Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

***Szakképesítés neve:*** Informatikai rendszer- és alkalmazás-üzemeltető technikus

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**South Brokes Zrt. hálózat bemutatása**

Haraszti Gyula, Kassai László, Mátravölgyi Bendegúz   
2/14B

Budapest, 2022.03.26

Tartalom

[Cégleírás 4](#_Toc99276986)

[South Brokers Zrt. szerverkörnyezetének dokumentációja 4](#_Toc99276987)

[Szolgáltatások: 5](#_Toc99276988)

[A cég felépítése: 6](#_Toc99276989)

[South Brokers 6](#_Toc99276990)

[Szolgáltatások részletezése 7](#_Toc99276991)

[sFTP: 7](#_Toc99276992)

[IIS: 7](#_Toc99276993)

[Email (IRedMail) 8](#_Toc99276994)

[Syslog: 8](#_Toc99276995)

[TFTP: 9](#_Toc99276996)

[AD: 9](#_Toc99276997)

[DC: 10](#_Toc99276998)

[RODC: 10](#_Toc99276999)

[File: 11](#_Toc99277000)

[DNS: 12](#_Toc99277001)

[DHCP: 13](#_Toc99277002)

[DHCP Failover 13](#_Toc99277003)

[Költségvetés 17](#_Toc99277004)

[A hálózat tesztelésének dokumentációja 18](#_Toc99277005)

[Zöld terület: Fő telephely: 18](#_Toc99277006)

[HSRP: 20](#_Toc99277007)

[Feszitőfa( Spanning Tree Protocol) 21](#_Toc99277008)

[Link Aggregation: 22](#_Toc99277009)

[ACL: 23](#_Toc99277010)

[NAT: 23](#_Toc99277011)

[EIGRP: 24](#_Toc99277012)

[IPSec: 25](#_Toc99277013)

[SSH: 26](#_Toc99277014)

[Port Security: 26](#_Toc99277015)

[DHCP Snooping: 27](#_Toc99277016)

[VTP(Vlan Trunk Protocol): 27](#_Toc99277017)

[Jelszó titkosítás: 27](#_Toc99277018)

[Narancssárga terület: adatközpont 28](#_Toc99277019)

[Multilink: 29](#_Toc99277020)

[WAN(Wide Area Network): 29](#_Toc99277021)

[Link Aggregation: 30](#_Toc99277022)

[Szerverek: 30](#_Toc99277023)

[DNS: 30](#_Toc99277024)

[sFTP: 30](#_Toc99277025)

[TFTP: 30](#_Toc99277026)

[SYSLOG-NTP: 30](#_Toc99277027)

[MAIL: 31](#_Toc99277028)

[WEB: 31](#_Toc99277029)

[Kék telephely: Bank 32](#_Toc99277030)

[Tűzfal: 33](#_Toc99277031)

[Object network: 33](#_Toc99277032)

[Policy-map: 33](#_Toc99277033)

[Class-map: 33](#_Toc99277034)

[Service-policy: 33](#_Toc99277035)

[NAT: 33](#_Toc99277036)

[ACL: 33](#_Toc99277037)

[Ip route: 33](#_Toc99277038)

[DHCP: 33](#_Toc99277039)

[Hivatkozások: 34](#_Toc99277040)

# Cégleírás

Cégünk egy MNB által felügyelt befektetési vállalat, az alkalmazottjaink a tőzsdén való kereskedéssel próbálják gyarapítani a befektető kliensek vagyonát. Mivel több tíz akár százmilliós összegekről van szó, elengedhetetlen, hogy folytonos, biztonságos hálózati hozzáférés legyen biztosítva a nálunk dolgozó kereskedőknek, mindazonáltal, hogy minden tranzakció valós időben történik az interneten, így akár pár perc leállás a rendszerben valakinek a befektetett vagyonát megfelezheti. Tudniillik a cégünk több száz ügyfél felettébb bizalmas adatait kezeli, tárolja, ezért meg kell akadályoznunk minden adatszivárgási lehetőséget. Ennek érdekében a hálózatban semmi olyan apró rés nem keletkezhet, ami bármely fenyegetésnek kiteheti ezeket. A cél eléréshez fizikai és virtuális korlátozásokat kellett használnunk egyidejűleg. Az informatikai részleg azt a feladatot kapta, hogy építse ki a cég új hálózati és üzemeltetési infrastruktúráját a Magyar Nemzeti Bank elvárásainak megfelelve.

# South Brokers Zrt. szerverkörnyezetének dokumentációja

A cég hálózatának tervezése közben minden olyan kritériummal számolnunk kellett, ami hibát, vagy leállást okozhat a rendszerben, hogy akár a véletlen tragédiaszerű, vagy megtervezett rosszindulatú események során is akadálymentesen folytatódhasson a kereskedelem. Ilyennek számít egy szolgáltatói leállás, vezeték meghibásodás, vagy akár belső rossz szándékú cselekmény. Ezek elkerülésének érdekében az elsődleges szervereink egy bérelt adatközpontban helyezkednek el, itt folytonos megfigyelés alatt áll őrök és nagy felbontású kamerák által, és monitorozva van minden hálózati forgalom. Itt az esedékes áramszüneteknél is biztosítva van az energiahálózat, szünetmentes áramellátással és tartalék aggregátorokkal, ezen kívül még számos kisebb terrorcselekmény ellen is védve van az épület. Mind ezek ellenére, az adaközpont meghibásodásának lehetősége nincs kizárva, ezért a cégünk saját telephelyén is kialakítottunk egy másodlagos szerverszobát, ami azonnal átvenné az összes üzemeltetési szerepkört a főszerverek esetleges meghibásodásánál. A két telep folytonos szinkronizációt végez el egymás között, hogy minimálisra csökkenjen az adatvesztés lehetősége. Esetleges áramszünet miatt a saját telepünk is szünetmentes tápegységekkel vannak ellátva, illetve beszereltünk egy saját dízel aggregátort is, ami az épület minden esszenciális létesítményét el tudja látni árammal. A szerverszobába történő belépés csak és kizárólag a hozzá jogosultak ujjlenyomatos azonosítása után történhet meg illetve papírformában is dokumentáljuk a belépő személyek nevét, személyi számát, bent tartózkodás időtartalmát és okát.

## Szolgáltatások:

Az adatközpotban található egy Windows és egy Linux operációs rendszerű főszerver, melyből a Windows szerver a következő szolgáltatásokat üzemelteti: sFTP, TFTP, NTP, Syslog, MAIL, IIS, FILE. A Linux szerver következő szolgáltatásokat üzemelteti: AD, DNS, DHCP. A telephelyünkön lévő másodlagos szervereink képesek átvenni a teljes üzemeltetést egy Linux SDC, DHCP Failover, MAIL szerver és egy folytonosan szinkronizálódó Windows szerver segítségével. A szolgáltatások bővebb kifejtésére lentebb kerül sor.

