 **Budapesti Műszaki SZC Bláthy  
Ottó Titusz Informatikai Technikum**

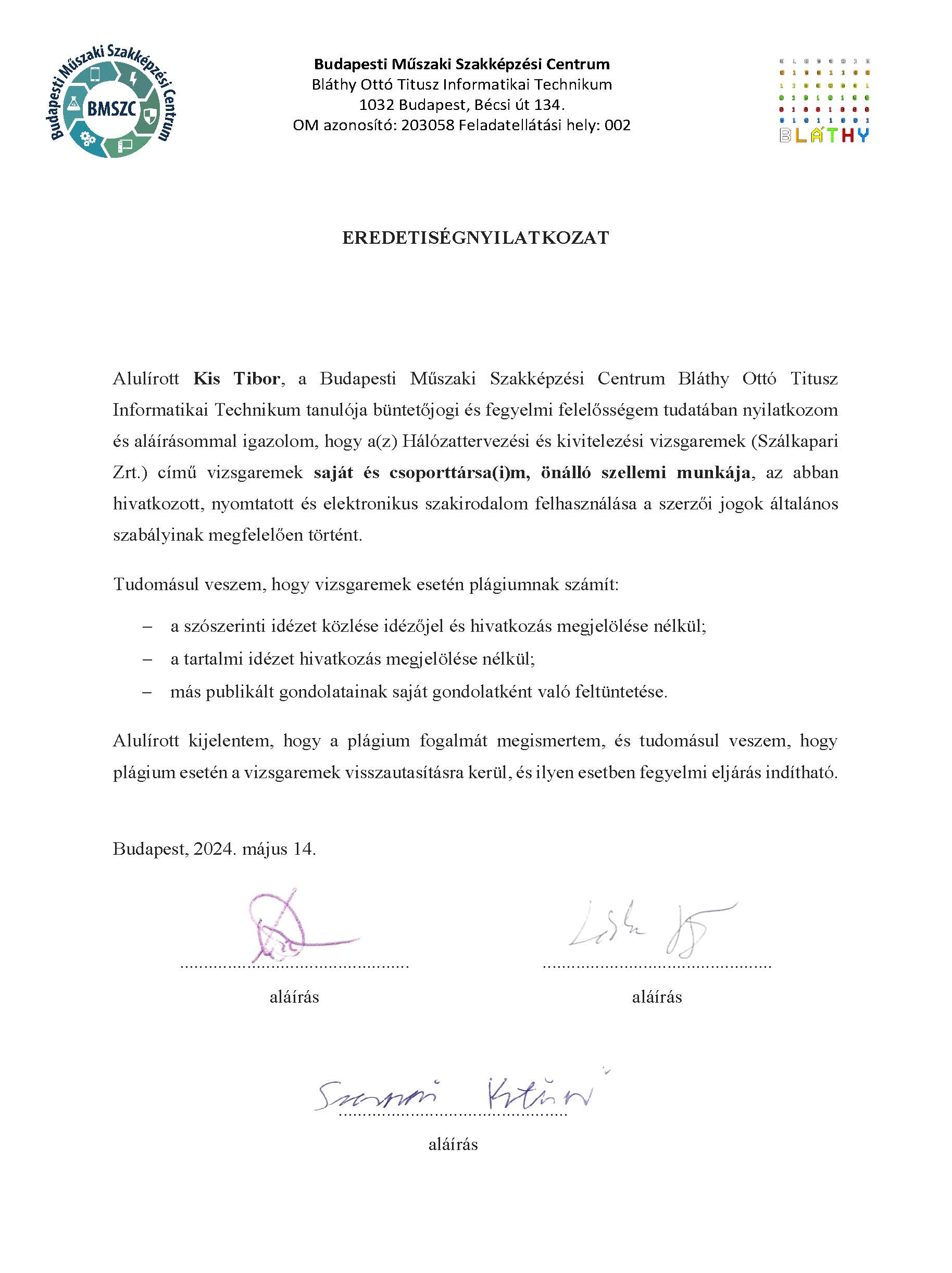
Hálózattervezési és kivitelezési vizsgaremek

Kis Tibor

Lócska Gergő István

Szamosi Krisztián Benjamin

2/14E – IT | 2024.



Tartalom

[1. Bevezetés 4](#_Toc166620149)

[2. Hálózat fizikai struktúrája 5](#_Toc166620150)

[3. Hálózati logikai struktúrája 6](#_Toc166620151)

[4. Alkalmazott hálózati konfigurációk 7](#_Toc166620152)

[4.1 Forgalomirányítás 7](#_Toc166620153)

[4.2 IP címek kiosztása 7](#_Toc166620154)

[6. Etherchannel 8](#_Toc166620155)

[7. Virtual Private Network 9](#_Toc166620156)

[8. Tűzfal - Adaptive Security Appliance 11](#_Toc166620157)

[9. Forgalomirányítón megvalósított biztonsági funkciók 13](#_Toc166620158)

[10. Vezeték nélküli hálózat 14](#_Toc166620159)

[11. Windows szerver konfigurálása 15](#_Toc166620160)

[11.1 DHCP 15](#_Toc166620161)

[11.2 Active Directory beállítása 15](#_Toc166620162)

[11.3 Biztonsági mentés 18](#_Toc166620163)

[12. Linux szerver konfigurálása 19](#_Toc166620164)

[12.1 Telepítés 19](#_Toc166620165)

[12.2 DNS 19](#_Toc166620166)

[12.3 SSH 20](#_Toc166620167)

[12.4 Samba 20](#_Toc166620168)

[12.5 Apache 21](#_Toc166620169)

[12.6 FTP 21](#_Toc166620170)

[13. Jövőbeni fejlesztések 22](#_Toc166620171)

[14. Csapatmunka 23](#_Toc166620172)

[15. Mellékletek 24](#_Toc166620173)

# Bevezetés

A Szálkapari Zrt., mint jelentős szereplő a bútoriparban, komplex hálózati infrastruktúrával rendelkezik, amely támogatja a bútorok tervezését, raktározását és értékesítését. Cégünk három telephellyel büszkélkedhet Magyarország és Szlovákia területein: egy áruházzal Pozsonyban, egy raktárral Sopronban és a központi irodával Győrben. Ez a területi elhelyezkedés nemcsak adóoptimalizálási szempontokból fontos, hanem különleges kihívásokat is jelent a hálózati infrastruktúra szempontjából.

