfigurálásához, ezek a szolgáltatások feleslegessé váltak. A web-alapú kezelés növelné a hálózati eszközökhöz való jogosulatlan hozzáférés kockázatát, és a támadási felületet. Ez a beállítás minden forgalomirányítón és kapcsolón konfigurálásra került.

2.1.11.6 SSH

A biztonság növelése érdekében a hálózati eszközöket Telnet helyett a forgalmat titkosító SSH-n keresztül lehet VTY vonalon elérni. A nagyobb biztonság érdekében az SSH 2-es verziója került beállításra, és 4096 bit hosszú RSA kulcsokat használ. A felhasználó hitelesítése az IT szakember számítógépén generált, 2048 bit hosszú aszimmetrikus kulcspár használatával történik. Ez a megoldás biztonságosabb, mint egy sima jelszó, mivel ez egy hosszabb, random karakterekből álló string, illetve csak az IT szakember gépén van eltárolva, nem úgy, mint a sima jelszó, ami az összes hálózati eszközön. A publikus kulcs minden forgalomirányitón manuálisan lett eltárolva, a privát kulcs és a felhasználónév pedig az IT szakember gépén található PuTTy nevű szoftverben el lett mentve egy új, Network\_Devices nevű session-be. Így az IT szakembernek csak a konfigurálni kívánt eszköz IP címét kell beírnia. A publikus és a privát kulcs pedig a *C:\SSH\keys* mappában van elmentve az IT szakember számítógépén public\_key.pub és private\_key.ppk néven. A kulcsok a PuTTY key generator nevű alkalmazással lettek generálva. Az *x-y. képen* látható a PuTTY-ban elmentett privát kulcs elérési útvonala és felhasználónév.

A képen szöveg, képernyőkép, képernyő, szoftver látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép – PuTTY: privát elérési útvonalának elmentése

A képen szöveg, képernyőkép, képernyő, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép – PuTTY: felhasználónév elmentése

Illetve a *x. képen* példaként az SSH konfigurációja a SZE-KKK-BR1-n, valamint a *x. képen* a sikeres csatlakozás.

A képen szöveg, képernyőkép, Betűtípus, menü látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép – SZE-KKK-BR1-n SSH konfiguráció

A képen szöveg, képernyőkép, Betűtípus, szoftver látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép – sikeres csatlakozás a SZE-KKK-BR1-hez SSH-n

2.1.11.7 Management VLAN

A kapcsolókon nem az alapértelmezett, 1-es VLAN lett konfigurálva management VLAN-ként, hanem a 37-es. Ezáltal megszűnt annak a veszélye, hogy a kapcsoló konfigurálása során valamelyik 1-es VLAN-ban maradt vagy került interfészhez csatlakozva valaki könnyedén, forgalomirányitó nélkül elérje a kapcsolók üzemeltetési síkját. Emellett meg lett nehezítve a hálózat felderítése a támadó számára, illetve csökkentve lett a VLAN ugrásos támadás sikeressége.

2.1.11.8 VLAN

Az alapértelmezett, 1-es VLAN nem lett alkalmazva a hálózat szegmentálása során. Ezzel meg lett nehezítve a hálózat felderítése a támadó számára, illetve csökkentve lett a VLAN ugrásos támadás sikeressége. Emellett megszűnt annak a veszélye, hogy a kapcsoló konfigurálása során valamelyik 1-es VLAN-ban maradt vagy került interfészhez csatlakozva valaki könnyedén, forgalomirányitó nélkül elérjen egy használatban lévő VLAN-ban található eszközöket.

2.1.11.9 Nem használt portok

Minden nem használt port le lett kapcsolva, access módba lett állítva, és a nem használt (black hole) 29-es VLAN-ba került. Így csak a használt portokon történhet forgalom. Ezzel csökkentve lett a különféle támadások, például a VLAN ugrás, a MAC-cím elárasztás, az ARP hamisítás, valamint a DHCP-hamisítás, vagy a DHCP-kiéheztetés esélye. Azonban ezek a veszélyek továbbra is fennállnak az aktív portokon, ezért ezeken további konfigurációkra van szükség.

2.1.11.10 Portbiztonság

A MAC-cím elárasztás és a DHCP-kiéheztetés ellen portbiztonság lett beállítva a kapcsolók access típusú interfészein, amikhez a végpontok csatlakoznak. A portbiztonság maximum 1 MAC-címet tanul meg sticky módszerrel, ami biztosítja, hogy egy megadott eszközöktől származó forgalomra korlátozódjon a hozzáférés a portokon. A legerősebb biztonságot nyújtó, alapértelmezett megsértési mód, a shutdown beállításával a kapcsolók leállítják a portot, ha eltérést talál az üzenet forrás MAC-címe és a megtanult cím között. A hálózat üzembe helyezése után minden switch futó konfigurációja el lett mentve az indító konfigurációba. Ezáltal biztosítva lett, hogy a kapcsolók csak az előre telepített végpontok MAC-címeit fogadják el újraindításuk után is.

2.1.11.11 Trunk portok

A kapcsolók trunk portjain ki lett kapcsolva a Dynamic Trunking Protocol (DTP) funkció, és be lett állítva, hogy csak az előre létrehozott VLAN-ok forgalmait engedjék át. Ezen kívül meg lett változtatva a native VLAN az alapértelmezett, 1-es VLAN-ról a nem használt 11-es VLAN-ra. Ezzel jelentősen csökkentve lett a VLAN ugrásos támadás kockázata.

2.1.11.12 DHCP Snooping

A DHCP Snooping kapcsolókon való beállításával lett megoldva a védekezés a DHCP-támadások ellen. A DHCP-hamisítás elleni védekezés érdekében a DHCP Snooping funkcióban a kapcsolók trönk portjait, valamint a DHCP-szerverhez csatlakozó portot megbízható (trusted) portként lettek beállítva. Ezzel biztosítva lett, hogy csak az előre telepített DHCP-szerver küldhessen DHCP válaszüzeneteket (DHCPOFFER, DHCPACK, DHCPNAK). A DHCP-kiéheztetés veszélye a nem megbízható (untrusted) portokon a DHCP-üzenetek korlátozásával lett csökkentve. A fogadható üzenetek száma négyre lett korlátozva. A DHCP Snooping minden használt VLAN-ban konfigurálva lett.

2.1.11.13 Dinamikus ARP-ellenőrzés

Az ARP-mérgezés és az ARP-hamisítás ellen a dinamikus ARP-ellenőrzés (DAI) lett konfigurálva a kapcsolókon. A DHCP Snoopinghoz hasonlóan lett beállítva, vagyis csak a szerverekhez csatlakozó és a trönk portok lettek megbízhatók. A nem megbízható portokon a forrás- és cél MAC- és IP-címeket a DHCP Snooping táblája alapján ellenőrzi, és eltérés esetén eldobja az ARP-üzenetet. A DAI minden használt VLAN-ban konfigurálva lett.

2.1.11.14 BPDU Guard

A feszítőfa elleni támadás különféle veszélyeket rejt magában, mint például közbeékelődést vagy szórási vihar keletkezését, ami az egész kapcsolt hálózat leállásához vezethet. Ez a BPDU Guard konfigurálásával lett kiküszöbölve, amely minden access módban és PortFast-tal konfigurált porton be lett állítva. Így, ha ezen portok valamelyikén egy BPDU érkezik, az a port letiltott állapotba kerül.

