## Leírás: logoDEBRECENI SZAKKÉPZÉSI CENTRUM BRASSAI SÁMUEL MŰSZAKI TECHNIKUM

### 4029 Debrecen, Víztorony u. 3.

### OM: 203033/099

PORTFÓLIÓ

### Köteles Ádám 13.b Papp László Nimród 13.b

### Szilágyi Gábor 13.b

Az ágazat megnevezése: **Informatika és Távközlés**

A szakma megnevezése: **Informatikai Rendszer-és Alkalmazás-üzemeltetői technikus**

A szakma azonosító száma: **506121202**

**Debrecen**

**2025**

A képen szöveg, levél, Betűtípus, papír látható

Előfordulhat, hogy a mesterséges intelligencia által létrehozott tartalom helytelen.

**Tartalom**

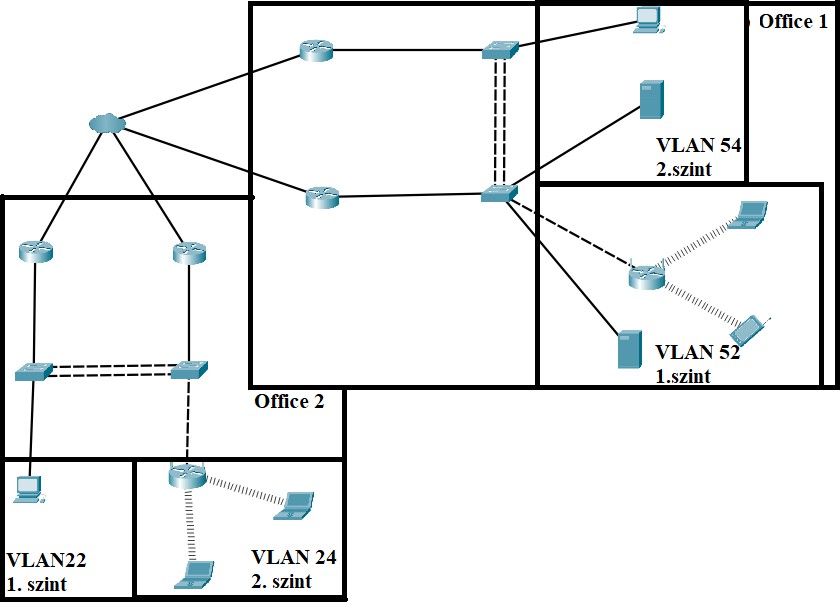
1. [Cégbemutatás 3](#_bookmark0)
2. [VTEC Hálózati topológia bemutatása 3](#_bookmark1)
   1. [Eszközök Használata 4](#_bookmark2)
   2. [Címzési Terv 4](#_bookmark3)
   3. [Alkalmazott Technológiák 6](#_bookmark4)
   4. [Eszközök Részletes Bemutatása 7](#_bookmark5)
   5. [Eszköz Konfigurációk Bemutatása 10](#_bookmark6)
   6. [Programozott Hálózatkonfiguráció 45](#_bookmark7)
3. [Tesztelés 48](#_bookmark8)
4. [Összefoglalás 50](#_bookmark9)
5. [Konfigurációs melléklet 52](#_bookmark10)
6. [Források 78](#_bookmark11)

# Cégbemutatás

A Virtual Technology Engineering Company (VTEC) egy vezető technológiai vállalat, amely innovatív megoldásokat nyújt a virtuális infrastruktúrák, hálózatok és mérnöki szolgáltatások terén. A Vállalat 2024-ben lett alapítva Debrecenben. A vállalat két irodát működtet: az egyik Debrecenben (Office 1) a másik pedig Berlinben (Office 2). A két iroda közötti kommunikáció biztosítására egy GRE Tunnel áll rendelkezésre. Ezek az irodák korszerű hálózati technológiákkal vannak felszerelve, amelyek biztosítják az adatkezelés és a kommunikáció hatékonyságát. A Vállalat hálózat karbantartással, építéssel, fejlesztéssel, weboldalak üzemeltetésével foglalkozik.

# VTEC Hálózati topológia bemutatása

A következő képen található a VTEC irodák hálózati topológiája:



# Eszközök Használata

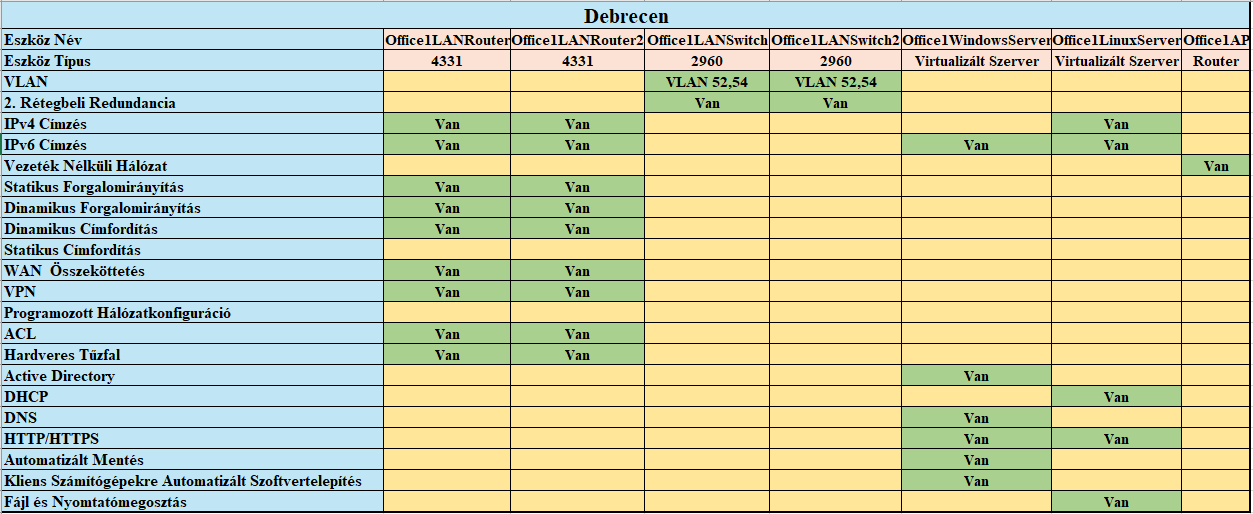
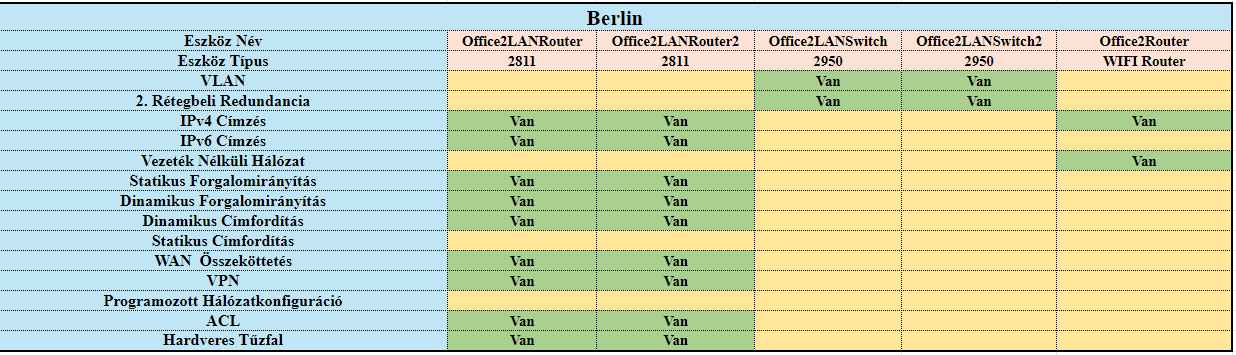
|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **4331**  **Router** | **2811**  **Router** | **2960**  **Switch** | **2950**  **Switch** | **Server** | **Wifi Router** | **Wifi AP** | **Telefon** | **Laptop** |
| **2 db** | **2 db** | **2 db** | **2 db** | **2 db** | **1 db** | **1 db** | **1 db** | **3 db** |

# Címzési Terv

|  |  |  |  |
| --- | --- | --- | --- |
| 172.16.0.0 | 24 | Network | OFFICE2 VLAN22 |
| 172.16.0.1 | 24 | FastEthernet0/0.2  2 | OFFICE2Router |
| 172.16.0.2 | 24 | FastEthernet0/0.2  2 | OFFICE2Router2 |
| DHCP |  |  | OFFICE2 VLAN22 |
| 172.16.0.50  -100 | 24 |  |  |
| 172.16.1.0 | 24 | Network | OFFICE2 VLAN24 |
| 172.16.1.1 | 24 | FastEthernet0/0.2  4 | OFFICE2Router |
| 172.16.1.2 | 24 | FastEthernet0/0.2  4 | OFFICE2Router2 |
| DHCP |  |  | OFFICE2 VLAN24 |
| 172.16.1.50  -100 | 24 |  |  |
| 172.168.0.0 | 24 | Network | OFFICE1 VLAN52 |
| 172.168.0.1 | 24 | GigabitEthernet0/  0/0.52 | OFFICE1Router |
| 172.168.0.2 | 24 | GigabitEthernet0/  0/0.52 | OFFICE1Router2 |
| 172.168.0.3 | 24 |  | OFFICE1 Linux Server |
| DHCP |  |  | OFFICE1 VLAN52 |
| 172.168.0.5  0-100 | 24 |  |  |
| 172.168.1.0 | 24 | Network | OFFICE1 VLAN54 |
| 172.168.1.1 | 24 | GigabitEthernet0/  0/0.54 | OFFICE1Router |
| 172.168.1.2 | 24 | GigabitEthernet0/  0/0.54 | OFFICE1Router2 |
| 172.168.1.3 | 24 |  | OFFICE1 Windows  Server |
| DHCP |  |  | OFFICE1 VLAN54 |

|  |  |  |  |
| --- | --- | --- | --- |
| 172.168.1.5  0-100 | 24 |  |  |
| 192.168.0.0 | 30 | Network | GRE-Tunnel |
| 192.168.0.1 | 30 | Tunnel0 | OFFICE1Router |
| 192.168.0.2 | 30 | Tunnel0 | OFFICE2Router |
| 192.168.0.4 | 30 | Network | GRE-Tunnel |
| 192.168.0.5 | 30 | Tunnel0 | OFFICE1Router2 |
| 192.168.0.6 | 30 | Tunnel0 | OFFICE2Router2 |
| 2001:DB8:5  4:54:: | 64 |  | OFFICE1 VLAN54 |
| 2001:DB8:5  4:54::1 | 64 | GigabitEthernet  1/0.54 | OFFICE1 Router |
| FE80::54 |  |  | OFFICE1 Router |
| 2001:DB8:5  4:54::2 | 64 | GigabitEthernet  1/0.54 | OFFICE1 Router2 |
| FE80::55 |  |  | OFFICE1 Router2 |
| 2001:DB8:5  4:54:: | 64 |  | OFFICE1 VLAN52 |
| 2001:DB8:5  2:52::1 | 64 | GigabitEthernet  1/0.52 | OFFICE1 Router |
| FE80::54 |  |  | OFFICE1 Router |
| 2001:DB8:5  2:52::2 | 64 | GigabitEthernet  1/0.52 | OFFICE1 Router2 |
| FE80::55 |  |  | OFFICE1 Router2 |
| 2001:DB8:5  2:52::3 | 64 |  | OFFICE1 Linux Server |
| 2001:DB8:5  4:54::3 | 64 |  | OFFICE1 Windows  Server |

# Alkalmazott Technológiák



*SEQ ábra \\* ARABIC 76. ábra Címzési Terv. A kép saját szerkesztés.*

# Eszközök Részletes Bemutatása

**4331 Router:** A Cisco 4000 Series családjába tartozik. Az eszközön 2 darab GigabitEthernet Interface található. Az eszköz 100 Mbps-től akár gigabites sávszélességet is támogat. Rendelkezik Integrált Szolgáltatásokkal: VPN, Tűzfal. Az eszköz támogatja a hálózat bővítését és testre szabását különféle bővítő modullal. 4331 router előnyei: Biztonság pl.: VPN, Tűzfal támogatása, Rugalmasság pl.: Bővíthetőség a hálózati igény szerint. 2 darab eszközt alkalmazunk az OFFICE 1-ben. Egy Site To Site VPN-t alkalmaztunk GRE Tunnel-re az Office

1 és Office 2 közöti kommunikáció biztosítására. A Két Office közötti dinamikus forgalomirányítást GRE Tunnel-ön keresztül OSPF segítségével valósítottuk meg. A portok szűrésére Zónázó Tűzfalakat (Zone Based Policy Firewall) használunk. Harmadik Rétegbeli redundanciát a GLBP biztosítja (Gateway Load Balancing Protocoll). Az eszközöket távoli hozzáféréssel is lehet konfigurálni SSH használatával. Az internet irányába Alapértelmezett Útvonalat (Default Route) alkalmazunk. A Belső privát hálózati címek publikus címre fordításához NAT/PAT-ot használunk. Egy publikus címre lesz fordítva az összes belső privát cím PAT Használatával.

**2811 Router:** A Cisco 2800 Series családjába tartozik. Az eszközön 2 darab FastEthernet Interface található. Ez az eszköz 10, illetve 100 Mbps sávszélességet támogat. Az eszköz támogat többféle biztonsági funkciót, mint pl.: Tűzfal, VPN. A tűzfal beépített állapotvizsgáló funkcióval rendelkezik. Illetve támogatja az IPsec és SSL VPN-t. 2 darab 2811- es routert használunk a hálózatban. Egy Site To Site VPN-t alkalmaztunk GRE Tunnel-re az Office 1 és Office 2 közöti kommunikáció biztosítására. A Két Office közötti dinamikus forgalomirányítást GRE Tunnel-ön keresztül OSPF segítségével valósítottuk meg. Az eszközöket távoli hozzáféréssel is lehet konfigurálni SSH használatával. 2811 router az OFFICE 2 hálózatában található, amiken pedig ezeket a szolgáltatásokat, illetve protokollokat alkalmaztunk: A Belső privát hálózati címek publikus címre fordításához NAT/PAT-ot használunk. Egy publikus címre lesz fordítva az összes belső privát cím PAT Használatával. Harmadik Rétegbeli redundanciát a GLBP biztosítja. Az Office 2 hálózatában a két 2811-es Router egy DHCP szerverként is szolgál így automatikusan kapnak IP címet a helyi klinesek.

**2960 Switch:** Ez a switch a Cisco 2960 Series családjába tartozik. Ez az eszköz 10/100 Mbps-es sávszélességet támogat. 24 db FastEthernet porttal rendelkezik. A VLAN-ok alkalmazása mikroszegmentálás (Egy biztonsági megközelítésre utal, amely tartalmazza a

hálózat szegmensekre osztását és biztonsági vezérlés alkalmazását minden egyes szegmensre, a szegmens követelményei alapján.) szempontjából. Második Rétegbeli redundanciát EtherChannel alkalmazásával valósítottuk meg. A hálózati hurkok megakadályozásához STP-t (Spanning Tree Protocol) használtunk. A biztonság megvalósításához a hozzáférési portokra Port biztonságot (Port Security) alkalmazunk. A DHCP hamisításos támadás ellen DHCP Snoopingot alkalmaztunk.

