**A képen szöveg, Betűtípus, embléma, tervezés látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.ÓSZC Bródy Imre Technikum**

**Informatika és Távközlés**

**Záróvizsga**

4-es csoport

**Készítette:**

Kulin István Dominik

Kiss Károly Alex

Csatári Dominik

**Tartalomjegyzék**

[Bevezetés 3](#_Toc197933562)

[Hálózati topológia 4](#_Toc197933563)

[MPLS 5](#_Toc197933564)

[IPsec VPN 5](#_Toc197933565)

[**Összegzés** 6](#_Toc197933566)

[Eszközök 6](#_Toc197933567)

[Telephelyek 7](#_Toc197933568)

[Hálózati Címzési Terv 8](#_Toc197933569)

[Hálózati Eszközök Konfigurálása 10](#_Toc197933570)

[VLAN beállítása 10](#_Toc197933571)

[HSRP redundancia 11](#_Toc197933572)

[NAT megoldás 14](#_Toc197933573)

[DHCP beállítás 14](#_Toc197933574)

[Szolgáltatások Konfigurálása 14](#_Toc197933575)

[Linux szerver konfiguráció: 14](#_Toc197933576)

[Windows szerver konfiguráció: 19](#_Toc197933577)

[Biztonsági Megoldások 19](#_Toc197933578)

[ACL-ek 19](#_Toc197933579)

[Tűzfalmegoldások 19](#_Toc197933580)

[VPN konfiguráció 19](#_Toc197933581)

[ACL beállítása 19](#_Toc197933582)

[Tesztelés és Dokumentáció 20](#_Toc197933583)

[Melléletek 21](#_Toc197933584)

[Router config file 21](#_Toc197933585)

[Switch config 25](#_Toc197933586)

[Források 28](#_Toc197933587)

# Bevezetés

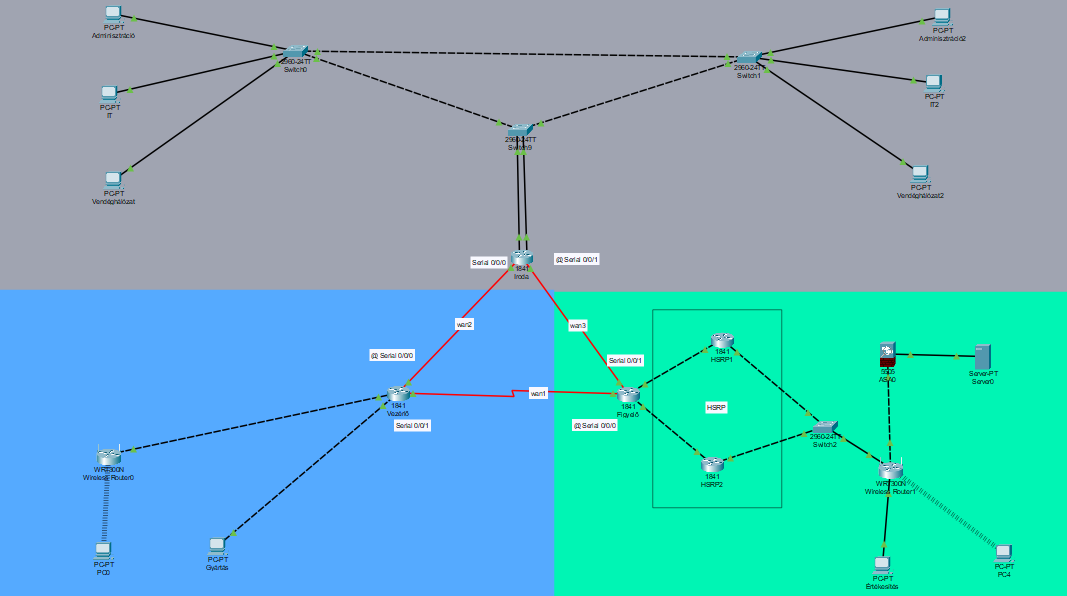
A hálózati infrastruktúra megfelelő tervezése és kivitelezése kulcsfontosságú egy vállalat hatékony működéséhez. A jelen dokumentáció célja egy közepes méretű vállalat három telephelyének hálózati struktúrájának megtervezése, kialakítása és tesztelése, figyelembe véve a modern informatikai követelményeket. A projekt során a hálózatnak biztosítania kell a vállalat üzleti és technikai igényeit, beleértve a stabil és biztonságos belső hálózatot, az internetkapcsolatot, valamint a távoli munkavégzéshez szükséges VPN megoldásokat.

A tervezés során kiemelt szempont a hálózat skálázhatósága, megbízhatósága és védelme, így a redundáns megoldások, a forgalomszabályozás és a biztonsági mechanizmusok (pl. tűzfalak, ACL-ek, VPN-ek) integrációja alapvető követelmény. A dokumentáció bemutatja a hálózati architektúrát, a címzési terveket, a konfigurációs beállításokat, valamint a megvalósított biztonsági intézkedéseket. A tesztelési szakasz célja a megfelelő működés ellenőrzése és az esetleges hibák javítása, így biztosítva a vállalat számára egy megbízható és fenntartható informatikai környezetet.

A dokumentáció további részében részletesen bemutatjuk a hálózati infrastruktúra tervezésének és megvalósításának lépéseit. Ismertetjük a tervezett hálózat felépítését, beleértve a különböző telephelyek közötti kapcsolatokat és a helyi hálózatok struktúráját. Részletezzük a címzési tervet, amely segít az IP-címek kiosztásában és a hálózati eszközök azonosításában. Ismertetjük a hálózati eszközök beállításait, amelyek biztosítják a zökkenőmentes működést és a biztonságos adatátvitelt. Kiemeljük a biztonsági intézkedéseket, mint a tűzfalak és VPN megoldások, amelyek védelmet nyújtanak a hálózati fenyegetésekkel szemben. Végül a tesztelési szakasz során ellenőrizzük a hálózat működését.

