Harkály Krisztián, Számadó Milán, Horváth Márió

[cég neve]

Záróvizsga 5. csoport

13.B

Tartalomjegyzék

Bevezetés a projekthez1

Hálózati topológia, feladat

Címzési terv2

A hálózatunk címzési terve

**Feladatleírás** 3

A feladat, megoldások

4

5

6

**Bevezetés a projekthez**

A közepes méretű vállalatok számára a megfelelő hálózati infrastruktúra kialakítása és fenntartása kulcsfontosságú a zökkenőmentes üzleti működéshez. A feladat, hogy egy ilyen vállalat három telephelyén kiépítésre kerüljön a megfelelő hálózati rendszer, amely biztosítja az összes üzleti és technikai igényt, különösen akkor, amikor a vállalat több telephellyel dolgozik, és folyamatos, megbízható adatátvitelt igényel. A tervezés során alapvető szempont, hogy a rendszer képes legyen támogatni a vállalat minden szempontból fontos tevékenységét, beleértve a napi működést, a biztonságot, valamint a rugalmasságot, amely lehetővé teszi a távoli munkavégzést is.

A három telephely összekapcsolása érdekében olyan stabil és gyors hálózati infrastruktúrára van szükség, amely nemcsak a belső adatforgalmat, hanem az internetkapcsolatokat is biztosítja. Az adatforgalom menedzselésének és a telephelyek közötti kapcsolat stabilitásának biztosítása érdekében a hálózati topológia tervezésekor figyelembe kell venni a redundanciát, a terheléselosztást és a hibatűrést is, hogy a vállalat működése ne szenvedjen késedelmet a különböző helyszínek közötti adatkommunikáció során. A helyi és távoli hálózati forgalom biztonságát is meg kell oldani, így a rendszerben megfelelő titkosítási és hitelesítési mechanizmusok alkalmazása válik szükségessé.

A belső hálózaton belül az egyes telephelyek közötti kommunikációt a vállalat mindennapi működése számára elengedhetetlenül fontos eszközök és szolgáltatások fogják igényelni, mint például fájlmegosztás, levelezés, vállalati alkalmazások elérése, vagy egyéb üzleti eszközök integrálása. A különböző telephelyek közötti fájlmegosztás és a központi adatbázis elérése alapvetően az üzleti hatékonyságot és a zökkenőmentes együttműködést szolgálja. Ezen kívül a biztonságos internetkapcsolat biztosítása a távoli elérés érdekében kulcsfontosságú, hiszen a vállalat dolgozóinak egyre több esetben van szükségük arra, hogy távolról is elérjék a vállalati erőforrásokat.

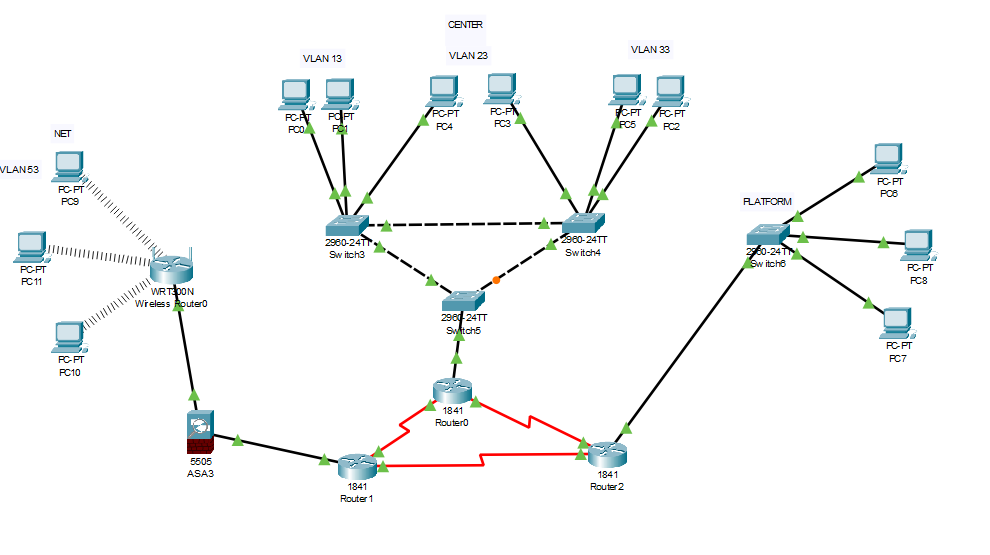
A távoli hozzáférést biztosító VPN kialakítása szintén elengedhetetlen, mivel a munkavállalók számára biztosítani kell a biztonságos kapcsolódást a vállalat belső rendszeréhez, akár otthoni munkavégzésről, akár egy másik telephelyről történik a csatlakozás. A VPN-nek nemcsak az adatbiztonságot kell garantálnia, hanem a kapcsolódás megbízhatóságát is, hiszen minden megszakadt kapcsolat komoly üzleti zűrzavart okozhat.