A területi széttagoltság és a különböző funkcionalitású telephelyek igénylik az adataink, erőforrásaink és kommunikációnk zökkenőmentes integrációját, ami elengedhetetlen a hatékony működéshez. A hálózati infrastruktúra vizsgálata ebben a kontextusban kiemelt jelentőséggel bír, hiszen ennek optimalizálása közvetlen hatással van a vállalati hatékonyságra és a működési költségekre. A vizsgálat célja, hogy feltárja a jelenlegi hálózati környezet erősségeit és gyengeségeit, javaslatokat tegyen a lehetséges fejlesztési irányokra, valamint felmérje a biztonsági kockázatokat és azok mérséklésének lehetőségeit.

A hálózati vizsgálat során külön figyelmet fordítunk az alábbi szempontokra:

1. Adatforgalom elemzése
2. Biztonsági protokollok
3. Hálózati redundancia
4. Teljesítményoptimalizálás

A hálózati vizsgálat eredményeinek integrálása nemcsak hogy javítja a vállalati folyamatokat, de hozzájárul a Szálkapari Zrt. piaci pozíciójának erősítéséhez, biztosítva, hogy a cég továbbra is élen járjon az innovációban és ügyfélkiszolgálásban. Ezáltal a vizsgálat nem csupán technikai felülvizsgálat, hanem stratégiai eszköz a vállalati siker érdekében

# Hálózat fizikai struktúrája

A vállalati hálózatban a kommunikáció létrejöttéhez a forrás és cél állomás összeköttetéséhez meg kell teremtenünk a csatornát, azt az átviteli közeget, amelyen keresztül az információ biztonságosan továbbítva lesz. Megvalósításunkban kétféle típust alkalmaztunk, a fizikai, vagy vezetékes, illetve a vezeték nélküli technológiát.

Telephelyeinken az adott létesítés idején legyakrabban alkalmazott technika lelhető fel. Mind csavart érpáras, de régebbi telephelyeken CAT5e az újabbakon már CAT6 típusúakat, változatos gyártóktól.

A hozzáférési és elosztási rétegek eszközeit a Cisco cég megbízható termék skálájáról választottuk.

Távközlési szolgáltatónk jóvoltából a telephelyeinket nagysebességű béreltvonali összeköttetést tudunk használni. A soproni telephely nagy sávszélességű internet csatlakozása kielégítően kiszolgálja a többi telephely igényét is. Az csatlakozás helyét a szolgáltató adott helyszínre adott kedvező ajánlata indokolta.

Minden telephelyen szervereket és nyomtatókat üzemeltetünk az adott irodai igények kiszolgálására.

Mobil eszközök számára az egyes helyszíneken a felhasználók számára hozzáférési pontokat (Access Point, AP) alakítottunk ki.

# Hálózati logikai struktúrája

Az elosztási réteg minden telephelyen több, logikailag különálló részre osztott. Alhálózatokat, VLAN-okat hoztunk létre szegmentált IP címzés alkalmazásával. Ennek több ismert oka van.

* Fizikai elhelyezkedés
* Logikai csoportosítás
* Terhelés csökkentése
* Biztonság
* Szórások hatókörének korlátozása

**Fő telephelyek és funkcióik:**

* **Győr (Központi iroda):** Itt található a vállalatirányítási rendszer (ERP), ami az üzleti folyamatokat (HR, pénzügy, raktárkezelés, értékesítés) koordinálja.
* **Sopron (Raktár):** A késztermékek tárolása és a logisztikai folyamatok kezelése történik itt.
* **Pozsony (Áruház):** Értékesítési pont, ahol közvetlen kapcsolatban állunk a végfelhasználókkal.

**Hálózati kapcsolatok:**

* **VPN (Virtual Private Network):** Távoli hozzáférés esetén VPN-t használunk, hogy biztosítsuk a biztonságos kapcsolatot az otthoni munkavégzés vagy távoli telephelyek számára.

**Tűzfalak és biztonsági szabályok:**

* Minden telephelyen tűzfalak vannak telepítve, amelyek szabályozzák a bejövő és kimenő forgalmat, és megakadályozzák a nem kívánt hozzáféréseket.

**Adatvédelmi intézkedések:**

* Az adatok titkosítása és biztonsági mentéseken keresztül biztosítjuk az információk védelmét.

Ez a hálózati logikai struktúra lehetővé teszi a Szálkapari Zrt. számára, hogy hatékonyan kezelje a területi kihívásokat, biztosítva a zökkenőmentes működést és a magas szintű biztonságot.