**2950 Switch:** Ez a switch a Cisco 2950 Series családjába tartozik. Ez az eszköz 10/100 Mbps-es sávszélességet támogat. 24 db FastEthernet porttal rendelkezik. A VLAN-ok alkalmazása mikroszegmentálás szempontjából. Második Rétegbeli redundanciát EtherChannel alkalmazásával valósítottuk meg. A hálózati hurkok megakadályozásához STP-t használtunk. A biztonság megvalósításához a hozzáférési portokra Port biztonságot (Port Security) alkalmazunk. A DHCP hamisításos támadás ellen DHCP Snoopingot alkalmazunk.

**Virtualizált Szerver Windows:** Az OFFICELAN.hu tartományhoz tartozik. A Szerver statikusan kapja meg a 172.168.1.3 ip címet. Az Active Directory működéséhez a Windows Server a DNS szolgáltató. A forward lookup zone-ba felvettük a Linux Szervert mint host típust majd létrehoztunk egy aliast(CNAME) és a [www.officelan.network](http://www.officelan.network/) címhez hozzárendeltük a Linux Szerver hostot. Továbbá létrehoztunk egy reverse lookup zone-t amiben hozzáadtuk a linux szervert pointerként. A Tartományba az összes VTEC dolgozóját felvettük és a megfelelő szerepkörökhöz osztottuk. A rendszergazdák közé tartozik Köteles Ádám, Szilágyi Gábor, Papp László Nimród, ennek megfelelően alkalmaztuk a jogosultságaikat. A többi felhasználó a dolgozók csoportjába tartozik Office1operátor, Office2operátor.

Egy Windows Server backup szolgáltatás van konfigurálva a Windows Serveren, amely, egy adott időbeállítás szerint készít biztonsági mentést a megadott fájlról. A biztonsági mentést a SAMBA szolgáltatás által megosztott mappába menti. A szerveren létre kell hozni egy Backup operátor felhasználót, amelynek a bejelentkezési adatai megegyeznek a Linux szerveren létrehozott SAMBA felhasználóval. Az OFFICE1 ÉS OFFICE2 felhasználók számítógépjeikre automatikusan feltelepül a Mozilla Firefox egy Group policy alkalmazásával. Továbbá elkészítettünk egy HTTPS szolgáltatást a szerveren. Létrehoztunk egy hálózati nyomtatót, amelyet megosztunk a hálózaton keresztül.

**Virtualizált Szerver Linux:** A Szerver statikusan kapja meg a 172.168.0.3 ip címet. DHCP szolgáltatást használunk a Linux szerveren, az isc-dhcp-server szolgáltatás segítségével, az /etc/dhcp/ mappában található a dhcpd.conf állomány amelyben beállítható az alhálózat

„range”-e, ahol 3 hálózati range-et állítottunk be, a hálózati topológiának megfelelően a 172.168.1.0/24 172.168.0.0/24 172.16.0.0/24 hálózati ranget használjuk, és mindegyik

hálózaton belül az 50.kiosztható címtől kezdve kapják az IP címeket a hálózati kliensek és a DNS kiszolgáló pedig a Windows server 172.168.1.3-as IP címe. Linux szerveren felkonfiguráltunk egy HTTP szolgáltatást, amely a 172.168.0.3-as IP címen keresztül érhető el a helyi hálózaton belül. A fájl megosztás megvalósítására SAMBA szolgáltatást használunk amelyben létrehoztunk egy mappát amelyet megosztottunk az OFFICELAN számára Továbbá a Windows Serveren Létrehoztunk egy Nyomtató megosztást.

**WIFI AP:** Ez a Wifi AP az Office 1 első szintjén található. A hozzáférési pont egy olyan eszköz, amely vezetéknélküli hálózatot hoz létre és lehetővé teszi, hogy eszközök, mint például laptopok, okostelefonok és táblagépek csatlakozzanak az internethez vagy egy helyi hálózathoz. A hozzáférési pont közvetítőként működik a vezeték nélküli eszközök és a vezetékes hálózat között. Az eszközök rádió hullámok segítségével képesek kommunikálni az Access point felé, amely ezután a vezetékes kapcsolaton keresztül továbbítja a kommunikációs kéréseket.

**WIFI Router:** A WIFI Router az Office 2 második szintjén található amely a 24-es vlan kliensei számára dinamikus IP cím osztást biztosít.

**PC:** A Dolgozók által használt számítógépek, Windows 10 Operációs rendszerrel ellátva. Ezen számítógépeken a Felhasználók Active Directory segítségével tudnak bejelentkezni a felhasználói fiókjaikba. A számítógépek dinamikusan vesznek fel IP címet egy DHCP Szerver által. Ezáltal az Office1 és Office2 alkalmazottai elérhetik egymást és a cég szolgáltatásait igénybe vehetik.

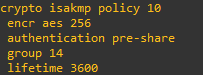
**Telefon:** Vezetéknélküli hálózat tesztelése mobiltelefon készüléken.

**Laptop:** Vezetéknélküli hálózat tesztelése.

# Eszköz Konfigurációk Bemutatása

#### OFFICE1

#### OFFICE1LANRouter GRE Over IPsec

****

* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Szabályrendszer létrehozása. A Titkosítás 256 bites aes. A Hitelesítés előre megosztott kulccsal működik. A kulccserének a (Diffie-Hellman group) 14-es csoportot adtuk meg és a szabály élettartalma 3600 mp.



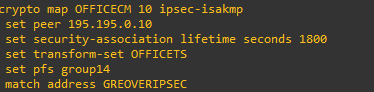
* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Az Előre megosztott kulcs definiálása(Kulcsnév: OFFICETOOFFICE), távoli kapcsolat megadása(195.195.0.10)



* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Ipsec transzformáció OFFICETS néven a policyban definiált szabályokkal.



* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Crypto map létrehozása 10-es priorítással OFFICECM néven. Távoli kapcsolat megadása(195.195.0.10). A Biztonsági hozzárendelés időtartamának beállítása 1800

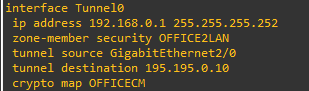
másodpercre. Transzformáció hozzárendelése a crypto maphez, Diffie-Hellman csoport hozzárendelése, hozzáférési lista hozzárendelése.

* + - * [Virtuális Privát Hálózat (VPN):](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat)
        + A virtuális magánhálózat lehetővé teszi a felhasználók számára, hogy egy nyilvános hálózaton keresztül úgy küldjenek és fogadjanak adatokat, mintha számítógépeik közvetlenül kapcsolódnának a helyi hálózathoz földrajzi helyüktől függetlenűl.
        + Két Fajtája van:

Remote Access (Távoli hozzáférés):

A számítógép egy távoli router által biztosított VPN szolgáltatásra csatlakozik.

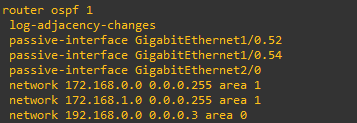
Site To Site: Két router között olyan mintha egy pont to piont kapcsolat alakulna ki amelyen tud kommunikálni a két privát hálózat. A forgalom ugyanúgy az interneten keresztűl megy titkosított (Ipsec) formában



* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

GRE Tunnel Konfigurálása. Interfacre IP cím megadása majd az OFFICE2LAN zonájához csatoljuk a forgalom ellenörzése miatt. GRE Tunnel forrás port megadása majd pedig a cél megadása távoli kapcsolat ip címe alapján. Crypto Map hozzárendelése a tunnel porthoz.

* + - * [GRE Tunnel(Generic Routing Encapsulation):](https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/)
        + Egy „pont-pont” kapcsolatot alakít ki egy távoli router és a helyi között.
        + Egy adatcsomagot egy másik adatcsomagba ágyaz.
        + A GRE Tunnel-ön keresztül lehet használni forgalomirányítási protokollokat.
        + A GRE Tunnel alapértelmezetten nem titkosítja a csomagot. Ipsec Konfigurálásával tudjuk biztosítani a csomagok titkosítását.



* + 1. *ábra OSPF konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

OSPF dinamikus forgalomirnyítás konfigurálása 1-es folyamat azonosító címmel. Passziváljuk az interfaceket amelyekre ne küldjön OSPF üzeneteket. Megadjuk a hálózatokat melyeket areaba sorolunk és hirdetünk egy másik routernek.

* + - * Dinamikus Forgalomirányítási Protokollok (OSPF, EIGRP, RIP):
        + OSPF:
* Egy kapcsolatállapot alapú protokoll amely, elérhetőve teszi

,hogy forgalomirányítási információkat osszanak meg a többi router között.

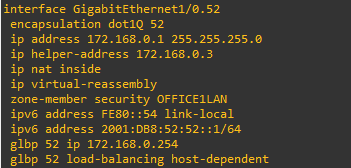
* Ezáltal a saját ismert hálózatukat dinamikusan megoszthatják a többi routerrel.



* + 1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Kiterjesztett hozzáférési lista létrehozása GREOVERIPSEC néven. 172.168.0.0 Hálózat és 172.16.0.0 Hálózat közötti forgalom engedélyezése.

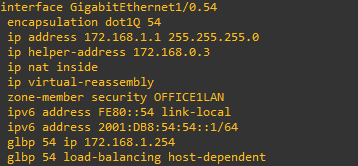
#### Interface

****

* + 1. *ábra Interface konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

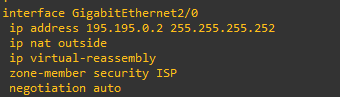
Subinterface felkonfigurálása az 52-es vlan számára, IP cím kiadása az interface-re, DHCP szerver ip megadása a kérések továbbítása a dhcp szerver felé, címfordítás belső oldala, OFFICE1LAN zóna csoporthoz hozzáadás, ipv6 címek megadása, glbp 52-es csoporthoz rendelés és virtuális cím megadása és terhelés megosztás beállítása host-dependentre.

* + - * [VLAN (Virtual Local Area Network):](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_helyi_h%C3%A1l%C3%B3zat)
        + Ugyanabban a VLAN-ban lévő hálózati eszközök úgy kommunikálnak mintha ugyan abba a szórási tartomtányba tartoznának fizikai elhelyezkedésüktől függetlenűl. Lehetővé teszi az eszközök együttes kezelését még akkor is ha nem ugyanarra a hálózati kapcsolóra csatlakoznak.
      * [Router On A Stick:](https://www.nwkings.com/what-is-router-on-a-stick)
        + A "Router on a stick" vagy ROAS egy olyan módszer, amelyben létrehozunk egy szubinterfészt a routeren, és VLAN címkézést használunk a forgalom megkülönböztetésére.
      * Harmadik Rétegbeli Redundancia (FHRP,GLBP):
        + Egy virtuális ip cím használatával a routerek eltudják osztani hogy melyik az aktív kiszolgáló.
        + Aktív kiszolgáló kiesése esetén a másdlagos router veszi át a szerepet.
        + GLBP:
* Gateway Load Balancing Protocol
* A protokollnak három fajta terheléselosztási módja van:
  + Host Dependent:
    - A kliens MAC cím alapján határozza meg az aktív routert.
  + [Round Robin:](https://community.cisco.com/t5/switching/glbp-round-robin-load-balancing/td-p/2126138)
    - Szekvenciálisan váltogatja az aktív routert.
    - Körönként váltja ,hogy melyik router felé halad a csomag ezzel biztosítva a megfelelő terheléselosztást.
  + Weighted:
    - A routereknek van egy megadott súlyuk (Weight) . A magasabb súlyú átjáró (Gateway) több csomagot kezel amíg a kevesebb súllyal rendelkező kevesebb csomagot kezel. (Például: R1: 50 , R2:100: R1 1 csomag, R2 2 csomag)
* Ipv4:
  + Internet Protocol Version 4
  + 32 bit hosszúságú
  + Bináris(2-es) számrendszert használja alapúl
  + Minden hálózati eszköz használja egymás azonosítására
* Ipv6:
  + Internet Protocol Version 6
  + 128 bit hosszúságú
  + Hexadecimális(16-os) számrendszert használja alapúl
  + Minden hálózati eszköz használja egymás azonosítására



* + 1. *ábra Interface konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Subinterface felkonfigurálása az 54-es vlan számára, IP cím kiadása az interface-re, DHCP szerver ip megadása a kérések továbbítása a dhcp szerver felé, címfordítás belső oldala, OFFICE1LAN zóna csoporthoz hozzáadás, ipv6 címek megadása, glbp 52-es csoporthoz rendelés és virtuális cím megadása és terhelés megosztás beállítása host-dependentre.



* + 1. *ábra Interface konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Az ISP felé menő interfészre megadjuk az ip címet majd beállítjuk a címfordítás külső oldalát, hozzárendeljük az ISP zonához

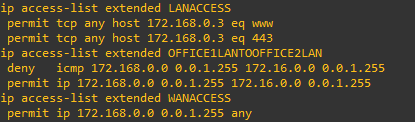
#### Zone Based Policy Firewall

****

* + 1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

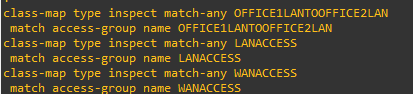
Zónák létrehozása

* + - * [Tűzfal:](https://docs.freebsd.org/hu/books/handbook/firewalls/)
        + A tűzfalakkal a rendszerünkön bejövő és kimenő forgalmat tudjuk szűrni. A tűzfalak egy vagy több "szabályrendszer" alapján vizsgálják az átmenő hálózati csomagokat, vagy továbbengedik ezeket vagy megállítják. A tűzfalak szabályai a csomagok egy vagy több jellemzőjét veszik szemügyre, amelyek lehetnek például a protokoll típusa, a forrás vagy cél hálózati címe, esetleg a forrás- vagy a célport.
        + Több fajtája van Példáúl: Zónázó Tűzfal, ASA



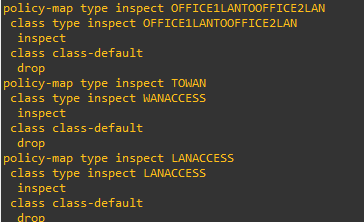
* + 1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Kiterjesztett hozzáférési lista létrehozása LANACCESS néven. Engedélyezük a 443-as porton a https forgalmat és a 80-as http (www) portot. Kiterjesztett hozzáférési lista létrehozása OFFICE1LANTOOFFICE2LAN néven. Letiltjuk a pingelést az Office1 hálózatából az office2- be.Majd minden más forgalom engedélyezése.Létrehozzuk a WANACCESS kiterjesztett hozzáférési listát melyben minden forgalmat engedélyezünk az OFFICE1-ből az internet irányába.



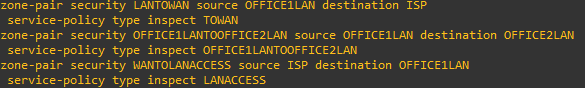
* + 1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Class mapek léterhozása match-any paranccsal amely a legelső megeggyező esetnél végrehajtja a megadott utasítást (engedélyez vagy tilt). OFFICE1LANTOOFFICE2LAN class maphez hozzácsatoljuk az hozzáférési listát. (OFFICE1LANTOOFFICE2LAN). LANACCESS class maphez hozzácsatoljuk az hozzáférési listát (LANACCESS). WANACCESS class maphez hozzácsatoljuk az hozzáférési listát (WANACCESS).



* + 1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Policy mapek létrehozása. OFFICE1LANTOOFFICE2LAN hozzárendeljük a OFFICE1LANTOOFFICE2LAN class mapet és megadjuk hogy állapotfigyelő(stateful) vizsgálatot biztosít. TOWAN hozzárendeljük a WANACCESS class mapet és megadjuk hogy állapotfigyelő(stateful) vizsgálatot biztosít. LANACCESS hozzárendeljük a LANACCESS class mapet és megadjuk hogy állapotfigyelő(stateful) vizsgálatot biztosít.