A rendszer megvalósítása után fontos a tesztelés is, amely során minden egyes hálózati komponens működését és együttműködését alaposan ellenőrizni kell, hogy a valós üzleti környezetben is stabilan és megbízhatóan működjön a rendszer. A tesztelésnek ki kell térnie a hálózati eszközök, a VPN, valamint az internetkapcsolat és a belső hálózat összes összetevőjének teljesítményére és biztonságára is.

**A projekt:**

Egy közepes méretű vállalatnak három telephelyét megterveztük. A rendszer támogatja a vállalat összes technikai igényét

**A hálózati topológia:**

****

Három telephelyet tartalmaz a vállalkozás hálózatja:

Az első telephely a Center telephely – ez lenne a fő adatközpont. Itt található a menedzsment.

Több szintű VLAN került kialakításra. Három VLAN lett létrehozva a telephelynél: VLAN 13, az adminisztrációs VLAN, VLAN 23: az IT VLAN. VLAN 33: Ez nem más, mint a vendéghálózat.

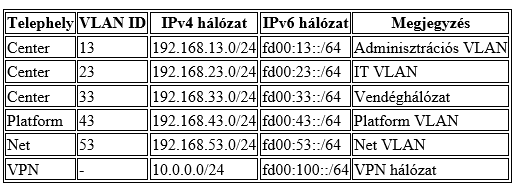
Ennél a telephelynél használtunk redundans forgalomirányítókat és kapcsolókat (a használt redundancia technológiája: HSRP és VRRP). Szükség volt a telephelynél a WLAN hozzáférési pontok használata (802.1x alapú hitelesítéssel). Az eszközökön elvégeztünk statikus és dinamikus IPv4, illetve IPv6 címzést is.

A második telephely a Platform telephely – ez a gyártás és a logisztikai telephely. Szintén található ennél a telephelynél egy VLAN: VLAN 43. Ez a gyártási folyamatok VLAN. A központi irodához (vagyis a Center telephelyhez) VPN kapcsolódás áll rendelkezésre. A VPN IPsec alapú. A telephelyen rendelkezésre áll egy helyi DHCP és DNS szolgáltatás redundanciával.

A harmadik telephely a Net telephely – az ügyfélszolgálat és az értékesítés telephelye. Itt található meg az értékesítési VLAN. Ennél a telephelynél rendelkezésre áll egy WLAN hozzáférési pont: egy Cisco WRT300N Wireless Router, ami a vezetéknélküli kapcsolatot biztosítja. Három eszköz van csatlakozva a hálózathoz a wireless routeren keresztül. Dinamikus címfordítást végeztünk (NAT és PAT).

Az összes telephelyek között rendelkezésre áll egy MPLS (Multiprotocol Label Switching) kapcsolat. Tartalékkapcsolatként IPsec VPN-t építettünk be. Az internetelérés a központi irodán keresztül történik.

**Hálózat címzési terv:**



Az összes telephelynél alkalmaztunk statikus és dinamikus IPv4/IPv6 címzést. Több VLAN ID kiosztásra került: három VLAN a Center telephely, és egy a Platform és a Net telephelyen.