# Alkalmazott hálózati konfigurációk

## Forgalomirányítás

A telephelyeken illetve azok között a dinamikus forgalomirányítást OSPF területek kialakításával oldottuk meg. Két területet hoztunk létre. Egy Area 0-t a gerinchálózatnak és egy Area 1-et a telephely belső hálózatára. Egy jellemző kódsor a két routerre:

*Gyor\_R0*

router ospf 1

network 130.10.10.0 0.0.0.3 area 0

network 130.10.10.8 0.0.0.3 area 0

network 10.10.10.0 0.0.0.3 area 1

network 10.10.20.0 0.0.0.3 area 1

*Gyor\_R1*

router ospf 1

network 192.168.1.0 0.0.0.31 area 1

network 192.168.1.32 0.0.0.31 area 1

network 192.168.1.64 0.0.0.7 area 1

network 192.168.1.72 0.0.0.7 area 1

network 192.168.1.80 0.0.0.7 area 1

network 10.10.10.0 0.0.0.3 area 1

## IP címek kiosztása

A teljes hálózaton alkalmaztunk Szerver PC általi, forgalomirányító általi és statikusan beállított IP cím kiosztást. Így történt mind az IPv4 mind az IPv6 címekre. Egy jellemző routeren kiadott parancssorozat az IPv4 címkiosztásra:

*Gyor\_R1*

ip dhcp pool poolvlan10

network 192.168.1.0 255.255.255.224

default-router 192.168.1.1

dns-server 192.168.1.75

domain-name butor.loc

exit

ip dhcp excluded-address 192.168.1.1 192.168.1.3

Ugyanezen az eszközön az IPv6 címek terjesztésének bekapcsolása:

ipv6 unicast-routing

ipv6 dhcp pool GYOR\_A\_v6

address prefix 2001:DB8:CAFE:10::/64

dns-server 2001:DB8:CAFE:40::B

domain-name butor.loc

exit

intetface g0/1.10

ipv6 address 2001:DB8:CAFE:10::1/64

ipv6 address fe80::10 link-local

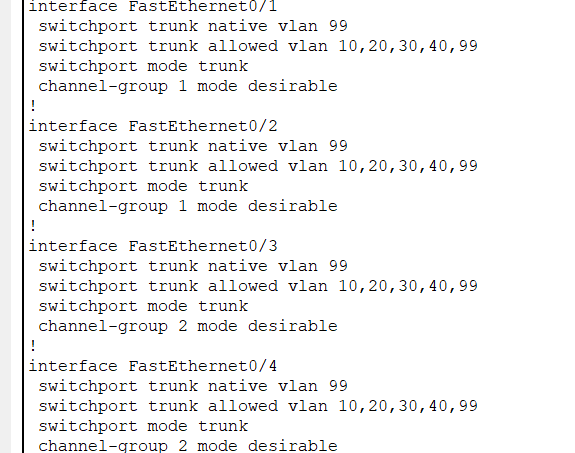
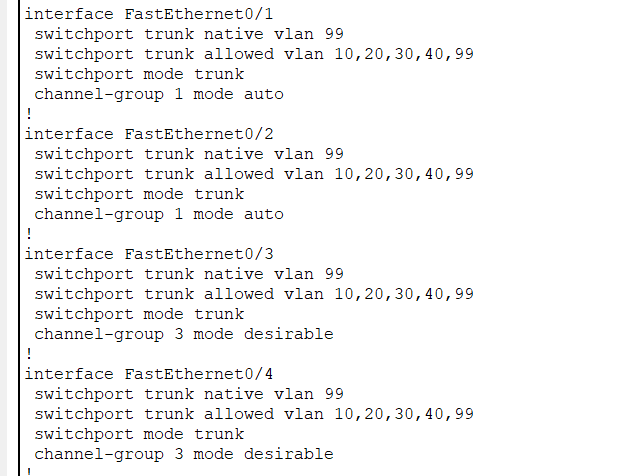
ipv6 dhcp server GYOR\_A\_v6

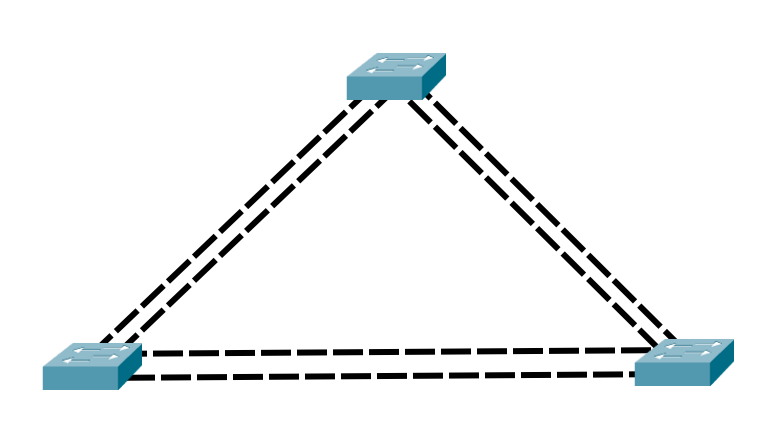
ipv6 nd managed-config-flag

# Etherchannel

Az EtherChannel előnyei

Az EtherChannel (portcsatorna) interfész számos előnnyel jár. Elsősorban lehetővé teszi a legtöbb konfigurációs feladat egyszerű végrehajtását, mivel nincs szükség a portok egyedi kezelésére. Ezáltal biztosítva van azok következetes beállítása. Az EtherChannel meglévő switchportokat használ, így elkerülhető a gyorsabb és drágább összeköttetés szükségessége a nagyobb sávszélesség eléréséhez. Továbbá az EtherChannel-hez tartozó portok között terheléselosztás valósul meg, ami hardvertől függően egy vagy több terheléselosztási módot is magában foglalhat. Ezek közé tartozik a forrás MAC és cél MAC terheléselosztás, valamint a forrás IP és cél IP terheléselosztás fizikai kapcsolatokon keresztül.Az EtherChannel redundanciát biztosít, mivel a teljes összerendezett köteg egy logikai kapcsolatot alkot. Emellett a csatorna valamely fizikai portjának kiesése nem okoz változást a topológiában, így nem szükséges az STP újraszámítása. Amíg legalább egy fizikai port aktív, az EtherChannel működőképes marad, de a kiesett portok miatt a teljes átbocsátóképesség csökkenhet.  
  