# A cég felépítése:

Cégünknek jelenleg 50 alkalmazottja van, akiket külön logikai csoportokba\* rendeztünk a HR-es kollegánk megbízásából.

ad

## South Brokers

* Ügyvezető igazgató (1 fő)
* Pénzügy (4 fő)
* Marketing (2 fő)
* HR (2 fő)
* Bróker
  + Bróker főnök (1 fő)
  + Junior (22 fő)
  + Senior (4 fő)
* IT
  + IT főnök (1 fő)
  + Szerver kezelő (2 fő)
  + Rendszergazdák (3 fő)
  + Gazdasági informatikus (2 fő)
  + Help Desk (4 fő)
* FTP felhasználók (2 fő)

# Szolgáltatások részletezése

(Ez a resz át lesz írva / fogalmazva csak meg nem tudtuk mit írjunk ide, es benne lesz hogy használj a cég)

## sFTP:

<ide ftp kep>

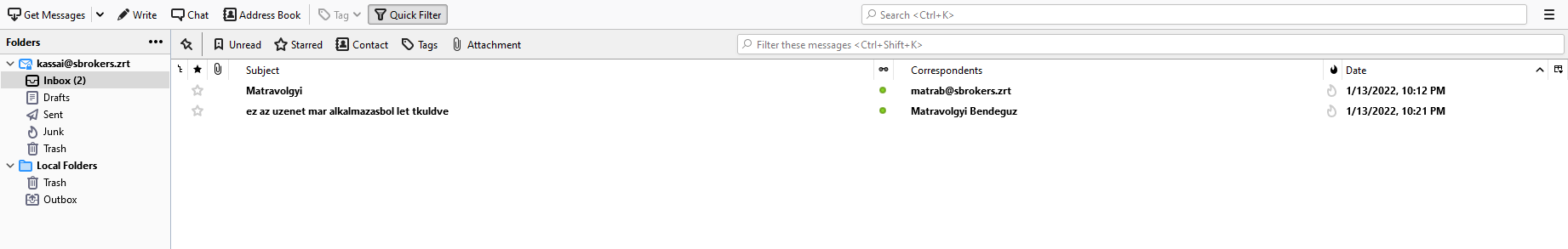
Az FTP (File Transfer Protocol), vagy más néven Fájlátviteli protokoll egy népszerű módszer két távoli rendszer közötti fájlátvitelhez. Az SFTP (SSH File Transfer Protocol vagy Secure File Transfer Protocol), vagy más néven Biztonságos fájlátviteli protokoll egy különálló protokoll SSH-val, ami hasonlóan működik, de biztonságos kapcsolaton keresztül. Előnye, hogy képes megnövelni a biztonságot és bejárni a fájlrendszert mind a helyi, mind a távoli rendszerben. Az SFTP majdnem minden esetben jobban kedvelt az FTP-nél, mert biztonságosabb, ráadásul SSH kapcsolattal képes más felhasználó kapcsolatán keresztül belépni. Az FTP egy olyan nem biztonságos protokoll, amelyet csak meghatározott esetekben használunk, vagy akkor, hogyha teljesen biztosak vagyunk benne, hogy megbízunk az adott hálózatban. Habár az SFTP nagyon sok grafikus eszközbe be van integrálva, ez a leírás bemutatja, hogy hogyan is használhatjuk az interaktív parancssoros kezelőfelületét.

## IIS:

<kep a https tanusitvanyrol url rewrite>

Az Internet Information Services (IIS, korábban Internet Information Server) a Microsoft által a Windows NT operációs rendszercsaládhoz készített bővíthető webszerver. Az IIS támogatja a HTTP, HTTPS, FTP, FTPS, SMTP és NNTP protokollokat. A Windows NT 4.0 óta a Windows NT alapú operációs rendszerek szerves részét képezi néhány kivételtől eltekintve Az IIS alapértelmezésben nincsen bekapcsolva a rendszereken. Az IIS Managert a Microsoft Management Console-on vagy a Vezérlőpultban, az Adminisztrációs eszközökön keresztül lehet elérni.

## Email (IRedMail)

Az iRedMail\* az ingyenes és nyílt forráskódú szolgáltatómail szerver megoldás. Az iRedMail egyszerűen tökéletes platform saját levelező szerver felépítéséhez a nyílt forráskódú eszközök segítségével. Az iRedMail könnyen működhet szinte minden UNIX alapú operációs rendszerben. Az iRedMail használatával egyszerűen teljeskörű, nyílt forráskódú és teljes funkcionalitású levelező szervert telepíthet néhány perc alatt, mindezt ingyen. Az iRedMail a nyílt forráskódú összetevők összegyűjtésével, majd a legjobb gyakorlat alkalmazásával végezte el. Eszközei jól teljesítik a felhasználók főbb feladatait. Az iRedMail egyik legjobb tulajdonsága, hogy professzionális támogatást kínál bizonyos problémák esetén. Az iRedMail használatának néhány előnye a magánélet, a nyílt forráskódú, alapértelmezés szerint biztonságos, a webmail, a naptárak, a kapcsolattartók elérhetősége, az ActiveSync, a korlátlan fiókok elérhetősége, támogatja a mainstream UNIX alapú operációs rendszereket, a háttérprogramokat, a víruskereső és a spam elleni védelmet, a webes adminisztrációs panelt, reprodukálható bevezetése és a professzionális technikai támogatás rendelkezésre állása. Miután elkezdte használni az iRedMail alkalmazást, rájön, hogy stabil és rugalmas terméket használ. Az iRedMail folyamatosan felülmúlja ügyfele elvárásait, és a maximális szintig kínálja a szakmai támogatást. Igazán meg fog elégedni az iRedMail rendszerével és munkájával.

mail

## Syslog:

A „Syslog szerver”Valóban utal egy alkalmazás, amely foglalkozik a syslog üzenetekkel nem pedig egy dedikált számítógép biztosítása az üzenetek fogadására. Tehát ne tévesszen oda, hogy ott a „szerver” szó.

A szerver / kliens modellt kissé nehéz megérteni Syslog szempontból is. Általában az ügyfél kapcsolatba lép a kiszolgálóval, és a kiszolgáló válaszol. A syslog-ban, A syslog kliens csak egy program, amely hibaüzeneteket, figyelmeztetéseket és hibakeresési üzeneteket továbbít. A syslog kliensnek nincs közvetlen kapcsolata a másikkal: küldi az üzeneteket, függetlenül attól, hogy valaki hallgatja-e őket. A Syslogd démon. Ez egy Syslog gyűjtő, így kiszolgálónak tekintik, annak ellenére, hogy soha nem válaszol az üzenetek kezdeményezőjére. Lehet, hogy a démon helyileg fut, vagy távoli syslog szerverként is megvalósítható az interneten keresztüli kapcsolódással.

## TFTP:

Az FTP-hez hasonlóan a TFTP ügyfél- és kiszolgálószoftvert is használ a két eszköz közötti kapcsolat létrehozására. Egy TFTP kliensből az egyes fájlok másolhatók (feltöltve), vagy letölhetők a kiszolgálóról. Más szóval, a szerver a fájlokat tárolja, amíg az ügyfél kéri vagy elküldi azokat. A TFTP-t a számítógép távoli elindításához és hálózati vagy útválasztó konfigurációs fájlok biztonsági mentéséhez is használhatja. A TFTP UDP-re támaszkodik az adatok szállítására.

## AD:

Az Active Directory\* egy címtárszolgáltatás vagy tároló, amely adatobjektumokat tárol a helyi hálózati környezetben. A szolgáltatás az adatokat rögzíti felhasználók, készülékek, alkalmazások, csoportok, és készülékek hierarchikus struktúrában. Az adatok felépítése lehetővé teszi, hogy egy helyről megtalálják a hálózathoz csatlakoztatott erőforrások részleteit. Alapvetően az Active Directory úgy működik, mint egy telefonkönyv a hálózat számára, így könnyedén megkeresheti és kezelheti az eszközöket.

ad

## DC:

Microsoft Windows környezetben a tartományvezérlő (domain controller, DC) olyan szerver, ami a Windows tartományon belül autentikációs és autorizációs szolgáltatásokat nyújt.