**Feladatleírás:**

* Létrehoztuk a hálózat topológiáját a Cisco Packet Tracer szimulációs környezetben. Megterveztük az alhálózatokat, és a címzési struktúrát.
* Konfiguráltuk az összes hálózati eszközöket, mint például a forgalomirányítókat, és a kapcsolókat.
* Implementáltuk forgalomirányítást a VLAN-ok között. A redundáns protokolokat (HSRP, VRRP) használjuk a hálózat kiépítésében. A WLAN hozzáférés WPA3 titkosítással történt meg, 802.1x hitelesítéssel egyaránt.
* Alkalmaztuk az IPv4 és IPv6 címzést, konfiguráltuk a statikus és dinamikus routing protokolokat (mint például az OSPFv2, az OSPFv3, és az EIGRP.) Beépítettük a NAT és a PAT megoldásokat.
* A hálózaton két kiszolgáló található: egy Linux kiszolgáló, és egy Windows Server alapú kiszolgáló.
* A Linux kiszolgálón egy Debian 12.10 rendszer fut, és bizonyos szolgáltatásokat futtatunk ezen a szervergépen.
* Ezek között találhatóak a DHCP szerver, a DNS szerver, A HTTP/HTTPS webszerver (Apache2 webszerver-t használunk.) Egy Samba fájlszervert is futtatunk a szerveren, főleg biztonsági mentésekre.
* A Windows kiszolgálón egy 64-bites Windows Server 2019 fut.
* Ez a kiszolgáló főleg egy Active Directory tartományvezérlő számára áll rendelkezésre, de fut rajta sok más szolgálatás, mint például egy fájlszerver, és nyomtatómegosztás.
* Csoportházirendekkel be van állítva az automatizált szoftvertelepítés az összes számítógépre a domainen.
* A hálózat biztonságára figyeltünk, beállítottuk az ACL-eket a fontos, érzékeny adatok védelmére.
* Hardveres tűzfalat használunk a védelemért, egy Cisco ASA 5505 eszközt.
* Ez alkalmas nekünk a hálózat hardveres tűzfal védelmére, és illetve még egy IPsec alapú VPN-t is biztosít.
* Teszteltük a telephelyek közötti kommunikáció, minden lezajlott sikeresen és bizonságosan, semmiféle hiba nélkül.
* Ping és traceroute alapú tesztelés sikeres volt. Ellenőriztük az ACL-eket, a VLAN-okat, és a VPN működését, ami szintén sikeresen lezajzlott.

**VPN:** A VPN a Virtual Private Network rövidítése. Általában a nyílt hálózaton egy privát alagút használatáról van szó, amelyen titkosított forgalom zajlik. A távoli elérése egy IPsec alapú VPN-en keresztül jön létre.

**DHCP:** A DHCP a Dynamic Host Configuration Protocol rövidítése. Ezzel dinamikusan ki tudjuk osztani az IP címeket.

**ACL:** Az ACL tulajdonképpen engedélyező és tiltó utasítások szekvenciális sorozata, amelyeket címekre, portokra, szolgáltatásokra vagy felsőbb rétegbeli protokollokra alkalmazhatunk. Ezek a listák határozzák meg a forgalomirányító számára, hogy mely csomagokat fogadja el és melyeket utasítsa vissza. Ezzel az ACL, lehetővé teszi a forgalom felügyeletét, s a meghatározott csomagok ellenőrzését is.

**VLAN:** A számítógép-hálózatok körében a virtuális helyi hálózat vagy látszólagos helyi hálózat (rövidebben virtuális LAN, virtual LAN, azaz VLAN) hálózati eszközök egy olyan csoportja, aminek tagjai úgy kommunikálnak, mintha ugyanabba a szórási tartományba tartoznának, fizikai elhelyezkedésüktől függetlenül.

**NAT:** A NAT a Network Address Translation rövidítése, magyarul címfordítás.

Háromféle NAT létezik:

1. statikus NAT
2. dinamikus NAT
3. kiterjesztett NAT (PAT)

**Statikus NAT:** A statikus NAT egy technológia, amely egy belső IP-címet állandóan egy nyilvános IP-címhez rendel, biztosítva ezzel a rendszer folyamatos elérhetőségét az interneten. Előnye a megbízhatóság, hátránya, hogy sok nyilvános IP-címet igényel.

**Dinamikus NAT:** A dinamikus NAT egy hálózati technológia, amely a belső IP-címeket ideiglenesen, egy rendelkezésre álló nyilvános IP-címre fordítja le. Ez a fordítás változhat, és nem állandó, így több belső eszköz is osztozhat egy nyilvános IP-címen. Előnye, hogy kevesebb nyilvános IP-címet igényel, de hátránya, hogy a kapcsolatok nem garantáltan azonos IP-címmel történnek.

**Kiterjesztett NAT:** A kiterjesztett NAT (PAT – Port Address Translation) lehetővé teszi, hogy több belső eszköz egyetlen nyilvános IP-címet használjon, különböző portszámok segítségével. Minden egyes belső kapcsolatot egyedi portszámhoz rendel, így több eszköz is ugyanazt az IP-címet oszthatja meg. Előnye a hatékony IP-cím használat, hátránya, hogy a portok korlátozott száma miatt nagy forgalom esetén problémák léphetnek fel.