# Hálózati topológia

A vállalat három telephelye:

* **Iroda** – fő adatközpont és menedzsment
* **Vezérlő** – gyártás és logisztika
* **Figyelő** – ügyfélszolgálat és értékesítés

A telephelyek közötti hálózati kapcsolatot egy **MPLS-alapú összeköttetés** biztosítja, amely garantálja az alacsony késleltetést és a megbízható adatátvitelt. A biztonság fokozása érdekében egy **IPsec VPN** tartalékkapcsolat is kiépítésre kerül, amely biztosítja a telephelyek közötti kommunikáció folytonosságát hálózati hiba esetén.

Egy további **redundáns összeköttetés** került beépítésre a hálózat stabilitásának növelése érdekében. A hálózati elemek közötti redundáns kapcsolatok meggátolják a hálózat teljes kiesését egy esetleges router vagy switch meghibásodás esetén.

## MPLS

**Mit jelent az MPLS-alapú összeköttetés?**

Az MPLS-alapú összeköttetés egy olyan megoldás, amelyet vállalati hálózatok összekapcsolására használnak, különösen több telephely esetén. Az MPLS segítségével egy szolgáltató **privát, biztonságos és megbízható** hálózatot hoz létre az ügyfél számára, amely lehetővé teszi az adatok gyors és garantált útvonalon történő továbbítását.

**Hogyan működik?**

1. **Címkézés (Labeling):** Az MPLS nem az IP-címek alapján irányítja a csomagokat, hanem **címkéket (label)** rendel hozzájuk.
2. **Gyorsított továbbítás (Label Switching):** Az útválasztók (routerek) az egyes csomagokhoz rendelt címkék alapján döntenek, merre továbbítsák azokat, ahelyett, hogy minden csomagnál újra kiértékelnék az IP-címet.
3. **Minőségbiztosítás (QoS - Quality of Service):** Az MPLS lehetővé teszi a forgalom osztályozását, így például a **hang-, videó- és adatforgalom eltérő prioritást** kaphat.

**Mikor érdemes MPLS-t használni?**

* **Több telephely összekapcsolására (WAN)** – ha több iroda vagy adatközpont között kell biztonságos kapcsolatot biztosítani.
* **Minőségi szolgáltatás (QoS) igény esetén** – például VoIP vagy videókonferencia esetén, ahol fontos az alacsony késleltetés.
* **Biztonságos és megbízható kapcsolat esetén** – az MPLS hálózatokat gyakran magánhálózatként (VPN-ként) használják.

## IPsec VPN

Az **IPsec VPN (Internet Protocol Security Virtual Private Network)** egy olyan technológia, amely titkosított és biztonságos kapcsolatot biztosít két vagy több hálózat között az interneten keresztül.

**Mit jelent az IPsec VPN?**

Az **IPsec (Internet Protocol Security)** egy protokollkészlet, amely biztosítja az adatok **titkosítását, hitelesítését és integritását** IP-alapú hálózatokon. A VPN (Virtual Private Network) pedig egy olyan megoldás, amely lehetővé teszi, hogy egy privát hálózatot hoz létre egy nyilvános hálózaton (például az interneten) keresztül. Az **IPsec VPN** tehát egy olyan VPN megoldás, amely **IPsec protokollokat használ a biztonságos adatkapcsolat kialakítására**.

**Hogyan működik az IPsec VPN?**

1. **Adatok titkosítása:** Az IPsec titkosítja a küldött adatokat, így azokat illetéktelenek nem tudják lehallgatni.
2. **Hitelesítés:** Az IPsec ellenőrzi, hogy a kapcsolat valóban a megfelelő küldőtől és fogadótól származik.
3. **Integritásvédelem:** Biztosítja, hogy az adatok ne sérüljenek meg és ne módosítsák őket az átvitel során.

Az IPsec VPN két fő működési módja:

* **Transport Mode:** Csak az adatcsomag hasznos tartalmát titkosítja (főleg végpontok közötti kommunikációhoz).
* **Tunnel Mode:** A teljes IP-csomagot titkosítja és egy új IP-fejlécet ad hozzá (általában hálózatok közötti biztonságos összeköttetésre használják).

**Miért jó egy IPsec VPN tartalékkapcsolat?**

Ha az MPLS főkapcsolat meghibásodik vagy nem elérhető, az **IPsec VPN képes átterelni a forgalmat az interneten keresztül**, miközben továbbra is **biztosítja az adatok titkosítását és védelmét**. Ez egy **olcsóbb** és rugalmasabb megoldás a redundancia biztosítására.

### **Összegzés**

* **MPLS** → Gyors, garantált, megbízható kapcsolat (de drágább).
* **IPsec VPN tartalék** → Olcsóbb, internetalapú, biztonságos alternatíva hiba esetén.
* Ezzel a kombinációval a hálózat **folyamatos működést** és **adatvédelmet** élvezhet még akkor is, ha az MPLS kapcsolat megszakad.

# Eszközök

A hálózati struktúrában az alábbi eszközök kaptak helyet:

* **Routerek (Cisco 1841)** a három fő csomóponton, redundáns kapcsolatokkal.

Támogatja a VPN funkciókat, valamint tűzfal szolgáltatásokat is kínál. A bővíthetőség érdekében különböző modulok hozzáadására is lehetőség van, így megbízható adatátvitelt biztosít a nagy sávszélességű alkalmazásokhoz. A router támogatja a legfontosabb protokollokat, mint az IP és OSPF így biztosítva a megbízható adatforgalmat.

* **Switch-ek (Cisco 2960-24TT)** az iroda és vezérlő helyi hálózatainak kezelésére.

24 darab 10/100 Ethernet porttal rendelkezik, valamint 2 darab 10/100/1000 SFP porttal a nagyobb sebességű kapcsolatokhoz. A switch támogatja a VLAN-ok létrehozását, lehetővé téve a hálózati forgalom hatékony szegmentálását.

* **ASA tűzfal** a figyelő telephelyen a szerverek és külső kapcsolatok védelmére.

Egy sokoldalú eszköz, amely ideális megoldást nyújt a kis- és középvállalkozások számára. Nyolc 10/100 Ethernet porttal rendelkezik, és képes 150 Mbps tűzfal teljesítményre.