* + 1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Zónapárok létrehozása. LANTOWAN zónapárba a forrás az OFFICE1LAN a cél pedig az ISP zónája. Továbbá hozzácsatoluk a TOWAN policyt. OFFICE1LANTOOFFICE2 zónapárba a forrás az OFFICE1LAN a cél pedig az OFFICE2LAN zónája. Továbbá hozzácsatoluk a OFFICE1LANTOOFFICE2 policyt. WANTOLANACCESS zónapárba a forrás az ISP a cél pedig az OFFICE1LAN zónája. Továbbá hozzácsatoluk a LANACCESS policyt.



Interfaceket zónákhoz rendeljük. Tunnel0 - OFFICE2LAN, GIG1/0.52 - OFFICE1LAN, GIG1/0.54 - OFFICE1LAN, GIG2/0 - ISP

#### NAT/PAT

**A black screen with yellow and orange text  AI-generated content may be incorrect.**

1. *ábra NAT/PAT konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

PAT beállítása a gigabitethernet2/0-ás portra. Létrehoztuk a NAT hozzáférési listát amely átengedi az OFFICE1 hálózatát.

* + NAT/PAT (Hálózati címfordítás):
    - Network Address Translaiton/Port Address Translation
    - A NAT lehetővé teszi , hogy egy privát címet átfordítsunk egy publikus címmé ezzel elérhetővé tegye az internethez való hozzáférést. Két féleképpen beállítható a címfordítás:
      * Statikusan:
        + Egy Statikusan beállított privát IP címet egy statikusan beállított publikus címre fordít.
      * Dinamikusan:
        + Egy Poolban (IP Címtartomány) lévő összes publikus IP címet dinamikusan kérés szerint rendeli privát IP címhez ezzel biztosítva az internet hozzáférést.
    - A Port Address Translation engedélyezi a portok használatát így egy darab publikus IP címhez több privát IP Cím társítható
      * Egy Poolban lévő pulbikus IP címeket is lehet egy adott portra fordítani így csökkentve a publikus IP címek felhasználását.



Gig1/0.52 és gig1/0.54 interfész beállítása a nat belső oldalának, majd a gig2/0 interfészt beállítjuk a nat külső oldalának.

#### Statikus Forgalomirányítás

****

1. *ábra NAT/PAT konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Statikus alapértelmezett útvonal az isp irányába.

* + Forgalomirányítás (Dinamikus, Statikus):
    - Két forgalomirányítási módszer létezik:
      * Dinamikus:
        + Egy Forgalomirányítási protokoll segítségével tanulja meg a hálózatot.
      * Statikus:
        + Manuálisan állítjuk be a távoli ismeretlen hálózat elérési pontját (Next Hop Router, Outgoing Interface).

#### OFFICE1LANRouter-2

#### GRE Over IPsec

Crypto map létrehozása az OFFICE1LANRouter-hez hasonlóan. Távoli kapcsolat megadása (195.195.0.14).

GRE Tunnel Konfigurálása hasonlóan az OFFICE1LANRouter-hez. Interface IP címe 192.168.0.5/30 majd pedig a tunnel céljának beállítjuk a 195.195.0.14-et.

OSPF dinamikus forgalomirányítás ugyanúgy lett megvalósítva, mint az OFFICE1LANRouter-en. A hirdetett hálózatban az eltérés annyi, hogy a 192.168.0.4/30-as hálózatot hirdetjük 0-ás areaba.

Kiterjesztett hozzáférési lista ugyanúgy lett felkonfigurálva.

#### Interface

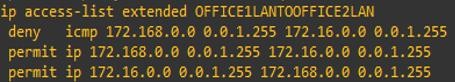
Az interface hasonlóan lett felkonfigurálva, mint az OFFICE1LANRouteren. IP cím 172.168.0.2/24 kiadása az interface-re, ipv6 cím beállítása a 2001:db8:52:52::2/64, illetve a link-local cím fe80::55-ös cím.

Az interface hasonlóan lett felkonfigurálva, mint az OFFICE1LANRouteren. IP cím 172.168.1.2/24 kiadása az interface-re, ipv6 cím beállítása a 2001:db8:54:54::2/64, illetve a link-local cím fe80::55-ös cím.

Az ISP felé menő interfészre megadjuk a 195.195.0.6 ip címet, a többi beállítás hasonló az OFFICE1LANRouter beállításaihoz.

#### Zone Based Policy Firewall

Zónák létrehozása ugyanúgy mint az OFFICE1LANRouter-en.



1. *ábra ZBPF Konfiguráció. A kép saját szerkesztés.*

LANACCESS és WANACCESS nevű kiterjesztett hozzáférési listákat úgyanúgy konfiguráljuk, mint az OFFICE1LANRouter-en. Kiterjesztett hozzáférési lista létrehozás

OFFICE1LANTOOFFICE2LAN néven. Letiltjuk a pingelést az Office1 hálózatából az office2- be.Majd minden más forgalom engedélyezése.

Class mapek létrehozása ugyanúgy, mint az OFFICE1LANRouter-en. Policy mapek létrehozása ugyanúgy, mint az OFFICE1LANRouter-en. Zónapárok létrehozása ugyanúgy, mint az OFFICE1LANRouter-en.

Interfaceket zónákhoz rendeljük ugyanúgy, mint az OFFICE1LANRouter-en.

#### NAT/PAT

A NAT minden konfigurációját ugyanúgy konfiguráltunk fel, mint az OFFICE1LANROUTER-en

#### Statikus Forgalomirányítás

Statikus alapértelmezett útvonal az isp irányába.

#### OFFICE1LANSwitch DHCP SNOOPING

A vlan1,52,54-en engedélyezzük a snoopingot. Továbbá engedélyzzük a globális használatát.

Az alábbi portokat: Port-channel1, Ethernet0/0 a megbízható módba kapcsoljuk. Illetve az Ethernet0/1-0/3ig bekapcsoljuk azt, hogy egy másodpercen belül hány dhcp kérést küldhetnek a porton.

*SEQ ábra \\* ARABIC 22. ábra DHCP Snooping Konfiguráció. A kép saját*



* [DHCP Snooping:](https://fiberroad.com/resources/glossary/what-is-dhcp-snooping-and-why-should-you-use-it/)
  + A DHCP snooping egy biztonsági funkció, amely megakadályozza a rosszindulatú eszközök DHCP üzenetek hamisítását és a hálózati kapcsolatok megszakítását. Úgy működik, hogy megvizsgálja a DHCP üzeneteket, és csak azokat engedi át, amelyek megbízható forrásoktól származnak. A DHCP

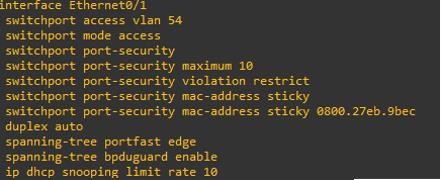
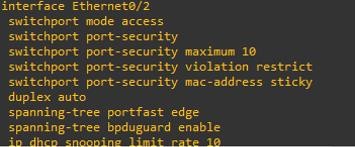
snooping switcheken és routereken használható a DHCP szerverek hamisítása, a kliens hamisítások és a szolgáltatásmegtagadásos támadások elleni védelemre.

* + Amikor a DHCP snooping engedélyezve van egy switch-en vagy router-en, az eszköz nyomon követi, hogy mely portok küldhetnek és fogadhatnak DHCP üzeneteket. Csak a megbízható forrásoktól származó üzeneteket engedi át, míg minden más üzenetet blokkol.

#### INTERFACES/SWITCHPORT/SPANNING-TREE/PORT-SECURITY

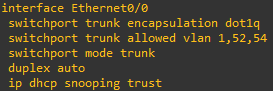
****

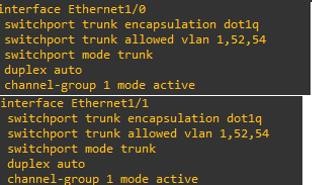
A spanning-tree módját Rapid-PVST-be állítjuk.



Hozzáférési módba helyezzük a portokat és az 54-es vlanhoz rendeljük. Bekapcsoljuk a Port-Security-it. A Maximum 10 darab különböző MAC címet tanúlhat meg mielőtt error- disabled állapotba kerül a port. Biztonság megsértési módot restrict-re állítjuk. A MAC címeket Sticky tulajdonsággal megtanúlja és megtartja az információkat. A portokon portfast-et állítunk be és bekapcsoljuk a bpduguardot. Továbba az Ethernet0/1-0/3ig bekapcsoljuk azt ,hogy egy másodpercen belül hány dhcp kérést küldhetnek a porton.

* [Switchport mode (Trunk, Access):](https://www.ruijienetworks.com/support/tech-gallery/what-is-a-switchport)
  + Két típusa van:
    - Hozzáférési port:
      * A hálózati hoszt egyetlen VLAN-hoz való csatlakozása hozzáférési porton keresztül történik, amely a virtuális hálózat adatáramlását is szabályozza. A hozzáférési port nem címkézett Ethernet kereteket kezel, mivel az adatok csak a meghatározott VLAN-on belül áramolhatnak.
    - Trunk port:
      * A trunk port több VLAN-nal is kommunikálhat, és jellemzően egy másik switchhez,routerhez van csatlakoztatva. A trunk port szabályozza az adatok átvitelét több VLAN között egy hálózaton. Ezt úgy éri el, hogy azonosítja a keret címkéit, amelyek meghatározzák az adat szándékolt célállomását.
      * Spanning-Tree (Feszítőfa protokoll):
        + Második rétegbeli hurkok elkerülését biztosítja.
        + A hálózaton kiválasztásra kerül egy Root Bridge a Bridge ID alapján. A legkisebb ID-val rendelkező router lesz a Root Bridge.
        + Az összes többi Switch a Root felé a legkisebb költséggel rendelkező portját választja ki Root Portnak.
        + Az összes többi port blokkolt vagy designated (Kijelölt) módba kerül.



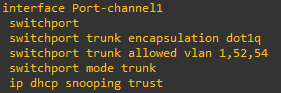


***26****. ábra Interface konfiguráció. A kép saját szerkesztés.*

A switcportokat trunk módba állítjuk és a keret beágyazást dot1q-ra állítjuk. Az 1,52,54 VLAN-ok forgalmát engedjük át. Az Ethernet0/0 portot megbízható módba kapcsoljuk. Az Ethernet1/0 és 1/1-et pedig 1-es csatorna csoportba helyezzük és kezdeményező állapotba helyezzük. LACP-t alkalmaztunk az Ethernchannelnél.

* + - * [Port-Security (Portbiztonság):](https://study-ccna.com/port-security/)
        + A port biztonság alkalmazásával a rendszergazda beállíthatja hogy a switch dinamikusan vagy statikusan vegye fel a MAC címeket , így megakadályozva, hogy egy támadó csatlakoztassa saját eszközét. Ezzel lehetőség van a port hozzáférésének korlátozására, így csak az engedélyezett eszközök használhatják azt.
        + A Port Violation Mode segítségével beállítható hogy milyen biztonsági lépéseket tegyen meg az eszköz amennyiben egy ismeretlen MAC címmel rendelkező eszköz csatlakozik és meghaladja az adminisztrátor által beállított maximum felvehető MAC címeket az adott porton.

#### ETHERCHANNEL



Az Ethernet1/0 és 1/1-et pedig 1-es csatorna csoportba helyezzük és kezdeményező állapotba helyezzük. LACP-t alkalmaztunk az Ethernchannelnél. A Port-channel1-et Trunk

módba állítjuk és a keret beágyazást dot1q-ra állítjuk. Az 1,52,54 VLAN-ok forgalmát engedjük át. Az portot megbízható módba kapcsoljuk.

* [EtherChannel:](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/etherchannel.pdf)
  + Az EtherChannel egyesíti az egyes Ethernet kapcsolatokat egyetlen logikai kapcsolattá, amely akár nyolc fizikai kapcsolat összesített sávszélességét biztosítja.
  + Három féle módban működhet:
    - ON-ON: Manuálisan konfiguráljuk be az Etherchannelt mind a két oldalon.
    - Illetve két féle dinamikusan egyeztető protokoll van:
      * PAGP:
        + Desirable (Kezdeményező) – Auto
        + Cisco Saját Tulajdona
        + Csak Cisco eszközökön használható
      * LACP:
        + Active (Kezdeményező) – Passive
        + Gyártó független
        + Bármilyen eszközön használható amennyiben Implementálta a gyártó az eszközbe.

#### OFFICE1LANSwitch-2

Az OFFICE1LANSwitch-2 eszközt ugyanúgy konfiguráltuk fel mint az OFFICE1LANSwitch-et.

#### Linux Server DHCP

#### dhcpd.conf

**subnet 172.168.1.0 netmask 255.255.255.0 {**

Definiáljuk a hálózati címet hálózati maszkkal.

**range 172.168.1.50 172.168.1.100;**

Beállítjuk a kioszható IP cím tartományt.

**option routers 172.168.1.254;**

Az Alapértelmezett átjáró beállítása.

**option domain-name-servers 172.168.1.3;**

DNS Kiszolgáló beállítása.

**option broadcast-address 172.168.1.255;**

Szórási cím beállítása.

**default-lease-time 600;**

Bérleti idő beállítása 600 másodpercre.

**max-lease-time 7200;**

Maximum bérleti idő beállítása 7200 másodperce.

**}**

**subnet 172.168.0.0 netmask 255.255.255.0 {**

Definiáljuk a hálózati címet hálózati maszkkal.

**range 172.168.0.50 172.168.0.100;**

Beállítjuk a kioszható IP cím tartományt.

**option routers 172.168.0.254;**

Az Alapértelmezett átjáró beállítása.

**option domain-name-servers 172.168.1.3;**

DNS Kiszolgáló beállítása.

**option broadcast-address 172.168.1.255;**

Szórási cím beállítása.

**default-lease-time 600;**

Bérleti idő beállítása 600 másodpercre.

**max-lease-time 7200;**

Maximum bérleti idő beállítása 7200 másodperce.

**}**

#### isc-dhcp-server

**INTERFACESv4=”enp0s3”**

DHCPv4 Bekapcsolása.

* [DHCP:](https://bytech.hu/dhcp/)
  + Dynamic Host Configuration Protocoll
  + Hálózati protokoll, melynek célja az IP címek, maszkok, DNS kiszolgálók és átjárók automatikus kiosztása.
  + Működése:
    - Négy lépésből áll:
      1. Discover (Felfedezés):
         * Egy hálózati kliens kérést küld szórási címen keresztül DHCP szerver keresés céljából.
      2. Offer (Ajánlat):
         * Ha a DHCP szerver pooljában van szabad IP cím akkor egy ajánlatot küld a kliens felé.

#### Fájl megosztás

* + - 1. Request (Kérés):
         * A DHCP szerver felé küld egy kérést a kliens melyben elfogadja a kiosztott ip címet és egyéb konfigurációt.
      2. Acknowledge (Megerősítés):
         * Megerősíti az IP cím kiosztást. A DHCP csomag tartalmazza a végleges dinamikusan kiosztott IP címet.

**apt install samba**

Samba szolgáltatás telepítése.

**mkdir /srv/OFFICESHARE/**

Létrehozzuk az OFFICESHARE könyvtárat.

**mkdir /srv/OFFICESHARE/Resources**

Létrehozzuk az RESOURCES könyvtárat.

**chmod -R 770 /srv/OFFICESHARE/**

Az egész OFFICESHARE könyvtárra és a benne lévő fájlokra kap jogosultságot a tulajdonos és minden csoport.

**groupadd officesambausers**

Hozzáadjuk az officesambausers csoportot.