**MPLS:** Az MPLS (Multiprotocol Label Switching) egy sokoldalú megoldás, amely a mai hálózatok által tapasztalt problémákra - sebesség, skálázhatóság, szolgáltatásminőség (QoS) menedzsment és forgalomirányítás - kínál megoldást. Az MPLS az adatokat egyik hálózati csomópontból a másikba rövid útvonalcímkék alapján irányítja, ahelyett hogy hosszú hálózati címeket használna.

**HTTP:** A HTTP (HyperText Transfer Protocol) egy információátviteli protokoll elosztott, kollaboratív, hipermédiás, információs rendszerekhez. A http egy kérés-válasz alapú protokoll kliens és szerver között. A webszerverek ezt a protokollt használják, a HTML fájlokat kiszolgálja a kliensekhez.

**IPsec:** Az Internet Protocol Security (IPsec) egy biztonságos hálózati protokollcsomag, amely hitelesíti és titkosítja az adatcsomagokat, hogy biztonságos, titkosított kommunikációt biztosítson két számítógép között.

**Eszközök**

**2960-24 Switch**

A Cisco Catalyst 2960-24 egy 24 portos, Layer 2-es switchekhez tartozó eszköz. A Cisco 2960-24 a Catalyst 2960 sorozat tagja.

**Főbb jellemző****1.Portok és teljesítmény**: A 2960-24 switch 24 darab 10/100 Mbps Ethernet porttal rendelkezik, amelyek biztosítják a gyors adatátvitelt és alacsony késleltetést a csatlakoztatott eszközök között, amely lehetővé teszi az intenzívebb adatforgalom kezelését, miközben a kisebb igényű alkalmazások számára is optimális sebességet biztosít. 2 uplink port 10/100/1000 Mbps sebeséggel rendelkezik. 16Gbps kapacitása van a switchnek, 16 MB DRAM-al rendelkezik.

**2.Kezelhetőség:** A Cisco Catalyst 2960-24 switch teljes mértékben menedzselhető, a soros konzol segítségével kezelhető a switch. A felületben beállítható bizonyos technológiák, mint például az SPAN, RSPAN, CiscoView, Cisco Discover Protocol (CDP), VTP (Virtual Trunking Protocol), BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clusterezés, és a Web alapú kezelhetőség.

**3.Hálózati biztonság**: A Cisco 2960-24 beépített biztonsági funkciókkal rendelkezik, mint például az 802.1X port alapú hitelesítés, amely lehetővé teszi, hogy a hálózathoz csak megfelelően hitelesített eszközök csatlakozhassanak. Ezen kívül támogatja a VLAN-ok (Virtuális Lokális Hálózatok) használatát, amellyel a hálózaton belül különböző szegmensek hozhatók létre.

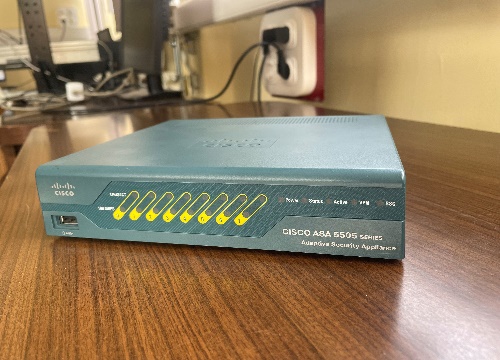
**Cisco ASA 5505**

**A Cisco ASA 5505** egy új generációs, teljes funkcionalitású biztonsági készülék kisvállalkozások, fiókirodák és vállalati távmunkás környezetek.

**Főbb jellemzők:**

**1. Típus:** Integrált tűzfal és VPN eszköz.

**2.Ethernet portok:** 8 db 10/100 Mbps Ethernet port, amelyek közül 8 portot használhatsz (6 alapértelmezett adatport és 2 "secure" port).

Console, USB port: 1 db konzolport (RJ-45), 1 db USB port (például szoftverfrissítéshez vagy mentésekhez).