Windows NT tartományokban minden tartományban kellett lennie egy elsődleges tartományvezérlőnek (Primary Domain Controller, PDC); az összes többi tartományvezérlő csak tartalék lehetett (Backup Domain Controller, BDC). A BDC képes a felhasználók autentikálására, de a tartomány változásait (új felhasználók, jelszóváltozások, csoporttagság-változások) csak a PDC-n keresztül lehet rögzíteni, ahonnan azután ezek a változások továbbterjednek a tartomány összes BDC-jére. Ha a PDC éppen elérhetetlen volt a változás ideje alatt, a változtatást nem lehet végrehajtani. Ha egy PDC végleg elérhetetlenné válik (például a hardver tönkremegy), egy létező BDC-t kell előléptetni PDC-nek. A PDC kritikus hibalehetőség-jellege miatt a bevált gyakorlat szerint a PDC-t kizárólag bejelentkeztetésre célszerű használni, fájl-, nyomtató- és alkalmazáskiszolgálóként nem, mert ezek a szolgáltatások lelassíthatják, esetleg lefagyaszthatják a rendszert. Egyes rendszergazdák ennél továbbmenve egy dedikált BDC-t is rendszerbe állítanak kizárólag arra a célra, hogy a PDC kiesése esetén PDC-vé lehessen előléptetni.

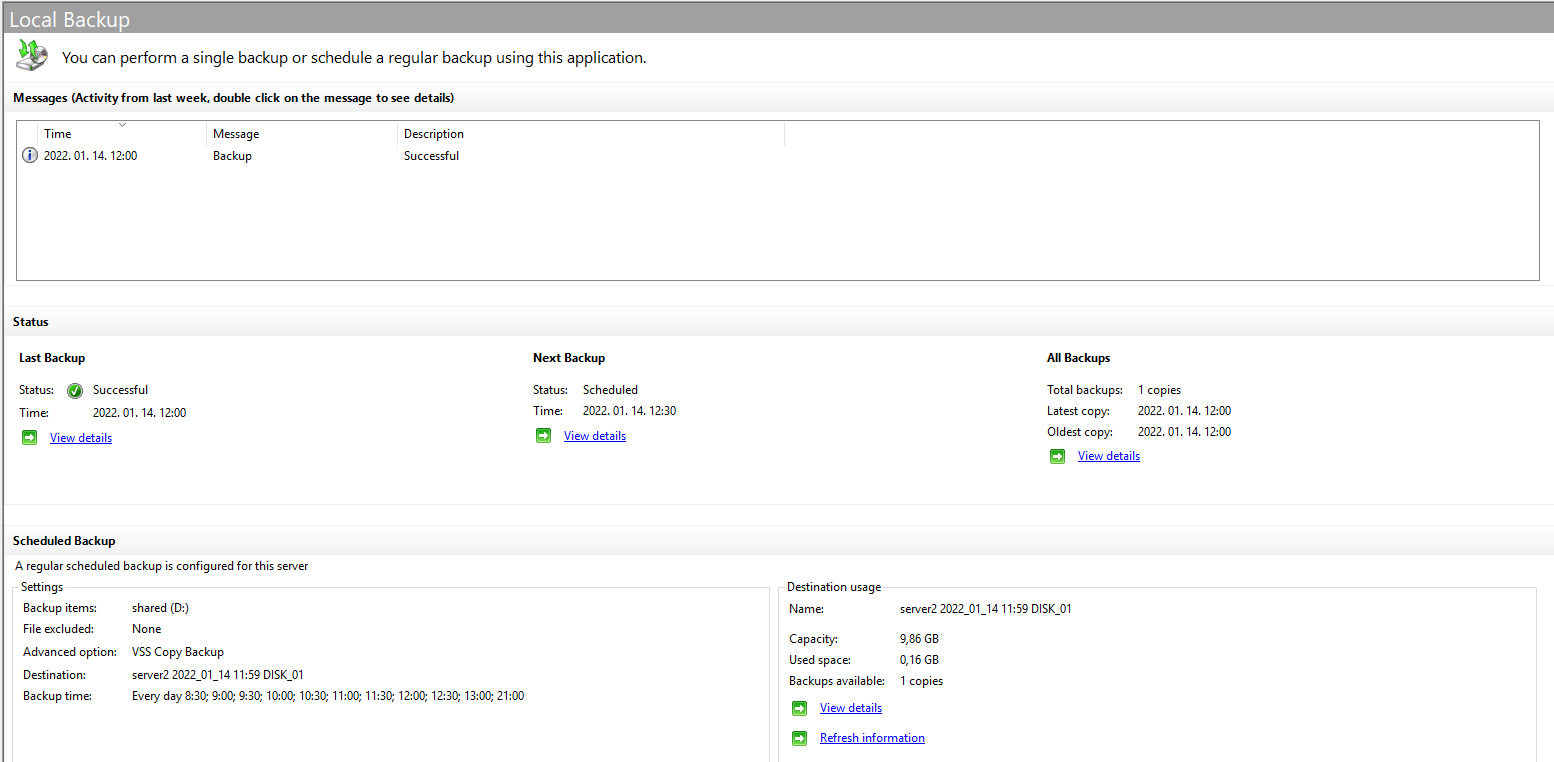
A Windows 2000-től bevezetett Active Directoryval („AD”) nagyrészt megszűnt az elsődleges és tartalék tartományvezérlők megkülönböztetése a multi-master replikáció bevezetésével. Így is megmaradt néhány szerepkör, amit csak 1-1 tartományvezérlő képes betölteni, ezeket műveleti kiszolgálóknak nevezik (egyes szerepkörökből tartományonként, másokból erdőnként egy létezhet. Ha egy műveleti főkiszolgáló kiesik, egy másik tartományvezérlő veheti át funkcióját (szabályos vagy „erőltetett” átadással).

## RODC:

A Windows Server 2008-ban bevezették az írásvédett/csak olvasható tartományvezérlő (Read-Only Domain Controller, RODC) üzemmódot a kevésbé biztonságos telephelyek számára. Ennek kapcsán a „hagyományosan” működő tartományvezérlőket, az RODC-ktől való megkülönböztetés miatt írható tartományvezérlőnek (writable domain controller) is nevezik.

## File:

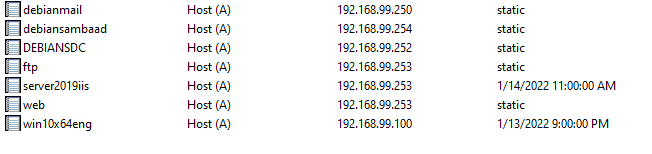
Samba kiszolgáló a legelterjedtebb vállalati megoldás, mert gyorsasága verhetetlen  
A vállalati helyi hálózat számítógépéit (munkaállomásait) egy vagy több fájlszerver szolgálja ki. Ezek biztosítják részükre a munkájukhoz szükséges közös adatállományokat, megosztásokat.  
A központosított adattárolásnak számtalan előnye van, minél nagyobb a hálózat, ez annál jobban érezhető. Néhány számítógép még szerver nélkül is használható, de, közös adatállományokat, megosztásokat igen nehézkes kialakítani, több számítógép felett már gyakorlatilag nélkülözhetetlen. A file szerverek segítségével menthetőek\* az adatok, biztosítható a dokumentumok védelme és kontrollt gyakorolhat a hozzáférési jogosultságokon is. Ezáltal növelhető a biztonság, hogy legközelebb ne a konkurenciánál találkozz a tőled elveszett információkkal