**usermod -aG officesambausers shared**

A shared felhasználót hozzáadja az officesambausers-hez.

**usermod -aG officesambausers officeadmin**

Az officeadmin felhasználót hozzáadja az officesambausers-hez.

**nano /etc/samba/smb.conf**

Belépünk az smb.conf-ba

**sudo systemctl restart smbd**

smbd szolgáltatás újraindítása.

**sudo ufw allow 'Samba'**

Samba szolgáltatás engedélyezése.

**sudo ufw reload**

Tűzfal újraindítása.

**sudo ufw enable**

Tűzfal bekapcsolása.

**sudo smbpasswd -a shared**

A létező shared nevű felhasználót hozzáadjuk a SAMBA-hoz

**sudo systemctl restart smbd**

Újranindítjuk az smbd szolgtatást.

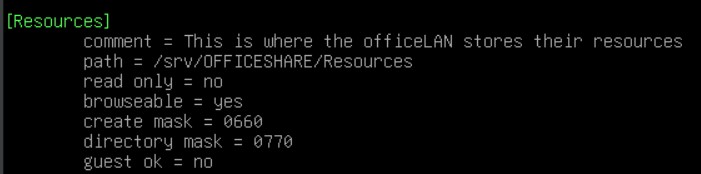
**chown officeadmin:officesambausers OFFICESHARE**

Megváltoztatjuk az OFFICESHARE könyvtár tulajdonosát officeadminról officesambausers-re.

**chown officeadmin:officesambausers Resources**

Megváltoztatjuk az RESOURCES könyvtár tulajdonosát officeadminról officesambausers-re.

#### smb.conf

****

path a RESOURCES mappa elérhetőségi útvonala.

[Fájl és nyomtatómegosztás:](https://hu.wikipedia.org/wiki/Samba_(szoftver))

A Samba az UNIX gépeken lévő fájl- és nyomtató erőforrásokat tesz elérhetővé Windows operációs rendszert használó számítógépekre.

Két Fő részből áll:

smbd

nmbd

Ezek a következő fő feladatok megvalósítására szolgálnak:

Fájl- és nyomtatási szolgáltatások

Hitelesítések és engedélyek kezelése

Névfeloldás

Tallózás

#### HTTP

**apt install apache2**

Apache2 Szolgáltatás telepítése.

**ufw allow 80**

Http engedélyezése.

**index.html**

Http Weboldal konfigurációja. A konfigurációs mellékletben megtalálható.

[HTTP/HTTPS:](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/)

HyperText Transfer Protocol/HyperText Transfer Protocol Secure

Weblapokat tölt be HyperText linkek segítségével.

Alkalmazás rétegbeli protokoll.

HTTP:

A kliens és a szerver közötti kapcsolat titkositatlan.

HTTPS:

A kliens és a szerver közötti kapcsolat titkosított ezzel biztosítva a privát adataink védelmének biztosítását.

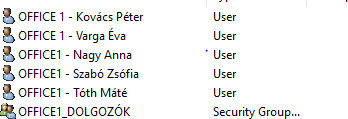
#### Windows Server Active Directory

ORGANIZATIONAL UNIT



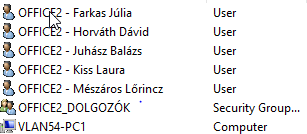
1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Az OFFICE-okat szervezeti egységekbe tagoljuk. OFFICE1LAN OU



1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

OFFICE1LAN szervezeti egységben létrehozott felhasználók a dolgozóknak. OFFICE2LAN OU



1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

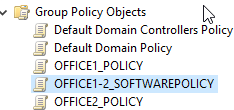
OFFICE1LAN szervezeti egységben létrehozott felhasználók a dolgozóknak.

GLOBÁLIS ADMINOK



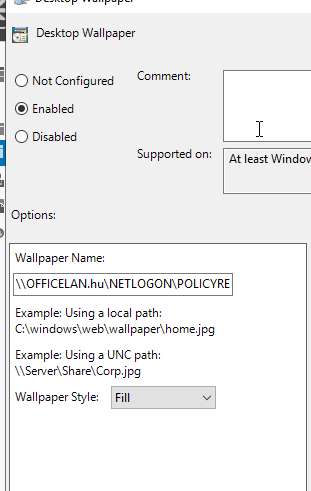
1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Globális admin felhasználók. GROUP POLICY OBJECT



1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Csoportházirend objektumok létrehozása. DESKTOP WALLPAPER SET

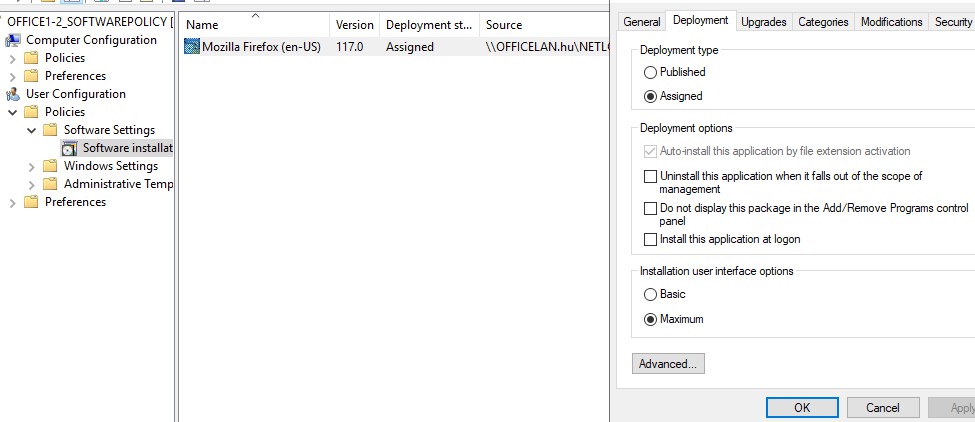


1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Automatikus Háttérkép beállítás. A háttérkép az összes hálózati eszköz számára elérhető.

* + [Active Directory:](https://drive.google.com/file/d/10MJPURiHBI-vjjCOrbIZvrcSFLUxM3Ss/view?usp=sharing)
    - Címtár szolgáltatás a Windows hálózati környezetben. A szerver központi adatbázisként szolgál és információkat tárol felhasználókról, munkaállomásokról, csoportokról és egyéb objektumokról a munkakörnyezetben.
    - Néhány alapszolgáltatás:
      * Hitelesítés: Felhasználók azonosítása.
      * Engedélyezés: Hozzáférések kezelése az erőforrásokhoz.
      * Biztonsági házirendek és jogosultságok kezelése.
      * Hálózati adminisztráció és automatizáció megkönnyítése.
    - Főbb protoklja:
      * LDAP (Lightweight Directory Access Protocoll): Az Active Directory adatbázisában tárolt információk lekérdezésére szolgál.
      * Kerberos Hitelesítés: Egy biztonságos jegyalapú hitelesítési protokoll. A felhasználó bejelentkezéskor egy jegyet kapnak, melyet az Active Drirectory használ a hitelesítéshez.
    - Az Active Directory struktúrája, logikai felépítése:
      * Hierachikus struktúrát alkalmaz, az alábbi sorrendben:
        1. Erdő (forest)
        2. Fa (tree)
        3. Tartomány (domain)

#### AUTOMATIZÁLT SZOFTVER TELEPÍTÉS POLICYVAL



1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Beállítjuk, hogy a gép az bármely dolgozó felhasználóval történő bejelentkezése esetén elinduljon automatikusan a Mozzila Firefox Telepítése.

#### DNS, DNS REVERSE/FORWARD LOOKUP ZONE

****

1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Létrehozzuk az officelan.network forward lookup zone-t., Illetve az ahhoz kapcsolódó Reverse lookup zone-t.

#### HOST (A RECORD), CNAME

****

1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Felveszünk két A RECORD-ot (linux és windows server) amelyre ip cím alapján hivatkoznak. Továbbá felveszünk egy CNAME-t, amelynek a fully qualified domain name az [www.officelan.network.](http://www.officelan.network/)

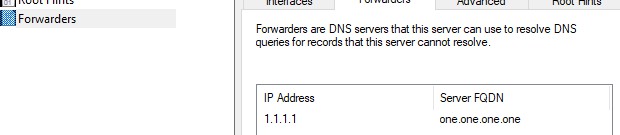
#### POINTER

****

1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Létrehozunk egy mutatót a linux szerverre.

#### FORWARDERs

****

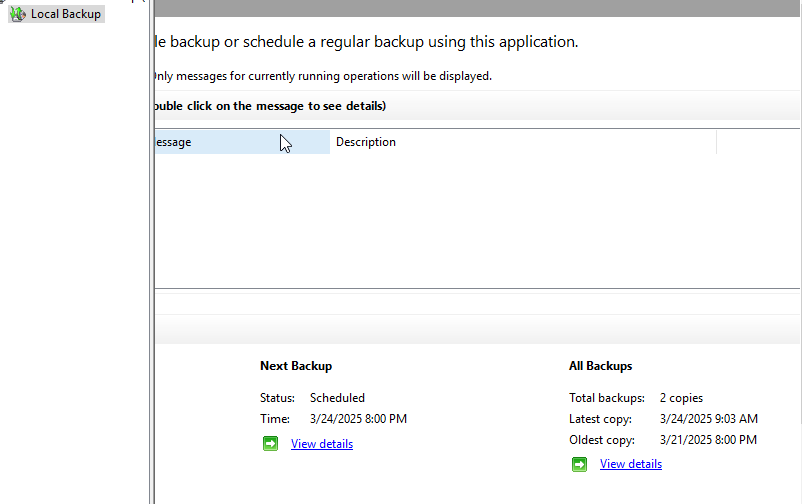
1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

Amennyiben nem találja meg a saját forward lookup zónáján belül a kért DNS nevet azt erre a DNS kiszolgáló felé irányítja.

* + DNS:
    - Domain Name System
    - Biztosítja a host nevek (például: [www.officelan.network](http://www.officelan.network/) ) IP címmé alakítását.

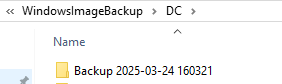
#### Automatizált Mentés

#### AUTOMATIZÁLT MENTÉS(BACKUP)

****

Beállítjuk azt, hogy milyen gyakorisággal mentse el az adott fájlt a Samba által megosztott mappába.

BACKEDUP FOLDER

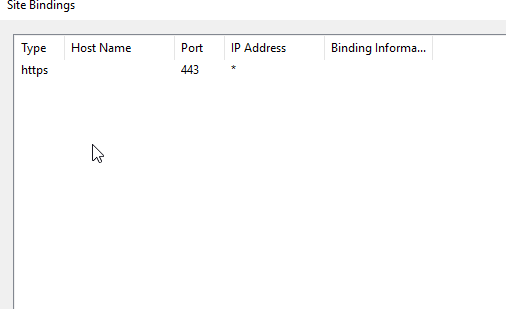


1. *ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

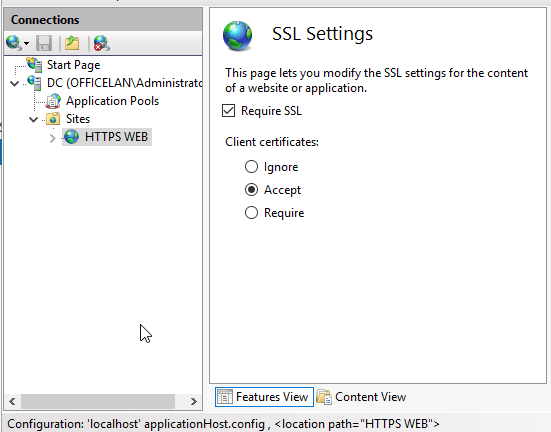
A mentés mappája

* + Automatizált Mentés:
    - Az automatizált mentés egy backup fájlt készít az eredeti példányról egy meghatározott időben.
    - Ezzel biztosítva azt ,hogy bármilyen hiba adodik az adott fájlal azt a fájlt vissza tudjuk tölteni egy előző állapotba.

#### HTTPS

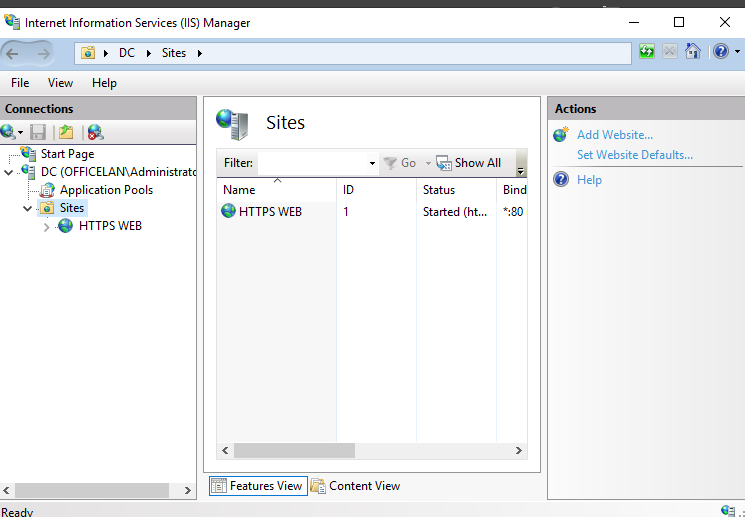
****

Hozzárendeljük a 443-as https portot a webhelyünkhoz.



*43. ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

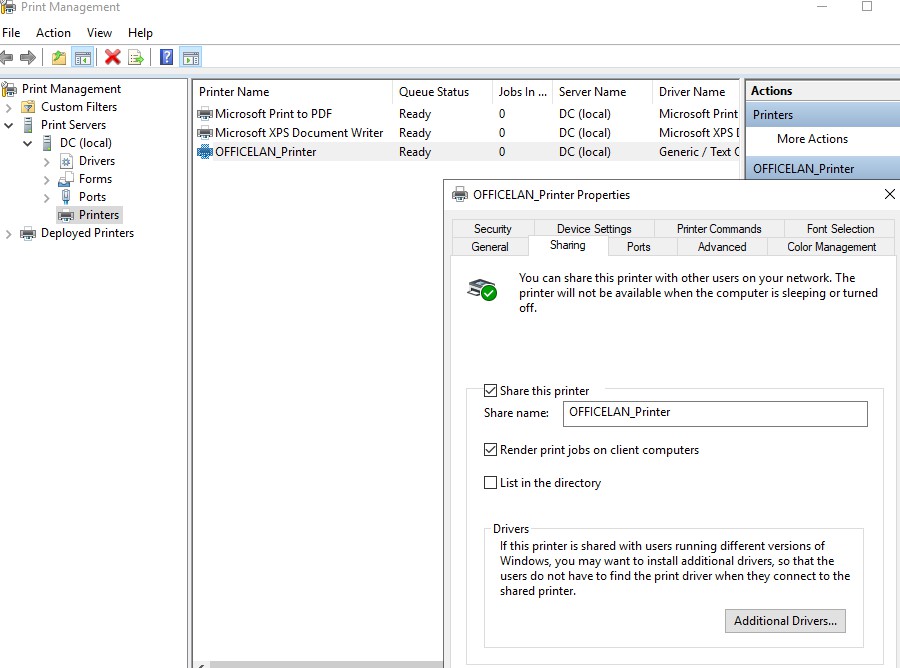
Beállítjuk, hogy az SSL használata kötelező legyen. Ezzel biztosítva a biztonságos kapcsolatot.



*SEQ ábra \\* ARABIC 44. ábra Windows Server Konfiguráció. A kép saját szerkesztés.*

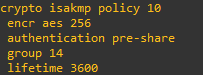
A létrehozott webhely státusza, illetve neve.

