# 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.

ábra 1\*

## 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

## sFTP:

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:

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.

## 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.

## File:

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.

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.

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.

A DNS-ben a doménnevek kiosztásának és az IP-címek hozzárendelésének a felelősségét delegálják; minden tartományhoz mérvadó névkiszolgáló (autoritatív névszerver) tartozik. A mérvadó névkiszolgálók felelősek a saját doménjeikért. Ezt a felelősséget tovább delegálhatják, így az al-doménekért más névkiszolgáló felelhet. Ez a mechanizmus áll a DNS elosztott és hibatűrő működése mögött, és ezért nem szükséges egyetlen központi címtárat fenntartani és állandóan frissíteni.

A tartománynévrendszerben egyéb információkat is tárolnak, például egy adott internetes tartomány számára e-mailt fogadó levelezőkiszolgálók listáját. Az egész világot behálózó, elosztott, kulcsszó-alapú átirányítási szolgáltatásként a Domain Name System az internet funkcionalitásának alapvető fontosságú eleme.

RFID tagek, UPC-k, IP-telefonszámok és még sok más egyéb tárolására is használható a DNS adatbázisa. A Domain Name System specifikálja az adatbázis technikai képességeit, emellett leírja az internetprotokollcsalád részét képező DNS protokollt, részletesen meghatározza a DNS-ben használt adatstruktúrákat és kommunikációt.

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)

PRINT: szerver ami egy nyomtatót kezel, vagy többet hálózaton keresztül

# Forgalomirányítás

## OSPF (Open Shortest Path First)

Jellemzők:

* gyors konvergencia
* osztály nélküli
* skálázható
  + bevezeti a terület fogalmát
* SPF algoritmus használ
  + Shortest Path First
* támogatja a VLSM-et és a CIDR-et
* frissítés csak változáskor
  + nincs periodikus frissítés
* hitelesítés
* AD távolság 110

OSPF adatbázisai:

* szomszédsági – adjacency database
* kapcsolatállapot – link-state database
* továbbítási adatbázis – forwarding database – irányítótábla

A képen szöveg látható

Automatikusan generált leírásOSPF üzenetek

* hello csomag
* adatbázis-leíró
* frissítő (kapcsolatállapot)
* nyugtázó

A képen szöveg látható

Automatikusan generált leírás

## EIGRP (Enhanced Interior Gateway Routing Protocol)

Korábban IGRP

Jellemzők:

* Távolság vektor alapú
* Saját szállítási protokoll: RTP
* Osztály nélküli
* Hitelesítés
* AD távolság 90
* Nem szórja tele a hálózatot hello csomagokkal

Csomagjai:

* Hello
* Frissítő
* Nyugta
* Lekérdező
* Válasz

Táblái:

* Szomszédsági
* Topológiai
* Forgalomirányító

DUAL (Diffusing Update ALgorithm):

* Hurok menetesítő algoritmus
* Sávszélleség és Késleltetés

Lehetséges az automatikus összevonás

* Előnye, hogy a forgalomirányító táblában egy bejegyzés van és könnyebb kezelni a forgalmat
* Hátránya, hogy az összevont hálózat minden címe egy irányba kell lenni-e

A képen szöveg látható

Automatikusan generált leírás

# VLAN (Virtual Local Area Network)

* A VLAN a második rétegben (layer 2) hozzuk létre.
* Szórási tartományok csökkennek a használatával.
* Gyakrabban LAN hálózaton használjuk, de léteznek MAN, WAN hálózaton is.

Előnyök:

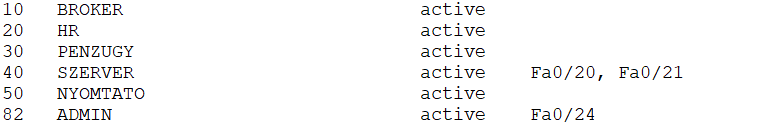
* biztonság
* költségcsökkentés
* szórási tartományok kisebbek

Típusok:

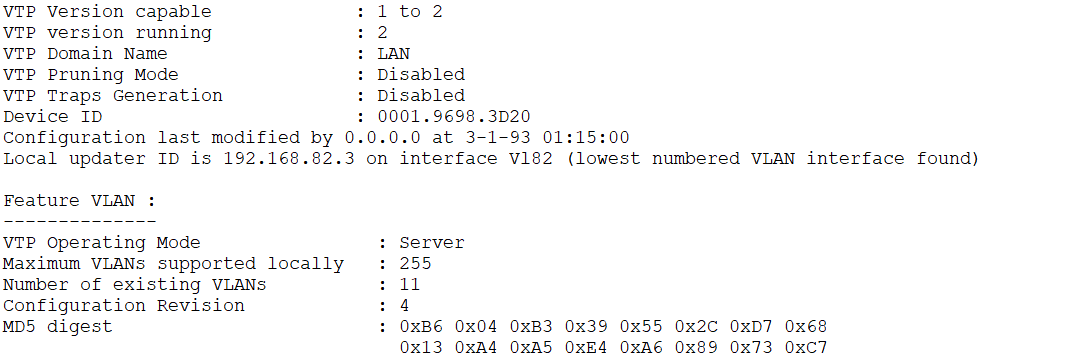
* adat VLAN
  + a felhasználók forgalmának létrehozva
* alapértelmezett VLAN
  + a kapcsoló alapértelmezett VLAN-ja
* natív VLAN
  + 802.1Q trönk porthoz rendelt
* felügyeleti VLAN
  + felügyeleti célból beállított

VoIP:

* Voice Over IP
* elkülönített VLAN-on továbbítjuk
* a hangminőség érdekében garantált sávszélesség szükséges
* más forgalommal szemben prioritást élvez



## VTP(VLAN Trunking Protocol)

a

# STP (Spanning Trunking Protocol)

Használat:

* Több, mint 2 kapcsoló egymással összekötésénél használjuk
* Ezzel redundás kapcsolatot hozunk létra a switchek között
* Szórási viharok és hurok kialakulását akadályozza meg

Rapid-PVST:

* Az STP egyik fajtája
* Gyorsabban konvergál

A képen asztal látható

Automatikusan generált leírás

# LACP (Link Aggregation Control Protocol)

Jellemzők:

* Portok összefogására használjuk
* A portok és kábelek összefogásával a továbbítási sávszélességet nagyítsuk
* Bármilyen típusú hálózati eszközön támogatott

Állapotai:

* Bekapcsolt (On): A portok nem használnak LACP-t
* Aktív (Active): Kapcsolatot kezdeményez és LACP csomagokat küld
* A képen szöveg látható

  Automatikusan generált leírásPasszív (Passive): Csak figyeli a beérkező csomagokat és válaszol rá

# WAN (Wide Area Network)

PPP (Point-to-Point Protocol)

Jellemzők:

* Pont-pont kapcsolati beágyazási módszer
* Soros kábel, telefonvonal, gerincvonal, mobiltelefonos hálózat, speciális rádiós kapcsolat vagy optikai szálas összeköttetésnél használható

Előnyei:

* Bármilyen típusú forgalomirányító eszközön támogatott
* Megfigyeli a kapcsolatok minőségét
* Támogatja a PAP és CHAP hitelesítést

## CHAP (Challenge-Handshake Authentication Protocol)

Működése:

* háromfázisú kézfogást használ
* MD5 titkosítással megvédi a jelszavat
* titkos kulcsokat küldenek egymásnak a forgalomirányítók

A képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

# DHCP (Dynamic Host Configuration Protocol)

Feladata:

* Egy megadott IP cím tartományból IP címek osztása
* DNS szerver cím osztás
* Alapértelmezett átjáró cím osztás

Eszközök:

* Forgalomirányító
* SzerverA képen szöveg látható

  Automatikusan generált leírás

# ACL (Access-Control List)

Feladata:

* Engedélyez vagy tilt hálózati címek belépését egy hálózatba

Típusai:

* Alapértelmezett (Standard)
* Kiterjesztett (Extended)

Elnevezés fajtái:

* Számozott
* Nevesített

A képen szöveg látható

Automatikusan generált leírás

# VPN (Virtual Private Network)

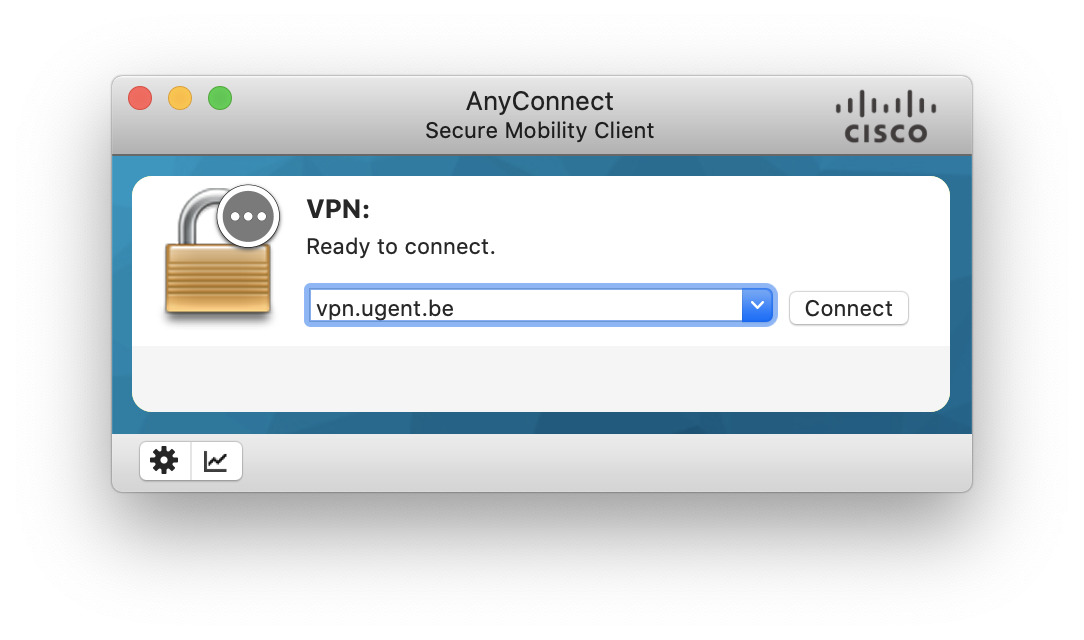
Jellemzők:

* Virtuális magánhálózat
* Eredeti hálózaton titkosított adat

Típusai:

* Távoli hozzáférés (Remote Access)
* Telephelyek közötti (Site-to-site)
* Extranet-alapú pont-pont (Extranet-based site-to-site)

Előnyei:

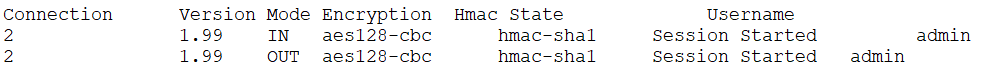
* Kölcségmegtakarító
* Biztonságos
* Skálázható
* Kompatibilis a szélessávú technológiákkal

# SSH (Secure SHell)

Jellemzői:

* Titkosítási protokoll
* Nyilvános kulcsú
* Távoli asztal elérést biztosít
* Port száma: 22

Feladata:

* Biztonságos csatornát hozzon létre

A képen asztal látható

Automatikusan generált leírásA képen szöveg látható

Automatikusan generált leírás

# NAT (Network Address Translation)

Feladata:

* Felhasználók IP címzésének elrejtése és új IP cím adása, amikor egy csomag elhagyja a belső hálózatot.

Működése:

* A kimenő csomag feladójának az IP címét kicseréli egy saját IP címre, mintha az eszköz küldte volna a csomagot.

Fajtái:

* Statikus NAT
* Dinamikus NAT
* PAT (Port Address Translation)

Egyéb:

* NAT Átjárhatóság (Traversal)
* SIP (Session Initiation Protocol)
* IP-szűrés

A képen szöveg, beltéri látható

Automatikusan generált leírás

# Port security

Feladata:

* Megvédje a hálózatot a belülről végrehajtott támadástól

Működése:

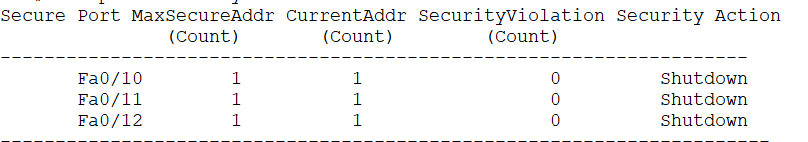
* Megjegyzi az eszköz a hozzákötött másik eszköz MAC címét

Használata:

1. Nem használt portokat kikapcsolt állapotba helyezése
2. Portok maximálisan megjegyehető MAC címek megadása
3. Manuálisan beírni a MAC címet vagy automatikusan megjegyeztetni

Típusai:

* Véd (Protect)
* Korlátoz (Restrict)
* Leállít (Shutdown)



# Cisco ASA (Adaptive Security Appliance)

Jellemzők:

* Cisco által fejlesztett tűzfal
* Használható hálózati és adatközponti tűzfalnak egyaránt
* Megkönnyíti a dinamikus irányítást és a telephely közötti VPN-t
* Teljes IPS, VPN és Egységes kommunikációt (Unified Communications) kínál
* Együttműködést biztosít fizikai és virtuális eszközök között

# 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$