Topológiai kialakítás a győri telephely hálózatában





# Virtual Private Network

A VPN (Virtual Private Network) konfigurációja és implementációja alapvető fontosságú a két szervezet belső hálózatai közötti biztonságos kommunikációhoz. A rendszerterv ebben a fejezetben részletesen bemutatja a VPN konfigurációt, kitérve a biztonsági aspektusokra és az előnyökre.

Konfiguráció Részletei:

A rendszerterv először is részletesen ismerteti a VPN konfigurációjának részleteit mindkét szervezet routerén. A konfiguráció magában foglalja az alábbi lépéseket:

* Access-listek definiálása az engedélyezett IP-címek és portok megadásához.
* ISAKMP (Internet Security Association and Key Management Protocol) politika beállítása a kulcsszerződés és a titkosítási algoritmusok meghatározásához.
* Az ISAKMP kulcsok és az IPsec transformációs készletek konfigurálása az autentikáció és a titkosítás számára.
* A kriptográfiai térképek beállítása az IPsec és ISAKMP konfigurációkhoz.

Biztonsági Aspektusok:

A rendszerterv kiemelten foglalkozik a VPN konfiguráció biztonsági részleteivel. Ezek a következők:

* Titkosítás: Az AES 256-bites titkosítás és az SHA algoritmusok használata adataink védelme érdekében.
* Előosztott kulcsok: Az előosztott kulcsok biztosítják az autentikációt és az adatok titkosítását a VPN kapcsolatokban.
* Access-listek: Az access-listek pontosan meghatározzák, hogy mely IP-címek és portok kommunikálhatnak egymással, ezáltal minimalizálva a támadási felületet.
* IPsec transformációs készlet: Az IPsec transformációs készlet biztosítja az adatok titkosítását és integritásának ellenőrzését az adatátvitel során.

A VPN konfiguráció és implementáció számos előnnyel jár mindkét fél számára

Az egyik ilyen a **biztonság**: A VPN egy biztonságos csatornát biztosít a két belső hálózat közötti kommunikációhoz, minimalizálva a külső fenyegetéseket és a bizalmas adatok illetéktelen hozzáférését. **Költségcsökkentés**, mert a VPN lehetővé teszi a két szervezet számára, hogy közös erőforrásokat használjanak, csökkentve a hálózati infrastruktúra költségeit.

VPN konfiguráció és implementáció megfelelő végrehajtása alapvető fontosságú a szervezetek belső hálózatai közötti biztonságos és hatékony kommunikációhoz. A rendszerterv részletesen dokumentálja a konfigurációt, kiemelve annak biztonsági részleteit és előnyeit.

A VPN működését a csatolt videóban mutatjuk be.[[1]](#footnote-1)

# Tűzfal - Adaptive Security Appliance

A hálózatban megvalósított konfiguráció részletes áttekintésével megérthetjük a tűzfalak és hálózati eszközök kritikus szerepét a biztonságos és hatékony hálózatok működtetésében. Az ASA (Adaptive Security Appliance) eszközök a Cisco egyik legnépszerűbb termékei, melyeket különösen a hálózati biztonság és az adatforgalom szabályozására használnak. A hálózatban megvalósított konfiguráció alapján az ASA konfigurációját és a hálózati kommunikációt mutatjuk be.

Az ASA konfiguráció alapjai

1. **Alapkialakítás és hozzáférési beállítások:**
   * A hostname beállítás megadja a tűzfal nevét, amely fontos a hálózatban lévő eszközök azonosításához.
   * Az enable password és a username/password beállítások a hozzáférési biztonságot szolgálják, hogy csak jogosult felhasználók férhessenek hozzá a tűzfalhoz.
2. **Interfész konfigurációk:**
   * nameif paranccsal az interfészek neveit állítjuk be (INSIDE, OUTSIDE), amelyek a hálózati architektúra érthetőségét segítik.
   * security-level beállítások különböző biztonsági szinteket jelölnek, ahol magasabb szám nagyobb biztonságot jelent. Az INSIDE interfész általában magasabb biztonsági szintet kap.
   * ip add paranccsal az IP-címeket rendeljük az interfészekhez.
3. **OSPF (Open Shortest Path First) routing:**
   * Az OSPF egy dinamikus útválasztási protokoll, amely segít az útvonalak automatikus kiválasztásában a hálózaton belül, hatékonyságát és skálázhatóságát növelve.
   * A hálózati parancsok (network) az OSPF által figyelt IP-cím tartományokat definiálják.
4. **Statikus útvonalak:**
   * A route paranccsal statikus útvonalat adunk meg, amely alapértelmezett útvonalként szolgál az adatforgalom számára, ha nincsenek egyéb elérhető vagy megfelelő dinamikus útvonalak.
5. **ACL (Access Control List) konfiguráció:**

Az ACL-ek a tűzfalakon keresztül menedzselik, hogy milyen forgalom engedélyezett vagy tiltott az egyes interfészeken. Az ACL-eket különösen fontos helyesen konfigurálni, hogy a hálózati biztonsági politikák érvényesüljenek.