#### Nyomtató megosztás

****

#### OFFICE2

#### OFFICE2LANRouter GRE Over IPsec

****

Szabályrendszer létrehozása. A Titkosítás 256 bites aes. A Hitelesítés előre megosztott kulccsal működik. A kulccserének a (Diffie-Hellman group) 14-es csoportot adtuk meg és a szabály élettartalma 3600 mp.



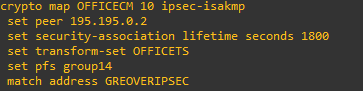
1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Előre megosztott kulcs definiálása (Kulcsnév: OFFICETOOFFICE), távoli kapcsolat megadása.



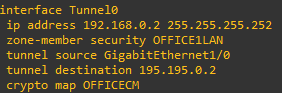
1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Ipsec transzformáció OFFICETS néven a policyban definiált szabályokkal.



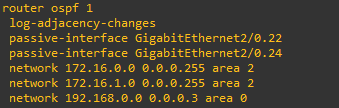
1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Crypto map létrehozása 10-es priorítással OFFICECM néven. Távoli kapcsolat megadása, Biztonsági hozzárendelés időtartalmát 1800 másodpercre állítottuk. Transzformáció hozzárendelése a crypto maphez, Diffie-Hellman csoport hozzárendelése, hozzáférési lista hozzárendelése.



1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

GRE Tunnel Konfigurálása. Interface IP cím megadása majd az OFFICE1LAN zonájához csatoljuk a forgalom ellenörzése miatt. GRE Tunnel forrás port megadása majd pedig a cél megadása távoli kapcsolat ip címe alapján. Crypto Map hozzárendelése a tunnel porthoz.



1. *ábra OSPF konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

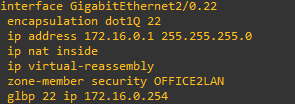
OSPF dinamikus forgalomirányítás konfigurálása 1-es folyamat azonosító címmel. Passziváljuk az interfaceket amelyekre ne küldjön OSPF üzeneteket. Megadjuk a hálózatokat melyeket areaba sorolunk és hirdetünk egy másik routernek



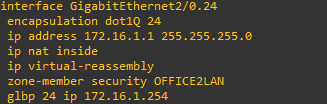
1. *ábra GRE Over IPsec konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Kiterjesztett hozzáférési lista létrehozása GREOVERIPSEC néven. 172.168.0.0 Hálózat és 172.16.0.0 Hálózat közötti forgalom engedélyezése.

#### Interface

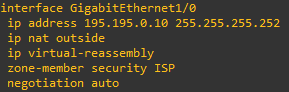
****

Subinterface felkonfigurálása az 22-es vlan számára, IP cím kiadása az interface-re, DHCP szerver ip megadása a kérések továbbítása a dhcp szerver felé, címfordítás belső oldala, OFFICE2LAN zóna csoporthoz hozzáadás, ipv6 címek megadása, glbp 22-es csoporthoz rendelés és virtuális cím megadása és terhelés megosztás beállítása host-dependentre.



1. *ábra Interface konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Subinterface felkonfigurálása az 24-es vlan számára, IP cím kiadása az interface-re, DHCP szerver ip megadása a kérések továbbítása a dhcp szerver felé, címfordítás belső oldala, OFFICE2LAN zóna csoporthoz hozzáadás, ipv6 címek megadása, glbp 24-es csoporthoz rendelés és virtuális cím megadása és terhelés megosztás beállítása host-dependentre.



1. *ábra Interface konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Az ISP felé menő interfészre megadjuk az ip címet majd beállítjuk a címfordítás külső oldalát, hozzárendeljük az ISP zonához.

#### Zone Based Policy Firewall

****

Zónák létrehozása



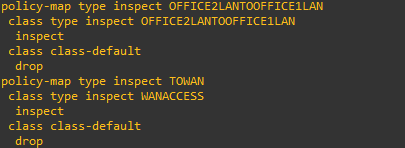
1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Kiterjesztett hozzáférési lista létrehozás OFFICE2LANTOOFFICE1LAN néven.Engedélyezzük a forgalmat OFFICE1 ÉS OFFICE2 között. Létrehozzuk a WANACCESS kiterjesztett hozzáférési listát melyben minden forgalmat engedélyezünk az OFFICE1-ből az internet irányába.



1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Class mapek léterhozása match-any paranccsal, amely a legelső megeggyező esetnél végrehajtja a megadott utasítást (engedélyez vagy tilt). OFFICE2LANTOOFFICE1LAN class maphez hozzácsatoljuk az hozzáférési listát. (OFFICE2LANTOOFFICE1LAN). LANACCESS class maphez hozzácsatoljuk az hozzáférési listát (LANACCESS). WANACCESS class maphez hozzácsatoljuk az hozzáférési listát (WANACCESS).



1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Policy mapek létrehozása. OFFICE1LANTOOFFICE2LAN hozzárendeljük a OFFICE1LANTOOFFICE2LAN class mapet és megadjuk, hogy állapotfigyelő(stateful) vizsgálatot biztosít. TOWAN hozzárendeljük a WANACCESS class mapet és megadjuk, hogy állapotfigyelő(stateful) vizsgálatot biztosít. LANACCESS hozzárendeljük a LANACCESS class mapet és megadjuk, hogy állapotfigyelő(stateful) vizsgálatot biztosít.



1. *ábra Zone Based Policy Firewall konfiguráció PuTTY-on keresztűl. A kép saját szerkesztés.*

Zónapárok létrehozása. LANTOWAN zónapárba a forrás az OFFICE1LAN a cél pedig az ISP zónája. Továbbá hozzácsatoluk a TOWAN policyt.

Interfaceket zónákhoz rendeljük. Tunnel0 - OFFICE2LAN, GIG1/0.22 -



OFFICE2LAN, GIG1/0.24 -OFFICE2LAN, GIG1/0 - ISP

#### NAT/PAT



PAT beállítása a gigabitethernet1/0-ás portra. Létrehoztuk a NAT hozzáférési listát amely átengedi az OFFICE2 hálózatát.

Gig1/0.22 és gig1/0.24 interfész beállítása a nat belső oldalának, majd a gig1/0 interfészt



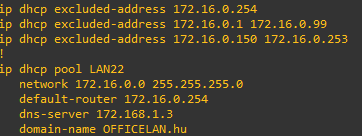
beállítjuk a nat külső oldalának

#### Statikus Forgalomirányítás

****

Statikus alapértelmezett útvonal az isp irányába.

#### DHCP

****

*66. ábra DHCP konfiguráció PuTTY-on keresztül. A kép saját szerkesztés.*

Lefoglaljuk a 172.16.0.254-es címet és a 172.16.0.1 és 172.16.0.99 közé eső címeket továbbá, lefoglaljuk a 172.16.0.150 ás 172.16.0.253 közé eső címeket. Majd létrehozzuk a DHCP Pool-t LAN22 néven, megadjuk a networkot,deafult-routert, dns-servert és domin- namet.

#### OFFICE2LANRouter-2

#### GRE Over IPsec

Crypto map létrehozása az OFFICE2LANRouter-hez hasonlóan. Távoli kapcsolat megadása (195.195.0.6).

GRE Tunnel Konfigurálása hasonlóan az OFFICE2LANRouter-hez. Interface IP címe 192.168.0.6/30 majd pedig a tunnel céljának beállítjuk a 195.195.0.6-ot.

OSPF dinamikus forgalomirányítás ugyanúgy lett megvalósítva, mint az OFFICE2LANRouter-en. A hirdetett hálózatban az eltérés annyi, hogy a 192.168.0.4/30-as hálózatot hirdetjük 0-ás areaba.

Kiterjesztett hozzáférési lista ugyanúgy lett felkonfigurálva.

#### Interface

Az interface hasonlóan lett felkonfigurálva, mint az OFFICE2LANRouteren. IP cím 172.16.0.2/24 kiadása az interface-re.

Az interface hasonlóan lett felkonfigurálva, mint az OFFICE2LANRouteren. IP cím 172.16.1.2/24 kiadása az interface-re.

Az ISP felé menő interfészre megadjuk a 195.195.0.14 ip címet, a többi beállítás hasonló az OFFICE2LANRouter beállításaihoz.

#### Zone Based Policy Firewall

A Tűzfal konfigurációját ugyanúgy készítettük el mint az OFFICE2LANRouter-en.

#### NAT/PAT

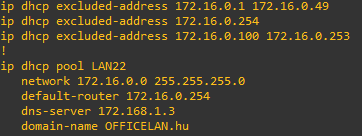
NAT konfigurációját ugyanúgy készítettük el mint az OFFICE2LANRouter-en.

#### Statikus Forgalomirányítás

****

Statikus alapértelmezett útvonal az isp irányába.

#### DHCP

****

*68. ábra DHCP konfiguráció. A kép saját szerkesztés.*

Lefoglaljuk a 172.16.0.254-es címet és a 172.16.0.1 és 172.16.0.49 közé eső címeket továbbá, lefoglaljuk a 172.16.0.100 és 172.16.0.253 közé eső címeket. Majd létrehozzuk a DHCP Pool-t LAN22 néven, megadjuk a networkot,deafult-routert, dns-servert és domin- namet.

#### OFFICE2LANSwitch

#### DHCP SNOOPING

****

A vlan1,22,24-en engedélyezzük a snoopingot. Továbbá engedélyzzük a globális használatát.

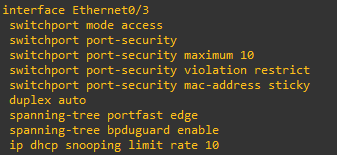
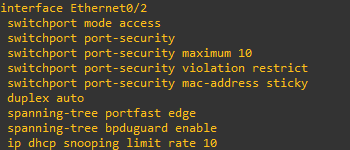
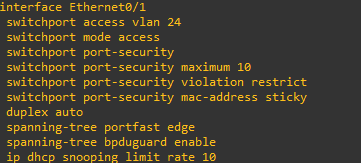


Az alábbi portokat: Port-channel1, Ethernet0/0 a megbízható módba kapcsoljuk. Illetve az Ethernet0/1-0/3ig bekapcsoljuk azt, hogy egy másodpercen belül hány dhcp kérést küldhetnek a porton.

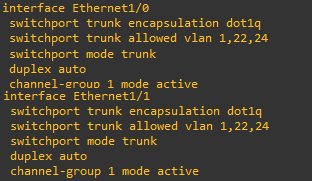
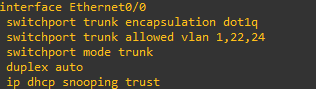
#### INTERFACES/SWITCHPORT/SPANNING-TREE/PORT-Security

***SEQ ábra \\* ARABIC 71****. ábra Interface konfiguráció. A kép saját*

A spanning-tree módját Rapid-PVST-be állítjuk.



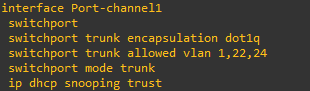
Hozzáférési módba helyezzük a portokat és az 24-es vlanhoz rendeljük. Bekapcsoljuk a Port-Security-it. A Maximum 10 darab különböző MAC címet tanulhat meg mielőtt error- disabled állapotba kerül a port. Biztonság megsértési módot restrict-re állítjuk. A MAC címeket Sticky tulajdonsággal megtanulja és megtartja az információkat. A portokon portfast-et állítunk be és bekapcsoljuk a bpduguardot. Továbba az Ethernet0/1-0/3ig bekapcsoljuk azt, hogy egy másodpercen belül hány dhcp kérést küldhetnek a porton.



*SEQ ábra \\* ARABIC 73. ábra Interface konfiguráció. A kép saját szerkesztés.*

A switcportokat trunk módba állítjuk és a keret beágyazást dot1q-ra állítjuk. Az 1,22,24 VLAN-ok forgalmát engedjük át. Az Ethernet0/0 portot megbízható módba kapcsoljuk. Az Ethernet1/0 és 1/1-et pedig 1-es csatorna csoportba helyezzük és kezdeményező állapotba helyezzük. LACP-t alkalmaztunk az Ethernchannelnél.

#### ETHERCHANNEL



Az Ethernet1/0 és 1/1-et pedig 1-es csatorna csoportba helyezzük és kezdeményező állapotba helyezzük. LACP-t alkalmaztunk az Ethernchannelnél. A Port-channel1-et Trunk módba állítjuk és a keret beágyazást dot1q-ra állítjuk. Az 1,22,24 VLAN-ok forgalmát engedjük át. Az portot megbízható módba kapcsoljuk.

#### OFFICE2LANSwitch-2

Az OFFICE1LANSwitch-2 eszközt ugyanúgy konfiguráltuk fel mint az OFFICE1LANSwitch-et.

# Programozott Hálózatkonfiguráció

Programozott Hálózatkonfigurációt python programozási nyelven valósítottuk meg és a paramiko segítségével készítettük el. SSH-n keresztül automatikusan felcsatlakozik a megfelelő jelszóval és névvel ezután pedig felkonfigurál egy DHCP szervert a OFFICE2LANRouteren, illetve az OFFICE2LANRouter-2 routeren konfigurál fel egy DHCP szervert a megfelelő paraméterekkel. Továbbá felkonfigurálja a a subinterfaceket megfelelő parancsok használatával.