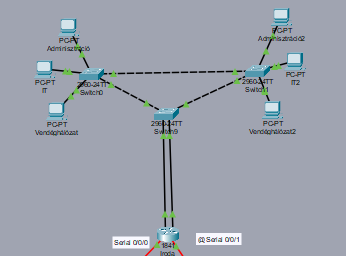
* **Vezeték nélküli routerek (WRT300N)** a vezeték nélküli eszközök támogatásához.

Egy vezeték nélküli eszköz, amely 300 Mbps sebességet kínál. Négy darab 10/100 Ethernet portja lehetővé teszi a vezetékes kapcsolatok létrehozását, míg a WAN port a szélessávú internetkapcsolatot biztosítja. A router támogatja a WPA/WPA2 biztonsági protokollokat, így védelmet nyújt a jogosulatlan hozzáférés ellen.

# Telephelyek

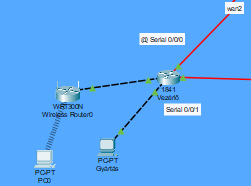
**Iroda (Központi telephely)**

Az iroda a hálózat központi eleme, amely egy adatközpontot, menedzsment funkciókat és több osztályt is kiszolgál. Az itt található eszközök közé tartoznak a **redundáns forgalomirányítók és kapcsolók**, amelyek HSRP vagy VRRP protokollokat alkalmaznak a hálózat rendelkezésre állásának maximalizálása érdekében.

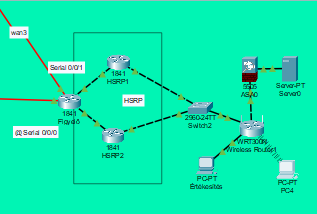
* **VLAN-kialakítás**:
  + VLAN 11: Adminisztráció
  + VLAN 21: IT
  + VLAN 31: Vendéghálózat
* **WLAN hozzáférés** biztosított, 802.1X hitelesítéssel.
* **IPv4/IPv6 támogatás**, statikus és dinamikus címzéssel.
* **Redundáns hálózati kapcsolat** az egyes szegmensek között, amely biztosítja a magas rendelkezésre állást.

**Vezérlő (Gyártás és Logisztika)**

A vezérlő telephely az ipari gyártási folyamatokat és a logisztikai rendszert kezeli. A hálózatnak biztosítania kell a megbízható kapcsolatot az adatközpont és a termelési egységek között.

* **Gyártási VLAN** a vezérlőrendszerek és ipari eszközök elkülönítésére.
* **VPN kapcsolat** az irodai központtal, amely lehetővé teszi a biztonságos adatátvitelt.
* **Helyi DHCP és DNS szolgáltatás redundanciával**, biztosítva a helyi hálózat autonóm működését hálózati probléma esetén is.
* **Redundáns kapcsolat a központi irodával**, amely minimalizálja a hálózati leállások hatását.

**Figyelő (Ügyfélszolgálat és Értékesítés)**

Ez a telephely az ügyfélszolgálati és értékesítési részleg számára biztosít hálózati hozzáférést.

* **Értékesítési VLAN** az ügyféladatok és a vállalati alkalmazások elkülönítésére.
* **WLAN hozzáférés**, vendégek és munkatársak számára egyaránt.
* **NAT/PAT megoldások** az internetkapcsolat hatékony kezelésére.
* **Redundáns kapcsolat a vezérlő telephellyel**, amely biztosítja az üzletmenet folyamatosságát hiba esetén

# Hálózati Címzési Terv

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Telephely** | **VLAN ID** | **IPv4 hálózat** | **IPv6 hálózat** | **Megjegyzés** |
| Iroda | 11 | 192.168.11.0/24 | fd00:11::/64 | Adminisztráció |
| Iroda | 21 | 192.168.21.0/24 | fd00:21::/64 | IT |
| Iroda | 31 | 192.168.31.0/24 | fd00:31::/64 | Vendéghálózat |
| Vezérlő | 41 | 192.168.41.0/24 | fd00:41::/64 | Gyártás |
| Figyelő | 51 | 192.168.51.0/24 | fd00:51::/64 | Értékesítés |
| VPN | - | 10.0.0.0/24 | fd00:100::/64 | VPN hálózat |

A táblázat részletesen bemutatja a hálózati címzési tervet, amely a vállalat különböző telephelyeire vonatkozik. A táblázatban szereplő információk segítenek a hálózati eszközök azonosításában és a forgalom hatékony kezelésében. A VLAN ID-k lehetővé teszik a hálózati szegmensek elkülönítését, míg az IPv4 és IPv6 címek biztosítják a megfelelő címzést a különböző eszközök számára.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Router** | **Hálózat** | **Port** | **dce/dte** | **Cím** |
| Iroda | wan2 | s0/0/0 | dte | 192.168.101.1 |
| Iroda | wan3 | s0/0/1 | dce | 192.168.102.1 |
| Figyelő | wan1 | s0/0/0 | dce | 192.168.103.2 |
| Figyelő | wan3 | s0/0/1 | dte | 192.168.102.2 |
| Vezérlő | wan2 | s0/0/0 | dce | 192.168.101.3 |
| Vezérlő | wan1 | s0/0/1 | dte | 192.168.103.3 |

A táblázat részletesen ismerteti a címzési tervet, amely a három telephelyet összekötő router eszközökre vonatkozik. Tartalmazza az eszközök neveit, a hálózat azonosítóit, a használt interfészeket, valamint a DCE/DTE szerepköröket és az egyes portokhoz rendelt IP-címeket. A WAN kapcsolatokat biztosító soros interfészek megfelelő konfigurációja elengedhetetlen a hálózat stabil működéséhez.

|  |  |  |  |
| --- | --- | --- | --- |
| **Switch** | **Név** | **Port** | **VLAN** |
| switch1 | Adminisztráció | fa0/1 | 11 |
| switch1 | IT | fa0/2 | 21 |
| switch1 | Vendéghálózat | fa0/3 | 31 |
| switch2 | Adminisztráció2 | fa0/1 | 11 |
| switch2 | IT2 | fa0/2 | 21 |
| switch2 | Vendeghálózat2 | fa0/3 | 31 |