**ACL definiálása és alkalmazása:**

* + access-list ALLOW\_PING extended permit icmp 130.10.10.16 255.255.255.252 any:

Ez az ACL-sor engedélyezi az ICMP forgalmat (általában ping kérésekhez használt), ami kiindul a 130.10.10.16/30 hálózatról és bármilyen cél felé irányul. Ez a beállítás lehetővé teszi a hálózati eszközök elérhetőségének ellenőrzését és a hálózati diagnosztika végrehajtását.

* + access-group ALLOW\_PING in interface OUTSIDE:

Ez a parancs alkalmazza az ALLOW\_PING ACL-t az OUTSIDE interfészen. Az alkalmazott ACL megadja, hogy az adott szabályok melyik interfészen legyenek érvényesek, így biztosítva, hogy a bejövő forgalmat szabályozzuk az adott interfészen

Előnyök

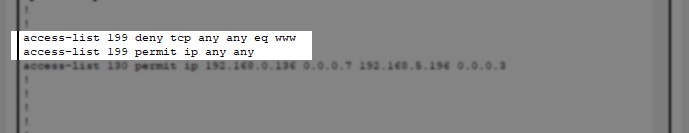
* **Biztonság:** Az interfészek és felhasználók szigorú beállításaival az ASA biztosítja, hogy csak megbízható forgalom haladhasson át a hálózaton, és csak jogosult személyek férjenek hozzá a kezelőfelülethez.
* **Skálázhatóság és rugalmasság:** Az OSPF használata lehetővé teszi a hálózat gyors adaptációját a változásokhoz, új eszközök integrálását és hibatűrő útvonalak kialakítását.
* **Kontroll és átláthatóság:** A részletes interfész- és biztonsági beállításokkal az IT csapat könnyen monitorozhatja és kezelheti a hálózati tevékenységeket, javítva a hálózati menedzsment hatékonyságát.

Ezek a beállítások és előnyök biztosítják, hogy a vállalati hálózatok biztonságosak, megbízhatóak és jól kezelhetőek maradjanak, ami alapvető a mai gyorsan változó informatikai környezetben.

# Forgalomirányítón megvalósított biztonsági funkciók

Alapvető biztonsági funkcióként a hálózat minden forgalomirányítója jelszavas védelemmel és hozzáférési szabályok beállításával korlátozza az eszközökhöz és erőforrásokhoz való hozzáférést.

Minden eszközön engedélyezve lett az SSH és felhasználó lett létrehozva, melynek jelszavát titkosítva tárolódik.

További biztonsági funkcióként a belső hálózaton a bárki által elérhető, Linux webserveren tárolt és publikált intranetes tartalmat a 443-as port (HTTPS) preferálásával és a 80-as port (HTTP) tiltásával szabályozzuk. Ez javítja az internetes kommunikáció biztonságát és védelmét valamint hozzájárul az adatvédelemhez és az adatbiztonsághoz. Egyes szabályozási irányelvek és adatvédelmi jogszabályok (pl. GDPR), elő is írják az adatok biztonságos továbbítását és tárolását, melyek így titkosított formában kerülnek továbbításra, így sokkal nehezebb azokat illetéktelenek számára megfigyelni vagy megváltoztatni.[[2]](#footnote-2)

# Vezeték nélküli hálózat

Elkerülhetetlen és nem is lehet cél a vezetéknélküli hálózat használata Az általuk biztosított számos előny mellett hátrányuk jelentéktelen. A mobilitás, a kényelem felhasználói oldalról, míg a skálázhatóság, költségcsökkentés vagy a telepítési rugalmasság tulajdonosi és rendszeradminisztrációs oldalról teszi vonzóvá a technológiát.

Több hálózati szegmensben is található WiFi hozzáférési lehetőség. Egyes helyeken ez Access Point-tal míg máshol WiFi Routerrel valósul meg.

Az Access Point-tal lefedett helyeken az egyes eszközök (számítógépek, okostelefonok, táblagépek stb.) kapcsolódását és csatlakozását oldja meg a vezetékes hálózathoz. A vezeték nélküli eszközök hozzáférnek a kábelen keresztül is elérhető erőforrásokhoz, mint nyomtatók, fájlkiszolgáló vagy akár a DHCP szolgáltatás.

Ezzel szemben a WiFi Router sokkal nagyobb elszigetelést és ezzel biztonságot szavatol a megfelelő beállításokkal. Egyedi tűzfallal vagy akár címfordítással kapcsolhatók be hálózatba az itt belépő eszközök.

# Windows szerver konfigurálása

## DHCP

A Windows Server 2016-os operációs rendszerre DHCP szolgáltatást telepítettünk. Beállításai alapján a Gyor\_B területnek a 192.168.1.32/27 hálózatszegmensből szolgáltat IP címet. Az alábbi képen jól látható, hogy a Windows10 kliens a 192.168.1.37-es IP címet kapta a megfelelő 192.168.1.33-as átjáró IP címével. Ennek megfelelően a bérlet is megjelent a szerver felügyeleti konzolján.



## Active Directory beállítása

A megfelelő IP cím kiosztása után a klienst a szerveren létrehozott AD-ba léptettük. A kép jobb oldali, szerver képernyőképen jól látszik, hogy fut a DNS szolgáltatás, ami nélkül az AD nem látná el a feladatát, illetve felül látszik, hogy létre lett hozva egy tartomány ***Gyor.Server0*** néven. A kliensen az alapértelmezett Workgroup munkacsoportból kezdeményeztük a gép tartományba léptetését a tartomány pontos nevének megadásával. 