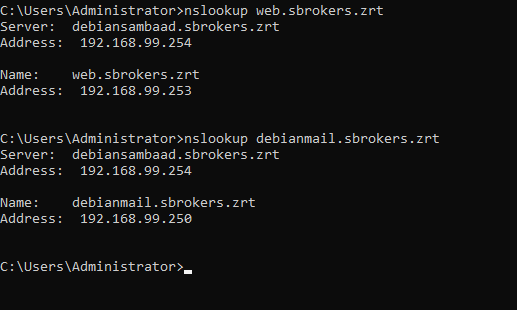
file megosztas

auto mentes

## DNS:

A Domain Name System (DNS), azaz a tartománynévrendszer egy hierarchikus, nagymértékben elosztott elnevezési rendszer számítógépek, szolgáltatások, illetve az internetre vagy egy magánhálózatra kötött bármilyen erőforrás számára. A részt vevő entitások számára kiosztott tartománynevekhez (doménekhez) különböző információkat társít. Legfontosabb funkciójaként az emberek számára értelmes tartományneveket a hálózati eszközök számára érthető numerikus azonosítókká „fordítja le”, „oldja fel”, melyek segítségével ezeket az eszközöket meg lehet találni, meg lehet címezni a hálózaton.  
Gyakran használt analógia a tartománynévrendszer magyarázatához, hogy az internet egyfajta telefonkönyve, amiből ki lehet keresni az emberek számára értelmezhető számítógép-állomásnevekhez tartozó IP-címeket. Például a www.example.com tartománynévhez a 192.0.32.10 (IPv4) és a 2620:0:2d0:200::10 (IPv6) címek tartoznak.  
A DNS lehetővé teszi internetes erőforrások csoportjaihoz nevek hozzárendelését olyan módon, hogy az ne függjön az erőforrások fizikai helyétől. Így a világhálós (WWW) hiperlinkek, internetes kapcsolattartási adatok konzisztensek és állandóak maradhatnak akkor is, ha az internet útválasztási rendszerében változás történik, vagy a részt vevő mobileszközt használ. Az internetes tartománynevek további célja az egyszerűsítés, egy doménnevet (pl. www.example.com) sokkal könnyebb megjegyezni, mint egy IP-címet, mint 208.77.188.166\* (IPv4) vagy 2001:db8:1f70::999:de8:7648:6e8 (IPv6). A felhasználók így megjegyezhetik a számukra jelentést hordozó web- (URL\*) és e-mail-címeket, anélkül, hogy tudnák, a számítógép valójában hogyan éri el ezeket.

look-up zone



nslookup

.

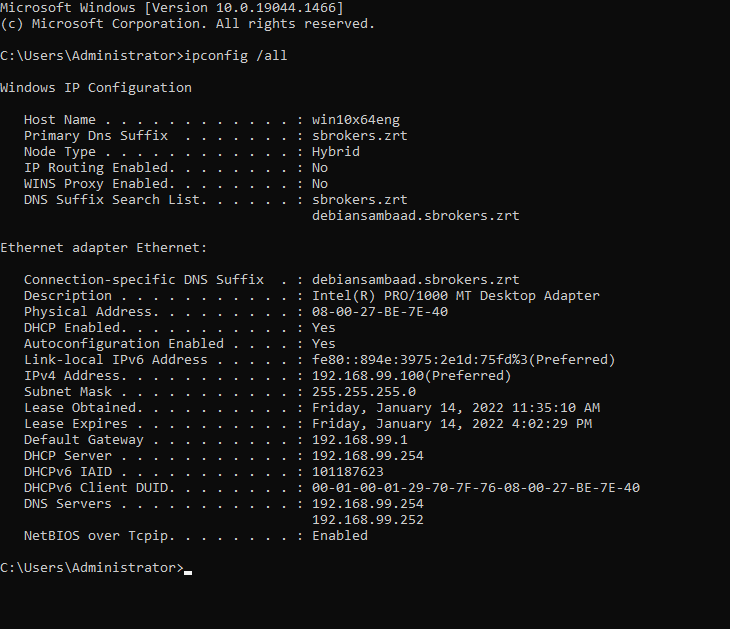
## DHCP:

Ez a protokoll azt oldja meg, hogy a TCP/IP hálózatra csatlakozó hálózati végpontok (például számítógépek) automatikusan megkapják a hálózat használatához szükséges beállításokat. Ilyen szokott lenni például az IP-cím, hálózati maszk, alapértelmezett átjáró stb.

A DHCP szerver-kliens alapú protokoll, nagy vonalakban a kliensek által küldött DHCP-kérésekből, és a szerver által adott DHCP-válaszokból áll\*.

A DHCP-vel dinamikusan oszthatóak ki IP-címek, tehát a hálózatról lecsatlakozó számítógépek IP-címeit megkapják a hálózatra felcsatlakozó számítógépek, ezért hatékonyabban használhatóak ki a szűkebb címtartományok

DHCP Failover: dhcp csak ha elbaszodik az elso akk ez lesz a kiszolgalo (átfogalmazás alatt)



ipconfig /all

A képen szöveg látható

Automatikusan generált leírás

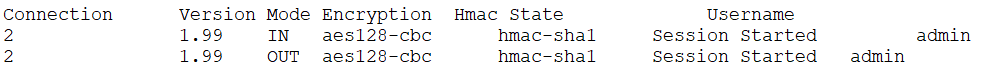
A képen szöveg látható

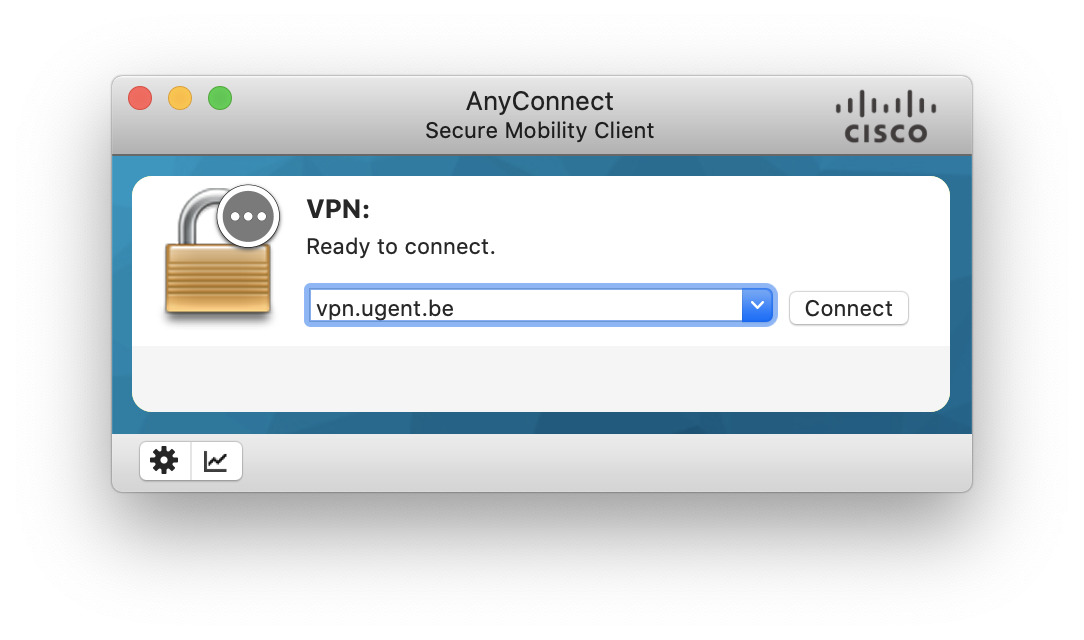
Automatikusan generált leírás

A képen szöveg látható

Automatikusan generált leírás

A képen asztal látható

Automatikusan generált leírás





A képen szöveg látható

Automatikusan generált leírás

# Költségvetés

Cisco 2911 Router (5db)

Ár: 3550$ /db

Cisco 2960 Switch (5db)

Ár: 2650$ /db

Cisco ASA (2db)

Ár: 6500$ /db

Cisco SOHO Router (1db)

Ár: 330$ /db

Cisco UCSB-5108-AC2 Server (6db)

Ár: 7000$ /db

Számitógép (11db)

Ár: 800$ /db

Cisco-Linksys WPSM54G Vezeték nélküli Nyomtató (2db)