A táblázat részletesen bemutatja a hálózati címzési tervet, amely a vállalat különböző telephelyein működő switchekhez tartozik. Tartalmazza az egyes eszközök nevét, a hozzárendelt portokat és a VLAN-azonosítókat. A VLAN-beállítások segítenek elkülöníteni a hálózat különböző részeit és felhasználóit.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Név** | **Port** | **Cím** | **Alhálózati maszk** | **Átjáró** | **DNS** |
| vezérlő router | fa0/0 | 192.168.41.1 | - | - | - |
| vezérlő router | fa0/1 | 192.168.42.1 | - | - | - |
| figyelő router | fa0/0 | 192.168.51.1 | - | - | - |
| figyelő router | fa0/1 |  | - | - | - |
| pc (gyártás) | fa0/0 | 192.168.41.4 | - | - | - |
| wifi | Internet | 192.68.42.2 | 255.255.255.255 | 192.168.42.1 | 5.4.3.2 |
| wifi2 | Internet | 192.168.51.2 | 255.255.255.255 | 192.168.51.1 | 5.4.3.2 |

A táblázat a vállalat hálózati eszközeinek konfigurációját mutatja be. A két wireless router esetében a táblázatban szerepel: alhálózati maszk, amely lehetővé teszi, hogy az eszközök azonosítani tudják, melyik hálózati tartományba esik egy adott IP-cím. A DNS szerver segít, hogy az eszközök domian neveket IP-címeket alakítsanak át. Az átjáró biztosítja a kapcsolatot a helyi hálózat és más hálózatok, például az Internet között.

# Hálózati Eszközök Konfigurálása

A hálózat gerincét routerek és switch-ek alkotják, amelyek megfelelő konfigurációja elengedhetetlen a stabil és biztonságos működéshez.

VLAN konfigurálás és Inter-VLAN routing: A hálózat megfelelő szegmentálása érdekében VLAN-ok kerülnek létrehozásra. Az egyes VLAN-ok közötti forgalmat egy Layer 3 switch vagy egy router kezeli Inter-VLAN routing segítségével.

HSRP/VRRP redundancia: Az elérhetőség növelése érdekében a redundancia megoldásokat alkalmazunk, így a HSRP vagy VRRP segítségével egy tartalék eszköz is készen áll a hálózati forgalom kezelésére meghibásodás esetén.

WLAN biztonság: A vezeték nélküli hálózat WPA3 titkosítással működik, amely biztosítja az illetéktelen hozzáférések elleni védelmet. Ezen felül 802.1X hitelesítést is alkalmazunk.

Routing protokollok: Az OSPFv2 és OSPFv3 protokollokat használjuk a hatékony és dinamikus útvonalválasztás érdekében, míg az EIGRP gyors konvergenciát biztosít.

NAT/PAT megoldások: A Figyelő telephelyen alkalmazott NAT és PAT lehetővé teszi a privát IP-címek nyilvános címekké történő átalakítását, ezáltal biztosítva az internetkapcsolatot.

## VLAN beállítása

A VLAN (Virtual Local Area Network) létrehozása lehetővé teszi, hogy egy hálózaton belül különböző szegmenseket alakítsunk ki, amelyek logikailag elkülönítik egymást, miközben fizikailag ugyanazon a hálózaton osztoznak. A VLAN konfigurálása során fontos, hogy az eszközök és portok megfelelően legyenek hozzárendelve a VLAN-okhoz. A VLAN-ok használata egyszerűsíti a hálózatok kezelését és növeli a biztonságot.

A VLAN-ok konfigurálásához az alábbi lépések szükségesek:

1. **Jelszavak beállítása:**

*enable secret jelszo* – enable jelszó beállítása

*username admin privilege 15 secret jelszo* - Helyi felhasználó (admin) jelszó beállítása

*line consol 0*

*password jelszo* - Konzol jelszó beállítás

*login*

*line vty 0 4*

*password jelszo* - Távoli hozzáférés jelszó beállítása

*login*

1. **VLAN létrehozása**:
   * **vlan <ID>** parancs a kívánt VLAN létrehozásához.
   * **name <név>** a VLAN név hozzárendeléséhez.
2. **Portok hozzárendelése**:
   * **interface <port>** a kívánt port kiválasztása.
   * **switchport mode access** a port hozzáférési módba állítása.
   * **switchport access vlan <ID>** a port VLAN-hoz rendelése.
3. **Portok ellenőrzése**:
   * **show vlan brief** a VLAN állapotának és hozzárendelt portjainak megjelenítéséhez használt parancs.

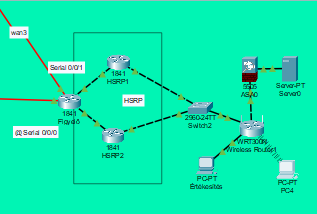
## HSRP redundancia

A távoli hálózatok eléréséhez alapértelmezett átjárót használunk, amely jellemzően a legközelebbi forgalomirányító interfészét jelöli, és az IP-címével hivatkozunk rá. Az alapértelmezett átjáró egyetlen kommunikációs végpontot szolgál ki így, ha meghibásodik, a hálózati elérhetőség problémákat okozhat. Ennek elkerülésére fejlesztették ki az FHRP (First Hop Redundancy Protocol) protokollokat.

A redundancia protokollok biztosítják, hogy a forgalom átirányítása megfelelően történjen, és meghatározzák, hogy a forgalmat melyik valódi forgalomirányító végezze. Ezenkívül a protokollok szabályozzák, hogy mikor kell átadni a továbbító szerepét egy készenléti forgalomirányítónak. A végberendezések számára a szerepváltás észrevétlen marad.