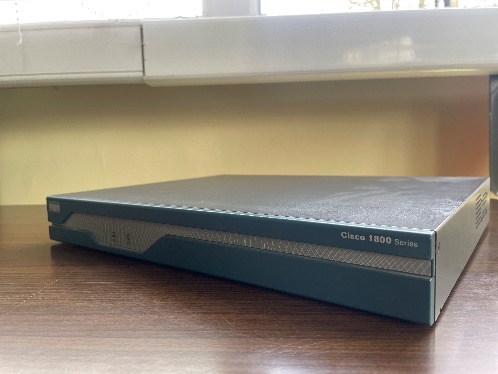
**3.VPN teljesítmény:** Akár 25 IPsec VPN kapcsolatot támogat egyszerre.

**4.Maximális párhuzamos kapcsolat**: 10 000 kapcsolatra képes. Ez a kis eszköz alapvető tűzfal, VPN és biztonsági feladatokat lát el, de nem igazán skálázható nagyobb vállalati környezetekhez.

**5.Biztonság**: Tűzfal, VPN, IDS/IPS alapú védelem.

**6. Támogatott licenszek**: A modellek lehetnek "Base" vagy "Security Plus" licensszel, ami extra funkciókat ad (pl. VPN bővítés).

**1841 Router**

**Főbb jellemzők:**

**1.Teljesítmény:** Ötszörös útválasztási teljesítménynövekedés a Cisco 1700 sorozathoz képest.

Az új generációs nagysebességű WAN-interfészkártyák (HWIC) támogatása. Több modulhely és nagyobb teljesítmény az interfészkártyákhoz

**2.Portok:** Opcionális beépített 10/100 megabites kapcsoló és két beépített 10/100 megabites LAN-port. USB-port jöv őbeli alkalmazásokhoz, például a VPN-hitelesítési adatok készüléken kívüli tárolásához.

**3.Alkalmazások:** Megnövekedett rugalmasság a gyorsabb VPN-kapcsolat és a jövőbeli alkalmazások számára készült belső AIM-modulhely révén.

**4.QoS (Quality of Service):** A minőségszolgáltatás támogatása, amely lehetővé teszi az adatok forgalmának priorizálását (pl. VoIP hívások vagy videókonferenciák).

**5.NAT (Network Address Translation):** A NAT támogatása lehetővé teszi több eszköz használatát egyetlen publikus IP címmel.

**Cisco 867VAE-W-E-K9**

1. Jellemzők és előnyök

 A Cisco 860VAE sorozatú ISR-ek belépő szintű, fix konfigurációjú útválasztók

1. Költséghatékony alap- vagy biztonságos kapcsolat minőségi szolgáltatással (QoS) a távmunkások számára és felügyelt CPE-eszközök a szolgáltatók számára
2. Három 10/100 Fast Ethernet switch port és két Gigabit Ethernet switch port a 2,4 GHz-es 802.11n FCC- vagy ETSI-kompatibilis vezeték nélküli LAN-nal rendelkező vezeték nélküli modellekben
3. Egy USB 2.0 port az USB-ről történő rendszerindításhoz vagy a konfiguráció betöltéséhez
4. IPv6 támogatás minden modellen
5. A Cisco 860VAE útválasztók támogatják a Gigabit Ethernet (GE) vagy a nagyon nagy sebességű DSL 2/aszimmetrikus DSL2+ (VDSL2/ADSL2+) szabványt egyetlen rögzített ISR-en.

**Cisco programozás:**

**OSPF Konfigurálása:**

Az OSPF (Open Shortest Path First) egy dinamikus irányítószolgáltatás, amelyet a három router közötti adatforgalom hatékony irányítására használtunk. Az OSPF biztosítja, hogy a routerek automatikusan frissítsék az útvonal táblákat, és dinamikusan optimalizálják a hálózati forgalmat.

Az OSPF konfigurálása az alábbi lépésekből állt:

* Minden routeren beállítottuk az OSPF protokollt, és meghatároztuk a megfelelő hálózati címeket.
* Az OSPF router-azonosítókat (Router-ID) konfiguráltuk minden routeren, hogy azonosíthassák egymást.
* A routerek közötti linket OSPF alhálózatként konfiguráltuk, hogy a dinamikus útvonalválasztás megfelelően működjön.
* OSPF típusú területeket (Area) hoztunk létre, és a routereket az ezekhez tartozó területekhez rendeltük.

Az OSPF biztosítja a hálózati redundanciát, mivel ha egy útvonal kiesik, a rendszer automatikusan egy alternatív utat választ, ezáltal növelve a hálózat megbízhatóságát.

