Budapesti Műszaki Szakképzési Centrum

Neumann János Informatikai Technikum

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

***száma:*** 5-0612-12-02

**VIZSGAREMEK**

**South Brokers ZRT. hálózatának bemutatása**

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

Budapest, 2022.03. 28

Tartalom

[Cégleírás 4](#_Toc100487327)

[A hálózat tesztelésének dokumentációja 5](#_Toc100487328)

[Zöld terület: Fő telephely: 6](#_Toc100487329)

[HSRP: 8](#_Toc100487330)

[Feszitőfa( Spanning Tree Protocol) 9](#_Toc100487331)

[Link Aggregation: 11](#_Toc100487332)

[ACL: 12](#_Toc100487333)

[NAT: 13](#_Toc100487334)

[EIGRP: 14](#_Toc100487335)

[15](#_Toc100487336)

[IPSec: 16](#_Toc100487337)

[SSH: 17](#_Toc100487338)

[Port Security: 18](#_Toc100487339)

[DHCP Snooping: 19](#_Toc100487340)

[VTP(Vlan Trunk Protocol): 19](#_Toc100487341)

[Jelszó titkosítás: 20](#_Toc100487342)

[Narancssárga terület: adatközpont 21](#_Toc100487343)

[Multilink: 22](#_Toc100487344)

[WAN(Wide Area Network): 23](#_Toc100487345)

[Link Aggregation: 23](#_Toc100487346)

[Szerverek: 24](#_Toc100487347)

[DNS: 24](#_Toc100487348)

[sFTP: 24](#_Toc100487349)

[TFTP: 25](#_Toc100487350)

[SYSLOG-NTP: 25](#_Toc100487351)

[MAIL: 26](#_Toc100487352)

[WEB: 26](#_Toc100487353)

[Kék telephely: Bank 27](#_Toc100487354)

[Tűzfal: 28](#_Toc100487355)

[Object network: 28](#_Toc100487356)

[Policy-map: 28](#_Toc100487357)

[Class-map: 28](#_Toc100487358)

[Service-policy: 28](#_Toc100487359)

[NAT: 29](#_Toc100487360)

[ACL: 29](#_Toc100487361)

[Ip route: 29](#_Toc100487362)

[DHCP: 29](#_Toc100487363)

[South Brokers Zrt. szerverkörnyezetének dokumentációja 30](#_Toc100487364)

[Szolgáltatások: 30](#_Toc100487365)

[South Brokers 31](#_Toc100487366)

[Szolgáltatások részletezése 32](#_Toc100487367)

[sFTP: 32](#_Toc100487368)

[IIS: 32](#_Toc100487369)

[Email (IRedMail) 33](#_Toc100487370)

[Syslog: 33](#_Toc100487371)

[TFTP: 35](#_Toc100487372)

[AD: 35](#_Toc100487373)

[DC: 36](#_Toc100487374)

[File: 37](#_Toc100487375)

[DNS: 38](#_Toc100487376)

[DHCP: 39](#_Toc100487377)

[DHCP Failover 39](#_Toc100487378)

[VPN 39](#_Toc100487379)

[Költségvetés 41](#_Toc100487380)

