1. **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.

1. **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.

**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.

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).

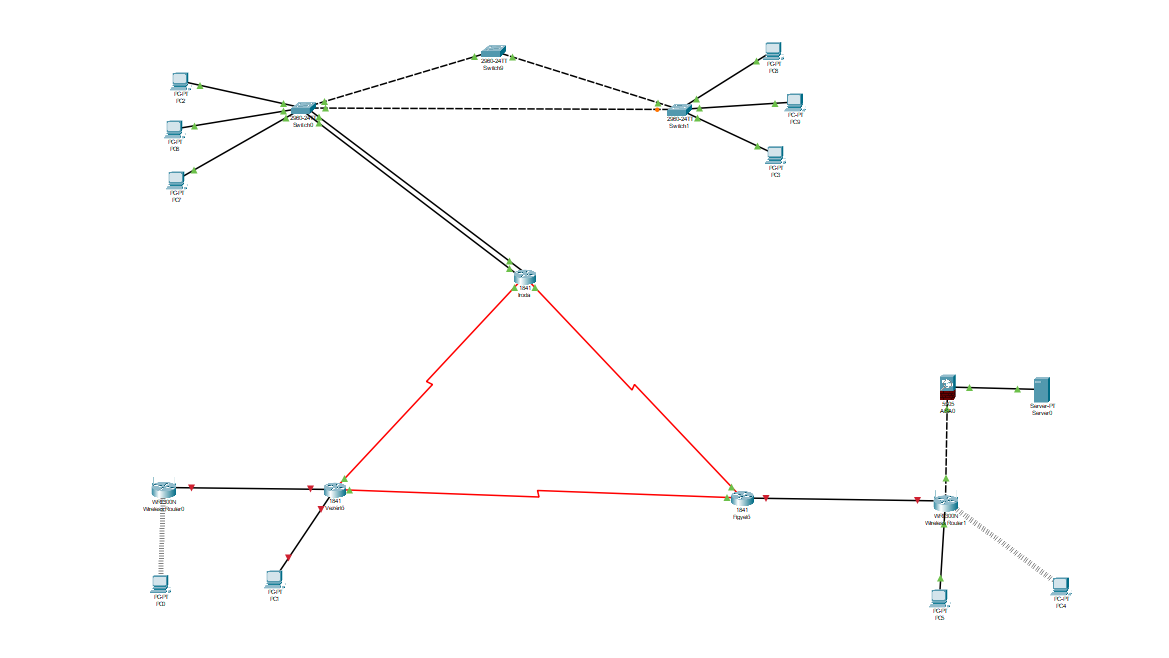
**Miért jó egy IPsec VPN tartalékkapcsolat?**

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.

r

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.

**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

1. **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.

1. **Hálózati Eszközök Konfigurálása**

* **Routerek és kapcsolók**: VLAN konfigurálás, Inter-VLAN routing, HSRP/VRRP redundancia.
* **WLAN**: WPA3 titkosítás és 802.1X hitelesítés.
* **Routing protokollok**: OSPFv2, OSPFv3, EIGRP.
* **NAT/PAT megoldások** a Figyelő telephelyen.

1. **Biztonsági Megoldások**

* **ACL-ek** az érzékeny adatok védelmére.
* **Tűzfal** (pl. Cisco ASA vagy pfSense).
* **VPN konfiguráció**: IPsec-alapú biztonságos kommunikáció.

1. **Szolgáltatások Konfigurálása**

* **Linux szerver**: DHCP, DNS, HTTP/HTTPS, mentés.
* **Windows szerver**: Active Directory, fájl- és nyomtatómegosztás, csoportházirend.

1. **Tesztelés és Dokumentáció**

* **Ping, traceroute** tesztek.
* **ACL-ek, VLAN-ok és VPN ellenőrzése.**