#### OFFICE2LANRouter

**import paramiko import time**

**def commands):**

**configure\_router(host,**

**username, password,**

#### try:

#### ssh = paramiko.SSHClient()

#### ssh.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy(

**))**

#### ssh.connect(hostname=host, username=username, password=password)

#### shell = ssh.invoke\_shell() for command in commands:

#### shell.send(command + '\n') time.sleep(1)

#### output = shell.recv(65535).decode("utf-8") print(output)

#### ssh.close()

#### except Exception as e:

#### print (f"Hiba történt: {e}")

#### if name == " main ": router\_ip = "172.16.0.1" username = "admin"

#### password = "office2administrator\_"

#### config\_commands = [ "enable\n" "office2secret\n" "configure terminal\n ",

#### "ip dhcp excluded-address 172.16.0.1 172.16.0.99\n ",

#### "ip dhcp excluded-address 172.16.0.254\n " "ip dhcp excluded-address 172.16.0.150

#### 172.16.0.253\n "

#### "ip dhcp pool LAN22\n ",

#### "network 172.16.0.0 255.255.255.0\n ",

#### "default-router 172.16.0.254\n ", "dns-server 172.168.1.3\n ", "domain-name OFFICELAN.HU\n " "exit\n ",

#### "interface GigabitEthernet2/0.22\n " "encapsulation dot1Q 22\n "

#### "ip address 172.16.0.1 255.255.255.0\n " "ip nat inside\n "

#### "ip virtual-reassembly\n "

#### "zone-member security OFFICE2LAN\n " "glbp 22 ip 172.16.0.254\n "

#### "interface GigabitEthernet2/0.24" "encapsulation dot1Q 24\n "

#### "ip address 172.16.1.1 255.255.255.0\n " "ip nat inside\n "

**"ip virtual-reassembly\n "**

**"zone-member security OFFICE2LAN\n " "glbp 24 ip 172.16.1.254"**

**"exit" "end",**

**"write memory"**

**]**

**configure\_router(router\_ip, username, password, config\_commands)**

#### OFFICE2LANRouter-2

#### import paramiko import time

#### def configure\_router(host, username, password, commands):

#### try:

#### ssh = paramiko.SSHClient()

#### ssh.set\_missing\_host\_key\_policy(paramiko.AutoAddPolicy(

**))**

#### ssh.connect(hostname=host, username=username, password=password)

#### shell = ssh.invoke\_shell() for command in commands:

#### shell.send(command + '\n') time.sleep(1)

#### output = shell.recv(65535).decode("utf-8") print(output)

#### ssh.close()

#### except Exception as e:

#### print (f"Hiba történt: {e}")

#### if name == " main ": router\_ip = "172.16.0.2" username = "admin"

#### password = "office2administrator\_"

#### config\_commands = [ "enable\n " "office2secret\n " "configure terminal\n ",

#### "ip dhcp excluded-address 172.16.0.1 172.16.0.49\n ",

#### "ip dhcp excluded-address 172.16.0.254\n " "ip dhcp excluded-address 172.16.0.150

#### 172.16.0.253\n "

**"ip dhcp pool LAN22\n ",**

**"network 172.16.0.0 255.255.255.0\n ",**

**"default-router 172.16.0.254\n ", "dns-server 172.168.1.3\n ", "domain-name OFFICELAN.HU\n " "exit\n ",**

**"interface GigabitEthernet2/0.22\n " "encapsulation dot1Q 22\n "**

**"ip address 172.16.0.2 255.255.255.0\n " "ip nat inside\n "**

**"ip virtual-reassembly\n "**

**"zone-member security OFFICE2LAN\n " "glbp 22 ip 172.16.0.254\n "**

**"interface GigabitEthernet2/0.24\n " "encapsulation dot1Q 24\n "**

**"ip address 172.16.1.2 255.255.255.0\n " "ip nat inside\n "**

**"ip virtual-reassembly"**

**"zone-member security OFFICE2LAN\n " "glbp 24 ip 172.16.1.254\n "**

**"exit\n " "end\n ",**

**"write memory\n "**

**]**

**configure\_router(router\_ip, username,** **password, config\_commands)**

# Tesztelés

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Teszt Célja** | **Érintett Ezközök** | **Leírás** | **Várt Eredmény** | **Eredmény** |
| 2. Rétegbeli redundancia | OFFICE1LANSwitch, OFFICE1LANRouter, OFFICE1LANRouter-2 | Az OFFICE1LANSwitch-en lekapcsoljuk a FastEthernet0/3-at és az OFFICE1LANRouter-ről megpingeljük az OFFICE1LANRouter2  belső IP címét. | Az OFFICE1LANRouter sikeresen megpingeli az OFFICE1LANRouter2-  t. | A Pingelés sikeres. |
| GLBP | OFFICE2LANRouter,  OFFICE2 vlan22 pc, OFFICE1 Windows Server | Kikapcsoljuk az OFFICE2LANRouter gig2/0 interfészét. Majd az FFICE2 vlan22-ben lévő pc-ről megpingeljük  az OFFICE1 Windows Serverét | Az OFFICE2-ből a kliens sikeresen megpingeli az OFFICE1 Windows servert. | A Pingelés sikeres. |
| OSPF | OFFICE2LANRouter, OFFICE2 vlan22 pc, OFFIC1  Windows Server | Kikapcsoljuk az OFFICE2LANRouter gig2/0 interfészét. Majd az FFICE2 vlan22-ben lévő pc-ről megpingeljük  az OFFICE1 Windows Serverét | Az OFFICE2-ből a kliens sikeresen megpingeli az OFFICE1 Windows servert. | A Pingelés sikeres. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| VPN | OFFICE1LANRouter,  OFFICE2LANRouter | Az összes forgalom az OFFICE2-OFFICE1,  illetve OFFICE1- OFFICE2 irányába titkosítva lesz. ESP keretbe lesz beágyazva. Ezt WireShark capture-  val teszteljük. | A wireshark alkalmazásban látjuk az ESP csomagokat. | A Wireshark alkalmazásban látjuk az ESP csomagokat. |
| Tűzfal | OFFICE1 Windows Server, OFFICE2 Vlan22 PC | Az OFFICE1 Windows Server-ről megpingeljük az OFFICE2 vlan22 PC-  t. Majd ezután ezt megismételjük az OFFICE2 felől az OFFICE1 Felé. | Az OFFICE1-ből történő pingelés sikertelen lesz mivel a **tűzfal le tiltja az pingelést** az OFFICE1 teljes hálózatából a pingelést az OFFICE2- Be. Majd az OFFICE2- ből történő pingelést elvégezzük, amely  sikeres lesz. | Az első pingelés sikertelen. A második pedig sikeres. |
| HTTP/HTTPS | OFFICE1 vlan54 PC | Az OFFICE1 vlan54-es hálózatában lévő gépen böngésző használatával beírjuk az alábbi weboldal címet: [www.officelan.network,](http://www.officelan.network/) ez a http weboldalra fog irányítani. Majd a HTTPS Weboldalunkra kattintva átirányít a HTTPS weboldalra. | Sikeresen eléri az felhasználó a http, illetve a https weboldalt. | A felhasználó megnyitotta a weboldalt. |
| DHCP | OFFICE2 vlan22 PC,  OFFICE1 vlan54 pc, Linux Szerver, OFFICE2 Routerei. | Az OFFICE2 vlan22-ben lévő pc számára kérünk DHCP-t, amelyet a Routerek szolgáltatnak. Illetve az OFFICE1-en a vlan54-ben léőv pc számára kérünk DCHP, amelyet a Linux Szerver  biztosít. | Sikeresen megkapják az eszközök az IP-t. | Az eszközök megkapták az ip-t. |
| Active Directory | OFFICE1 vlan54 PC | Bejelentkezünk az OFFICE1 vlan54-es hálózatában lévő gépre bármely dolgozói fiókkal. Továbbá megtekintjük azt, hogy megkapta-e az Active  Directory által beállított háttérképet. | Sikeresen bejelentkezünk a fiókba és a megfelelő háttérkép van beállítva. | Bejelentkezett a felhasználó és az előre beállított háttérkép van beállítva. |
| Fájl És Nyomtatómegosztás | Linux Server, Windows Server | A Resources mappát a Linuxon hálózaton keresztül megosztjuk. Továbbá a Windows Szerveren keresztül megosztunk egy  nyomtatót. | A hálózaton lévő eszközök elérik a megosztott mappát. Illetve nyomtatót. | A felhasználok elérik a nyomtatót és a megosztott mappát |
| Automatizált mentés | Windows Server | A Windows serveren beállítottuk, hogy mindennap este 8-kor készítsen egy mentést a Samba által megosztott mappába. | Elkészül a mentés a Resources mappába | Mindennap est0 8 órakkor ment automatikusan. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Kliens Számítógépekre automatizált szoftvertelepítés | OFFICE1 vlan54 PC | Bejelentkezünk az OFFICE1 vlan54-es hálózatában lévő gépre bármely dolgozói fiókkal és automatikusan  feltelepül a Mozzilla Firefox. | Bejelentkezés után feltelepül a Böngésző. | A bejelentkezés után feltelepült a Böngésző. |

# Összefoglalás

A cég azért alapult meg, hogy innovatív megoldásokat nyújtson a virtuális infrastruktúrák, hálózatok és mérnöki szolgáltatások terén. A Projekt készítése alatt sok új tapasztalatra tettünk szert amelyet későbbi munkáink során fogunk tudni alkalmazni és hasznosítani. Elkészítettük a VTEC teljes hálózatát. Az egyik Telephely Debrecenben helyezkedik el a másik pedig Berlinben.

#### Tapasztalatok melyekre szert tettünk:

* A projekt készítése alatt sokat fejlődött a kommunikációs készségünk, csapatmunka, problémamegoldó képességünk. Továbbá a szakmai tudásunk fejlődött:
  + Megtanultunk felépíteni korszerű technológiák segítségével egy kisebb vállalati hálózatot.
  + OSPF, GLBP, NAT/PAT, VPN, GRE-TUNNEL, IPSEC, Spanning-tree,

VLAN, Port-Security, ZPF protokollok és használatával a switcheken és routereken, wifi routereken és access point eszközökön egyaránt fejlesztettük az ismereteinket.

* + Alkalmaznunk kellett megfelelő szervereket ezeket egy Linux és egy Windows szerver feltelepítésének a segítségével oldottuk meg, melyeknek a használat során megtanultuk az alábbi szolgáltatások alkalmazását, konfigurálását és működését:
    - Active Directory, DHCP, DNS, HTTP/HTTPS, Fájl és nyomtatómegosztás, Automatizált Szoftvertelepítés, Automatizált mentés

#### Projekt során felmerülő nehézségek, problémák:

* Tűzfal: A megfelelő forgalom engedélyezése a protokollok figyelembevételével. Például: Nem engedélyeztük az OfficeLAN2-Ből az

OfficeLAN1 felé menő HTTPS kéréseket, ezáltal az office2ből nem érték el a felhasználók a HTTPS oldalt.

* Automatizált Szoftvertelepítés: Egy megfelelő MSI Package találása okozott problémát mivel a legtöbb MSI, amit próbáltunk használni rendszergazdai jogosultságokat követelt a telepítéshez ez pedig problémát okozott egy átlag felhasználónak/dolgozónak, aki nem rendelkezik ilyen jogokkal.

A működőképes állapotról a videó elérhető az alábbi linken 2025.június 30.-ig: <https://drive.google.com/file/d/17jW94rCII507takyyrZfeMYl10EyV0o4/view?usp=sharing>

# Konfigurációs melléklet

#### OFFICE1LANRouter

#### hostname Office1LANRouter enable secret office1secret\_

#### username admin secret office1administrator\_ boot-start-marker

#### boot-end-marker

#### logging message-counter syslog no aaa new-model

#### ip source-route

#### no ip icmp rate-limit unreachable ip cef

#### no ip domain lookup ipv6 unicast-routing ipv6 cef

#### multilink bundle-name authenticated archive

#### log config hidekeys

#### crypto isakmp policy 10 encr aes 256 authentication pre-share group 14

#### lifetime 3600

#### crypto isakmp key OFFICETOOFFICE address 195.195.0.10 crypto ipsec transform-set OFFICETS esp-aes 256 esp-sha-

#### hmac

#### crypto map OFFICECM 10 ipsec-isakmp set peer 195.195.0.10

#### set security-association lifetime seconds 1800 set transform-set OFFICETS

#### set pfs group14

#### match address GREOVERIPSEC ip tcp synwait-time 5

#### class-map type inspect match-any OFFICE1LANTOOFFICE2LAN match access-group name OFFICE1LANTOOFFICE2LAN

#### class-map type inspect match-any LANACCESS match access-group name LANACCESS

#### class-map type inspect match-any WANACCESS match access-group name WANACCESS

#### policy-map type inspect OFFICE1LANTOOFFICE2LAN class type inspect OFFICE1LANTOOFFICE2LAN

#### inspect

#### class class-default drop

#### policy-map type inspect TOWAN class type inspect WANACCESS

#### inspect

#### class class-default drop

#### policy-map type inspect LANACCESS class type inspect LANACCESS

#### inspect

#### class class-default drop

#### zone security OFFICE2LAN zone security OFFICE1LAN zone security ISP

#### zone-pair security LANTOWAN source OFFICE1LAN destination ISP

#### service-policy type inspect TOWAN

#### zone-pair security OFFICE1LANTOOFFICE2LAN source OFFICE1LAN destination OFFICE2LAN

#### service-policy type inspect OFFICE1LANTOOFFICE2LAN

#### zone-pair security WANTOLANACCESS source ISP destination OFFICE1LAN

#### service-policy type inspect LANACCESS interface Tunnel0

#### ip address 192.168.0.1 255.255.255.252

#### zone-member security OFFICE2LAN tunnel source GigabitEthernet2/0 tunnel destination 195.195.0.10 crypto map OFFICECM

#### interface Ethernet0/0 no ip address shutdown

#### duplex auto

#### interface GigabitEthernet0/0 no ip address

#### shutdown duplex full speed 1000

#### media-type gbic negotiation auto

#### interface GigabitEthernet1/0 no ip address

#### negotiation auto

#### interface GigabitEthernet1/0.52 encapsulation dot1Q 52

#### ip address 172.168.0.1 255.255.255.0

#### ip helper-address 172.168.0.3 ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE1LAN ipv6 address FE80::54 link-local ipv6 address 2001:DB8:52:52::1/64

#### glbp 52 ip 172.168.0.254

#### glbp 52 load-balancing host-dependent interface GigabitEthernet1/0.54

#### encapsulation dot1Q 54

#### ip address 172.168.1.1 255.255.255.0

#### ip helper-address 172.168.0.3 ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE1LAN ipv6 address FE80::54 link-local ipv6 address 2001:DB8:54:54::1/64 glbp 54 ip 172.168.1.254

#### glbp 54 load-balancing host-dependent interface GigabitEthernet2/0

#### ip address 195.195.0.2 255.255.255.252

#### ip nat outside

#### ip virtual-reassembly zone-member security ISP negotiation auto

#### interface GigabitEthernet3/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet4/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet5/0 no ip address

#### shutdown negotiation auto

#### router ospf 1

#### log-adjacency-changes

#### passive-interface GigabitEthernet1/0.52 passive-interface GigabitEthernet1/0.54 passive-interface GigabitEthernet2/0 network 172.168.0.0 0.0.0.255 area 1

#### network 172.168.1.0 0.0.0.255 area 1

#### network 192.168.0.0 0.0.0.3 area 0 ip forward-protocol nd

#### ip route 0.0.0.0 0.0.0.0 195.195.0.1

#### no ip http server

#### no ip http secure-server

#### ip nat inside source list NAT interface GigabitEthernet2/0 overload

#### ip access-list standard NAT permit 172.168.0.0 0.0.1.255

#### ip access-list extended GREOVERIPSEC

#### permit ip 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255

#### ip access-list extended LANACCESS permit tcp any host 172.168.0.3 eq www

**permit tcp any host 172.168.0.3 eq 443**

**ip access-list extended OFFICE1LANTOOFFICE2LAN**

**deny icmp 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255**

**permit ip 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255**

**ip access-list extended WANACCESS permit ip 172.168.0.0 0.0.1.255 any**

**no cdp log mismatch duplex control-plane**

**gatekeeper shutdown line con 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous stopbits 1**

**line aux 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous stopbits 1**

**crypto key generate rsa 1024**

**line vty 0 4 login local**

**transport input ssh end**

#### OFFICE1LANRouter-2

**hostname Office1LANRouter2 enable secret office1secret\_**

**username admin secret office1administrator\_ boot-start-marker**

**boot-end-marker**

**logging message-counter syslog no aaa new-model**

**ip source-route**

**no ip icmp rate-limit unreachable ip cef**

**no ip domain lookup ipv6 unicast-routing ipv6 cef**

**multilink bundle-name authenticated archive**

**log config hidekeys**

**crypto isakmp policy 10 encr aes 256 authentication pre-share group 14**

**lifetime 3600**

**crypto isakmp key OFFICETOOFFICE address 195.195.0.14**

#### crypto ipsec transform-set OFFICETS esp-aes 256 esp-sha- hmac

#### crypto map OFFICECM 10 ipsec-isakmp set peer 195.195.0.14

#### set security-association lifetime seconds 1800 set transform-set OFFICETS

#### set pfs group14

#### match address GREOVERIPSEC ip tcp synwait-time 5

#### class-map type inspect match-any OFFICE1LANTOOFFICE2LAN match access-group name OFFICE1LANTOOFFICE2LAN

#### class-map type inspect match-any LANACCESS match access-group name LANACCESS

#### class-map type inspect match-any WANACCESS match access-group name WANACCESS

#### policy-map type inspect OFFICE1LANTOOFFICE2LAN class type inspect OFFICE1LANTOOFFICE2LAN

#### inspect

#### class class-default drop

#### policy-map type inspect TOWAN class type inspect WANACCESS

#### inspect

#### class class-default drop

#### policy-map type inspect LANACCESS class type inspect LANACCESS

#### inspect

#### class class-default drop

#### zone security OFFICE2LAN zone security OFFICE1LAN zone security ISP

#### zone-pair security LANTOWAN source OFFICE1LAN destination ISP

#### service-policy type inspect TOWAN

#### zone-pair security OFFICE1LANTOOFFICE2LAN source OFFICE1LAN destination OFFICE2LAN

#### service-policy type inspect OFFICE1LANTOOFFICE2LAN

#### zone-pair security OFFICE2LANTOOFFICE1LAN source OFFICE2LAN destination OFFICE1LAN

#### service-policy type inspect OFFICE1LANTOOFFICE2LAN

#### zone-pair security WANTOLANACCESS source ISP destination OFFICE1LAN

#### service-policy type inspect LANACCESS interface Tunnel0

#### ip address 192.168.0.5 255.255.255.252

#### zone-member security OFFICE2LAN tunnel source GigabitEthernet2/0 tunnel destination 195.195.0.14 crypto map OFFICECM