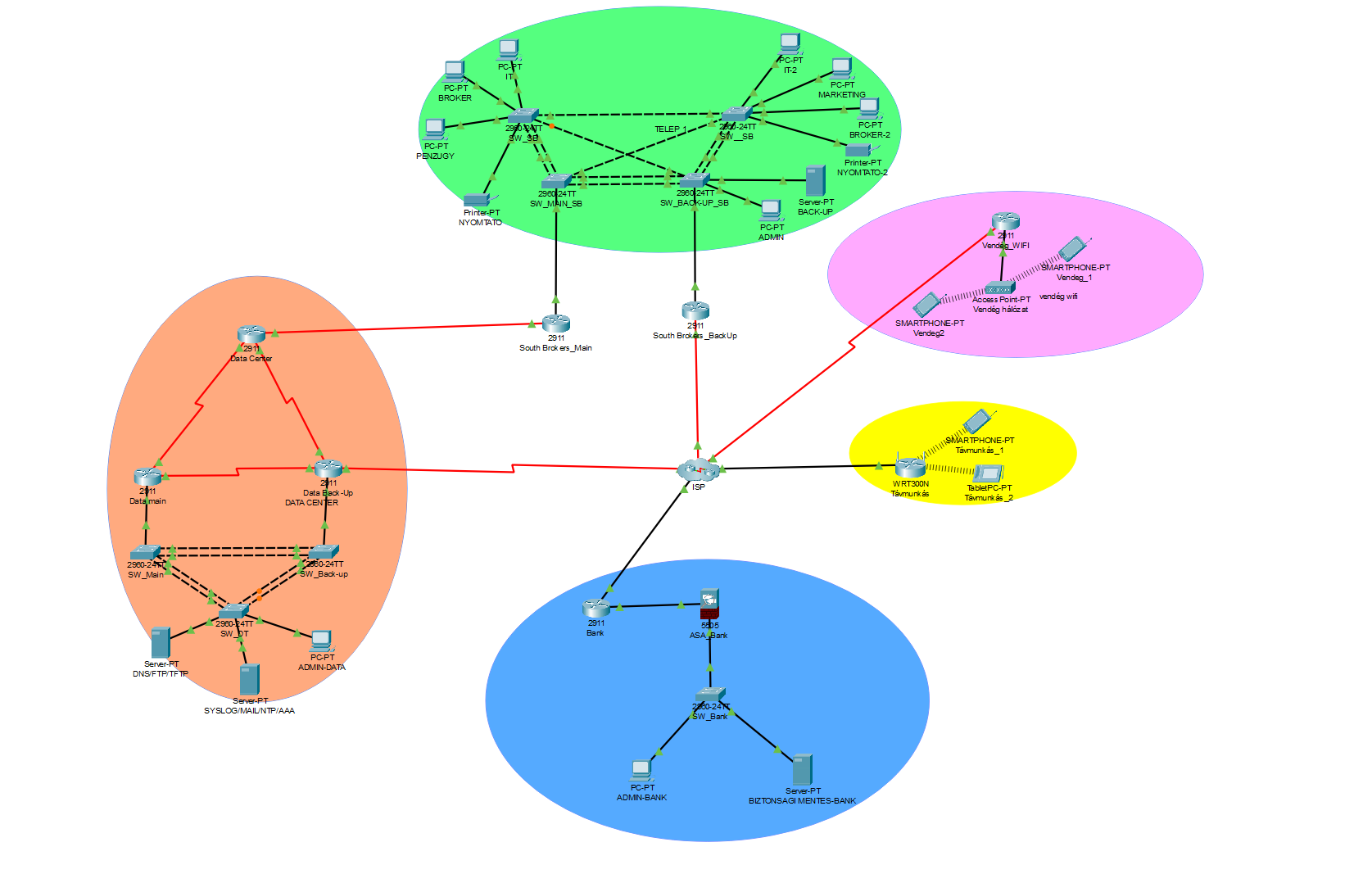
[Hálózat programozás: 42](#_Toc100487381)

[Hivatkozások: 43](#_Toc100487382)

# 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.

# 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 50 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

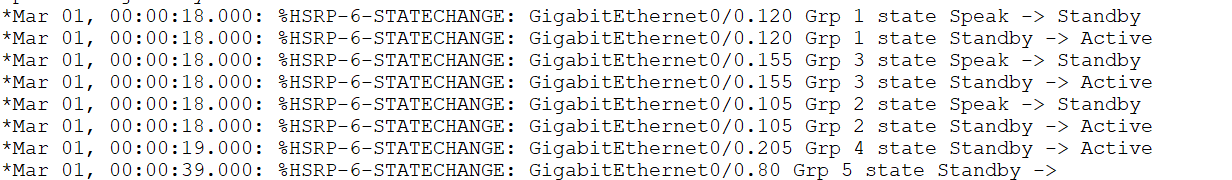
Kapcsolók:

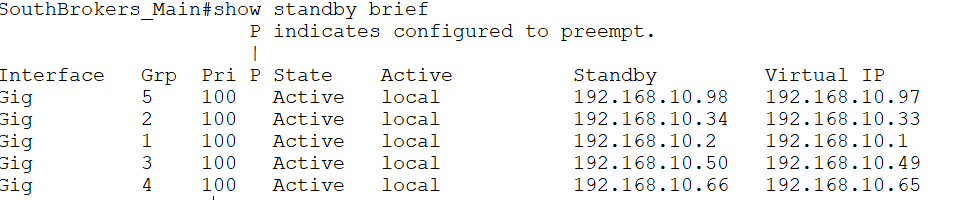
* Port security
  + Az interfészek maximum 1 Mac címet tanulnak meg, ismeretlen cím esetén lekapcsolnak.
* DHCP Snooping
  + Csak az ismert interfészeknek oszt címet DHCP-vel
* Vlan Trunk Protocol
  + Cisco protokoll: kapcsolók közötti Vlan információ csere
* Jelszó titkosítás
  + Service password-encryption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



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.

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)

A képen szöveg látható

Automatikusan generált leírásAhoz, 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.

A képen asztal látható

Automatikusan generált leírásA 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

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.



### 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.

A képen szöveg látható

Automatikusan generált leírásCégünknél 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.

### 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.

A képen szöveg látható

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

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



### 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.



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

A képen szöveg látható

Automatikusan generált leírásUtolsó 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.

### 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 |  |

A képen szöveg látható

Automatikusan generált leírásÖsszes 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.

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.

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>

### A képen szöveg látható Automatikusan generált leírás

### 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.

A képen szöveg látható

Automatikusan generált leírásEzért 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.

A képen szöveg látható

Automatikusan generált leírásTitkosításnál 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.

### 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)

A képen szöveg látható

Automatikusan generált leírásAz összes forgalomirányító és kapcsoló 2es verziójú SSH-al és 2048Bit hosszú kulccsal van felkonfigurálva. A belépésez szükséges adatok;  
Felhasználónév: Sbrokers jelszó:Sbrokers1234.

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





### 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.

A képen szöveg látható

Automatikusan generált leírás 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.

A képen szöveg látható

Automatikusan generált leírásMinden 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.

### 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 képen szöveg látható

Automatikusan generált leírás** 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



### Jelszó titkosítás:

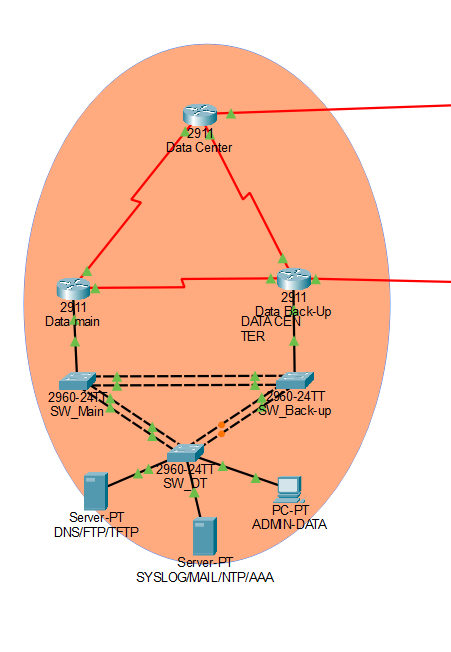
Minden eszközön be lett állítva privilegizált, vonali és konzoli jelszó, emellett egy üzenet fogad bejelentkezéskor, hogy illetékteleneknek tilos a belépés.



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.



## 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:

A képen szöveg látható

Automatikusan generált leírásHasonló 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.

### 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.

A képen szöveg látható

Automatikusan generált leírás

### Link Aggregation:

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

A képen szöveg látható

Automatikusan generált leírás

## Szerverek:

### DNS:

A képen szöveg látható

Automatikusan generált leírásA 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.