A tartományvezérlő a kérelemre egy olyan felhasználó nevét és jelszavát kéri be, akinek joga van a beléptetést végrehajtani. Ha ezt megkapta egy üdvözlő ablakkal rögzíti a belépés tényét, majd újraindítás után már lehetőség van akár egy az AD-n létrehozott felhasználóval is belépni.



Belépés után - az Iroda szervezeti egység tagjaként - Példa Ottó nevű felhasználónk a számára beállított megosztott meghajtót az egyszerűség kedvéért "*Z: megh*ajtó”-ként felcsatolva sikeresen eléri.



Csoportházirend átgondolt beállításaival az egyes szervezeti egységek, így azok tagjai a felhasználók, hálózaton illetve az egyes végponti gépeken alkalmazott jogai, lehetőségei jól szabályozhatók. Óriási előnye, hogy ennek menedzselését a rendszergazda vagy az erre a feladatra jogosultságokkal ellátott személy, központosított módon láthatja el. A felhasználó számára is előnyökkel járhat. Épületen belül a különböző gépeken belépve, az azonosítása után akár mindig ugyanaz a munkakörnyezet fogadhatja, így növelve a kényelmét és a hatékonyságát.

A szerveren megosztott nyomtatási szolgáltatás is fut. A kliens megtalálta és telepítette is a szerveren található és az AD által terjesztett Canon nyomtatót.

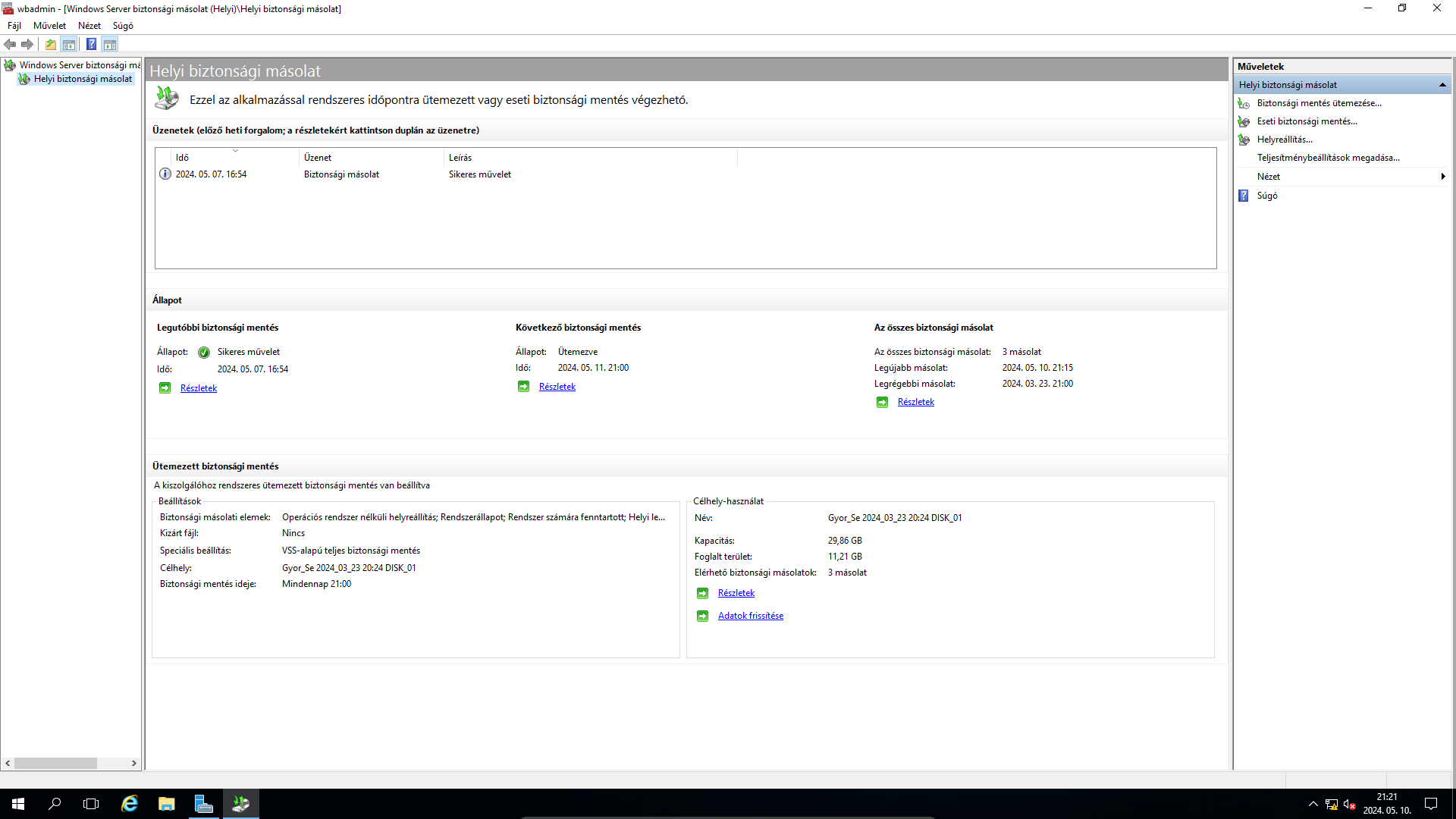


További beállításokkal finomíthatók a felhasználó nyomtatásra vonatkozó jogai.

## Biztonsági mentés

A kiszolgáló biztonsági mentése elengedhetetlen a fontos adatok elvesztésének megakadályozása érdekében. Az időszakos biztonsági mentések konfigurálása lehetővé teszi a rendszer visszaállítását olyan váratlan események előfordulása esetén, mint például a hardverösszetevők meghibásodása, a rendszer helytelen konfigurálása vagy vírusok jelenléte.