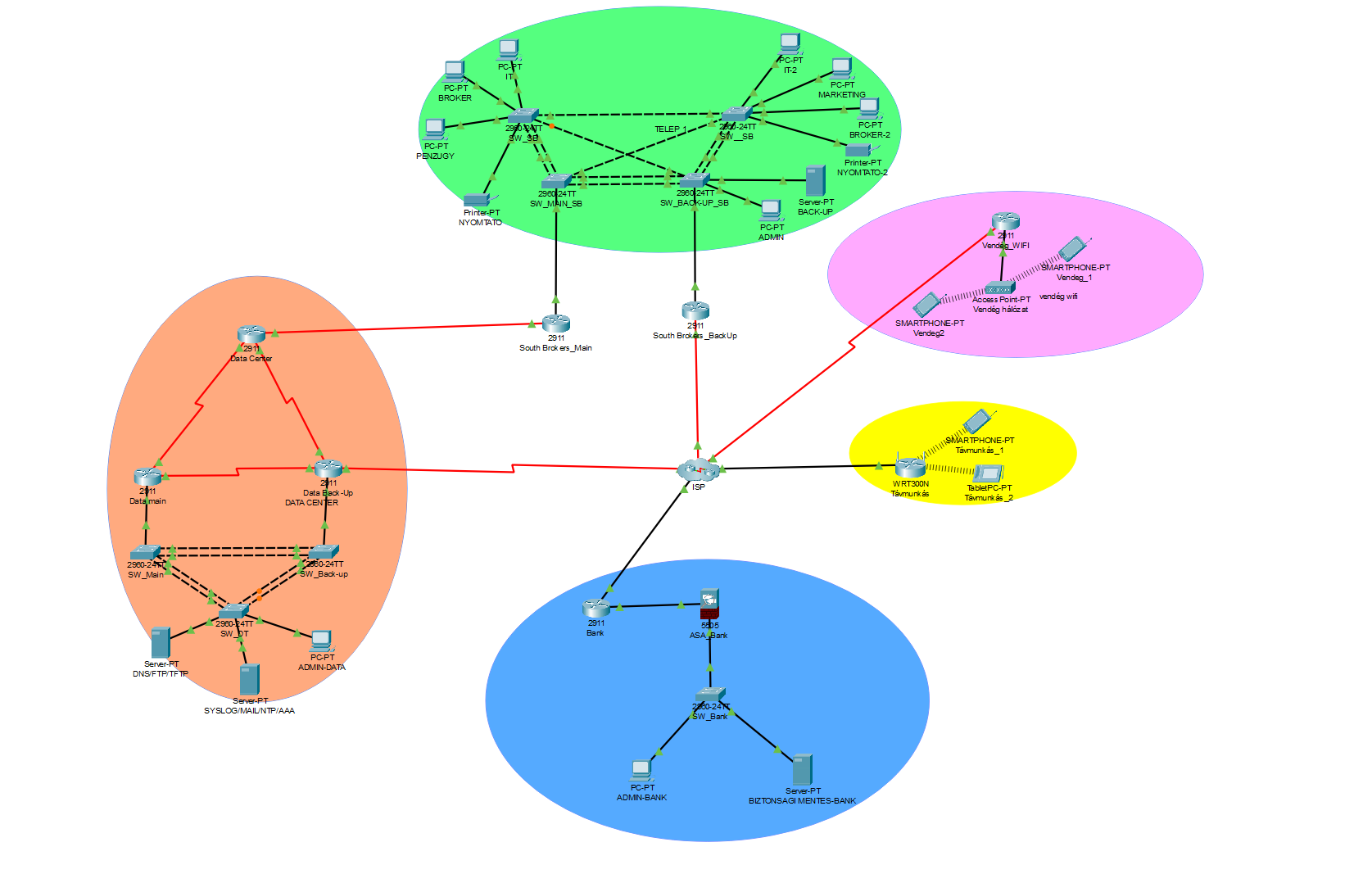
Ár: 5000$ /db

Összese: 105,130$

**A cég belső hálózatát kívülről csak és kizárólag céges laptopokról és a Cisco AnyConnect VPN használatával lehet elérni, ami össze van kötve egy mobiltelefonos kétfaktoros hitelesítési rendszerrel. Ez önmagában kizárja azt a lehetőséget, hogy egy illetéktelen egy megfelelő felhasználónév és jelszó párosával beléphessen a belső hálózatunkba. A fő domain szervezeti egységei és felhasználói erősen korlátozott jogkörrel rendelkeznek, hogy ne tudjanak hozzáférni, vagy módosítani olyan fájlokat, amik az ügyfelek adatainak védelmét veszélyezteti. A céges számítógépeken minden idegen eredetű eszköz és alkalmazás futtatása le van tiltva. Minden olyan hozzáférési pont ami külső, vagy szolgáltatói hálózathoz csatlakozik egy nagy teljesítményű Cisco ASA tűzfallal van védve, ezzel fizikailag is megakadályozva a támadásokat. A vezeték nélüli vonalak fokozott sebezhetősége miatt a Wi-Fi hálózatunk nincs közvetlen összeköttetésbe a belső hálózattal..**

# A hálózat tesztelésének dokumentációja

A prototípus topológiájának felépítéséhez a Cisco Packet Tracer és GNS3 virtualizációs alkalmazásokat használtuk. A következő képen látható a teljes hálózat.



A zöld terület a cégünk budapesti telephelye, a rózsaszín az itt megtalálható vezeték nélküli vendég hálózat, a narancssárga egy bérelt adatközpont szerepét tölti be, a kék rész a Magyar Nemzeti Bank adattároló egysége, illetve a sárga terület a cég távolról dolgozó kollegáit reprezentálja.

## Zöld terület: Fő telephely:

Ez a South Brokers Zrt. fő irodája, ahol 60 alkalmazottunk dolgozik. Az internet és az adatközpontban lévő saját szervereink elérése érdekében zökkenőmentes kapcsolatot kellett kialakítanunk.

A Cisco Packet Tracerben a következő eszközöket használtuk ezen a területen:

* 2db Cisco 2911 forgalomirányító
* 4db Cisco 2960 kapcsoló
* Nyomtatók
* Számítógépek
* 1db tartalék szerver

A területen a következő protokollokat használtuk:

* Harmadik rétegbeli redundáns megoldás:
  + HSRP
    - A fő router (South Brokers\_Main) esetleges meghibásodása esetén a South Brokers\_BackUp forgalomirányító veszi át az irányítási szerepköröket.
* Második rétegbeli redundáns megoldások:
  + STP
    - Hurkok és szórási viharok elkerülése érdekében
  + Link Aggregation
    - Port összefogás
    - Nagyobb sávszélesség

Forgalomirányítók:

* ACL
  + Csak az admin tudja pingelni a szervert
  + Csak az admin éri el SSH-val a kapcsolókat és forgalomirányítókat.
* PAT
  + A belső címeket a kimenő interfész címére fordítja kilépéskor.
* EIGRP
  + Dinamikus forgalomirányítás a VLAN-ok és a telephelyek között.
* IPsec
  + Titkosított, biztonságos kapcsolat az iroda és az adatközpont között.
* SSH
  + Titkosított távoli hozzáférést biztosít az adminnak

Kapcsolók:

* Port security
  + Az interfészek maximum 1 Mac címet tanulnak meg, ismeretlen cím esetén lekapcsolnak.
* DHCP Snooping
  + Csak az ismert interfészeknek oszt címet DHCP-vel
* Vlan Trunk Protocol
  + Cisco protokoll: kapcsolók közötti Vlan információ csere
* Jelszó titkosítás
  + Service password-encryption
  + Secret jelszavak használata
* SSH
  + Titkosított távoli hozzáférést biztosít az adminnak

### HSRP:

A HSRP (Hot Standby Router Protocol) működése nagyon egyszerű. A protokoll egy virtuális IP címet kínál fel a LAN hálózatunk számára (természetesen a LAN alhálózatunkból) alapértelmezett átjáróként. Ez a virtuális IP címet fogjuk alapértelmezett átjáróként beállítani a LAN állomásain. A virtuális IP címen több forgalomirányító is osztozik, egymás között megbeszélve, hogy melyikük fogja az alapértelmezett átjáró feladatát ellátni, vagyis a tényleges adatforgalmat közvetíteni. (A virtuális IP cím mellé egy virtuális MAC címet is rendel a HSRP. (Admin, 2021.02.09)

Beállítása nagyon egyezrű. Előszőr belépünk a kiválasztott interfész-be majd kiadjuk a Standby <szám> ip <ip cím> parancsot. Utána megadjuk a priorítás értékét a standby <szám> prioirty 105 paranccsal. A kiadott pioritás szám miatt biztosan ő lesz az active router.