2.1.11.15 Root guard

A hálózat stabilitása és a feszítőfa protokoll megfelelő működésének érdekében a root guard funkció lett alkalmazva a multilayer switcheken. Bár a hálózatban jelenleg nincsen második rétegben hurok, viszont az esetleges jövőbeli bővítések során keletkezhet. Biztonsági szempontból a root guard használata azért fontos, mert megakadályozza, hogy egy rosszindulatú vagy hibás konfigurációjú eszköz gyökérponti hídként vegye át az irányítást a Spanning Tree protokoll felett. A másodi rétegben levő kapcsolóknál ez a beállítás nem lett alkalmazva, mivel az access típusú portjait a BPDU guard védi. Az egymást összekötő trunk portjain lehetne alkalmazni, de ha hurok keletkezik a hálózatban a későbbi bővítések miatt, akkor a kapcsolók ezen portjain is érkezhet BPDU a gyökérponti hídtól. Ekkor ezen a porton megszűnne a bejövő keretek továbbítása, illetve folyamatosan Syslog üzenetet kapnánk. Mindkét harmadik rétegbeli kapcsoló összes használt és nem használt portján be lett állítva a root guard, hogy a jövőben is biztosítva legyen, hogy minden VLAN-ban az adott harmadik rétegbeli kapcsoló maradjon a gyökérponti híd.

2.1.11.16 CDP letiltása

A Cisco Felderítő Protokoll hasznos hálózati eszközök konfigurálásánál és hibaelhárításánál, viszont CDP-üzenetek elfogásával a támadó fontos információkat tudhat meg a hálózatról. A CDP előnyös a hálózati hibák elhárításához, ezért egy köztes megoldásként CDP-üzenetek küldése csak a hálózati eszközök között engedélyezett, és a végpontok fele pedig tiltott. Mivel a CDP alapvetően engedélyezett minden interfészen, ezért a végpontokhoz csatlakozókon a no cdp enable parancs lett kiadva.

2.1.11.17 ACL-ek

A hálózati eszközöket távolról, VTY vonalon csak az IT szakember alhálózatából lehet elérni. Ezért minden hálózati eszközön létre lett hozva egy VTYv4 nevű normál, nevesített és egy VTYv6 nevű kiterjesztett, nevesített ACL, amely a VTY vonalakon csak az IT szakember alhálózatából származó, bemenő forgalmat engedélyezi, és minden mást tilt. Mindegyik telepen mindegyik IPv4-es IT alhálózatból származó forgalmat engedélyezi, így a 10.11.169.0/28, a 10.23.169.0/29 és a 10.37.169.0/29 alhálózatból lehet elérni a hálózati eszközöket távolról. Azért van szükség az összes privát IPv4-es alhálózat engedélyezésére, mivel az interneten keresztül is el tudja érni az IT szakember a más telephelyen lévő hálózati eszközöket a tunneling-nek köszönhetően. Az IPv6 esetében is mindegyik IT alhálózatból (2001:db8:c1c1:abb5::/64, 2001:db8:c1c1:bab3::/64, 2001:db8:c1c1:c1b5::/64) mindegyik épületben lévő mindegyik hálózati eszközt el lehet érni. Az IPv6-os ACE-k célja any.

A management VLAN-okba csak az IT szakember alhálózatából származó forgalom engedélyezett. Ez a feltétel a MANAGEMENTv4 nevű normál, nevesített és MANAGEMENTv6 nevű kiterjesztett, nevesített ACL-ekben lett megfogalmazva, ami a

* KKK-MLS1 VLAN 11
* KKK-MLS2 VLAN 11

interfészén, és a

* DEB-KKK-BR1 G0/0/0.11
* DEB-KKK-BR2 G0/0/0.11
* SZE-KKK-BR1 G0/0/0.11
* SZE-KKK-BR2 G0/0/0.11

alinterfészén a kimenő forgalmat szűri. A forrás alhálózatok ugyanúgy lettek megadva, mint a távoli elérést korlátozó ACL-eknél. Az IPv6-os ACE-k célja any.

Az IT szakember alhálózatát semelyik másik, a cégben dolgozók számára létrehozott alhálózatokból semmilyen protokollon keresztül nem lehet elérni. Csak a szerverek és a többi IT alhálózatból, illetve a management VLAN-ból származó forgalom engedélyezett az IT szakember alhálózata felé. Ezt a ITv4 nevű kiterjesztett, nevesített ACL-ek biztosítják, ami a

* KKK-MLS1 VLAN 69
* KKK-MLS2 VLAN 69

interfészén, és a

* DEB-KKK-BR1 G0/0/0.69
* DEB-KKK-BR2 G0/0/0.69
* SZE-KKK-BR1 G0/0/0.69
* SZE-KKK-BR2 G0/0/0.69

alinterfészén a kimenő forgalmat szűri. Az ACE-k célja any. Az ACL-ek csak IPv4-es címeket szűrnek, mivel IPv6-os címmel bárhonnan el lehet érni az alhálózatot és mindent nem lehet tiltani. Azonban az IT szakembernek el kell érnie a többi VLAN-ban lévő számitógépet SSH, RDP vagy ICMP protokollon keresztül. Ezek válasz üzeneteit viszont tiltja az ACL, de ezen protokollok átengedése biztonsági kockázat. Ezért a probléma a következő ACE használatával lett megoldva, ami az ACL elején található és ami engedélyezi a TCP válaszforgalmat:

permit tcp any any established

A vezetéknélküli routerek alhálózatából származó forgalom nem érheti el a többi alhálózatot semmilyen protokollon keresztül, de minden más forgalom engedélyezett. Mivel egyik alhálózatot sem érhetik el, ezért az ACL rövidítése érdekében az egész 10.0.0.0/8 és 2001:db8:c1c1::/48 hálózat elérése lett tiltva. Ezt a WIFIv4 és WIFIv6 nevű kiterjesztett, nevesített ACL-ek biztosítják, ami a

* KKK-MLS1 VLAN 41
* KKK-MLS2 VLAN 41

interfészén, és a

* DEB-KKK-BR1 G0/0/0.41
* DEB-KKK-BR2 G0/0/0.41
* SZE-KKK-BR1 G0/0/0.41
* SZE-KKK-BR2 G0/0/0.41

alinterfészén a bemenő forgalmat szűri. Az összes ACE forrása any. Azonban a Wi-Fi hozzáférés hitelesítése a központi RADIUS szerver biztosítja, illetve a vezetéknélküli forgalomirányítóhoz csatlakozó eszközök a központi DHCP szervertől kapnak IP címet. Ezért a tiltások előtt engedélyezve lett, hogy az adott szervereket el lehet érni DHCP (67-es UDP port) és RADIUS (1812-es és 1813-as UDP port) protokollal.

Mivel a KKK-MLS1 harmadik rétegbeli kapacsolón mindegyik előbb említett ACL létre lett hozva, ezért példaként a *x. képen* látszódnak a létrehozott ACL-ek.

A képen szöveg, képernyőkép, Betűtípus látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép – ACL-ek az KKK-MLS1-en

2.1.11.18 unicast Reverse Path Forwarding (uRPF)

Minden telephelyen a kapcsolókhoz csatlakozó forgalomirányítók, valamint a harmadik rétegbeli kapcsolók esetében uRPF került konfigurálásra. Ez a beállítás a bemenő forgalmat szűri a forgalomirányítók alinterfészein, illetve a harmadik rétegbeli kapcsolók virtuális interfészein. A csomagok forrás IP-címének érvényességét azért kell ellenőrizni, hogy megakadályozzuk a hamis IP-címekkel végrehajtott túlterheléses támadásokat. Az IP-címhamisítás problémája egyrészt az az, hogy az ilyen forgalom valódi forrása nem követhető vissza, ami megnehezíti a támadások kivédését. Ezenfelül az IP-címhamisítás lehetővé teheti ACL szabályok megkerülését is. Például, ha az IT-szakember VLAN-ját egyik belső alhálózatból sem lehet elérni, viszont egy támadó mégis hozzáférhet, ha egy hamis forrás IP-címet használ. Ezek a biztonsági kockázatok indokolták a strict módú uRPF konfigurálását. Az uRPF beállítások azért a szélső forgalomirányítókra, illetve a harmadik rétegbeli kapcsolókra kerültek, hogy a hamisított csomagok feleslegesen ne jussanak tovább a hálózat belső részeire. Az IPv4-es és az IPv6-os csomagok is szűrve vannak.