A windows Servernek beépített megoldása van erre, amelyet hozzá lehet adni a szolgáltatásokhoz. A mentések automatizálásával és megfelelő ütemezéssel igyekeznünk kell a kár minimalizálására. Rendkívül fontos átgondolnunk a mentések tárolásának módját és helyét és begyakorolni a visszaállítás módját annak sikerességének ellenőrzésével.



# Linux szerver konfigurálása

## Telepítés

A linux szerver a soproni telephelyen üzemel. A telepítés után a Sopron-linux nevet és statikusan beállított IP címet (192.168.0.138/30) kapott. Számos szolgáltatás fut rajta.

DNS, Apache, SSH, FTP, Samba

## DNS

BIND9 DNS szerver szolgáltatás fut rajta. A Windows 10 kliensről tesztelve a butor.loc nevet a Linux feloldja majd sikeres ping válaszokat küld.



## SSH

Egy távoli Windows 10 kliens gépről léptünk be SSH-val. Az azonosítás sikeres volt és a Promptban megjelent a Linux, majd ezután futatható volt akár az MC alkalmazás is.   


## Samba

Az Ubuntu és Windows számítógépek összekapcsolásának egyik legáltalánosabb módja a Samba beállítása fájlkiszolgálóként. Mi is ezt használtuk.



## Apache

Az apache telepítése és aktiválása után – a már működőképes SSH és a Samba segítségével - az alapértelmezett mappába feltöltöttük az egyelőre statikus intranetes információs oldal összetevőit, két HTML fájlt és a hozzájuk tartozó, stílusukat leíró CSS állományt.

A feltöltés után ugyancsak a távoli Windows 10 kliens böngészőjével teszteltünk.[[3]](#footnote-3)

## FTP

Az Ubuntu szerverre telepítettünk egy FTP kiszonlgálót is. Bár a disztribúció alapértelmezett alkalmazása a VSFTPD meglehetősen elterjedt és népszerű választás a biztonságos és hatékony fájlátvitelre, nem használjuk. A klienseken kizárólag Windows operációs rendszerek futnak. Ezekhez a Samba az ideális és megfelelően rugalmas megoldás. Az FTP előkészítésével azonban felkészülhetünk Linux vagy IOS operációs rendszerekkel való kommunikációra.