<kep>

Elengedhetetlen beállítás a track parancs hiszen így a router figyeli az interfészt és egy esetleges meghibásodás során 10el csokkenti a prioriítás értéket így a standby üzemmódban lévő router veszi át a forgalomirányítást. Utolsó bealláítás a preempt ami mindig a legmagasabb értékű prioirty-vel rendelkező routert nevezi ki activnak.

<kep>

Természetesen, az összes VLAN-ra be lett állítva így teljes a harmadik rétegbeli redundancia. A virtuális ip címek minden hálózat 2. kiosztható ip címét kapták meg.

### Feszitőfa( Spanning Tree Protocol)

A 2. rétegben kezelt keretek fejlécében nem találunk olyan mezőt, amely ellátná azt a feladatot, amelyért a 3. rétegben az IP protokoll time-to-live mezője felelős, vagyis annak detektálása, hogy az adott PDU hurokba kerül. Ilyen hurkok akkor alakulnak ki, ha alternatív útvonalak is rendelkezésre állnak a hálózatban két eszköz között. Mivel a 2. rétegben a kapcsolók üzenetszórás vagy elárasztás esetén minden portjukon (kivéve ahol bejött) kiküldik keretet, üzenetszórási vihart, instabil MAC-cím táblát és duplikáltan megkapott kereteket kapunk eredményül. Ennek következtében a hálózatunk drasztikusan belassul és használhatatlanná válik. Ez ellen véd minket az STP protokoll. (Admin, 2021.02.05)

Ahoz, hogy jól és stablian működjön a HSRP be kellet állítani bizonyos dolgokat. Az első dolog volt, hogy beálítottuk a Rapid-PVST-t ami gyorsan konvergál és használja a PVST+ funkciókat. Ezt a spanning-tree mode rapid-pvst parancsal tudjuk aktiválni. Figyelembe kellet venni, hogy nagy az erőforrás igénye így minőségi kapcsolókat használtunk.

<kep>

A következő beállítás a fő és másodlagos kapcsolók kinevezése. Ez a lépés nem kötelező, de ajánlott. Beállítás után a csomagok a legrövidebb úton fognak haladni az elsődleges kapcsolóhoz, ha az esetleg meghibásodik akkor a csomagok az előre beállított másodlagos kapcsoló felé veszik az irányt. Cégünknél az elsődleges kapcsoló az SW\_MAIN\_SB lett ahol a 80,105,120,155,205 vlanok lettek bellítva míg az SW\_BACK-UP\_SB-nél a 99-es vlan ami egyben az ADMIN vlan is. Ezzel a parancsal tudjuk aktiválni a szeperköröket: spanning-tree vlan <szam> root primary/secondary

<kep>

Cégünknél a védelem a legfontosabb így védekezünk a BPDU támadások ellen. Minden végeszközön beállítottuk a spanning-tree bpduguard enable paranccsal hiszen ezeknek a keretknek nagy szerepe van az elsődleges kapcsoló választásában így megakadályozzuk, hogy egy külső személy beavatkozzon a választásba és olyan információkat tudjon meg ami nem juthatna el hozzá. Így az adott portokon a kapcsoló nem fogad el BPDU kereteket.

Másik fontos beállítás a Portfast amit szintén a végeszközökön állítunk be így felgyorsítjuk a konvergenciát és a beállított portok automatikusan forwarding állapotban lesznek. Miután beléptünk egy interfész-be adjuk ki a következő parancsot, hogy aktiváljuk a PortFastot: spanning-tree portfast.

<kep>

### Link Aggregation:

Link Aggregation másnéven port összefogás megoldja, hogy a kapcsolók több fizika kábelt virtuálisan összekössünk, így növeli a sávszélességet anélkül, hogy drága gigibit vagy akár optikai kábelt kéne venni. Másik hasznos funkciója, hogyha egyik kábel megsérülne attól még a hálózat jól fog működni.

Cégünknél nem csak cisco kapcsoló található ezért LACP-t használtunk, ami más gyártó által forgalmazott kapcsolóval is jól együtt tud működni. Konfigurálása nagyon egyszerű először létre kell hozni egy „port-channelt” az interface port-channel <szam> paranccsal. Ezután megadhatjuk, a natív vlan vonalat vagy akár, hogy az adott port trunk módba legyen-e. Következő lépésként több interfészbe kell belépni amit lekapcsolunk majd kiadjuk a channel-group <szam> mode <active/passive/desitable/on> parancsot. Az utolsó paraméter attól függ, hogy milyen portokolt használunk, PAGP-T vagy LACP-T. Előbbinél az „active” mód javaslott cégünk is így állította be.

<kep>

### ACL:

A hozzáférési jogosultság ellenőrzése (access control) valamilyen védett objektum, számítógép vagy számítógép-hálózat biztonságát szolgáló különböző védelmi eljárások összessége. Az informatikában a hozzáférési jogosultság feladata a számítógép erőforrásainak vagy magának a számítógépes hálózatnak a védelme illetéktelen felhasználástól. A hozzáférési jogosultság dönti el, hogy egy személynek, vagy egy a számítógépen futó eljárásnak (process) van-e lehetősége valamilyen objektum elérésére. Ez lehet egy fájl vagy valamilyen hardver eszköz stb. (Atobot, 2018)

A fő telephelyünkön több ACL is védi a hálózatot. Egyaránt használunk szabványos és kiterjesztett ACL-t is. Konfigurálása kis logikai gondolkodást igényel hiszen föntről lefele fut le, ha az elején letiltottunk mindent akkor hiába alítottuk be, hogy valamit engedélyezzen.

Csak az „admin” tudja pingelni a DataCenter szervereit a dolgozók csak elérik a web,ftp,tftp szolgáltatásokat.

<kep>

Fontosnak tartjuk a távoli konfigurálásának lehetőségét ezért minden kapcsolónkra egy azonos acl került fel ami csak az admin gépnek engedélyezi az ssh-t.

<kep>

### NAT:

A hálózati címfordítás (angolul Network Address Translation) a címfordításra képes hálózati eszközök (pl. router) kiegészítő szolgáltatása, mely lehetővé teszi a belső hálózatra kötött gépek közvetlen kommunikációját tetszőleges protokollokon keresztül külső gépekkel anélkül, hogy azoknak saját nyilvános IP-címmel kellene rendelkezniük. A hálózati címfordító a belső gépekről érkező csomagokat az internetre továbbítás előtt úgy módosítja, hogy azok feladójaként saját magát tünteti fel, így az azokra érkező válaszcsomagok is hozzá kerülnek majd továbbításra, amiket – a célállomás címének módosítása után – a belső hálózaton elhelyezkedő eredeti feladó részére ad át. (InternetArchiveBot 2022)

A South Brokers telephelyünkön a South Brokers\_Backup forgalomirányítónk végez PAT-ot, ami túlterheléses NAT. Ez azt jelenti, hogy először létre kell hozni egy ACL listát, ahol megadjuk az engedélyezett hálózatot.

<kep>

Ezután a ip nat inside source list <acl szamunk> interface <kimenő interfész> overload parancsot adjuk ki.