2.1.11.19 WLAN

A cégben található vezeték nélküli routereken a cég dolgozói számára létrehozott Wi-Fi SSID szórása le van tiltva, így azt az ott dolgozóknak manuálisan kell beállítaniuk, ha kapcsolódni szeretnének a hálózathoz a vezeték nélküli eszközeikkel. A legmodernebb biztonsági módszer, a WPA3-Enterprise lett engedélyezve. Az AD DS és a RADIUS (  
FreeRADIUS) szerver integrációja lett megvalósítva a Wi-Fi hozzáférés központi hitelesítésére. A felhasználók csatlakozhatnak a hálózathoz a tartomány-hitelesítő adataik használatával. A vezeték nélküli routerek külön VLAN-ban vannak, így a vezeték nélküli eszközöktől származó forgalom jól elkülönül a hálózat többi forgalmától.

A vendégek számára vendég Wi-Fi lett létrehozva, ahol szintén a WPA3-as biztonsági módszer van alkalmazva. A vendégek a tárgyalóban és a konferenciateremben lehelyezett papíron olvashatják a szükséges jelszót a vendég Wi-Fi-hez való csatlakozáshoz.

2.1.11.20 OSPFv2 és OSPFv3 hitelesítés

Az OSPF dinamikus útválasztásának védelmére mindkét verzióban hitelesítés lett beállítva, hogy a támadó az OSPF csomagok megváltoztatásával, vagy hamisak küldésével ne tudja megváltoztatni a forgalomirányítást és ezáltal ne téríthesse el a hálózat forgalmát. Az OSPFv2-nél az egyszerű, szöveges, titkosítatlan jelszó helyett az MD5 kriptográfia hash algoritmus van használva a biztonságosabb hitelesítésre és a csomag sértetlenségének ellenőrzésére. Mindegyik telephelyen minden terület egyedi kulcs és kulcs azonosító párost kapott. Ezek a párosok az *x. táblázatban* láthatóak.

|  |  |  |  |
| --- | --- | --- | --- |
| **OSPFv2 hitelesítés** | | | |
| **Telephely** | **Terület** | **Kulcs azonosító** | **Kulcs** |
| Budapest | 0 | 84 | G7pL2qR4sW5kX9zB |
| 5 | 138 | hT8sR0vJ3pW4nY6x |
| 10 | 196 | Q9tM1aE5fV6kL2zY |
| Debrecen | 0 | 121 | A9hbL3kmX457qZ1p |
| Szeged | 0 | 92 | Z8ggJ2evK053dQ9m |

x. táblázat - OSPFv2 hitelesítés

A hálózatban az OSPFv3 hitelesítés IPsec alapú, mely minden OSPFv3 területen egyedi SPI és megosztott kulcs használatával biztosítja a kapcsolatok biztonságát. A nagyobb biztonság érdekében mindegyik telephely mindegyik területéhez egyedi SPI és kulcs páros lett konfigurálva. Így, ha egy terület hitelesítését feltörik, akkor a támadás csak az adott területre tud koncentrálódni. Az SHA-1 hash algoritmus lett alkalmazva. Az SPI és kulcs párosok az *x. táblázatban* találhatóak.

|  |  |  |  |
| --- | --- | --- | --- |
| **OSPFv3 hitelesítés** | | | |
| **Telephely** | **Terület** | **SPI** | **Kulcs** |
| Budapest | 0 | 2008 | 3F2A1B8C9D1E4F6A7B8C9D0E1F2A3B4C5D6E7F8A |
| 5 | 12075 | 7A4B1C8D9E2F6A1B8D9E4C5F1A2B3C4D5E6F7A8B |
| 10 | 21478 | 1E2A3B4C5D6E7F8A9B0C1D2E3F4A5B6C7D8E9F0A |
| Debrecen | 0 | 905 | 0A1B2C3D4E5F6A7B8C9D0E1F2A3B4C5D6E7F8A9B |
| Szeged | 0 | 5641 | 9F8E7D6C5B4A3C2D1E0F9A8B7C6D5E4F3A2B1C0D |

x. táblázat - OSPFv3 hitelesítés

A *x. képen* látható, hogy a SZE-KKK-IR-on az OSPFv2 és az OSPFv3 hitelesítés már konfigurálva lett, ezért a SZE-KKK-BR1 a SZE-KKK-IR hello üzeneteit nem tudja fogadni, mivel a hitelesítés még ott nem lett beállítva, ezért lejár a dead időzítő és a szomszédság megszűnik. A SZE-KKK-BR1 konfigurálása után viszont újra helyre áll a szomszédsági viszony.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

x. kép – OSPFv2 és OSPFv3 hitelesítés konfigurálása és tesztelése a SZE-KKK-BR1 routeren

2.1.11.21 EIGRP hitelesítés

Az EIGRP által küldött forgalomirányítási információk védelmére hitelesítés lett beállítva. Az egyszerű, szöveges, titkosítatlan jelszó helyett MD5 kriptográfia hash algoritmus van használva a biztonság erősítésére és a csomag sértetlenségének ellenőrzésére. Mivel az EIGRP-nél kötelező a key-chain használata, ezért létre lett hozva egy KEYEIGRP néven. A kulcs a huszonötös azonosítót kapta és 2024 szeptember elsejétől végtelen ideig érvényes. Az IPv6-os és az IPv4-es szomszédok is ugyanazzal a kulccsal hitelesítik egymást. A kulcs, ami konfigurálásra került a következő: F7#h8m$Q2!xK4pL

A *x. képen* látható, hogy a KKK-IR routeren már konfigurálásra került az EIGRP hitelesítés, de a SZE-KKK-IR-en még nem, ezért a szomszédság megszűnik. Miután a SZE-KKK-IR forgalomirányító is konfigurálva lett, újra létre jön az IPv4-es és az IPv6-os EIGRP szomszédság.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

*x. kép – EIGRP hitelesítés konfigurálása és tesztelése a SZE-KKK-IR routeren*

2.1.11.22 BGP hitelesítés

A BGP hitelesítés a forgalomirányítási információk védelmére szolgál. Az egyszerű, szöveges, titkosítatlan jelszó helyett az MD5 hash algoritmus van használva a biztonság erősítésére és a csomag sértetlenségének ellenőrzésére. IPv4-nél és IPv6-nál ugyanazok a kulcsok lettek alkalmazva, viszont a kulcsok eltérnek telephelyenként. A kulcsok a *x. táblázatban* találhatóak.

|  |  |
| --- | --- |
| **BGP hitelesítés** | |
| **Telephely** | **Kulcs** |
| Budapest | D3s6!aP9v#4@bQ8R |
| Szeged | R#7qT!m4L0s3^N2x |
| Debrecen | 8Y%jLz9!F@1r2Vp# |

x. táblázat - BPGP hitelesítés

A *x. képen* látható példaként a KKK-IR BPG hitelesítésének konfigurációja.

A képen szöveg, Betűtípus, képernyőkép, sor látható

Automatikusan generált leírás

x. kép – KKK-IR-en a BGP hitelesítés konfigurációja

2.1.11.23 Passzív interfész

Az OSPF konfigurálásánál a végpontok felé néző interfészek passzívok lettek. Ez a beállítás növeli a biztonságot az útválasztási információk terjesztésének korlátozásával, csökkentve a potenciális támadási felületet. Nagyon sok passzív interfészt kellett volna beállítani, ezért az egyszerű konfigurálás érdekében a ”passive-interface default” parancs lett alkalmazva és a ”no passive-interface” paranccsal lettek beállítva a nem passzív interfészek.