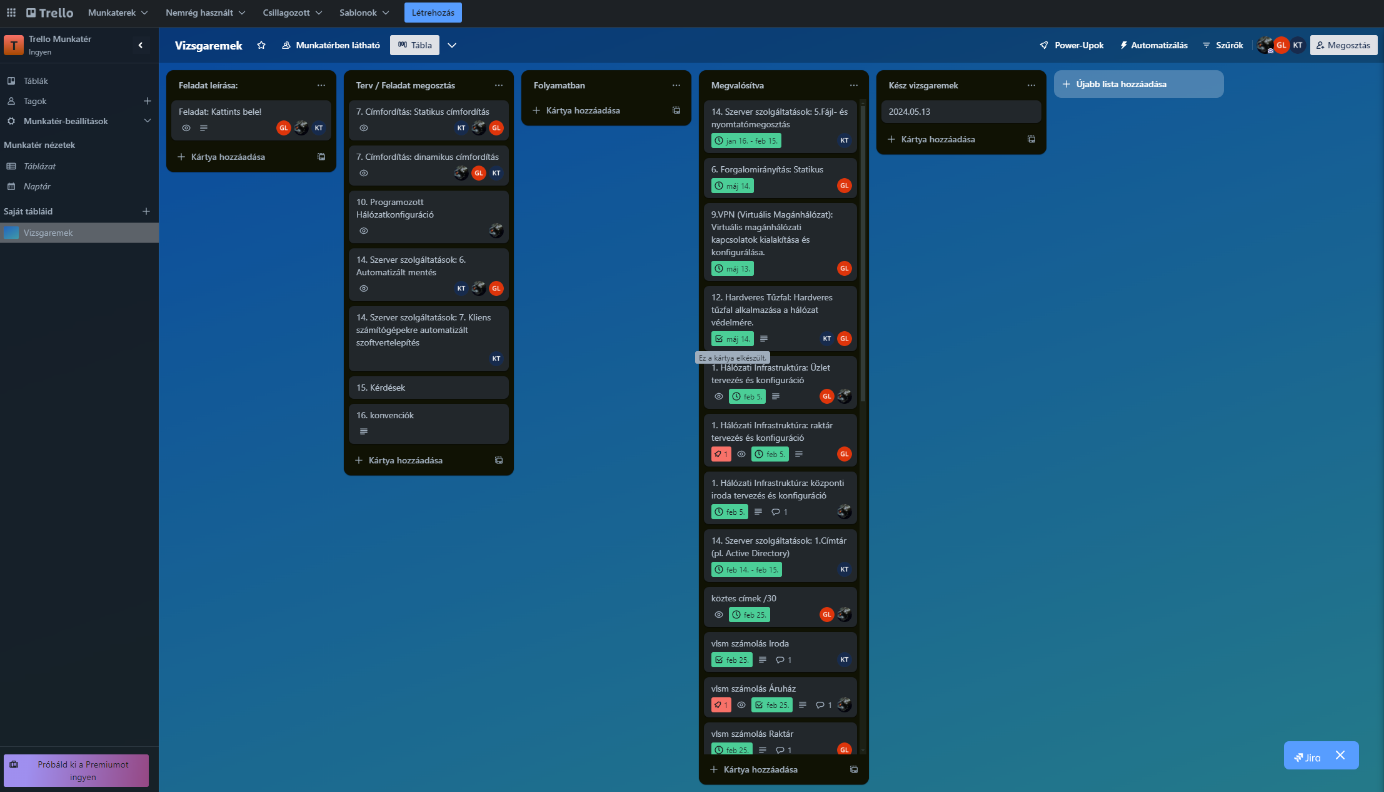
# Jövőbeni fejlesztések

A ***statikus és dinamikus címfordítás*** olyan technikák, amelyek segítenek az IP címek és hálózati címek kezelésében, hogy hatékonyabbá tegyék a hálózatokat és optimalizálják a hálózati erőforrásokat. Ezáltal javulhat a hálózat teljesítménye és rugalmassága. A programozott hálózatkonfiguráció lehetővé teszi a hálózati eszközök automatikus beállítását és irányítását, amely jelentősen csökkentheti az emberi beavatkozásra fordított időt és erőforrásokat. Ezáltal a hálózatok gyorsabban és hatékonyabban reagálhatnak az üzleti igényekre. Az ***automatizált mentés*** lehetővé teszi az adatok biztonságos és rendszeres másolatokban való tárolását, ami kulcsfontosságú a vállalati adatvédelem és az üzleti folytonosság szempontjából. A számítógépekre ***automatizált szoftvertelepítés*** lehetővé teszi az operációs rendszerek és alkalmazások gyors és egyszerű telepítését és frissítését, ami csökkentheti az informatikai támogatásra fordított időt és költségeket, valamint növelheti az alkalmazottak produktivitását. A ***DMZ létrehozása*** (Demilitarized Zone) egy olyan hálózati terület létrehozását jelenti, amely elválasztja a belső hálózatot a külső hálózatoktól, így növelve a hálózati biztonságot és csökkentve a támadások kockázatát. A jövőben meghatározásra kell kerüljön, hogy költségszempontok alapján a DMZ vagy a felhő alapú megoldások tudnak megvalósulni. Ezt befolyásolhatja a felhő technológia elterjedése és ezzel együtt árainak csökkenése.

# Csapatmunka

A csapatmunka megvalósításához elengedhetetlen tényező az együttműködés, türelem és egy kis humor. Természetesen többféle kommunikációs csatornát is igénybe kellett vennünk, úgy mint: Trello, Microsoft Teams, Messenger, személyes találkozó. Teams megbeszéléseket leginkább minden vasárnap este 18:00-tól tartottunk, amik általában 1-2 órát emésztettek fel. A határidő közeledtével ezek a megbeszélések sűrűsödtek és tovább is tartottak az eddigi 1-2 óránál.

Trello-t leginkább tervezés, feladat kiosztásra használtuk.



Továbbá a Github hatékonnyá tette a közös munkavégzést. Közös tárhelyként tudtuk használni, így nem kellett egymásnak küldözgetni az aktuális vizsgaremek fájlokat.

# Mellékletek

Hálózati topológia:

Költségvetés

A cég hálózata a következő eszközöket igényli:

|  |  |  |
| --- | --- | --- |
| **Eszköz** | **Mennyiség (darab)** | **Összeg  USD** |
| PC (személyi számítógép) | 20 db | 27 855 $ |
| Laptop | 5 db | 6963 $ |
| Switch 2960 | 7 db | 8715 $ |
| Router 2911 | 8 db | 37 800 $ |
| Linksys WRT300N | 3db | 120 $ |
| Multilayer switch 3650 | 2 db | 18 572 $ |
| Server | 3 db | 15 833 $ |
| Access Point | 1 db | 130 $ |
| Nyomtató | 4 db | 1522 $ |
| ASA 5506 (tűzfal) | 1 db | 1261 $ |

**1 USD = 360 HUF (középárfolyam)**

**Összköltség az eszközökre: 118771 $ - 42 757 560 HUF**Továbbá felmerülő költségek:  
- Eszközök telephelyekre történő szállítása, maximum keret 500.000 HUF   
- Eszközök beszerelése, konfigurálás, munkadíj, maximum keret: 7.196.400 HUF  
  
**A teljes hálózat kialakításának bekerülési értéke: 50 453 960 HUF**

Tesztelés

Mellékelt video anyagban többcélúan teszteltük a hálózatot. Forgalomirányítás, biztonság és szolgáltatások működését demonstráljuk.

* vpn\_teszt.mp4

Két telephely szervere közötti kommunikáció VPN-en kersztüli megvalósítása

* pt-80port-acl-tilt-demo.mp4

teljes hálózaton tiltott 80-as port és engedélyezett HTTPS protokoll tesztelése böngésző és Apache szerver között

* ssh-smb-apache-demo.mp4

Ubuntu Samba szerver megosztásainak tesztelése egy Windows10 kliens gépen

* pt-tracert-demo.mp4

hálózati forgalom útvonalának nyomon követése két véletlenszerűen választott, külön telephelyen található gép között.

1. KisTibor\_LócskaGergőIstván\_SzamosiKrisztiánBenjamin\_video.pptx | 1. dia | vpn\_teszt.mp4 [↑](#footnote-ref-1)
2. KisTibor\_LócskaGergőIstván\_SzamosiKrisztiánBenjamin\_video.pptx | 2. dia | pt-80port-acl-tilt-demo.mp4 [↑](#footnote-ref-2)
3. KisTibor\_LócskaGergőIstván\_SzamosiKrisztiánBenjamin\_video.pptx | 5. dia | ssh-smb-apache-demo.mp4 [↑](#footnote-ref-3)