A hibatűrő forgalomirányító működése: Amennyiben az aktív forgalomirányító meghibásodik, a redundancia protokoll automatikusan átállítja a készenléti forgalomirányítót aktív állapotba. Ennek folyamata a következő lépésekből áll:

* A készenléti (standby) forgalomirányító nem kap Hello üzeneteket az aktív forgalomirányítótól.
* A tartalék forgalomirányító átveszi a továbbító forgalomirányító szerepét.
* Mivel az új továbbító forgalomirányító átveszi a virtuális forgalomirányító IP- és MAC-címét is, a hálózati állomások számára a szolgáltatás folytatódik, és nem tapasztalható megszakítás.

A HSRP (Hot Standby Router Protocol) egy Cisco által kifejlesztett protokoll, amely redundanciát biztosít a forgalomirányítók között. Célja, hogy a hálózati eszközök számára egyetlen virtuális alapértelmezett átjárót jelenítsen meg. A protokoll biztosítja, hogy ha az aktív forgalomirányító meghibásodik, egy passzív forgalomirányító átvegye a szerepét, így elkerülve a hálózati megszakadásokat.

*#standby 1 ip 192.168.55.5*

*#standby 1 priority 150*

*#standby 1 preempt*

*#standby 2 ip 192.168.55.5*

*#standby 2 priority 100*

*#standby 2 preempt*

WPA titkosítás

A WPA3 titkosítás a legújabb Wi-Fi biztonsági szabvány, amely erősebb védelmet biztosít a vezeték nélküli hálózatok számára. A WPA3 többek között javítja a jelszókezelést, fokozza a védekezést a brute-force támadások ellen, és biztonságosabb titkosítást biztosít, különösen nyilvános hálózatokon. Azonban mivel a WPA3 nem minden eszközzel kompatibilis, nem volt kivitelezhető a teljes körű implementálása, így a WPA2 titkosítást alkalmazzuk.

A WPA2 titkosítás az egyik legelterjedtebb és legmegbízhatóbb megoldás a vezeték nélküli hálózatok védelmére. A WPA2 az AES titkosítást alkalmazza, amely az egyik legerősebb titkosítási algoritmus. Emellett védelmet nyújt a hálózati forgalom lehallgatásával szemben, és meggátolja az illetéktelen hozzáférést a Wi-Fi hálózathoz. A WPA2 széles körben elterjedt, és bár nem kínálja azokat a fejlesztéseket, amelyeket a WPA3, még mindig rendkívül biztonságos megoldást jelent a legtöbb felhasználó számára.

*Az alábbiakban részletesen bemutatjuk a WPA2 néhány biztonsági előnyét:*

**Erős titkosítás (AES)**

A WPA2 a rendkívül biztonságos Advanced Encryption Standard (AES) titkosítást alkalmazza, amely blokkonként védi az adatokat. Az AES 128, 192 vagy 256 bites kulcsmérettel működik, és még modern számítási kapacitással is rendkívül nehéz feltörni. Ez a titkosítási technológia garantálja, hogy a vezeték nélküli hálózatokon továbbított adatok biztonságban maradjanak, megakadályozva a jogosulatlan hozzáférést.

**Egyedi kulcshasználat**

A WPA2 minden adatátvitelhez egyedi titkosítási kulcsot hoz létre a négyutas kézfogási folyamat során. Ez biztosítja, hogy minden kapcsolat saját kulccsal védett, amelyet csak az adott eszközök ismernek, így csökkentve az adatok elfogásának és dekódolásának kockázatát.

**Integritásellenőrzés (TKIP)**

A WPA2 olyan beépített biztonsági mechanizmusokat tartalmaz, amelyek garantálják az adatcsomagok sértetlenségét. A Temporal Key Integrity Protocol (TKIP) segítségével képes észlelni és blokkolni az adatforgalom módosítására irányuló támadásokat. Ez különösen hatékony védelmet biztosít a közbeékelődéses (man-in-the-middle) támadások ellen, mivel azonnal észlelhetővé válik, ha egy illetéktelen fél megpróbálja manipulálni a hálózaton továbbított adatokat.

OSPFv2 Protokoll

Az Open Shortest Path First (OSPF) egy dinamikus útvonalválasztási protokoll, amelyet nagy és összetett IP-hálózatok hatékony kezelésére terveztek. Az OSPF kapcsolatállapot-alapú (link-state) protokoll, amely gyors konvergenciát biztosít és támogatja a hálózat hierarchikus felépítését. A protokoll az alábbi főbb jellemzőkkel bír:

* **Hierarchikus felépítés:** Az OSPF területekre (area) osztja a hálózatot, amely növeli a skálázhatóságot és csökkenti az útvonalválasztási táblák méretét.
* **Költségalapú útválasztás:** Az OSPF az interfészek költségét használja az útvonal kiválasztására. Az alacsonyabb költségű útvonalakat preferálja.
* **Gyors konvergencia:** Az OSPF gyorsan alkalmazkodik a hálózat változásaihoz, és csak az érintett hálózatokat frissíti.
* **Hitelesítés:** Támogatja a hitelesítési mechanizmusokat az adatforgalom biztonságának növelésére.

**OSPF konfigurálása egy routeren:**

Az alábbi példa egy router OSPF beállítását mutatja három különböző hálózatra, mindegyik az area 0-hoz tartozik:

*router ospf 115*

*log-adjacency-changes*

*network 192.168.11.0 0.0.0.255 area 0*

*network 192.168.21.0 0.0.0.255 area 0*

*network 192.168.31.0 0.0.0.255 area 0*

Ebben a konfigurációban:

* Az **OSPF 115**-ös folyamata engedélyezve van.
* Három hálózat került beállításra az **area 0**-ban.
* A **log-adjacency-changes** parancs engedélyezi a kapcsolati állapot változásainak naplózását.
* A wildcard maszk segítségével az adott hálózatokat specifikáltuk.

Az OSPF megfelelő beállítása biztosítja a hálózat megbízható és hatékony működését, valamint optimalizálja az útvonalválasztási döntéseket.

## NAT megoldás

A NAT (Network Address Translation) olyan hálózati megoldás, amely a helyi (privát) IP-címeket nyilvános IP-címekre cseréli, miközben lehetővé teszi, hogy több eszköz osztozzon ugyanazon a nyilvános IP-címen.