2.1.11.24 HSRP hitelesítés

A HSRP-vel konfigurált forgalomirányítók közötti üzenetváltások biztonságának érdekében hitelesítés lett beállítva. A nagyobb biztonság elérése és az üzenetek sértetlenségének ellenőrzése érdekében a hitelesítés az MD5 hash algoritmust használja az egyszerű, szöveges, titkosítatlan jelszó helyett. Minden telephelyen más kulcs van használva, de telephelyenként az IPv6-os és IPv4-es csoport ugyanazt a kulcsot használja. Ezek a *x. táblázatban* találhatóak.

|  |  |
| --- | --- |
| **HSRP hitelesítés** | |
| **Telephely** | **Kulcs** |
| Budapest | T7v@2u$M!qW9bZ3^ |
| Szeged | eR5&hX4!jN8p$W1m |
| Debrecen | Y8^fS3\*zZ2@qJ7!k |

x. táblázat - HSRP hitelesítés

2.1.11.25 Direkt kulcsok

A dinamikus forgalomirányító protokollok és a HSRP hitelesítésére direkt kulcsok lettek konfigurálva. Ennek okai a következők:

* Egyszerűbb konfigurálni a hálózati eszközöket direkt kulccsal, így gyorsabb a hálózat telepítése. Emellett nagy mértékben csökken a hibázás esélye a telepítés során.
* Könnyebb nyilvántartani a hitelesítéshez használt kulcsokat. Ez segíti a hálózat karbantartását
* Nagyon sokféle hitelesítés és azokon belül is sokféle kulcs van alkalmazva, ezáltal sok key-chain kellett volna létrehozni a hálózati eszközökön. Ez rossz hatással lett volna a hálózat teljesítményére

2.1.11.26 Hardveres tűzfal: ASA

2.1.12 WIFI

2.1.13 Bannerek

2.2 WAN

2.2.1 Internetszolgáltató

Az internetszolgáltató választásánál cél volt, hogy ismert és a telephelyek távolsága miatt az egész országban elérhető legyen. Három szolgáltató felelt meg az elvárásoknak a Magyar Telekom Nyrt, a Yettel Magyarország Zrt, és a One Magyarország (Digi). Miután mind háromtól árajánlat lett kérve a Telekomra esett a választás, mivel ez a cég adta legjobb ár-értékű ajánlatot. Figyelembe lett véve a maximális sávszélesség, amit a szolgáltató képes nyújtani, illetve az optikai kábel bekötésének, az internetnek, illetve a publikus IPv4 cím bérlésének a költsége. A Telekomtól kapott árajánlat a *x. képen* látható. Ez a szolgáltató egyik értékesítési konzultánsának, Dániel Józsefnek az egyik válasz üzenete. Ez havi, nettó költséget jelent. Az optikai kábel bekötése ingyenes.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

x. kép – Telekom ajánlata

A szolgáltatótól viszont három feladatot kaptunk: hirdessük a kapott publikus IPv4 címeinket BGP-vel, állítsuk be a BPG hitelesítést, illetve konfiguráljuk PPPoE kliensként a forgalomirányítót, ami az ISP-hez csatlakozik.

2.2.2 BGP, statikus forgalomirányítás

A szolgáltatótól kapott /27-es méretű címtartomány el lett osztva a telephelyek között. Ezek a Border Gateway nevű protokollal vannak hirdetve a szolgáltató felé. Privát AS számok lettek használva, mivel a szolgáltatótól vannak az IPv4-es címek bérelve és a hálózat mérete se követeli meg, hogy az európai RIR-nél (RIPE NCC) egy publikus AS szám legyen kérve. A használt privát ASN-ek a szolgáltatóval egyeztetve lettek. Az ISP forgalomirányítói a Telekom publikus AS számával lettek megadva a telephelyek routerein. Mivel ezzel csak a címtartományunk van hirdetve és a telephelyek routerei nem kapnak hirdetéseket, ezért egy statikus alapértelemezett útvonal lett megadva az ISP felé a PPPoE konfigurálása során. Az ASN-nek a *x. táblázatban* láthatóak. Példaként a *x. képen* látható a DEB-KKK-IR router BPG konfigurációja, és a *x. képen* a BPG szomszédság ellenőrzése.

A szolgáltatótól kapott IPv6-os címek is ugyanúgy vannak hirdetve, mint az IPv4-esek. IPv6 esetében azonban létre kellett hozni egy peer-group-ot és az IPv6-os szomszédot bele kellett rakni. A peer-group név a szegedi forgalomirányítón PEERSZ, a debrecenin PEERD, és a központin PEERK. Mindkét address-family-ben az IPv4-es és IPv6-os cím is aktiválva lett, így, ha az ISP routere egyik címen nem érhető el, akkor is lehet hirdetni mindkét típusú IP címtartományt. Mivel IPv6 esetében nem lehet automatikusan létrehozni egy statikus alapértelemezett útvonalat, ezért mindegyik telephely esetében manuálisan lettek megadva.

|  |  |
| --- | --- |
| **AS számok** | |
| **Telephely** | **ASN** |
| ISP | 5483 |
| Budapest | 65001 |
| Szeged | 65003 |
| Debrecen | 65002 |

x. táblázat – Az ISP és a telephelyek AS számai

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

x. kép – DEB-KKK-IR BGP konfigurációja

A képen szöveg, Betűtípus, képernyőkép, szám látható

Automatikusan generált leírás

x. kép – DEB-KKK-IR-n BGP ellenőrzése

2.2.3 PPPoE

A Telekom kérésére a routerihez csatlakozó forgalomirányítóinkat PPPoE kliensként kellett konfigurálni, hogy az ISP PPPoE szervere hitelesíteni tudja a routereinket. A konfiguráció során mind a három routeren létre lett hozva egy Dialer interfész 1-es számmal, ahol az MTU a maximális, 1492-es értékre lett állítva, illetve meg lett adva a szolgáltatótól kapott IP cím és a jelszó. Emellett hozzá lett rendelve az 1-es pool és a ppp ipcp route default paranccsal biztosítva lett, hogy a PPPoE kapcsolat létrejötte és a hitelesítés után a forgalomirányító táblába bekerüljön egy IPv4-es alapértelmezett útvonal az ISP felé. Az autentikáció során a szolgáltató kérésére nem a sima, szöveges jelszót használó PAP, hanem a biztonságosabb, titkosított jelszavú CHAP lett alkalmazva. A PPP beágyazás is konfigurálva lett a Dialer 1-es interfészen. A fizikai interfészek nem kaptak IP címet, hanem PPPoE kliensként lettek konfigurálva és az egyes pool lett hozzárendelve. Mind a három routeren azonos interfész, vagyis a GigabitEthernet 0/0 lett konfigurálva, és az előbb leírt beállítások is megegyeznek a forgalomirányítókon. Csak a jelszavak, illetve az IP címek térnek el. Az ISP a routereinket a hosztnevük alapján vette fel felhasználóként a PPPoE szerverén. Az *x. táblázatban* látható a kiosztott jelszavak és IP címek. A *x. képen* példaként a KKK-IR PPPoE kliensként való konfigurációja, valamint a *x. képen* a PPPoE kapcsolat létre jöttének ellenőrzése látható.