### sFTP:

A képen szöveg látható

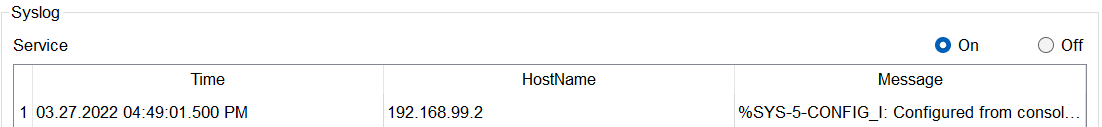
Automatikusan generált leírás A Pénzügynek lett kialakítva, hogy gyorsan és biztonságosan tudjanak fájlokat fel-le tölteni. Elérhető az Sbrokers.ftp.hu-n keresztül, bejelentkezési adatok; Penzugy -Penzugy1234

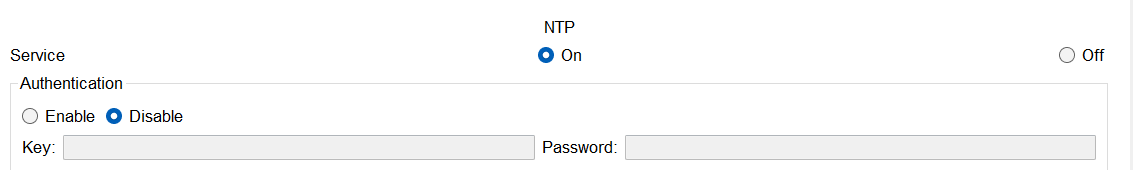
### TFTP:

A képen szöveg látható

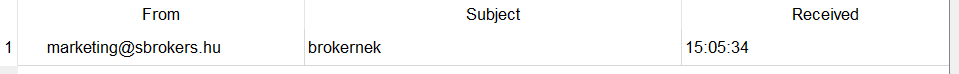
Automatikusan generált leírás Naponta készítünk biztonsági mentést minden eszköz konfigurációjáról a szerverre így egy esetleges meghibásodás során azonnal vissza tudjuk tölteni a konfigurációkat.

### 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.

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.

### MAIL:

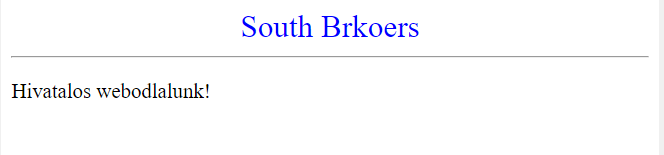
A képen szöveg látható

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

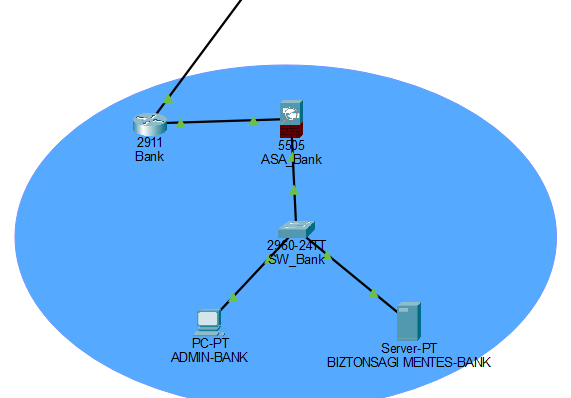
### WEB:

A képen szöveg látható

Automatikusan generált leírás 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.



## Kék telephely: Bank



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

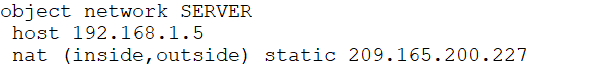
Használt protokollok:

* 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.

### Policy-map:

A képen szöveg látható

Automatikusan generált leírás

### Class-map:

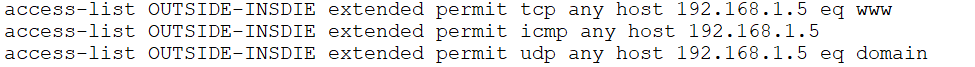
### Service-policy:

### 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.

### 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.

A képen szöveg látható

Automatikusan generált leírás

# 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, , , , 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, szerver és egy folytonosan szinkronizálódó Windows szerver segítségével. A szolgáltatások bővebb kifejtésére lentebb kerül sor.