A NAT három fő típusa:

* **Statikus NAT,** ahol egy privát IP-t egy fix nyilvános IP-hez rendelnek
* **dinamikus NAT,** amely egy IP-címkészletet oszt ki a privát címekhez
* **kiterjesztett NAT (Port Address Translation - PAT),** amely több privát IP-t egy nyilvános IP-n keresztül kezeli különböző portokkal.

A NAT segít a hálózatok védelmében, csökkenti az IP-címek igényét és biztosítja a belső hálózat védelmét az internetes támadásokkal szemben.

## DHCP beállítás

*#ip dhcp excluded-address 192.168.41.1 192.168.41.10*

*#ip dhcp pool lan1*

*#network 192.168.41.0 255.255.255.0*

*#default-router 192.168.41.1*

*#dns-server 4.3.2.1*

*#end*

# Szolgáltatások Konfigurálása

## Linux szerver konfiguráció:

DHCP szerver: Automatikus IP-cím kiosztás a hálózat eszközei számára.

DNS szerver: Névfeloldás biztosítása a belső hálózaton belül.

HTTP/HTTPS szerver: A belső vállalati portál és webszolgáltatások futtatása.

Biztonsági mentések: Rendszeres mentések tárolása NAS eszközön vagy felhőalapú tárhelyen.

**IP-cím beállítása:** szerver IP címe

*nano /etc/network/interfaces*

*auto 1o*

*iface 1o inet loopback*

allow-hotplug enp1s0

*iface enp0s3 inet static*

*address 192.168.10.1*

*netmask 255.255.255.0*

*ifdown enp0s3*

*ifup enp0s3*

**Telepítés**

*apt install isc-dhcp-server*

Telepítés után a program nem indul el, hibát jelez. Elvégezzük a beállításokat.

**Alap:** Telepítés után létrejön a **/etc6dhcp/dhcp.conf** állomány. Itt felvehetünk alhálózatokat, amelyek részére IP címet szolgáltatunk.

*option domain-name „név”;*

*optiopn domain-name-servers 192.168.10.1, 8.8.8.8;*

*default-lease-time 600;*

*max-lease-time 7200;*

*subnet 192.168.10.0 netmask 255.255.255.0 {*

*range 192.168.10.0 192.168.10.254;*

*option routers 192.168.10.1; }*

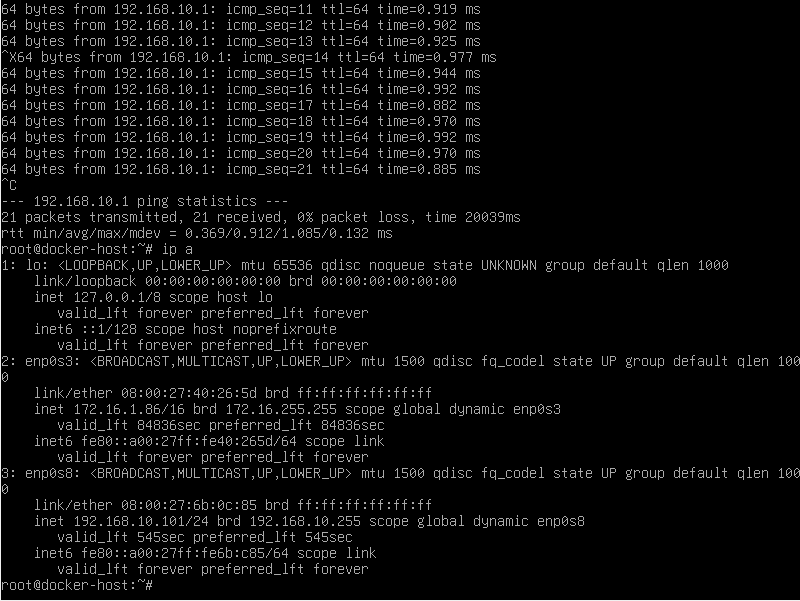
A **/etc/default/isc-server** fájlban beállítjuk a hálózatikártyát.

*INTERFACESv4=”enp0s3”*

**Tesztelés:**

*dhcp -t*

**Újraindítás:** Újra indítjuk a DHCP szervert.

** *systemctl start isc-dhcp-server*

**BIND9 telepítése és alap konfigurálása**

**Telepítés**

*sudo apt update*

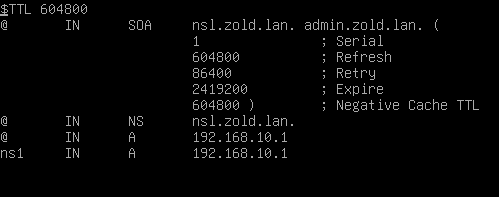
*sudo apt install bond9 bind9utils bind9-doc -y*

**Zónafájl előkészítése**

Példa: saját zóna example.local létrehozása.

**Létrehozunk egy zónafájlt**

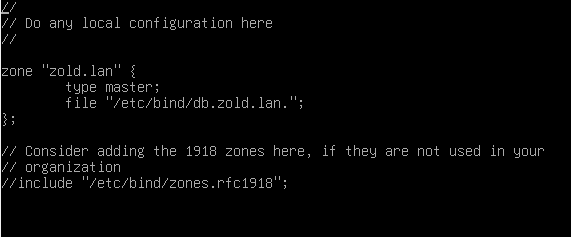
*sudo nano /etc/bind/db.example.local*



**Zónafájl hozzáadása a named.conf.local fájlhoz**

*sudo nano /etc/named.conf.local*

Hozzáadjuk:



**Konfiguráció ellenőrzése:**

*sudo named.checkconf*

*sudo named-checkzone example.local /etc/bind/db.example.local*

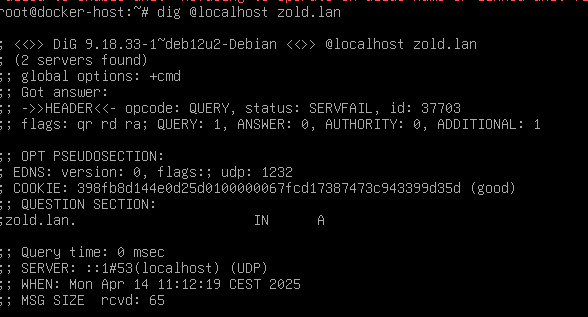
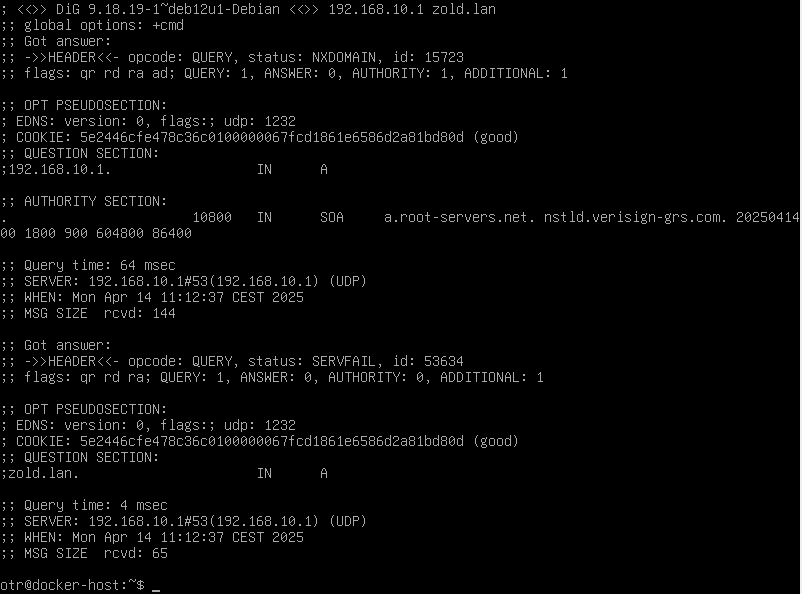
**Szolgáltatás újraindítása**

*sudo systemctl restart bind9*

*sudo systemctl enable bind9*

**Tesztelés**

*dig @localhost example.local*

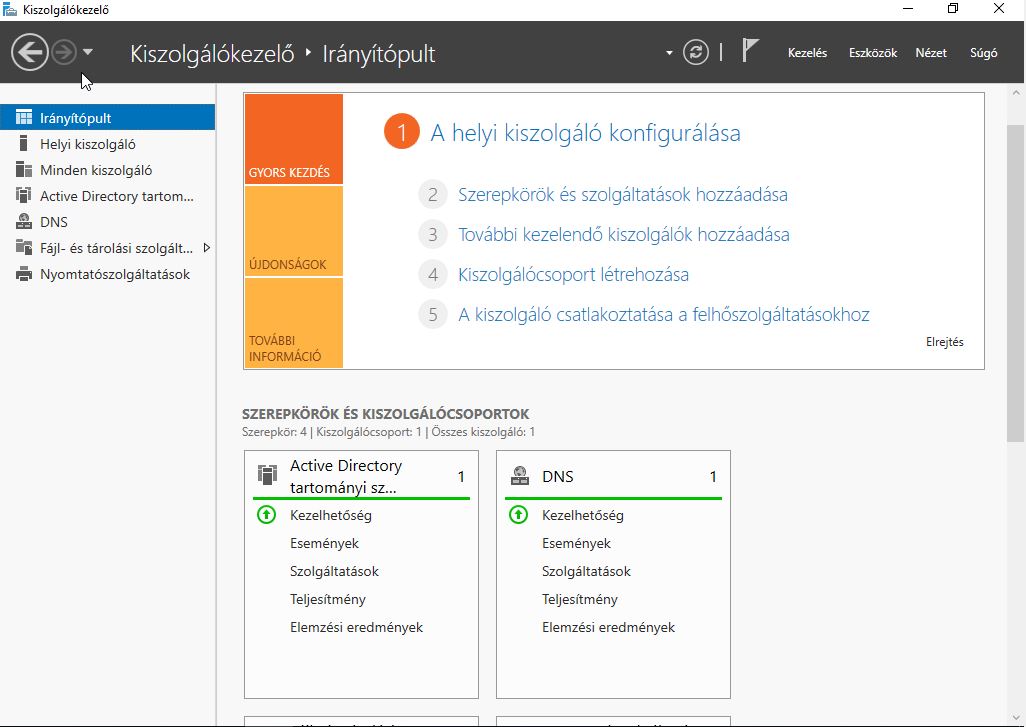


## Windows szerver konfiguráció:

Active Directory (AD): A felhasználók és eszközök központi menedzsmentje.

Fájlszerver és nyomtatómegosztás: Dokumentumok és nyomtatók központi kezelése és megosztása.

Csoportházirendek (GPO-k): A vállalati biztonsági és működési szabályok érvényesítése.



# Biztonsági Megoldások

ACL-ek (Hozzáférési listák): A hálózati hozzáférési szabályokat ACL-ek segítségével határozzuk meg, amelyek korlátozzák az illetéktelen hozzáféréseket és biztosítják az érzékeny adatok védelmét.

Tűzfalmegoldások: Cisco ASA vagy pfSense tűzfalakat alkalmazunk a hálózat külső és belső fenyegetésekkel szembeni védelmére, szűrve a bejövő és kimenő forgalmat.

VPN konfiguráció: Az IPsec-alapú VPN biztonságos kommunikációt biztosít a telephelyek között, valamint a távoli munkavégzést végző dolgozók számára.

## ACL beállítása

Az ACL (Access Control List) egy hálózati szűrési mechanizmus, amely szabályokat határoz meg a forgalom engedélyezésére vagy tiltására egy adott eszközön, például egy routeren vagy tűzfalon. Az ACL-ek segítségével korlátozható a hozzáférés bizonyos IP-címekhez, hálózatokhoz vagy protokollokhoz, növelve ezzel a biztonságot és a hálózati forgalom irányítását. Két fő típusa van: a standard ACL, amely csak az IP-forráscím alapján szűr, és az extended ACL, amely több kritériumot, például célcímet és protokollt is figyelembe vesz.