<kep>

Utolsó lépsként belépünk a belső hálózatba irányuló interfészbe és kiadjunk az ip nat inside míg a külső interfészbe az ip nat outside parancsot. Így már kész is vagyunk és minden egyes belső címet lefordít a külsőn lévő címre ha a csomag elhagyja a hálózatot.

<kep>

### EIGRP:

Cisco által fejlesztett, távolság vektor alapú, osztály nélküli dinamikus forgalomirányítást végző protokoll, ami saját szállítási protokollt használ, ami az RTP. Előnye, hogy hurok mentes útvonalakat biztosít, amit a DUAL algoritmus segítségével számol ki emiatt nem szórja tele hello csomaggal a hálózatot.

|  |  |
| --- | --- |
| CSOMAGJAI: | TÁBLÁI: |
| Hello | Szomszédsági |
| Frissítő | Topológiai |
| Nyugta | Forgalomirányító |
| Lekérdező |  |
| Válasz |  |

Összes telephelyen EIGRP van hiszen terhelésmegosztás szempontból sokkal jobb, mint az OSPF. Process ID-nak a 4-et választottuk az auto summary funkciót kikapcsoltuk hiszen használunk VLSM-t, az összes interfészt, ami kapcsolóba megy beállítottunk passsive módba, hogy ne terhelje a hálózatot.

<kep>

Természetesen hitelesítve vannak az útvonalak ezért létre hoztunk egy key chain-t Sbrokers néven, amihez hozzá rendeltünk egy key-t és végül megadtuk a jelszót, ami Sbrokers1234.

<kep>

Ezután belépünk egy interfészbe, ahol hozzá rendeljuk a key-chain-t majd md5-tel titkosítjuk a csomagokat. Eheze két parancs szükéseges az első, ip authentication mode eigrp <eigrp process id szam> md5 majd az ip authentication key-chain eigrp <eigrp process id szam> <key chain>

<kep>

### IPSec:

Az **Internet Protocol Security** (**IPsec**) egy protokoll csomag az Internet Protokoll (IP) alapú kommunikáció biztonságosabbá tételére a kommunikációs viszony minden egyes csomagja hitelesítésével és titkosításával. (InternetArchiveBot, 2021)

Cégünknél nagyon sok kényes adat van ezért elengedhetetlen volt, hogy a fő telephelyünk és a Data Center között titkosított átjárónk legyen. A legkorszerűbb titkosítási és hitelesítési technológiát használtuk.

Ezért az IPsec protokollunk ESP+AH ami azt jelenti, hogy előszőr titkosít utána hitelesít. Megbizonyosodik arról, hogy minden csomag egyedi és semmi se lett módosítva. Miután létre jött a kapcsolat, egy számláló elindul és minden egyes küldött csomagnál az értéke megnő így biztosan tudja milyen számozású csomagot kell kapjon.

Titkosításnál AES 256-ot választottuk, Integritásnál pedig SHA hiszen biztonságosabb, mint az MD5, hitelesítésnél „pre-shared” hiszen egyszerű fel konfigurálni kis környezetbe és csak az adminnak kell tudnia kommunikálni a DataCenterrel. Utolsó dolog a DIiffie-Hellman, aminél 5ös csoportot állítottunk be.

<kép>

### SSH:

A Secure Shell (röviden: SSH) egy szabványcsalád, és egyben egy protokoll is, amit egy helyi és egy távoli számítógép közötti biztonságos csatorna kiépítésére fejlesztettek ki. Nyilvános kulcsú titkosítást használ a távoli számítógép hitelesítésére, és opcionálisan a távoli számítógép is hitelesítheti a felhasználót. (InternetArchiveBot, 2020)

Az összes forgalomirányító és kapcsoló 2es verziójú SSH-al és 2048Bit hosszú kulccsal van felkonfigurálva. A belépésez szükséges adatok;  
Felhasználónév: Sbrokers jelszó: Sbrokers1234.  
<kép>

Védelmi beállítások miatt 1eszközről maximum 3x lehet próbálkozni utána nem enged több próbálkozást 3percig így kiküszöböli a Brute-Force támadást.

<kép>

### Port Security:

A portvédelem egy elengedhetetlen védelmi funkció egy cégnél. Segít megakadályozni az illetéktelen behatolást, mégpedig úgy, hogy hozzá rendel az interfészhez egy MAC címet és ha másik eszközt használunk lekapcsolja a portot és megnöveli a számlálóját így a rendszergazda látja, hogy valaki próbálkozott. Sajnos könnyen kicselezhető hiszen, ha ismerjük az adott gép MAC címét pár perc alatt MAC cím hamisítást tudunk csinálni így kijátszottuk a rendszert.

Több dolgot betudunk állítani, cégünknél minden porthoz maximum 1db mac címet tanul meg a kapcsoló ezt a switchport port-security maximum 1 paranccsal tudjuk megoldani. A MAC címet automatikusan tanitatjuk meg az eszközzel a switchport port-security mac-address sticky parancsal majd beállítjuk, hogy automatikusan lekapcsolj a portot, ha esteleg más próbálkozna, szükséges parancs hozzá: switchport port-security violation shutdown.

<kep>

Minden használaton kívüli portot lekapcsoltunk, es külön vlan-ba raktuk így ha valaki mégis felkapcsolná a portot nem fog tudni kommunikálni senkivel mert nincs beállítva a forgalomirányítás.

<kep>

### DHCP Snooping:

Nem mehetünk el amellett, hogy lehet bentről indul a támadás vagy pedig adat szivárgás így gondoskodni kell arról, hogy csak megbízható portoktól kapjunk DHCP kérést így ha valaki saját DCHP szolgáltatást hozna létre az ip dhcp snooping trust parancs miatt nem fog a harmadik féltől lévő DHCP szervertől IP címet kapni.

<kep>

### VTP(Vlan Trunk Protocol):

A VTP-t akkor érdemes használni, ha egy hálózatban sok vlan és kapcsoló található. Ez egy Cisco által kifejlesztett protokoll, ami megkönnyíti a VLANok konfigurálását és karbantartását. Így elég egy kapcsolón törölni vagy hozzá adni egy új vlan-t és az összes kapcsoló megtanulja.

Cégünknél SW\_MAIN\_SB kapcsoló lett kinevezve szervernek, ami azt jelenti, hogy őt kell konfigurálni ahhoz hogy a többi tanuljon tőle. Jelszóval van ellátva, ami a Sbrokers1234 domain név pedig Sbrokers és természetesen 2-es verzióval van felkonfigurálva. A többi kapcsoló kliensnek van beállítva

<kep>

### Jelszó titkosítás:

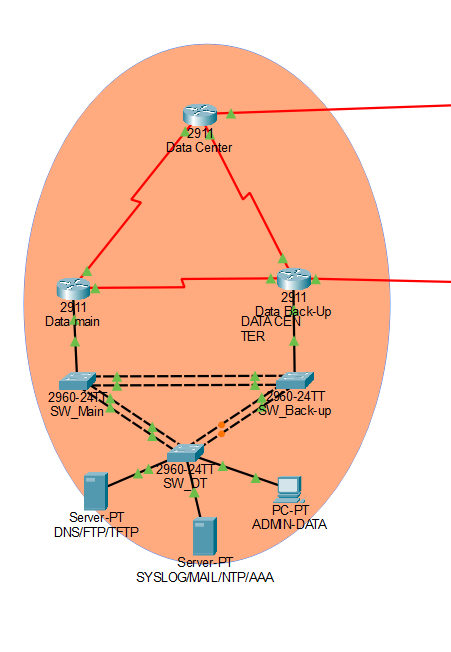
Minden eszközön be lett állítva privilegizált, vonali és konzoli jelszó, emellett egy üzenet fogad bejelentkezéskor, hogy illetékteleneknek tilos a belépés.