|  |  |  |
| --- | --- | --- |
| PPPoE paraméterei | | |
| **Eszköz** | **IP cím** | **Jelszó** |
| KKK-IR | 203.5.100.34 | DXl2hucBm2 |
| DEB-KKK-IR | 203.5.100.38 | A3SnLFYINU |
| SZE-KKK-IR | 203.5.100.42 | RJmP8JciAb |

x. táblázat – ISP-től kapott PPPoE paraméterek

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

x. kép – KKK-IR PPPoE konfigurációja

A képen szöveg, képernyőkép, Betűtípus, szám látható

Automatikusan generált leírás

x. kép – KKK-IR-n PPPoE ellenőrzése

2.2.4 PAT, SNAT

Mind a három telephelynél NAT lett alkalmazva. A szolgáltatótól kapott /27-es címtartomány lett szétosztva úgy, hogy a központi (KKK-IR) egy /28-as, a szegedi (SZE-KKK-IR) és a debreceni (DEB-KKK-IR) telephely pedig egy /29 címtartományt kapott. A NAT egyik típusa, a PAT lett konfigurálva pool-okkal. Mindegyik említett forgalomirányítón a NAT külső interfésze a Dialer1. Hogy a proxy szervert kívülről is el lehessen érni, ezért SNAT lett beállítva a KKK-IR routeren. A belső, privát címek engedélyezésre, meghatározásara normál, nevesített ACL lett létre hozva mindegyik forgalomirányítón PAT névvel, illetve a pool-ok is PAT névvel lettek létrehozva. A *x. táblázatban* láthatóak a konfigurált címek a NAT beállítása során.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **NAT címek** | | | | |
| **Eszköz** | **Pool** | **Maszk** | **SNAT** | **Belső hálózat** |
| KKK-IR | 203.55.100.2 - 203.55.100.14 | /28 | 203.55.100.1 | 10.11.0.0 /16 |
| DEB-KKK-IR | 203.55.100.17 - 203.55.100.22 | /29 | - | 10.37.0.0 /16 |
| SZE-KKK-IR | 203.55.100.25 - 203.55.100.30 | 10.23.0.0 /16 |

x. táblázat – NAT címek

2.2.5 DMVPN

2.2.6 EIGRP

3. Szerverek

3.1 Windows szerverek

3.1.1 ADDS, RODC, Sub domain

3.1.2 Group Policy

3.1.3 WDS

3.1.4 Radius

3.2 Linux szerverek

3.2.1 KKK-LIN

3.2.1.1 Ansible

3.2.1.2 LibreNMS

3.2.1.3 Webszerver

3.2.1.4 Email

3.2.1.5 Rsyslog

3.2.2 KKK-VPN

3.2.2.1 Wireguard

3.2.3 Rsyslog kliens

3.3 Felhő

3.3.1 Amazon Web Services

A kettő vezető felhőszolgáltató (Amazon Web Services, Microsoft Azure) közül az AWS lett választva. Ennek okai a következők:

* Az AWS a legtöbb szolgáltatással rendelkezik, több mint 200 különböző szolgáltatással. Ennek köszönhetően, ha később igény merülne fel egy újabb szolgáltatásra, akkor kevesebb eséllyel kell új szolgáltatót használni, és ezáltal könnyebb lesz a felhőszolgáltatások kezelése.
* Az AWS gyakran vezető szerepet játszik az új technológiák és szolgáltatások bevezetésében. Így a legtöbb esetben tudjuk alkalmazni a legújabb lehetőségeket.
* Az AWS volt az első nagyobb felhőszolgáltatás, amely a piacon megjelent, és jelentős szerepet játszott a felhőalapú számítástechnika népszerűsítésében. Több nagy vállalat használja világszerte, mint például a Netflix vagy a Facebook. Bár a Microsoft Azure-t is sok nagy cég használja (pl. Volkswagen), de az AWS-t olyan a technológia fejlődésben élen lévő vállatok is, mint például a NASA vagy a Forma-1.

3.3.2 A felhő

A webkiszolgáló felhőbe telepítésére azért volt szükség, hogy egyszerűen skálázható, megbízható és könnyen karbantartható legyen. A skálázhatóság azért fontos, mert később a cég növekedése miatt többen fogják felkeresni a weboldalt akár a világ minden részéről. A megbízhatóság és a könnyű karbantartás pedig azért szükséges, hogy a webkiszolgáló folyamatosan elérhető legyen. A fájlkiszolgáló szolgáltatás a weboldalon megjelenő képek tárolása miatt kellett. Az adatbázis szolgáltatás a termékek adatainak tárolása miatt kellett. Ezek is a felhőben vannak, hogy a webkiszolgáló gyorsan és mindig elérje őket. Ezek a megoldások együttesen biztosítják a webszerver teljesítményét és rugalmasságát, optimális felhasználói élményt nyújtva.

A szolgáltatások a svéd régióban (Stockholm, eu-north-1) lettek létre hozva. Bár a frankfurti közelebb van, a cég arra számít, hogy az észak-európai országokban nagyobb lesz a kereslet a magyar zenék iránt, mint Európa többi részén.

3.3.3 Webkiszolgáló

Az AWS egy Saas típusú szolgáltatása, az EC2 lett alkalmazva a webkiszolgáló létrehozásánál. Mivel nem rég jött létre a cég, még nem számítanak sok vásárlóra. Csak egy t3.micro instance lett létrehozva, amely 2 vCPU-val és 1 GB memóriával rendelkezik. Amiatt, hogy a cég a kezdeti időszakban még kevés vásárlóra számít és a költségek csökkentése érdekében ez az instance megfelelőnek lett találva. A t3.micro havonta 750 órát futhat ingyenes 12 hónapig, Az alacsony erőforrás, illetve a költségek csökkentése miatt Windows helyett Debian 12 operációs rendszer van a virtuális gépen. Mivel webkiszolgálóként van bekonfigurálva, ezáltal a virtuális gép egy olyan biztonsági csoportot kapott, ami engedélyezi az SSH mellett a HTTP és HTTPS forgalmat az internet felől. A beállításoknál a központ publikus címtartománya lett megadva, így az ssh forgalom csak a központ felől engedélyezett. Az a virtuális gép SSH-n keresztüli eléréséhez szükséges RSA privát kulcs az IT szakember számítógépén a *C:\felhő* mappában Webszerver-kulcs.pem névű fájlban van eltárolva. A kulcson csak az IT szakember felhasználójának csak olvasás, valamint olvasás és végrehajtás joga van. Ez kötelező beállítás volt. A mappában megnyitott parancssorban a *x. képen* látható parancsot kell kiadni a webkiszolgáló eléréséhez.

A képen szöveg, képernyőkép, Betűtípus látható

Automatikusan generált leírás

x. kép - Webkiszolgáló elérése

A virtuális gépen Apache2 webszerver fut és az index.php, valamint a styles.css fájlok a */var/www/html* mappában vannak. A weboldal adatbázishoz való hozzáféréséhez telepítve lett a php, a libapache2-mod-php és a php-mysql csomag. A Certbot is telepítve és használva lett, hogy egyszerűen lehessen szerezni SSL/TLS tanúsítványt, hogy biztosítva legyen a HTTPS kapcsolat a webszerverhez. A Certbot az automatikus domain ellenőrzés után a tanúsítványt a Let’s Encrypt-től szerezte. Az instance a webszerver nevet kapta. Az instance hálózati paraméterei a *x. képen* láthatóak.

A képen szöveg, képernyőkép, Betűtípus, szoftver látható

Automatikusan generált leírás

x. kép - Az EC2 hálózati paraméterei

3.3.4 Fájlkiszolgáló szolgáltatás

A fájlkiszolgáló létrehozásához az AWS egy Paas típusú szolgáltatása, az S3 lett alkalmazva. Létre lett hozva egy webszerverkepek bucket, amiben a weboldalon megjelenő képek vannak tárolva. A létrehozott bucket és néhány eltárolt kép a *x. képen* látható.