Ebben az esetben egy egyszerű hozzáférési alkalmaztunk annak érdekében, hogy a Vezérlő wifi hálózata ne tudja elérni a gyártást. Ehhez egy standard ACL-t használtunk, amely az IP-cím alapján szűri meg a forgalmat.

A konfigurációban az alábbi két szabály biztosítja, hogy a Vezérlő Wi-fi hálózata ne férjen hozzá a gyártási szegmenshez:

*access-list 1 deny 192.168.41.0 0.0.0.255*

*access-list 1 permit any*

*#interface fastetherne 0/1*

*#ip access-group 1 out*

Az első parancs tiltja a gyártási hálózat elérését, míg a második engedélyez minden más forgalmat.

# Tesztelés és Dokumentáció

Ping és traceroute tesztek: Az elérhetőség és a hálózati útvonalak ellenőrzése.

ACL-ek és VLAN-ok tesztelése: Az egyes biztonsági és szegmentációs beállítások működésének ellenőrzése.

VPN kapcsolatok ellenőrzése: A titkosított adatforgalom és a távoli elérések tesztelése.

Hálózati teljesítmény mérése: A sávszélesség, késleltetés és csomagvesztés vizsgálata.

Redundancia tesztelése: A HSRP/VRRP és egyéb redundáns megoldások megfelelő működésének szimulációja, meghibásodási szcenáriók modellezésével.

**\*Iroda mindent lát, szervert mindenhonnan el lehet érni, a többi csak a saját kis részét, vlan-ját\***

## Melléletek

# Router config file

*Iroda*

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Iroda

enable secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

no ip cef

no ipv6 cef

username admin privilege 15 secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

spanning-tree mode pvst

interface FastEthernet0/0

no ip address

duplex auto

speed auto

interface FastEthernet0/1

ip address 192.168.10.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1.11

encapsulation dot1Q 11 native

ip address 192.168.11.1 255.255.255.0

interface FastEthernet0/1.21

encapsulation dot1Q 21

ip address 192.168.21.1 255.255.255.0

interface FastEthernet0/1.31

encapsulation dot1Q 31

ip address 192.168.31.1 255.255.255.0

interface Serial0/0/0

ip address 192.168.101.1 255.255.255.0

interface Serial0/0/1

ip address 192.168.102.1 255.255.255.0

clock rate 2000000

interface Ethernet0/1/0

ip address 192.168.52.1 255.255.255.0

duplex auto

speed auto

interface Vlan1

no ip address

shutdown

router ospf 115

log-adjacency-changes

network 192.168.11.0 0.0.0.255 area 0

network 192.168.21.0 0.0.0.255 area 0

network 192.168.31.0 0.0.0.255 area 0

router rip

ip classless

ip flow-export version 9

line con 0

exec-timeout 5 0

password jelszo

logging synchronous

login

line aux 0

line vty 0 4

password jelszo

login

end

Vezérlő

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Vezerlo

enable secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

no ip cef

no ipv6 cef

username admin privilege 15 secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 192.168.41.1 255.255.255.0

duplex auto

speed auto

interface FastEthernet0/1

ip address 192.168.42.1 255.255.255.0

duplex auto

speed auto

interface Serial0/0/0

ip address 192.168.101.3 255.255.255.0

clock rate 2000000

interface Serial0/0/1

ip address 192.168.103.3 255.255.255.0

interface Ethernet0/1/0

ip address 192.168.53.2 255.255.255.0

duplex auto

speed auto

interface Vlan1

no ip address

shutdown

ip classless

ip flow-export version 9

line con 0

exec-timeout 5 0

password jelszo

logging synchronous

login

line aux 0

line vty 0 4

password jelszo

login

end

Figyelő

version 12.4

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Figyelo

enable secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

no ip cef

no ipv6 cef

username admin privilege 15 secret 5 $1$mERr$wB3NZSHhqFlanwjPTagF.1

spanning-tree mode pvst

interface FastEthernet0/0

ip address 192.168.56.2 255.255.255.0

duplex auto

speed auto

ipv6 address FD00:51::1/64

ipv6 enable

interface FastEthernet0/1

ip address 192.168.55.2 255.255.255.0

duplex auto

speed auto

interface Serial0/0/0

ip address 192.168.103.2 255.255.255.0

clock rate 2000000

interface Serial0/0/1

ip address 192.168.102.2 255.255.255.0

interface Vlan1

no ip address

shutdown

router rip

network 192.168.55.0

network 192.168.56.0

ip classless

ip flow-export version 9

line con 0

exec-timeout 5 0

password jelszo

logging synchronous

login

line aux 0

line vty 0 4

password jelszo

login

end

# Switch config

version 15.0

no service timestamps log datetime msec

no service timestamps debug datetime msec

no service password-encryption

hostname Switch

spanning-tree mode pvst

spanning-tree extend system-id

interface FastEthernet0/1

switchport trunk allowed vlan 11-51

switchport mode trunk

interface GigabitEthernet0/1

switchport trunk allowed vlan 11-51

switchport mode trunk

interface FastEthernet0/2

switchport access vlan 11

switchport trunk allowed vlan 11-51

switchport mode trunk

interface GigabitEthernet0/2

switchport access vlan 21

switchport trunk allowed vlan 11-51

switchport mode trunk

interface Vlan1

no ip address

shutdown

line con 0

line vty 0 4

login

line vty 5 15

login

end

# Források

Eszközleírások

<https://www.router-switch.com/pdf2html/pdf/cisco1841-datasheet.pdf>

<https://www.router-switch.com/pdf2html/pdf/ws-c2960-24tt-l-datasheet.pdf>

<https://www.router-switch.com/pdf2html/pdf/asa5505-bun-k9-datasheet.pdf>

<https://downloads.linksys.com/downloads/datasheet/1224638994502/WRT300N-EU_ds.pdf>

Hálózati elemek

<https://szit.hu/doku.php?id=oktatas:halozat:cisco>

<https://www.cisco.com/c/en/us/support/index.html>