#### interface FastEthernet0/0 no ip address

#### shutdown duplex half

#### interface GigabitEthernet1/0 no ip address

#### negotiation auto

#### interface GigabitEthernet1/0.52 encapsulation dot1Q 52

#### ip address 172.168.0.2 255.255.255.0

#### ip helper-address 172.168.0.3 ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE1LAN ipv6 address FE80::55 link-local ipv6 address 2001:DB8:52:52::2/64 glbp 52 ip 172.168.0.254

#### interface GigabitEthernet1/0.54 encapsulation dot1Q 54

#### ip address 172.168.1.2 255.255.255.0

#### ip helper-address 172.168.0.3 ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE1LAN ipv6 address FE80::55 link-local ipv6 address 2001:DB8:54:54::2/64 glbp 54 ip 172.168.1.254

#### interface GigabitEthernet2/0

#### ip address 195.195.0.6 255.255.255.252

#### ip nat outside

#### ip virtual-reassembly zone-member security ISP negotiation auto

#### interface GigabitEthernet3/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet4/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet5/0 no ip address

#### shutdown negotiation auto

#### router ospf 1

#### log-adjacency-changes

#### passive-interface GigabitEthernet1/0.52 passive-interface GigabitEthernet1/0.54 network 172.168.0.0 0.0.0.255 area 1

#### network 172.168.1.0 0.0.0.255 area 1

#### network 192.168.0.4 0.0.0.3 area 0 ip forward-protocol nd

#### ip route 0.0.0.0 0.0.0.0 195.195.0.5

#### no ip http server

#### no ip http secure-server

#### ip nat inside source list NAT interface GigabitEthernet2/0 overload

#### ip access-list standard NAT permit 172.168.0.0 0.0.1.255

#### ip access-list extended GREOVERIPSEC

#### permit ip 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255

#### ip access-list extended LANACCESS permit tcp any host 172.168.0.3 eq www permit tcp any host 172.168.0.3 eq 443

#### ip access-list extended OFFICE1LANTOOFFICE2LAN

#### deny icmp 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255

#### permit ip 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255

#### permit ip 172.16.0.0 0.0.1.255 172.168.0.0 0.0.1.255

#### ip access-list extended WANACCESS permit ip 172.168.0.0 0.0.1.255 any

#### no cdp log mismatch duplex control-plane

#### gatekeeper shutdown line con 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### line aux 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### crypto key generate rsa 1024

#### line vty 0 4 login local

#### transport input ssh end

#### OFFICE2LANRouter

**hostname Office2Router2 enable secret office2secret\_**

**username admin secret office2administrator\_ boot-start-marker**

**boot-end-marker**

#### logging message-counter syslog no aaa new-model

#### ip source-route

#### no ip icmp rate-limit unreachable ip cef

#### ip dhcp excluded-address 172.16.0.1 172.16.0.49 ip dhcp excluded-address 172.16.0.254

#### ip dhcp excluded-address 172.16.0.100 172.16.0.253 ip dhcp pool LAN22

#### network 172.16.0.0 255.255.255.0

#### default-router 172.16.0.254

#### dns-server 172.168.1.3 domain-name OFFICELAN.hu

#### no ip domain lookup no ipv6 cef

#### multilink bundle-name authenticated archive

#### log config hidekeys

#### crypto isakmp policy 10 encr aes 256 authentication pre-share group 14

#### lifetime 3600

#### crypto isakmp key OFFICETOOFFICE address 195.195.0.6 crypto ipsec transform-set OFFICETS esp-aes 256 esp-sha-

#### hmac

#### crypto map OFFICECM 10 ipsec-isakmp set peer 195.195.0.6

#### set security-association lifetime seconds 1800 set transform-set OFFICETS

#### set pfs group14

#### match address GREOVERIPSEC ip tcp synwait-time 5

#### class-map type inspect match-any OFFICE2LANTOOFFICE1LAN match access-group name OFFICE2LANTOOFFICE1LAN

#### class-map type inspect match-any WANACCESS match access-group name WANACCESS

#### policy-map type inspect OFFICE2LANTOOFFICE1LAN class type inspect OFFICE2LANTOOFFICE1LAN

#### inspect

#### class class-default drop

#### policy-map type inspect TOWAN class type inspect WANACCESS

#### inspect

#### class class-default drop

#### zone security OFFICE2LAN zone security OFFICE1LAN zone security ISP

#### zone-pair security LANTOWAN source OFFICE2LAN destination ISP

#### service-policy type inspect TOWAN

#### zone-pair security OFFICE2LANTOOFFICE1LAN source OFFICE2LAN destination OFFICE1LAN

#### service-policy type inspect OFFICE2LANTOOFFICE1LAN

#### zone-pair security OFFICE1LANTOOFFICE2LAN source OFFICE1LAN destination OFFICE2LAN

#### service-policy type inspect OFFICE2LANTOOFFICE1LAN interface Tunnel0

#### ip address 192.168.0.6 255.255.255.252

#### zone-member security OFFICE1LAN tunnel source GigabitEthernet1/0 tunnel destination 195.195.0.6 crypto map OFFICECM

#### interface FastEthernet0/0 no ip address

#### shutdown duplex half

#### interface GigabitEthernet1/0

#### ip address 195.195.0.14 255.255.255.252

#### ip nat outside

#### ip virtual-reassembly zone-member security ISP negotiation auto

#### interface GigabitEthernet1/0.22 zone-member security OFFICE2LAN

#### interface GigabitEthernet1/0.24 zone-member security OFFICE2LAN

#### interface GigabitEthernet2/0 no ip address

#### zone-member security ISP negotiation auto

#### interface GigabitEthernet2/0.22 encapsulation dot1Q 22

#### ip address 172.16.0.1 255.255.255.0

#### ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE2LAN glbp 22 ip 172.16.0.254

#### interface GigabitEthernet2/0.24 encapsulation dot1Q 24

#### ip address 172.16.1.1 255.255.255.0

#### ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE2LAN glbp 24 ip 172.16.1.254

#### interface GigabitEthernet3/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet4/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet5/0 no ip address

#### shutdown negotiation auto

#### router ospf 1

#### log-adjacency-changes

#### passive-interface GigabitEthernet2/0.22 passive-interface GigabitEthernet2/0.24 network 172.16.0.0 0.0.0.255 area 2

#### network 172.16.1.0 0.0.0.255 area 2

#### network 192.168.0.4 0.0.0.3 area 0 ip forward-protocol nd

#### ip route 0.0.0.0 0.0.0.0 195.195.0.13

#### no ip http server

#### no ip http secure-server

#### ip nat inside source list NAT interface GigabitEthernet1/0 overload

#### ip access-list standard NAT permit 172.16.0.0 0.0.1.255

#### ip access-list extended GREOVERIPSEC

#### permit ip 172.16.0.0 0.0.1.255 172.168.0.0 0.0.1.255

#### ip access-list extended OFFICE2LANTOOFFICE1LAN

#### permit ip 172.16.0.0 0.0.1.255 172.168.0.0 0.0.1.255

#### permit ip 172.168.0.0 0.0.1.255 172.16.0.0 0.0.1.255

#### ip access-list extended WANACCESS permit ip 172.16.0.0 0.0.1.255 any

#### no cdp log mismatch duplex control-plane

#### gatekeeper shutdown line con 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### line aux 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### crypto key generate rsa 1024

#### line vty 0 4 login local

#### transport input ssh end

#### OFFICE2LANRouter-2

#### hostname Office2Router enable secret office2secret\_

#### username admin secret office2administrator\_ boot-start-marker

#### boot-end-marker

#### logging message-counter syslog no aaa new-model

#### ip source-route

#### no ip icmp rate-limit unreachable ip cef

#### ip dhcp excluded-address 172.16.0.254

#### ip dhcp excluded-address 172.16.0.1 172.16.0.99

#### ip dhcp excluded-address 172.16.0.150 172.16.0.253 ip dhcp pool LAN22

#### network 172.16.0.0 255.255.255.0

#### default-router 172.16.0.254

#### dns-server 172.168.1.3 domain-name OFFICELAN.hu

#### no ip domain lookup no ipv6 cef

#### multilink bundle-name authenticated archive

#### log config hidekeys

#### crypto isakmp policy 10 encr aes 256 authentication pre-share group 14

#### lifetime 3600

#### crypto isakmp key OFFICETOOFFICE address 195.195.0.2 crypto ipsec transform-set OFFICETS esp-aes 256 esp-sha-

#### hmac

#### crypto map OFFICECM 10 ipsec-isakmp set peer 195.195.0.2

#### set security-association lifetime seconds 1800 set transform-set OFFICETS

#### set pfs group14

#### match address GREOVERIPSEC ip tcp synwait-time 5

#### class-map type inspect match-any OFFICE2LANTOOFFICE1LAN match access-group name OFFICE2LANTOOFFICE1LAN

#### class-map type inspect match-any WANACCESS match access-group name WANACCESS

#### policy-map type inspect OFFICE2LANTOOFFICE1LAN class type inspect OFFICE2LANTOOFFICE1LAN

#### inspect

#### class class-default drop

#### policy-map type inspect TOWAN class type inspect WANACCESS

#### inspect

#### class class-default drop

#### zone security OFFICE2LAN zone security OFFICE1LAN zone security ISP

#### zone-pair security LANTOWAN source OFFICE2LAN destination ISP

#### service-policy type inspect TOWAN

#### zone-pair security OFFICE2LANTOOFFICE1LAN source OFFICE2LAN destination OFFICE1LAN

#### service-policy type inspect OFFICE2LANTOOFFICE1LAN interface Tunnel0

#### ip address 192.168.0.2 255.255.255.252

#### zone-member security OFFICE1LAN tunnel source GigabitEthernet1/0 tunnel destination 195.195.0.2 crypto map OFFICECM

#### interface FastEthernet0/0 no ip address

#### shutdown duplex half

#### interface GigabitEthernet1/0

#### ip address 195.195.0.10 255.255.255.252

#### ip nat outside

#### ip virtual-reassembly zone-member security ISP negotiation auto

#### interface GigabitEthernet2/0 no ip address

#### negotiation auto

#### interface GigabitEthernet2/0.22 encapsulation dot1Q 22

#### ip address 172.16.0.2 255.255.255.0

#### ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE2LAN glbp 22 ip 172.16.0.254

#### interface GigabitEthernet2/0.24 encapsulation dot1Q 24

#### ip address 172.16.1.2 255.255.255.0

#### ip nat inside

#### ip virtual-reassembly

#### zone-member security OFFICE2LAN glbp 24 ip 172.16.1.254

#### interface GigabitEthernet3/0 no ip address

#### shutdown negotiation auto

#### interface GigabitEthernet4/0 no ip address

#### shutdown

#### negotiation auto router ospf 1

#### log-adjacency-changes

#### passive-interface GigabitEthernet2/0.22 passive-interface GigabitEthernet2/0.24 network 172.16.0.0 0.0.0.255 area 2

#### network 172.16.1.0 0.0.0.255 area 2

#### network 192.168.0.0 0.0.0.3 area 0 ip forward-protocol nd

#### ip route 0.0.0.0 0.0.0.0 195.195.0.9

#### no ip http server

#### no ip http secure-server

#### ip nat inside source list NAT interface GigabitEthernet1/0 overload

#### ip access-list standard NAT permit 172.16.0.0 0.0.1.255

#### ip access-list extended GREOVERIPSEC

#### permit ip 172.16.0.0 0.0.1.255 172.168.0.0 0.0.1.255

#### ip access-list extended OFFICE2LANTOOFFICE1LAN

#### permit ip 172.16.0.0 0.0.1.255 172.168.0.0 0.0.1.255

#### ip access-list extended WANACCESS permit ip 172.16.0.0 0.0.1.255 any

#### no cdp log mismatch duplex control-plane

#### gatekeeper shutdown line con 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### line aux 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous stopbits 1

#### crypto key generate rsa 1024

#### line vty 0 4 login local

#### transport input ssh end

#### OFFICE1LANSwitch

**hostname OFFICE1LANSwitch enable secret office1secret\_**

**username admin secret office1administrator\_ boot-start-marker**

**boot-end-marker**

**logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL**

#### logging buffered 50000

#### logging console discriminator EXCESS no aaa new-model

#### no ip icmp rate-limit unreachable no ip cef

#### no ip domain-lookup

#### ip dhcp snooping vlan 1,52,54 ip dhcp snooping

#### no ipv6 cef

#### spanning-tree mode rapid-pvst spanning-tree extend system-id

#### vlan internal allocation policy ascending ip tcp synwait-time 5

#### interface Port-channel1 switchport

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### ip dhcp snooping trust interface Ethernet0/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### ip dhcp snooping trust interface Ethernet0/1

#### switchport access vlan 54 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky

#### switchport port-security mac-address sticky 0800.27eb.9bec

#### duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/2 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/3 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet1/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/1

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/2

#### duplex auto interface Ethernet1/3

#### duplex auto interface Ethernet2/0

#### duplex auto interface Ethernet2/1

#### duplex auto interface Ethernet2/2

#### duplex auto interface Ethernet2/3

#### duplex auto interface Ethernet3/0

#### duplex auto interface Ethernet3/1

#### duplex auto interface Ethernet3/2

#### duplex auto interface Ethernet3/3

#### duplex auto interface Vlan1

#### no ip address shutdown

#### ip forward-protocol nd no ip http server control-plane

#### line con 0

#### exec-timeout 0 0

#### privilege level 15 logging synchronous

#### line aux 0

#### exec-timeout 0 0

**privilege level 15 logging synchronous**

**crypto key generate rsa 1024**

**line vty 0 4 login local**

**transport input ssh end**

#### OFFICE1LANSwitch-2

#### hostname OFFICE1LANSwitch2 enable secret office1secret\_

#### username admin secret office1administrator\_ boot-start-marker

#### boot-end-marker

#### logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

#### logging buffered 50000

#### logging console discriminator EXCESS no aaa new-model

#### no ip routing

#### no ip icmp rate-limit unreachable no ip cef

#### no ip domain-lookup

#### ip dhcp snooping vlan 1,52,54 ip dhcp snooping

#### no ipv6 cef

#### spanning-tree mode rapid-pvst spanning-tree extend system-id

#### vlan internal allocation policy ascending ip tcp synwait-time 5

#### interface Port-channel1 switchport

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### ip dhcp snooping trust interface Ethernet0/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### ip dhcp snooping trust interface Ethernet0/1

#### switchport access vlan 52 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky

#### switchport port-security mac-address sticky 0800.2792.477d

#### duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping trust

#### interface Ethernet0/2 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/3 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet1/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/1