A képen szöveg, képernyőkép, szám, Betűtípus látható

Automatikusan generált leírás

x. kép - Webszerverkepek nevű bucket

3.3.5 Adatbázis szolgáltatás

Az adatbázis kiszolgáló létrehozásánál az AWS egyik Paas típusú szolgáltatása, az RDS lett alkalmazva. Egy db.t3.micro instance lett létrehozva, amely 1 vCPU-val és 1 GB memóriával rendelkezik és MySQL motort használ. Ez is, mint a t3.micro megfelelőnek lett találva a kezdeti időszakra. Ugyanúgy 12 hónapon keresztül 750 órát futhat ingyenesen. Az instance a webszervertermekek nevet kapta. A db.t3.micronak csak privát IP címe van, így csak az AWS-en létrehozott szolgáltatások érhetik el. A biztonság növelése érdekében jelszó lett alkalmazva. Az adatbázis szolgáltatás eléréséhez szükséges paraméterek az *x. táblázatban* láthatóak. A hálózati beállításai a *x. képen* láthatóak.

|  |  |
| --- | --- |
| **Adatbázis kiszolgáló elérése** | |
| **Paraméter neve** | **Paraméter értéke** |
| Hosztnév | webszervertermekek.c3k6ggiwmhhx.eu-north-1.rds.amazonaws.com |
| Portszám | 3306 |
| Felhasználónév | admin |
| Jelszó | KOlaleha879 |

x. táblázat - Az adatbázis kiszolgáló eléréshez szükséges paraméterek

A képen szöveg, képernyőkép, Betűtípus, szám látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

x. kép - Az RDS hálózati beállításai

A kiszolgálón egy webserver nevű adatbázis és benne egy products nevű tábla lett létrehozva. A táblában title, description, price és image\_url mezők vannak. Több tábla nem lett létrehozva, mivel a weboldal további fejlesztése a cégben dolgozó webfejlesztő feladata. Ezért a weboldalon egyelőre a Kosárba gombra kattintva egy üzenet ugrik fel, ami tájékoztatja a felhasználót arról, hogy csak telefonon keresztül lehet rendelni, valamint a telefonszám is megjelenik.

3.3.6 A weboldal

A webkiszolgáló publikus IP címéhez a No-IP (<https://www.noip.com/>) weboldalon egy domén név, kkk.sytes.net lett hozzárendelve, hogy a vásárlók egyszerűen elérjék a cég weboldalát. Az oldal a következő URL-lel érhető el, ahogy a *x. képen* látható.

<https://kkk.sytes.net/>

A képen szöveg, képernyőkép látható

Automatikusan generált leírás

x. kép - <https://kkk.sytes.net/>

4.Automatizáció

A hálózatban több automatizációs folyamat található meg. Mivel a Windows szerverek alapvetően elég ingatagok, ezért ezek alapvető konfigurációját Ansible-el valósítjuk meg, amihez a szerver **a KKK-LIN** eszközöné fut. Ansible segítségével a következő szolgáltatásokat telepítjük és konfiguráljuk a Windows szervereinken (*x. táblázat*). Ezen kívül a Active Directory környezet felépítésére és a felhasználók létrehozására, PowerShell scripeteket írtunk, amiket egy batch file (kötegfájl) lefuttatásával lehet elindítani. A felhasználók egy *.csv* file-ban lesznek megtalálhatók, és így ez a folyamat is automatizáltan fog működni.

|  |  |
| --- | --- |
| **Windows szerver Ansible** | |
| **Eszközök** | **Szolgáltatások** |
| KKK-ADDS  KKK-RODC | ADDS |
| DNS |
| AD DFS |
| FSRM |
| KKK-ADDS | DHCP |

x. táblázat – Ansible-el telepített szolgáltatások

Továbbá a **KKK-LIN** szerveren egy webszerver fut, ami egy távoli konfigurációs felület. Az Active Directory-s bejelentkezés segítségével lehet használni. A rendszergazda megadhatja ezen a felületen, hogy mit szeretne konfigurálni, és az oldal segítségével összekattinthatja a konfigurációt, majd IP cím, SSH felhasználónév, SSH jelszó, és enable jelszó megadását követően rá tudja küldeni SSH segítségével az összerakott kódot az adott eszközre. A weboldalt az *x. képen* lehet látni.

KÉP HELYE

A következő képen (*y. kép*), pedig az oldal működőképességét mutatjuk be.

KÉP HELYE

Az Ansible kódok megírásánál arra törekedtünk, hogy tökéletesen elkészítse az adott konfigurációt az eszközhöz, és ha másodszorra is lefuttatjuk, akkor ne legyen már változás a feladatoknál. Az Ansible kódok, és a PowerShell scriptek a dokumentáció végén a hivatkozások részben tekinthetők meg.

4.1 Ansible kódok

4.1.1 ADDS

Az Active Directory telepítését és felkonfigurálását végzi el a playbook. A playbookban alapvető Windows *(új néven: microsoft.ad)* modul segítségével, létrehozza a *„kkk.com”* tartományt a **KKK-ADDS** szerveren, majd, ha szükséges akkor újraindítja, és ezt követően domain kontrolleré promótálódik a szerver. A következő play a DNS kliens beállítása a **KKK-RODC** szerveren, ami ahhoz szükséges, hogy csatlakoztathassuk a kkk.com tartományba, ezért beálltja a **KKK-ADDS** IPv4 és IPv6 címét DNS kiszolgálónak. Ezelőtt van egy tesztelés, ami arra szolgál, hogy ha be van már állítva ez a két cím az eszközön akkor ugorja át az előbb leírt lépést. Ezután már csak két play van a playbookban, az első becsatlakoztatja a domainbe a **KKK-RODC** eszközt, majd, ha szükséges újraindítja, a második feltelepíti az Active Directory Domain Services és DNS szolgáltatást, majd ezután Read-Only Domain Controlleré lépteti elő, és ha szükséges újraindítja. Az *x-y.* képen a sikeres első és a *changed* állapot nélküli második futtatás, valamint az Active Directory Users and Computers-ből kivágott képernyőkép arról, hogy tényleg működött a kód látható a képeken.

|  |
| --- |
| A képen képernyőkép, szöveg, Színesség látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – adds.yaml első futtatás |

|  |
| --- |
| A képen képernyőkép, szöveg látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – adds.yaml második futtatás |

|  |
| --- |
| *A képen szöveg, képernyőkép, Betűtípus, szám látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – Domain controllerek |

4.1.2 DNS

A DNS (*Domain Name Services*) szolgáltatást a *dns.yaml* playbookban konfiguráljuk. Első körben a **KKK-ADDS** szerveren beállítja DNS szervernek önmagát és a **KKK-RODC** szervert (IPv4 és IPv6 címeket egyaránt) ezzel megteremtve azt, hogy rekordokat replikálja az írásvédett tartományvezérlőre. Az egész playbook a **KKK-ADDS** szervert konfigurálja. Mivel ehhez nincs alapvető modul, csak community, PowerShell parancsok segítségével kell megoldani a konfigurációt és a tesztelést ahhoz, hogy a második futtatásnál ne legyen *changed* állapotú task. Ennek következtében, az első playben a szerver beállítása előtt még leteszteljük, hogy már be van-e állítva neki a 4 IP cím. A következő play először végig nézi, hogy létezik-e:

* a 113.11.10.in-addr.arpa fordított dns zóna
* a 10.11.113.5-s rekord (A rekord tesztelés)
* a 2001:db8:c1c1:abfa::5 rekord (AAAA rekord tesztelés)
* a mail.kkk.com rekord (CNAME rekord tesztelés)
* a DNS továbbító beállítása

Ezután az előbbi taskok kimenetét használva, ha a megadott szövegrészletek nincsenek bent a kimenetben, akkor lefuttatja a taskokat, amik az inventory fájlban leírt részletek segítségével végig loopol az ott leírtakon. A taskok a következő beállításokat végzik.