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

## 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)

Szerver szoba kialakitása:

## Active Directory

Az Active Directory egy Microsoft címtárszolgáltatás vagy tároló, amely adatobjektumokat tárol a helyi hálózati környezetben hierarchikus struktúrákban. Ez a szolgáltatás a Windows szerverünkön fut

## Domain Controller

A DC, azaz a tartományvezérlő autentikéciós és autorizációs szolgáltatásokat nyújt tartományon belül, ami a fő Linux szerverünkön fut, és a teljes hálózati területen az Sbrokers.zrt domain nevet használtuk.

## Secondary Domain Controller

A fő Domain Controller meghibásodása során a másodlagos tartományvezértlő veszi át a szerepet, hogy a szolgáltatások továbbra is futhassanak. Ezt mi egy második Linux szerveren futtatjuk.

## Domain Name System

A DNS, azaz a tartománynév rendszer a fő Linux szerverünkön fut, ami lényegében IP címekhez rendel hozzá tartományneveket, ezzel leegyszerűsítve a címalapú hozzáféréseket. Ez a fő Linux szerverünkön fut.

## Dynamic Host Configuration Protocol (DHCP)

A DHCP egy protokoll, ami automatikusan ellátja a végeszközöket IP címmel. Ez a szolgáltatás szintén a fő Linux szerverünkön fut.

## DHCP Failover

A fő DHCP szolgáltató szerver leállása esetén átveszi a címosztás szerepkörét.

## Internet Information Services

Ez egy Microsoftos webszerver szolgáltatás, ami a Windows szerverünkön fut, és biztosítja a weboldalunk elérhetőségét HTTPS kapcsolaton keresztül.

## SSH File Transfer Protocol (sFTP)

Ez biztosítja két távoli rendszer között a fájlátvitelt. A sima FTP kapcsolatnál biztonságosabb, mert SSH protokollal van kiegészítve. Ez a Windows szerverünkön fut.

## File management

A nálunk dolgozó kollegáknak biztosítva van egy saját és egy közös terület, ahova adatokat tudnak menteni, megosztani. A saját mappák 2, a közös 10 Gigabájtnyi tárhellyel rendelkeznek.

## Group Policy Object

GPO-k segítségével a felhasználók engedélyeit, jogköreit korlátozzuk, hogy ezzel elkerüljük a potenciálisan káros programok futtatását, vagy külső eszközök használatát.

## Email (IRedMail)

Az IRedMail egy nyílt forráskódú email szerverszolgáltatás, ami által egy saját, privát levelezőrendszert futtatunk. Ez egy harmadik Linux szerveren fut.

## Print server

Hálózati nyomtatómegosztás, amit távolról is lehet működtetni.