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,52,54 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/2

#### duplex auto interface Ethernet1/3

#### duplex auto interface Ethernet2/0

#### duplex auto interface Ethernet2/1

#### duplex auto interface Ethernet2/2

#### duplex auto interface Ethernet2/3

#### duplex auto interface Ethernet3/0

**duplex auto interface Ethernet3/1**

**duplex auto interface Ethernet3/2**

**duplex auto interface Ethernet3/3**

**duplex auto interface Vlan1**

**no ip address**

**no ip route-cache shutdown**

**ip forward-protocol nd no ip http server control-plane**

**line con 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**line aux 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**crypto key generate rsa 1024**

**line vty 0 4 login local**

**transport input ssh end**

#### OFFICE2LANSwitch

**hostname OFFICE2LANSwitch enable secret office2secret\_**

**username admin secret office2administrator\_ boot-start-marker**

**boot-end-marker**

**logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL**

**logging buffered 50000**

**logging console discriminator EXCESS no aaa new-model**

**no ip routing**

**no ip icmp rate-limit unreachable no ip cef**

**no ip domain-lookup**

**ip dhcp snooping vlan 1,22,24 ip dhcp snooping**

**no ipv6 cef**

**spanning-tree mode rapid-pvst spanning-tree extend system-id**

**vlan internal allocation policy ascending ip tcp synwait-time 5**

#### interface Port-channel1 switchport

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### ip dhcp snooping trust interface Ethernet0/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### duplex auto

#### ip dhcp snooping trust interface Ethernet0/1

#### switchport access vlan 24 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/2 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/3 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet1/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/1

#### switchport trunk encapsulation dot1q

**switchport trunk allowed vlan 1,22,24 switchport mode trunk**

**duplex auto**

**channel-group 1 mode active interface Ethernet1/2**

**duplex auto interface Ethernet1/3**

**duplex auto interface Ethernet2/0**

**duplex auto interface Ethernet2/1**

**duplex auto interface Ethernet2/2**

**duplex auto interface Ethernet2/3**

**duplex auto interface Ethernet3/0**

**duplex auto interface Ethernet3/1**

**duplex auto interface Ethernet3/2**

**duplex auto interface Ethernet3/3**

**duplex auto interface Vlan1**

**no ip address**

**no ip route-cache shutdown**

**ip forward-protocol nd no ip http server control-plane**

**line con 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**crypto key generate rsa 1024**

**line aux 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**line vty 0 4 login local**

**transport input ssh end**

#### OFFICE2LANSwitch-2

**hostname OFFICE2LANSwitch2 enable secret office2secret\_**

#### username admin secret office2administrator\_ boot-start-marker

#### boot-end-marker

#### logging discriminator EXCESS severity drops 6 msg-body drops EXCESSCOLL

#### logging buffered 50000

#### logging console discriminator EXCESS no aaa new-model

#### no ip routing

#### no ip icmp rate-limit unreachable no ip cef

#### no ip domain-lookup

#### ip dhcp snooping vlan 1,22,24 ip dhcp snooping

#### no ipv6 cef

#### spanning-tree mode rapid-pvst spanning-tree extend system-id

#### vlan internal allocation policy ascending ip tcp synwait-time 5

#### interface Port-channel1 switchport

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### ip dhcp snooping trust interface Ethernet0/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### duplex auto

#### ip dhcp snooping trust interface Ethernet0/1

#### switchport access vlan 22 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky

#### switchport port-security mac-address sticky 0800.2725.04d3

#### duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/2 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet0/3 switchport mode access switchport port-security

#### switchport port-security maximum 10 switchport port-security violation restrict switchport port-security mac-address sticky duplex auto

#### spanning-tree portfast edge spanning-tree bpduguard enable ip dhcp snooping limit rate 10

#### interface Ethernet1/0

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/1

#### switchport trunk encapsulation dot1q switchport trunk allowed vlan 1,22,24 switchport mode trunk

#### duplex auto

#### channel-group 1 mode active interface Ethernet1/2

#### duplex auto interface Ethernet1/3

#### duplex auto interface Ethernet2/0

#### duplex auto interface Ethernet2/1

#### duplex auto interface Ethernet2/2

#### duplex auto interface Ethernet2/3

#### duplex auto interface Ethernet3/0

#### duplex auto interface Ethernet3/1

#### duplex auto interface Ethernet3/2

#### duplex auto interface Ethernet3/3

#### duplex auto interface Vlan1

#### no ip address

#### no ip route-cache shutdown

#### ip forward-protocol nd no ip http server

**control-plane line con 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**crypto key generate rsa 1024**

**line aux 0**

**exec-timeout 0 0**

**privilege level 15 logging synchronous**

**line vty 0 4 login local**

**transport input ssh end**

#### Linux Server

#### sudo apt install isc-dhcp-server nano /etc/dhcp/dhcpd.conf

#### subnet 172.168.1.0 netmask 255.255.255.0 {

#### range 172.168.1.50 172.168.1.100;

#### option routers 172.168.1.254;

#### option domain-name-servers 172.168.1.3;

#### option broadcast-address 172.168.1.255;

#### default-lease-time 600;

#### max-lease-time 7200;

**}**

#### subnet 172.168.0.0 netmask 255.255.255.0 {

#### range 172.168.0.50 172.168.0.100;

#### option routers 172.168.0.254;

#### option domain-name-servers 172.168.1.3;

#### option broadcast-address 172.168.1.255;

#### default-lease-time 600;

#### max-lease-time 7200;

**}**

#### nano /etc/default/isc-dhcp-server

#### INTERFACESv4=”enp0s3”

#### apt install samba

#### mkdir /srv/OFFICESHARE/

#### mkdir /srv/OFFICESHARE/Resources chmod -R 770 /srv/OFFICESHARE/ groupadd officesambausers

#### usermod -aG officesambausers shared usermod -aG officesambausers officeadmin nano /etc/samba/smb.conf

#### [Resources]

#### comment = This is where the officeLAN stores their resources path = /srv/OFFICESHARE/Resources

#### read only = no browseable = yes create mask = 0660

#### directory mask = 0770 guest ok = no

#### chown officeadmin:officesambausers OFFICESHARE chown officeadmin:officesambausers Resources sudo systemctl restart smbd

#### sudo ufw allow 'Samba' sudo ufw reload

#### sudo ufw enable

#### sudo smbpasswd -a shared sudo systemctl restart smbd apt install apache2

#### ufw allow ’Apache’

#### nano /var/www/html/index.html

#### <!DOCTYPE html>

#### <html lang="hu">

#### <head>

#### <meta charset="UTF-8">

#### <meta name="viewport" content="width=device-width, initial-scale=1.0">

#### <title>Virtual Technology Engineering Company</title>

#### <link [href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist](https://cdn.jsdelivr.net/npm/bootstrap%405.3.0/dist)

#### /css/bootstrap.min.css" rel="stylesheet">

#### <script [src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/](https://cdn.jsdelivr.net/npm/bootstrap%405.3.0/dist/) js/bootstrap.bundle.min.js"></script>

#### </head>

#### <body class="bg-light text-center py-5">

#### <nav class="navbar navbar-expand-lg navbar-dark bg- dark">

#### <div class="container">

#### <a class="navbar-brand" href="#">VTEC</a>

#### <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false" aria- label="Toggle navigation">

#### <span class="navbar-toggler-icon"></span>

#### </button>

#### <div class="collapse navbar-collapse" id="navbarNav">

#### <ul class="navbar-nav ms-auto">

#### <li class="nav-item"><a class="nav-

#### link" href="#">Kezdőlap</a></li>

#### <li class="nav-item"><a class="nav- link" href="#">HTTPS Weboldalunk</a></li>

#### <li class="nav-item dropdown">

#### <a class="nav-link dropdown- toggle" href="#" id="authDropdown" role="button" data- bs-toggle="dropdown" aria-expanded="false">

#### Bejelentkezés / Regisztráció

#### </a>

#### <div class="dropdown-menu dropdown-menu-end p-4" style="width: 300px;">

#### <ul class="nav nav-tabs" id="authTabs" role="tablist">

#### role="presentation">

#### <li class="nav-item"

#### <button class="nav-

#### link active" id="login-tab" data-bs-toggle="tab" data- bs-target="#login" type="button" role="tab">Bejelentkezés</button>

#### </li>

#### <li class="nav-item"

#### role="presentation">

#### <button class="nav-

#### link" id="register-tab" data-bs-toggle="tab" data-bs- target="#register" type="button" role="tab">Regisztráció</button>

#### </li>

#### </ul>

#### <div class="tab-content mt-3"

#### id="authTabsContent">

#### <div class="tab-pane fade

#### show active" id="login" role="tabpanel">

#### <h5 class="mb-

#### 3">Bejelentkezés</h5>

#### <form>

#### <div class="mb-3">

#### <label

#### for="email" class="form-label">Email cím</label>

#### <input type="email" class="form-control" id="email" placeholder="Email">

#### </div>

#### <div class="mb-3">

#### <label for="password" class="form-label">Jelszó</label>

#### <input type="password" class="form-control" id="password" placeholder="Jelszó">

#### </div>

#### <button type="submit" class="btn btn-primary w- 100">Bejelentkezés</button>

#### </form>

#### </div>

#### <div class="tab-pane fade" id="register" role="tabpanel">

#### 3">Regisztráció</h5>

#### <h5 class="mb-

#### <form>

#### <div class="mb-3">

#### <label for="reg-email" class="form-label">Email cím</label>

#### <input type="email" class="form-control" id="reg-email" placeholder="Email">

#### </div>

#### <div class="mb-3">

#### <label for="reg-password" class="form-label">Jelszó</label>

#### <input type="password" class="form-control" id="reg-password" placeholder="Jelszó">

#### </div>

#### <button type="submit" class="btn btn-success w- 100">Regisztráció</button>

#### </form>

#### </div>

#### </div>

#### </div>

#### </li>

#### </ul>

#### </div>

#### </div>

#### </nav>

#### <div class="container bg-white p-4 rounded shadow mt- 4">

#### <h1 class="mb-3">Virtual Technology Engineering Company</h1>

#### <h2 class="mt-4">Cégbemutatás</h2>

#### <p>A Virtual Technology Engineering Company (VTEC) egy vezető technológiai vállalat, amely innovatív megoldásokat nyújt a virtuális infrastruktúrák, hálózatok és mérnöki szolgáltatások terén. </p>

#### <p>A Vállalat 2024-ben lett alapítva Debrecenben. A vállalat két irodát működtet: az egyik Debrecenben (Office 1), a másik pedig Berlinben (Office 2). A két iroda közötti kommunikáció biztosítására egy GRE Tunnel áll rendelkezésre. </p>

#### <p>Ezek az irodák korszerű hálózati technológiákkal vannak felszerelve, amelyek biztosítják az adatkezelés és a kommunikáció hatékonyságát. </p>

#### <p>A Vállalat hálózat karbantartással, építéssel, fejlesztéssel, weboldalak üzemeltetésével foglalkozik.

#### </p>

#### </div>

#### <footer class="bg-dark text-white text-center py-3 mt- 5">

#### <p class="mb-0">&copy; 2025 Virtual Technology Engineering Company. Minden jog fenntartva.</p>

**</footer>**

**</body>**

**</html>**

# Források

[What Is Microsegmentation? - Palo Alto Networks](https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation) 2025.02.03

[Cisco 2811 Integrated Services Router - Cisco Community](https://community.cisco.com/t5/networking-knowledge-base/cisco-2811-integrated-services-router/ta-p/3116259) 2025.02.03 [https://drive.google.com/file/d/1mzgXdbv5FJQrf0wYs7vPH4XYZKB5Ta](https://drive.google.com/file/d/1mzgXdbv5FJQrf0wYs7vPH4XYZKB5TaYb/view?usp=sharing)

[Yb/view?usp=sharing](https://drive.google.com/file/d/1mzgXdbv5FJQrf0wYs7vPH4XYZKB5TaYb/view?usp=sharing) 2025.02.03

[https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-](https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-%20kulcsfontossagu-eszkoze/) [kulcsfontossagu-eszkoze/](https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-%20kulcsfontossagu-eszkoze/) 2025.02.05

[https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-](https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-kulcsfontossagu-eszkoze/) [kulcsfontossagu-eszkoze/](https://controlblog.hu/access-point-ap-a-vezetek-nelkuli-halozatok-kulcsfontossagu-eszkoze/) 2025.02.05

[https://hu.wikipedia.org/wiki/Virtu%C3%A1lis\_helyi\_h%C3%A1l%C3%](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_helyi_h%C3%A1l%C3%B3zat)

[B3zat](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_helyi_h%C3%A1l%C3%B3zat) 2025.02.11

[https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/etherchannel.pdf) [4SY/config\_guide/sup6T/15\_3\_sy\_swcg\_6T/etherchannel.pdf](https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst6500/ios/15-4SY/config_guide/sup6T/15_3_sy_swcg_6T/etherchannel.pdf) 2025.02.11

<https://study-ccna.com/port-security/> 2025.02.16 [https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-](https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html)

[area-network.html](https://www.cisco.com/c/en/us/products/switches/what-is-a-wan-wide-area-network.html) 2025.02.17

<https://docs.freebsd.org/hu/books/handbook/firewalls/> 2025.02.24 [https://hu.wikipedia.org/wiki/Virtu%C3%A1lis\_mag%C3%A1nh%C3%A](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat)

[1l%C3%B3zat](https://hu.wikipedia.org/wiki/Virtu%C3%A1lis_mag%C3%A1nh%C3%A1l%C3%B3zat) 2025.02.29

<https://www.nwkings.com/what-is-router-on-a-stick> 2025.02.29 [https://fiberroad.com/resources/glossary/what-is-dhcp-snooping-and-why-](https://fiberroad.com/resources/glossary/what-is-dhcp-snooping-and-why-should-you-use-it/)

[should-you-use-it/](https://fiberroad.com/resources/glossary/what-is-dhcp-snooping-and-why-should-you-use-it/) 2025.03.01 [https://www.digihost.hu/knowledgebase/20/Mitl-redundans-](https://www.digihost.hu/knowledgebase/20/Mitl-redundans-egyhalozat.html)

[egyhalozat.html](https://www.digihost.hu/knowledgebase/20/Mitl-redundans-egyhalozat.html) 2025.03.01

<https://www.ruijienetworks.com/support/tech-gallery/what-is-a-switchport> <https://bytech.hu/dhcp/> 2025.03.01 [https://drive.google.com/file/d/10MJPURiHBIvjjCOrbIZvrcSFLUxM3Ss/vie](https://drive.google.com/file/d/10MJPURiHBIvjjCOrbIZvrcSFLUxM3Ss/view?usp=sharing)

[w?usp=sharing](https://drive.google.com/file/d/10MJPURiHBIvjjCOrbIZvrcSFLUxM3Ss/view?usp=sharing) 2025.03.09

<https://hu.wikipedia.org/wiki/Samba_(szoftver)> 2025.03.09

[https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) [protocol-http/](https://www.cloudflare.com/learning/ddos/glossary/hypertext-transfer-protocol-http/) 2025.03.13

[https://community.cisco.com/t5/switching/glbp-round-robin-load-](https://community.cisco.com/t5/switching/glbp-round-robin-load-balancing/td-p/2126138) [balancing/td-p/2126138](https://community.cisco.com/t5/switching/glbp-round-robin-load-balancing/td-p/2126138) 2025.03.15

<https://www.cloudflare.com/learning/network-layer/what-is-gre-tunneling/> 2025.03.16