<kep>

Privilegizált jelszónál secret módba adtuk meg a jelszót, ami azt jelenti, hogy md5-el van titkosítva így ha valaki megnézi a konfigurációt szemmel nem értelmezhető jelszót fog találni. Sajnos a másdik 2 helyen csak sima, nem titkositt jelszót tudunk megadni, de a service password-encryption parancs miatt titkosítja ezeket a jelszavakat is. A vonali jelszók: Sbrokers1234 míg a privilegizált Sbrokers.

<kep>

## Narancssárga terület: adatközpont



Ez a South Brokers Zrt. bérelt adatközponja. Itt találhatóak meg az elsődleges szerverek.

Használt protokollok és szerver szolgáltatások:

* HSRP
* ACL
* IPsec
* Multilink
* EIGRP
* Portösszefogás
* SSH
* VTP
* Port Security
* PAT
* WAN
* STP
* Szerverszolgáltatások:
  + DNS
    - Címfeloldás
  + sFTP
    - Biztonságos fájl megosztás
  + TFTP
    - Adatmentés
  + SYSLOG
    - A hálózati eszközök és kapcsolatok monitorozása
  + MAIL
    - Saját belső levelezőrendszer
  + NTP
    - Közös időzóna
  + WEB
    - reszponzív weboldal

### Multilink:

Hasonló az EtherChannel-hez hiszen több serail portot fogunk össze, hogy 1db virtuális vonalat hozzunk létre így pénzt spórolunk mert nem kell drága optikai kábelt venni, de mégis gyors és biztonságos vonalat hozunk létre.

<kep>

### WAN(Wide Area Network):

Magyarul nagy kiterjedésű hálózat, ami két távoli területet kapcsol össze biztonságosan pont-pont kapcsolati beágyazási módszerrel. Többféle protokollt támogat köztük a CHAP és PAP-et.

A bank terület a CHAP hitelesítést alkalmaztuk, hiszen biztonságosabb, megfigyeli a kapcsolatok minőségét és bármilyen típusú forgalomirányító eszközön támogatott.

CHAP hitelesítés egy háromfázisú kézfogást használ és MD5-ös titkosítást. Előre meghatározott felhasználónév, jelszó párost hoztunk létre. Beállítás után titkos kulcsokat küldenek egymásnak a forgalomirányítók.

<kép>

### Link Aggregation:

Bérelt adatközpontunkban csak CISCO eszköz található ezért PAGP protokollal van ellátva a port összefogás.

<kep>

## Szerverek:

### DNS:

A legtöbb szolgáltatásunk DNS-névvel van ellátva így a dolgozóknak nem kell tudniuk a fix ip címet csak a cég nevét és a szolgáltatást. Így mindenkinek egyszerűbb és biztonságosabb.

<kép>

### sFTP:

A Pénzügynek lett kialakítva, hogy gyorsan és biztonságosan tudjanak fájlokat fel-le tölteni. Elérhető az Sbrokers.ftp.hu-n keresztül, bejelentkezési adatok; Penzugy -Penzugy1234

### TFTP:

Naponta készítünk biztonsági mentést minden eszköz konfigurációjáról a szerverre így egy esetleges meghibásodás során azonnal vissza tudjuk tölteni a konfigurációkat.

<kep>

### SYSLOG-NTP:

Az összes eszközünket monitorozzuk ezért minden egyes belépéskor egy üzenet érkezik a szerverre, ami a pontos dátum időt mutat és hogy mit csináltak az adott eszközön, lekapcsoltak egy portot vagy átírtak egy ip címet.

<kep>

Az NTP szerverünk autchentikációval van ellátva és minden eszközünkön kiadtuk a service timespan datetime msc parancsot így megjelenik a dátum-óra-perc-másodperc a syslog szerveren.

<kep>

### MAIL:

Saját belső levelező rendszert alakítottunk ki biztonsági okok miatt, mindenki saját felhasználónév és jelszó párossal rendelkezik így minden dolgozó eléri a másikat.

<kep>

<kep>

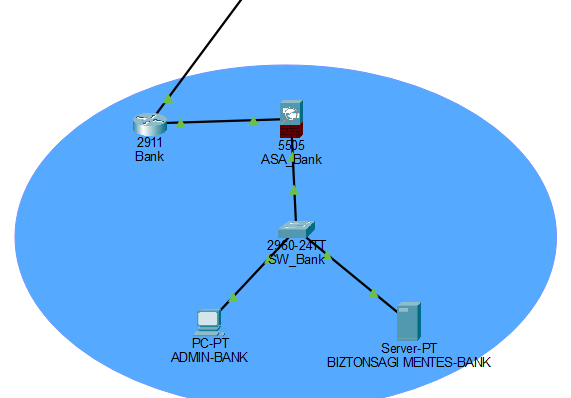
### WEB:

Cégünknek fontos a megjelenés ezért saját weboldallal rendelkezik, ami elérhető a [www.sbrokers.hu](http://www.sbrokers.hu) címen emellett a az MNB is elérhető a [www.mnb.hu](http://www.mnb.hu) címen.

<kep>

<kep>

## Kék telephely: Bank



Ezen a területen rendszerezett fizikai adatmentést végzünk. Itt a biztonság mindennél fontosabb.

Használt protokollok:

* EIGRP
* SSH
* Port security
* DHCP snooping
* Tűzfal: Cisco ASA 5505
  + NAT
  + IP route
  + DHCP
  + SSH
  + ACL
  + Policy-map
  + Class-map
  + Object network
  + Service-policy
  + VLAN

## Tűzfal:

A banknál Cisco Adaptive Security Appliance(ASA) hardeveres biztonsági tűzfalat használunk a hálózat határán. Míg a belső telephelyen 100as biztonsági szint működik a kulső részre 0át álítottunk így senki se tudja elérni a belső részt.

### Object network:

Object-ek segítségével a különböző konfigurációs területek könnyebbé és átláthatóbbá válhatnak, ide tartozik az ACL és NAT is. SERVER néven hoztuk létre.

<kep>

### Policy-map:

<kep>

### Class-map:

### Service-policy:

### NAT:

A bank statikus natot alkalmaz egyedül a web server számára így kívülről is elérhető.

<kep>

### ACL:

Meglévő alapértelmezett szabályokat felül tudjuk bírálni (pl: beengedjük a pingelést). A banknál csak kiterjesztett ACL található, amik kiengedik a DNS, WEB csomagokat így elérhető a WEB szerver.

<kep>

### Ip route:

Statikus forgalom irányítást alkalmaztunk a külső terület felől annak érdekében,hogy bárhonnan érkezhet a kérés a web szerver felé a kérés sikeres legyen.

### DHCP:

A belső admin gépünk DHCP-n keresztül kap IP címet az ASA-tól.

<kep>

# Hivatkozások:

Admin, 2021.02.09 A cikk címe: Redundáns alapértelmezett átjáró (HSRP)

URL: <https://iktblog.hu/2021/02/09/redundans-alapertelmezett-atjaro-a-hsrp-protokoll/>

Letöltve: 2022.03.26

Admin, 2021.02.05 A cikk címe: STP védelmi mechanizmusok

URL: <https://iktblog.hu/2021/02/05/stp-vedelmi-mechanizmusok/>

Letöltve: 2022. 03. 26

Atobot, 2018.09.10 A cikk címe: A hozzáférési jogosultság ellenőrzése

URL: <https://shorturl.at/yGTWY>

Letöltve: 2022. 03. 26

InternetArchiveBot, 2022:01.25 A cikk címe: Hálózati címfordítás

Url: <https://shorturl.at/dpF46>

Letöltve: 2022. 03. 26

InternetArchiveBot, 2021.08.01 A cikk címe: IPsec

Url: <https://shorturl.at/blxH6>

Letöltve: 2022. 03. 26.

InternetArchiveBot, 2020,06.20 A cikk címe: Secure Shell

Url: <http://shorturl.at/clwxI>

Letöltve: 2022. 03. 26.