**VLAN-ok és Switch konfigurálása – Rövidített verzió**

A VLAN-ok (Virtual Local Area Networks) segítségével a hálózaton belül logikailag elkülöníthetjük az eszközöket, így javítva a biztonságot, teljesítményt és kezelhetőséget. A projektben öt switch-en alakítottuk ki a szükséges VLAN-okat, amelyek az eszközök és munkacsoportok közötti adatforgalom szegmentálását biztosították.

**1. VLAN-ok tervezése:** A következő VLAN-okat hoztuk létre:

* **VLAN 13 (Admin):** Adminisztráció számára.
* **VLAN 23 (IT):** IT osztály számára.
* **VLAN 33 (Vendég):** Vendég hozzáférés.
* **VLAN 43 (Platform):** Gyártás és logisztika.
* **VLAN 53 (Net):** Ügyfélszolgálat és értékesítés

**2. Switch konfigurálás:** A switch-ek portjait hozzárendeltük a megfelelő VLAN-okhoz, így biztosítva, hogy a forgalom csak azon eszközök között áramoljon, amelyek ugyanabban a VLAN-ban vannak.

* **VLAN-ok létrehozása:** Minden switch-en létrehoztuk a VLAN-okat, pl. vlan 10, vlan 20 stb.
* **Portok hozzárendelése:** A portokat a megfelelő VLAN-okhoz rendeltük, például a sales csoport portjait VLAN 10-hez.
* **Trunk portok beállítása:** Az inter-VLAN kommunikációhoz trunk portokat konfiguráltunk a switchek között.

**3. Inter-VLAN Routing:** A routereken konfiguráltuk az inter-VLAN routingot a "Router on a Stick" (ROAS) megoldással, ahol minden VLAN-hoz külön alhálózati interfész tartozik, és a forgalom ezen keresztül történik.

**4. Biztonság:** A hálózat biztonsága érdekében port security-t, DHCP snooping-ot és ARP inspection-t alkalmaztunk a switch-eken, hogy megakadályozzuk a nem kívánt hálózati támadásokat.

**5. Tesztelés:** A konfigurálás után teszteltük a VLAN-ok közötti kommunikációt és biztosítottuk, hogy a forgalom a kívánt módon áramoljon a hálózaton.

Ezáltal egy jól szegmentált és biztonságos hálózati infrastruktúrát alakítottunk ki, amely hatékonyan támogatta a vállalat működését.

**DHCP Konfigurálása**

A Dynamic Host Configuration Protocol (DHCP) lehetővé teszi, hogy a hálózati eszközök automatikusan IP-címet kapjanak a routertől, így nem szükséges manuálisan konfigurálni az eszközök IP-címeit. A DHCP segítségével biztosítottuk, hogy a hálózati eszközök dinamikusan kapjanak IP-címet, és könnyen csatlakozhassanak a hálózatra.

A DHCP konfigurálása az alábbi lépésekből állt:

* Beállítottuk a DHCP szervert a routereken, és meghatároztuk a DHCP tartományokat az egyes alhálózatok számára.
* A DHCP szerverek meghatározták az IP-címeket és az egyéb konfigurációs adatokat (pl. DNS, gateway) az eszközök számára.
* A DHCP konfiguráció biztosította, hogy minden új eszköz automatikusan IP-címet kapjon a hálózaton.

**Források**

**A szövegekhez több oldal is rendelkezésre állt amiből tudtunk forrást meríteni.**

* [**https://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data\_sheet\_c78-693249.html**](https://www.cisco.com/c/en/us/products/collateral/routers/800-series-routers/data_sheet_c78-693249.html)
* [**https://github.com/Harkalykrisz/VizsgaPFG**](https://github.com/Harkalykrisz/VizsgaPFG)
* [**https://hu.wikipedia.org/wiki/Kezd%C5%91lap**](https://hu.wikipedia.org/wiki/Kezd%C5%91lap)
* [**https://www.cisco.com/c/dam/global/hu\_hu/products/isr2/1800\_Quick\_Look\_Guide\_HUN.pdf**](https://www.cisco.com/c/dam/global/hu_hu/products/isr2/1800_Quick_Look_Guide_HUN.pdf)
* [**https://szit.hu/doku.php?id=oktatas:halozat:cisco**](https://szit.hu/doku.php?id=oktatas:halozat:cisco)

**A Chat GPT nevezetű mesterséges intelligencia is segített 1-2 dologban!**