## Virtaul Private Network

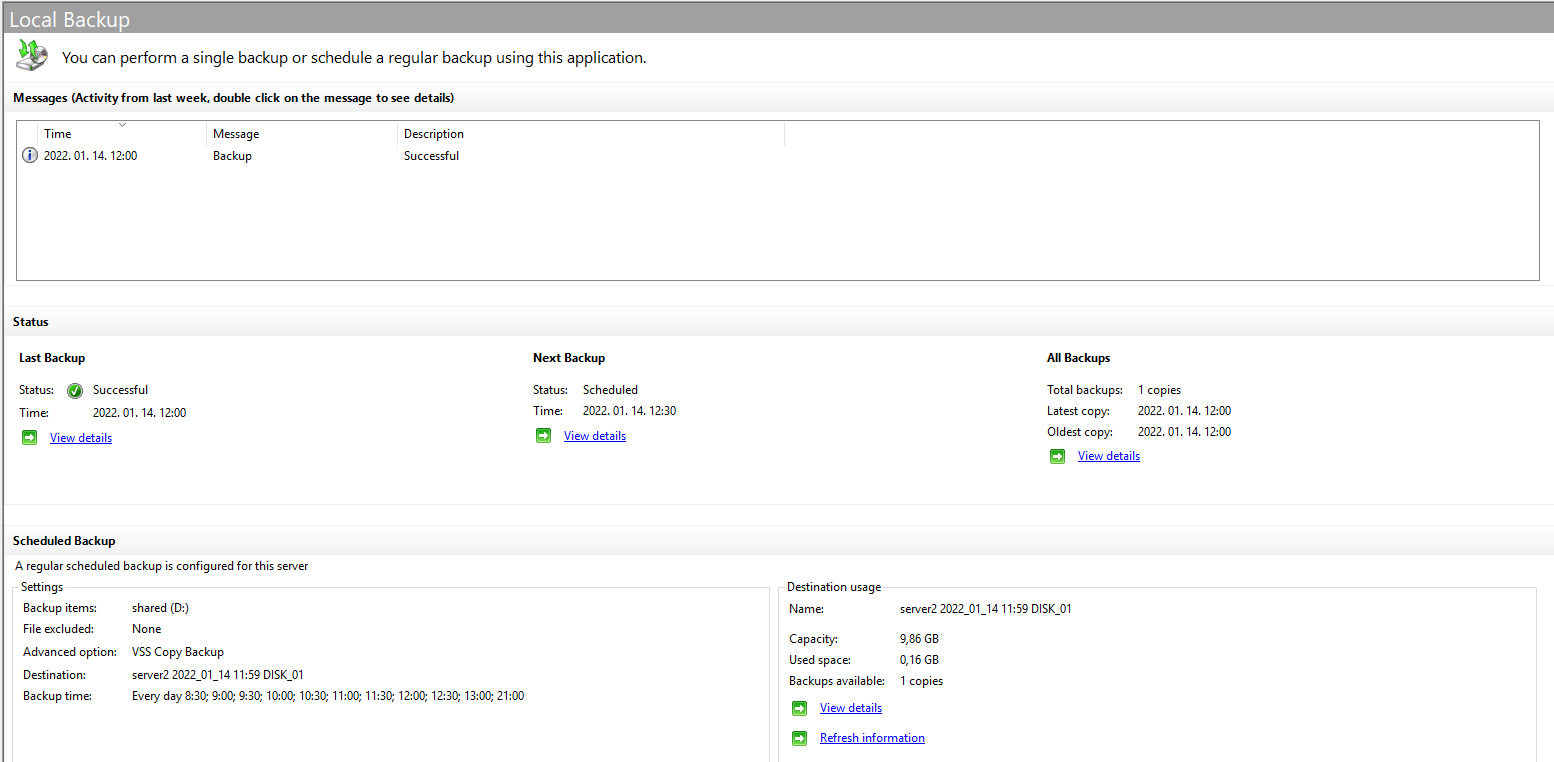
A virtuális magánhálózat, azaz VPN segítségével amikor külső hálózattal kommunkilálunk, a belső hálózati címeket a VPN szerver által adott virtuális címekre fordítja, ezzel elrejtve az eredeti forráscímeket. Ez a harmadik Linux szerverünkön fut.

<roviden alltalanossagban mire hasznaljuk, es cegunknell hogyan muokdik>

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

# South Brokers ZRT. Szerverei

## Mikrotik router

## Debian AD DC DNS DHCP

**Hardware és Software beállítások:**

* Hálózati kártya 🡪Belső hálózat
* Processzormagok száma: 2
* Memória mérete: 1024 Mb
* Tárhely: 50 Gb (OS)
* Operációs Rendszer: Debian 11.2.0

**Telepített szolgáltatások:**

* Active Directory
* Domain Controller
* Domain Name System (DNS)
* Dynamic Host Configuration Protocol (DHCP)

**Beállítások:**

* Szerver adminisztrátor jelszava: Aa123456
* Statikus IP cím (192.168.99.254)
* Hostname (debiansambaad)
* Szervezeti Egységek felvevésre kerültek (sbrokers.zrt)
  + 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)

# 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 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..**

## Hálózat programozás:

Cégünknél az összes kapcsoló elérhető távolról így bármikor tudjuk őket konfigurálni, akár egyszerre egy jól megírt paranccsal.

Hálózat programozás
A képen szöveg látható

Automatikusan generált leírásLenti képen látható, hogy átneveztük az eszközt és lekérdeztük az interfész táblát.

1. Hálózat programozás

# 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.