* Tartománynévrendszer elsődleges zónáinak létrehozása
* A rekordok létrehozása
* AAAA rekordok létrehozása
* CNAME rekordok létrehozása
* DNS forwarder felvétele

Az *x-y. képeken* az első futtatás és a *changed* állapot nélküli második futtatás látható. Ezután a *x-y. képeken* a DNS konzolban látható, hogy a rekordok és zónák tényleg létrejöttek. Ezek mind a következő oldalakon találhatóak

|  |
| --- |
| A képen szöveg, képernyőkép, Betűtípus, tervezés látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – dns.yaml első futtatás |
| A képen szöveg, képernyőkép látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – dns.yaml második futtatás |
| *A képen szöveg, képernyőkép, szám, szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – KKK-ADDS DNS konzol |

|  |
| --- |
| *A képen szöveg, képernyőkép, szám, menü látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – KKK-RODC DNS konzol |

4.1.3 DHCP

A DHCP (*Dynamic Host Configuration Protocol*) szolgáltatást a *dhcp.yaml* playbook konfigurálja. A folyamat átláthatósága és megkönnyítése érdekében az *inventory.yaml*-ben az egyes IPv4-es és IPv6-os scopeok beállításait felvettük, így loopok segítségével könnyebben és átláthatóbban létrehozhatóak az adott scope-ok. A script a következő taskokon, lépéseken keresztül konfigurálja fel **a KKK-ADDS** Windows szervert DHCP szerverré:

* Letelepíti a dinamikus állomáskonfiguráló protokoll szolgáltatást és a hozzátartozó vezérlési eszközöket
* Ha szükséges újraindítja az eszközt
* Megnézi, hogy a DHCP modul létezik-e
* A DHCP szervert engedélyei a tartományba
* A Server Managert értesíti arról, hogy sikeres volt a telepítés
* Beállítja, hogy regisztrálja a csatlakozó eszközöket DNS szerverbe
* Létrehozza, és konfigurálja a DHCPv4 scope-okat
* Létrehozza, és konfigurálja a DHCPv6 poolokat

Mivel a legtöbb konfiguráció (a beépített szolgáltatás telepítésen kívül) nem elérhető az alap ansible moduleban, ezért PowerShell scriptek segítségével lettek ezek megvalósítva, így a konfiguráció során, a *changed\_when: false* értéket használtuk fel sok helyen. Az ansible playbook lefutását az *x-y. képeken* láthatóják, majd az *x-y. képeken*, pedig a szerveren a DHCP management console-ból, hogy valóban létrejöttek ezek a scope-ok a megadott opciókkal és kizárásokkal.

|  |
| --- |
| *A képen képernyőkép, szöveg, Multimédiás szoftver, Grafikai szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – dhcp.yaml első futás |

|  |
| --- |
| *A képen képernyőkép, szöveg látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – dhcp.yaml második futás |

|  |
| --- |
| A képen szöveg, képernyőkép, szoftver, szám látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – KKK-ADDS IPv4 scope |

|  |
| --- |
| A képen szöveg, képernyőkép látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – KKK-ADDS IPv6 scope |

4.1.4 ADDFS

Az Active Directory Distributed File System (*ADDFS*) szolgáltatás telepítését és konfigurálását az *addfs.yaml* playbook végzi. A szolgáltatás telepítését, mindkét szerveren elvégezzük, mivel ez a lényege, hogy több helyen is jelen legyen a file szerver. A playbook a következő playeken és taskokon keresztül végzi el a konfigurációt:

* Telepíti a szolgáltatást (és a replikációhoz szükséges szolgáltatást is) vezérlőeszközökkel együtt
  + Ha szükséges újraindítja az eszközöket
* Létrehozza a mappákat *„C:\”* elérési útvonal alá
* Megosztja ezeket a mappákat Samba segítségével
* Lecsekkolja, hogy létezik-e a DFS namespace gyökér, ha még nem akkor folytatja
* Elkészíti a namespace rootot
* Hozzáadja a namespace mappákat a namespace root-alá
* Másodlagos hozzáférést is készít hozzá
* Elkészíti a replikációs csoportot
* Hozzáadja a szervereket
* Beállítja a replikálni való mappákat
* Létrehozza a kapcsolatot a két eszköz között
* Frissíti a kapcsolat attribútumait a replikációhoz (loop segítségével)

A *x-y. képeken* az első, illetve második lefutást lehet megtekinteni, amiben van egy probléma, a második futásnál, a **KKK-ADDS** szerveren a Files nevű mappa megosztása, valamiért minden alkalommal (az első futtatást követően) *changed* állapotba kerül, és ezt nem is tudtuk kijavítani. A *x-y. képeken* a konzolból mutatjuk be, hogy sikeresen lefutott a playbook, és meg is csinálta, valamint az *x-y. képeken* az látható, hogy a két szerveren ugyanúgy létrejött ugyanaz a file, lokális, valamint hálózaton keresztüli elérésnél is.

|  |
| --- |
| A képen szöveg, képernyőkép, szoftver, Multimédiás szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – addfs.yaml első futás (1. play) |

|  |
| --- |
| A képen szöveg, képernyőkép, Betűtípus látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.  x. kép – addfs.yaml első futás (2. play) |

|  |
| --- |
| *A képen képernyőkép, szöveg látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – addfs.yaml második futás |

|  |
| --- |
| *A képen szöveg, képernyőkép, Betűtípus, sor látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.* x. kép – Replikációs csatlakozások |

|  |
| --- |
| *A képen szöveg, képernyőkép, szám, szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.* x. kép – Replikációs tagság |

|  |
| --- |
| A képen szöveg, szám, Betűtípus, képernyőkép látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.x. kép – Replikációs mappák |

|  |
| --- |
| *A képen szöveg, képernyőkép, szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.* x. kép – Replikálódás KKK-ADDS |

|  |
| --- |
| *A képen szöveg, képernyőkép, Betűtípus, szoftver látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – Replikálódás KKK-RODC |

4.1.5 FSRM

Az File Server Resource Manager (*FSRM*) szolgáltatás telepítését az *fsrm.yaml* file végzi. Ezt is mindkét szerverre alkalmazzuk, mivel az összes Active Directory Distributed File System által kezelt és replikált mappának a beállítását és korlátozását ezzel végezzük el. Minden mappára az ahhoz tartozó csoportokra jellemző fájl kiterjesztéseket engedélyezzük és minden mást korlátozunk. Ezen felül, van egy *hard* korlát beállítva mindegyik csoportra, ami később növelhető a fileok mérete alapján. A következő lépéseken halad keresztül:

* Telepíti az FSRM szolgáltatást management tools-okkal együtt
* Létrehozza a kvótákat (maximum méret korlátozása)
* Létrehozza a fájl kiterjesztés szűrésére alkalmas csoportokat
* Alkalmazza a fájl kiterjesztés szűrését a mappákra

|  |
| --- |
| *A képen szöveg, képernyőkép, képernyő, szoftver látható  Automatikusan generált leírás*x. kép – fsrm.yaml első futás |

Az *x-y. képeken* a playbook sikeres lefutását lehet végigtekinteni, valamint a *x-y. képeken* a létrejött beállításokat, majd az *x. képen* azt, hogy ténylegesen működik egy file screening egy *„a.exe”* nevű fájl másolásával az IT mappába (nem lehetséges).

|  |
| --- |
| *A képen szöveg, képernyőkép, képernyő, Betűtípus látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.* x. kép – fsrm.yaml második futás |

|  |
| --- |
| *A képen szöveg, képernyőkép, sor, szám látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – File groupok |

|  |
| --- |
| *A képen szöveg, képernyőkép, szoftver, Weblap látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – File screenek |

|  |
| --- |
| *A képen szöveg, szám, Betűtípus, sor látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – File kvóták |

|  |
| --- |
| *A képen szöveg, képernyőkép, Betűtípus látható  Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.*x. kép – Fájl másolásos tesztelés |

4.2 PowerShell

Az organizational unitek (*ou-k*), groupok (*csoportok*), és felhasználók létrehozására, és csoportba csatlakoztatására, *.ps1* scripteket írtunk, amik segítségével, csak fel kell másolni az adott eszközökre a két-két scriptet, a *.csv* file, ami tartalmazza a felhasználó adatokat, amik a létrehozásukhoz szükségesek, valamint egy *.bat* fájlt, aminek a lefuttatásával meggyorsítjuk a lefuttatást is. A kódokat, a hivatkozásoknál tekinthetik meg valamint a .bat file rövidebb kimenetét az *x-y. képeken* láthatják.

KÉPEK HELYE

5. Árkalkuláció

A hálózat kialakításához szükséges eszközök ára, illetve telepenkénti darabszáma a *x. táblázatban* látható. A táblázatban fel van tüntetve az eszközök darabára, összára, illetve a teljes összár. Az árak 2024.11.14.-i árat jelképezik, ekkor lett az árajánlat kiállítva. A legtöbb eszközből több is lett vásárolva a telepítés soráni vagy utáni hibák gyors javítására.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Árkalkuláció** | | | | | |
| **Eszközök** | **Központ (db)** | **Debrecen (db)** | **Szeged (db)** | **Darabár** | **Összár** |
| 24 portos MLS | 3 db | 0 db | 0 db | 505 882 Ft | 1 517 646 Ft |
| 48 portos L2 switch | 3 db | 2 db | 2 db | 388 263 Ft | 2 717 841 Ft |
| SFP modul (10Gbps) | 26 db | 18 db | 18 db | 34 625 Ft | 2 146 750 Ft |
| Router | 4 db | 4 db | 4 db | 112 500 Ft | 1 350 000 Ft |
| Wifi router | 1 db | 1 db | 1 db | 174 999 Ft | 524 997 Ft |
| Wifi AP | 3 db | 0 db | 0 db | 87 990 Ft | 263 970 Ft |
| ASA | 1 db | 0 db | 0 db | 342 000 Ft | 342 000 Ft |
| Windows szerver (Main ADDS) | 1 db | 0 db | 0 db | 1 401 328 Ft | 1 401 328 Ft |
| Windows szerver | 1 db | 1 db | 1 db | 1 114 344 Ft | 3 343 032 Ft |
| Linux szerver | 2 db | 0 db | 0 db | 1 373 979 Ft | 2 747 958 Ft |
| NAS | 1 db | 0 db | 0 db | 901 560 Ft | 901 560 Ft |
| Háttértár | 16 db | 1 db | 1 db | 43 170 Ft | 777 060 Ft |
| Nagy rack szekrény | 1 db | 0 db | 0 db | 324 700 Ft | 324 700 Ft |
| Kis rack szekrény | 0 db | 1 db | 1 db | 91 500 Ft | 183 000 Ft |
| UTP kábel(100m) | 26 db | 4 db | 5 db | 12 000 Ft | 420 000 Ft |
| RJ45-s csatlakozó (100db) | 5 db | 3 db | 3 db | 395 Ft | 4 345 Ft |
| RJ45-aljzat | 80 db | 20 db | 26 db | 805 Ft | 101 430 Ft |
| Számítógépek | 36 db | 8 db | 12 db | 193 070 Ft | 10 811 920 Ft |
| Monitor | 36 db | 8 db | 12 db | 48 599 Ft | 2 721 544 Ft |
| Billentyűzet | 40 db | 12 db | 16 db | 3 399 Ft | 231 132 Ft |
| Egér | 40 db | 12 db | 16 db | 1 889 Ft | 128 452 Ft |
|  |  |  |  | **Összár:** | **32 960 665 Ft** |

x. táblázat - Árkalkuláció

A *x. táblázatban* látható az eszközök, és a hozzájuk tartozó oldalak URL-jei, amiken az eszközök megvásárolhatóak. Az oldalak néhány paramétert is tartalmaznak.

|  |  |
| --- | --- |
| **Eszközök - Oldalak** | |
| **Eszközök** | **Elérés** |
| 24 portos MLS | <https://www.senetic.hu/product/CBS250-24FP-4X-EU> |
| 48 portos L2 switch | <https://www.senetic.hu/product/CBS220-48P-4X-EU> |
| SFP modul (10Gbps) | <https://www.senetic.hu/product/UACC-CM-RJ45-MG> |
| Router | <https://buyrouterswitch.com/cisco-isr4431-k9-p-5751-price.html> |
| Wifi router | <https://www.mediamarkt.hu/hu/product/_asus-rt-be92u-h%C3%A1roms%C3%A1vos-be9700-wifi-7-aimesh-router-1x10g-wan-lan-fekete-90ig0950-mo9a0v-1465454.html?utm_source=arukereso.hu&utm_medium=psm-product%20feed&utm_content=1465454&aku=d5fb9471a0f52d597f1475a5f1d4f33b> |
| Wifi AP | <https://www.konzolvilag.hu/pc/lan-wifi-asus-dual-band-wifi-6-router-ax5700-mbps-rt-ax86u-pro> |
| ASA | <https://www.router-switch.com/asa5508-k9-p-23193.html> |
| Windows szerver (Main ADDS) | <https://www.senetic.hu/product/EMEA_PER550SPL3?listingSource=servers> |
| Windows szerver | <https://www.senetic.hu/product/EMEA_PER450SPL3?listingSource=servers> |
| Linux szerver | <https://www.senetic.hu/product/EMEA_PER550SPL6?listingSource=servers> |
| NAS | <https://www.senetic.hu/product/TS-1232PXU-RP-4G?listingSource=storage> |
| Háttértár | <https://aqua.hu/alkatreszek/4tb-seagate-35-ironwolf-nas-merevlemez-st4000vn006-t1197148> |
| Nagy rack szekrény | https://aqua.hu/periferiak/conteg-42u-19-i7-allo-rackszekreny-600x1000mm-fekete--ri7-42-60100-h-t207995 |
| Kis rack szekrény | https://aqua.hu/periferiak/intellinet-12u-19-fali-rack-szekreny-600x600-712088-t618394 |
| UTP kábel(100m) | https://kabelvilag.hu/Gembird-UTP-fali-dobozos-kabel-100m-CAT6 |
| RJ45-s csatlakozó (100db) | https://www.aliexpress.com/item/1005003304055489.html?spm=a2g0o.productlist.main.11.4c1d5bNd5bNdTT&algo\_pvid=896e1681-d6c6-44c1-a7ae-bdc7a12eaabd&algo\_exp\_id=896e1681-d6c6-44c1-a7ae-bdc7a12eaabd-5&pdp\_npi=4%40dis%21HUF%211656.24%21393.21%21%21%214.17%210.99%21%40210385a817315783758132168ea839%2112000025107419993%21sea%21HU%210%21ABX&curPageLogUid=kM3u3fl81I6e&utparam-url=scene%3Asearch%7Cquery\_from%3A |
| RJ45-aljzat | https://www.aliexpress.com/item/1005003223306465.html?spm=a2g0o.productlist.main.1.748f3i5N3i5NIk&algo\_pvid=55d60275-f5de-446b-9532-a5f5af62ce6b&algo\_exp\_id=55d60275-f5de-446b-9532-a5f5af62ce6b-0&pdp\_npi=4%40dis%21HUF%214464.31%21393.21%21%21%2111.24%210.99%21%402103850917315785195226603efbd2%2112000026896671927%21sea%21HU%210%21ABX&curPageLogUid=GruRMaUx5tk3&utparam-url=scene%3Asearch%7Cquery\_from%3A |
| Számítógépek | <https://www.pcx.hu/?action=prodConfig2/getConfig&processor=854682&processor_piece=1&processorCooler=320078&processorCooler_piece=1&motherboard=774508&motherboard_piece=1&memory=162236&memory_piece=1&ssd=978850&ssd_piece=2&powerSupply=791003&powerSupply_piece=1&computerCase=126826&computerCase_piece=1&systemCooler=676667&systemCooler_piece=3&assembly=1&assembly_piece=1&biosUpdate=-12&biosUpdate_piece=1> |
| Monitor | <https://www.mediamarkt.hu/hu/product/_asus-vy249hf-w-24-s%C3%ADk-fullhd-100-hz-16-9-freesync-ips-led-monitor-1446251.html> |
| Billentyűzet | <https://www.mediamarkt.hu/hu/product/_hama-casano-vezet%C3%A9kes-magyar-billenty%C5%B1zet-53813-1104669.html> |
| Egér | <https://www.mediamarkt.hu/hu/product/_isy-icm-1000-fekete-vezet%C3%A9kes-eg%C3%A9r-1276188.html> |

x. táblázat - Eszközök oldalai

A csapat munkadíja 27 000 000 Ft. Tehát a projekt összköltsége: **59 960 665 Ft**

6. Tesztelés

6.1 Hálózat

6.2 Szerverek

7. Összegzés